KNACK BOX

Higher Education Risk Management

จัดการความเสี่ยงอย่างไร ให้มหาวิทยาลัยบรรลุเป้าหมาย

อวิรุทธ์ ฉัตรมาลาทอง

ขับเคลื่อนมหาวิทยาลัยให้บรรลุเป้าหมายภายใต้ภูมิทัศน์และบริบทใหม่
ด้วยเครื่องมือ Risk Management ที่จะทำให้ผู้บริหารนำองค์กร
อย่างมีประสิทธิภาพ พร้อมสร้างโอกาสและผลลัพธ์ใหม่

Higher Education Risk Management

จัดการความเสี่ยงอย่างไร ให้มหาวิทยาลัยบรรลุเป้าหมาย

อวิรุทธ์ ฉัตรมาลาทอง
Page Knack Box: กล่องขนมสมองของนักเรียนรู้

ขับเคลื่อนมหาวิทยาลัยให้บรรลุเป้าหมายภายใต้ภูมิทัศน์และบริบทใหม่
ด้วยเครื่องมือ Rick Management ที่จะทำให้ผู้บริหารนำองค์กร
อย่างมีประสิทธิภาพ พร้อมสร้างโอกาสและผลลัพธ์ใหม่

จัดการความเสี่ยงอย่างไร ให้มหาวิทยาลัยบรรลุเป้าหมาย

Higher Education Risk Management

ผู้เขียน : ดร.อวิรุทธ์ ฉัตรมาลาทอง
บรรณาธิการ : ไพลิน มู้จันทร์
พิสูจน์อักษร : ชุติกาญจน์ ดีกระจ่าง และทีมงานคุณภาพสำนักพิมพ์วิช
ออกแบบปกและรูปเล่ม : ทีมงานคุณภาพสำนักพิมพ์วิช

ISBN 978-616-612-731-7
พิมพ์ครั้งที่ 1 มิถุนายน 2567

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

อวิรุทธ์ ฉัตรมาลาทอง.
จัดการความเสี่ยงอย่างไร ให้มหาวิทยาลัยบรรลุเป้าหมาย = Higher Education Risk Management.-- กรุงเทพฯ : ม.ป.พ., 2567.
192 หน้า.

1. การศึกษาขั้นอุดมศึกษา -- การบริหาร. 2. การบริหารความเสี่ยง. I. ชื่อเรื่อง.

378.1
ISBN 978-616-612-731-7

จัดทำโดย

ดร.อวิรุทธ์ ฉัตรมาลาทอง
59/289 หมู่บ้านชนันธรกรีนวิลล์ ซอย 7 ถนนบางบอน 3 แขวงหนองแขม เขตหนองแขม กรุงเทพมหานคร
โทรศัพท์: 08 6416 1566

คำนำ

ภายใต้ภูมิทัศน์ของอุดมศึกษา (higher education landscape) ที่เปลี่ยนไป มหาวิทยาลัยทุกแห่งทั่วโลกต่างเผชิญกับความเสี่ยงและโอกาสใหม่ ๆ ประกอบกับสภาพแวดล้อมทั้งภายในและภายนอกมหาวิทยาลัย ไม่ว่าจะเป็น โครงสร้างประชากร เทคโนโลยีดิจิทัล โมเดลทางการศึกษาและการเรียนรู้ สภาพเศรษฐกิจและสังคม นโยบายและกฎหมาย แนวโน้มอุตสาหกรรมและตลาดแรงงาน ล้วนต่างกดดันมหาวิทยาลัยอย่างรอบด้าน เป็นสาเหตุให้มหาวิทยาลัยต้องปรับรูปแบบการดำเนินพันธกิจ (mission model) ให้เท่าทันปัจจุบันหรือรุดไปยังอนาคต เพื่อให้สามารถรักษาไว้ซึ่งคุณค่า (value) พร้อมขับเคลื่อนสถาบันให้สามารถบรรลุเป้าหมาย พร้อมกับตอบสนองความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสีย สังคม เศรษฐกิจ และประเทศชาติ

หนังสือ **“จัดการความเสี่ยงอย่างไร ให้มหาวิทยาลัยบรรลุเป้าหมาย Higher Education Risk Management”** เล่มนี้ จัดทำขึ้นเพื่อบอกเล่าเรื่องราวเกี่ยวกับแนวทางการบริหารความเสี่ยงที่มุ่งเน้นที่บริบทของมหาวิทยาลัย (higher education risk management) ซึ่งประกอบไปด้วย แนวคิดพื้นฐานของการบริหารความเสี่ยงในสถาบันอุดมศึกษา ระบบการบริหารความเสี่ยงที่ถูกนำมาใช้จริงในสถาบันอุดมศึกษา ตัวอย่างกรณีศึกษาการบริหารความเสี่ยงที่เกิดขึ้นในสถาบันอุดมศึกษา ตลอดจนรวบรวมแนวโน้มความเสี่ยงที่มหาวิทยาลัยต้องเผชิญท่ามกลางการเปลี่ยนแปลงในยุคเศรษฐกิจใหม่ (new economy) และความไม่แน่นอน (uncertainty) ของการบริหารมหาวิทยาลัย ที่จะทำให้ผู้บริหารและผู้ปฏิบัติงานในสถาบันอุดมศึกษาเข้าใจเรื่องบริหารความเสี่ยงมากยิ่งขึ้น พร้อมนำไปประยุกต์ใช้กับสภาพปัจจุบันและอนาคตที่สถาบันอุดมศึกษาต้องเผชิญเพื่อการบรรลุเป้าหมายตามที่มุ่งหวัง

อวิรุทธ์ ฉัตรมาลาทอง
มิถุนายน 2567

คำนิยม

ผู้นำมหาวิทยาลัยต้องมองอนาคต การบริหารจัดการความเสี่ยงที่มีประสิทธิภาพสำคัญยิ่งในยุคที่มีความไม่แน่นอนสูง

หนังสือ **“จัดการความเสี่ยงอย่างไร ให้มหาวิทยาลัยบรรลุเป้าหมาย Higher Education Risk Management”** โดย **ดร.อวิรุทธ์ ฉัตรมาลาทอง** เขียนขึ้นจากการปฏิบัติและประสบการณ์ที่สำนักงานการจัดการความเสี่ยงของจุฬาลงกรณ์มหาวิทยาลัย เนื้อหาครอบคลุมทั้งการวิเคราะห์ การประเมิน และการจัดการความเสี่ยง พร้อมตัวอย่างกรณีศึกษาที่สามารถนำไปปรับใช้ได้จริง

รองศาสตราจารย์ ดร.ณัฐชา ทวีแสงสกุลไทย
อดีตรองอธิการบดี ด้านการวางและกำหนดยุทธศาสตร์
นวัตกรรมและพันธกิจสากล (2563-2565)

คำขอบคุณ

ขอขอบพระคุณผู้มีอุปการคุณทุกท่านที่สนับสนุนและมีส่วนร่วมกับผมในการจัดทำหนังสือเล่มนี้ ตั้งแต่ทีมงานเล็ก ๆ ของผมที่พร้อมก้าวเดินไปด้วยกัน ครูบาอาจารย์ที่ประสาทวิชา ผู้บังคับบัญชาที่มอบโอกาสในงานบริหารความเสี่ยง ผู้บริหารมหาวิทยาลัยทั่วประเทศที่เชิญชวนไปแลกเปลี่ยนประสบการณ์ร่วมกัน และผู้ติดตามเพจเล็ก ๆ อย่าง “Knack Box” ที่มอบพลังบวกให้ผมแชร์เรื่องราวดี ๆ มาอย่างต่อเนื่อง

ขอขอบพระคุณคุณแม่ที่สนับสนุนทุกความสำเร็จ ตลอดจนครอบครัวที่เป็นรากฐานที่มั่นคงเสมอมา และท้ายที่สุดก็ต้องขอขอบคุณตัวผมเอง สำหรับความพยายามในการสร้างคุณค่าและประโยชน์ให้แก่องค์กร สังคม ประเทศชาติ ด้วยพลังกาย พลังใจ และพลังสติปัญญาในครั้งนี้

อวิรุทธ์ ฉัตรมาลาทอง

มิถุนายน 2567

สารบัญ

สารบัญรูปภาพ

สารบัญตาราง

ส่วนที่ 1

แนวคิดพื้นฐานของการบริหารความเสี่ยงในอุดมศึกษา

(Foundation of Higher Education Risk Management)

ท่ามกลางวิวัฒนาการของบริบทโลกที่เข้าสู่ความเปราะบาง (brittle) เต็มไปด้วยความวิตกกังวล (anxiety) ความสัมพันธ์ของสิ่งต่าง ๆ ที่ซับซ้อน (nonlinear) และปรากฏการณ์ที่เข้าใจได้ยากกว่าในอดีต (incomprehensible) ซึ่งเรียกรวมกันว่า "BANI" ส่งผลให้ภูมิทัศน์ทางอุดมศึกษาที่เปลี่ยนแปลงไปทั้งในประเทศไทยและทั่วโลก เผชิญกับความเสี่ยงในการดำเนินพันธกิจทั้งในด้านวิชาการและบริหารจัดการให้สถาบันอุดมศึกษาสามารถปรับตัวให้สอดรับกับสภาพเศรษฐกิจ สังคม เทคโนโลยี นโยบาย กฎระเบียบใหม่ สิ่งแวดล้อม และพัฒนาการส่งมอบคุณค่าให้แก่ผู้มีส่วนได้ส่วนเสียได้สอดคล้องกับความต้องการและความคาดหวังที่เปลี่ยนแปลงไป ตลอดจนสามารถบริหารจัดการสถาบันอุดมศึกษาให้ดำรงอยู่ได้อย่างยั่งยืน ดังนั้น ความเข้าใจพื้นฐานของการบริหารความเสี่ยง (risk management) จึงเป็นจุดเริ่มต้นของหนังสือเล่มนี้ที่จะนำไปสู่การบริหารความเสี่ยงให้มหาวิทยาลัยบรรลุเป้าหมาย

1.1 หลักการบริหารความเสี่ยง

นิยามศัพท์ที่เกี่ยวข้องกับความเสี่ยง (risk)

ในประเทศไทย ตลาดหลักทรัพย์แห่งประเทศไทยได้ให้นิยามคำว่า ความเสี่ยง (risk) หมายถึง "โอกาสหรือเหตุการณ์ที่ไม่แน่นอน หรือสิ่งที่ทำให้แผนงานหรือการดำเนินงานอยู่ ณ ปัจจุบันไม่บรรลุวัตถุประสงค์หรือเป้าหมายที่กำหนดไว้ และในที่สุดแล้วอาจก่อให้เกิดผลกระทบหรือความเสียหายต่อองค์กร ทั้งในแง่ของผลกระทบที่เป็นตัวเงินหรือผลกระทบต่อภาพลักษณ์และชื่อเสียงขององค์กร"

ในขณะที่ สถาบันวิจัยระบบสาธารณสุข (สวรส.) ได้ให้ความหมายของคำว่าความเสี่ยง (risk) หมายถึง "เหตุการณ์ที่เกิดขึ้นที่ไม่เป็นไปตามความคาดหวังหรือความไม่แน่นอน มีโอกาสที่จะประสบกับความสูญเสียหรือสิ่งที่ไม่พึงประสงค์ ได้แก่ ภัยธรรมชาติ การทุจริต การลักขโมย ความเสียหายของระบบเทคโนโลยีสารสนเทศ การถูกดำเนินการทางกฎหมาย การบาดเจ็บ ความเสียหาย เหตุร้าย การเกิดอันตราย สูญเสียทรัพย์สิน สูญเสียชื่อเสียง ภาพลบขององค์กร และบุคลากรเกิดความไม่แน่นอน การไม่พิทักษ์สิทธิหรือศักดิ์ศรี หรือเกิดความสูญเสียจนต้องมีการชดใช้ค่าเสียหาย"

ดังนั้น สามารถสรุปได้ว่า ความเสี่ยง (risk) หมายถึง ความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้นและส่งผลต่อการบรรลุกลยุทธ์และวัตถุประสงค์ขององค์กร เหตุการณ์ที่อาจเกิดขึ้น อาจส่งผลกระทบต่อกลยุทธ์และวัตถุประสงค์ขององค์กร การขาดความสามารถในการคาดการณ์ถึงเหตุการณ์ที่จะเกิดขึ้นรวมถึงผลกระทบที่ตามมาได้อย่างครบถ้วนก่อให้เกิดความไม่แน่นอนสำหรับองค์กร

นิยามศัพท์ที่เกี่ยวข้องกับปัจจัยเสี่ยง (risk factor)

หมายถึง สาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ใด ๆ ขององค์กร ทั้งนี้สาเหตุของความเสี่ยงอาจมาจากปัจจัยภายใน เช่น กฎระเบียบ ข้อบังคับภายในองค์กร ประสบการณ์ของบุคลากร และระบบการทำงาน และอาจมาจากปัจจัยภายนอก เช่น สภาพเศรษฐกิจ การเมือง สังคม และกฎหมาย ซึ่งปัจจัยเสี่ยงนี้ต้องเป็นสาเหตุที่สามารถวิเคราะห์และกำหนดแนวทางในการจัดการได้

นิยามศัพท์ที่เกี่ยวข้องกับการบริหารความเสี่ยง (risk management)

การบริหารความเสี่ยงมีการให้นิยามไว้อย่างหลากหลายซึ่งจะแตกต่างกันไปตามมุมมองของนักวิชาการแต่ละท่าน แต่นิยามที่ได้รับการยอมรับอย่างแพร่หลายที่สุดนิยามหนึ่ง คือนิยามที่ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ได้ให้ความหมายไว้ในมิติของ **“การบริหารความเสี่ยงทั่วทั้งองค์กร หรือ Enterprise Risk Management (ERM)”** กล่าวคือ “การบริหารความเสี่ยงทั่วทั้งองค์กร คือ กระบวนการที่บุคคลทั่วทั้งองค์กรได้มีส่วนร่วมในการคิดวิเคราะห์และคาดการณ์ถึงเหตุการณ์หรือความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งการระบุแนวทางในการจัดการความเสี่ยงดังกล่าวให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้เพื่อช่วยให้องค์กรบรรลุวัตถุประสงค์ที่ต้องการ”

กล่าวอีกนัยหนึ่ง **“การบริหารความเสี่ยง”** คือ การบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการ การดำเนินงานต่าง ๆ โดยลดมูลเหตุแต่ละโอกาสที่องค์กรจะเกิดความเสียหายเพื่อให้ระดับและขนาดของความเสียหายที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุม และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายขององค์กรเป็นสำคัญนั่นเอง

ดังนั้น จะเห็นได้ว่า การบริหารความเสี่ยงจึงเป็นวิธีที่มีความเป็นเหตุเป็นผลซึ่งถูกนำมาใช้ในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ และติดตามความเสี่ยงที่เกี่ยวข้องกับกิจกรรมของหน่วยงาน หรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยลดความสูญเสียและลดโอกาสในการไม่บรรลุเป้าหมายให้เหลือน้อยที่สุดและเพิ่มโอกาสแก่องค์กรมากที่สุด หรือก็คือการบริหารและจัดการปัจจัยเสี่ยงเพื่อลดโอกาสที่จะเกิดปัจจัยเสี่ยง และ/หรือ ผลกระทบของความเสียหายจากปัจจัยเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

“การบริหารความเสี่ยง” (risk management) คือ กระบวนการจัดการความเสี่ยงเพื่อให้สามารถควบคุมและดำเนินการต่าง ๆ กับความเสี่ยงได้อย่างมีประสิทธิภาพ ประกอบด้วย 4 ขั้นตอนหลัก ดังนี้

ขั้นตอนที่ 1 การระบุความเสี่ยง (risk identification) หมายถึง ขั้นตอนการระบุความเสี่ยงว่า ความเสี่ยงที่เราได้ดำเนินการอยู่นั้นมีความเสี่ยงอะไรบ้าง ซึ่งความเสี่ยงที่ต้องพิจารณามี 5 ประเภทหลัก ได้แก่

1. ความเสี่ยงภายนอกที่ไม่สามารถทำนายได้ (external unpredictable)
2. ความเสี่ยงภายนอกที่สามารถทำนายได้ (external predictable)
3. ความเสี่ยงภายในที่ไม่เกี่ยวกับทางเทคนิค (internal nontechnical)
4. ความเสี่ยงด้านเทคนิค (technical)
5. ความเสี่ยงด้านกฎหมาย (legal)

ขั้นตอนที่ 2 การประเมินความเสี่ยง (risk assessment) หมายถึง ขั้นตอนการประเมินความเสี่ยงเพื่อวิเคราะห์หาระดับของความเสี่ยงโดยแบ่งเป็น 2 ส่วน คือ โอกาสที่จะเกิดความเสี่ยง (likelihood) และผลกระทบของความเสี่ยง (impact)

ขั้นตอนที่ 3 การตอบสนองความเสี่ยง (risk response) หมายถึง ขั้นตอนการหาแนวทางแก้ไขความเสี่ยง สามารถแบ่งแนวทางการแก้ไขออกเป็น 5 วิธี ได้แก่

1. การหลีกเลี่ยงความเสี่ยง (avoid)
2. การยอมรับความเสี่ยง (accept)
3. การถ่ายโอนความเสี่ยง (transfer)
4. การยอมรับแต่ต้องเฝ้าระวังอย่างใกล้ชิด (accept passively)
5. การลดความเสี่ยง (mitigate)

ขั้นตอนที่ 4 การจัดทำเอกสารและการควบคุมความเสี่ยง (risk documentation and control) **“การจัดทำเอกสารความเสี่ยง”** หมายถึง การจัดทำเอกสารหรือการนำเอกสารมาอ้างอิงประกอบการบริหารความเสี่ยง เช่น ฐานข้อมูลจากโครงการที่ผ่านมา (historical database) เพื่อนำมาเป็นข้อมูลอ้างอิงกับโครงการในปัจจุบันและใช้ประเมินโครงการ (post project assessment) และปรับปรุงข้อมูลสำคัญ (archive update) **“การควบคุมความเสี่ยง”** หมายถึง ขั้นตอนการควบคุมความเสี่ยงโดยแบ่งเป็น 4 ลักษณะ ได้แก่

1. การควบคุมเพื่อป้องกัน (preventive control) ใช้เพื่อป้องกันหรือลดความเสียหาย
2. การควบคุมเพื่อการตรวจสอบติดตาม (detective control) ใช้ค้นหาให้พบความเสี่ยง
3. การควบคุมเพื่อแก้ไขข้อบกพร่อง (corrective control) ใช้ปรับปรุงแก้ไขข้อผิดพลาด
4. การควบคุมเพื่อแนะนำวิธีปฏิบัติงาน (directive control)

นิยามศัพท์ที่เกี่ยวข้องกับการบริหารความเสี่ยงองค์กร (enterprise risk management)

ทั้งนี้ ตลาดหลักทรัพย์แห่งประเทศไทย ได้ให้นิยามของการบริหารความเสี่ยงองค์กร (enterprise risk management) อย่างเฉพาะเจาะจงไว้ว่า “เป็นกระบวนการที่ปฏิบัติโดยคณะกรรมการ ผู้บริหาร และบุคลากรทุกคนในองค์กร เพื่อช่วยในการกำหนดกลยุทธ์และดำเนินงาน โดยกระบวนการบริหารความเสี่ยงได้รับการออกแบบเพื่อให้สามารถบ่งชี้เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อองค์กรและสามารถจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับ เพื่อให้ได้รับความมั่นใจอย่างสมเหตุสมผลในการบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้ ประกอบด้วย 8 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 สภาพแวดล้อมภายในองค์กร (internal environment) หมายถึง ปัจจัยต่าง ๆ เช่น จริยธรรม วิธีการทำงานของผู้บริหารและบุคลากร รูปแบบการจัดการของฝ่ายบริหาร วิธีการมอบหมายอำนาจหน้าที่และความรับผิดชอบ ซึ่งผู้บริหารต้องมีการกำหนดร่วมกันกับพนักงานในองค์กร ส่งผลให้มีการสร้างจิตสำนึก การตระหนักและรับรู้เรื่องความเสี่ยง และการควบคุมแก่พนักงานทุกคนในองค์กร โดยสภาพแวดล้อมภายในองค์กรนี้เป็นพื้นฐานที่สำคัญสำหรับกรอบการบริหารความเสี่ยง ซึ่งมีอิทธิพลต่อการกำหนด

กลยุทธ์และเป้าหมายขององค์กร การกำหนดกิจกรรม การบ่งชี้ ประเมิน และจัดการความเสี่ยงอีกด้วย

ขั้นตอนที่ 2 การกำหนดวัตถุประสงค์ (objective setting) องค์กรควรมีการกำหนดวัตถุประสงค์ในการดำเนินการที่ชัดเจน เพื่อให้มั่นใจว่าวัตถุประสงค์ที่กำหนดนั้นมีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ โดยการบริหารจัดการให้อยู่ในกรอบของความเสี่ยงที่ยอมรับได้

ขั้นตอนที่ 3 การบ่งชี้เหตุการณ์ (event identification) ในกระบวนการบ่งชี้เหตุการณ์ควรต้องพิจารณาปัจจัยความเสี่ยงทุกด้านที่อาจเกิดขึ้น เช่น ความเสี่ยงด้านกลยุทธ์ การเงิน บุคลากร การปฏิบัติงาน กฎหมาย ภาษีอากร ระบบงาน สิ่งแวดล้อม ความสัมพันธ์ระหว่างเหตุการณ์ที่อาจเกิดขึ้น แหล่งความเสี่ยง ทั้งจากสภาพแวดล้อมภายในและภายนอกองค์กร

สภาพแวดล้อมภายนอกองค์กรเป็นองค์ประกอบต่าง ๆ ที่อยู่ภายนอกองค์กร ซึ่งมีอิทธิพลต่อวัตถุประสงค์หรือเป้าหมายขององค์กร ยกตัวอย่างเช่น

1. วัฒนธรรม การเมือง กฎหมาย ข้อบังคับ การเงิน เทคโนโลยี เศรษฐกิจ สภาพแวดล้อมในการแข่งขันทั้งภายในประเทศและต่างประเทศ
2. ตัวขับเคลื่อนหลักและแนวโน้มที่ส่งผลกระทบต่อวัตถุประสงค์ขององค์กร
3. การยอมรับและคุณค่าของผู้มีส่วนได้ส่วนเสียภายนอกองค์กร
4. สภาพแวดล้อมภายในองค์กรเป็นสิ่งต่าง ๆ ที่อยู่ภายในองค์กรและมีอิทธิพลต่อเป้าหมายขององค์กร
5. ขีดความสามารถขององค์กร ในแง่ของทรัพยากรและความรู้ เช่น เงินทุน เวลา บุคลากร กระบวนการ ระบบและเทคโนโลยี
6. ระบบสารสนเทศ การไหลของข้อมูล และกระบวนการตัดสินใจทั้งที่เป็นทางการและไม่เป็นทางการ
7. ผู้มีส่วนได้ส่วนเสียภายในองค์กร
8. นโยบาย วัตถุประสงค์ และกลยุทธ์องค์กร
9. การรับรู้คุณค่าและวัฒนธรรมองค์กร
10. มาตรฐานและแบบจำลองที่พัฒนาโดยองค์กร
11. โครงสร้าง เช่น ระบบการจัดการ บทบาทหน้าที่และความรับผิดชอบ

การระบุเหตุการณ์อาจดำเนินการโดยการสัมภาษณ์ผู้บริหารระดับสูงหรือฝ่ายจัดการที่รับผิดชอบในแผนงานหรือการดำเนินการนั้น และรวบรวมประเด็นความเสี่ยงสำคัญที่ได้รับความสนใจหรือเป็นประเด็นที่กังวล เพื่อนำมาจัดทำภาพรวมความเสี่ยงขององค์กร (corporate risk profile) โดยตลาดหลักทรัพย์แห่งประเทศไทยได้จำแนกประเภทของความเสี่ยงออกเป็น 4 ประเภท ได้แก่

1. ความเสี่ยงด้านกลยุทธ์ (strategic risk: S) คือ ความเสี่ยงที่เกี่ยวข้องกับการกำหนดแผนกลยุทธ์ แผนการดำเนินงาน และการนำแผนดังกล่าวไปปฏิบัติอย่างไม่เหมาะสม รวมถึงการเปลี่ยนแปลงจากปัจจัยภายนอกและปัจจัยภายใน อันส่งผลกระทบต่อการกำหนดกลยุทธ์หรือการดำเนินงานเพื่อให้บรรลุวัตถุประสงค์หลัก เป้าหมาย และแนวทางการดำเนินงานขององค์กร

2. ความเสี่ยงด้านปฏิบัติการ (operational risk: O) คือ ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงานของแต่ละกระบวนการหรือกิจกรรมภายในองค์กร รวมทั้งความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการข้อมูลด้านเทคโนโลยีสารสนเทศและข้อมูลความรู้ต่าง ๆ เพื่อให้การปฏิบัติงานบรรลุเป้าหมายที่กำหนด ซึ่งความเสี่ยงด้านปฏิบัติการจะส่งผลกระทบต่อประสิทธิภาพของกระบวนการทำงานและการบรรลุวัตถุประสงค์หลักขององค์กรในภาพรวม

3. ความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการทางการเงิน (financial risk: F) ซึ่งอาจเป็นความเสี่ยงที่เกิดจากปัจจัยภายใน เช่น การบริหารจัดการด้านสภาพคล่อง ด้านเครดิต ด้านเงินลงทุน หรือจากปัจจัยภายนอก เช่น การเปลี่ยนแปลงของอัตราดอกเบี้ย อัตราแลกเปลี่ยน หรือความเสี่ยงที่คู่สัญญาไม่สามารถปฏิบัติตามภาระผูกพันที่ตกลงไว้อันส่งผลกระทบต่อการดำรงอยู่ รวมถึงส่งผลให้เกิดความเสียหายต่อองค์กร

4. ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามกฎระเบียบ (compliance risk: C) ข้อบังคับของหน่วยงานกำกับดูแล เช่น คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ รวมทั้งความเสี่ยงที่เกี่ยวกับกฎหมายต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจของกลุ่มตลาดหลักทรัพย์ ซึ่งเมื่อมีความเสี่ยงด้านนี้เกิดขึ้นจะส่งผลกระทบต่อชื่อเสียงและภาพลักษณ์ขององค์กรโดยรวม

ขั้นตอนที่ 4 การประเมินความเสี่ยง (risk assessment) เป็นขั้นตอนที่จะต้องดำเนินการต่อจากการระบุความเสี่ยง โดยการประเมินความเสี่ยงประกอบด้วย 2 กระบวนการหลัก ได้แก่

1. การวิเคราะห์ความเสี่ยง โดยจะพิจารณาสาเหตุและแหล่งที่มาของความเสี่ยง ผลกระทบที่ตามมาทั้งในทางบวกและทางลบ รวมทั้งโอกาสที่อาจเกิดขึ้นของผลกระทบที่จะตามมา จะต้องมีการระบุถึงปัจจัยที่มีผลต่อผลกระทบและโอกาสที่จะเกิดขึ้น ทั้งนี้เหตุการณ์หรือสถานการณ์หนึ่ง ๆ อาจจะเกิดผลที่ตามมาและกระทบต่อวัตถุประสงค์/เป้าหมายหลายด้าน นอกจากนั้นในการวิเคราะห์ควรพิจารณาถึงมาตรการจัดการความเสี่ยงที่ดำเนินการอยู่ ณ ปัจจุบัน รวมถึงประสิทธิผลของมาตรการดังกล่าวด้วย

2. การประเมินความเสี่ยง จะเป็นการเปรียบเทียบระหว่างระดับของความเสี่ยงที่ได้จากการวิเคราะห์ความเสี่ยง เทียบกับระดับความเสี่ยงที่ยอมรับได้ (risk appetite) ในกรณีที่ระดับของความเสี่ยงไม่อยู่ในระดับที่ยอมรับได้ของเกณฑ์การยอมรับความเสี่ยง ความเสี่ยงดังกล่าวจะได้รับการจัดการทันที ซึ่งเกณฑ์ที่ใช้ในการประเมินความเสี่ยงควรสะท้อนถึงคุณค่า วัตถุประสงค์ และทรัพยากรขององค์กร โดยเกณฑ์บางประเภทอาจพัฒนาได้จากข้อกำหนดทางกฎหมายหรือข้อบังคับของหน่วยงานกำกับดูแลหรือหน่วยงานที่เป็นสมาชิกอยู่ ทั้งนี้เกณฑ์ที่กำหนดต้องสอดคล้องกับนโยบายความเสี่ยงขององค์กรและมีการทบทวนอย่างต่อเนื่อง ซึ่งปัจจัยที่นำมาพิจารณาเพื่อประกอบการกำหนดเกณฑ์ความเสี่ยงมีดังนี้

1) ลักษณะและประเภทของผลกระทบที่สามารถเกิดขึ้น
2) ประเมินผลกระทบ
3) แนวทางในการระบุโอกาสในการเกิดขึ้น (impact)
4) กรอบเวลาของโอกาสและผลกระทบที่เกิดขึ้น (likelihood)
5) แนวทางในการกำหนดระดับความเสี่ยง (level of risk)
6) ระดับของความเสี่ยงที่สามารถยอมรับได้
7) ระดับของความเสี่ยงที่จะต้องจัดการ

ขั้นตอนที่ 5 การตอบสนองความเสี่ยง (risk response) การกำหนดแผนจัดการความเสี่ยงจะมีการนำเสนอแผนจัดการความเสี่ยงที่จะดำเนินการต่อที่ประชุมคณะผู้บริหาร เพื่อพิจารณาและขออนุมัติการจัดสรรทรัพยากรที่จำเป็นต้องใช้ดำเนินการ (ถ้ามี) ในการคัดเลือกแนวทางในการจัดการความเสี่ยงที่เหมาะสมที่สุดจะคำนึงถึงความเสี่ยงที่ยอมรับได้ (risk appetite) กับต้นทุนที่เกิดขึ้นเปรียบเทียบกับประโยชน์ที่จะได้รับ รวมถึงข้อกฎหมายและข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง ความรับผิดชอบที่มีต่อสังคมระดับความเสี่ยงที่ยอมรับได้ คือ ระดับความเสี่ยงที่ตลาดหลักทรัพย์แห่งประเทศไทยยอมรับได้ โดยยังคงให้องค์กรสามารถดำเนินธุรกิจ และบรรลุเป้าหมายหรือวัตถุประสงค์ที่วางไว้

ทั้งนี้ในการตัดสินใจเลือกแนวทางในการจัดการความเสี่ยงอาจต้องคำนึงถึงความเสี่ยงที่อาจเกิดขึ้น หากไม่มีการจัดการ ซึ่งอาจไม่สมเหตุสมผลในแง่มุมเศรษฐศาสตร์ เช่น ความเสี่ยงที่ส่งผลกระทบในทางลบอย่างมีนัยสำคัญ แต่โอกาสที่จะเกิดขึ้นน้อยมาก แนวทางในการจัดการความเสี่ยงอาจพิจารณาดำเนินการเป็นรายกรณีไป หรืออาจดำเนินการไปพร้อม ๆ กับความเสี่ยงอื่น ๆ ซึ่งแนวทางในการจัดการความเสี่ยงมีดังนี้

1. การหลีกเลี่ยง (avoid) เป็นการดำเนินการเพื่อหลีกเลี่ยงเหตุการณ์ที่ก่อให้เกิดความเสี่ยง มักใช้ในกรณีที่ความเสี่ยงมีความรุนแรงสูง ไม่สามารถหาวิธีลด/จัดการให้อยู่ในระดับที่ยอมรับได้

2. การร่วมจัดการ (share) เป็นการร่วมหรือถ่ายโอนความเสี่ยงทั้งหมดหรือบางส่วนไปยังบุคคลหรือหน่วยงานภายนอกองค์กร ให้ช่วยแบกรับภาระความเสี่ยงแทน เช่น การซื้อประกันภัย

3. การลด (reduce) เป็นการจัดหามาตรการจัดการ เพื่อลดโอกาสการเกิดเหตุการณ์ความเสี่ยงหรือลดผลกระทบที่อาจเกิดขึ้นให้อยู่ในระดับที่ยอมรับได้ เช่น การเตรียมแผนฉุกเฉิน (contingency plan)

4. การยอมรับ (accept) ความเสี่ยงที่เหลือในปัจจุบันอยู่ในระดับที่ยอมรับได้ โดยไม่ต้องดำเนินการใด ๆ เพื่อลดโอกาสหรือผลกระทบที่อาจเกิดขึ้นอีก มักใช้กับความเสี่ยงที่ต้นทุนของมาตรการจัดการสูง ไม่คุ้มกับประโยชน์ที่ได้รับ

ขั้นตอนที่ 6 กิจกรรมการควบคุม (control activities) คือ นโยบายและกระบวนการปฏิบัติงาน เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เพื่อป้องกันไม่ให้เกิดผลกระทบต่อเป้าหมายขององค์กร เนื่องจากแต่ละองค์กรมีการกำหนดวัตถุประสงค์และเทคนิคการนำไปปฏิบัติเป็นของเฉพาะองค์กร ดังนั้น กิจกรรมการควบคุมจึงมีความแตกต่างกัน ซึ่งอาจแบ่งได้เป็น 4 ประเภท คือ

1. การควบคุมเพื่อการป้องกัน (preventive control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก

2. การควบคุมเพื่อให้ตรวจพบ (detective control) เป็นวิธีการควบคุมเพื่อให้ค้นพบข้อผิดพลาดที่ได้เกิดขึ้นแล้ว

3. การควบคุมโดยการชี้แนะ (directive control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ

4. การควบคุมเพื่อการแก้ไข (corrective control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้น และป้องกันไม่ให้เกิดซ้ำอีกในอนาคต ทั้งนี้ในการดำเนินกิจกรรมการควบคุมควรต้องคำนึงถึงความคุ้มค่าในด้านค่าใช้จ่ายและต้นทุนกับผลประโยชน์ที่คาดว่าจะได้รับด้วย โดยกิจกรรมการควบคุมควรมีองค์ประกอบดังนี้

1) วิธีการดำเนินงาน (ขั้นตอน กระบวนการ)

2) การกำหนดบุคลากรภายในองค์กรเพื่อรับผิดชอบการควบคุมนั้น ซึ่งควรมีความรับผิดชอบดังนี้

(1) พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

(2) พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยง

(3) กำหนดระยะเวลาแล้วเสร็จของงาน

ขั้นตอนที่ 7 ข้อมูลและการติดต่อสื่อสาร (information and communication) สารสนเทศเป็นสิ่งจำเป็นสำหรับองค์กรในการบ่งชี้ ประเมิน และจัดการความเสี่ยงข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งข้อมูลภายในและภายนอกองค์กร ควรได้รับการบันทึกและสื่อสารไปยังบุคลากรในองค์กรอย่างเหมาะสมทั้งในด้านรูปแบบและเวลา

เพื่อให้สามารถปฏิบัติงานตามหน้าที่และความรับผิดชอบได้ รวมถึงเป็นการรายงานการบริหารจัดการความเสี่ยงเพื่อให้ทุกคนในองค์กรได้รับทราบถึงความเสี่ยงที่เกิดขึ้นและผลของการบริหารจัดการความเสี่ยงเหล่านั้น ซึ่งครอบคลุมถึงการสื่อสารจากระดับบนลงล่าง ระดับล่างไปสู่บน และการสื่อสารระหว่างหน่วยงานการบริหารความเสี่ยงควรใช้ทั้งข้อมูลในอดีตและปัจจุบัน ข้อมูลในอดีตจะแสดงแนวโน้มของเหตุการณ์และช่วยคาดการณ์การปฏิบัติงานในอนาคต ส่วนข้อมูลปัจจุบันมีประโยชน์ต่อผู้บริหารในการพิจารณาความเสี่ยงที่เกิดขึ้นในกระบวนการ สายงาน หรือหน่วยงาน ซึ่งช่วยให้องค์กรสามารถปรับเปลี่ยนกิจกรรมการควบคุมตามความจำเป็นเพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้

ขั้นตอนที่ 8 การติดตาม (monitoring) กระบวนการบริหารความเสี่ยงที่ดำเนินการภายในตลาดหลักทรัพย์แห่งประเทศไทย มีความจำเป็นต้องได้รับการสื่อสารถึงการประเมินความเสี่ยงและการควบคุม ความคืบหน้าในการบริหารความเสี่ยง การดูแลติดตามแนวโน้มของความเสี่ยงหลัก รวมถึงการเกิดเหตุการณ์ผิดปกติอย่างต่อเนื่อง เพื่อให้มั่นใจว่า

1. เจ้าของความเสี่ยง (risk owner) มีการติดตามประเมินสถานการณ์ วิเคราะห์และบริหารความเสี่ยงที่อยู่ภายใต้ความรับผิดชอบของตนอย่างสม่ำเสมอและเหมาะสม

2. ความเสี่ยงที่มีผลกระทบสำคัญต่อการบรรลุวัตถุประสงค์ขององค์กร ได้รับการรายงานถึงความคืบหน้าในการบริหารความเสี่ยง และแนวโน้มของความเสี่ยงต่อผู้บริหารที่รับผิดชอบและคณะอนุกรรมการบริหารความเสี่ยง

3. ระบบการควบคุมภายในที่วางไว้มีความเพียงพอ เหมาะสม มีประสิทธิผล และมีการนำมาปฏิบัติใช้จริงเพื่อป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้น รวมทั้งมีการปรับปรุงแก้ไขการควบคุมภายในอยู่เสมอเพื่อให้สอดคล้องกับสถานการณ์หรือความเสี่ยงที่เปลี่ยนไป

ทั้งนี้ฝ่ายบริหารความเสี่ยงจะประสานงานให้ฝ่ายจัดการที่รับผิดชอบความเสี่ยงรายงานสถานะความเสี่ยง รวมถึงกระบวนการบริหารความเสี่ยงให้ที่ประชุมผู้บริหาร คณะอนุกรรมการบริหารความเสี่ยง คณะอนุกรรมการตรวจสอบ และคณะกรรมการตลาดหลักทรัพย์ฯ เพื่อทราบและพิจารณาต่อไป

กล่าวโดยสรุป นิยามของ **“การบริหารความเสี่ยงเชิงสัมพันธ์ระดับองค์กร” (enterprise risk management) ตามแนว The Committee of Sponsoring of the Treadway Commission (COSO)** คือ กระบวนการที่เป็นผลมาจากคณะกรรมการบริษัท ฝ่ายบริหาร และพนักงาน สร้างขึ้นและร่วมกันปฏิบัติในการกำหนดกลยุทธ์และในการปฏิบัติงานทั่วทั้งองค์กร กระบวนการบริหารความเสี่ยงสร้างขึ้นเพื่อระบุเหตุการณ์ที่อาจเกิดขึ้นที่มีผลกระทบสำคัญต่อองค์กร และเพื่อการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ รวมทั้งเพื่อสร้างความมั่นใจอย่างสมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ขององค์กร

1.2 กรอบการบริหารความเสี่ยงในระดับสากล

1.2.1 COSO ERM (2017)

ประเด็นที่ 1 นิยามของการบริหารความเสี่ยงขององค์กร

หากเปรียบเทียบนิยามของการบริหารความเสี่ยงขององค์กรที่ปรากฏใน COSO ERM (2004) กับ COSO ERM (2017) จะเห็นว่า นิยามของการบริหารความเสี่ยงขององค์กรเดิมจะเปิดกว้าง กล่าวคือ เป็นกระบวนการใด ๆ ก็ตามที่ทำโดยบุคคลภายในองค์กร ตั้งแต่การกำหนดเป้าหมาย การระบุเหตุการณ์ที่มีผลกระทบต่อเป้าหมาย และการจัดการเหตุการณ์เหล่านั้นให้อยู่ในระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ ในขณะที่นิยามใหม่ที่ปรากฏตาม COSO ERM (2017) จะมีการระบุอย่างชัดเจนมากขึ้นว่าหมายถึงเฉพาะวัฒนธรรม ความรู้ความสามารถ และแนวปฏิบัติในการบริหารความเสี่ยงที่บูรณาการร่วมกับการกำหนดกลยุทธ์และผลการปฏิบัติงานเพื่อสร้างการรักษาและการทำให้คุณค่าเกิดขึ้นจริงเท่านั้น

ประเด็นที่ 2 การบูรณาการ

หากเปรียบเทียบการบูรณาการของการบริหารความเสี่ยงขององค์กรที่ปรากฏใน COSO ERM (2004) กับ COSO ERM (2017) จะเห็นว่า การบริหารความเสี่ยงขององค์กรในรูปแบบเดิมจะใช้ลูกบาศก์ 3 มิติ เพื่อแสดงการบูรณาการ 8 องค์ประกอบของการบริหารความเสี่ยงขององค์กรเข้ากับวัตถุประสงค์ทั้ง 4 ด้าน ได้แก่ ด้านกลยุทธ์ (strategic) ด้านการดำเนินงาน (operations) ด้านการรายงาน (reporting) และด้านการปฏิบัติตาม

กฎระเบียบ (compliance) โดยมีการประยุกต์กับหน่วยงานตั้งแต่ระดับองค์กร (entity level) ลงไปถึงหน่วยย่อย ๆ ในองค์กร (subsidiary) ในขณะที่การบริหารความเสี่ยงขององค์กรในรูปแบบใหม่จะใช้แผนที่นำทางแสดงการบูรณาการ 5 องค์ประกอบของการบริหารความเสี่ยงขององค์กรเข้ากับการดำเนินงานตามปกติของกิจการ ตั้งแต่พันธกิจ วิสัยทัศน์ และคุณค่าหลัก การพัฒนากลยุทธ์ การกำหนดวัตถุประสงค์ทางธุรกิจ การนำไปใช้ และผลการปฏิบัติงาน ไปจนถึงการทำให้คุณค่าเพิ่มขึ้น

รูปที่ 1 เปรียบเทียบการบูรณาการของการบริหารความเสี่ยงขององค์กร ระหว่าง COSO ERM (2004) (รูปซ้าย) กับ COSO ERM (2017) (รูปขวา)

สืบค้นจาก "Enterprise Risk Management - Integrated Framework Executive Summary", 2004, p. 5. และ "Enterprise Risk Management: Integrating with Strategy and Performance", 2017, p. 18.

ประเด็นที่ 3 การแยกระหว่างการกำกับดูแลกิจการกับการบริหารความเสี่ยง

การบริหารความเสี่ยงขององค์กร COSO ERM (2017) ได้มีการแยกการกำกับดูแลกิจการที่สนับสนุนให้เกิดการบริหารความเสี่ยงขององค์กร ได้แก่ การกำกับดูแลและวัฒนธรรมและการสารสนเทศ การสื่อสารและการรายงาน ออกจากการบริหารความเสี่ยงที่ทำทั่วทั้งองค์กร ได้แก่ กลยุทธ์และการกำหนดวัตถุประสงค์ ผลการปฏิบัติงาน และการสอบทานปรับปรุงแก้ไข

ประเด็นที่ 4 การเชื่อมโยงกับกลยุทธ์

การบริหารความเสี่ยงขององค์กร COSO ERM (2017) ให้แนวทางในการพิจารณาจากความเสี่ยงตั้งแต่ขั้นตอนการกำหนดกลยุทธ์ โดยแบ่งออกเป็น 3 มุมมอง ได้แก่ มุมมองด้านความเสี่ยงจากกลยุทธ์ไม่สอดคล้องกับพันธกิจ วิสัยทัศน์ และคุณค่าหลัก มุมมองด้าน

ความเสี่ยงจากกลยุทธ์ที่เลือก และมุมมองด้านความเสี่ยงจากการนำกลยุทธ์และวัตถุประสงค์ทางธุรกิจไปปฏิบัติ

รูปที่ 2 แนวทางในการพิจารณาความเสี่ยงในขั้นตอนการกำหนดกลยุทธ์

สืบค้นจาก "Enterprise Risk Management: Integrating with Strategy and Performance", 2017, p. 21.

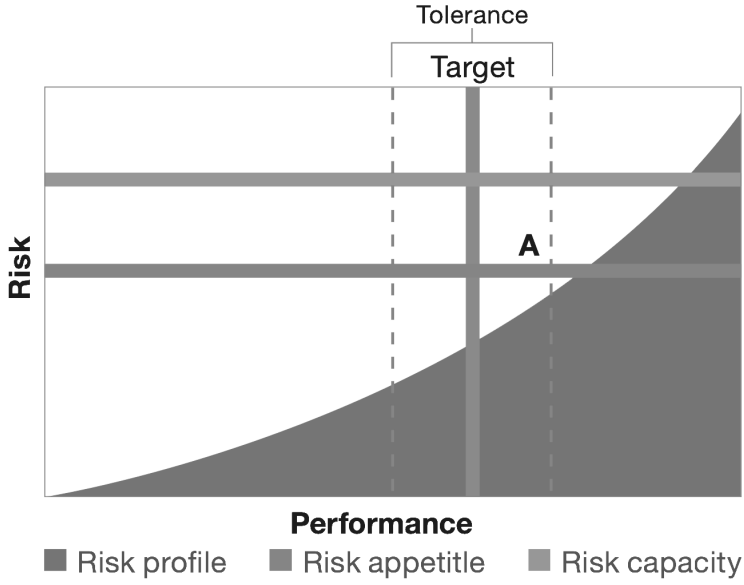
ประเด็นที่ 5 ระดับความเสี่ยงที่ยอมรับได้

หากเปรียบเทียบนิยามระดับความเสี่ยงที่ยอมรับได้ของการบริหารความเสี่ยงขององค์กรที่ปรากฏใน COSO ERM (2004) กับ COSO ERM (2017) จะเห็นได้ว่า การบริหารความเสี่ยงขององค์กรรูปแบบเดิม มีการกำหนดนิยามของระดับความเสี่ยงที่ยอมรับได้ (risk appetite) ว่าหมายถึง ระดับความเสี่ยงที่ไม่มีผลกระทบต่อความสำเร็จตามเป้าหมายที่วางไว้ ในขณะที่การบริหารความเสี่ยงขององค์กรรูปแบบใหม่จะหมายถึงประเภทและค่าความเสี่ยงที่องค์กรเต็มใจยอมรับในการสร้างคุณค่า ซึ่งจัดเตรียมโดยผู้บริหารและต้องผ่านการอนุมัติโดยคณะกรรมการบริษัท โดยการกำหนดระดับความเสี่ยงที่ยอมรับได้นั้นจะต้องสอดคล้องกับการพัฒนากลยุทธ์ เพื่อช่วยในการสร้างวัฒนธรรมในการบริหารความเสี่ยง และค้นหาความสมดุลที่เหมาะสมระหว่างความเสี่ยงและโอกาส

ประเด็นที่ 6 โปรไฟล์ความเสี่ยง

การบริหารความเสี่ยงขององค์กร COSO ERM (2017) ได้พัฒนาโปรไฟล์ความเสี่ยง (risk profile) โดยแสดงผ่านเส้นกราฟแสดงความสัมพันธ์ระหว่างความเสี่ยงที่เปลี่ยนแปลงไปในแต่ละผลการปฏิบัติงาน เพื่อใช้ในการกำหนดความสามารถในการรับความเสี่ยง (risk capacity) ระดับความเสี่ยงที่ยอมรับได้ (risk appetite) เป้าหมายผลการปฏิบัติงาน

(performance targets) ระดับความเบี่ยงเบนความเสี่ยง (tolerance) ค่าความเสี่ยง (amount of risk) ที่องค์กรยินดีรับไว้ในการดำเนินการ เพื่อให้บรรลุวัตถุประสงค์ตามพันธกิจขององค์กร



รูปที่ 3 โปรไฟล์ความเสี่ยงในการกำหนดระดับความเสี่ยงที่องค์กรสามารถรับได้ ระดับความเสี่ยงที่สอดคล้องกับเป้าหมายผลการปฏิบัติงาน

สืบค้นจาก "Enterprise Risk Management: Integrating with Strategy and Performance", 2017, p. 23.

ประเด็นที่ 7 การตอบสนองความเสี่ยง

เดิมการบริหารความเสี่ยงขององค์กร COSO ERM (2004) กำหนดวิธีการตอบสนองความเสี่ยงไว้ 4 วิธี ได้แก่ ยอมรับ (accept) ลด (reduce) แบ่งปัน (share) และหลีกเลี่ยง (avoid) ต่อมาการบริหารความเสี่ยงขององค์กร COSO ERM (2017) ได้มีการเพิ่มวิธีการตอบสนองความเสี่ยงขึ้นมาอีก 1 วิธี ได้แก่ การดำเนินการต่อ (pursue) สำหรับการเลือกใช้กลยุทธ์เพื่อการเติบโตอย่างก้าวกระโดด เช่น การขยายการดำเนินงานหรือการพัฒนาผลิตภัณฑ์ใหม่ เป็นการดำเนินการต่อโดยยอมรับความเสี่ยงที่สูงขึ้นเพื่อให้บรรลุผลการปฏิบัติงานที่สูงขึ้น

ประเด็นที่ 8 การเชื่อมโยงกับการควบคุมภายใน

กรอบการบริหารความเสี่ยงขององค์กร COSO ERM (2017) แม้จะมีความแตกต่างจากกรอบการควบคุมภายใน COSO IC (2013) ที่มีมาก่อนอยู่หลายประการ แต่ก็ไม่ได้ถูกพัฒนามาเพื่อแทนที่กรอบการควบคุมดังกล่าวแต่อย่างใด หากแต่จะต้องนำมาใช้งานร่วมกัน

ดังนั้น จะเห็นได้ว่า การบริหารความเสี่ยงที่เป็นมาตรฐานสากล อย่างกรอบการบริหารความเสี่ยงขององค์กร COSO ERM 2017 นำมาใช้เป็นแนวทางสำหรับองค์กรย่อมส่งเสริมให้เกิดการบริหารความเสี่ยงที่มีทิศทางเดียวกันโดยเชื่อมโยงกันทั้งระดับองค์กร ระดับส่วนงาน และหน่วยงาน โดยกำหนดให้การบริหารความเสี่ยงเป็นส่วนหนึ่งในการตัดสินใจ กำหนดเป้าหมายและยุทธศาสตร์ วางแผนปฏิบัติงานทั้งภารกิจสร้างผลผลิตหลักและภารกิจสนับสนุนการดำเนินงาน ซึ่งพบว่าสถาบันอุดมศึกษาในประเทศไทยส่วนใหญ่มักใช้กรอบการบริหารความเสี่ยงขององค์กร COSO ERM เป็นกรอบสำคัญในการวางระบบบริหารความเสี่ยง

1.2.2 ISO 31000/2018

ISO 31000 ได้รับการเผยแพร่ครั้งแรกใน ค.ศ. 2009 และมีการเผยแพร่เวอร์ชันปรับปรุงในเดือนกุมภาพันธ์ 2018 อย่างไรก็ตาม วัตถุประสงค์โดยรวมของ ISO 31000 ยังคงเหมือนเดิม คือ การรวมการจัดการความเสี่ยงเข้ากับระบบการจัดการเชิงกลยุทธ์และการปฏิบัติงาน เวอร์ชัน 2018 นั้นคล้ายกับเวอร์ชันดั้งเดิมมาก แต่มีการเปลี่ยนแปลงดังนี้

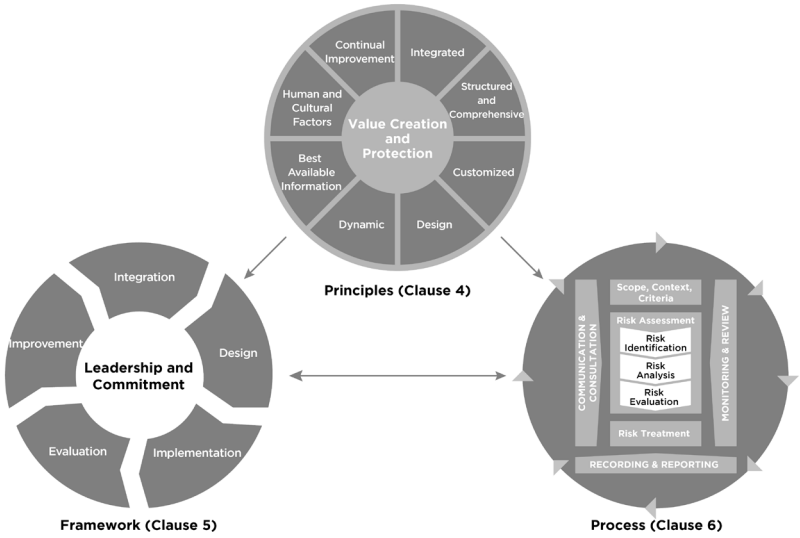
1. หลักการของการบริหารความเสี่ยงได้รับการทบทวนแล้ว เนื่องจากเป็นเกณฑ์สำคัญสำหรับการบริหารความเสี่ยงที่ประสบความสำเร็จ

2. เน้นย้ำถึงความสำคัญของความเป็นผู้นำโดยผู้บริหารระดับสูง เช่นเดียวกับการบูรณาการการบริหารความเสี่ยง โดยเริ่มจากการกำกับดูแลองค์กร

3. เน้นมากขึ้นในธรรมชาติแบบวนซ้ำของการจัดการความเสี่ยง เนื่องจากความรู้และการวิเคราะห์ใหม่นำไปสู่การแก้ไขกระบวนการ การดำเนินการ และการควบคุม

4. เนื้อหามีความคล่องตัวโดยมุ่งเน้นที่การรักษาโมเดลระบบเปิดเพื่อให้เหมาะสมกับความต้องการและบริบทที่หลากหลายมากขึ้น

โครงสร้างโดยรวมและแนวทางที่นำมาใช้โดย ISO 31000 รุ่น 2018 นั้นแสดงให้เห็นได้ดีที่สุด โดยรูปที่ 4 ซึ่ง ISO 31000 ระบุว่า การจัดการความเสี่ยงนั้นขึ้นอยู่กับหลักการ (principles) กรอบแนวคิด (framework) และกระบวนการ (process)



รูปที่ 4 หลักการ กรอบแนวคิด และกระบวนการบริหารความเสี่ยงของ ISO 31000

1. หลักการ (principles)

ISO 31000 ระบุว่า วัตถุประสงค์ของการจัดการความเสี่ยงคือการสร้างและปกป้องคุณค่า โดยหลักการที่กำหนดไว้ใน ISO 31000 ให้แนวทางเกี่ยวกับลักษณะของการจัดการความเสี่ยงที่มีประสิทธิผล การสื่อสารคุณค่าและอธิบายความตั้งใจและวัตถุประสงค์ โดยหลักการสำคัญ 8 ประการของ ISO 31000 มีดังนี้

1. กรอบแนวคิดและกระบวนการควรได้รับการปรับแต่งและเป็นสัดส่วน
2. การมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียอย่างเหมาะสมและทันเวลาเป็นสิ่งที่จำเป็น
3. ต้องใช้แนวทางที่มีโครงสร้างและครอบคลุม
4. การบริหารความเสี่ยงเป็นส่วนสำคัญของกิจกรรมขององค์กรทั้งหมด
5. การบริหารความเสี่ยงต้องมีการคาดการณ์ ตรวจจับ รับทราบ และตอบสนองต่อการเปลี่ยนแปลง
6. การจัดการความเสี่ยงพิจารณาถึงข้อจำกัดของข้อมูลที่มีอยู่อย่างชัดเจน

7. ปัจจัยด้านมนุษย์และวัฒนธรรมมีอิทธิพลต่อการจัดการความเสี่ยงทุกด้าน

8. การจัดการความเสี่ยงได้รับการปรับปรุงอย่างต่อเนื่องผ่านการเรียนรู้และประสบการณ์

หลักการ 5 ข้อแรกเป็นแนวทางในการออกแบบและการวางแผนความคิดริเริ่มการบริหารความเสี่ยง ซึ่งหลักการเหล่านี้มักถูกสรุปอย่างเป็นสัดส่วน สอดคล้องกัน ฝังแน่นและเป็นพลวัต (dynamic) และหลักการที่ 6, 7 และ 8 เกี่ยวข้องกับการดำเนินงานของโครงการริเริ่มการบริหารความเสี่ยง จาก 3 หลักการหลังดังกล่าวเหล่านี้ยืนยันว่าควรใช้ข้อมูลที่ดีที่สุด ควรพิจารณาปัจจัยมนุษย์และวัฒนธรรม และการจัดการความเสี่ยงควรมีการปรับปรุงอย่างต่อเนื่อง

2. กรอบแนวคิด (framework)

หลักการบริหารความเสี่ยงและกรอบการทำงานมีความเกี่ยวข้องกันอย่างใกล้ชิด โดยหลักการจะทำหน้าที่สรุปสิ่งที่ต้องบรรลุ และกรอบการทำงานจะทำหน้าที่ให้ข้อมูลเกี่ยวกับวิธีการบรรลุการบูรณาการที่จำเป็น

แนวทาง ISO 31000 เน้นที่ความเป็นผู้นำและความมุ่งมั่น (leadership and commitment) ประสิทธิผลของการบริหารความเสี่ยงจะขึ้นอยู่กับการรวมเข้ากับทุกด้านขององค์กร รวมถึงการตัดสินใจ โดยองค์ประกอบสำคัญของกรอบแนวคิดบริหารความเสี่ยงตามแนวทาง ISO 31000 มีดังนี้

1. การบูรณาการ (integration)
2. การออกแบบ (design)
3. การนำไปใช้ (implementation)
4. การประเมิน (evaluation)
5. การปรับปรุง (improvement)

ISO 31000 อธิบายว่า กรอบแนวคิดควรสนับสนุนกิจกรรมการบริหารความเสี่ยงในองค์กรอย่างไร ซึ่งมักจะเรียกว่า สถาปัตยกรรมความเสี่ยง กลยุทธ์ และโพรโทคอลขององค์กร ซึ่งรายละเอียดเกี่ยวกับขอบเขตของความเป็นผู้นำและความมุ่งมั่น (leadership and commitment) และช่วงของกิจกรรมที่เกี่ยวข้องกับการออกแบบและการนำความคิดริเริ่มการบริหารความเสี่ยงไปใช้มีดังนี้

สถาปัตยกรรมการบริหารความเสี่ยง (Risk Management Architecture)	กลยุทธ์การบริหารความเสี่ยง (Risk Management Strategy)	โพรโทคอลการจัดการความเสี่ยง (Risk Management Protocols)
• โครงสร้างคณะกรรมการและเงื่อนไขการอ้างอิง • หน้าที่และความรับผิดชอบ • ข้อกำหนดการรายงานภายใน • การควบคุมการรายงานภายนอก • การเตรียมการประกันการบริหารความเสี่ยง	• ปรัชญาการบริหารความเสี่ยง • การจัดเตรียมการจัดการความเสี่ยงแบบฝัง (embedding risk management) • ยอมรับความเสี่ยงและทัศนคติต่อความเสี่ยง • การทดสอบเกณฑ์มาตรฐานสำหรับนัยสำคัญ • คำชี้แจง/นโยบายเฉพาะด้านความเสี่ยง • เทคนิคการประเมินความเสี่ยง • ลำดับความสำคัญความเสี่ยงสำหรับปีปัจจุบัน	• เครื่องมือและเทคนิค • ระบบจำแนกความเสี่ยง • ขั้นตอนการประเมินความเสี่ยง • กฎและขั้นตอนการควบคุมความเสี่ยง • การตอบสนองต่อเหตุการณ์ประเด็น และเหตุการณ์ต่าง ๆ • เอกสารและการเก็บบันทึก • การฝึกอบรมและการสื่อสาร • ขั้นตอนการตรวจสอบและโพรโทคอล • การรายงาน/การเปิดเผย/การรับรอง

3. กระบวนการ (process)

กระบวนการจัดการความเสี่ยงเกี่ยวข้องกับการใช้นโยบาย ขั้นตอน และวิธีปฏิบัติอย่างเป็นระบบกับกิจกรรมการสื่อสารและการให้คำปรึกษา (communicating and consulting) การกำหนดบริบท (scope context) การประเมินความเสี่ยง (risk assessment) การจัดการความเสี่ยง (risk treatment) ติดตามตรวจสอบ ทบทวน (monitoring and review) การบันทึกและรายงานความเสี่ยง (recording and reporting) ซึ่งแต่ละขั้นตอนมีรายละเอียดดังนี้

3.1 การสื่อสารและการให้คำปรึกษา (communicating and consulting)

เกี่ยวข้องกับการสื่อสารการบริหารความเสี่ยงให้แก่ผู้ที่มีส่วนเกี่ยวข้องทั้งภายในและภายนอกองค์กร รวมถึงการให้คำแนะนำเกี่ยวกับขั้นตอนและกระบวนการบริหารความเสี่ยง เพื่อให้เกิดความเข้าใจในการตัดสินใจดำเนินการบริหารความเสี่ยง ทราบถึง

ความจำเป็นในการดำเนินการบริหารความเสี่ยง ตลอดจนทราบขอบเขตการดำเนินงาน โดยมีการสื่อสารแลกเปลี่ยนข้อมูลระหว่างผู้ที่เกี่ยวข้องเพื่อให้เกิดความเข้าใจในแนวคิด หลักการ และวิธีปฏิบัติที่ตรงกัน ตลอดจนสามารถวิเคราะห์และจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ รวมไปถึงนำความเชี่ยวชาญด้านต่าง ๆ มารวมกันในแต่ละขั้นตอนของกระบวนการจัดการความเสี่ยง สร้างความมั่นใจว่าความคิดเห็นที่แตกต่างกันจะได้รับการพิจารณา เมื่อกำหนดเกณฑ์ความเสี่ยงและประเมินความเสี่ยง ให้ข้อมูลที่เพียงพอเพื่ออำนวยความสะดวกในการกำกับดูแลความเสี่ยงและการตัดสินใจ และการสร้างความรู้สึกไม่แบ่งแยกและความเป็นเจ้าของในหมู่ผู้ที่ได้รับผลกระทบจากความเสี่ยง

3.2 ขอบเขต บริบท และเกณฑ์ (scope, context and criteria) ซึ่งเกี่ยวข้องกับ

1) การกำหนดวัตถุประสงค์และขอบเขตของกิจกรรมการบริหารความเสี่ยง

2) การระบุบริบทหรือสภาพแวดล้อมภายนอกและภายในมีความสัมพันธ์และเกี่ยวข้องกับองค์กร

การกำหนดสภาพแวดล้อมภายนอก สภาพแวดล้อมภายนอก หมายถึง องค์ประกอบต่าง ๆ ที่อยู่ภายนอกองค์กรที่มีอิทธิพลต่อความสำเร็จของวัตถุประสงค์ขององค์กร สภาพแวดล้อมภายนอก ประกอบด้วย เศรษฐกิจ การเมือง วัฒนธรรม กฎหมาย ข้อบังคับการเงิน สภาพแวดล้อมในการแข่งขันทั้งภายในประเทศและต่างประเทศ รวมถึงการยอมรับของผู้มีส่วนได้ส่วนเสียภายนอก การทำความเข้าใจสภาพแวดล้อมภายนอกองค์กรจะช่วยสร้างความมั่นใจได้ว่า ผู้มีส่วนได้ส่วนเสียขององค์กร รวมถึงวัตถุประสงค์ของผู้ที่มีส่วนได้ส่วนเสียนั้น ๆ ได้รับการนำมาพิจารณาเพื่อกำหนดเกณฑ์ความเสี่ยง

การกำหนดสภาพแวดล้อมภายใน สภาพแวดล้อมภายใน หมายถึง สิ่งที่อยู่ภายในองค์กรซึ่งมีอิทธิพลต่อความสำเร็จของวัตถุประสงค์ขององค์กร สภาพแวดล้อมภายในขององค์กร ประกอบด้วย นโยบาย วัตถุประสงค์ วิสัยทัศน์ พันธกิจ และกลยุทธ์ที่จะต้องประสบความสำเร็จ ขีดความสามารถขององค์กรในรูปของทรัพยากรและความรู้ ระบบสารสนเทศ ผู้มีส่วนได้ส่วนเสียภายในองค์กร การรับรู้ คุณค่า และวัฒนธรรมองค์กร โครงสร้าง

โดยกระบวนการบริหารความเสี่ยงจะต้องสอดคล้องในทิศทางเดียวกันกับวัฒนธรรม กระบวนการ และโครงสร้างขององค์กร

3) กำหนดเกณฑ์ความเสี่ยงโดยระบุจำนวนและประเภทของความเสี่ยงที่ยอมรับได้

4) กำหนดเกณฑ์การประเมินความสำคัญของความเสี่ยงและเพื่อสนับสนุนการตัดสินใจ

3.3 การประเมินความเสี่ยง (risk assessment) ซึ่งเกี่ยวข้องกับ

1) การระบุความเสี่ยงเพื่อค้นหา รับรู้ และอธิบายความเสี่ยงที่อาจช่วยหรือป้องกันการบรรลุวัตถุประสงค์และความหลากหลายของผลที่ตามมาที่จับต้องได้หรือจับต้องไม่ได้

2) การวิเคราะห์ธรรมชาติและลักษณะของความเสี่ยง รวมถึงระดับความเสี่ยง แหล่งที่มาของความเสี่ยง ผลที่ตามมา โอกาส เหตุการณ์ สถานการณ์จำลอง การควบคุม และประสิทธิผล

3) การประเมินความเสี่ยงเพื่อสนับสนุนการตัดสินใจโดยเปรียบเทียบผลการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยงที่กำหนดขึ้นเพื่อกำหนดความสำคัญของความเสี่ยง

การประเมินความเสี่ยง ประกอบด้วยกระบวนการหลัก ๆ 3 กระบวนการดังต่อไปนี้

1) การระบุความเสี่ยง (risk identification) คือ องค์กรจะต้องทำการระบุถึงแหล่งที่มาของความเสี่ยงและระบุปัจจัยเสี่ยง ตลอดจนพื้นที่ที่ได้รับผลกระทบ เหตุการณ์ และสาเหตุรวมถึงผลที่จะตามมา เป้าหมายของขั้นตอนนี้จะเป็นการจัดทำรายการของความเสี่ยง จากเหตุการณ์ที่ทำให้ความสำเร็จของวัตถุประสงค์เพิ่มขึ้น ป้องกันไม่ให้เกิดความสำเร็จขึ้น ลดระดับความสำเร็จลง หรือทำให้ความสำเร็จเกิดการล่าช้า

2) การวิเคราะห์ความเสี่ยง (risk analysis) ซึ่งจะเป็นข้อมูลเพื่อใช้ในการประเมินความเสี่ยง และการตัดสินใจในการจัดการกับความเสี่ยง โดยการพิจารณาถึงผลกระทบ (impact) และโอกาสในการเกิด (likelihood) ความเสี่ยง การวิเคราะห์อาจจะเป็นได้ทั้งการวิเคราะห์เชิงคุณภาพ (qualitative) กึ่งปริมาณ (semi-quantitative) หรือเชิงปริมาณ (quantitative) หรือผสมผสานกันไป

3) การประเมินความเสี่ยง (risk evaluation) โดยจะบ่งบอกถึงระดับความสำคัญ (degree of risk) ของความเสี่ยง เป็นสถานะของความเสี่ยงที่ได้จากการวิเคราะห์ผลกระทบและโอกาสของแต่ละปัจจัยเสี่ยง ซึ่งแบ่งเป็นระดับ เช่น สูงมาก สูง ปานกลาง และต่ำ โดยองค์กรจะเป็นผู้พิจารณาระดับความสำคัญของความเสี่ยงเพื่อนำมาดำเนินการ

3.4 การจัดการความเสี่ยง (risk treatment) เกี่ยวข้องกับ

1) การเลือกตัวเลือกการจัดการความเสี่ยงที่เหมาะสมที่สุด

2) การออกแบบแผนการจัดการความเสี่ยงโดยระบุวิธีรักษาทางเลือกที่จะดำเนินการ

แนวทางในการจัดการความเสี่ยงจะประกอบด้วย

1) การหลีกเลี่ยงความเสี่ยง (risk avoidance) เป็นการเลี่ยงกิจกรรมที่เป็นสาเหตุนำมาซึ่งความเสี่ยง โดยการตัดสินใจที่จะไม่เริ่มต้นหรือดำเนินการต่อในกิจกรรมที่เกิดความเสี่ยงขึ้น ซึ่งจะมีผลกระทบต่อองค์กร เช่น การหยุดดำเนินการ การยกเลิกโครงการ หรือการมอบให้ผู้บริการภายนอกเป็นผู้ดำเนินการแทน

2) การลดความเสี่ยง (risk reduction) เป็นการลดความถี่หรือโอกาสที่จะเกิด (likelihood) ความเสี่ยง หรือผลกระทบ (impact) หรือความเสียหายที่จะเกิดขึ้น โดยการควบคุมภายในหรือปรับปรุงเปลี่ยนแปลงการดำเนินงานเพื่อช่วยลดโอกาสที่จะเกิดความเสียหาย ลดความเสียหาย หรือทั้งสองอย่าง เช่น การฝึกอบรมให้กับบุคลากร การจัดทำคู่มือการปฏิบัติงาน การจัดทำแผนสำรองเพื่อรับมือไว้ล่วงหน้าก่อนที่ความสูญเสียจะเกิดขึ้นจริง ซึ่งจะช่วยให้เกิดความตระหนักถึงความเสี่ยงและช่วยให้ลดระดับความรุนแรงของความสูญเสียลงได้

3) การแบ่งปันความเสี่ยงให้กับหน่วยงานอื่น ๆ (risk sharing) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้หน่วยงานอื่นทั้งภายในและภายนอกองค์กร เพื่อช่วยลดโอกาสที่จะเกิดความเสี่ยงหรือระดับความรุนแรงของความเสียหายจากความเสี่ยงหนึ่ง ๆ เช่น การทำประกันภัยในรูปแบบต่าง ๆ การจัดหาผู้เชี่ยวชาญจากภายนอกมาดำเนินการแทนในกรณีที่บุคลากรภายนอกนั้นมีทักษะหรือความชำนาญมากกว่า

4) การยอมรับหรือเก็บรักษาความเสี่ยงไว้ (risk acceptance) เป็นความเสี่ยงที่หน่วยงานสามารถยอมรับได้ เนื่องจากความเสี่ยงนั้นมีโอกาสเกิดขึ้นน้อย และผลกระทบความเสี่ยงไม่มาก หรือเป็นความเสี่ยงที่มีต้นทุนในการจัดการสูง ไม่คุ้มค่ากับผลที่จะได้รับ

3.5 การติดตามและตรวจสอบ (monitoring and reviewing) เกี่ยวข้องกับ

1) การปรับปรุงคุณภาพและประสิทธิผลของการออกแบบกระบวนการการนำไปปฏิบัติ และผลลัพธ์

2) การเฝ้าติดตามกระบวนการจัดการความเสี่ยงและผลลัพธ์ โดยมีการกำหนดความรับผิดชอบอย่างชัดเจน

3) วางแผน รวบรวม และวิเคราะห์ข้อมูล บันทึกผล และให้ข้อเสนอแนะ

4) รวมผลลัพธ์ในการจัดการประสิทธิภาพ การวัดผล และการรายงานกิจกรรม

3.6 การบันทึกและการรายงาน (recording and reporting) เกี่ยวข้องกับ

1) การสื่อสารกิจกรรมการบริหารความเสี่ยงและผลลัพธ์ทั่วทั้งองค์กร

2) การให้ข้อมูลเพื่อการตัดสินใจ

3) การปรับปรุงกิจกรรมการบริหารความเสี่ยง

4) การให้ข้อมูลความเสี่ยงและการโต้ตอบกับผู้มีส่วนได้ส่วนเสีย

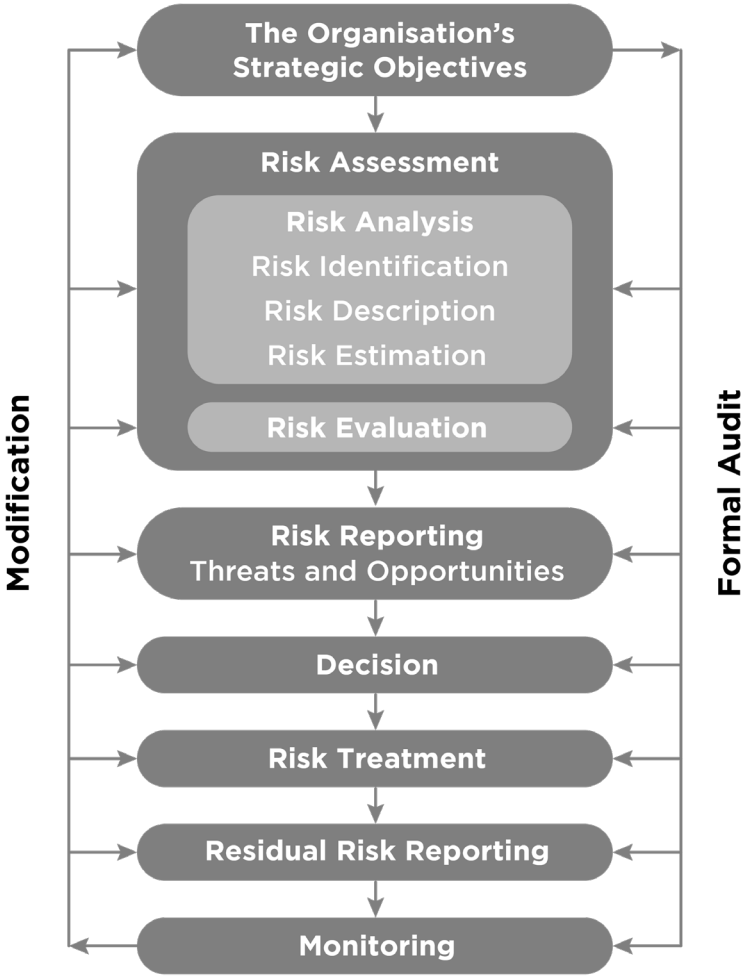
1.2.3 Federation of European Risk Management Associations (FERMA)

นอกจากกรอบการบริหารความเสี่ยงที่นำมาประยุกต์ใช้กันอย่าง COSO ERM 2017 และ ISO 31000 ที่ได้นำเสนอในข้างต้นแล้วนั้น ยังมีกรอบการบริหารความเสี่ยงที่พัฒนาขึ้นโดยองค์กรอื่น ๆ ซึ่งในหนังสือเล่มนี้ได้รวบรวมไว้เพื่อเป็นประโยชน์ต่อผู้อ่านในการนำไปปรับใช้เป็นแนวทางการบริหารความเสี่ยงของสถาบันอุดมศึกษาต่อไป

มาตรฐานการบริหารความเสี่ยง (Risk Management Standard) ที่จัดทำขึ้นโดย FERMA หรือ Federation of European Risk Management Associations ซึ่งเชื่อว่าการบริหารความเสี่ยงเป็นส่วนสำคัญของการจัดการเชิงกลยุทธ์ขององค์กร เป็นกระบวนการที่องค์กรจัดการกับความเสี่ยงที่เกี่ยวข้องกับกิจกรรมของตนอย่างเป็น

ระบบ โดยมีเป้าหมายในการบรรลุผลประโยชน์อย่างยั่งยืนภายในแต่ละกิจกรรมและในพอร์ตโฟลิโอ (portfolio) ของกิจกรรมทั้งหมด จุดเน้นของการจัดการความเสี่ยงที่ดี คือ การระบุและจัดการกับความเสี่ยงเหล่านี้โดยมีวัตถุประสงค์เพื่อเพิ่มมูลค่าสูงสุดอย่างยั่งยืนให้กับทุกกิจกรรมขององค์กร ซึ่งรวบรวมความเข้าใจเกี่ยวกับศักยภาพและข้อเสียของปัจจัยเหล่านั้นทั้งหมดที่อาจส่งผลต่อองค์กร ช่วยเพิ่มความน่าจะเป็นของความสำเร็จและลดทั้งความน่าจะเป็นของความล้มเหลวและความไม่แน่นอนในการบรรลุวัตถุประสงค์โดยรวมขององค์กร

การบริหารความเสี่ยงควรเป็นกระบวนการที่ต่อเนื่องและกำลังพัฒนาซึ่งดำเนินไปทั่วทั้งกลยุทธ์ขององค์กร และการดำเนินการตามกลยุทธ์นั้น ควรจัดการกับความเสี่ยงทั้งหมดที่เกี่ยวข้องกับกิจกรรมขององค์กรทั้งในอดีต ปัจจุบัน และอนาคตอย่างเป็นระบบ จะต้องบูรณาการเข้ากับวัฒนธรรมขององค์กรด้วยนโยบายที่มีประสิทธิภาพ และโปรแกรมที่นำโดยผู้บริหารระดับสูงที่สุด ต้องแปลกลยุทธ์เป็นวัตถุประสงค์ทางยุทธวิธีและการปฏิบัติงาน โดยมอบหมายความรับผิดชอบทั่วทั้งองค์กร มีผู้จัดการและพนักงานแต่ละคนที่รับผิดชอบในการจัดการความเสี่ยงเป็นส่วนหนึ่งของรายละเอียดงาน สนับสนุนความรับผิดชอบ การวัดผลการปฏิบัติงาน และการให้รางวัล ซึ่งจะช่วยส่งเสริมประสิทธิภาพการปฏิบัติงานในทุกระดับ โดยกระบวนการบริหารความเสี่ยงตามกรอบของ FERMA มีขั้นตอนดังต่อไปนี้



รูปที่ 5 กรอบแนวคิดและกระบวนการบริหารความเสี่ยงของ FERMA

1. กระบวนการจัดการความเสี่ยง

ในกระบวนการบริหารจัดการความเสี่ยงตามมาตรฐาน FERMA เริ่มต้นจากการกำหนดวัตถุประสงค์เชิงกลยุทธ์ขององค์กร จึงนำไปสู่ขั้นตอนต่อไป คือ

1.1 การประเมินความเสี่ยง (risk assessment) การประเมินความเสี่ยงถูกกำหนดโดย ISO/IEC Guide 73 ว่าเป็นกระบวนการโดยรวมของการวิเคราะห์ความเสี่ยงและการประเมินความเสี่ยง ซึ่งประกอบไปด้วยขั้นตอนสำคัญ 2 ขั้นตอน ได้แก่

การวิเคราะห์ความเสี่ยง (risk analysis) และการประเมินความเสี่ยง (risk evaluation) โดยมีเนื้อหารายละเอียดในแต่ละขั้นตอนดังนี้

1.1.1 การวิเคราะห์ความเสี่ยง ประกอบไปด้วยขั้นต่าง ๆ ดังนี้

1) การระบุความเสี่ยง (risk identification) การระบุความเสี่ยงกำหนดขึ้นเพื่อระบุความเสี่ยงขององค์กรต่อความไม่แน่นอน สิ่งนี้ต้องการความรู้ที่ลึกซึ้งขององค์กรตลาดที่กิจการหรือองค์กรดำเนินการ สภาพแวดล้อมทางกฎหมาย สังคม การเมือง และวัฒนธรรมที่มีอยู่ ตลอดจนการพัฒนาความเข้าใจที่ถูกต้องเกี่ยวกับวัตถุประสงค์เชิงกลยุทธ์และการดำเนินงานขององค์กร รวมถึงปัจจัยที่สำคัญต่อความสำเร็จและภัยคุกคามและโอกาสที่เกี่ยวข้องกับความสำเร็จของวัตถุประสงค์เหล่านี้

การระบุความเสี่ยงควรได้รับการติดต่ออย่างเป็นระบบเพื่อให้แน่ใจว่ากิจกรรมที่สำคัญทั้งหมดภายในองค์กรได้รับการระบุและความเสี่ยงทั้งหมดที่เกิดจากกิจกรรมเหล่านี้ที่กำหนดไว้ ความผันผวนทั้งหมดที่เกี่ยวข้องกับกิจกรรมเหล่านี้ควรได้รับการระบุและจัดหมวดหมู่

โดยกิจกรรมทางธุรกิจและการตัดสินใจสามารถจำแนกได้หลายวิธี ตัวอย่างเช่น

(1) ด้านยุทธศาสตร์ สิ่งเหล่านี้เกี่ยวข้องกับวัตถุประสงค์เชิงกลยุทธ์ระยะยาวขององค์กร สิ่งเหล่านี้อาจได้รับผลกระทบจากพื้นที่ต่าง ๆ เช่น ความพร้อมของเงินทุน ความเสี่ยงด้านอำนาจอธิปไตยและทางการเมือง การเปลี่ยนแปลงทางกฎหมายและกฎระเบียบ ชื่อเสียง และการเปลี่ยนแปลงในสภาพแวดล้อมทางกายภาพ

(2) ด้านการดำเนินงาน สิ่งเหล่านี้เกี่ยวข้องกับปัญหาในแต่ละวันที่องค์กรต้องเผชิญในขณะที่มุ่งมั่นที่จะบรรลุวัตถุประสงค์เชิงกลยุทธ์

(3) ด้านการเงิน สิ่งเหล่านี้เกี่ยวข้องกับการจัดการและการควบคุมการเงินขององค์กรอย่างมีประสิทธิภาพ และผลกระทบของปัจจัยภายนอก เช่น ความพร้อมของสินเชื่ออัตราแลกเปลี่ยนเงินตราต่างประเทศ การเคลื่อนไหวของอัตราดอกเบี้ย และความเสี่ยงต่อตลาดอื่น ๆ

(4) ด้านการจัดการความรู้ สิ่งเหล่านี้เกี่ยวข้องกับการจัดการที่มีประสิทธิภาพและการควบคุมแหล่งความรู้ การผลิต การป้องกัน และการสื่อสาร ปัจจัยภายนอกอาจรวมถึงการใช้โดยไม่ได้รับอนุญาตหรือการละเมิดทรัพย์สินทางปัญญา ไฟฟ้าดับ

ในพื้นที่ และเทคโนโลยีการแข่งขัน ปัจจัยภายในอาจทำให้ระบบทำงานผิดพลาดหรือสูญเสียพนักงานหลัก

(5) ด้านการปฏิบัติตาม ข้อกังวลเหล่านี้ เช่น สุขภาพและความปลอดภัยสิ่งแวดล้อม คำอธิบายทางการค้า การคุ้มครองผู้บริโภค การปกป้องข้อมูล แนวทางปฏิบัติในการจ้างงาน และประเด็นด้านกฎระเบียบ

แม้ว่าที่ปรึกษาภายนอกสามารถระบุความเสี่ยงได้ แต่แนวทางภายในองค์กรที่มีกระบวนการและเครื่องมือที่สื่อสารกัน สอดคล้องกัน และประสานงานกันเป็นอย่างดีมีแนวโน้มที่จะมีประสิทธิภาพมากกว่า **“ความเป็นเจ้าของ”** ของกระบวนการบริหารความเสี่ยงเป็นสิ่งสำคัญ ตัวอย่างเทคนิคที่ใช้ในการระบุความเสี่ยงมีดังนี้

- การระดมความคิด
- แบบสอบถาม
- การศึกษาทางธุรกิจที่พิจารณากระบวนการทางธุรกิจแต่ละอย่างและอธิบายทั้งกระบวนการภายในและปัจจัยภายนอกที่มีอิทธิพลต่อกระบวนการเหล่านั้น
- การเปรียบเทียบอุตสาหกรรม
- การวิเคราะห์สถานการณ์
- การประชุมเชิงปฏิบัติการการประเมินความเสี่ยง
- การสอบสวนเหตุการณ์
- การตรวจสอบและการตรวจสอบ
- HAZOP (การศึกษาอันตรายและการใช้งาน)

2) คำอธิบายความเสี่ยง (risk description) วัตถุประสงค์ของคำอธิบายความเสี่ยง คือ เพื่อแสดงความเสี่ยงที่ระบุในรูปแบบที่มีโครงสร้าง เช่น โดยใช้ตารางคำอธิบายความเสี่ยงที่เรียกว่า **“ตารางโอเวอร์ลีฟ (Table Overleaf)”** สามารถใช้เพื่ออำนวยความสะดวกในการอธิบายและประเมินความเสี่ยง การใช้โครงสร้างที่ออกแบบมาอย่างดีมีความจำเป็นเพื่อให้แน่ใจว่า การระบุความเสี่ยง คำอธิบาย และกระบวนการประเมินอย่างครอบคลุม เมื่อพิจารณาถึงผลที่ตามมาและความน่าจะเป็นของความเสี่ยงแต่ละอย่างที่ระบุไว้ในตาราง ควรจัดลำดับความสำคัญของความเสี่ยงที่สำคัญที่ต้องวิเคราะห์ในรายละเอียดเพิ่มเติม การระบุความเสี่ยงที่เกี่ยวข้องกับกิจกรรมทางธุรกิจและการตัดสินใจ

อาจถูกจัดประเภทเป็น กลยุทธ์ โครงการ/ยุทธวิธี การปฏิบัติงาน สิ่งสำคัญคือต้องรวมการจัดการความเสี่ยงไว้ในขั้นตอนแนวคิดของโครงการตลอดจนอายุของโครงการหนึ่ง ๆ

3) การติดตามการประเมินความเสี่ยง (risk estimation monitoring)

การประมาณความเสี่ยงอาจเป็นการประเมินเชิงปริมาณ กึ่งเชิงปริมาณ หรือเชิงคุณภาพในแง่ของความน่าจะเป็นที่จะเกิดขึ้นและผลที่ตามมา ตัวอย่างเช่น ผลที่ตามมาทั้งในแง่ของภัยคุกคาม (ความเสี่ยงด้านลบ) และโอกาส (ความเสี่ยงด้านบวก) อาจสูง ปานกลาง หรือต่ำ ความน่าจะเป็นอาจสูง ปานกลาง หรือต่ำ แต่ต้องมีคำจำกัดความที่แตกต่างกันในแง่ของภัยคุกคามและโอกาส

ตารางที่ 1 ระบุระดับของผลที่ตามมา – ทั้งภัยคุกคามและโอกาส

ระดับ	คำจำกัดความ
สูง	- ส่งผลกระทบทางการเงินต่อองค์กรมีแนวโน้มที่จะเกิน £x - ส่งผลกระทบต่อกลยุทธ์ขององค์กรหรือกิจกรรมการดำเนินงานอย่างมีนัยสำคัญ - ส่งผลต่อความกังวลของผู้มีส่วนได้ส่วนเสียที่สำคัญ
กลาง	- ส่งผลกระทบทางการเงินต่อองค์กรน่าจะอยู่ระหว่าง £x ถึง £y - ส่งผลกระทบต่อกลยุทธ์ขององค์กรหรือกิจกรรมการดำเนินงานในระดับปานกลาง - เกี่ยวข้องกับความกังวลของผู้มีส่วนได้ส่วนเสียในระดับปานกลาง
ต่ำ	- ส่งผลกระทบทางการเงินต่อองค์กรน่าจะน้อยกว่า £y - ส่งผลกระทบต่อกลยุทธ์ขององค์กรหรือกิจกรรมการดำเนินงานในระดับต่ำ - เกี่ยวข้องกับความกังวลของผู้มีส่วนได้ส่วนเสียในระดับต่ำ

ตารางที่ 2 ระบุระดับความน่าจะเป็นของการเกิดขึ้น – ภัยคุกคาม

การประเมิน	คำอธิบาย	ตัวชี้วัด
สูง (น่าจะ)	มีแนวโน้มที่จะเกิดขึ้นทุกปี หรือมีโอกาสเกิดขึ้นมากกว่า 25%	- มีโอกาสเกิดขึ้นได้หลายครั้งภายในระยะเวลาหนึ่ง (เช่น 10 ปี) - เกิดขึ้นเมื่อไม่นานมานี้
ปานกลาง (เป็นไปได้)	มีแนวโน้มที่จะเกิดขึ้นในระยะเวลา 10 ปี หรือน้อยกว่า 25% มีโอกาสที่จะเกิดขึ้น	- อาจเกิดขึ้นมากกว่า 1 ครั้งภายในระยะเวลา (เช่น 10 ปี) - อาจควบคุมได้ยากเนื่องจากอิทธิพลภายนอกบางอย่าง - มีประวัติการเกิดขึ้นหรือไม่
ต่ำ (ระยะไกล)	ไม่น่าจะเกิดขึ้นในระยะเวลา 10 ปี หรือน้อยกว่า 2% ที่จะเกิดขึ้น	- ไม่ได้เกิดขึ้น - ไม่น่าจะเกิดขึ้น

ตารางที่ 3 ระบุความน่าจะเป็นของการเกิดขึ้น – โอกาส

การประเมิน	คำอธิบาย	ตัวชี้วัด
สูง (น่าจะ)	ผลลัพธ์ที่น่าพอใจมีแนวโน้มที่จะบรรลุผลสำเร็จใน 1 ปี หรือมีโอกาสเกิดขึ้นมากกว่า 75%	โอกาสที่ชัดเจนซึ่งสามารถวางใจได้ด้วยความแน่นอนที่สมเหตุสมผล เพื่อให้บรรลุในระยะสั้นตามกระบวนการจัดการปัจจุบัน
ปานกลาง (เป็นไปได้)	โอกาสที่สมเหตุสมผลของผลลัพธ์ที่ดีใน 1 ปี มีโอกาสเกิดขึ้น 25% ถึง 75%	โอกาสที่อาจทำได้ แต่ต้องมีการจัดการอย่างรอบคอบ โอกาสที่อาจเกิดขึ้นเหนือแผน
ต่ำ (ระยะไกล)	มีโอกาสเกิดผลดีในระยะกลาง หรือมีโอกาสเกิดขึ้นน้อยกว่า 25%	โอกาสที่เป็นไปได้ซึ่งยังไม่ได้ถูกตรวจสอบโดยฝ่ายบริหารอย่างเต็มที่ โอกาสที่จะประสบความสำเร็จมีน้อยบนพื้นฐานของทรัพยากรการจัดการที่กำลังใช้อยู่ในปัจจุบัน

วิธีและเทคนิคการวิเคราะห์ความเสี่ยง สามารถใช้เทคนิคต่าง ๆ เหล่านี้ในการวิเคราะห์ความเสี่ยงได้ เช่น

สำหรับความเสี่ยงขาขึ้น (upside risk)

- สำรวจตลาด
- การสำรวจ
- ทดสอบการตลาด
- วิจัยและพัฒนา
- การวิเคราะห์ผลกระทบทางธุรกิจ

สำหรับความเสี่ยงขาลง (downside risk)

- การวิเคราะห์ภัยคุกคาม
- การชี้บ่งอันตรายแบบการวิเคราะห์ความผิดพลาดของระบบด้วยวิธีต้นไม้ (Fault Tree Analysis: FTA)
- โหมดความล้มเหลวและการวิเคราะห์ผลกระทบ (Failure Mode and Effects Analysis: FMEA)

สำหรับความเสี่ยงทั้ง 2 ประเภท

- การสร้างแบบจำลองการพึ่งพา
- การวิเคราะห์ SWOT (จุดแข็ง จุดอ่อน โอกาส ภัยคุกคาม)
- การวิเคราะห์แผนผังเหตุการณ์
- การวางแผนความต่อเนื่องทางธุรกิจ
- BPEST (ธุรกิจ การเมือง เศรษฐกิจ การวิเคราะห์ทางสังคม เทคโนโลยี)
- การสร้างแบบจำลองตัวเลือกจริง
- การตัดสินใจภายใต้เงื่อนไขของความเสี่ยงและความไม่แน่นอน
- อนุมานทางสถิติ
- การวัดแนวโน้มศูนย์กลางและการกระจายตัว
- PESTLE (การเมือง เศรษฐกิจ สังคม เทคนิค กฎหมาย สิ่งแวดล้อม)

4) โปรไฟล์ความเสี่ยง (risk profile) ผลลัพธ์ของกระบวนการวิเคราะห์ความเสี่ยงสามารถใช้เพื่อสร้างโปรไฟล์ความเสี่ยงซึ่งให้คะแนนที่มีนัยสำคัญของความเสี่ยงแต่ละประเภท และจัดเตรียมเครื่องมือสำหรับการจัดลำดับความสำคัญ

ของความพยายามในการบำบัดความเสี่ยง จัดอันดับความเสี่ยงที่ระบุแต่ละรายการเพื่อให้มุมมองของความสำคัญสัมพัทธ์ กระบวนการนี้ช่วยให้สามารถจับคู่ความเสี่ยงกับพื้นที่ธุรกิจที่ได้รับผลกระทบ อธิบายขั้นตอนการควบคุมหลักที่มีอยู่ และระบุพื้นที่ที่ระดับของการลงทุนในการควบคุมความเสี่ยงอาจเพิ่มขึ้น ลดลง หรือแบ่งปันส่วนใหม่ ความรับผิดชอบช่วยให้มั่นใจว่า **“ความเป็นเจ้าของ”** ของความเสี่ยงได้รับการยอมรับและจัดสรรทรัพยากรการจัดการที่เหมาะสม

1.1.2 การประเมินความเสี่ยง (risk evaluation) เมื่อกระบวนการวิเคราะห์ความเสี่ยงเสร็จสิ้น จำเป็นต้องเปรียบเทียบความเสี่ยงโดยประมาณกับเกณฑ์ความเสี่ยงที่องค์กรกำหนดขึ้น เกณฑ์ความเสี่ยงอาจรวมถึงต้นทุนและผลประโยชน์ที่เกี่ยวข้อง ข้อกำหนดทางกฎหมาย ปัจจัยทางเศรษฐกิจสังคมและสิ่งแวดล้อม ความกังวลของผู้มีส่วนได้ส่วนเสีย ฯลฯ การประเมินความเสี่ยงจึงถูกนำมาใช้ในการตัดสินใจเกี่ยวกับความสำคัญของความเสี่ยงต่อองค์กรและความเสี่ยงเฉพาะแต่ละอย่างควรเป็นการยอมรับหรือรักษา

1.2 การจัดการความเสี่ยง (risk treatment) การจัดการความเสี่ยงเป็นกระบวนการคัดเลือกและดำเนินมาตรการเพื่อปรับเปลี่ยนความเสี่ยง การจัดการความเสี่ยงรวมถึงเป็นองค์ประกอบหลัก การควบคุม/บรรเทาความเสี่ยง ตัวอย่างเช่น การหลีกเลี่ยงความเสี่ยง การถ่ายโอนความเสี่ยง การลดความเสี่ยง

ระบบการจัดการความเสี่ยง ควรมีอย่างน้อย

- การดำเนินงานขององค์กรอย่างมีประสิทธิภาพและประสิทธิผล
- การควบคุมภายในที่มีประสิทธิภาพ
- การปฏิบัติตามกฎหมายและระเบียบข้อบังคับ

กระบวนการวิเคราะห์ความเสี่ยงช่วยให้การดำเนินงานขององค์กรมีประสิทธิภาพและประสิทธิผล โดยระบุความเสี่ยงที่ต้องการความสนใจฝ่ายบริหารพวกเขาจะต้องจัดลำดับความสำคัญของการดำเนินการควบคุมความเสี่ยงในแง่ของศักยภาพที่จะเป็นประโยชน์ต่อองค์กร

ประสิทธิผลของการควบคุมภายใน คือ ระดับที่ความเสี่ยงจะถูกกำจัดหรือลดลงโดยมาตรการควบคุมที่เสนอ และความคุ้มค่าของการควบคุมภายในเกี่ยวข้องกับต้นทุนการดำเนินการควบคุม เทียบกับผลประโยชน์การลดความเสี่ยงที่คาดหวัง

การควบคุมที่เสนอจะต้องมีการวัดในแง่ของผลกระทบทางเศรษฐกิจที่อาจเกิดขึ้นหากไม่มีการดำเนินการใด ๆ เทียบกับต้นทุนของการดำเนินการที่เสนอ และมักจะต้องการข้อมูลและข้อสมมติที่ละเอียดกว่าที่หาได้ในทันที

ประการสำคัญ ต้องมีการกำหนดต้นทุนในการดำเนินการ สิ่งนี้จะต้องคำนวณด้วยความแม่นยำ เนื่องจากจะกลายเป็นพื้นฐานอย่างรวดเร็วสำหรับการวัดความคุ้มค่าการสูญเสียที่คาดหวังหากไม่มีการดำเนินการจะต้องถูกประมาณการด้วย และโดยการเปรียบเทียบผลลัพธ์ ฝ่ายบริหารสามารถตัดสินใจได้ว่าจะใช้มาตรการควบคุมความเสี่ยงหรือไม่

องค์กรต้องเข้าใจกฎหมายที่บังคับใช้ และต้องใช้ระบบควบคุมเพื่อให้เป็นไปตามข้อกำหนด มีความยืดหยุ่นในบางครั้งเท่านั้น ซึ่งค่าใช้จ่ายในการลดความเสี่ยงอาจไม่สมส่วนกับความเสี่ยงนั้นโดยสิ้นเชิง

วิธีหนึ่งในการได้รับการคุ้มครองทางการเงินจากผลกระทบของความเสี่ยง คือ การจัดหาเงินทุนเพื่อความเสี่ยงซึ่งรวมถึงการประกันภัย อย่างไรก็ตาม ควรตระหนักว่าการสูญเสียหรือองค์ประกอบบางอย่างของการสูญเสียจะไม่สามารถประกันได้ เช่น ค่าใช้จ่ายที่ไม่มีประกันที่เกี่ยวข้องกับเหตุการณ์ด้านสุขภาพ ความปลอดภัย หรือสิ่งแวดล้อมที่เกี่ยวข้องกับการทำงาน ซึ่งอาจรวมถึงความเสียหายต่อขวัญกำลังใจของพนักงานและชื่อเสียงขององค์กร

1.3 การรายงานความเสี่ยงและการสื่อสาร แบ่งออกเป็น

1.3.1 การรายงานภายใน ซึ่งระดับต่าง ๆ ภายในองค์กรต้องการข้อมูลที่แตกต่างจากกระบวนการบริหารความเสี่ยง

คณะกรรมการบริษัท ควร:

- รู้เกี่ยวกับความเสี่ยงที่สำคัญที่สุดที่องค์กรต้องเผชิญ
- ทราบถึงผลกระทบที่เป็นไปได้ต่อมูลค่าผู้ถือหุ้นของการเบี่ยงเบนต่อช่วงประสิทธิภาพที่คาดหวัง

- สร้างความตระหนักรู้ในระดับที่เหมาะสมทั่วทั้งองค์กร
- รู้ว่าองค์กรจะจัดการวิกฤตอย่างไร
- รู้ถึงความสำคัญของความมั่นใจของผู้มีส่วนได้ส่วนเสียในองค์กร
- รู้วิธีจัดการการสื่อสารกับชุมชนการลงทุนตามความเหมาะสม
- มั่นใจได้ว่ากระบวนการบริหารความเสี่ยงทำงานได้อย่างมีประสิทธิภาพ
- เผยแพร่นโยบายการบริหารความเสี่ยงที่ชัดเจนครอบคลุมปรัชญาและความรับผิดชอบในการบริหารความเสี่ยง

หน่วยธุรกิจ ควร:

- ตระหนักถึงความเสี่ยงที่เข้าข่ายความรับผิดชอบ ผลกระทบที่อาจเกิดขึ้นกับพื้นที่อื่น ๆ และผลที่ตามมาที่อาจเกิดขึ้นกับพื้นที่อื่น ๆ
- มีตัวบ่งชี้ประสิทธิภาพที่ช่วยให้พวกเขาสามารถติดตามกิจกรรมทางธุรกิจและกิจกรรมทางการเงินที่สำคัญ ความคืบหน้าไปสู่วัตถุประสงค์และระบุการพัฒนาที่จำเป็นต้องมีการแทรกแซง (เช่น การคาดการณ์และงบประมาณ)
- มีระบบที่สื่อสารความแปรปรวนในงบประมาณและการคาดการณ์ด้วยความถี่ที่เหมาะสมเพื่อให้สามารถดำเนินการได้
- รายงานอย่างเป็นระบบและทันทีต่อผู้บริหารระดับสูงที่รับรู้ความเสี่ยงหรือความล้มเหลวของมาตรการควบคุมที่มีอยู่

บุคลากรภายในองค์กร ควร:

- เข้าใจความรับผิดชอบต่อความเสี่ยงของแต่ละบุคคล
- เข้าใจวิธีที่พวกเขาสามารถเปิดใช้งานการปรับปรุงอย่างต่อเนื่องของการตอบสนองการบริหารความเสี่ยง
- เข้าใจว่าการบริหารความเสี่ยงและการรับรู้ความเสี่ยงเป็นส่วนสำคัญของวัฒนธรรมองค์กร
- รายงานอย่างเป็นระบบและทันทีต่อผู้บริหารระดับสูงที่รับรู้ความเสี่ยงหรือความล้มเหลวของมาตรการควบคุมที่มีอยู่

1.3.2 การรายงานภายนอก ซึ่งบริษัทจำเป็นต้องรายงานต่อผู้มีส่วนได้ส่วนเสียอย่างสม่ำเสมอ โดยกำหนดนโยบายการบริหารความเสี่ยงและประสิทธิภาพในการบรรลุวัตถุประสงค์

ผู้มีส่วนได้ส่วนเสียจำนวนมากขึ้นมองหาองค์กรเพื่อให้หลักฐานของการจัดการที่มีประสิทธิภาพของผลการดำเนินงานที่ไม่ใช่ทางการเงินขององค์กรในด้านต่าง ๆ เช่น กิจการชุมชน สิทธิมนุษยชน หลักปฏิบัติในการจ้างงาน สุขภาพและความปลอดภัยและสิ่งแวดล้อม

การเตรียมการสำหรับการรายงานอย่างเป็นทางการของการบริหารความเสี่ยงควรระบุไว้อย่างชัดเจนและพร้อมสำหรับผู้มีส่วนได้ส่วนเสีย โดยการรายงานอย่างเป็นทางการควรมีรายละเอียดดังนี้

- วิธีการควบคุม โดยเฉพาะความรับผิดชอบในการบริหารความเสี่ยง
- กระบวนการที่ใช้ในการระบุความเสี่ยงและวิธีการจัดการความเสี่ยงโดยระบบการจัดการความเสี่ยง
- ระบบควบคุมหลักที่ใช้ในการจัดการความเสี่ยงที่สำคัญ
- มีระบบติดตามและตรวจสอบในสถานที่

ข้อบกพร่องที่สำคัญใด ๆ ที่ระบบค้นพบหรือในตัวระบบ ควรรายงานพร้อมกับขั้นตอนที่ดำเนินการเพื่อจัดการกับข้อบกพร่องเหล่านั้น

2. โครงสร้างและการบริหารการจัดการความเสี่ยง

2.1 นโยบายการบริหารความเสี่ยง นโยบายการบริหารความเสี่ยงขององค์กรควรกำหนดแนวทางและความต้องการความเสี่ยงและแนวทางการบริหารความเสี่ยง นโยบายควรกำหนดความรับผิดชอบในการบริหารความเสี่ยงทั่วทั้งองค์กร นอกจากนี้ควรอ้างอิงข้อกำหนดทางกฎหมายสำหรับคำชี้แจงนโยบาย เช่น เพื่อสุขภาพและความปลอดภัย

สิ่งที่แนบมากับกระบวนการบริหารความเสี่ยงคือ ชุดเครื่องมือและเทคนิคแบบบูรณาการเพื่อใช้ในขั้นตอนต่าง ๆ ของกระบวนการทางธุรกิจ เพื่อให้ทำงานได้อย่างมีประสิทธิภาพ กระบวนการบริหารความเสี่ยงต้องการดังนี้

1) คำมั่นสัญญาจากผู้บริหารสูงสุดและผู้บริหารระดับสูงขององค์กร

2) การกำหนดความรับผิดชอบภายในองค์กร

3) การจัดสรรทรัพยากรที่เหมาะสมสำหรับการฝึกอบรมและการพัฒนาการรับรู้ความเสี่ยงที่เพิ่มขึ้นโดยผู้มีส่วนได้ส่วนเสียทั้งหมด

2.2 บทบาทของคณะกรรมการ คณะกรรมการมีหน้าที่กำหนดทิศทางเชิงกลยุทธ์ขององค์กร ตลอดจนสร้างสภาพแวดล้อมและโครงสร้างการบริหารความเสี่ยงให้ดำเนินการได้อย่างมีประสิทธิภาพ ซึ่งอาจผ่านกลุ่มผู้บริหาร คณะกรรมการที่ไม่เป็นผู้บริหาร คณะกรรมการตรวจสอบ หรือหน่วยงานอื่นที่เหมาะสมกับแนวทางการดำเนินงานขององค์กร และสามารถทำหน้าที่เป็น **"ผู้สนับสนุน"** ในการบริหารความเสี่ยง คณะกรรมการควรพิจารณาในการประเมินระบบการควบคุมภายในเป็นอย่างน้อยดังต่อไปนี้

1) ลักษณะและขอบเขตของความเสี่ยงด้านลบที่บริษัทยอมรับได้ภายในธุรกิจเฉพาะของตน

2) โอกาสที่ความเสี่ยงดังกล่าวจะกลายเป็นความจริง

3) วิธีจัดการความเสี่ยงที่ยอมรับไม่ได้

4) ความสามารถของบริษัทในการลดความน่าจะเป็นและผลกระทบต่อธุรกิจให้เหลือน้อยที่สุด

5) ต้นทุนและประโยชน์ของความเสี่ยงและกิจกรรมการควบคุมที่ดำเนินการ

6) ประสิทธิผลของกระบวนการบริหารความเสี่ยง

7) ความเสี่ยงจากการตัดสินใจของคณะกรรมการ

2.3 บทบาทของหน่วยธุรกิจ ซึ่งรวมถึงสิ่งต่อไปนี้

1) หน่วยธุรกิจมีหน้าที่หลักในการจัดการความเสี่ยงในแต่ละวัน

2) การจัดการหน่วยธุรกิจมีหน้าที่ส่งเสริมการรับรู้ความเสี่ยงภายในการดำเนินงาน พวกเขาควรแนะนำวัตถุประสงค์การบริหารความเสี่ยงในธุรกิจของพวกเขา

3) การบริหารความเสี่ยงควรเป็นรายการประชุมฝ่ายบริหารเป็นประจำเพื่อให้พิจารณาความเสี่ยงและจัดลำดับความสำคัญของงานโดยพิจารณาจากการวิเคราะห์ความเสี่ยงที่มีประสิทธิผล

4) การจัดการหน่วยธุรกิจควรตรวจสอบให้แน่ใจว่า การบริหารความเสี่ยงรวมอยู่ในขั้นตอนแนวคิดของโครงการตลอดทั้งโครงการ

2.4 บทบาทของการบริหารความเสี่ยง หน่วยงานบริหารความเสี่ยงอาจมีตั้งแต่ผู้จัดการความเสี่ยงรายเดียว ผู้จัดการความเสี่ยงนอกเวลา ไปจนถึงแผนกบริหารความเสี่ยงเต็มรูปแบบทั้งนี้ขึ้นอยู่กับขนาดขององค์กร

บทบาทของฝ่ายบริหารความเสี่ยงควรมีดังต่อไปนี้

1) กำหนดนโยบายและกลยุทธ์การบริหารความเสี่ยง

2) เป็นผู้นำหลักด้านการบริหารความเสี่ยงในระดับกลยุทธ์และระดับปฏิบัติการ

3) การสร้างวัฒนธรรมการรับรู้ความเสี่ยงภายในองค์กร รวมทั้งการศึกษาที่เหมาะสม

4) กำหนดนโยบายและโครงสร้างความเสี่ยงภายในสำหรับหน่วยธุรกิจ

5) การออกแบบและทบทวนกระบวนการบริหารความเสี่ยง

6) ประสานงานกิจกรรมการทำงานต่าง ๆ ที่ให้คำแนะนำเกี่ยวกับปัญหาการบริหารความเสี่ยงภายในองค์กร

7) การพัฒนากระบวนการตอบสนองความเสี่ยง รวมถึงแผนงานฉุกเฉินและความต่อเนื่องทางธุรกิจ

8) จัดทำรายงานความเสี่ยงสำหรับคณะกรรมการและผู้มีส่วนได้ส่วนเสีย

2.5 บทบาทของการตรวจสอบภายใน บทบาทของผู้ตรวจสอบภายในมีแนวโน้มที่จะแตกต่างกันไปในแต่ละองค์กร ในทางปฏิบัติ บทบาทของผู้ตรวจสอบภายในอาจรวมถึงบางส่วนหรือทั้งหมดต่อไปนี้

1) เน้นงานตรวจสอบภายในเกี่ยวกับความเสี่ยงที่สำคัญตามที่ระบุโดยฝ่ายบริหารและการตรวจสอบกระบวนการบริหารความเสี่ยงทั่วทั้งองค์กร

2) ให้ความมั่นใจในการบริหารความเสี่ยง

3) ให้การสนับสนุนอย่างแข็งขันและมีส่วนร่วมในกระบวนการบริหารความเสี่ยง

4) อำนวยความสะดวกในการระบุ/ประเมินความเสี่ยง และให้ความรู้แก่เจ้าหน้าที่สายงานในการบริหารความเสี่ยงและการควบคุมภายใน

5) ประสานงานการรายงานความเสี่ยงต่อคณะกรรมการ คณะกรรมการตรวจสอบ ฯลฯ

ในการกำหนดบทบาทที่เหมาะสมที่สุดสำหรับองค์กรใดองค์กรหนึ่ง ผู้ตรวจสอบภายในควรตรวจสอบให้แน่ใจว่า ข้อกำหนดทางวิชาชีพสำหรับความเป็นอิสระและความเที่ยงธรรมจะไม่ถูกละเมิด

2.6 ทรัพยากรและการนำไปปฏิบัติ ควรมีการกำหนดทรัพยากรที่จำเป็นในการดำเนินการตามนโยบายการบริหารความเสี่ยงขององค์กรอย่างชัดเจนที่ระดับการจัดการแต่ละระดับและภายในแต่ละหน่วยธุรกิจ นอกเหนือจากหน้าที่การปฏิบัติงานอื่น ๆ ที่พวกเขาอาจมี ผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงควรมีบทบาทในการประสานงานนโยบาย/กลยุทธ์การบริหารความเสี่ยงที่กำหนดไว้อย่างชัดเจน คำจำกัดความที่ชัดเจนเช่นเดียวกันเป็นสิ่งจำเป็นสำหรับผู้ที่เกี่ยวข้องในการตรวจสอบและทบทวนการควบคุมภายในและการอำนวยความสะดวกในกระบวนการบริหารความเสี่ยง การบริหารความเสี่ยงควรฝังอยู่ภายในองค์กรด้วยกลยุทธ์และกระบวนการด้านงบประมาณ ควรเน้นในการปฐมนิเทศและการฝึกอบรมและการพัฒนาอื่น ๆ ทั้งหมดตลอดจนภายในกระบวนการปฏิบัติงาน เช่น โครงการพัฒนาผลิตภัณฑ์/บริการ

3. การติดตามและทบทวนกระบวนการบริหารความเสี่ยง

การจัดการความเสี่ยงที่มีประสิทธิภาพจำเป็นต้องมีโครงสร้างการรายงานและทบทวนเพื่อให้แน่ใจว่ามีการระบุและประเมินความเสี่ยงอย่างมีประสิทธิภาพ และมีการควบคุมและการตอบสนองที่เหมาะสม ควรดำเนินการตรวจสอบการปฏิบัติตามนโยบายและมาตรฐานอย่างสม่ำเสมอ และทบทวนประสิทธิภาพมาตรฐานเพื่อระบุโอกาสในการปรับปรุง

ควรจำไว้ว่า องค์กรมีพลวัตและดำเนินการในสภาพแวดล้อมแบบไดนามิก การเปลี่ยนแปลงในองค์กรและสภาพแวดล้อมในการดำเนินงานต้องได้รับการระบุและปรับเปลี่ยนระบบอย่างเหมาะสม กระบวนการติดตามควรให้ความมั่นใจว่ามีการควบคุมที่เหมาะสมสำหรับกิจกรรมขององค์กร และมีความเข้าใจและปฏิบัติตามขั้นตอน การเปลี่ยนแปลงในองค์กรและสภาพแวดล้อมที่ดำเนินการต้องได้รับการระบุและการเปลี่ยนแปลงที่เหมาะสมที่ทำกับระบบต่าง ๆ

กระบวนการตรวจสอบและทบทวนควรกำหนดดังนี้

1. มาตรการที่นำมาใช้ส่งผลให้เป็นไปตามที่ตั้งใจไว้

2. ขั้นตอนที่นำมาใช้และข้อมูลที่รวบรวมเพื่อดำเนินการประเมินมีความเหมาะสม

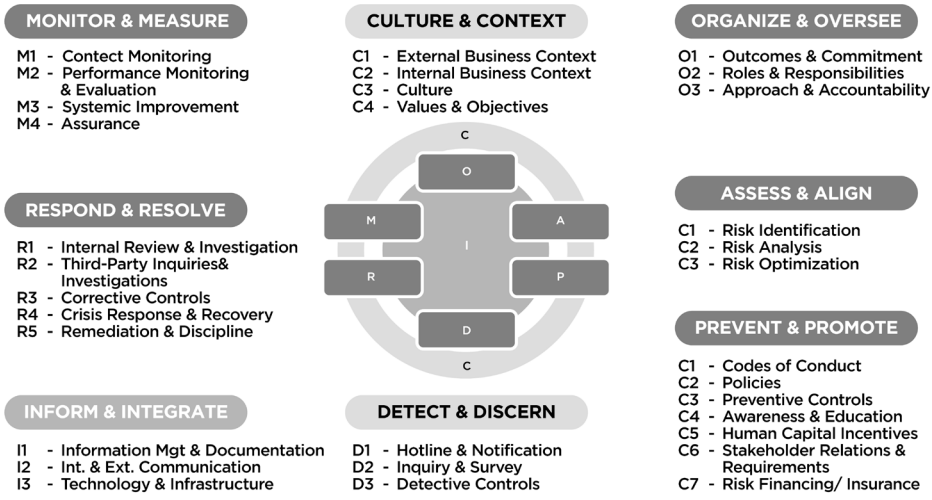
3. ความรู้ที่ได้รับการปรับปรุงจะช่วยให้ตัดสินใจได้ดีขึ้น และระบุบทเรียนที่สามารถเรียนรู้สำหรับการประเมินและการจัดการความเสี่ยงในอนาคต

1.2.4 GRC Capability Model “Red Book” 2.0

สำหรับองค์กรที่มีการวางระบบบริหารความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผลแล้ว การบริหารความเสี่ยงอาจถือได้ว่าเป็นเพียงหนึ่งกระบวนการที่จะนำพาให้องค์กรมีการบริหารจัดการอย่างมีธรรมาภิบาลเท่านั้น ในระดับสากลจึงมีหลักการในการบูรณาการการบริหารความเสี่ยงเข้ากับธรรมาภิบาล (governance) และการปฏิบัติตามข้อกำหนด (compliance) ขึ้น ในประเทศไทย หลักเกณฑ์การประเมินกระบวนการปฏิบัติงานและการจัดการของรัฐวิสาหกิจ (State Enterprise Assessment Model: SE-AM) ได้กำหนดให้เรื่องของ GRC: Governance Risk and Compliance เป็นหนึ่งในส่วนสำคัญที่จะช่วยให้การบริหารความเสี่ยงขององค์กรเป็นไปอย่างมีประสิทธิภาพ ซึ่งผู้เขียนเห็นว่า ในอนาคต ในสถาบันอุดมศึกษาน่าจะมีการนำกรอบแนวคิดนี้มาประยุกต์ใช้กันอย่างแพร่หลายมากขึ้น จึงควรที่จะเรียนรู้ไว้เพื่อใช้ยกระดับกระบวนการบริหารความเสี่ยงต่อไป

GRC Capability Model

Open Compliance and Ethics Group (OCEG) ผู้พัฒนากรอบแนวคิด **“GRC”** ขึ้นใน ค.ศ. 2002 กล่าวว่า หัวใจของกรอบแนวคิด OCEG คือ GRC Capability Model แม้ว่าจะมีมาตรฐานและกรอบแนวทางต่าง ๆ ที่กล่าวถึงองค์ประกอบของธรรมาภิบาล การจัดการความเสี่ยงและการปฏิบัติตามข้อกำหนด แต่ OCEG GRC Capability Model เป็นเพียงแนวทางเดียวที่ให้แนวทางปฏิบัติที่ครอบคลุมและมีรายละเอียดสำหรับระบบ GRC แบบบูรณาการ รูปที่ 6 แสดงถึงองค์ประกอบต่าง ๆ ที่ประกอบกันเป็นระบบ GRC ที่สมบูรณ์



รูปที่ 6 องค์ประกอบของ GRC Capability Model

การใช้องค์ประกอบใน GRC Capability Model และแนวทางปฏิบัติภายในมีส่วนช่วยองค์กรดังนี้

1. บรรลุวัตถุประสงค์ทางธุรกิจ
2. ป้องกัน ตรวจจับ และลดความทุกข์ยากที่อาจเกิดขึ้นในองค์กร
3. ส่งเสริมวัฒนธรรมองค์กร
4. กระตุ้นและสร้างแรงบันดาลใจในการดำเนินการที่ต้องการ
5. เพิ่มความมั่นใจของผู้มีส่วนได้ส่วนเสีย
6. ปรับปรุงการตอบสนองและเพิ่มประสิทธิภาพ
7. เตรียมและปกป้ององค์กร
8. เพิ่มประสิทธิภาพทางเศรษฐกิจและสังคม

GRC: การกำกับดูแล (Governance) การบริหารความเสี่ยง (Risk) การปฏิบัติตามข้อกำหนด (Compliance)

องค์กรกำลังรวมกิจกรรม GRC เพื่อให้บรรลุตามหลักการปฏิบัติงานในลักษณะที่มีประสิทธิผล มีประสิทธิภาพ และมีการตอบสนองที่ดี เพื่อให้บรรลุผลสำเร็จสูงสุด GRC คือ ระบบของบุคคล กระบวนการ และเทคโนโลยีที่จะช่วยให้องค์กรมีความสามารถดังนี้

1. เข้าใจและจัดลำดับความสำคัญของความคาดหวังของผู้มีส่วนได้ส่วนเสีย
2. กำหนดวัตถุประสงค์ทางธุรกิจที่สอดคล้องกับค่านิยมและความเสี่ยง
3. บรรลุวัตถุประสงค์ในขณะที่ปรับโปรไฟล์ความเสี่ยงให้เหมาะสมและปกป้องมูลค่า
4. ดำเนินการภายในขอบเขตทางกฎหมาย สัญญา ภายในองค์กร สังคม และจริยธรรม
5. ให้ข้อมูลที่เกี่ยวข้องที่เชื่อถือได้และทันเวลาแก่ผู้มีส่วนได้ส่วนเสียที่เหมาะสม
6. เปิดใช้งานการวัดประสิทธิภาพและประสิทธิผลของระบบ

ดังนั้น **“กิจกรรม GRC”** คือ กระบวนการหรือกิจกรรมใด ๆ ที่เอื้อต่อหรือเป็นส่วนหนึ่งของระบบ กระบวนการและฟังก์ชันที่มักจะรวมอยู่ด้วย ได้แก่

1. ธรรมาภิบาล
2. การจัดการกลยุทธ์และผลการดำเนินธุรกิจ
3. การบริหารความเสี่ยง
4. การปฏิบัติตามข้อกำหนด
5. การควบคุมภายใน
6. ความปลอดภัยขององค์กร
7. กฎหมาย
8. เทคโนโลยีสารสนเทศ
9. จริยธรรมทางธุรกิจ
10. ความยั่งยืนและความรับผิดชอบต่อสังคม
11. การจัดการคุณภาพ
12. ทุนมนุษย์และวัฒนธรรม
13. การตรวจสอบและการประกัน
14. การเงิน

โดยแต่ละส่วนนี้มีส่วนสนับสนุนความสามารถขององค์กรในการขับเคลื่อนประสิทธิภาพตามหลักการ และทุกส่วนสามารถได้รับประโยชน์จากการสื่อสารที่ได้รับการปรับปรุง กลยุทธ์ที่ใช้ร่วมกัน กระบวนการทั่วไป กำหนดการที่ประสานกัน และเทคโนโลยีแบบบูรณาการ

กระบวนการภายใต้พื้นที่ของการกำกับดูแล การจัดการความเสี่ยง และการปฏิบัติตามข้อกำหนด มีความสำคัญอย่างยิ่งต่อความสำเร็จของระบบ ดังนั้น การดูคำจำกัดความให้ลึกยิ่งขึ้นจึงมีประโยชน์อย่างมาก

• **ธรรมาภิบาล (governance)** คือ วัฒนธรรม ค่านิยม พันธกิจ โครงสร้างของนโยบาย กระบวนการ และมาตรการที่องค์กรได้รับการกำกับและควบคุม ธรรมาภิบาลในบริบทนี้ไม่จำกัดเฉพาะกิจกรรมของคณะกรรมการ หน่วยงานกำกับดูแลในระดับต่าง ๆ ทั่วทั้งองค์กรก็มีบทบาทสำคัญเช่นกัน

• **ความเสี่ยง (risk)** คือ การวัดความเป็นไปได้ของสิ่งที่เกิดขึ้นซึ่งจะส่งผลต่อการบรรลุวัตถุประสงค์ การบริหารความเสี่ยงจึงเป็นการประยุกต์ใช้กระบวนการและโครงสร้างอย่างเป็นระบบที่ช่วยให้องค์กรสามารถระบุ ประเมิน วิเคราะห์ เพิ่มประสิทธิภาพ ติดตาม ปรับปรุง หรือโอนความเสี่ยงในขณะที่สื่อสารความเสี่ยงและการตัดสินใจเกี่ยวกับความเสี่ยงไปยังผู้มีส่วนได้ส่วนเสีย เป้าหมายที่เหนือกว่าของการบริหารความเสี่ยงคือการตระหนักถึงโอกาสที่อาจเกิดขึ้นในขณะที่จัดการผลกระทบจากความเสี่ยง

• **การปฏิบัติตามข้อกำหนด (compliance)** คือ การปฏิบัติตามและความสามารถในการแสดงให้เห็นถึงการปฏิบัติตามข้อกำหนดที่ได้รับคำสั่ง ซึ่งกำหนดโดยกฎหมายและข้อบังคับ ตลอดจนข้อกำหนดโดยสมัครใจที่เกิดจากภาระผูกพันตามสัญญาและนโยบายชั่วคราว

บทบาทสำคัญและความรับผิดชอบ

1. บทบาทของคณะกรรมการ (role of board) คณะกรรมการมีหน้าที่กำกับดูแลระบบและเป็นผู้รับผลประโยชน์หลักของระบบ เนื่องจากระบบ GRC ที่เข้มแข็งช่วยให้สามารถส่งข้อมูลที่ถูกต้องแม่นยำ ซึ่งจำเป็นต่อการกำกับดูแลอย่างมีประสิทธิภาพ ดังนั้น คณะกรรมการจะต้องเป็นผู้เฝ้าติดตามผลประโยชน์ของผู้ถือหุ้นและผู้มีส่วนได้ส่วนเสีย

หน้าที่สำคัญของคณะกรรมการมีดังนี้

1) กำหนดวัตถุประสงค์และผลลัพธ์ที่ต้องการของระบบ

2) กำหนดกฎบัตรสำหรับการมีส่วนร่วมในระบบ

3) ตรวจสอบวัตถุประสงค์ทางธุรกิจและให้แน่ใจว่าสอดคล้องกับค่านิยมและความเสี่ยง

4) มีความรู้เกี่ยวกับการออกแบบและการทำงานของระบบ
5) ได้รับการประกันอย่างสม่ำเสมอว่าระบบมีประสิทธิภาพ
6) ได้รับการรับรองตามสมควรว่าคำรับรองของฝ่ายบริหารนั้นถูกต้อง
7) กำกับดูแลกิจกรรมการควบคุมของผู้บริหารระดับสูง
8) คัดเลือก ประเมิน ชดเชย และยกเลิกผู้บริหารระดับสูง
9) การจัดการกับปัญหาระยะยาวที่อาจเกินวาระการดำรงตำแหน่งของผู้บริหารระดับสูง

เพื่อให้บรรลุความรับผิดชอบดังกล่าว คณะกรรมการจำเป็นต้องมีหลักธรรมาภิบาลที่มีประสิทธิผล ภายใต้กฎหมายของสหรัฐฯ ธรรมาภิบาลเป็นสิ่งจำเป็นต่อการปฏิบัติหน้าที่ของกรรมการที่จะต้องปฏิบัติด้วยความสุจริตใจ

2. บทบาทของฝ่ายบริหารจัดการ (role of management) ฝ่ายบริหารต้องดำเนินการวางแผนเชิงกลยุทธ์และดำเนินการตามระบบ GRC โดยรวม

หน้าที่สำคัญของผู้บริหารมีดังนี้
1) ออกแบบ ดำเนินการ และปฏิบัติการระบบที่มีประสิทธิภาพ
2) ให้การรับรองอย่างสม่ำเสมอเกี่ยวกับประสิทธิภาพของระบบ
3) สื่อสารกับผู้มีส่วนได้ส่วนเสียที่สำคัญเกี่ยวกับประสิทธิภาพของระบบ
4) ประเมินและเพิ่มประสิทธิภาพการทำงานของระบบ

3. บทบาทของการประกัน (role of assurance) ฝ่ายบริหารควรได้รับและให้การรับรองอย่างสม่ำเสมอเกี่ยวกับประสิทธิภาพและประสิทธิผลของระบบ GRC การทบทวนโดยอิสระสามารถเปิดมุมมองของระบบที่เผยให้เห็นจุดอ่อนในการออกแบบหรือการดำเนินงาน และยังเปิดโอกาสให้มีการบูรณาการและแลกเปลี่ยนแนวทางปฏิบัติที่ดีที่สุดจากพื้นที่หนึ่งไปยังอีกองค์กรหนึ่ง ในส่วนของคณะกรรมการนั้นจำเป็นต้องได้รับการประกันอย่างสม่ำเสมอเกี่ยวกับประสิทธิภาพของระบบ และควรใช้ข้อมูลที่พัฒนาขึ้นโดยอิสระจากฝ่ายบริหาร จำเป็นต้องมีการตรวจสอบโดยอิสระโดยบุคลากรภายในหรือภายนอก โดยบุคลากรภายนอกจะได้รับความเป็นอิสระในระดับสูงสุด ไม่ว่าในกรณีใด

ผู้ให้การประกัน (หรือบุคลากรประกัน) ไม่ว่าภายในหรือภายนอกมีหน้าที่ดังนี้
1) ให้การรับรองว่ามีการระบุ ประเมิน จัดการ และติดตามความเสี่ยงอย่างเหมาะสม

2) ให้การรับรองอย่างสม่ำเสมอแก่คณะกรรมการและผู้บริหารว่าระบบทำงานได้อย่างมีประสิทธิภาพตามที่ออกแบบไว้

กายวิภาคของ GRC Capability Model

เพื่อให้ได้ระบบ GRC ที่มีประสิทธิภาพสูง GRC Capability Model™ — Red Book — ได้จัดเตรียมส่วนประกอบหลัก (components) องค์ประกอบ (elements) และแนวทางปฏิบัติที่ทุกองค์กรควรนำไปใช้และจัดการ

ส่วนประกอบ (components)

จะรวมเอาองค์ประกอบแบบบูรณาการของระบบ GRC ที่มีประสิทธิภาพสูง มีการทำงานค่อนข้างเป็นลำดับ เพื่อเพิ่มขีดความสามารถที่มีอยู่ ส่วนประกอบทั้งหมดต้องทำงานอย่างต่อเนื่องและสม่ำเสมอเพื่อให้ได้ระบบ GRC ที่มีประสิทธิภาพสูง

ผลลัพธ์ของระบบสากล (universal system outcomes)

universal system outcomes เป็นผลลัพธ์ที่คาดหวังและวัดผลได้ของระบบ GRC ที่มีประสิทธิภาพสูง ซึ่งผลลัพธ์ที่คาดหวังมีดังนี้

1. บรรลุวัตถุประสงค์ทางธุรกิจ และเพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจที่ต้องการ ระบบ GRC ทุกระบบต้องมีส่วนช่วยในการบรรลุวัตถุประสงค์ทางธุรกิจเหล่านั้น

2. ส่งเสริมวัฒนธรรมองค์กร สร้างแรงบันดาลใจและส่งเสริมวัฒนธรรมองค์กรในด้านประสิทธิภาพ ความรับผิดชอบ ความซื่อสัตย์ ความไว้วางใจ และการสื่อสารที่เปิดกว้าง

3. เพิ่มความมั่นใจของผู้มีส่วนได้ส่วนเสียและความไว้วางใจในองค์กร

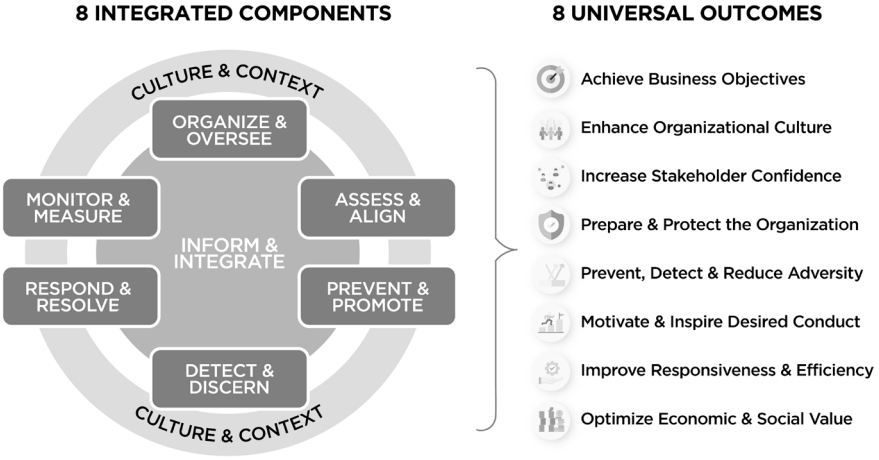
4. เตรียมความพร้อมและปกป้ององค์กร คือ การเตรียมองค์กรเพื่อจัดการกับความเสี่ยงและข้อกำหนด และปกป้ององค์กรจากผลกระทบด้านลบของเหตุการณ์ไม่พึงประสงค์ การไม่ปฏิบัติตาม และพฤติกรรมที่ผิดจรรยาบรรณ

5. ป้องกัน ตรวจจับ และลดความทุกข์ยาก กีดกัน ป้องกัน และแสดงถึงผลที่ตามมาหากมีการประพฤติมิชอบ ลดความเสียหายที่จับต้องได้และจับต้องไม่ได้ที่เกิดจากเหตุการณ์ไม่พึงประสงค์ (ทั้งที่สามารถควบคุมได้และที่ไม่สามารถทำได้ เช่น ภัยธรรมชาติ) การไม่ปฏิบัติตามข้อกำหนดและพฤติกรรมที่ผิดจรรยาบรรณ และโอกาสที่เหตุการณ์ที่คล้ายกันจะเกิดขึ้นในอนาคต

6. กระตุ้นและสร้างแรงบันดาลใจในการดำเนินการที่ต้องการ ให้สิ่งจูงใจและรางวัลสำหรับพฤติกรรมที่พึงประสงค์ โดยเฉพาะอย่างยิ่งเมื่อเผชิญกับสถานการณ์ที่ท้าทาย

7. ปรับปรุงการตอบสนองและประสิทธิภาพ มีการปรับปรุงการตอบสนองอย่างต่อเนื่อง (ความรวดเร็วและความคล่องตัว) และประสิทธิภาพ (ความเร็วและคุณภาพ) ของกิจกรรมระบบ GRC ทั้งหมด

8. เพิ่มประสิทธิภาพทางเศรษฐกิจและมูลค่าทางสังคม เพิ่มประสิทธิภาพการจัดสรรทุนมนุษย์และทุนทางการเงินให้กับกิจกรรมของระบบ GRC เพื่อเพิ่มมูลค่าสูงสุดที่สร้างประโยชน์ต่อองค์กรและสังคมที่ดำเนินงาน



รูปที่ 7 ตัวอย่าง GRC Capability Model

องค์ประกอบ (elements)

แต่ละองค์ประกอบรวบรวมแนวปฏิบัติที่เกี่ยวข้องไว้ในระบบ GRC ที่มีประสิทธิภาพสูง แต่ละองค์ประกอบประกอบด้วยการอภิปรายเกี่ยวกับหลักการและแหล่งที่มาทั่วไปของความล้มเหลว ตลอดจนแนวทางปฏิบัติที่สนับสนุนความสำเร็จ แต่ละองค์ประกอบยังรวมรายการของสิ่งที่ส่งมอบหลักและเทคโนโลยีที่เกี่ยวข้องกับองค์ประกอบ และอาจรวมถึงข้อกำหนดที่เกี่ยวข้องที่ดึงมาจากฐานข้อมูลตามข้อกำหนดของ OCEG โดยระบบ GRC ประกอบด้วยส่วนประกอบแบบบูรณาการที่ช่วยให้องค์กรสามารถ 1) เข้าใจและจัดลำดับความสำคัญความคาดหวังของผู้มีส่วนได้ส่วนเสีย 2) เพิ่มประสิทธิภาพวัตถุประสงค์ทางธุรกิจให้สอดคล้องกับค่านิยมและความเสี่ยง 3) บรรลุวัตถุประสงค์พร้อมกับจัดการ

กับความเสี่ยง 4) ดำเนินการภายในขอบเขตทางกฎหมาย สัญญา ภายใน สังคม และจริยธรรม 5) ให้ข้อมูลที่เกี่ยวข้อง เชื่อถือได้ และทันเวลาแก่ผู้มีส่วนได้ส่วนเสียที่เหมาะสม และ 6) ให้ความมั่นใจว่าระบบมีประสิทธิภาพ โดยส่วนประกอบของการบูรณาการ GRC แบ่งออกได้ทั้งสิ้น 8 องค์ประกอบ โดยมีรายละเอียดดังนี้

องค์ประกอบที่หนึ่ง: วัฒนธรรมและบริบท (culture & context)

ความเข้าใจวัฒนธรรมปัจจุบันและบริบททางธุรกิจทั้งภายในและภายนอกที่องค์กรดำเนินการ ช่วยให้ระบบ GRC สามารถจัดการกับความเป็นจริงในปัจจุบันได้ และระบุโอกาสที่จะส่งผลกระทบต่อบริบทเพื่อให้สอดคล้องกับผลลัพธ์ขององค์กรที่ต้องการมากขึ้น

1. บริบท (context) แบ่งออกเป็นบริบทภายนอกและบริบทภายใน

1.1 บริบททางธุรกิจภายนอก

1) กำหนดบริบทของธุรกิจภายนอก โดย

(1) ระบุปัจจัยบริบทภายนอกธุรกิจที่เกี่ยวข้อง ซึ่งปัจจัยภายนอกต่าง ๆ อาจเป็น

- กองกำลังอุตสาหกรรม (คู่แข่ง ห่วงโซ่อุปทาน ตลาดแรงงาน ฯลฯ)
- กลไกตลาด (ข้อมูลประชากรของลูกค้า ภาวะเศรษฐกิจ ฯลฯ)
- พลังทางเทคโนโลยี (การเปลี่ยนแปลงทางเทคโนโลยีและความก้าวหน้า ฯลฯ)
- พลังทางสังคม (ความต้องการของชุมชน กระแสสื่อ ฯลฯ)
- สภาพแวดล้อมการกำกับดูแล
- กองกำลังทางภูมิรัฐศาสตร์ (ท่าบังคับในปัจจุบัน ฯลฯ)

(2) ระบุเหตุผลและโอกาสในการโน้มน้าวบริบทภายนอก

2) วิเคราะห์ผู้มีส่วนได้ส่วนเสียภายนอกและความต้องการของผู้มีอิทธิพล โดย

(1) ระบุผู้มีส่วนได้ส่วนเสียภายนอกที่สำคัญและผู้มีอิทธิพลต่อความคิดเห็น รวมถึงวิเคราะห์และจัดลำดับความสำคัญของความต้องการและข้อกำหนดของพวกเขา โดยผู้มีส่วนได้ส่วนเสียภายนอกหรือผู้มีอิทธิพล ได้แก่ ผู้ถือหุ้น หน่วยงานจัดอันดับ เจ้าหนี้และผู้จัดการการจัดจำหน่ายอื่น ๆ ลูกค้า ซัปพลายเออร์/พันธมิตร ชุมชน สื่อ และรัฐบาล

(2) วิเคราะห์ความต้องการและการรับรู้ของผู้มีส่วนได้ส่วนเสียภายนอกและผู้มีอิทธิพลสำหรับข้อกำหนดที่ชัดเจนหรือที่ได้รับ

(3) ระบุโอกาสที่องค์กรสามารถส่งผลกระทบต่อการรับรู้และข้อกำหนดของผู้มีส่วนได้ส่วนเสียและผู้มีอิทธิพล

1.2 บริบททางธุรกิจภายใน เกี่ยวข้องกับการทำความเข้าใจคนที่มีอยู่ กระบวนการ เทคโนโลยี โครงสร้างองค์กร ผู้มีส่วนได้ส่วนเสีย และสินทรัพย์หลักที่ขับเคลื่อนมูลค่าองค์กร

1) กำหนดบริบทภายใน ซึ่งเป็นการระบุโครงสร้างหลักและสินทรัพย์ที่กำหนดบริบทภายใน โดย

(1) ระบุโครงสร้างองค์กร: หน่วยธุรกิจหลัก หน่วยงานสำคัญ ครอบครัวงานหลักและบทบาท และทีมงานชั่วคราวและข้ามสายงาน

(2) ระบุสินทรัพย์ทุนมนุษย์ที่สำคัญ: ครอบครัวงาน ตำแหน่ง บทบาท และการมอบหมายชั่วคราวที่มีอำนาจเหนือกระบวนการที่สำคัญ ข้อมูลและทรัพย์สิน พนักงานสัญญาจ้างและตัวแทนอื่น ๆ ที่กระทำการในนามของกิจการ และบุคลากรสำคัญ รวมทั้งผู้บริหารระดับสูงและพนักงานสำคัญอื่น ๆ

(3) ระบุทรัพย์สินทางเทคโนโลยีที่สำคัญ: โครงสร้างพื้นฐานเครือข่าย คอมพิวเตอร์ฮาร์ดแวร์/ซอฟต์แวร์อุปกรณ์วิจัยและอุปกรณ์ปฏิบัติการอื่น ๆ

(4) ระบุสินทรัพย์ข้อมูลที่สำคัญ: ข้อมูลที่เป็นความลับและความลับทางการค้า ข้อมูลลูกค้าและข้อมูลพนักงาน

(5) ระบุสินทรัพย์ทางกายภาพที่สำคัญ: อาคาร สิ่งอำนวยความสะดวก และอุปกรณ์ปฏิบัติการ

(6) ระบุกระบวนการทางธุรกิจที่สำคัญ: การเงิน การขายและการตลาด การผลิต การจัดหา การกระจายและการปฏิบัติตาม การบริการลูกค้า การวิจัยและพัฒนา และการจ้างงาน

(7) ระบุผลิตภัณฑ์และบริการที่สำคัญ

(8) ระบุความสัมพันธ์ระหว่างองค์ประกอบของโครงสร้าง คน กระบวนการ เทคโนโลยี ข้อมูล และสินทรัพย์ทางกายภาพ เพื่อทำความเข้าใจว่าทรัพยากรทำงานร่วมกันอย่างไรเพื่อบรรลุวัตถุประสงค์

2) กำหนดการเปลี่ยนแปลงที่จำเป็นในการจัดแนวบริบทภายในและระบบ GRC ระบุการเปลี่ยนแปลงที่เป็นไปได้ในบริบทภายในที่อาจส่งผลต่อด้านการออกแบบระบบ GRC หรือรับรองความสอดคล้อง โดย

(1) กำหนดแง่มุมของบริบทภายในที่ควรเปลี่ยนแปลงเพื่อให้ระบบ GRC สามารถรองรับวัตถุประสงค์ขององค์กรได้

(2) กำหนดว่าการออกแบบระบบ GRC จะสอดคล้องกับโครงสร้างของบริบทภายในอย่างไร

(3) ระบุตัวกระตุ้นสำหรับการพิจารณาการเปลี่ยนแปลงในระบบ GRC เพื่อตอบสนองต่อการเปลี่ยนแปลงในบริบทภายใน

2. วัฒนธรรม (culture) ทำความเข้าใจกับวัฒนธรรมองค์กรที่มีอยู่ รวมถึงบรรยากาศขององค์กรและแนวความคิดส่วนบุคคลเกี่ยวกับความซื่อสัตย์ การปฏิบัติตามข้อกำหนด ความเสี่ยง และแนวทางการจัดการ โดยมีแนวทางในการทำความเข้าใจเกี่ยวกับวัฒนธรรมองค์กรดังต่อไปนี้

2.1 วิเคราะห์วัฒนธรรมเชิงจริยธรรม คือ การวิเคราะห์องค์ประกอบที่สังเกตได้และเป็นทางการในองค์กร รวมถึงทัศนคติส่วนบุคคลเกี่ยวกับระดับที่พนักงานเชื่อว่าองค์กรคาดหวังและสนับสนุนพฤติกรรมที่รับผิดชอบและความซื่อสัตย์ โดย

1) รวบรวมกลุ่มตัวอย่างที่เพียงพอของพนักงานเป็นระยะ ๆ เพื่อประเมินบรรยากาศทางจริยธรรม รวมถึงคำถามเกี่ยวกับ

(1) การรับรู้เกี่ยวกับค่านิยม/หลักการที่ระบุไว้ และการสนับสนุนขององค์กร

(2) ความชัดเจนของขั้นตอนที่สามารถหยิบยก อภิปราย และรายงานปัญหาที่อาจเกิดขึ้นได้โดยไม่ต้องกลัวว่าจะถูกตอบโต้

(3) วิธีที่ผู้นำและหัวหน้างานแสดงให้เห็นถึงความแข็งแกร่งทางจริยธรรมและความเฉียบแหลมทางธุรกิจ

(4) การประพฤติผิดสังเกตโดยพนักงาน

(5) ประเภทของการกระทำผิดที่สังเกตได้

(6) กดดันให้มีส่วนร่วมในการประพฤติผิดจรรยาบรรณหรือรับรู้ผลตอบแทนจากการประพฤติผิดจรรยาบรรณ

(7) ความเต็มใจของพนักงานในการรายงานการประพฤติมิชอบ

(8) พอใจกับการตอบสนองขององค์กรต่อรายงานการประพฤติมิชอบ

(9) เมื่อใดและอย่างไรที่ผู้นำและหัวหน้างานหารือเกี่ยวกับพฤติกรรมที่คาดหวังและความซื่อสัตย์

2) ระบุวิธีที่องค์กรอภิปรายสิ่งต่อไปนี้ผ่านช่องทางการสื่อสารที่หลากหลายคือ

(1) ความสำคัญของคุณธรรม ค่านิยม และหลักการในการตัดสินใจ

(2) ความสำคัญของการถามคำถามและตั้งประเด็นเมื่อมีข้อกังวล

(3) วิธีการรายงานเหตุการณ์และถามคำถาม

(4) การรับประกันว่าเหตุการณ์จะได้รับการตอบสนองทันท่วงที

(5) การรับประกันว่าการรายงานเหตุการณ์จะไม่ส่งผลให้เกิดการตอบโต้ใด ๆ

(6) ความมุ่งมั่นต่อตัวเลือกการรายงานที่ไม่เปิดเผยตัว

(7) แนวทางในการตัดสินใจอย่างมีจริยธรรม

3) กำหนดวัตถุประสงค์ มาตรการ เป้าหมาย และความคิดริเริ่มที่มีจริยธรรมเพื่อรวมไว้ในแผนกลยุทธ์ของระบบ GRC

2.2 วิเคราะห์ภาวะผู้นำอย่างมีจริยธรรม คือ การวิเคราะห์ว่าผู้นำกำหนด **“การปฏิบัติให้เห็นเป็นแบบอย่างโดยผู้นำองค์กร”** ที่เหมาะสมและจำลองพฤติกรรมทั้งในคำพูดและการกระทำหรือไม่ โดย

1) รวบรวมกลุ่มตัวอย่างเป็นระยะ ๆ เพื่อทำความเข้าใจการรับรู้ว่าผู้นำได้ปฏิบัติดังนี้

(1) สื่อสารจรรยาบรรณและความซื่อสัตย์เป็นสำคัญ

(2) ต้นแบบจริยธรรม

(3) ตรวจสอบให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียภายในได้รับการฝึกอบรมอย่างเหมาะสมเกี่ยวกับจริยธรรมและจัดลำดับความสำคัญ

(4) เชื่อมโยงจริยธรรมกับตัวชี้วัดประสิทธิภาพองค์กร

(5) ตัดสินใจอย่างมีจริยธรรม

(6) พูดคุยเกี่ยวกับจริยธรรมหรือความซื่อสัตย์ที่เกี่ยวข้องกับวัตถุประสงค์ ความคิดริเริ่ม และความสำเร็จขององค์กร

2) ตรวจสอบว่ามีการพิจารณาจรรยาบรรณและความซื่อตรงในการประเมิน ส่งเสริม และคัดเลือกผู้นำหรือไม่

3) ตรวจสอบว่าผู้นำที่มีศักยภาพและได้รับการเลื่อนตำแหน่งใหม่ได้รับการฝึกอบรมเกี่ยวกับ

(1) การตัดสินใจอย่างมีจริยธรรม

(2) จริยธรรมเชื่อมโยงกับวัตถุประสงค์ขององค์กรอย่างไร

(3) วิธีสื่อสารผลกระทบของจริยธรรมต่อผลการปฏิบัติงานขององค์กร

4) เปรียบเทียบวัตถุประสงค์ มาตรการ เป้าหมาย และการริเริ่มของผู้นำที่มีจริยธรรมกับผลลัพธ์ที่บรรลุ

2.3 วิเคราะห์วัฒนธรรมความเสี่ยง คือ วิเคราะห์สภาพที่มีอยู่และความคิดของแต่ละบุคคลเกี่ยวกับวิธีที่พนักงานรับรู้ความเสี่ยง ผลกระทบต่องานของพวกเขาและองค์กรโดยรวม โดย

1) ขอตัวอย่างข้อมูลที่เพียงพอเป็นระยะเพื่อประเมินวัฒนธรรมความเสี่ยง

2) กำหนดสถานะที่ต้องการของตัวชี้วัด climate/การรับรู้ความเสี่ยง

3) กำหนดวัตถุประสงค์ มาตรการ เป้าหมาย และความคิดริเริ่มด้านบรรยากาศความเสี่ยงเพื่อรวมไว้ในแผนกลยุทธ์ระบบ GRC

2.4 วิเคราะห์การมีส่วนร่วมของคณะกรรมการ คือ วิเคราะห์ระดับที่คณะกรรมการมีส่วนร่วมในองค์กร โดย

1) ถามคณะกรรมการเกี่ยวกับความสบายใจที่จะหยิบยกประเด็นขึ้นมาหรือไม่ รู้สึกสบายใจกับการจัดการที่ท้าทายหรือไม่ ข้อเสนอแนะของคุณได้รับการพิจารณาอย่างรอบคอบหรือไม่ คุณมีส่วนร่วมแค่ไหนในการกำหนดกลยุทธ์และ/หรือการตรวจสอบคณะกรรมการมีผลหรือไม่

2) ถามผู้บริหารว่าคณะกรรมการมีผลหรือไม่ สมาชิกคณะกรรมการมีส่วนร่วมหรือไม่ มีผลกระทบต่อธุรกิจหรือไม่

3) วิเคราะห์การมีส่วนร่วมของคณะกรรมการ โดยจำแนกว่าคณะกรรมการเป็นแบบเชิงรุกหรือเชิงรับ (active or passive) จำนวนการประชุมต่อปี ความถี่ของการประชุมที่ไม่มีผู้เข้าร่วม ขอบเขตของทรัพยากรอิสระที่จัดหาให้โดยสมาชิกคณะกรรมการ ระดับของ cross board การมีส่วนร่วมระหว่างสมาชิกในคณะกรรมการ

2.5 วิเคราะห์วัฒนธรรมการกำกับดูแลและรูปแบบการจัดการ คือ วิเคราะห์แนวทางที่มีอยู่เพื่อควบคุม จัดการ และเปิดใช้งานแรงงาน โดย

1) ระบุตำแหน่งที่ได้รับมอบหมายอำนาจการตัดสินใจของฝ่ายบริหาร

2) กำหนดวิธีการกำหนดและบังคับใช้ความรับผิดชอบและความรับผิดชอบ

3) ทำความเข้าใจว่าคณะกรรมการมีส่วนในการบริหารองค์กรอย่างไร

4) ทำความเข้าใจระดับความเป็นทางการหรือไม่เป็นทางการของฝ่ายบริหารที่เกี่ยวข้อง

5) เข้าใจปรัชญาเกี่ยวกับการตัดสินใจแบบรวมศูนย์หรือแบบกระจายอำนาจ

6) เข้าใจปรัชญาเกี่ยวกับการวัดผลองค์กร กลุ่ม และรายบุคคล

2.6 วิเคราะห์การมีส่วนร่วมของพนักงาน คือ วิเคราะห์วัฒนธรรมพนักงานที่มีอยู่ รวมถึงระดับความพึงพอใจ ความภักดี และการมีส่วนร่วมของพนักงาน โดย

1) ประเมินมุมมองของพนักงานเกี่ยวกับการจัดตำแหน่งค่านิยมส่วนบุคคลกับภารกิจและค่านิยมขององค์กร

2) ถามตัวอย่างพนักงานเกี่ยวกับความพึงพอใจกับค่าตอบแทนความรับผิดชอบ โอกาสในการทำงาน เพื่อนร่วมงาน ผู้บังคับบัญชา ผู้บริหารระดับสูงและพนักงาน

3) ถามตัวอย่างพนักงานเกี่ยวกับระดับความมุ่งมั่นต่อองค์กร การว่าจ้าง ความภักดี และยินดีแนะนำนายจ้างให้กับเพื่อน

4) ถามกลุ่มตัวอย่างเกี่ยวกับการรับรู้ของพวกเขาเกี่ยวกับความมุ่งมั่นของผู้บริหารต่อความสามารถ นโยบาย/แนวทางการว่าจ้าง นโยบาย/การปฏิบัติการฝึกอบรม นโยบาย/แนวทางปฏิบัติในการวัดผลนโยบาย/แนวทางปฏิบัติในการประเมินผลการปฏิบัติงาน นโยบาย/แนวทางปฏิบัติในการส่งเสริมการขาย ให้คำปรึกษา/แนะนำเส้นทางอาชีพ นโยบาย/แนวทางการชดเชย และนโยบาย/แนวทางการให้รางวัล/วินัย

5) ถามผู้บริหารเป็นระยะเกี่ยวกับความมุ่งมั่นต่อพนักงาน รวมถึงมุมมองเกี่ยวกับความมุ่งมั่นในความสามารถ นโยบาย/แนวทางการว่าจ้าง นโยบาย/การปฏิบัติการฝึกอบรม นโยบาย/แนวทางปฏิบัติในการประเมินผลการปฏิบัติงาน นโยบาย/แนวทางปฏิบัติในการส่งเสริมการขาย ให้คำปรึกษา/แนะนำเส้นทางอาชีพ นโยบาย/แนวทางการชดเชย นโยบาย/แนวทางการให้รางวัล/วินัย บทบาท/งานและเส้นทางอาชีพและการเลิกจ้าง/การเกษียณอายุ

3. ค่านิยมและวัตถุประสงค์ขององค์กร (values & objectives) เกี่ยวข้องกับการกำหนดสิ่งที่องค์กรต้องการบรรลุและค่านิยมที่องค์กรต้องการ

3.1 กำหนดภารกิจและวิสัยทัศน์ คือ การสร้างแถลงการณ์อย่างเป็นทางการเกี่ยวกับภารกิจและวิสัยทัศน์ขององค์กร โดยกำหนดภารกิจ สิ่งที่องค์กรจะทำ กำหนดวิสัยทัศน์ว่าองค์กรจะเป็นอย่างไร

3.2 กำหนดมูลค่า คือ การสร้างแถลงการณ์อย่างเป็นทางการเกี่ยวกับค่านิยมหลักที่องค์กรถือครองและนำไปใช้กับการตัดสินใจทางธุรกิจ โดย

1) ให้คณะกรรมการหรือคณะอนุกรรมการที่ได้รับมอบหมายและผู้มีส่วนได้ส่วนเสียภายในที่เหมาะสมมีส่วนร่วมในกระบวนการพัฒนาค่านิยม

2) จัดทำเอกสารแสดงค่านิยมแยกกันหรือเป็นส่วนหนึ่งของเอกสารอื่น เช่น กฎบัตรหรือจรรยาบรรณ

3) จัดทำคำแถลงค่านิยมให้กับผู้มีส่วนได้ส่วนเสียภายใน

4) จัดทำคำแถลงค่านิยมแก่ผู้มีส่วนได้ส่วนเสียภายนอก

5) ทบทวนคำแถลงค่านิยมเป็นระยะเพื่อพิจารณาการแก้ไขตามการเปลี่ยนแปลงทางธุรกิจภายในและภายนอก การจัดการ บริบททางกฎหมายหรือวัฒนธรรม

6) กำหนดขั้นตอนและสิ่งกระตุ้นเพื่อทบทวนมูลค่าขององค์กร

3.3 กำหนดวัตถุประสงค์ทางธุรกิจ คือ การกำหนดชุดวัตถุประสงค์ทางธุรกิจที่วัดผลได้สมดุลซึ่งสอดคล้องกับพันธกิจ วิสัยทัศน์ และค่านิยมขององค์กร โดย

1) กำหนดวัตถุประสงค์ทางธุรกิจระดับสูงให้สอดคล้องกับค่านิยมและความเสี่ยง ได้แก่

(1) วัตถุประสงค์เชิงกลยุทธ์

(2) วัตถุประสงค์ทางการเงิน

(3) วัตถุประสงค์ของลูกค้า

(4) วัตถุประสงค์ของกระบวนการปฏิบัติงาน

(5) วัตถุประสงค์การเรียนรู้และการเติบโต

(6) วัตถุประสงค์ในการปฏิบัติตามข้อกำหนด

(7) วัตถุประสงค์การรายงาน

2) ลำดับวัตถุประสงค์ทางธุรกิจระดับสูงสู่ระดับล่างในองค์กร รวมถึงหน่วยธุรกิจ แผนก ทีม และบุคคล

3) กำหนดความรับผิดชอบเพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจในแต่ละระดับ

3.4 กำหนดตัวบ่งชี้ เป้าหมาย และความคลาดเคลื่อน คือ การกำหนดชุดตัวบ่งชี้นำ (leading indicator) และตัวบ่งชี้ตาม (lagging indicator) ที่สมดุลที่ช่วยให้ฝ่ายบริหารเข้าใจว่า องค์กรบรรลุเป้าหมายตามวัตถุประสงค์ทางธุรกิจภายในเกณฑ์ความคลาดเคลื่อนที่กำหนดหรือไม่ โดย

1) ใช้ตัวชี้วัด (นำและตาม) เพื่อช่วยกำหนดว่าเกิดอะไรขึ้นหรือคาดการณ์ว่าจะเกิดอะไรขึ้น

2) กำหนดเป้าหมายที่แสดงค่าตัวบ่งชี้ที่ต้องการภายในระยะเวลาที่กำหนด

3) กำหนดความคลาดเคลื่อนที่แสดงถึงขีดจำกัดบนและขีดจำกัดล่างที่ยอมรับได้ของค่าตัวบ่งชี้

3.5 ได้รับความมุ่งมั่นในภารกิจ วิสัยทัศน์ ค่านิยม และวัตถุประสงค์ คือ การรับความมุ่งมั่นจากผู้บริหารและสมาชิกคณะกรรมการเกี่ยวกับสิ่งที่องค์กรจะบรรลุในขณะที่ดำเนินชีวิตตามค่านิยม โดย

1) ได้รับความมุ่งมั่นของผู้บริหารระดับสูงและสมาชิกคณะกรรมการต่อภารกิจ วิสัยทัศน์ ค่านิยม

2) ได้รับความมุ่งมั่นของผู้บริหารระดับสูงและสมาชิกคณะกรรมการเพื่อวัตถุประสงค์

3.6 ภารกิจด้านการสื่อสาร วิสัยทัศน์ และค่านิยม คือ การสื่อสารพันธกิจ วิสัยทัศน์ และค่านิยมแก่ผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก โดย

1) พัฒนาแม่แบบสำหรับการสื่อสารพันธกิจ วิสัยทัศน์ และค่านิยมขององค์กร เพื่อให้มีความสอดคล้องกันในแต่ละการสื่อสารที่เป็นทางการ

2) สื่อสารพันธกิจ วิสัยทัศน์ และค่านิยมขององค์กรแก่ผู้บริหารและพนักงานอย่างไม่เป็นทางการและบ่อยครั้ง ในการประชุมและการนำเสนอโดยผู้นำ

3) สื่อสารพันธกิจ วิสัยทัศน์ และค่านิยมแก่ผู้มีส่วนได้ส่วนเสียภายในและภายนอกอย่างเป็นทางการดังนี้

(1) จรรยาบรรณ

(2) เว็บไซต์ของนิติบุคคล

(3) รายงานและการสื่อสารไปยังผู้ถือหุ้นและผู้มีส่วนได้ส่วนเสียอื่น ๆ

(4) การโพสต์สถานที่ทำงาน

(5) อภิปรายว่าผลลัพธ์ของแต่ละกลุ่ม แผนก หน่วยธุรกิจ หรือหน่วยงานสนับสนุนการบรรลุภารกิจ วิสัยทัศน์ ค่านิยม และวัตถุประสงค์ขององค์กรเป็นอย่างไร

องค์ประกอบที่สอง: จัดระเบียบและดูแล (organize & oversee)

จัดระเบียบและดูแลระบบ GRC เพื่อให้เกิดการบูรณาการและเมื่อมีการปรับเปลี่ยนรูปแบบการดำเนินงานที่มีอยู่ของธุรกิจและกำหนดให้กับความรับผิดชอบเฉพาะของผู้บริหาร อำนาจในการตัดสินใจ และความรับผิดชอบเพื่อให้บรรลุเป้าหมายของระบบ

1. ผลลัพธ์และความมุ่งมั่น (outcomes & commitment) เกี่ยวข้องกับการกำหนดเป้าหมายของระบบ GRC และรับความมุ่งมั่นของคณะกรรมการและผู้บริหาร

1.1 กำหนดขอบเขตของระบบ GRC หรือระบบย่อยที่อยู่ระหว่างการพิจารณา โดย

1) กำหนดว่าจะกำหนดและนำระบบ GRC ไปใช้ทั่วทั้งองค์กรหรือไม่ หรือจะระบุเป็นขั้นตอนโดยกล่าวถึงส่วนต่าง ๆ เช่น

(1) พื้นที่ความเสี่ยงในวงกว้าง (โปรแกรมการปฏิบัติตามกฎระเบียบ โปรแกรมความเสี่ยงทางการเงิน ฯลฯ) หรือ

(2) พื้นที่เสี่ยงในวงแคบ (การควบคุมภายในเกี่ยวกับการรายงานทางการเงิน การปฏิบัติตามการจ้างงาน การจัดการความเสี่ยงจากการทุจริต)

2) หากใช้แนวทางแบบ staged approach ให้จัดลำดับความสำคัญและประสานงานโครงการพัฒนาเพื่อให้แน่ใจว่าสามารถบูรณาการได้

1.2 กำหนดรูปแบบและเป้าหมายของระบบ GRC กำหนดรูปแบบโดยรวมของระบบ GRC รวมถึงสิ่งที่จะทำให้สำเร็จและความเกี่ยวข้องกับวัตถุประสงค์ทางธุรกิจ

1) กำหนดภารกิจและวิสัยทัศน์ของระบบ GRC เป็นจุดเริ่มต้นสำหรับแผนยุทธศาสตร์ GRC

2) กำหนดแนวทางทั่วไปของระบบ GRC ไม่ว่าจะเป็นแนวทางการบังคับหรือส่งเสริม ปรัชญา สั่งการหรือการทำงานร่วมกัน

3) กำหนดเป้าหมาย ตัวชี้วัด เกณฑ์ และความคลาดเคลื่อนของระบบ GRC ที่วัดได้สำหรับการรวมไว้ในแผนกลยุทธ์ GRC ที่สนับสนุนวัตถุประสงค์สากล กำหนดความรับผิดชอบสำหรับแต่ละเป้าหมายของระบบ GRC รวมถึงการมอบหมายเอกสารอำนาจตามความเหมาะสม

4) อธิบายว่าเป้าหมายของระบบ GRC สนับสนุนวัตถุประสงค์ทางธุรกิจอย่างไร

1.3 รับความมุ่งมั่นต่อระบบ GRC เกี่ยวกับการขอรับการอนุญาตเป็นลายลักษณ์อักษรอย่างชัดเจนและการสนับสนุนระดับสูงสำหรับระบบ GRC โดย

1) รับคำมั่นสัญญาและมอบอำนาจจากคณะกรรมการ

2) รับคำมั่นสัญญาจากผู้บริหารระดับสูงเพื่อสนับสนุนระบบ GRC

2. บทบาทและความรับผิดชอบ (roles and responsibilities) คือ การกำหนดและเปิดใช้งานผ่านอำนาจการตัดสินใจและทรัพยากร โดยแต่ละบทบาทมีหน้าที่รับผิดชอบในแง่มุมที่สำคัญของระบบ GRC

2.1 กำหนดและเปิดใช้งานการกำกับดูแลบทบาทและความรับผิดชอบของระบบ GRC

1) กำหนดบทบาทการกำกับดูแล responsibilities และ accountabilities สำหรับแต่ละแง่มุมของระบบ GRC โดยกำหนดคุณลักษณะที่สำคัญของโครงสร้างการกำกับดูแล (เช่น คณะกรรมการ) และบุคลากร (เช่น สมาชิกในคณะกรรมการ) รวมถึงความเป็นอิสระจากผู้บริหาร ความเป็นกลางในการวิเคราะห์ ความซื่อสัตย์สุจริตและจรรยาบรรณ ความขยันหมั่นเพียร มีความสามารถเพียงพอในการดำเนินกิจกรรมที่ได้รับมอบหมาย รวมทั้งหนังสือรับรองวิชาชีพที่เป็นที่ยอมรับโดยทั่วไปซึ่งสอดคล้องกับบทบาท ความโปร่งใสของการปฏิบัติและกิจกรรม และเพิ่มสมาชิกโครงสร้างการกำกับดูแลใหม่เป็นระยะ

2) กำหนดความรับผิดชอบในการกำกับดูแลทั่วไปสำหรับ

(1) กำกับและอนุมัติวัตถุประสงค์และผลลัพธ์ของระบบ GRC ที่คาดหวัง

(2) การกำหนดกฎบัตรสำหรับคณะกรรมการ (และโครงสร้างการกำกับดูแลอื่น ๆ) การมีส่วนร่วมในระบบ

(3) มีความรู้เกี่ยวกับการออกแบบและการทำงานของระบบ

(4) ได้รับการประกันอย่างสม่ำเสมอว่าระบบมีประสิทธิภาพ

(5) ให้การรับรองตามสมควรว่าคำรับรองของฝ่ายบริหารเกี่ยวกับองค์กรและระบบนั้นถูกต้องโดยใช้ข้อมูลที่พัฒนาขึ้นโดยอิสระจากฝ่ายจัดการ

3) กำหนดความรับผิดชอบในด้านการดำเนินงานของระบบ GRC ที่ต้องการมุมมองและความเป็นอิสระของคณะกรรมการ

4) กำหนดความรับผิดชอบ GRC ของสมาชิกคณะกรรมการและคณะกรรมการชุดย่อย

5) กำหนดลักษณะงานและเกณฑ์การประเมินผลการปฏิบัติงานสำหรับบุคลากรที่กำกับดูแล

6) ตรวจสอบภูมิหลังของบุคลากรที่ได้รับการว่าจ้างหรือเลื่อนขั้นเป็นบทบาทการกำกับดูแล

7) กำหนดและจัดทำแผนหลักสูตรเฉพาะทางสำหรับบุคลากรกำกับดูแล ซึ่งรวมถึงส่วนที่เกี่ยวข้องของหลักสูตรพื้นฐาน OCEG GRC

8) ตรวจสอบให้แน่ใจว่าบุคลากรที่กำกับดูแลได้รับและรักษาข้อมูลประจำตัวทางวิชาชีพที่เกี่ยวข้องกับบทบาท GRC ของพวกเขา

2.2 กำหนดและเปิดใช้งานบทบาทการจัดการและความรับผิดชอบ เกี่ยวข้องกับการกำหนดบทบาทการจัดการ responsibilities และ accountabilities ของระบบ GRC

1) กำหนดความรับผิดชอบในด้านการดำเนินงานของระบบ GRC ที่ต้องการมุมมองและความเป็นอิสระของคณะกรรมการ รวมถึง

(1) ตรวจสอบและชี้นำวัตถุประสงค์ทางธุรกิจให้สอดคล้องกับผลลัพธ์ของระบบที่ต้องการ

(2) ประเมินหรือตรวจสอบการประเมินและติดตามความเสี่ยงที่มีลำดับความสำคัญสูงสุดอย่างอิสระ

(3) เฝ้าติดตามกิจกรรมการควบคุมใด ๆ ที่ดำเนินการโดยผู้บริหารระดับสูง

(4) ติดตามตรวจสอบกิจกรรมการควบคุมของผู้บริหารระดับสูง

(5) การสละข้อกำหนดของระบบในสถานการณ์ที่กำหนด

(6) คัดเลือก ประเมิน ชดเชย และเลิกจ้างผู้บริหารระดับสูง

(7) การจัดการกับปัญหาระยะยาวที่อาจเกินวาระการดำรงตำแหน่งของผู้บริหารระดับสูง

2) กำหนดความรับผิดชอบ GRC เฉพาะสำหรับบทบาทการจัดการ รวมถึง

(1) ประธานเจ้าหน้าที่บริหารมีหน้าที่สนับสนุนหรือเป็นผู้นำในการดำเนินการตามระบบ GRC

(2) ประธานเจ้าหน้าที่ฝ่ายการเงินมีหน้าที่รับผิดชอบในการอนุมัติและดูแลการจัดสรรทรัพยากรและงบประมาณ และมีส่วนร่วมในกระบวนการประเมินความเสี่ยง

(3) หัวหน้าเจ้าหน้าที่ความเสี่ยงมีหน้าที่รับผิดชอบในการพัฒนากรอบการเพิ่มประสิทธิภาพความเสี่ยงและรวบรวมและวิเคราะห์ความเสี่ยงในระดับองค์กร

(4) ประธานเจ้าหน้าที่ฝ่ายปฏิบัติตามข้อกำหนดมีหน้าที่เป็นผู้นำในกระบวนการประเมินความเสี่ยงด้านการปฏิบัติตามข้อกำหนด ดูแลการออกแบบและการนำโปรแกรมการปฏิบัติตามข้อกำหนดไปใช้เพื่อป้องกัน ตรวจจับ และแก้ไขการไม่ปฏิบัติตามกฎหมาย

(5) หัวหน้าเจ้าหน้าที่ฝ่ายจริยธรรมมีหน้าที่ในการประเมินและส่งเสริมวัฒนธรรมจริยธรรมผ่านการฝึกอบรม การสื่อสาร และการควบคุมอื่น ๆ (ซึ่งมักจะรวมกับหัวหน้าเจ้าหน้าที่การปฏิบัติตามกฎระเบียบ)

(6) ประธานเจ้าหน้าที่ฝ่ายกฎหมายมีหน้าที่เป็นผู้นำในกระบวนการประเมินความเสี่ยงทางกฎหมาย อนุมัตินโยบายและการควบคุมเพื่อให้มั่นใจว่าปฏิบัติตามข้อกำหนดทางกฎหมาย

(7) หัวหน้าเจ้าหน้าที่ฝ่ายบุคคลมีหน้าที่รับผิดชอบในการดูแลและดำเนินการตามแรงจูงใจและการควบคุมทุนมนุษย์ แนวปฏิบัติในการเป็นผู้นำที่มีจริยธรรม การรวมข้อกำหนดเข้ากับรายละเอียดงานและการประเมินประสิทธิภาพ การสื่อสารของผู้มีส่วนได้ส่วนเสียภายใน และอาจรวมถึงโครงการริเริ่มด้านการศึกษาและการเรียนรู้ทั้งหมด

(8) ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยีมีหน้าที่ประสานงานการเลือกและการประยุกต์ใช้เทคโนโลยีเพื่อสนับสนุนการทำงานของ GRC

3) กำหนดรายละเอียดงานและเกณฑ์การประเมินประสิทธิภาพที่เกี่ยวข้องกับ GRC สำหรับผู้บริหารในบทบาทของ GRC

4) ตรวจสอบภูมิหลังของผู้บริหารที่ได้รับการว่าจ้างหรือเลื่อนขั้นเป็นหน่วยงานที่สำคัญหรือบทบาท GRC

5) กำหนดและจัดทำแผนหลักสูตรเฉพาะทางสำหรับการจัดการในบทบาท GRC ซึ่งรวมถึงส่วนที่เกี่ยวข้องของหลักสูตร OCEG GRC Fundamentals

6) ตรวจสอบให้แน่ใจว่าฝ่ายบริหารได้รับและรักษาข้อมูลรับรองทางวิชาชีพที่เกี่ยวข้องกับความรับผิดชอบ GRC ของตน

2.3 กำหนดและเปิดใช้งานบทบาทความเป็นผู้นำและความรับผิดชอบ คือการกำหนดบุคคลเพื่อทำหน้าที่เป็นผู้นำเพื่อสนับสนุนระบบ GRC และกำหนดวิธีการเพื่อให้แน่ใจว่าพวกเขามีจริยธรรมตามบทบาทที่ต้องการ โดย

1) ระบุและเลือกบุคคลในระดับต่าง ๆ ขององค์กรเพื่อทำหน้าที่เป็นผู้นำและผู้สนับสนุนระบบ GRC

2) กำหนดความรับผิดชอบของผู้นำและผู้สนับสนุนเพื่อทลายอุปสรรคในการเปลี่ยนแปลง พัฒนา buy-in สำหรับระบบ GRC สื่อสารผลลัพธ์ที่ต้องการของระบบและวิธีการที่เกี่ยวข้องกับวัตถุประสงค์ทางธุรกิจ

3) กำหนดและสื่อสารชุดจริยธรรมของบทบาทที่จำเป็นซึ่งผู้บริหารระดับสูงได้ให้คำมั่นสัญญาและความต้องการของผู้นำที่ได้รับมอบหมาย

4) ตรวจสอบภูมิหลังของผู้นำและผู้สนับสนุนเพื่อหาความไม่ลงรอยกันกับการเป็นผู้นำที่มีจริยธรรม (เช่น การประพฤติผิดก่อนหน้านี้) และเพื่อให้แน่ใจว่าสอดคล้องกับจริยธรรมของบทบาทที่กำหนดไว้ซึ่งจำเป็นสำหรับผู้นำ

5) มีส่วนร่วมในการสนทนากับผู้นำอย่างสม่ำเสมอเกี่ยวกับค่านิยมที่ได้รับการคาดหวัง และกำหนดความคาดหวังเกี่ยวกับวิธีการแบ่งปัน ไล่ตาม และติดตามตลอดจนวิธีการแก้ไขเหตุการณ์ที่ล้มเหลวและการทำลายความไว้วางใจ

6) กำหนดและนำเสนอหลักสูตรเฉพาะสำหรับผู้นำ ที่รวมส่วนที่เกี่ยวข้องของหลักสูตรพื้นฐาน OCEG GRC Fundamentals

2.4 กำหนดและเปิดใช้งานบทบาทการทำงานของระบบ GRC คือ กำหนดบทบาทที่จำเป็นในการส่งมอบ ดำเนินการ และดำเนินการตามแนวทางปฏิบัติของระบบ GRC โดย

1) กำหนดบทบาทที่รับผิดชอบกิจกรรมหลักของ GRC ดังต่อไปนี้

(1) วิธีการ นโยบาย/ขั้นตอน มาตรฐาน การพัฒนาคำศัพท์และการบำรุงรักษา

(2) การระบุความเสี่ยงและความต้องการ การวิเคราะห์ และการเพิ่มประสิทธิภาพ

(3) การดำเนินการตามความคิดริเริ่ม/การจัดการพอร์ตโครงการ

(4) ความสัมพันธ์กับผู้มีส่วนได้ส่วนเสีย

(5) สายด่วน

(6) การสอบสวนและการแก้ปัญหา

(7) การวัดประสิทธิภาพ

(8) การสื่อสาร รวมทั้งการประชาสัมพันธ์

(9) การจัดการข้อมูล

(10) เทคโนโลยี

2) กำหนดรายละเอียดงานและเกณฑ์การประเมินประสิทธิภาพที่เกี่ยวข้องกับบทบาทการปฏิบัติงานของ GRC แต่ละบทบาท

3) ตรวจสอบภูมิหลังของบุคลากรที่ได้รับการว่าจ้าง โอนย้าย หรือเลื่อนขั้นเป็นบทบาทการปฏิบัติงานของ GRC

4) กำหนดและจัดทำแผนหลักสูตรเฉพาะทางสำหรับบทบาทการปฏิบัติงานของ GRC ซึ่งรวมถึงส่วนที่เกี่ยวข้องของหลักสูตรพื้นฐานของ OCEG GRC Fundamentals

5) เฝ้าติดตามว่าบุคลากรฝ่ายปฏิบัติการได้รับและรักษาข้อมูลรับรองทางวิชาชีพที่เกี่ยวข้องกับบทบาท GRC ของตนหรือไม่

2.5 กำหนดและเปิดใช้งานการประกันบทบาทและความรับผิดชอบ (หัวหน้าฝ่ายตรวจสอบ ผู้ตรวจสอบภายนอก) คือ การกำหนดบทบาทการประกัน responsibilities และ accountabilities สำหรับระบบ GRC โดย

1) กำหนดคุณลักษณะที่สำคัญของบุคลากรด้านการรับประกัน ได้แก่

(1) ความเป็นอิสระจากผู้บริหาร

(2) ความเป็นกลางในการวิเคราะห์

(3) ความซื่อสัตย์

(4) ความขยันหมั่นเพียร

(5) มีความสามารถเพียงพอในการดำเนินกิจกรรมที่ได้รับมอบหมาย รวมทั้งหนังสือรับรองวิชาชีพที่เป็นที่ยอมรับโดยทั่วไปซึ่งสอดคล้องกับบทบาท

(6) การเข้าถึงคณะกรรมการโดยตรงและเป็นอิสระสำหรับผู้บริหารระดับสูงที่รับผิดชอบด้านการประกันอิสระ

2) กำหนดความรับผิดชอบทั่วไปสำหรับบุคลากรด้านการประกัน เพื่อให้การรับรองอย่างอิสระต่อคณะกรรมการและผู้บริหาร ได้แก่

(1) ความเสี่ยงและข้อกำหนด (ภายนอกและภายใน) ได้รับการระบุ ประเมิน จัดการ รายงาน และติดตามโดยใช้วิธีการที่มีประสิทธิภาพ

(2) มีข้อมูลคุณภาพที่จำเป็นในการตัดสินใจของระบบ GRC และลดต้นทุนในการควบคุม

(3) ระบบ GRC ได้รับการออกแบบอย่างเหมาะสมเพื่อจัดการกับความเสี่ยงและข้อกำหนดที่ระบุ

(4) กระบวนการบริหารความเสี่ยงได้รับการออกแบบเพื่อระบุ ประเมิน จัดการ รายงานและติดตามชุดความเสี่ยงที่ครอบคลุม (และข้อกำหนดสำหรับ) การบรรลุวัตถุประสงค์ขององค์กรภายใน ค่านิยมขององค์กร

(5) ระบบ GRC ทำงานตามที่ออกแบบไว้

3) กำหนดลักษณะงานและเกณฑ์การประเมินผลการปฏิบัติงานสำหรับบุคลากรที่รับประกัน

4) ตรวจสอบภูมิหลังของบุคลากรที่ได้รับการว่าจ้างหรือเลื่อนขั้นเป็นบทบาทการประกัน

5) กำหนดและจัดทำแผนหลักสูตรเฉพาะสำหรับบุคลากรด้านประกัน ซึ่งรวมถึงส่วนที่เกี่ยวข้องของหลักสูตรพื้นฐาน OCEG GRC

3. แนวทางและความรับผิดชอบ (approach & accountability) คือ การกำหนดแนวทางในการฝัง ผสานรวม และจัดระบบ GRC กับธุรกิจ และสร้างความรับผิดชอบสำหรับแต่ละแง่มุมของระบบ

3.1 จัดสรรบทบาทและความรับผิดชอบของ GRC ให้กับบุคลากรและคณะกรรมการ โดย

1) จัดสรรความรับผิดชอบให้กับบุคคลและคณะกรรมการที่มีบทบาทหลักอื่น ๆ ช่วยให้บรรลุการทำงานร่วมกันและมีประสิทธิภาพ รวมถึงมีความเที่ยงธรรมและมีความเป็นอิสระ

2) แบ่งแยกบทบาทบางอย่างดังนี้

(1) แยกบทบาทในการเปิดเผยการประพฤติมิชอบและจุดอ่อน (การปฏิบัติตาม การตรวจสอบภายใน) ออกจากบทบาทในการปกป้ององค์กรตามกฎหมาย (ที่ปรึกษาทั่วไป)

(2) แยกบทบาทในการเปิดเผยการประพฤติมิชอบและจุดอ่อน (การปฏิบัติตาม การตรวจสอบภายใน) ออกจากบทบาทที่เกี่ยวกับวัตถุประสงค์และแรงจูงใจในการดำเนินธุรกิจรายไตรมาสที่อาจกระทบต่อความเที่ยงธรรม

(3) แยกบทบาทที่เกี่ยวข้องกับการดำเนินการและดำเนินการควบคุมป้องกันและสอบสวน (การเงิน การปฏิบัติตาม) ออกจากบทบาทที่ประเมินประสิทธิภาพของการควบคุมและโครงสร้างเหล่านั้น (การตรวจสอบภายใน)

(4) แยกบทบาทที่เกี่ยวข้องกับการสอบสวนการประพฤติผิดและจุดอ่อนที่ถูกกล่าวหา ออกจากบุคคลที่ถูกกล่าวหาว่าเป็นหรือมีความเป็นไปได้ที่จะมีส่วนเกี่ยวข้องกับการประพฤติผิดที่ถูกกล่าวหาและออกจากผู้ที่มีความสัมพันธ์การรายงานโดยตรงกับบุคคลดังกล่าว

3) ออกแบบการรายงานที่เพียงพอเพื่อให้แน่ใจว่ามีความเป็นอิสระและความเที่ยงธรรมที่จำเป็น

4) พัฒนาโครงสร้างองค์กรที่เสนอสำหรับระบบ GRC เพื่อให้สามารถรายงานผลตามวัตถุประสงค์ได้

5) ตรวจดูโครงสร้างที่เสนอกับบุคคลที่จะรับราชการในบทบาทสำคัญภายในระบบ GRC

6) สรุปและจัดทำเอกสารโครงสร้างระบบ GRC รวมถึงสายการรายงานในแผนกลยุทธ์ GRC

7) ได้รับการอนุมัติแผนโครงสร้างจากหน่วยงานที่เหมาะสม

3.2 กำหนดกระบวนการระบบ GRC และบูรณาการร่วมกับกระบวนการทางธุรกิจ โดย

1) กำหนดกระบวนการของระบบ GRC และประสานกับกระบวนการทางธุรกิจที่มีอยู่

2) กำหนดว่าจะดำเนินการอย่างไรและเมื่อใด

3) สร้างปฏิทินแบบรวมสำหรับกระบวนการที่สำคัญของระบบ GRC และกระบวนการทางธุรกิจที่เกี่ยวข้อง

3.3 กำหนดแนวทางการวัดและประเมินผล ประสิทธิภาพ และการตอบสนองของระบบ GRC โดย

1) ปรับแต่งผลลัพธ์ของระบบ GRC ที่ต้องการเพื่อให้แน่ใจว่าสามารถวัดหรือประเมินผลได้

2) จัดสรรความรับผิดชอบเพื่อให้บรรลุผลลัพธ์ของระบบ GRC ให้กับบุคลากรหลัก

3) ออกแบบรายงานสำหรับผู้บริหารระดับสูงและคณะกรรมการ

4) กำหนดตารางเวลาสำหรับการดำเนินการประเมินระบบ GRC อย่างต่อเนื่องและเป็นระยะ

5) กำหนดเป้าหมายและเกณฑ์สำหรับตัวบ่งชี้การวัดแต่ละรายการและเหตุการณ์สำคัญที่ครบกำหนด

3.4 กำหนดแนวทางการจัดการการเปลี่ยนแปลงองค์กร เป็นการกำหนดแนวทางในการเตรียมองค์กรให้พร้อมสำหรับการเปลี่ยนแปลงใด ๆ ที่ระบบ GRC อาจต้องการต่อบุคลากร กระบวนการ และเทคโนโลยี โดย

1) ระบุประเด็นสำคัญที่ระบบ GRC อาจส่งผลกระทบอย่างมีนัยสำคัญต่อหน่วยธุรกิจ แผนกบุคลากร ความสัมพันธ์ของผู้มีส่วนได้ส่วนเสีย กระบวนการ และเทคโนโลยี

2) ประเมินความพร้อมของพื้นที่ที่ได้รับผลกระทบหลักและองค์กรโดยรวมในการบูรณาการการเปลี่ยนแปลง

3) กำหนดแผนการจัดการการเปลี่ยนแปลงเฉพาะเพื่อจัดการกับความท้าทายและความเสี่ยงที่คาดการณ์ไว้

3.5 พัฒนา รักษา และอนุมัติกรณีทางธุรกิจ คือ การพัฒนากรณีธุรกิจสำหรับระบบ GRC และได้รับอนุญาตจากผู้บริหารระดับสูงและคณะกรรมการ โดย

1) สร้างแผนกลยุทธ์และกรณีธุรกิจ

2) รับมอบอำนาจจากผู้บริหารระดับสูงและคณะกรรมการ

3) รับเงินทุนสำหรับแนวทาง

องค์ประกอบที่สาม: ประเมินและจัดตำแหน่ง (assess & align)

เกี่ยวข้องกับการประเมินความเสี่ยงและปรับโปรไฟล์ความเสี่ยงขององค์กรให้เหมาะสมด้วยโครงการริเริ่ม ยุทธวิธี และกิจกรรมต่าง ๆ ซึ่งประกอบด้วย 3 ขั้นตอน ดังนี้

1. การระบุความเสี่ยง (risk identification) คือ การระบุเหตุการณ์ แรงขับเคลื่อน และปัจจัยที่อาจส่งผลต่อความสำเร็จของวัตถุประสงค์ทางธุรกิจ รวมถึงการไม่ปฏิบัติตามข้อกำหนดที่กำหนดโดยกฎหมาย มาตรฐาน นโยบายภายใน หรือขอบเขตบังคับหรือโดยสมัครใจอื่น ๆ การระบุความเสี่ยงสามารถกระทำได้โดย

1.1 ระบุวัตถุประสงค์และการดำเนินงานทางธุรกิจที่ได้รับผลกระทบ คือ การระบุวัตถุประสงค์ทางธุรกิจหลักและการดำเนินงานที่อาจได้รับผลกระทบจากความเสี่ยง

1.2 ระบุการเปลี่ยนแปลงทั้งปัจจัยภายในและภายนอกที่ก่อให้เกิดความเสี่ยง คือ การระบุเหตุการณ์ไม่พึงประสงค์ที่อาจเกิดขึ้นจากการเปลี่ยนแปลงปัจจัยภายในและภายนอกที่ส่งผลต่อความเสี่ยง

1.3 ระบุความเสี่ยงด้านความซื่อสัตย์และจริยธรรม คือ การระบุสถานการณ์ที่บุคคลที่ทำงานคนเดียวหรือกับผู้อื่นจะพยายามแหกกฎ ไม่ว่ากฎนั้นจะได้รับคำสั่งจากแหล่งภายนอกหรือภายในนโยบายโดยสมัครใจ

1.4 ระบุความเสี่ยงในการปฏิบัติตามข้อกำหนด คือ การระบุสถานการณ์ที่มีความเสี่ยงเกิดขึ้นเนื่องจากการไม่ปฏิบัติตามข้อกำหนดที่ได้รับคำสั่งจากภายนอกหรือภาระผูกพันขององค์กรภายใต้สัญญา ข้อตกลงโดยสมัครใจ และนโยบายภายใน

1.5 ระบุความเสี่ยงในการปฏิบัติงาน คือ การระบุสถานการณ์ที่ความเสี่ยงเป็นผลมาจากกระบวนการภายใน บุคลากร และเทคโนโลยีที่ไม่เพียงพอหรือล้มเหลว

1.6 ระบุความเสี่ยงทางเศรษฐกิจ คือ การระบุสถานการณ์ที่อาจเกิดความเสี่ยงทางการเงิน

1.7 ระบุความเสี่ยงที่อาจก่อให้เกิดโอกาสที่จะเกิดความเสี่ยง คือ ระบุพื้นที่ที่การจัดการความเสี่ยงอย่างมีประสิทธิภาพจะช่วยให้องค์กรมีโอกาสเชิงกลยุทธ์หรือยุทธวิธี

1.8 ระบุแนวโน้มความเสี่ยงและความสัมพันธ์ คือ ระบุแนวโน้มของความเสี่ยงแต่ละประเภทและความเสี่ยงที่เกี่ยวข้องมีความสัมพันธ์กันอย่างไร

1.9 จัดหมวดหมู่ความเสี่ยง คือ การระบุประเภทและลำดับความสำคัญของการประเมินผลกระทบสำหรับแต่ละความเสี่ยงที่ระบุ

1.10 มอบหมายความรับผิดชอบในการตรวจสอบการเปลี่ยนแปลงในปัจจัยพื้นฐาน คือ การกำหนดความรับผิดชอบในการติดตามเงื่อนไขและแหล่งที่มาของความเสี่ยง

2. การวิเคราะห์ความเสี่ยง (risk analysis) คือ การกำหนดโปรไฟล์ความเสี่ยงในปัจจุบัน โดยการวิเคราะห์ความเสี่ยงโดยธรรมชาติและความเสี่ยงที่เหลือหลังจากพิจารณากิจกรรมการเพิ่มประสิทธิภาพความเสี่ยงในปัจจุบัน ซึ่งสามารถกระทำได้โดย

2.1 วิเคราะห์ความเสี่ยงโดยธรรมชาติ คือ วิเคราะห์ความเปราะบางโดยธรรมชาติขององค์กรจากความน่าจะเป็นและผลกระทบของความเสี่ยง โดยไม่คำนึงถึงการควบคุมในปัจจุบัน สิ่งจูงใจ และกิจกรรมเพิ่มประสิทธิภาพความเสี่ยงอื่น ๆ

2.2 วิเคราะห์แนวทางปัจจุบันเพื่อเพิ่มประสิทธิภาพความเสี่ยง คือ ระบุแนวทางปัจจุบันเพื่อปรับความเสี่ยงให้เหมาะสมโดยบรรเทาผลกระทบด้านลบของความเสี่ยงและระบุโอกาสที่นำเสนอโดยความเสี่ยง

2.3 กำหนดความเสี่ยงที่เหลืออยู่ในปัจจุบัน คือ กำหนดระดับความเสี่ยงที่เหลืออยู่หลังจากนำแนวทางการเพิ่มประสิทธิภาพที่ใช้ในปัจจุบันไปใช้กับความเสี่ยง

2.4 จัดลำดับความสำคัญความเสี่ยง คือ ประเมินความเสี่ยงโดยธรรมชาติและความเสี่ยงที่เหลือตามเกณฑ์ความเสี่ยง รวมถึงประสิทธิผล ประสิทธิภาพ และการตอบสนองของกิจกรรมการเพิ่มประสิทธิภาพในปัจจุบัน เพื่อให้สามารถกำหนดลำดับความสำคัญได้

3. การเพิ่มประสิทธิภาพความเสี่ยง (risk optimization) คือ การประเมินและปรับใช้ตัวเลือกการเพิ่มประสิทธิภาพความเสี่ยงที่เลือก ซึ่งสามารถกระทำได้โดย

3.1 ประเมินกลยุทธ์และกิจกรรมในการเพิ่มประสิทธิภาพความเสี่ยง เมื่อความเสี่ยงที่เหลือในปัจจุบันไม่สามารถยอมรับได้ หรือเมื่อกิจกรรมการเพิ่มประสิทธิภาพในปัจจุบันสามารถปรับปรุงให้ดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผลมากขึ้น

3.2 กำหนดความเสี่ยงที่เหลือตามแผน โดยวิเคราะห์ผลกระทบที่คาดการณ์ไว้ซึ่งกิจกรรมการเพิ่มประสิทธิภาพตามแผนจะมีต่อโอกาสและผลกระทบเพื่อกำหนดความเสี่ยงที่เหลือตามแผน

3.3 กำหนดกิจกรรมการเพิ่มประสิทธิภาพ โดยระบุกิจกรรมการเพิ่มประสิทธิภาพในปัจจุบันและที่วางแผนไว้ซึ่งระบุถึงความเสี่ยงสูงโดยเนื้อแท้ และหากพวกเขาหยุดดำเนินการอย่างมีประสิทธิภาพ จะทำให้องค์กรมีความเสี่ยงในระดับที่ยอมรับไม่ได้

3.4 พัฒนาตัวบ่งชี้ความเสี่ยงที่สำคัญที่แจ้งฝ่ายบริหาร เมื่อเหตุการณ์ความเสี่ยงที่สำคัญเกิดขึ้น ใกล้เข้ามา หรืออาจเกิดขึ้น

3.5 พัฒนาแผนเพิ่มประสิทธิภาพความเสี่ยง โดยพัฒนาแผนการดำเนินงานและการจัดการเพื่อเพิ่มประสิทธิภาพกิจกรรม

องค์ประกอบที่สี่: ป้องกันและส่งเสริม (prevent & promote)

ส่งเสริมและจูงใจความประพฤติที่พึงประสงค์ และป้องกันเหตุการณ์และกิจกรรมที่ไม่พึงประสงค์ โดยใช้การควบคุมร่วมกับสิ่งจูงใจ

1. จรรยาบรรณ เกี่ยวข้องกับการใช้หลักจรรยาบรรณและแนวทางการตัดสินใจด้านจริยธรรมสำหรับคณะกรรมการ พนักงาน และองค์กร ซึ่งสามารถกระทำได้โดย

1.1 พัฒนาจรรยาบรรณ คือ การทำงานร่วมกับผู้มีส่วนได้ส่วนเสียที่เหมาะสมเพื่อพัฒนาจรรยาบรรณที่กล่าวถึงภารกิจขององค์กร วิสัยทัศน์ ค่านิยม นโยบายหลัก และการดำเนินธุรกิจที่คาดหวัง

1.2 ดำเนินการและจัดการจรรยาบรรณ คือ การแจกจ่ายและจัดการจรรยาบรรณเพื่อให้แน่ใจว่า ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งหมดได้รับหลักจรรยาบรรณ รวมถึงรับรองว่าพวกเขาจะปฏิบัติตามหลักปฏิบัติและหลักปฏิบัติที่ให้เกียรติ สังเกต และบังคับใช้ และยังคงมีความเกี่ยวข้องต่อไป

1.3 พัฒนาและดำเนินการตามแนวทางการตัดสินใจอย่างมีจริยธรรม คือ การทำงานร่วมกับผู้มีส่วนได้ส่วนเสียที่เหมาะสม เพื่อพัฒนาและนำแนวทางปฏิบัติในการเลือกแนวทางปฏิบัติที่สอดคล้องกับพันธกิจ วิสัยทัศน์ ค่านิยม นโยบายหลัก และการดำเนินธุรกิจที่คาดหวังขององค์กร เมื่อสถานการณ์ไม่ได้ครอบคลุมถึงหลักจรรยาบรรณ นโยบาย หรือขั้นตอนการปฏิบัติงานอย่างชัดเจน

2. นโยบาย เกี่ยวข้องกับการพัฒนา ดำเนินการ และจัดการนโยบายที่จัดการกับความเสี่ยงและข้อกำหนด ซึ่งสามารถกระทำได้โดย

2.1 กำหนดโครงสร้างนโยบาย โดยสร้างโครงสร้างการจัดระเบียบเพื่อระบุและสร้างนโยบายที่สนับสนุนระบบ GRC

2.2 พัฒนานโยบาย โดยพัฒนานโยบายเชิงป้องกันและสั่งการแบบผสมผสานเพื่อจัดการกับข้อกำหนด ความเสี่ยง และวัตถุประสงค์ของโปรแกรมอื่น ๆ

2.3 การดำเนินการและจัดการนโยบาย โดยดำเนินการสื่อสารและจัดการนโยบายเพื่อให้แน่ใจว่านโยบายเหล่านั้นดำเนินการและมีความเกี่ยวข้องต่อไป

3. การควบคุมเชิงป้องกัน เกี่ยวข้องกับการกำหนดกระบวนการ ทุนมนุษย์ เทคโนโลยี และกิจกรรมการควบคุมทางกายภาพ เพื่อป้องกันและ/หรือลดโอกาสและผลกระทบของเหตุการณ์ไม่พึงประสงค์และการประพฤติมิชอบ ซึ่งสามารถกระทำได้โดย

3.1 จัดตั้งการควบคุมกระบวนการป้องกัน โดยกำหนดกิจกรรมและขั้นตอนการควบคุมกระบวนการป้องกันเพื่อลดโอกาสและ/หรือผลกระทบของเหตุการณ์ไม่พึงประสงค์ การไม่ปฏิบัติตาม และการประพฤติมิชอบ

3.2 จัดตั้งการควบคุมทุนมนุษย์เชิงป้องกัน โดยสร้างการควบคุมทุนมนุษย์เชิงป้องกันเพื่อลดโอกาสและ/หรือผลกระทบของเหตุการณ์ไม่พึงประสงค์ การไม่ปฏิบัติตามและการประพฤติมิชอบ

3.3 จัดตั้งการควบคุมเทคโนโลยีเชิงป้องกัน โดยสร้างการควบคุมเทคโนโลยีป้องกันเพื่อลดโอกาสและ/หรือผลกระทบของเหตุการณ์ไม่พึงประสงค์ การไม่ปฏิบัติตาม และการประพฤติมิชอบ

3.4 สร้างการควบคุมทางกายภาพเชิงป้องกัน โดยสร้างการควบคุมทางกายภาพเชิงป้องกันเพื่อลดโอกาสและ/หรือผลกระทบของเหตุการณ์ไม่พึงประสงค์ การไม่ปฏิบัติตาม และการประพฤติมิชอบ

4. การรับรู้และการศึกษา เกี่ยวข้องกับการให้ความรู้แก่คณะกรรมการ ผู้บริหาร พนักงาน และองค์กรขยายเกี่ยวกับความประพฤติที่คาดหวัง และเพิ่มทักษะและแรงจูงใจที่จำเป็นในการช่วยให้องค์กรบรรลุผลการปฏิบัติงานตามหลักการ ซึ่งสามารถกระทำได้โดย

4.1 กำหนดความตระหนักและแผนการศึกษา โดยจัดทำแผนเพื่อแจ้งและให้ความรู้แก่คณะกรรมการ ผู้บริหาร พนักงาน และองค์กรขยายเกี่ยวกับความรับผิดชอบ GRC และการปฏิบัติที่คาดหวัง

4.2 กำหนดแผนหลักสูตร โดยพัฒนาหลักสูตรเฉพาะงานและโปรแกรมการฝึกอบรมที่เหมาะสมสำหรับคณะกรรมการ ผู้บริหารระดับสูง พนักงาน และองค์กรขยายเพื่อให้เป็นไปตามความรับผิดชอบของ GRC

4.3 พัฒนาหรือได้รับเนื้อหา โดยพัฒนาหรือรับเนื้อหาที่ไม่มีอยู่ในหลักสูตรหรือแผนการศึกษา และแก้ไขเนื้อหาใด ๆ ที่จำเป็นต้องอัปเดตในวัตถุประสงค์การเรียนรู้ปัจจุบัน

4.4 ดำเนินการศึกษา โดยดำเนินการและจัดการโปรแกรมการศึกษาเพื่อให้แน่ใจว่ากลุ่มเป้าหมายแต่ละรายบรรลุวัตถุประสงค์การเรียนรู้และสามารถถ่ายทอดความรู้และทักษะไปยังงานของพวกเขา

4.5 จัดให้มีสายด่วน โดยกำหนดวิธีการสำหรับพนักงานและผู้มีส่วนได้ส่วนเสียอื่น ๆ เพื่อขอคำแนะนำเกี่ยวกับการปฏิบัติในอนาคตและถามคำถามทั่วไปเกี่ยวกับความรับผิดชอบของ GRC รวมถึงตัวเลือกสำหรับการไม่เปิดเผยตัวตนในสถานที่ที่จำเป็นหรือได้รับอนุญาต

4.6 ให้การสนับสนุนแบบบูรณาการ โดยกำหนดวิธีให้พนักงานได้รับคำถามเกี่ยวกับข้อกำหนดของ GRC ภายในสภาพแวดล้อมการทำงานปกติ

5. แรงจูงใจจากทุนมนุษย์ เกี่ยวข้องกับการใช้สิ่งจูงใจด้านทุนมนุษย์ซึ่งให้ผลตอบแทนและจูงใจความประพฤติที่ต้องการ ซึ่งสามารถกระทำได้โดย

5.1 อุปถัมภ์ความเป็นผู้นำทางจริยธรรม โดยอุปถัมภ์และส่งเสริมความเป็นผู้นำที่กำหนด **"การปฏิบัติให้เห็นเป็นแบบอย่างโดยผู้นำองค์กร"** ที่เหมาะสม และเป็นแบบอย่างพฤติกรรมทั้งในคำพูดและการกระทำ

5.2 พัฒนาการประเมินตามแรงจูงใจและการตัดสินใจส่งเสริมการขาย โดยดำเนินการทบทวนประสิทธิภาพในทุกระดับขององค์กรที่มีเกณฑ์ที่เกี่ยวข้องกับประสิทธิภาพของระบบ GRC และใช้เกณฑ์เดียวกันนี้ในการส่งเสริมบุคคล

5.3 พัฒนาแผนค่าตอบแทนที่พิจารณาดำเนินการตามความคาดหวัง โดยออกแบบแผนค่าตอบแทนและโครงสร้างโบนัสที่สอดคล้องกับพฤติกรรมที่ต้องการและไม่ตอบแทนการกระทำที่ไม่พึงประสงค์

5.4 พัฒนาโปรแกรมรางวัล โดยจัดทำโปรแกรมรางวัลสำหรับพนักงานทุกคนและผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่ยกย่องบุคคลและหน่วยขององค์กรสำหรับการแสดงพฤติกรรมที่ต้องการ

6. ความเสี่ยงด้านการเงิน/การประกันภัย เกี่ยวข้องกับการพัฒนาหรือได้มาซึ่งเครื่องมือแบ่งปันความเสี่ยงและการจัดหาเงินทุน ซึ่งรวมถึง การประกันภัย การชดใช้เงินสำรอง จำเลย และนิติบุคคล สำหรับลดหรือขจัดผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงอย่างเหมาะสม ซึ่งสามารถกระทำได้โดย

6.1 ประเมินความต้องการและทางเลือกด้านการเงิน

6.2 ประเมินความต้องการหรือความต้องการความเสี่ยงด้านการเงินและทางเลือกที่มี

6.3 กำหนดวัตถุประสงค์ทางการเงินความเสี่ยง

6.4 กำหนดวัตถุประสงค์และข้อจำกัดในการแบ่งปันความเสี่ยงสำหรับความเสี่ยงหรือพอร์ตความเสี่ยงที่กำหนด

6.5 ออกแบบกลยุทธ์ความเสี่ยงด้านการเงิน

6.6 ออกแบบพอร์ตโฟลิโอของเครื่องมือและแนวทางการแบ่งปันความเสี่ยง

6.7 ดำเนินการตามกลยุทธ์ด้านการเงินความเสี่ยง

6.8 ดำเนินการเครื่องมือหรือโครงสร้างการแบ่งปันความเสี่ยงและซื้อประกัน

7. ความสัมพันธ์และข้อกำหนดของผู้มีส่วนได้ส่วนเสีย เกี่ยวข้องกับการโต้ตอบกับผู้มีส่วนได้ส่วนเสียเพื่อกำหนดความคาดหวัง ซึ่งส่งผลต่อความต้องการและมีอิทธิพลต่อมุมมองที่อาจมีผลกระทบต่อองค์กร ซึ่งสามารถกระทำได้โดย

7.1 ทำความเข้าใจผู้มีส่วนได้ส่วนเสีย โดยวิจัยและวิเคราะห์องค์กรและบุคคลสำคัญที่เกี่ยวข้องภายในเขตเลือกตั้งของผู้มีส่วนได้ส่วนเสียต่าง ๆ เพื่อทำความเข้าใจข้อกังวลและวิธีที่ดีที่สุดที่จะเกี่ยวข้องกับพวกเขา

7.2 พัฒนาแผนความสัมพันธ์ของผู้มีส่วนได้ส่วนเสีย โดยจัดทำแผนความสัมพันธ์กับผู้มีส่วนได้ส่วนเสีย รวมถึงแผนการสื่อสาร สำหรับแต่ละเขตเลือกตั้งของผู้มีส่วนได้ส่วนเสีย

7.3 ระบุและติดตามกิจกรรมตามข้อกำหนดของ issuing authority โดยกำหนดว่าหน่วยงานของรัฐ องค์กรมาตรฐาน และหน่วยงานอื่น ๆ ที่ออกคำสั่ง มาตรฐาน หรือคำแนะนำ มีผลกระทบอย่างมีนัยสำคัญต่อข้อกำหนด GRC ขององค์กรและติดตามกิจกรรมของพวกเขา

7.4 แสดงความคิดเห็นในรายการที่วางแผนหรือเสนอ โดยเข้าร่วมอย่างแข็งขันในการพัฒนาอาณัติ มาตรฐาน และคำแนะนำผ่านเส้นทางความคิดเห็นต่าง ๆ

7.5 เสนออาณัติ มาตรฐาน หรือแนวทาง โดยเสนอการพัฒนาอาณัติ มาตรฐาน และคำแนะนำอย่างแข็งขันแก่ issuing authority

องค์ประกอบที่ห้า: ตรวจจับและแยกแยะ (detect & discern)

คือ การตรวจจับพฤติกรรม เหตุการณ์ จุดอ่อนของระบบ GRC และความกังวลเกี่ยวกับผู้มีส่วนได้ส่วนเสียที่เกิดขึ้นจริงและที่อาจเกิดขึ้นได้ โดยใช้เครือข่ายที่กว้างขวางของการรวบรวมข้อมูลและเทคนิคการวิเคราะห์

1. สายด่วนและการแจ้งเตือน (hotline & notification) เกี่ยวข้องกับการจัดเตรียมแนวทางที่หลากหลายในการรายงานความสงสัย หรือเหตุการณ์ของการไม่ปฏิบัติตาม หรือประพฤติผิดจรรยาบรรณ หรือเพื่อระบุข้อกังวลเกี่ยวกับจุดอ่อนของระบบ GRC ซึ่งสามารถกระทำได้โดย

1.1 จับการแจ้งเตือน โดยใช้ระบบการแจ้งเตือนที่จะแจ้งเตือนองค์กรถึงเหตุการณ์หรือข้อสงสัยเกี่ยวกับการไม่ปฏิบัติตามกฎหมาย การละเมิดนโยบายของบริษัท และความกังวลเกี่ยวกับการรับรู้ถึงพฤติกรรมที่ผิดจรรยาบรรณหรือจุดอ่อนของระบบ GRC

1.2 การแจ้งเตือนตัวกรองและเส้นทาง โดยการแจ้งเตือนข่าวกรองและเส้นทางสำหรับการจัดการโดยไม่คำนึงถึงเส้นทางที่ได้รับการแจ้งเตือนที่กำหนด

1.3 ปฏิบัติตามข้อกำหนดของสายด่วนและการปกป้องข้อมูล โดยตรวจสอบให้แน่ใจว่าเส้นทางสายด่วนสำหรับการแจ้งเตือนเป็นไปตามข้อกำหนดเฉพาะที่กำหนดไว้ในท้องที่ที่ประกาศนั้นเกิดขึ้นและที่องค์กรดำเนินการอยู่

2. สอบถามและสำรวจ (inquiry & survey) คือ การหาข้อมูลเป็นระยะเพื่อทำความเข้าใจการรับรู้ถึงความเสี่ยง ความคืบหน้าไปสู่วัตถุประสงค์และการเกิดเหตุการณ์และกิจกรรมที่ไม่พึงประสงค์ ซึ่งสามารถกระทำได้โดย

2.1 กำหนดเส้นทางหลายทางเพื่อให้ได้มุมมองพนักงานและผู้มีส่วนได้ส่วนเสีย โดยกำหนดโอกาสในการได้รับมุมมองของพนักงานและผู้มีส่วนได้ส่วนเสียเกี่ยวกับความเสี่ยง ระบบ GRC ความประพฤติ และความมุ่งมั่นขององค์กรต่อค่านิยมที่ระบุไว้

2.2 กำหนดแนวทางแบบบูรณาการทั่วทั้งองค์กรเพื่อทำแบบสำรวจ โดยกำหนดแนวทางการสำรวจที่ลดภาระในเรื่องการสำรวจและให้มุมมองรวมของข้อมูลที่ได้รับจากพนักงานและผู้มีส่วนได้ส่วนเสียอื่น ๆ

2.3 กำหนดแนวทางแบบบูรณาการเพื่อการประเมินตนเอง โดยกำหนดแนวทางการประเมินตนเองที่รวมการประเมินความรับผิดชอบและผลลัพธ์ที่เกี่ยวข้องกับระบบ GRC เข้ากับการประเมินตนเองอื่น ๆ ที่บังคับใช้กับฝ่ายบริหาร

2.4 รวบรวมข้อมูลผ่านการสังเกตและการสนทนา โดยกำหนดวิธีการรวบรวมความคิดเห็นอย่างไม่เป็นทางการผ่านการสังเกต การประชุมกลุ่ม การสนทนากลุ่ม และการสนทนาเป็นรายบุคคล

2.5 รายงานข้อมูลและผลการวิจัย โดยให้ข้อมูลและข้อค้นพบจากวิธีการสอบถามทั้งหมดแก่ผู้บริหาร

3. การควบคุมแบบค้นพบ (detective control) คือ การสร้างกระบวนการทุนมนุษย์ กิจกรรมเทคโนโลยีและการควบคุมทางกายภาพ เพื่อตรวจจับเหตุการณ์และพฤติกรรมที่ไม่พึงประสงค์ ตลอดจนจุดอ่อนในระบบ GRC ซึ่งสามารถกระทำได้โดย

3.1 จัดตั้ง detective process controls โดยกำหนดกิจกรรมและขั้นตอนการควบคุมกระบวนการที่ตรวจจับเหตุการณ์ไม่พึงประสงค์ การไม่ปฏิบัติตามข้อกำหนดและการประพฤติมิชอบ

3.2 จัดตั้ง detective human capital process controls โดยจัดตั้งกิจกรรมและขั้นตอนการควบคุมทุนมนุษย์เพื่อตรวจหาเหตุการณ์ไม่พึงประสงค์ การไม่ปฏิบัติตาม และการประพฤติมิชอบ

3.3 สร้าง detective physical controls โดยติดตั้งการควบคุมทางกายภาพที่จำเป็นเพื่อให้การเฝ้าระวังการควบคุมป้องกันทางกายภาพและพื้นที่ที่สามารถสังเกตการไม่ปฏิบัติตามหรือการปฏิบัติที่ผิดจรรยาบรรณทางกายภาพได้

3.4 จัดตั้งและสร้าง detective technology controls โดยดำเนินการและตรวจสอบการควบคุมเทคโนโลยีตรวจจับอัตโนมัติเพื่อระบุการประพฤติมิชอบที่เกิดขึ้นจริงหรือที่อาจเกิดขึ้นในทันที

3.5 รวบรวมและวิเคราะห์ผลการควบคุม โดยรวบรวมและวิเคราะห์ข้อมูลทั้งหมดที่รวบรวมผ่านวิธีการตรวจจับต่าง ๆ เพื่อระบุรูปแบบการประพฤติมิชอบ เหตุการณ์ไม่พึงประสงค์ และจุดอ่อนอื่น ๆ ที่อาจไม่มีใครสังเกตเห็น

องค์ประกอบที่หก: ตอบสนองและแก้ปัญหา (respond & resolve)

คือ การตอบสนองและกู้คืนจากเหตุการณ์การไม่ปฏิบัติตามข้อกำหนดและการปฏิบัติที่ผิดจรรยาบรรณ หรือความล้มเหลวของระบบ GRC เพื่อให้องค์กรสามารถแก้ไขปัญหาแต่ละอย่างในทันที และป้องกันหรือแก้ไขปัญหาที่คล้ายคลึงกันอย่างมีประสิทธิภาพและประสิทธิผลมากขึ้นในอนาคต

1. การตรวจสอบและการสอบสวนภายใน (internal review & investigation) เกี่ยวข้องกับการทบทวนและเตรียมพร้อมที่จะสอบสวนข้อกล่าวหา หรือข้อบ่งชี้ของการประพฤติมิชอบ หรือความล้มเหลวของระบบ GRC เพื่อทำความเข้าใจข้อเท็จจริง สถานการณ์ สาเหตุ และการแก้ไขที่เหมาะสม ซึ่งสามารถกระทำได้โดย

1.1 กำหนดกระบวนการตรวจสอบและสอบสวน โดยกำหนดขั้นตอนสำหรับการสอบสวนเพิ่มเติม การตรวจสอบ การร้องเรียน หรือรายงานเกี่ยวกับการปฏิบัติตามข้อกำหนดหรือประเด็นด้านจริยธรรม ตลอดจนปัญหาที่ตรวจพบระหว่างการตรวจสอบอย่างต่อเนื่อง หรือการประเมินระบบ GRC เป็นระยะ

1.2 เตรียมสอบสวน โดยเตรียมดำเนินกิจกรรมของขั้นตอนการตรวจสอบของกระบวนการแก้ไขปัญหา

1.3 การดำเนินการสอบสวน โดยดำเนินการตรวจสอบที่สอดคล้องกับแผนและสื่อสารกับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องในขณะที่รักษาสถานะสิทธิพิเศษที่เหมาะสม

1.4 รายงานผลการสอบสวน โดยสื่อสารผลการสอบสวนที่เหมาะสมไปยังผู้บริหาร หน่วยงานกำกับดูแล และผู้มีส่วนได้ส่วนเสียตามความเหมาะสม

2. การสอบถามและการสอบสวนของบุคคลที่สาม เกี่ยวข้องกับการจัดการและตอบสนองต่อข้อซักถามและการสอบสวนจากภายนอก ซึ่งสามารถกระทำได้โดย

2.1 เตรียมตัวและตอบคำถามของบุคคลที่สาม โดยระบุและตอบคำถามจากบุคคลที่สาม

2.2 เตรียมระบุการสอบสวนของบุคคลที่สาม โดยกำหนดวิธีการเพื่อให้แน่ใจว่าบุคคลที่เหมาะสมทราบเกี่ยวกับการสอบสวนของบุคคลที่สามที่ริเริ่มขึ้น

2.3 เตรียมจัดการการสอบสวนของบุคคลที่สาม โดยกำหนดนโยบาย ขั้นตอน และความรับผิดชอบในการจัดการการสืบสวนของบุคคลที่สามประเภทต่าง ๆ

2.4 เตรียมเลือกทีมภายในสำหรับการสอบสวนบุคคลที่สาม โดยกำหนดขั้นตอนการคัดเลือกทีมของบุคคลที่จะเป็นตัวแทนขององค์กรในระหว่างการสอบสวนเฉพาะ

2.5 เตรียมตอบสนองต่อการสอบสวนของบุคคลภายนอกโดยเฉพาะ โดยกำหนดขั้นตอนในการพัฒนาการตอบสนองต่อการสอบสวนที่เฉพาะเจาะจง

3. การควบคุมแบบแก้ไข (corrective controls) เกี่ยวข้องกับการกำหนดกระบวนการทุนมนุษย์ เทคโนโลยี และกิจกรรมการควบคุมทางกายภาพ เพื่อแก้ไขผลที่ไม่พึงประสงค์ซึ่งเป็นผลมาจากเหตุการณ์ กิจกรรม และพฤติกรรมที่ไม่พึงประสงค์ ซึ่งสามารถกระทำได้โดย

3.1 กำหนดการควบคุมกระบวนการแก้ไข เพื่อหยุด ชะลอ และฟื้นตัวจากเหตุการณ์ไม่พึงประสงค์ และยับยั้งเหตุการณ์ไม่พึงประสงค์ในอนาคต

3.2 สร้างการควบคุมทุนมนุษย์ที่ถูกต้อง โดยสร้างการควบคุมทุนมนุษย์แก้ไขที่หยุด ชะลอ และฟื้นตัวจากเหตุการณ์ไม่พึงประสงค์ และยับยั้งเหตุการณ์ไม่พึงประสงค์ในอนาคต

3.3 สร้างการควบคุมเทคโนโลยีที่ถูกต้อง โดยการสร้างการควบคุมเทคโนโลยีการแก้ไขที่หยุด ชะลอ และฟื้นตัวจากเหตุการณ์ไม่พึงประสงค์ และยับยั้งเหตุการณ์ไม่พึงประสงค์ในอนาคต

3.4 สร้างการควบคุมทางกายภาพที่ถูกต้อง โดยสร้างการควบคุมทางกายภาพที่ถูกต้องเพื่อหยุด ชะลอ และฟื้นตัวจากเหตุการณ์ไม่พึงประสงค์ และยับยั้งเหตุการณ์ไม่พึงประสงค์ในอนาคต

3.5 ติดตามและรายงานการควบคุมที่ถูกต้อง โดยติดตามและรายงานความคืบหน้าของกิจกรรมการควบคุมการแก้ไข

4. การตอบสนองต่อวิกฤต ความต่อเนื่อง และการกู้คืน (crisis response, continuity and recovery) เกี่ยวข้องกับการวางแผนและตอบสนองต่อปัญหาวิกฤต การหยุดชะงักของธุรกิจ และเหตุการณ์สำคัญอื่น ๆ ซึ่งสามารถกระทำได้โดย

4.1 พัฒนาการตอบสนองต่อวิกฤตและแผนต่อเนื่อง โดยพัฒนาแผนรองรับวิกฤตประเภทต่าง ๆ และการฟื้นตัวจากธุรกิจที่หยุดชะงัก

4.2 ระบุความพร้อมและตอบสนองในภาวะวิกฤต โดยกำหนดบุคลากรที่จะรับผิดชอบในการเตรียมความพร้อมสำหรับวิกฤตและผู้ที่จะนำไปใช้เป็นทีมตอบสนองวิกฤตสำหรับวิกฤตที่ระบุแต่ละประเภท

4.3 แผนการทดสอบและขั้นตอนการทดสอบ โดยทดสอบและประเมินแผนวิกฤตและขั้นตอนต่าง ๆ

4.4 แผนประสานงาน โดยประสานงานแผนความต่อเนื่องและการตอบสนองต่าง ๆ เพื่อรอการหยุดชะงักของธุรกิจที่อาจครอบคลุมมากกว่าหนึ่งสิ่งอำนวยความสะดวก

5. การแก้ไขและวินัย (remediation & discipline) เกี่ยวข้องกับการแก้ไขปัญหาที่มีหลักฐานยืนยันโดยแก้ไขจุดอ่อนในระบบ GRC และอบรมสั่งสอนบุคคลที่เหมาะสม ซึ่งสามารถกระทำได้โดย

5.1 แก้ไขระบบ GRC โดยแก้ไขปัญหา/เหตุการณ์ที่รายงานแต่ละรายการบันทึกผลลัพธ์ และเสนอการเปลี่ยนแปลงที่เหมาะสมกับระบบ GRC เพื่อหลีกเลี่ยงปัญหาที่คล้ายกันในอนาคต

5.2 วินัยส่วนบุคคล ในการประพฤติมิชอบ

5.3 เปิดเผยแนวทางแก้ไขปัญหา โดยให้เปิดเผยข้อค้นพบและการแก้ปัญหาการสอบสวนแก่ผู้มีส่วนได้ส่วนเสียเมื่อมีความจำเป็นและเหมาะสม

องค์ประกอบที่เจ็ด: ตรวจสอบและวัดผล (monitor & measure)

คือ การตรวจสอบ วัดผล และปรับเปลี่ยนระบบ GRC เป็นระยะและต่อเนื่อง เพื่อให้แน่ใจว่าระบบดังกล่าวเอื้อต่อวัตถุประสงค์ทางธุรกิจในขณะที่มีประสิทธิภาพ ประสิทธิผล และตอบสนองต่อสภาพแวดล้อมที่เปลี่ยนแปลงไป

1. การตรวจสอบบริบท (context monitoring) เกี่ยวข้องกับการติดตามและวิเคราะห์การเปลี่ยนแปลงในบริบทภายในและภายนอกเพื่อพิจารณาว่าจำเป็นต้องเปลี่ยนแปลงระบบ GRC หรือไม่ ซึ่งสามารถกระทำได้โดย

1.1 ตรวจสอบบริบทภายนอก โดยตรวจสอบการเปลี่ยนแปลงอย่างต่อเนื่องในสภาพแวดล้อมภายนอกที่อาจส่งผลโดยตรง ทางอ้อม หรือสะสมต่อองค์กร

1.2 ตรวจสอบบริบทภายใน โดยตรวจสอบการเปลี่ยนแปลงสภาพแวดล้อมภายในอย่างต่อเนื่องที่อาจส่งผลโดยตรง ทางอ้อม หรือสะสมต่อองค์กร

2. การติดตามและประเมินผลการปฏิบัติงาน (performance monitoring & evaluation) เกี่ยวข้องกับการตรวจสอบและประเมินประสิทธิภาพของระบบ GRC เป็นระยะเพื่อให้แน่ใจว่าได้รับการออกแบบและดำเนินการอย่างมีประสิทธิผล มีประสิทธิภาพ และตอบสนองต่อบริบทภายนอกและภายในที่เปลี่ยนแปลงไป ซึ่งสามารถกระทำได้โดย

2.1 ตรวจสอบและประเมินการออกแบบระบบ GRC โดยกำหนดตารางเวลาสำหรับการประเมินความเหมาะสมของการออกแบบระบบ GRC ใหม่เป็นระยะตามข้อกำหนดที่ระบุและความเสี่ยงที่สำคัญ

2.2 ทบทวนและพิจารณาความเสี่ยง โดยทบทวนความเสี่ยงที่ได้รับการประเมินก่อนหน้านี้ หรือที่เพิ่งระบุและพิจารณาใหม่ หรือประเมินเป็นครั้งแรกโดยพิจารณาจากข้อมูลที่ดีที่สุดที่มีอยู่ในปัจจุบัน

2.3 ระบุกิจกรรมการเพิ่มประสิทธิภาพความเสี่ยงที่เกี่ยวข้อง โดยทบทวนกิจกรรมการเพิ่มประสิทธิภาพความเสี่ยงที่เกี่ยวข้องเพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูง

2.4 วิเคราะห์ศักยภาพสำหรับความล้มเหลว โดยวิเคราะห์ศักยภาพที่กิจกรรมการเพิ่มประสิทธิภาพความเสี่ยงจะล้มเหลวและวิธีที่อาจล้มเหลว

2.5 ระบุข้อมูลการตรวจสอบ โดยระบุข้อมูลที่จะใช้เพื่อสนับสนุนการประเมินประสิทธิภาพของกิจกรรมการปรับความเสี่ยงให้เหมาะสมและ/หรือประสิทธิภาพโดยรวมของระบบ GRC

2.6 ดำเนินการตรวจสอบกิจกรรม โดยดำเนินกิจกรรมการติดตามเพื่อสนับสนุนการประเมินประสิทธิภาพของระบบ

2.7 วิเคราะห์และรายงานผลการตรวจสอบ โดยวิเคราะห์ผลลัพธ์ของกิจกรรมการตรวจสอบเพื่อระบุจุดอ่อนและโอกาสในการปรับปรุงระบบในทันที

3. การปรับปรุงระบบ (systemic improvement) เกี่ยวข้องกับการใช้ข้อมูลจากการตรวจสอบเป็นระยะ รวมถึงกิจกรรมการตรวจจับอย่างต่อเนื่องเพื่อระบุโอกาสในการปรับปรุงระบบ GRC ซึ่งสามารถกระทำได้โดย

3.1 พัฒนาแผนการปรับปรุง โดยพัฒนาแผนการจัดลำดับความสำคัญสำหรับการดำเนินการปรับปรุงโปรแกรม

3.2 ดำเนินการริเริ่มการปรับปรุง โดยดำเนินการตามแผนปฏิบัติการเฉพาะและความคิดริเริ่มที่มีจุดประสงค์เพื่อปรับปรุงโปรแกรม

4. การรับประกัน (assurance) เกี่ยวข้องกับการให้การรับรองแก่ฝ่ายบริหารและคณะกรรมการว่าระบบ GRC มีความน่าเชื่อถือ มีประสิทธิภาพ และตอบสนองได้ดี ซึ่งสามารถกระทำได้โดย

4.1 การประเมินแผนประกัน โดยกำหนดขอบเขต ขั้นตอน และเกณฑ์ที่จำเป็นเพื่อให้ระดับความเชื่อมั่นที่ต้องการ

4.2 ประเมินผลการประกัน โดยดำเนินการตามขั้นตอน ประเมินผลตามเกณฑ์และจัดส่งรายงาน

องค์ประกอบที่แปด: แจ้งและบูรณาการ (inform & integrate)

คือ การรวบรวม จัดทำเอกสาร และจัดการข้อมูล GRC เพื่อให้ข้อมูลส่งผ่านทั่วทั้งองค์กรได้อย่างมีประสิทธิภาพและแม่นยำ รวมถึงส่งผ่านไปสู่ผู้มีส่วนได้ส่วนเสียภายนอก

1. การจัดการข้อมูลและเอกสาร (information management & documentation) เกี่ยวข้องกับการดำเนินการและจัดการระบบการจัดการบันทึกแบบบูรณาการ เพื่อให้ข้อมูล GRC มีความเกี่ยวข้อง เชื่อถือได้ ทันเวลา ปลอดภัย และพร้อมใช้งาน ซึ่งสามารถกระทำได้โดย

1.1 พัฒนาโครงสร้างการจำแนกประเภทการจัดการข้อมูล GRC โครงสร้าง โดยกำหนดคำจำกัดความ การจำแนกประเภท และขั้นตอนที่จำเป็นในการระบุและจัดการข้อมูล GRC ในองค์กรและองค์กรขยาย โดยเป็นส่วนหนึ่งของแผนการจัดการข้อมูล

1.2 พัฒนานโยบายและขั้นตอนในการรวบรวมข้อมูล GRC โดยกำหนดนโยบายและขั้นตอนที่จำเป็นในการรวบรวมข้อมูล GRC จากแหล่งที่มาภายในและภายนอกองค์กรและองค์กรขยาย โดยเป็นส่วนหนึ่งของแผนการจัดการข้อมูล

1.3 พัฒนาข้อมูล GRC การเข้าถึง การใช้งาน และโอนนโยบายและขั้นตอน โดยกำหนดนโยบายและขั้นตอนที่จำเป็นในการเข้าถึง การใช้ และถ่ายโอนข้อมูล GRC ในองค์กรและองค์กรขยาย โดยเป็นส่วนหนึ่งของแผนการจัดการข้อมูล

1.4 พัฒนานโยบายการจัดเก็บและการกำจัดข้อมูล GRC และขั้นตอน โดยกำหนดนโยบายและขั้นตอนที่จำเป็นในการจัดเก็บข้อมูล GRC ในองค์กรและขยายองค์กรตามข้อกำหนดและวัตถุประสงค์ในการกู้คืน ซึ่งเป็นส่วนหนึ่งของแผนการจัดการข้อมูล

2. การสื่อสารภายในและภายนอก (internal & external communication) เกี่ยวข้องกับการนำเสนอข้อมูลที่เกี่ยวข้อง เชื่อถือได้ และทันเวลาแก่ผู้ฟังที่เหมาะสมตามที่ได้รับมอบอำนาจหรือตามความจำเป็นในการปฏิบัติหน้าที่และกำหนดทัศนคติอย่างมีประสิทธิผล ซึ่งสามารถกระทำได้โดย

2.1 พัฒนาแผนการรายงาน โดยจัดทำแผนเพื่อให้แน่ใจว่าสอดคล้องกับข้อกำหนดการรายงานที่จำเป็นและจัดทำรายงานที่ต้องการต่อผู้บริหาร คณะกรรมการและผู้มีส่วนได้ส่วนเสีย

2.2 พัฒนาแผนการสื่อสาร โดยกำหนดวิธีที่องค์กรจะจัดการการสื่อสารที่เกี่ยวข้องกับ GRC ที่ไม่ใช่รายงานที่เป็นทางการ

3. เทคโนโลยีและโครงสร้างพื้นฐาน (technology & infrastructure) เกี่ยวข้องกับการเปิดใช้งานระบบ GRC ด้วยสถาปัตยกรรมเทคโนโลยีที่รวมเข้าด้วยกัน และใช้การลงทุนที่มีอยู่ในเทคโนโลยีตามความเหมาะสม ซึ่งสามารถกระทำได้โดย

3.1 ประเมินความต้องการและช่องว่างทางเทคโนโลยี โดยระบุช่องว่างและระบบที่มีประสิทธิภาพต่ำกว่าในสภาพแวดล้อมเทคโนโลยีที่มีอยู่

3.2 พัฒนาเทคโนโลยี GRC ซึ่งเป็นส่วนหนึ่งของแผนยุทธศาสตร์ GRC โดยพัฒนาแผนสำหรับการใช้เทคโนโลยีเพื่อให้กระบวนการ GRC และกระแสข้อมูลสามารถทำงานได้

1.3 กรอบการบริหารความเสี่ยงในประเทศไทย

1.3.1 หลักเกณฑ์กระทรวงการคลัง ว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562

เนื่องด้วยกระทรวงการคลังได้กำหนดหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานภาครัฐ พ.ศ. 2561 กำหนดให้หน่วยงานภาครัฐประเมินการควบคุมภายในแล้วรายงานต่อกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ผู้กำกับดูแล เพื่อปรับปรุงการควบคุมภายในให้มีประสิทธิภาพเหมาะสมกับสภาพแวดล้อมและความเสี่ยงที่เปลี่ยนแปลงไปอยู่เสมอนั้น ด้วยความตระหนักว่าการบริหารความเสี่ยงเป็นกลไกสำคัญในการพัฒนามหาวิทยาลัยให้เป็นองค์กรสมรรถนะสูงและมีธรรมาภิบาลในการบริหาร มหาวิทยาลัยดำเนินการบริหารจัดการความเสี่ยงและควบคุมภายในให้เป็นไปตามหลักเกณฑ์ข้างต้น พร้อมกับหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 โดยมีกระบวนการรายงานการบริหารความเสี่ยงและวางระบบควบคุมภายใน ตามมาตรฐานการบริหารจัดการความเสี่ยงดังนี้

หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 ออกโดยอาศัยอำนาจตามความในมาตรา 39 แห่งพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 เพื่อให้การดำเนินงานบรรลุวัตถุประสงค์ตามยุทธศาสตร์ที่หน่วยงานของรัฐกำหนด โดยมีการกำหนดหลักเกณฑ์เกี่ยวกับการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐไว้ดังต่อไปนี้

ข้อ 1 หลักเกณฑ์นี้เรียกว่า “หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562”

ข้อ 2 หลักเกณฑ์นี้ให้ใช้บังคับในรอบระยะเวลาบัญชีของหน่วยงานของรัฐถัดจากปีที่กระทรวงการคลังประกาศเป็นต้นไป

ข้อ 3 ให้หน่วยงานของรัฐตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐที่แนบท้ายหลักเกณฑ์ฉบับนี้

ข้อ 4 กรณีหน่วยงานของรัฐ มีเจตนาหรือปล่อยปละละเลยในการปฏิบัติตามมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐที่กระทรวงการคลังกำหนด โดยไม่มีเหตุอันควร ให้กระทรวงการคลังพิจารณาความเหมาะสมในการเสนอความเห็นเกี่ยวกับพฤติการณ์ของหน่วยงานของรัฐดังกล่าวให้ผู้ที่เกี่ยวข้องดำเนินการตามอำนาจและหน้าที่ต่อไป

ต่อมา ในเดือนมีนาคม 2562 กระทรวงการคลังได้มีการออกมาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เพื่อให้หน่วยงานของรัฐใช้เป็นกรอบหรือแนวทางพื้นฐานในการกำหนดนโยบายการจัดทำแผนการบริหารจัดการความเสี่ยงและการติดตามประเมินผล รวมทั้งการรายงานผลเกี่ยวกับการบริหารจัดการความเสี่ยง อันจะทำให้เกิดอย่างสมเหตุสมผลต่อผู้ที่เกี่ยวข้องทุกฝ่าย และการบริหารงานของหน่วยงานของรัฐสามารถบรรลุตามวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ และเพื่อให้สอดคล้องกับพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 หมวด 4 การบัญชี การรายงานและการตรวจสอบ มาตรา 79[1]

1. มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐเป็นมาตรฐานเบื้องต้นซึ่งจัดทำขึ้นตามแนวทางการบริหารจัดการความเสี่ยงของสากลโดยกำหนดให้เหมาะสมกับบริบทของหน่วยงานของรัฐในประเทศไทย ทั้งนี้มีการให้คำนิยามของคำต่าง ๆ และมาตรฐานการบริหารจัดการความเสี่ยง โดยมีรายละเอียดดังนี้

[1] มาตรา 79 บัญญัติให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายในและการบริหารจัดการความเสี่ยงโดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนดซึ่งการบริหารจัดการความเสี่ยงเป็นกระบวนการที่ใช้ในการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงานของรัฐ เพื่อให้หน่วยงานของรัฐสามารถดำเนินการให้บรรลุวัตถุประสงค์ รวมถึงเพิ่มศักยภาพและขีดความสามารถให้หน่วยงานของรัฐ

คำนิยาม

“หน่วยงานของรัฐ” หมายถึง (1) ส่วนราชการ (2) รัฐวิสาหกิจ (3) หน่วยงานของรัฐสภา ศาลยุติธรรม ศาลปกครอง ศาลรัฐธรรมนูญ องค์กรอิสระตามรัฐธรรมนูญ และองค์กรอัยการ (4) องค์การมหาชน (5) ทุนหมุนเวียนที่มีฐานะเป็นนิติบุคคล (6) องค์กรปกครองส่วนท้องถิ่น (7) หน่วยงานอื่นของรัฐตามที่กฎหมายกำหนด

“ผู้กำกับดูแล” หมายความว่า บุคคล หรือคณะบุคคล ผู้มีหน้าที่รับผิดชอบในการกำกับดูแลหรือบังคับบัญชาของหน่วยงานของรัฐ

“หัวหน้าหน่วยงานของรัฐ” หมายความว่า ผู้บริหารสูงสุดของหน่วยงานของรัฐ

“ฝ่ายบริหาร” หมายถึงผู้บริหารทุกระดับของหน่วยงานของรัฐ

“ผู้รับผิดชอบ” หมายถึงคณะบุคคลหรือหน่วยงานที่ได้รับมอบหมายให้ทำหน้าที่เกี่ยวกับการบริหารจัดการความเสี่ยงของหน่วยงานของรัฐที่อยู่ภายใต้การบริหารจัดการของหัวหน้าหน่วยงาน

“การบริหารจัดการความเสี่ยง” หมายถึงกระบวนการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อหน่วยงานของรัฐ เพื่อให้หน่วยงานของรัฐสามารถดำเนินงานให้บรรลุวัตถุประสงค์ของหน่วยงาน รวมถึงเพื่อเพิ่มศักยภาพและขีดความสามารถให้หน่วยงานของรัฐ

“ความเสี่ยง” หมายความว่า ความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้น และเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ของหน่วยงาน

มาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ

1. หน่วยงานของรัฐต้องจัดให้มีการบริหารจัดการความเสี่ยง เพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลแก่ผู้มีส่วนได้ส่วนเสียของหน่วยงานว่าหน่วยงานได้ดำเนินการบริหารจัดการความเสี่ยงอย่างเหมาะสม

2. ฝ่ายบริหารของหน่วยงานของรัฐต้องจัดให้มีสภาพแวดล้อมที่เหมาะสมต่อการบริหารจัดการความเสี่ยงภายในองค์กร อย่างน้อยประกอบด้วย การมอบหมายผู้รับผิดชอบเรื่องการบริหารจัดการความเสี่ยง การกำหนดวัฒนธรรมของหน่วยงานของรัฐที่ส่งเสริมการบริหารจัดการความเสี่ยง รวมถึงการบริหารทรัพยากร

3. หน่วยงานของรัฐต้องมีการกำหนดวัตถุประสงค์เพื่อใช้ในการบริหารจัดการความเสี่ยงที่เหมาะสม รวมถึงมีการสื่อสารการบริหารจัดการความเสี่ยงของวัตถุประสงค์ด้านต่าง ๆ ต่อบุคลากรที่เกี่ยวข้อง

4. การบริหารจัดการความเสี่ยงต้องดำเนินการในทุกระดับของหน่วยงานของรัฐ

5. การบริหารจัดการความเสี่ยง อย่างน้อยต้องประกอบด้วย การระบุความเสี่ยง การประเมินความเสี่ยง และการตอบสนองความเสี่ยง

6. หน่วยงานของรัฐต้องจัดทำแผนบริหารจัดการความเสี่ยงอย่างน้อยปีละครั้ง และต้องมีการสื่อสารแผนบริหารจัดการความเสี่ยงกับผู้ที่เกี่ยวข้องทุกฝ่าย

7. หน่วยงานของรัฐต้องมีการติดตามประเมินผลการบริหารจัดการความเสี่ยง และทบทวนแผนการบริหารจัดการความเสี่ยงอย่างสม่ำเสมอ

8. หน่วยงานของรัฐต้องมีการรายงานการบริหารจัดการความเสี่ยงของหน่วยงานต่อผู้ที่เกี่ยวข้อง

9. หน่วยงานของรัฐสามารถพิจารณานำเครื่องมือการบริหารความเสี่ยงที่เหมาะสมมาประยุกต์ใช้กับหน่วยงาน เพื่อให้การบริหารจัดการความเสี่ยงของหน่วยงานเกิดประสิทธิภาพสูงสุด

ทั้งนี้เพื่อให้บรรลุวัตถุประสงค์ของหน่วยงานของรัฐ หน่วยงานของรัฐจะต้องจัดทำแผนบริหารจัดการความเสี่ยง โดยต้องจัดให้มีผู้รับผิดชอบ ซึ่งต้องประกอบด้วยฝ่ายบริหารและบุคลากรที่มีความรู้ความเข้าใจเกี่ยวกับการจัดทำยุทธศาสตร์และการบริหารจัดการความเสี่ยงของหน่วยงานของรัฐ ดำเนินการเกี่ยวกับการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ ทั้งนี้ไม่ควรเป็นผู้ตรวจสอบภายในของหน่วยงานของรัฐ โดยผู้รับผิดชอบมีหน้าที่ในการจัดทำแผนการบริหารจัดการความเสี่ยง ติดตามประเมินผลการบริหารจัดการความเสี่ยง จัดทำรายงานผลตามแผนการบริหารจัดการความเสี่ยง และพิจารณาทบทวนแผนการบริหารจัดการความเสี่ยง โดยมีรายละเอียดดังต่อไปนี้

1. ให้หัวหน้าหน่วยงานของรัฐหรือผู้กำกับดูแลแล้วแต่กรณี กำกับดูแลฝ่ายบริหาร ผู้รับผิดชอบและบุคลากรที่เกี่ยวข้องให้มีการบริหารจัดการความเสี่ยงให้เป็นไปตามแผนการบริหารจัดการความเสี่ยงที่กำหนดไว้

2. ให้ฝ่ายบริหารและผู้รับผิดชอบต้องจัดให้มีการติดตามประเมินผลการบริหารจัดการความเสี่ยง โดยติดตามประเมินผลอย่างต่อเนื่องในระหว่างการปฏิบัติงาน หรือติดตามประเมินผลเป็นรายครั้ง หรือใช้ทั้งสองวิธีร่วมกัน กรณีพบข้อบกพร่องที่มีสาระสำคัญให้รายงานทันที

3. ให้ผู้รับผิดชอบของหน่วยงานของรัฐจัดทำรายงานผลการบริหารจัดการความเสี่ยง และเสนอให้หัวหน้าหน่วยงานของรัฐหรือผู้กำกับดูแลแล้วแต่กรณี พิจารณาอย่างน้อยปีละ 1 ครั้ง

4. หัวหน้าหน่วยงานของรัฐหรือผู้กำกับดูแลแล้วแต่กรณี สามารถกำหนดนโยบาย วิธีการ และระยะเวลาการรายงานการบริหารจัดการความเสี่ยง

5. ให้หน่วยงานของรัฐดำเนินการจัดส่งรายงานแผนการบริหารจัดการความเสี่ยง หรือรายงานผลการบริหารจัดการความเสี่ยง หรือข้อมูลเพิ่มเติมอื่น ๆ เกี่ยวกับกระบวนการบริหารจัดการความเสี่ยงตามรูปแบบ วิธีการ และระยะเวลาที่กรมบัญชีกลางหรือสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจกำหนด ในกรณีที่คณะกรรมการนโยบายรัฐวิสาหกิจร้องขอ

กรณีหน่วยงานของรัฐไม่สามารถปฏิบัติตามหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐได้ให้ขอทำความตกลงกับกระทรวงการคลัง

อนึ่ง สำหรับหน่วยงานของรัฐที่ได้ดำเนินการหรืออยู่ระหว่างการบริหารจัดการความเสี่ยงให้ดำเนินการต่อไปจนกว่าจะแล้วเสร็จ และให้ถือปฏิบัติตามหลักเกณฑ์การบริหารจัดการความเสี่ยงนี้ในรอบระยะเวลาบัญชีถัดไป สำหรับหน่วยงานของรัฐที่ยังไม่ได้ดำเนินการบริหารจัดการความเสี่ยง ให้ถือปฏิบัติตามหลักเกณฑ์การบริหารจัดการความเสี่ยงฉบับนี้ในรอบระยะเวลาบัญชีถัดไป

นอกจากนี้ ในเดือนกุมภาพันธ์ 2564 กระทรวงการคลังได้มีการออก**แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่อง หลักการบริหารจัดการความเสี่ยง** เพื่อเป็นกรอบแนวทางการบริหารจัดการความเสี่ยงซึ่งได้ผสานกรอบแนวคิดด้านการบริหารจัดการความเสี่ยงขององค์กรชั้นนำต่าง ๆ ประกอบด้วย Committee of Sponsoring Organizations of the Treadway Commission (COSO) และ International Organization for Standardization (ISO) รวมถึงการบริหารจัดการความเสี่ยงในภาครัฐของประเทศต่าง ๆ มากำหนดเป็นแนวทางการบริหารจัดการความเสี่ยง สำหรับหน่วยงานของรัฐตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ โดยหน่วยงานของรัฐสามารถนำหลักการบริหารจัดการความเสี่ยงระดับองค์กรดังกล่าวเป็นแนวทางในการพัฒนาระบบการบริหารจัดการความเสี่ยงขององค์กร เพื่อให้การบริหารจัดการความเสี่ยงเป็นเครื่องมือสำคัญในการบริหารงานให้เป็นไปตามหลักธรรมาภิบาล ทั้งนี้หัวหน้าหน่วยงานของรัฐมีหน้าที่รับผิดชอบโดยตรงในการจัดให้มีระบบการบริหารจัดการความเสี่ยงของหน่วยงานของรัฐที่มีประสิทธิภาพ เพื่อประโยชน์ของประชาชนและผู้มีส่วนได้ส่วนเสียทุกฝ่าย

รูปที่ 8 แนวทางหลักการบริหารจัดการความเสี่ยงระดับองค์กร

อย่างไรก็ดี การบริหารจัดการความเสี่ยงแต่ละหน่วยงานอาจมีความแตกต่างกันไป โดยขึ้นอยู่กับขนาด โครงสร้าง และความสามารถในการรองรับความเสี่ยงของหน่วยงาน แนวทางการบริหารจัดการความเสี่ยงฉบับนี้อาจมีเนื้อหาบางส่วนเกี่ยวข้องกับการควบคุมภายใน เนื่องจากการควบคุมภายในถือเป็นส่วนหนึ่งของการบริหารจัดการความเสี่ยงระดับองค์กร ดังนั้น หน่วยงานอาจดำเนินการบริหารจัดการความเสี่ยงโดยเชื่อมโยงการควบคุมภายในและการบริหารจัดการความเสี่ยงเข้าด้วยกัน อนึ่ง อาจกล่าวได้ว่า การบริหารจัดการความเสี่ยงถือเป็นส่วนหนึ่งของการบริหารองค์กรอย่างมีธรรมาภิบาล โดยปัจจัยหลักของการบริหารจัดการความเสี่ยงที่ประสบความสำเร็จเกิดจากความมุ่งมั่นของหัวหน้าหน่วยงานของรัฐและผู้กำกับดูแล

2. หลักการบริหารจัดการความเสี่ยงระดับองค์กร สามารถแบ่งออกเป็น 2 ส่วน ได้แก่

2.1 กรอบการบริหารจัดการความเสี่ยง เป็นพื้นฐานของการบริหารจัดการความเสี่ยงที่ดี เพื่อให้การบริหารจัดการความเสี่ยงเป็นเครื่องมือช่วยหน่วยงานในการกำหนดแผนระดับองค์กร (strategic plans) และการกำหนดวัตถุประสงค์เป็นไปอย่างมีประสิทธิผล รวมถึงการตัดสินใจของผู้บริหารอยู่บนฐานข้อมูลสารสนเทศที่สมบูรณ์ ส่งผลให้หน่วยงานของรัฐสามารถดำเนินงานบรรลุวัตถุประสงค์หลักขององค์กร และเพื่อเพิ่มศักยภาพและขีดความสามารถของหน่วยงาน หน่วยงานของรัฐจึงควรพิจารณานำกรอบการบริหารจัดการความเสี่ยงนี้ไปปรับใช้ในการวางระบบการบริหารจัดการความเสี่ยงของหน่วยงาน เพื่อให้หน่วยงานได้รับประโยชน์สูงสุดจากการบริหารจัดการความเสี่ยงอย่างแท้จริง โดยหน่วยงานของรัฐแต่ละแห่งอาจมีศักยภาพที่แตกต่างกันในการนำกรอบการบริหารจัดการความเสี่ยงทั้งหมดไปปรับใช้ ทั้งนี้ขึ้นอยู่กับความพร้อมของหน่วยงาน โดยกรอบบริหารจัดการความเสี่ยงประกอบด้วยหลักการ 8 ประการ ดังนี้

1) การบริหารจัดการความเสี่ยงต้องดำเนินการแบบบูรณาการทั่วทั้งองค์กร ควรมีลักษณะดังนี้

(1) การบริหารจัดการความเสี่ยงต้องมีการบริหารจัดการในภาพรวมมากกว่าแยกเดี่ยว เนื่องจากความเสี่ยงของกิจกรรมหนึ่งอาจมีผลกระทบต่อความเสี่ยงของกิจกรรมอื่น เช่น ความเสี่ยงของความล่าช้าในระบบการขนส่งวัตถุดิบไม่เพียงกระทบต่อกิจกรรมการผลิต อาจมีผลกระทบด้านการส่งมอบสินค้า ค่าปรับที่อาจจะเกิดขึ้น รวมถึงชื่อเสียงขององค์กร

(2) การบริหารความเสี่ยงควรผนวกเข้าเป็นส่วนหนึ่งของการดำเนินงานขององค์กร รวมถึงกระบวนการจัดทำแผนกลยุทธ์ และกระบวนการประเมินผล

(3) การบริหารจัดการความเสี่ยงต้องช่วยสนับสนุนกระบวนการตัดสินใจในทุกระดับขององค์กร

2) ความมุ่งมั่นของผู้กำกับดูแล หัวหน้าหน่วยงานของรัฐ และผู้บริหารระดับสูง การบริหารจัดการความเสี่ยงจะประสบความสำเร็จขึ้นอยู่กับความมุ่งมั่นของผู้กำกับดูแล หัวหน้าหน่วยงานของรัฐ และผู้บริหารระดับสูง หน่วยงานของรัฐบางแห่งมีผู้กำกับดูแลในรูปแบบคณะกรรมการซึ่งมีหน้าที่ในการกำกับฝ่ายบริหารให้มีการบริหาร

จัดการตามหลักธรรมาภิบาล ผู้กำกับดูแลซึ่งมีหน้าที่ดังกล่าวจะมีหน้าที่ในการกำกับการบริหารจัดการความเสี่ยงด้วย สำหรับหัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูงมีหน้าที่ความรับผิดชอบในการบริหารจัดการความเสี่ยง

การกำกับการบริหารจัดการความเสี่ยง เป็นกระบวนการที่ทำให้ผู้กำกับดูแลเกิดความมั่นใจว่า หัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูงได้บริหารจัดการความเสี่ยงอย่างเหมาะสม เพียงพอ และมีประสิทธิผล

หัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูงมีหน้าที่โดยตรงในการสร้างระบบบริหารจัดการความเสี่ยงที่มีประสิทธิผล ประกอบด้วย การสร้างสภาพแวดล้อมวัฒนธรรมองค์กร และระบบการบริหารบุคคลที่เหมาะสม การจัดสรรทรัพยากรที่เพียงพอในการบริหารจัดการความเสี่ยง การดำเนินงานตามกระบวนการบริหารจัดการความเสี่ยง การพัฒนาระบบข้อมูลสารสนเทศ การรายงานและการสื่อสาร เป็นต้น

ผู้กำกับดูแล (ถ้ามี) อาจตั้งคณะกรรมการบริหารจัดการความเสี่ยง (หรืออนุกรรมการ หรือคณะที่ปรึกษา) ขึ้น ซึ่งประกอบด้วยผู้มีทักษะประสบการณ์และความเชี่ยวชาญเกี่ยวกับการดำเนินงานของหน่วยงาน เช่น หน่วยงานที่มีการใช้ระบบเทคโนโลยีสารสนเทศเป็นหลักในการดำเนินงาน อาจจำเป็นต้องมีผู้เชี่ยวชาญอิสระในการกำกับหรือให้ความเห็นเกี่ยวกับความเพียงพอและความเหมาะสมของการบริหารจัดการความเสี่ยงในเรื่องความเสี่ยงทางไซเบอร์ของหัวหน้าหน่วยงานของรัฐและผู้บริหารระดับสูง

3) การสร้างและรักษาบุคลากรและวัฒนธรรมที่ดีขององค์กร การขับเคลื่อนหน่วยงานของรัฐต้องอาศัยบุคลากรที่มีศักยภาพ การบริหารทรัพยากรบุคคลเริ่มตั้งแต่การสรรหา การพัฒนาบุคลากรให้มีความรู้ความสามารถ การส่งเสริมและรักษาไว้ซึ่งบุคลากรที่มีความรู้ความสามารถ โดยบุคลากรถือว่าเป็นสินทรัพย์หลักขององค์กรที่ทำให้องค์กรประสบความสำเร็จ การสร้างบุคลากรให้มีความรู้และทักษะในการบริหารจัดการความเสี่ยงถือเป็นส่วนหนึ่งของการบริหารจัดการความเสี่ยง บุคลากรควรมีพฤติกรรมตระหนักถึงความเสี่ยง (risk-aware behavior) รวมถึงพฤติกรรมการตัดสินใจโดยใช้ข้อมูลสารสนเทศและข้อมูลการบริหารจัดการความเสี่ยง การสร้างพฤติกรรมที่ดี (desired behaviors) ในการส่งเสริมการบริหารจัดการความเสี่ยงผ่านวัฒนธรรมที่ดีขององค์กรเป็นสิ่งสำคัญ การสร้างวัฒนธรรมที่สนับสนุนการบริหารจัดการความเสี่ยงประกอบด้วย

(1) การสื่อสารและการตระหนักถึงนโยบายการบริหารจัดการความเสี่ยงของหน่วยงาน

(2) การสร้างความตระหนักถึงหน้าที่ต่อองค์กรในการแจ้งข้อมูลผิดปกติ

(3) การสร้างพฤติกรรมการแบ่งปันข้อมูลภายในองค์กร

(4) การสร้างพฤติกรรมการตัดสินใจตามนโยบายการบริหารจัดการความเสี่ยง

(5) การสร้างพฤติกรรมการตระหนักถึงความเสี่ยงและโอกาส

4) การมอบหมายหน้าที่ความรับผิดชอบด้านการบริหารจัดการความเสี่ยง หน่วยงานควรมีการกำหนดอำนาจ หน้าที่ ความรับผิดชอบในเรื่องของการบริหารจัดการความเสี่ยงอย่างชัดเจนและเหมาะสม ประกอบด้วย เจ้าของความเสี่ยง (risk owners) ซึ่งรับผิดชอบในการติดตามการรายงาน หรือการส่งสัญญาณความเสี่ยง ผู้รับผิดชอบในการตัดสินใจในกรณีที่ความเสี่ยงเกิดขึ้นในระดับที่กำหนดไว้ และผู้ที่มีหน้าที่ในการควบคุมกำกับติดตามให้มีการบริหารจัดการความเสี่ยงตามแผนการบริหารจัดการความเสี่ยง

5) การตระหนักถึงผู้มีส่วนได้ส่วนเสีย การบริหารจัดการความเสี่ยงนอกจากจะคำนึงถึงวัตถุประสงค์ขององค์กรเป็นหลักแล้ว ผู้บริหารต้องคำนึงถึงผู้มีส่วนได้ส่วนเสียในการบริหารจัดการความเสี่ยงด้วย โดยเฉพาะความคาดหวังของผู้รับบริการหรือความคาดหวังของประชาชนที่มีต่อองค์กร รวมถึงผลกระทบที่มีต่อสังคม เศรษฐกิจ และสภาพแวดล้อม

6) การกำหนดยุทธศาสตร์/กลยุทธ์ วัตถุประสงค์ และการตัดสินใจ การบริหารจัดการความเสี่ยงเป็นเครื่องมือช่วยผู้บริหารในการกำหนดยุทธศาสตร์/กลยุทธ์ขององค์กรเพื่อให้หน่วยงานมั่นใจว่า ยุทธศาสตร์/กลยุทธ์ขององค์กรสอดคล้องกับพันธกิจตามกฎหมายและหน้าที่ความรับผิดชอบของหน่วยงาน ยุทธศาสตร์/กลยุทธ์อาจหมายรวมถึงแผนปฏิบัติราชการระยะยาว แผนปฏิบัติราชการระยะปานกลาง หรือแผนปฏิบัติราชการประจำปีของหน่วยงาน

เมื่อหน่วยงานของรัฐกำหนดยุทธศาสตร์/กลยุทธ์โดยสอดคล้องกับความเสี่ยงที่ยอมรับได้ระดับองค์กรแล้ว การบริหารจัดการความเสี่ยงจะถูกใช้เป็นเครื่องมือในการกำหนดทางเลือกของงาน/โครงการ (งานใหม่ ๆ) และการกำหนดวัตถุประสงค์ระดับ

การปฏิบัติงาน รวมถึงการมอบหมายความรับผิดชอบในการบริหารจัดการความเสี่ยงทั่วทั้งองค์กรโดยอาจกำหนดเป็นส่วนหนึ่งของตัวชี้วัดผลการปฏิบัติงาน (KPI)

7) การใช้ข้อมูลสารสนเทศ ในปัจจุบัน ข้อมูลสารสนเทศเป็นสิ่งสำคัญอย่างยิ่งในการดำเนินงานของหน่วยงาน องค์กรที่มีการบริหารจัดการข้อมูลสารสนเทศอย่างมีประสิทธิภาพจะส่งผลโดยตรงต่อการบริหารจัดการความเสี่ยง หน่วยงานควรพิจารณาใช้ข้อมูลสารสนเทศในการบริหารจัดการความเสี่ยง เพื่อให้ผู้บริหารสามารถตัดสินใจโดยใช้ข้อมูลความเสี่ยงเป็นพื้นฐาน หน่วยงานควรกำหนดประเภทข้อมูลที่ต้องรวบรวม วิธีการรวบรวมและการวิเคราะห์ข้อมูล และบุคคลที่ควรได้รับข้อมูล

ข้อมูลความเสี่ยง ประกอบด้วย เหตุการณ์ที่เป็นผลกระทบทางลบหรือทางบวกต่อองค์กร สาเหตุความเสี่ยง ตัวผลักดันความเสี่ยง หรือตัวชี้วัดความเสี่ยงที่สำคัญ (key risk indicators) ข้อมูลสารสนเทศต้องมีความถูกต้อง เชื่อถือได้ เกี่ยวข้องกับการตัดสินใจและทันต่อเวลา ทั้งนี้หน่วยงานอาจพิจารณาการรวบรวมการประมวลผล หรือการวิเคราะห์ความเสี่ยงแบบอัตโนมัติเพื่อลดข้อผิดพลาดจากบุคคล (human errors)

8) การพัฒนาอย่างต่อเนื่อง การบริหารจัดการความเสี่ยงต้องมีการพัฒนาอย่างต่อเนื่อง ความสมบูรณ์ของระบบบริหารจัดการความเสี่ยงขึ้นอยู่กับขนาดโครงสร้างศักยภาพขององค์กร รวมถึงการใช้ระบบสารสนเทศในการบริหารจัดการความเสี่ยง หน่วยงานอาจพิจารณาทำ benchmarking เพื่อพัฒนาระบบบริหารจัดการความเสี่ยงขององค์กรอย่างต่อเนื่อง หน่วยงานอาจพัฒนาระบบการบริหารจัดการความเสี่ยงโดยเริ่มต้นจากการบริหารจัดการความเสี่ยงแบบ Silo พัฒนาเป็นการบริหารจัดการความเสี่ยงแบบบูรณาการ และพัฒนาต่อเนื่องโดยมีการฝังการบริหารจัดการความเสี่ยงเข้าสู่กระบวนการการดำเนินงานโดยปกติของการดำเนินงานและการตัดสินใจบนพื้นฐานข้อมูลด้านความเสี่ยง

2.2 กระบวนการจัดการความเสี่ยง เป็นกระบวนการที่เกิดขึ้นอย่างเป็นวงจรและต่อเนื่อง (routine processes) ของการบริหารจัดการความเสี่ยง ซึ่งตั้งอยู่บนพื้นฐานของกรอบการบริหารจัดการความเสี่ยงของหน่วยงาน ประกอบไปด้วย

การวิเคราะห์องค์กร

ในการวิเคราะห์องค์กร หน่วยงานต้องเข้าใจเกี่ยวกับพันธกิจตามกฎหมาย อำนาจหน้าที่ และความรับผิดชอบของหน่วยงาน รวมถึงยุทธศาสตร์ชาติ ยุทธศาสตร์ระดับกระทรวง และนโยบายของรัฐบาลที่เกี่ยวข้องกับหน่วยงาน โดยการวิเคราะห์องค์กรต้องวิเคราะห์ทั้งปัจจัยภายในและปัจจัยภายนอกองค์กร หน่วยงานอาจเลือกใช้เครื่องมือการวิเคราะห์องค์กร เช่น

1. SWOT Analysis เป็นการวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรค
2. PESTLE Analysis เป็นการวิเคราะห์ด้านการเมือง (Political) ด้านเศรษฐกิจ (Economic) ด้านสังคม (Social) ด้านเทคโนโลยี (Technological) ด้านกฎหมาย (Legal) และด้านสภาพแวดล้อม (Environmental)

การกำหนดนโยบายการบริหารจัดการความเสี่ยง

ผู้บริหารเป็นผู้กำหนดนโยบายบริหารจัดการความเสี่ยง และผู้กำกับดูแลเป็นผู้ให้ความเห็นชอบนโยบายดังกล่าว โดยนโยบายการบริหารจัดการความเสี่ยงอาจระบุถึงวัตถุประสงค์ของการบริหารจัดการความเสี่ยง บทบาทหน้าที่ความรับผิดชอบของการบริหารจัดการความเสี่ยง และความเสี่ยงที่ยอมรับได้ระดับองค์กร

ความเสี่ยงที่ยอมรับได้ระดับองค์กร (risk appetite) หมายถึง ระดับความเสี่ยงในภาพรวมขององค์กรที่หน่วยงานยอมรับเพื่อดำเนินงานให้บรรลุวัตถุประสงค์ขององค์กร การระบุความเสี่ยงที่ยอมรับได้ระดับองค์กรเป็นการแสดงเจตนารมณ์ของผู้บริหารและผู้กำกับดูแลในการดำเนินงานขององค์กร การกำหนดความเสี่ยงที่ยอมรับได้ควรคำนึงถึงศักยภาพขององค์กรในเรื่องการจัดการความเสี่ยง โดยศักยภาพในการจัดการความเสี่ยงขององค์กร (risk capacity) ขึ้นอยู่กับงบประมาณ บุคลากร และความคาดหวังของผู้มีส่วนได้ส่วนเสีย ทั้งนี้หน่วยงานอาจระบุระดับความเสี่ยงที่ยอมรับได้เป็น 5 ระดับ เช่น ปฏิเสธความเสี่ยง ยอมรับความเสี่ยงได้น้อย ยอมรับความเสี่ยงได้ปานกลาง เต็มใจยอมรับความเสี่ยง และยอมรับความเสี่ยงได้มากที่สุด

หน่วยงานอาจแสดงนโยบายความเสี่ยงที่ยอมรับได้ในแต่ละประเภทความเสี่ยงเพื่อให้ผู้บริหารระดับรองลงมาสามารถนำไปใช้ในการบริหารจัดการความเสี่ยงในระดับสำนัก กอง ศูนย์ กลุ่ม หรือนำไปสู่การระบุระดับความเสี่ยงที่ยอมรับได้สำหรับประเภทความเสี่ยงย่อย

การระบุความเสี่ยง

การระบุความเสี่ยง คือ การระบุเหตุการณ์ที่อาจเกิดขึ้นที่มีผลกระทบต่อวัตถุประสงค์ของหน่วยงานทั้งในด้านบวกและด้านลบ ในการระบุความเสี่ยง หน่วยงานอาจทำรายชื่อความเสี่ยงทั้งหมด (risk inventory) รายชื่อความเสี่ยงต้องมีการปรับปรุงอย่างสม่ำเสมอโดยอาศัยข้อมูลที่เป็นปัจจุบัน การระบุความเสี่ยง หน่วยงานควรระบุข้อมูลเกี่ยวกับความเสี่ยงดังนี้

1. เหตุการณ์ความเสี่ยง

2. สาเหตุของความเสี่ยง หรือตัวผลักดันความเสี่ยง โดยการวิเคราะห์ถึงสาเหตุที่แท้จริง (root cause) ของความเสี่ยง

3. ผลกระทบทั้งด้านลบและ/หรือด้านบวก

หน่วยงานอาจจัดกลุ่มความเสี่ยงที่มีลักษณะหรือมีผลกระทบที่เหมือนกันไว้ในประเภทความเสี่ยงเดียวกัน เพื่อให้การพิจารณาและการบริหารจัดการความเสี่ยงประเภทเดียวกันมีมุมมองในภาพรวมชัดเจนมาก

การประเมินความเสี่ยง ประกอบด้วย

1. การกำหนดเกณฑ์การประเมินความเสี่ยง หน่วยงานอาจให้คะแนนความเสี่ยงตามเกณฑ์การประเมินความเสี่ยงด้านต่าง ๆ เช่น ด้านโอกาส ด้านผลกระทบ รวมถึงด้านความสามารถขององค์กรในการจัดการความเสี่ยง และด้านลักษณะของความเสี่ยง โดยช่วงคะแนนอาจกำหนดเป็น 3 ช่วงคะแนน หรือ 5 ช่วงคะแนน

2. การให้คะแนนความเสี่ยง วิธีการให้คะแนนความเสี่ยง เช่น การสัมภาษณ์ การทำแบบสำรวจ การประชุมเชิงปฏิบัติการระหว่างหน่วยงานภายใน การทำ benchmarking การวิเคราะห์สถานการณ์ (scenario analysis) ทั้งนี้การให้คะแนนความเสี่ยงของแต่ละกองงาน (Silo thinking) เพียงวิธีเดียวอาจทำให้การให้คะแนนความเสี่ยงมีความคลาดเคลื่อนได้

3. การพิจารณาความเสี่ยงในภาพรวม เมื่อหน่วยงานประเมินความเสี่ยงในแต่ละความเสี่ยงที่มีต่อวัตถุประสงค์ของกิจกรรมแล้ว หน่วยงานต้องพิจารณาผลกระทบของความเสี่ยงที่มีต่อวัตถุประสงค์ในระดับกลุ่มและผลกระทบที่มีต่อหน่วยงานในภาพรวม เช่น ผลกระทบต่อความเสี่ยงที่มีต่อกิจกรรมอาจมีน้อย แต่มีผลกระทบต่อวัตถุประสงค์ระดับกอง หรือความเสี่ยงสองความเสี่ยงที่ไม่มีผลกระทบต่อกิจกรรม อาจมีผลกระทบต่อหน่วยงานในภาพรวม

4. การจัดลำดับความเสี่ยง เมื่อหน่วยงานพิจารณาให้คะแนนความเสี่ยงแล้ว หน่วยงานต้องจัดลำดับความเสี่ยง เพื่อนำไปสู่การพิจารณาจัดสรรทรัพยากรในการตอบสนองความเสี่ยง หน่วยงานอาจใช้คะแนนความเสี่ยง (โอกาส x ผลกระทบ) ในการจัดลำดับความเสี่ยง โดยความเสี่ยงที่เท่ากันอาจพิจารณาปัจจัยอื่นประกอบ เช่น ความสามารถของหน่วยงานในการบริหารจัดการความเสี่ยงด้านนั้น ๆ หรือลักษณะของความเสี่ยงที่มีผลกระทบต่อหน่วยงาน

การตอบสนองความเสี่ยง

การตอบสนองความเสี่ยง คือ กระบวนการตัดสินใจของฝ่ายบริหารในการจัดการความเสี่ยงที่อาจจะเกิดขึ้น โดยผู้บริหารควรพิจารณาประเด็นดังต่อไปนี้ในการตัดสินใจเลือกวิธีการตอบสนองความเสี่ยงเพื่อจัดทำแผนบริหารจัดการความเสี่ยงของหน่วยงาน

1. การจัดการต้นเหตุของความเสี่ยง
2. ทางเลือกวิธีการจัดการความเสี่ยง
3. ทรัพยากรที่ต้องใช้ในการบริหารจัดการความเสี่ยง

หน่วยงานสามารถพิจารณาเลือกวิธีการจัดการความเสี่ยงวิธีที่ใดวิธีหนึ่งหรือหลายวิธี โดยการพิจารณาวิธีการจัดการความเสี่ยงควรคำนึงถึงต้นทุนกับประโยชน์ที่ได้รับของวิธีการจัดการความเสี่ยงแต่ละวิธี

ตัวอย่างวิธีการจัดการความเสี่ยง ประกอบด้วย

1. ปฏิเสธความเสี่ยงโดยไม่ดำเนินงานในกิจกรรมที่มีความเสี่ยง ได้แก่ กิจกรรมที่มีความเสี่ยงสูงและหน่วยงานไม่สามารถยอมรับความเสี่ยงนั้นได้ หน่วยงานอาจพิจารณาไม่ดำเนินงานในกิจกรรมนั้น ๆ

2. การลดโอกาสของความเสี่ยง เช่น การลดโอกาสของความเสี่ยงการทุจริตด้านการเงิน โดยการวางระบบการควบคุมภายใน ได้แก่ การแบ่งแยกหน้าที่ การตรวจสอบการสอบทาน และการกระทบยอด

3. การลดผลกระทบของความเสี่ยง เช่น การทำประกัน หรือการใช้เครื่องมือป้องกันความเสี่ยงทางการเงิน (hedging instruments)

4. การโอนความเสี่ยง หน่วยงานอาจเลือกใช้วิธีการถ่ายโอนความเสี่ยงของกิจกรรมที่หน่วยงานเห็นว่าควรดำเนินการเพื่อประโยชน์ของประชาชน แต่หน่วยงานมีข้อจำกัดที่ไม่สามารถดำเนินการเองได้ หรือไม่สามารถบริหารจัดการความเสี่ยงได้ เช่น

การให้ภาคเอกชนดำเนินการโดยมีการโอนความเสี่ยงและผลตอบแทนไปด้วย (Public Private Partnership: PPP)

5. ยอมรับความเสี่ยงโดยไม่ดำเนินการจัดการความเสี่ยง เนื่องจากความเสี่ยงอยู่ในระดับที่หน่วยงานยอมรับได้ หรือต้นทุนในการบริหารจัดการความเสี่ยงมีมากกว่าประโยชน์ที่ได้รับ

6. ใช้มาตรการการเฝ้าระวัง หน่วยงานต้องกำหนดข้อมูลที่ต้องมีการเก็บรวบรวมการวิเคราะห์การแจ้งเตือน และการดำเนินการเมื่อเหตุการณ์เกิดขึ้น เช่น ความเสี่ยงของปริมาณน้ำในเขื่อนมากเนื่องจากปริมาณน้ำฝน

7. การทำแผนฉุกเฉิน การจัดทำแผนฉุกเฉินเป็นการระบุขั้นตอนเมื่อเกิดเหตุการณ์ความเสี่ยงขึ้นโดยต้องระบุบุคคลและวิธีการดำเนินการที่ชัดเจน เช่น ความเสี่ยงกรณีที่เจ้าหน้าที่ไม่สามารถเข้าสถานที่ทำงานได้

8. การส่งเสริมหรือผลักดันเหตุการณ์ที่อาจจะเกิดขึ้น เมื่อเหตุการณ์ที่อาจจะเกิดขึ้นส่งผลกระทบเชิงบวกกับองค์กร รวมถึงกำหนดแผนการดำเนินงานเมื่อเหตุการณ์เกิดขึ้น

แผนการบริหารจัดการความเสี่ยงอาจประกอบด้วย วิธีการจัดการความเสี่ยง บุคคลที่รับผิดชอบในการบริหารจัดการความเสี่ยง ตัวชี้วัดความเสี่ยงที่สำคัญ วิธีการติดตามและการรายงานความเสี่ยง

การติดตามและทบทวน

การติดตามและทบทวนเป็นกระบวนการที่ให้ความเชื่อมั่นว่า การบริหารจัดการความเสี่ยงที่มีอยู่ยังคงมีประสิทธิผล เนื่องจากความเสี่ยงเป็นสิ่งที่เกิดขึ้นและเปลี่ยนแปลงตลอดเวลา ดังนั้น การติดตามและทบทวนเป็นกระบวนการที่เกิดขึ้นสม่ำเสมอ ปัจจัยที่ทำให้หน่วยงานต้องทบทวนการบริหารจัดการความเสี่ยง ได้แก่ การเปลี่ยนแปลงที่สำคัญซึ่งเกิดจากปัจจัยภายในและภายนอก หรือผลการดำเนินงานไม่เป็นไปตามเป้าหมายที่กำหนดไว้

การติดตามและทบทวนการบริหารจัดการความเสี่ยงสามารถดำเนินการอย่างต่อเนื่องหรือเป็นระยะ ซึ่งควรดำเนินการในทุกกระบวนการของการบริหารจัดการความเสี่ยง การติดตามและทบทวนอาจนำไปสู่การเปลี่ยนแปลงของแผนการปฏิบัติงานขององค์กร การเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ รวมถึงการพัฒนาระบบบริหารจัดการความเสี่ยง

การสื่อสารและการรายงาน

การสื่อสารเป็นการสร้างความตระหนัก ความเข้าใจ และการมีส่วนร่วมของกระบวนการบริหารจัดการความเสี่ยง การสื่อสารเป็นการให้และรับข้อมูล (two-way communication) หน่วยงานควรมีช่องทางการสื่อสารทั้งภายในและภายนอก โดยการสื่อสารภายในต้องเป็นการสื่อสารจากผู้บริหารไปยังผู้ใต้บังคับบัญชา (top down) จากผู้ใต้บังคับบัญชาไปยังผู้บริหาร (bottom up) และระหว่างหน่วยงานย่อยภายใน (across divisions)

หน่วยงานควรกำหนดบุคคลที่ควรได้รับข้อมูล ประเภทของข้อมูลที่ควรได้รับ ความถี่ของการรายงาน รูปแบบและวิธีการรายงาน เพื่อให้ผู้กำกับดูแล ผู้บริหาร และผู้มีส่วนได้ส่วนเสียได้รับข้อมูลสารสนเทศที่ถูกต้อง ครบถ้วน เกี่ยวข้องกับการตัดสินใจ และทันต่อเวลา

การสื่อสารและรายงานต่อผู้กำกับดูแล เป็นการสื่อสารและการรายงานความเสี่ยงในภาพรวมขององค์กร เพื่อสนับสนุนหน้าที่ของผู้กำกับดูแลในการกำกับการบริหารจัดการความเสี่ยงของฝ่ายบริหาร

หน่วยงานอาจพิจารณากำหนดตัวชี้วัดความเสี่ยงที่สำคัญ (key risk indicator) เพื่อติดตามข้อมูลความเสี่ยงและการรายงานเมื่อระดับความเสี่ยงถึงจุดตัวชี้วัดความเสี่ยงที่สำคัญ

ดังนั้น จากแนวคิดพื้นฐานของการบริหารความเสี่ยงในอุดมศึกษาทั้งในระดับสากลและในระดับประเทศ จะเห็นได้ว่า การบริหารความเสี่ยง (risk management) เป็นสิ่งสำคัญต่อการขับเคลื่อนองค์กรให้ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมาย ท่ามกลางวิวัฒนาการทางเศรษฐกิจ สังคม เทคโนโลยี นโยบาย กฎระเบียบใหม่ สิ่งแวดล้อม และพัฒนาการส่งมอบคุณค่าให้แก่ผู้มีส่วนได้ส่วนเสีย ที่ส่งผลให้องค์กรต่าง ๆ ไม่เฉพาะสถาบันอุดมศึกษาเท่านั้นที่ต้องปรับตัว แต่ยังมีความจำเป็นต้องนำหลักการและกระบวนการบริหารความเสี่ยงมาใช้เพื่อสร้างโอกาสใหม่ที่ท้าทาย ปรับปรุงกระบวนการที่เป็นจุดอ่อน พร้อมกับเตรียมพร้อมรับมือกับภัยที่อาจจะเกิดขึ้นได้ทุกเมื่อ โดยในส่วนที่ 2 จะกล่าวถึงระบบบริหารความเสี่ยงของสถาบันอุดมศึกษาทั่วโลก เพื่อฉายภาพให้เห็นว่า มหาวิทยาลัยต่าง ๆ ทั่วโลกนั้นให้ความสำคัญกับการวางระบบบริหารความเสี่ยงและใช้การบริหารความเสี่ยงเป็นเครื่องมือเชิงกลยุทธ์สำคัญที่นำพาองค์กรให้บรรลุเป้าหมาย

ส่วนที่ 2

ระบบบริหารความเสี่ยงของอุดมศึกษาในต่างประเทศ

(Risk Management System in Global Higher Education)

ในส่วนที่ 2 นี้ จะกล่าวถึงภาพรวมของระบบการบริหารความเสี่ยงในมหาวิทยาลัยต่าง ๆ ในต่างประเทศที่ได้พัฒนาระบบการบริหารความเสี่ยงขึ้นซึ่งปฏิบัติตามกรอบการบริหารความเสี่ยงสากลที่ได้กล่าวถึงไว้ในส่วนที่ 1 ตั้งแต่นโยบายการจัดการความเสี่ยง กรอบการทำงาน และกระบวนการในการจัดการความเสี่ยงที่มหาวิทยาลัยแต่ละแห่งนำไปปฏิบัติ เช่น การระบุความเสี่ยง การวิเคราะห์ การประเมิน และการตรวจสอบความเสี่ยง มุ่งเน้นไปที่การปรับปรุงกระบวนการตัดสินใจและการรับผิดชอบในการจัดการเพื่อยกระดับคุณภาพและผลลัพธ์ของการดำเนินงานในมหาวิทยาลัยให้สามารถบรรลุวัตถุประสงค์และเป้าหมาย โดยมีรายละเอียดดังต่อไปนี้

2.1 International Islamic University Malaysia: IIUM – ประเทศมาเลเซีย

2.1.1 วัตถุประสงค์การบริหารความเสี่ยง (risk management objectives)

การบริหารความเสี่ยงของมหาวิทยาลัยอิสลามนานาชาติมาเลเซีย ถือเป็นส่วนสำคัญของแนวทางการจัดการที่ดีที่สุดและเป็นองค์ประกอบที่สำคัญของการกำกับดูแลกิจการที่ดี เนื่องจากช่วยปรับปรุงการตัดสินใจและยกระดับผลลัพธ์และความรับผิดชอบ จุดประสงค์คือ การฝังการจัดการความเสี่ยงลงในกระบวนการทางธุรกิจและการทำงานผ่านกระบวนการอนุมัติ ที่สำคัญคือทบทวนกระบวนการและการควบคุม ไม่ได้กำหนดให้การบริหารความเสี่ยงเป็นข้อกำหนดเพิ่มเติม มหาวิทยาลัยอิสลามนานาชาติมาเลเซียได้นำเอาการจัดการความเสี่ยงตามมาตรฐาน **“ISO 31000:2009 — หลักการและแนวทางปฏิบัติ”** มาใช้ในการบริหารความเสี่ยง ซึ่งมาตรฐานสากลนี้สามารถนำไปใช้ได้ทั่วทั้ง IIUM และกับกิจกรรมที่หลากหลายรวมถึงการออกแบบกลยุทธ์การตัดสินใจ การดำเนินงาน กระบวนการ หน้าที่ โครงการ ผลิตภัณฑ์ บริการ และสินทรัพย์

โดยวัตถุประสงค์ของการบริหารความเสี่ยงของ IIUM มีดังต่อไปนี้

1. ปกป้องมหาวิทยาลัยจากความเสี่ยงและผลที่ตามมาอย่างมีนัยสำคัญในการแสวงหาเป้าหมายและวัตถุประสงค์เชิงกลยุทธ์ที่มหาวิทยาลัยระบุไว้

2. จัดให้มีกรอบการบริหารความเสี่ยงที่สอดคล้องกัน โดยจะระบุ พิจารณา และจัดการความเสี่ยงที่เกี่ยวข้องกับกระบวนการในสำนักงานและหน้าที่ของมหาวิทยาลัยในกระบวนการอนุมัติ ทบทวน และควบคุมที่สำคัญ

3. ส่งเสริมการจัดการแบบ proactive มากกว่าการจัดการแบบ reactive

4. ให้ความช่วยเหลือและปรับปรุงคุณภาพของการตัดสินใจทั่วทั้งมหาวิทยาลัย

5. ปฏิบัติตามข้อกำหนดทางกฎหมาย

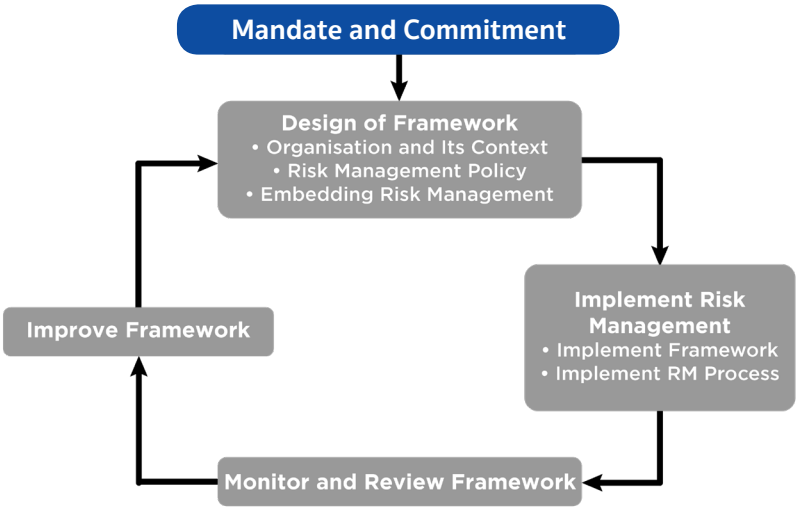
6. ช่วยเหลือในการปกป้องทรัพย์สินของมหาวิทยาลัย รวมถึงบุคลากร การเงิน ทรัพย์สิน ข้อมูล และชื่อเสียง

นโยบายนี้เสริมหลักจรรยาบรรณของมหาวิทยาลัย 2011 (CUGG) หลักธรรมาภิบาลของมาเลเซียปี 2555 (MCGG) แผนปฏิบัติการเพื่อการดำเนินการตามแผนคุณธรรมแห่งชาติ (NIP) ของการอุดมศึกษา 2010-2015 และนโยบายที่เกี่ยวข้องใด ๆ ในความมุ่งมั่นสู่วัตถุประสงค์สำคัญหลายประการที่กำหนดให้สำนักงานยุทธศาสตร์องค์กรเป็นแหล่งความรู้สำหรับการจัดการและลดความเสี่ยงในการดำเนินงานของ IIUM และเป็นผู้นำในอุตสาหกรรม

2.1.2 กรอบการบริหารความเสี่ยง (risk management framework)

จากรูปที่ 9 แสดงความสัมพันธ์ระหว่างองค์ประกอบของกรอบงานสำหรับการจัดการความเสี่ยงของมาตรฐาน ISO 31000:2009 รวมถึงขั้นตอนสำคัญในการดำเนินการและการสนับสนุนอย่างต่อเนื่องของกระบวนการบริหารความเสี่ยง องค์ประกอบของกรอบการบริหารความเสี่ยงนี้ คือ

1. อาณัติและความมุ่งมั่น (mandate and commitment)
2. การออกแบบกรอบการบริหารความเสี่ยง (design of framework)
3. การดำเนินการบริหารความเสี่ยง (implement risk)
4. การตรวจสอบและทบทวนกรอบงาน (monitor and review framework)
5. การปรับปรุงกรอบงานอย่างต่อเนื่อง (improve framework)



รูปที่ 9 ความสัมพันธ์ระหว่างองค์ประกอบของกรอบงาน (Framework) สำหรับการจัดการความเสี่ยง

องค์ประกอบของการจัดการประกอบไปด้วย

1. กำหนดและรับรองนโยบายการบริหารความเสี่ยง
2. ตรวจสอบให้แน่ใจว่าวัฒนธรรมและนโยบายการบริหารความเสี่ยงมีความสอดคล้องกัน
3. จัดวัตถุประสงค์การบริหารความเสี่ยงให้สอดคล้องกับวัตถุประสงค์และกลยุทธ์ของมหาวิทยาลัย
4. กำหนดตัวบ่งชี้ประสิทธิภาพการบริหารความเสี่ยงที่สอดคล้องกับตัวบ่งชี้ประสิทธิภาพของมหาวิทยาลัย
5. รับรองการปฏิบัติตามกฎหมายและระเบียบข้อบังคับ
6. กำหนดความรับผิดชอบ (accountability) และหน้าที่ (responsibility) ในระดับที่เหมาะสม
7. ตรวจสอบให้แน่ใจว่ามีการจัดสรรทรัพยากรที่จำเป็นให้กับการบริหารความเสี่ยง
8. สื่อสารประโยชน์ของการบริหารความเสี่ยงให้กับผู้มีส่วนได้ส่วนเสียทั้งหมด
9. ตรวจสอบให้แน่ใจว่ากรอบการบริหารความเสี่ยงยังคงมีความเหมาะสมอยู่

กรอบการบริหารความเสี่ยงของ IIUM ประกอบด้วยขั้นตอนสำคัญ 3 ขั้นตอน ได้แก่

1. กำหนดกลยุทธ์องค์กรเป็นประจำทุกปี จัดการบริหารความเสี่ยงให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ

2. การนำระเบียบวิธีกระบวนการที่เป็นทางการและเป็นมาตรฐานมาใช้ในการบริหารความเสี่ยงทั่วทั้งธุรกิจ

3. การรักษาโครงสร้างที่กำหนดความเป็นเจ้าของและความรับผิดชอบในการติดตามและปรับปรุงการบริหารความเสี่ยง

ควรใช้กรอบการบริหารความเสี่ยง โดยมีวัตถุประสงค์เพื่อ

1. สื่อสารนโยบายและขั้นตอนการจัดการความเสี่ยงในระดับองค์กร

2. จัดทำแนวทางความรับผิดชอบและหน้าที่ในการบริหารความเสี่ยง

3. สร้างความเข้าใจในกระบวนการที่ดำเนินการซึ่งเอื้อต่อความสำเร็จของการดำเนินการบริหารความเสี่ยงจากมุมมองในวงกว้างของมหาวิทยาลัย

4. แสดงให้เห็นว่าความเสี่ยงเกี่ยวข้องกับการบรรลุวัตถุประสงค์ขององค์กรอย่างไร

5. เน้นความสำคัญของการบริหารความเสี่ยงที่มีต่อวิสัยทัศน์และพันธกิจของ IIUM ตลอดจนทิศทางเชิงกลยุทธ์ของ IIUM ในการเป็น Premier Global Islamic Research University

2.1.3 บทบาทและความรับผิดชอบในการบริหารความเสี่ยง (roles & responsibilities)

มหาวิทยาลัยอิสลามนานาชาติมาเลเซียมีบุคคล กลุ่มบุคคล หรือหน่วยงานที่เกี่ยวข้องในการบริหารความเสี่ยงตามกรอบการบริหารความเสี่ยงให้เป็นระบบและมีประสิทธิผลดังต่อไปนี้

1. คณะกรรมการบริหาร (Board of Governors: BOG) คือ ผู้มีอำนาจสูงสุดในการจัดการและกำหนดนโยบายของมหาวิทยาลัย มีหน้าที่รับรองนโยบายการบริหารความเสี่ยงของ IIUM และกำกับดูแลการดำเนินการบริหารความเสี่ยงภายในมหาวิทยาลัยตามคำแนะนำของคณะกรรมการบริหารความเสี่ยงของ IIUM หรือคณะกรรมการที่ได้รับมอบหมาย

2. หัวหน้าส่วนงาน/หน่วยงานในมหาวิทยาลัย บทบาทของคณะกรรมการบริหารมหาวิทยาลัยและหัวหน้าศูนย์การศึกษา หน่วยงาน และสำนักงานต่าง ๆ รวมอยู่ในคำแถลงนโยบาย เนื่องจากพวกเขามีความรับผิดชอบและรับผิดชอบต่อความเสี่ยงทั้งหมดที่มีอยู่ในโดเมนของตน จึงเป็นสิ่งสำคัญที่ผู้จัดการสายงานทุกคนต้องสนับสนุนผู้บังคับบัญชาของตนให้เหนือกว่าเพื่อให้มั่นใจว่าแนวทางที่อิงตามความเสี่ยงได้รับการปรับใช้และฝังอยู่ในกระบวนการทางธุรกิจทั้งหมดอย่างสมบูรณ์

3. คณะกรรมการตรวจสอบและความเสี่ยงของ IIUM มีหน้าที่

1) จัดตั้งคณะกรรมการบริหารความเสี่ยง IIUM ที่ได้รับมอบหมาย (ระดับคณะกรรมการ) หรือคณะกรรมการเทียบเท่าใด ๆ รวมถึงการแต่งตั้งประธานและสมาชิกของคณะกรรมการดังกล่าวจะต้องได้รับอนุมัติจาก BOG ในเรื่องคำแนะนำของคณะกรรมการบริหาร IIUM-University

2) ความรับผิดชอบอื่น ๆ ในเรื่องของการ

(1) สรุปการดำเนินการตามกรอบการบริหารความเสี่ยงของ IIUM และความคืบหน้าในการบรรเทาผลกระทบ

(2) ทบทวนกรอบการบริหารความเสี่ยงและประเมินประสิทธิผลของแผนบริหารความเสี่ยง

(3) เพื่อให้แน่ใจว่ากระบวนการบริหารความเสี่ยงถูกฝังอยู่ในการตัดสินใจทางธุรกิจ

(4) เพื่อทบทวนความเสี่ยงที่รุนแรง มีนัยสำคัญที่ระบุโดยฝ่ายบริหารและเพื่อให้แน่ใจว่ามีการดำเนินแผนการบรรเทาผลกระทบ

(5) เพื่อแนะนำกลยุทธ์เพื่อควบคุม **“ความเสี่ยงด้านลบ”** ที่สำคัญและใช้ประโยชน์จาก **“โอกาสความเสี่ยงด้านบวก”**

(6) เพื่อรับ อภิปราย และทบทวนรายงานการบริหารความเสี่ยงของกลุ่ม

(7) เพื่อแนะนำการปรับปรุงวิธีการดำเนินการ IIUM Risk Management เมื่อจำเป็น

4. สำนักงานยุทธศาสตร์องค์กร (Office of Corporate Strategy) มีหน้าที่

1) กำหนด เสนอแนะ และจัดการแนวทางปฏิบัติ โปรแกรมการบริหารความเสี่ยงของ IIUM ที่ดีที่สุดสำหรับมหาวิทยาลัย โดยมีวัตถุประสงค์เพื่อจัดการและลดผลกระทบของการสูญเสียต่อฐานะการเงินของมหาวิทยาลัยและปกป้องชื่อเสียงของมหาวิทยาลัย

2) เพื่อประสานกิจกรรมการทำงานต่าง ๆ และให้คำแนะนำเกี่ยวกับปัญหาการบริหารความเสี่ยงภายในมหาวิทยาลัย

3) เพื่อให้มั่นใจว่าความเสี่ยงหลักทั้งหมดได้รับการระบุและมีระบบการควบคุมภายในที่จำเป็นเพื่อจัดการและควบคุมความเสี่ยงตามหลักจรรยาบรรณของมหาวิทยาลัย 2011 (CUGG) ประมวลกฎหมายมาเลเซีย

4) เพื่อให้แน่ใจว่าดำเนินการตามนโยบายและกลยุทธ์ในการบริหารความเสี่ยงของมหาวิทยาลัย

5) เพื่อเป็นผู้ประสานงานหลักของการบริหารความเสี่ยงในระดับกลยุทธ์และปฏิบัติการ

5. คณะกรรมการเทคนิคการบริหารความเสี่ยงของ IIUM (IIUM Risk Management Technical Committee) ทำหน้าที่เป็นกลุ่ม **“think tank”** ซึ่งจะมีผู้อำนวยการฝ่ายกลยุทธ์องค์กรเป็นประธาน สมาชิกจะถูกกำหนดโดยประธานเพื่ออำนวยความสะดวกในกระบวนการดำเนินการตามโปรแกรมการบริหารความเสี่ยงของมหาวิทยาลัย สมาชิกอาจเป็นตัวแทนจากสำนักงานที่สามารถให้การกำกับดูแลความเสี่ยงและทำงานเป็นส่วนสำคัญของโครงสร้างความเสี่ยงแบบบูรณาการเพื่อช่วยในการระบุความเสี่ยง การวิเคราะห์ การจัดการควบคุม และการรายงาน และยังช่วยกระบวนการประสานงานการจัดสรรทรัพยากรที่จำเป็นสำหรับการนำกลยุทธ์และโปรแกรมความเสี่ยงไปปฏิบัติ รวมถึงให้คำแนะนำในการปรับปรุงพัฒนาแก่คณะกรรมการบริหารความเสี่ยง IIUM

6. หัวหน้าศูนย์การศึกษา/แผนก/สำนักงาน/หน่วยธุรกิจเชิงกลยุทธ์ (COS/D&O/SBU) โดยบทบาทจะต้องจัดตั้งขึ้นหรือเป็นส่วนหนึ่งของการแต่งตั้งการบริหารที่เทียบเท่าที่ COS/D&O/SBU และจะเป็นประธาน โดยหัวหน้า COS/D&O/SBU สมาชิกจะถูกกำหนดโดยหัวหน้าภายใน COS/D&O/SBU ซึ่งมีบทบาทหน้าที่ดังนี้

1) เพื่อทบทวนการลงทะเบียนความเสี่ยงของแผนกและให้แน่ใจว่ามีการดำเนินการบรรเทาผลกระทบและแผนปฏิบัติการที่เหมาะสม เพื่อให้แน่ใจว่ากระบวนการจัดการความเสี่ยงฝังอยู่ในกระบวนการตัดสินใจทางธุรกิจ

2) เพื่อส่งเสริมและแนะนำการมีส่วนร่วมของเจ้าหน้าที่แผนกในการฝึกอบรมการจัดการความเสี่ยง IIUM และโปรแกรมการรับรู้

3) เพื่อทบทวนความเสี่ยงทั้งหมดที่ระบุโดยฝ่ายบริหาร และมีแผนในการบรรเทาผลกระทบ

4) เพื่อแนะนำการปรับปรุงวิธีการดำเนินการ IIUM Risk Management เมื่อจำเป็น

5) เพื่อส่งเสริมความตระหนักในความเสี่ยงในการดำเนินงานโดยแนะนำวัตถุประสงค์การบริหารความเสี่ยงในองค์กรและการปฏิบัติการ

6) เพื่อรวมการบริหารความเสี่ยงในขั้นตอนแนวคิดของโครงการและกิจกรรมตลอดการดำเนินโครงการและกิจกรรม

7) เพื่อระบุบุคคลที่จะได้รับแต่งตั้งให้เป็นผู้ประสานงานความเสี่ยงซึ่งมีหน้าที่รับผิดชอบในการประสานงานนโยบายและกลยุทธ์การบริหารความเสี่ยงสำหรับ COS/D&O/SBU กำหนดไว้อย่างชัดเจนและเป็นส่วนหนึ่งของตัวชี้วัดประสิทธิภาพหลัก (KPI)

7. ผู้ประสานงานความเสี่ยงที่ COS/D&O/SBU มีหน้าที่ในการช่วยหัวหน้าของ COS/D&O/SBU ในการจัดการและบริหารพอร์ตความเสี่ยงขององค์กร และการจัดการจัดระเบียบ และประสานงานช่วงทบทวนการบริหารความเสี่ยงองค์กรเป็นระยะภายใน COS/D&O/SBU นอกจากนี้ผู้ประสานงานความเสี่ยงยังมีหน้าที่ ได้แก่

1) ติดตามและตรวจสอบแผนปฏิบัติการผ่านการประชุม หรือหารือกับเจ้าภาพความเสี่ยงแต่ละราย หรือเจ้าของกระบวนการภายใน COS/D&O/SBU หรือร่วมกับผู้ประสานงานความเสี่ยง COS/D&O/SBU ในการจัดการความเสี่ยงข้ามสายงาน

2) รับผิดชอบในการปรับปรุงข้อมูลความเสี่ยงในระบบการจัดการข้อมูลความเสี่ยง (RiMS) ในเวลาที่เหมาะสม

3) ระบุความต้องการการฝึกอบรมของ COS/D&O/SBU ที่เกี่ยวข้องกับการบริหารความเสี่ยง

4) จัดทำรายงานการจัดการการบริโภคตามความจำเป็น

5) ติดต่อประสานงานกับสำนักงานกลยุทธ์องค์กรในเรื่องที่เกี่ยวข้องกับการบริหารความเสี่ยงและการบริหารความเสี่ยงองค์กร

8. เจ้าภาพความเสี่ยง (Risk Owners) คือ บุคคลหรือนิติบุคคลที่ได้รับมอบอำนาจให้จัดการความเสี่ยงโดยเฉพาะและมีหน้าที่รับผิดชอบในการทำเช่นนั้น บทบาทของเจ้าของความเสี่ยง ได้แก่

1) เพื่อกำหนดความเสี่ยงที่ต้องการการบรรเทาและแผนฉุกเฉิน

2) เพื่อสร้างกลยุทธ์การลดความเสี่ยงและเหตุการณ์ฉุกเฉิน และทำการวิเคราะห์ต้นทุนผลประโยชน์ของกลยุทธ์ที่เสนอ

3) เพื่อทำให้กระบวนการบรรเทาผลกระทบเป็นจริง โดยการจัดสรรทรัพยากรหรืองบประมาณที่เพียงพอ

4) เพื่อติดตาม ควบคุม และปรับปรุงสถานะของความเสี่ยงตลอดวงจรชีวิตโครงการซึ่งเจ้าของความเสี่ยงอาจเป็นสมาชิกของทีมงานโครงการ

9 สำนักงานตรวจสอบภายใน (Internal Audit) มีหน้าที่ดังนี้

1) มุ่งเน้นงานตรวจสอบภายในเกี่ยวกับความเสี่ยงที่รุนแรง สูง และมีนัยสำคัญตามที่ผู้บริหารระบุ และการตรวจสอบกระบวนการบริหารความเสี่ยงทั่วทั้งมหาวิทยาลัย

2) ให้ความเชื่อมั่นในการบริหารความเสี่ยง

3) ให้การสนับสนุนอย่างแข็งขันและมีส่วนร่วมในกระบวนการบริหารความเสี่ยง

4) ดำเนินการตรวจสอบหลังการดำเนินการของการบริหารความเสี่ยงของมหาวิทยาลัย

10. พนักงานในมหาวิทยาลัย (University Staff) พนักงานของ IIUM ทุกคนมีหน้าที่เกี่ยวกับการบริหารความเสี่ยงดังนี้

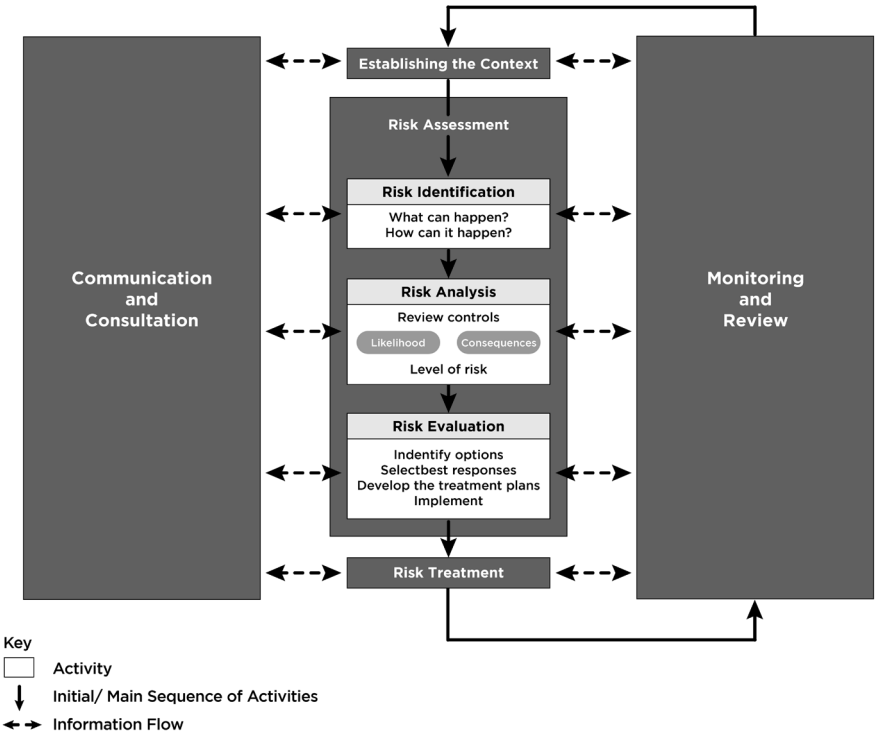
1) แจ้งฝ่ายบริหารในขอบเขตการปฏิบัติงานของตนเองบนพื้นฐานความเสี่ยงใหม่และที่เกิดขึ้นอย่างต่อเนื่อง

2) แจ้งฝ่ายบริหารทันทีเมื่อทราบถึงผู้ใดก็ตามที่ดำเนินกิจกรรมหรือการกระทำที่ไม่เหมาะสมที่อาจก่อให้เกิดความสูญเสีย ซึ่งอาจเป็นอันตรายต่อความสำเร็จของเป้าหมายและวัตถุประสงค์ของ IIUMs

3) สนับสนุนและมีส่วนร่วมในการฝึกอบรมการบริหารความเสี่ยงในประเด็นที่ได้รับอนุมัติ

2.1.4 กระบวนการบริหารความเสี่ยง (risk management process)

มหาวิทยาลัยนำ ISO 31000:2009 กรอบบริหารความเสี่ยง มาใช้ในทุกระดับของมหาวิทยาลัยทั้งด้านเชิงกลยุทธ์และด้านการปฏิบัติงาน ดังรูปที่ 10 โดยกระบวนการบริหารความเสี่ยงมีขั้นตอนดังนี้



รูปที่ 10 กระบวนการบริหารความเสี่ยงของ International Islamic University Malaysia

ขั้นกำหนดบริบท (establish the context)

การกำหนดตัวแปรภายนอกและภายในที่จะนำมาพิจารณาในการบริหารความเสี่ยง และกำหนดขอบเขตและเกณฑ์ความเสี่ยงสำหรับนโยบายการบริหารความเสี่ยง

ขั้นการระบุความเสี่ยง (risk identification)

เกี่ยวข้องกับความพยายามระบุความเสี่ยงที่อาจเกิดขึ้นทั้งหมดที่อาจมีผลกระทบต่อการบรรลุวัตถุประสงค์ทางธุรกิจที่ระบุ เกี่ยวข้องกับการตรวจสอบแหล่งที่มาของความเสี่ยงทั้งหมดและข้อมูลจากมุมมองของผู้มีส่วนได้ส่วนเสียทั้งหมดทั้งภายในและภายนอก องค์ประกอบของความเสี่ยงบางส่วนจะอยู่ภายใต้การควบคุมของเรา (เรียกว่า ความเสี่ยงที่ควบคุมได้) ในขณะที่ส่วนอื่น ๆ จะไม่อยู่ภายใต้การควบคุมของเรา (หรือที่เรียกว่า ความเสี่ยงโดยธรรมชาติ) ดังนั้น จึงต้องพิจารณาการควบคุมความเสี่ยงทั้งภายในและภายนอกเมื่อระบุความเสี่ยง

ขั้นการวิเคราะห์ความเสี่ยง (risk analysis)

ในขั้นนี้ดำเนินการโดยการระบุและรับรู้สาเหตุที่เป็นไปได้ซึ่งนำไปสู่ความเสี่ยงที่ระบุ นอกจากนี้ยังเกี่ยวข้องกับการประมาณความน่าจะเป็นของเหตุการณ์ความเสี่ยงที่เกิดขึ้นและผลที่ตามมาหรือผลกระทบในบริบทของมาตรการควบคุมภายในที่มีอยู่ สาเหตุและผลกระทบที่ตามมาจะมีความจำเป็นในการพัฒนาการดำเนินการบรรเทาผลกระทบและการประเมินผลกระทบหรือการสูญเสียที่อาจเกิดขึ้น

ขั้นการประเมินความเสี่ยง (risk evaluation)

วัตถุประสงค์ของการประเมินความเสี่ยงคือ เพื่อช่วยในการตัดสินใจตามผลของการวิเคราะห์ความเสี่ยง เกี่ยวกับความเสี่ยงที่ต้องการการรักษาและลำดับความสำคัญสำหรับการดำเนินการจัดการ เกี่ยวข้องกับการเปรียบเทียบระดับความเสี่ยงโดยวิเคราะห์จากเกณฑ์ความเสี่ยงที่กำหนดขึ้นเมื่อพิจารณาบริบทจากการเปรียบเทียบนี้ ความจำเป็นในการรักษาสามารถพิจารณาได้

ขั้นการจัดการความเสี่ยง (risk treatment)

คือ การปฏิบัติต่อความเสี่ยงหรือการตอบสนองความเสี่ยง เกี่ยวข้องกับการเลือกหนึ่งตัวเลือกหรือมากกว่าสำหรับการปรับเปลี่ยนความเสี่ยง และการนำทางเลือกเหล่านั้นไปใช้ เมื่อนำไปใช้แล้ว การจัดการหรือปรับเปลี่ยนการควบคุม แผนการจัดการความเสี่ยงเป็นการดำเนินการเพื่อป้องกัน ตรวจจับ หรือจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ การออกแบบแผนการจัดการความเสี่ยงควรอยู่บนพื้นฐานของความเข้าใจที่ครอบคลุมเกี่ยวกับความเสี่ยงที่เกี่ยวข้อง การระบุสาเหตุของความเสี่ยงเป็นสิ่งสำคัญโดยเฉพาะอย่างยิ่งเพื่อให้สิ่งเหล่านี้ได้รับการรักษาและไม่ใช่แค่อาการเท่านั้น

ขั้นการติดตามและทบทวน (monitor and review)

คือ ขั้นของการติดตามให้แน่ใจว่ามีการทบทวนและการรายงานอย่างสม่ำเสมอตลอดจนอัปเดตข้อมูลความเสี่ยงทุกประเภทที่เกี่ยวข้องกับโปรไฟล์ความเสี่ยงของมหาวิทยาลัย เพื่อระบุการเปลี่ยนแปลงและพิจารณาว่าการตอบสนองและการบรรเทาความเสี่ยงที่ตกลงกันไว้ก่อนหน้านี้จัดการความเสี่ยงตามที่ตั้งใจไว้หรือไม่ ต้องพร้อมที่จะรับมือกับภัยคุกคามและโอกาสที่เกิดขึ้นใหม่ตลอดจนการติดตามตรวจสอบ หากมีการระบุความเสี่ยงแต่อยู่นอกขอบเขตของหน่วยงาน จำเป็นต้องยกระดับ ลดระดับ หรือแจ้งให้หน่วยงานที่เกี่ยวข้องทราบโดยทั่วกัน

2.2 Qatar University – ประเทศกาตาร์

2.2.1 วัตถุประสงค์การบริหารความเสี่ยง (risk management objectives)

วัตถุประสงค์ของกระบวนการและขั้นตอนการจัดการความเสี่ยงภายในมหาวิทยาลัยกาตาร์มีดังต่อไปนี้

1. สนับสนุนการตัดสินใจที่มีประสิทธิภาพซึ่งสอดคล้องกับพันธกิจ วิสัยทัศน์ และค่านิยมของมหาวิทยาลัยกาตาร์ (QU)
2. ใช้แนวทางการบริหารความเสี่ยงอย่างเป็นระบบและสม่ำเสมอเพื่อให้แน่ใจว่าความเสี่ยงที่สำคัญทั้งหมดในทุกหมวดหมู่ได้รับการระบุและจัดการอย่างมีประสิทธิภาพ
3. การสนับสนุนในการบรรลุผลสำเร็จตามวัตถุประสงค์ของ QU
4. กำหนดความมุ่งมั่นของมหาวิทยาลัยตามหลักการของการบริหารความเสี่ยงและรวมสิ่งเหล่านี้เข้ากับทุกด้านของมหาวิทยาลัย
5. ช่วยในการจับโอกาสและลดภัยคุกคาม
6. ส่งเสริมวัฒนธรรมการบริหารความเสี่ยง
7. อธิบายบทบาทและความรับผิดชอบของฝ่ายบริหารความเสี่ยง สถาบันและผู้มีส่วนได้ส่วนเสียของ QU

ผู้มีส่วนเกี่ยวข้องในกระบวนการดังกล่าว ได้แก่ ประธาน รองประธาน ที่ปรึกษาด้านกฎหมาย คณบดี ผู้อำนวยการ/หัวหน้าแผนก คณะ เจ้าหน้าที่บัญชี/การเงิน นักเรียนและพนักงานทุกคน

2.2.2 กรอบการบริหารความเสี่ยง (risk management framework)

มหาวิทยาลัยกาตาร์ได้อ้างอิงแนวทางของ SAB ในการพัฒนาและดำเนินการตามกรอบการบริหารความเสี่ยงและกระบวนการเพื่อดูแลและจัดการความเสี่ยงของสถาบัน วัตถุประสงค์ของกรอบบริหารความเสี่ยง (risk management framework) คือ เพื่อช่วย QU ในการบูรณาการการบริหารความเสี่ยงเข้ากับกิจกรรมและหน้าที่ที่สำคัญ กรอบการทำงานนี้ช่วยให้ข้อมูลเกี่ยวกับความเสี่ยงของสถาบันที่ได้รับจากกระบวนการการจัดการความเสี่ยง สามารถรายงานได้อย่างเพียงพอและใช้เป็นพื้นฐานสำหรับการตัดสินใจและความรับผิดชอบทั่วทั้ง QU กรอบการบริหารความเสี่ยงประกอบด้วยองค์ประกอบหลัก 8 ส่วน และนำไปใช้กับ QU ดังนี้

1. ภาวะผู้นำของผู้บริหาร เกี่ยวข้องกับการตระหนักถึงแนวทางและดูแลการบูรณาการแนวปฏิบัติด้านการจัดการความเสี่ยงในสถาบัน

2. การจัดตั้งนโยบายการจัดการความเสี่ยง เกี่ยวข้องกับการกำหนดแนวทางของสถาบันต่อการจัดการความเสี่ยง กำหนดกรอบความเสี่ยงและความเบี่ยงเบนต่อความเสี่ยง ประกอบด้วย โครงร่างภาระรับผิดชอบ (accountability) และความรับผิดชอบ (responsibility) ที่สำคัญสำหรับการจัดการความเสี่ยง

3. การกำหนดความรับผิดชอบสำหรับการจัดการความเสี่ยง เกี่ยวข้องกับการสนับสนุนให้ผู้บริหารระดับสูงกำหนดความรับผิดชอบสำหรับการจัดการความเสี่ยง ความรับผิดชอบในการบริหารความเสี่ยงแบบวันต่อวันตกแก่พนักงานทุกระดับ

4. การฝังการจัดการความเสี่ยงเข้ากับกระบวนการทางธุรกิจ คือ การเปิดตัวกลยุทธ์การจัดการการเปลี่ยนแปลงและปรับความเสี่ยงขั้นสุดท้าย ซึ่งเป็นกระบวนการจัดการที่เฉพาะเจาะจงสำหรับสถาบันและปรับแนวปฏิบัติด้านการจัดการความเสี่ยงทั้งหมดให้สอดคล้องกับการตัดสินใจที่เกี่ยวข้อง

5. การพัฒนาวัฒนธรรมความเสี่ยงเชิงบวก คือ ชุดของทัศนคติ ค่านิยม และพฤติกรรมที่มีร่วมกัน ซึ่งกำหนดลักษณะที่สถาบันพิจารณาความเสี่ยงในกิจกรรมประจำวัน

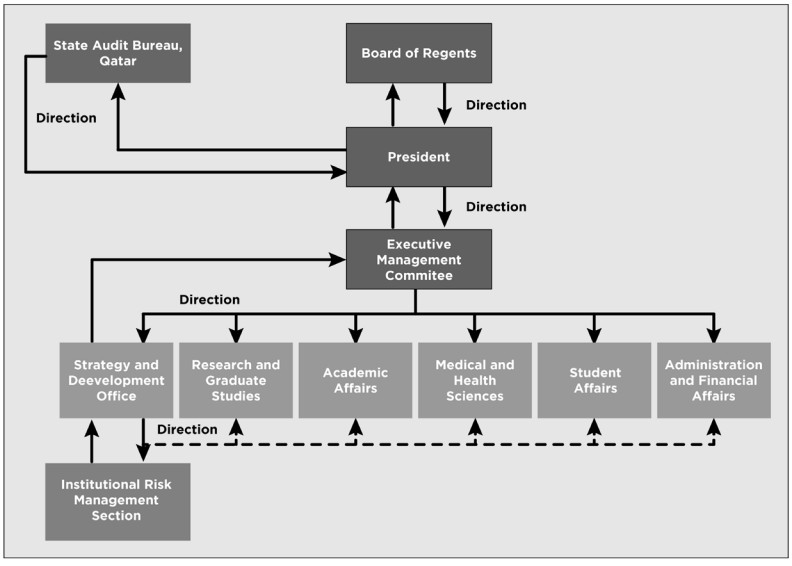
6. การสื่อสารและให้คำปรึกษาเกี่ยวกับความเสี่ยง เกี่ยวข้องกับการจัดเตรียมการดำเนินการเพื่อสื่อสารและปรึกษากับผู้มีส่วนได้ส่วนเสียที่เหมาะสม ตลอดจนแหล่งข้อมูลเกี่ยวกับความเสี่ยงอย่างทันท่วงทีและมีประสิทธิภาพ

7. การรักษาความสามารถในการบริหารความเสี่ยง เป็นการรักษาระดับความสามารถที่เหมาะสมเพื่อใช้ทั้งกรอบการบริหารความเสี่ยงและจัดการความเสี่ยงที่กำลังดำเนินอยู่

8. การทบทวนและปรับปรุงการบริหารความเสี่ยง ระดับความเสี่ยงที่รับได้อาจเปลี่ยนแปลงได้ ดังนั้น การแก้ไขแบบรวดเร็วในนโยบาย ขั้นตอน และกิจกรรมที่วางไว้เพื่อติดตาม รายงาน และลดความเสี่ยง รวมถึงการตรวจจับผลการลดความเสี่ยง

2.2.3 บทบาทและความรับผิดชอบในการบริหารความเสี่ยง (roles & responsibilities)

มหาวิทยาลัยกาตาร์มีบุคคล กลุ่มบุคคล หรือหน่วยงานที่เกี่ยวข้องในการบริหารความเสี่ยงตามกรอบการบริหารความเสี่ยงให้เป็นระบบและมีประสิทธิผล ซึ่งการกำกับดูแลการบริหารความเสี่ยงแสดงไว้ดังรูปที่ 11 โดยมีรายละเอียดดังต่อไปนี้



รูปที่ 11 การกำกับดูแลการบริหารความเสี่ยงของ Qatar University

1. **สำนักงานตรวจเงินแผ่นดิน – กาตาร์ (State Audit Bureau – Qatar)** ทำหน้าที่

1) ออกแนวทางการบริหารความเสี่ยง (The GUIDE)

2) ดูแลรักษาและปรับปรุงแนวทางเพื่อให้สอดคล้องกับแนวทางปฏิบัติที่ดีที่สุดต่อไป

3) ขอให้ทุกหน่วยงานที่เกี่ยวข้องส่งข้อมูลความเสี่ยงไปยังสำนักงาน

4) ประสานงานการอภิปรายระหว่างหน่วยงานเรื่องความเสี่ยงทั่วไปและความเสี่ยงร่วมกัน

5) ดำเนินการตรวจสอบและทบทวนแนวทางปฏิบัติในการบริหารความเสี่ยง

2. **สภามหาวิทยาลัย QU (Board of Regents: BOR)** ทำหน้าที่

1) แจ้งการลงทะเบียนความเสี่ยงในสถาบันของ QU ระดับความเสี่ยงที่ยอมรับได้ ระดับความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ และโปรไฟล์ความเสี่ยง

2) ทบทวนรายงานการจัดการความเสี่ยงประจำปี

3. **สำนักงานอธิการบดี (President Office)** ทำหน้าที่

1) ส่งทะเบียนความเสี่ยงของสถาบันอย่างเป็นทางการของ QU ไปยังสำนักงานตรวจเงินแผ่นดิน – กาตาร์ (QSAB)

2) จัดการการตอบสนองของคำขอข้อมูลความเสี่ยงทั้งหมดที่ออกโดย QSAB

4. **คณะกรรมการบริหาร (Executive Management Committee: EMC)** ทำหน้าที่

1) รับรองทำทะเบียนความเสี่ยงของ QU และกระบวนการและขั้นตอนการบริหารความเสี่ยง

2) กำหนดความเสี่ยงในสถาบันของ QU การยอมรับความเสี่ยง และข้อมูลภาพรวมความเสี่ยง

3) ระบุและรับรองความเสี่ยง การจัดประเภท แผนการรักษา และเจ้าของสถาบันของ QU ทุกปี

4) จัดให้มีการมุ่งเน้นเชิงกลยุทธ์ในการบริหารความเสี่ยง เพื่อให้มั่นใจว่าการระบุความเสี่ยงได้รับการบูรณาการและสอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์ที่สำคัญ

5) ตรวจสอบให้แน่ใจว่า BOR ได้รับแจ้งถึงความเสี่ยงของสถาบันทั้งหมดและมีการดำเนินแผนปฏิบัติการที่เหมาะสมผ่านรายงาน RM ประจำปี

6) ทบทวนและให้ข้อเสนอแนะเกี่ยวกับรายงานการบริหารความเสี่ยงประจำปี และให้คำแนะนำเกี่ยวกับวิธีจัดการกับความเสี่ยงในอนาคตและเสนอแนวทางแก้ไข

7) ทบทวนแนวทางของ QU ต่อการบริหารความเสี่ยงและอนุมัติการเปลี่ยนแปลงหรือปรับปรุงกระบวนการทุกปี

8) ปลูกฝังวัฒนธรรมความเสี่ยงด้วยการสนับสนุนนโยบาย พฤติกรรม และเอกสาร สนับสนุนอื่น ๆ ซึ่งสนับสนุนการรับความเสี่ยงที่เหมาะสม

5. ประธานเจ้าหน้าที่ฝ่ายกลยุทธ์และพัฒนา (Chief Strategy and Development Officer: CSDO) ทำหน้าที่

1) กำหนดแนวทางเชิงกลยุทธ์ด้วยทรัพยากรที่จำเป็นสำหรับการบริหารความเสี่ยง และรับรองการดำเนินการที่เหมาะสมของกระบวนการ ขั้นตอน และกิจกรรมที่เกี่ยวข้องกับการบริหารความเสี่ยงที่ได้รับอนุมัติของ QU

2) ทบทวนและให้ข้อเสนอแนะเกี่ยวกับรายงานการบริหารความเสี่ยงประจำปีสำหรับการส่งข้อมูลของคณะกรรมการบริหาร (EMC)

3) ทบทวนรายงานเกี่ยวกับความเสี่ยงของสถาบัน QU และแผนการจัดการความเสี่ยงอย่างต่อเนื่อง รวมถึงแผนบริหารความต่อเนื่องทางธุรกิจและให้ข้อมูลอัปเดตเป็นประจำแก่ EMC ตามความจำเป็น

4) ทบทวนรายงานความเสี่ยงของสถาบันที่สำคัญและแจ้ง EMC เกี่ยวกับความเสี่ยงที่เกิดขึ้นใหม่ซึ่งอาจทำให้ QU มีความเสี่ยงที่อาจเกิดขึ้น

5) ตรวจสอบให้แน่ใจว่า QU มีความรับผิดชอบในการบริหารความเสี่ยงและแผนการจัดการ

6) ตรวจสอบให้แน่ใจว่ามีกลไกการรายงานและการส่งต่อที่เหมาะสม

7) ตรวจสอบให้แน่ใจว่ามีการฝึกอบรมและทรัพยากรที่เพียงพอ เพื่อให้แน่ใจว่ากระบวนการและขั้นตอนสามารถนำไปใช้ได้

6. แผนกตรวจสอบภายในและการปฏิบัติตามกฎระเบียบ (Internal Audit and Compliance Department) ทำหน้าที่

1) ทบทวนการปฏิบัติตามและประสิทธิผลของกระบวนการและขั้นตอนการบริหารความเสี่ยงของ QU โดยยึดตามแบบจำลองความเสี่ยงของ QU ที่ได้รับอนุมัติ

2) ทำงานร่วมกับส่วนการบริหารความเสี่ยงของสถาบัน (Institutional Risk Management Section: IRM) ในการตรวจสอบการจัดการความเสี่ยงที่สำคัญ

7. ส่วนการบริหารความเสี่ยงของสถาบัน (Institutional Risk Management Section: IRM) ทำหน้าที่

1) แนะนำ CSDO เกี่ยวกับความเสี่ยงที่สำคัญของสถาบันและความเสี่ยงที่เกิดขึ้นใหม่

2) ตรวจสอบให้แน่ใจว่ามีการสื่อสารอย่างมีประสิทธิภาพของกระบวนการยกระดับการบริหารความเสี่ยงกับตัวแทนความเสี่ยงทั่วทั้ง QU

3) จัดให้มีการตระหนักรู้และการฝึกอบรมที่จำเป็นแก่ตัวแทนความเสี่ยงและชุมชน QU เพื่อดำเนินการตามกระบวนการการบริหารความเสี่ยงอย่างต่อเนื่อง

4) ทบทวนและหารือเกี่ยวกับความเสี่ยงที่สำคัญและแผนการรักษากับเจ้าของความเสี่ยงที่เกี่ยวข้อง

5) จัดทำรายงานเกี่ยวกับความเสี่ยงที่สำคัญและความเสี่ยงของสถาบันที่เกิดขึ้นใหม่ และกลยุทธ์การรักษาความเสี่ยงที่กำลังดำเนินอยู่ เช่น ทะเบียนความเสี่ยงสถาบัน

6) พัฒนา แนะนำ บริหารจัดการ และปรับปรุงกระบวนการและขั้นตอนการจัดการความเสี่ยงของ QU

7) รายงานต่อ CSDO เกี่ยวกับประสิทธิภาพของกระบวนการการจัดการความเสี่ยงและให้คำแนะนำในการปรับปรุงกระบวนการและขั้นตอนของการบริหารความเสี่ยงทุกปี

8) จัดตั้งและรักษาทะเบียนความเสี่ยงของสถาบันของ QU

9) ทบทวนระดับความเสี่ยงที่ยอมรับได้ ระดับความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ และโปรไฟล์ความเสี่ยง

10) ส่งเสริมวัฒนธรรมของการจัดการความเสี่ยงภายใน QU

11) อำนวยความสะดวกในการระบุความเสี่ยงผ่านการประชุมเชิงปฏิบัติการความเสี่ยง การประชุมระดมความคิด การสัมภาษณ์ โดยใช้เครื่องมือความเสี่ยงที่ได้รับอนุมัติ มาตรฐาน/มหาวิทยาลัยหากมี

12) ติดตามข่าวสารล่าสุดเกี่ยวกับการจัดการความเสี่ยงโดยสื่อสารกับ SAB เกี่ยวกับปัญหา การพัฒนา และการอัปเดตทั้งหมด

13) ใช้ประโยชน์จากการทำงานร่วมกันที่เป็นไปได้สำหรับการระบุความเสี่ยงและการรักษา

8. เจ้าภาพความเสี่ยง (Risk Owners) ทำหน้าที่

1) ตรวจสอบให้แน่ใจว่ามีการระบุ ประเมิน จัดการ และติดตามความเสี่ยง

2) กำหนดระดับความเสี่ยงที่เหมาะสม

3) เลือกเจ้าภาพผู้รับผิดชอบในการจัดการความเสี่ยง

4) ตรวจสอบให้แน่ใจว่ากิจกรรมการจัดการความเสี่ยงถูกรวมเข้ากับกิจกรรมการปฏิบัติงาน

5) สังเกตสภาพแวดล้อมภายในและภายนอกสำหรับภัยคุกคามและโอกาสที่เกิดขึ้น

6) ตรวจสอบให้แน่ใจว่ากิจกรรมการจัดการความเสี่ยงถูกรวมเข้ากับกิจกรรมการปฏิบัติงาน

7) สังเกตสภาพแวดล้อมภายในและภายนอกสำหรับภัยคุกคามและโอกาสที่เกิดขึ้น

9. ผู้ดูแลงานบริหารความเสี่ยง (Risk Champions) ทำหน้าที่

1) พัฒนา บำรุงรักษา ทบทวน และปรับปรุงทะเบียนความเสี่ยงโดยประสานงานกับเจ้าของความเสี่ยงที่เกี่ยวข้องในระดับหน่วยสำหรับแต่ละภาคส่วน

2) สื่อสารทะเบียนความเสี่ยงขององค์กรกับหน่วยงานกับส่วน IRM

3) รายงานต่อเจ้าของความเสี่ยงเกี่ยวกับความคืบหน้าของกระบวนการจัดการความเสี่ยง การดำเนินการบำบัดความเสี่ยง และความเสี่ยงใด ๆ ที่เกิดขึ้น

4) จัดทำเอกสารแนวปฏิบัติที่ดีและเหตุการณ์ความเสี่ยง

5) ส่งเสริมวัฒนธรรมการจัดการความเสี่ยงภายในหน่วยงาน

10. เจ้าภาพความเสี่ยง (Risk Treatment Owner) ทำหน้าที่

1) ดำเนินการและติดตามความคืบหน้าในการดำเนินการตามแผนการรักษาหรือมาตรการบรรเทาผลกระทบ

2) ให้ข้อมูล รายงาน และอัปเดตแก่เจ้าของความเสี่ยง

2.2.4 กระบวนการบริหารความเสี่ยง (risk management process)

การจัดการความเสี่ยงเป็นกระบวนการปรับปรุงอย่างต่อเนื่องเพื่อประเมิน จัดการ ติดตาม และสื่อสารความเสี่ยงที่สำคัญไปยังผู้บริหารระดับสูง กระบวนการและขั้นตอนการบริหารความเสี่ยงของมหาวิทยาลัยกาตาร์จะสอดคล้องกับ ISO 31000:2018 Risk Management – Guidelines โดยกระบวนการบริหารความเสี่ยงมีขั้นตอนดังนี้

ขั้นที่ 1 ขอบเขต บริบท หลักเกณฑ์ (scope context principle) ด้วยการกำหนดขอบเขต บริบท และเกณฑ์ QU จะสามารถระบุวัตถุประสงค์และกำหนดตัวแปรภายนอกและภายในที่จะนำมาพิจารณาเมื่อจัดการความเสี่ยง สามารถทำได้ดังนี้

1. การกำหนดขอบเขตสำหรับกิจกรรมการจัดการความเสี่ยงซึ่งสามารถนำไปใช้ในระดับต่าง ๆ เช่น กลยุทธ์ การดำเนินงาน โครงการ หรือกิจกรรมอื่น ๆ
2. การกำหนดวัตถุประสงค์แบบกว้าง
3. การระบุผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง
4. จัดเครื่องมือและเทคนิคการประเมินความเสี่ยงที่เหมาะสม
5. จัดเตรียมทรัพยากรที่จำเป็น ความรับผิดชอบ และบันทึกที่ต้องเก็บไว้
6. สร้างความสัมพันธ์กับโครงการ กระบวนการ และกิจกรรมอื่น ๆ

ขั้นที่ 2 การระบุความเสี่ยง (risk identification) การระบุความเสี่ยงต้องใช้ความเสี่ยงที่คาดการณ์ได้อย่างเหมาะสม ซึ่งอาจมีผลกระทบอย่างมีนัยสำคัญต่อมหาวิทยาลัย ความเสี่ยงคือเหตุการณ์หรือการกระทำใด ๆ ที่มีผลกระทบที่ไม่แน่นอนที่อาจส่งผลกระทบต่อวัตถุประสงค์ของ QU ความเสี่ยงเกิดขึ้นได้มากจากความเป็นไปได้ที่โอกาสจะไม่เกิดขึ้น เช่นเดียวกับความเสี่ยงที่ภัยคุกคามจะเกิดขึ้น เกิดข้อผิดพลาด หรือความเสียหาย/การบาดเจ็บเกิดขึ้น ในขั้นตอนนี้ ความเสี่ยงจะต้องถูกจัดประเภทโดยใช้หมวดหมู่ความเสี่ยงของ QU ซึ่งการระบุความเสี่ยงจะเกิดขึ้นในระดับต่าง ๆ ดังนี้

1. ระดับสถาบัน ความเสี่ยงด้านกลยุทธ์และการดำเนินงานที่สำคัญทั้งหมดซึ่งเกี่ยวข้องกับการไม่สามารถบรรลุวัตถุประสงค์ของ QU กล่าวได้ว่าเกี่ยวข้องกับผู้บริหารระดับสูง

2. ระดับยุทธศาสตร์ ความเสี่ยงที่ส่งผลต่อกลยุทธ์หรือวัตถุประสงค์เชิงกลยุทธ์ของแต่ละภาคส่วน กล่าวได้ว่าเกี่ยวข้องกับระดับ Vice President

3. ระดับปฏิบัติการ ความเสี่ยงซึ่งเกี่ยวข้องกับกระบวนการที่มีอยู่และใช้งานไม่ได้แก้ไขได้ดีที่สุดตามระดับหน่วย

ขั้นที่ 3 การประเมินความเสี่ยง (risk evaluation) การตัดสินใจควรคำนึงถึงการเปรียบเทียบผลการวิเคราะห์ความเสี่ยงโดยรวมกับความเสี่ยงระดับสถาบันของ QU และความคลาดเคลื่อนโดยการเปรียบเทียบผลลัพธ์จากการประเมินความเสี่ยงกับระดับความเสี่ยงโดยรวม (โอกาส x ผลที่ตามมา) เพื่อกำหนดระดับความเสี่ยง นอกจากนี้ ผลกระทบที่เกิดขึ้นจริงและที่รับรู้ต่อผู้มีส่วนได้ส่วนเสียทั้งภายนอกและภายในและความเสี่ยงนั้นเป็นที่ยอมรับหรือไม่ ในการประเมินความเสี่ยง จำเป็นสำหรับ QU ที่จะต้องสะท้อนให้เห็นว่าความเสี่ยงนั้นสามารถเป็นส่วนสำคัญของสิ่งที่พวกเขาทำตามวิสัยทัศน์ พันธกิจ และกลยุทธ์

ขั้นที่ 4 พัฒนาทางเลือก (develop alternatives) เป็นการระบุและประเมินทางเลือกหรือกลยุทธ์ในการตอบสนองอย่างเป็นระบบต่อความเสี่ยง โดยพิจารณาจากความเสี่ยงในระดับสถาบันของ QU จุดมุ่งหมายของขั้นตอนนี้ คือ การเปรียบเทียบผลกระทบของความเสี่ยงกับการสูญเสียที่อาจเกิดขึ้น/และกำหนดวิธีจัดสรรทรัพยากรดังนี้

ทางเลือก/กลยุทธ์ภัยคุกคาม

1. หลีกเลี่ยง (avoidance) รูปแบบการจัดการความเสี่ยงโดยการปฏิเสธธุรกรรม ข้อเสนอ โครงการ หรือกิจกรรมที่ก่อให้เกิดภัยคุกคาม

2. การโอน (sharing) เป็นรูปแบบการจัดการความเสี่ยงโดยการแลกเปลี่ยนหรือโอนความเสี่ยงกับบุคคลอื่นผ่านสัญญาหรือประกัน

3. ลด (reduction) เป็นรูปแบบหนึ่งของการจัดการความเสี่ยงเชิงป้องกัน โดยมีจุดมุ่งหมายเพื่อลดโอกาสหรือผลที่ตามมา/ความรุนแรงหรือทั้งสองอย่างของภัยคุกคาม

4. ยอมรับ (acceptance) หน่วยงานจะเลือกตัวเลือกนี้เมื่อภัยคุกคามอยู่ภายในขีดจำกัดความเบี่ยงเบนต่อระดับความเสี่ยงที่ยอมรับได้และการควบคุมที่มีอยู่ก็เพียงพอแล้ว หรือไม่มีการดำเนินการใด ๆ เพิ่มเติมที่ฝ่ายบริหารตั้งใจจะนำไปปฏิบัติ หรือค่าใช้จ่ายในการบรรเทาภัยคุกคามนั้นสูงกว่าต้นทุนของภัยคุกคามนั้นเอง หรือภัยคุกคามและระดับคงเหลือในปัจจุบันเป็นที่ยอมรับโดยผู้บริหารซึ่งเป็นส่วนหนึ่งของกลยุทธ์โดยรวม

5. ยกระดับ (escalate) รูปแบบของการจัดการที่รับรองว่าภัยคุกคามจะถูกส่งต่อไปยังเจ้าของที่ถูกต้องเพื่อให้แน่ใจว่าได้รับการยอมรับ เข้าใจ และจัดการอย่างเหมาะสม

ทางเลือกด้านโอกาส/กลยุทธ์เชิงโอกาส

1. การใช้ประโยชน์ (exploit) รูปแบบการจัดการที่ทำให้มีโอกาสเกิดขึ้นอย่างแน่นอน

2. การถ่ายทอด (share) รูปแบบการจัดการที่เกี่ยวข้องกับบุคคลที่สามในการจัดการโอกาสที่เกิดขึ้น

3. ส่งเสริม (enhance) รูปแบบการจัดการที่เพิ่มผลกระทบของโอกาส

4. ยอมรับ (except) รูปแบบการจัดการที่แผนการจัดการหรือการดำเนินการคือ การใช้หรือยอมรับโอกาสเพื่อที่จะไล่ตามนั้น

5. ยกระดับ (escalate) รูปแบบหนึ่งของการจัดการที่ส่งผ่านโอกาสไปยังเจ้าของที่ถูกต้อง เพื่อให้มั่นใจว่าได้รับการยอมรับ เข้าใจ และจัดการอย่างเหมาะสม

ขั้นที่ 5 การตอบสนองต่อความเสี่ยง (respond to risks) ภาวะผู้นำของผู้บริหารมีส่วนสำคัญต่อการประเมินทางเลือกและตัดสินใจว่าจะจัดสรรทรัพยากรอย่างไรเพื่อจัดการกับความเสี่ยงที่สำคัญที่ QU เผชิญอยู่ เมื่อมีการตัดสินใจเกี่ยวกับวิธีการตอบสนองต่อความเสี่ยงและการจัดสรรความเป็นเจ้าของแล้ว ควรมีการบันทึกแผนการรักษาอย่างเหมาะสม

ขั้นที่ 6 การตรวจสอบและทบทวน (monitoring and reviewing) คือ ขั้นของการตรวจสอบให้แน่ใจว่ามีการทบทวนและการรายงานอย่างสม่ำเสมอ ตลอดจนอัปเดตข้อมูลความเสี่ยงทุกประเภทที่เกี่ยวข้องกับโปรไฟล์ความเสี่ยงของ QU เพื่อระบุการเปลี่ยนแปลงและพิจารณาว่าการตอบสนองและการบรรเทาความเสี่ยงที่ตกลงกันไว้ก่อนหน้านี้จัดการความเสี่ยงตามที่ตั้งใจไว้หรือไม่ ด้วยธรรมชาติที่หลากหลายและมีพลวัตของสภาพแวดล้อมของ QU สิ่งสำคัญคือต้องพร้อมที่จะรับมือกับภัยคุกคามและโอกาสที่เกิดขึ้นใหม่ตลอดจนการติดตามตรวจสอบ หากมีการระบุความเสี่ยงแต่อยู่นอกขอบเขตของหน่วยงาน จำเป็นต้องยกระดับ ลดระดับ หรือแจ้งให้หน่วยงานที่เกี่ยวข้องทราบโดยทั่วกัน

ขั้นที่ 7 สื่อสาร ให้คำปรึกษา การเรียนรู้ (communication, consultation, learning) การสื่อสารและการปรึกษาหารือที่มีประสิทธิภาพเป็นสิ่งสำคัญเพื่อให้แน่ใจว่าผู้ที่รับผิดชอบในการดำเนินการการจัดการความเสี่ยง เข้าใจพื้นฐานในการตัดสินใจและเหตุผลที่เลือกวิธีการรักษาเฉพาะ การจัดการความเสี่ยงจะได้รับการปรับปรุงผ่านการสื่อสาร

และการให้คำปรึกษาที่มีประสิทธิภาพเมื่อหน่วย QU ทั้งหมดเข้าใจมุมมองของกันและกัน ขั้นตอนนี้เกิดขึ้นตั้งแต่ขั้นตอนที่ 1 ถึงขั้นตอนที่ 6

ขั้นที่ 8 บันทึกการบำรุงรักษาและการรายงาน (records maintenance and reporting) กระบวนการจัดการความเสี่ยงและผลลัพธ์เป็นความพยายามอย่างต่อเนื่อง ซึ่งเป็นส่วนสำคัญในการกำกับดูแลของ QU ช่วยปรับปรุงการสื่อสารระหว่างผู้มีส่วนได้ส่วนเสีย เนื่องจากกิจกรรมของกระบวนการจัดการความเสี่ยง ได้รายงานไปยังแผนก IRM และคณะกรรมการบริหาร (EMC) จึงต้องมีการอัปเดตและประเมินผลอย่างสม่ำเสมอ เพื่อให้มีประสิทธิภาพและประสิทธิผล ผลลัพธ์ยังมีให้กับพนักงานตามความเหมาะสม ซึ่งจะช่วยในการตัดสินใจ ปรับปรุงกิจกรรมการจัดการความเสี่ยง ความโปร่งใส และการติดตามความเสี่ยงกับความเสี่ยงในระดับสถาบันที่ QU ระบุไว้

2.3 Carleton University: CU – ประเทศแคนาดา

2.3.1 วัตถุประสงค์การบริหารความเสี่ยง (risk management objectives)

มหาวิทยาลัยคาร์ลตันมุ่งมั่นที่จะเป็นผู้นำที่ท้าทาย มีพลังและสร้างสรรค์ในการศึกษาระดับอุดมศึกษา โดยจัดให้มีสภาพแวดล้อมการเรียนรู้ที่เข้าถึงได้ ปรับตัวได้ และท้าทายเพื่อพัฒนาผู้สำเร็จการศึกษาและการวิจัยที่ตอบสนองความต้องการของชุมชนระดับภูมิภาค ระดับชาติ และระดับนานาชาติ มหาวิทยาลัยตระหนักดีว่าสามารถใช้โอกาสในฐานะผู้นำและมีนวัตกรรมในการศึกษาระดับอุดมศึกษาหรือการวิจัย หากประชาคมมหาวิทยาลัยยินดีที่จะยอมรับและดำเนินชีวิตด้วยความเสี่ยงที่มีการจัดการในระดับหนึ่ง การจัดการความเสี่ยงที่มีประสิทธิผลเป็นสิ่งจำเป็นสำหรับการตัดสินใจเชิงกลยุทธ์ที่มีประสิทธิภาพ และการดำเนินการตามกระบวนการทางธุรกิจที่มีประสิทธิภาพ มีประสิทธิผลและแข็งแกร่ง ซึ่งช่วยให้มหาวิทยาลัยคว้าโอกาสในขณะที่ปฏิบัติตามมาตรฐานที่กำหนดในด้านความรับผิดชอบ การปฏิบัติตามข้อกำหนด ความน่าจะเป็น และความโปร่งใส

ในการสนับสนุนความสำเร็จของเป้าหมายเชิงกลยุทธ์และเชิงปฏิบัติการของมหาวิทยาลัย วัตถุประสงค์ของนโยบาย คือ เพื่อสร้างความตระหนักในการจัดการความเสี่ยง โดยเฉพาะอย่างยิ่งนโยบายนี้ให้คำแนะนำสำหรับผู้บริหารทุกระดับและผู้มีส่วนได้ส่วนเสียอื่น ๆ เพื่อการส่งเสริมดังนี้

1. ความตระหนักในความเสี่ยงทางธุรกิจที่เกี่ยวข้องกับการดำเนินงานของมหาวิทยาลัย

2. การตระหนักรู้ถึงความเสี่ยงที่สำคัญขององค์กรที่มหาวิทยาลัยเผชิญ

3. ใช้วิจารณญาณในการตัดสินใจ

4. ใช้ความระมัดระวังในระดับที่เหมาะสมในการปฏิบัติงานประจำวัน การรับความเสี่ยงอย่างชาญฉลาดในการแสวงหาแนวคิดและนวัตกรรมใหม่ ๆ

5. การปฏิบัติตามกฎหมายให้เป็นมาตรฐานขั้นต่ำ

2.3.2 กรอบการบริหารความเสี่ยง (risk management framework)

กรอบการบริหารความเสี่ยงเป็นองค์ประกอบหลักของความรับผิดชอบในการกำกับดูแลกิจการของฝ่ายบริหารของมหาวิทยาลัยและคณะกรรมการผู้ว่าการ กรอบการทำงานจะถูกนำไปใช้โดยเจ้าหน้าที่ทุกคนของมหาวิทยาลัยและหน่วยงานที่ควบคุม และจะระบุตัวเลือกสำหรับการปรับปรุงและปรับปรุงนโยบาย แนวทางปฏิบัติด้านการบริหารและการควบคุมภายใน และช่วยให้แน่ใจว่ามีความเกี่ยวข้อง ความปลอดภัย ความอยู่รอด การปฏิบัติตามข้อกำหนด และความรับผิดชอบอย่างต่อเนื่องในแต่ละวัน

การดำเนินการตามกรอบนี้คาดว่าจะช่วยให้ผู้จัดการและผู้นำทางวิชาการสามารถ:

1. ระบุโอกาสทางวิชาการและการวิจัยที่เป็นไปได้และยั่งยืน

2. สนับสนุนการตัดสินใจดำเนินการหรือยุติกิจกรรม

3. หลีกเลี่ยงโอกาสที่อาจทำให้มหาวิทยาลัยมีความเสี่ยงมากเกินไป

4. มั่นใจได้ในการส่งมอบบริการและผลิตภัณฑ์คุณภาพสูง

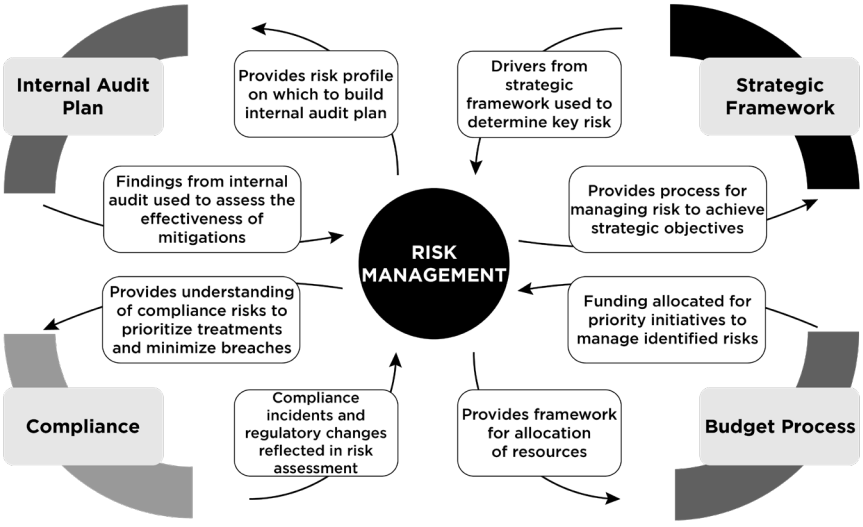
5. ตระหนักถึงการจัดการควบคุมการบริหารที่มีประสิทธิภาพและประสิทธิผลมากขึ้น

6. สนับสนุนการตัดสินใจด้านทรัพยากรและปริมาณงาน

7. วางแผนการตอบสนองที่ประสานกัน และการจัดการความเสี่ยงและเหตุการณ์ความเสี่ยงที่เกิดขึ้นใหม่

กรอบการบริหารความเสี่ยงของมหาวิทยาลัยถูกพัฒนาขึ้นในรูปแบบที่เรียกว่า "โมเดลมูลค่าการกำกับดูแล (Governance Value Model)"

การจัดการความเสี่ยงมีความเชื่อมโยงที่สำคัญหลายประการกับกิจกรรมการกำกับดูแลด้านอื่น ๆ ที่เกิดขึ้นทั่วทั้งมหาวิทยาลัยคาร์ลตัน โมเดลมูลค่าการกำกับดูแล (รูปที่ 12) แสดงให้เห็นถึงประโยชน์บางประการที่การบริหารความเสี่ยงอย่างเข้มแข็งมีให้ในด้านอื่น ๆ ของมหาวิทยาลัย และในทางกลับกัน โมเดลนี้ช่วยให้คณะกรรมการและผู้บริหารระดับสูงได้รับข้อมูลที่ทันเวลา สม่ำเสมอ และประเมินความเสี่ยง เพื่อช่วยในการตัดสินใจที่สมดุล



รูปที่ 12 การบริหารความเสี่ยงของ Carleton University

2.3.3 บทบาทและความรับผิดชอบในการบริหารความเสี่ยง (roles & responsibilities)

มหาวิทยาลัยคาร์ลตันมีบุคคล กลุ่มบุคคล หรือหน่วยงานที่เกี่ยวข้องในการบริหารความเสี่ยงตามกรอบการบริหารความเสี่ยงให้เป็นระบบและมีประสิทธิผลดังต่อไปนี้

1. คณะกรรมการบริหาร (Board of Governors) คณะกรรมการบริหารมีหน้าที่ในการกำกับดูแลแผนการบริหารความเสี่ยง และความเสี่ยงที่สำคัญขององค์กร รวมถึงมาตรการจัดการความเสี่ยงที่เกี่ยวข้อง คณะกรรมการบริหารโดยผ่านคณะกรรมการตรวจสอบและบริหารความเสี่ยง จะทำหน้าที่ในการ

1) อนุมัตินโยบายเกี่ยวกับการบริหารความเสี่ยง

2) อนุมัติการจัดทำทะเบียนความเสี่ยงขององค์กร

3) ตรวจสอบประสิทธิผลของกระบวนการบริหารความเสี่ยง

4) อนุมัติการดำเนินการจัดการเพื่อปรับปรุงการบริหารความเสี่ยง

2. อธิการบดีมหาวิทยาลัย มีหน้าที่

1) จัดให้มีการกำกับดูแลการบริหารความเสี่ยงทั่วไป เพื่อให้แน่ใจว่ามีการนำการจัดการความเสี่ยงระดับองค์กรมาใช้ทั่วทั้งมหาวิทยาลัย

2) ประเมินแผนปฏิบัติการความเสี่ยงสูงสุด และทบทวน/อนุมัติตัวเลือกการรักษาความเสี่ยงที่สำคัญ

3) ส่งเสริมวัฒนธรรมการบริหารความเสี่ยงในทุกระดับของมหาวิทยาลัย

3. รองอธิการบดี มีหน้าที่รับผิดชอบต่ออธิการบดีในการบริหารความเสี่ยง และมีหน้าที่ในการ

1) พัฒนาและดำเนินการตามนโยบายและขั้นตอนสำหรับการบริหารความเสี่ยง

2) กำหนดโปรไฟล์ความเสี่ยงของมหาวิทยาลัยและทัศนคติของมหาวิทยาลัยต่อความเสี่ยงเกี่ยวกับประเด็นสำคัญเฉพาะ

3) ระบุและจัดการความเสี่ยงขององค์กรที่มหาวิทยาลัยเผชิญและส่งข้อมูลนี้ไปยังอธิการบดีและคณะกรรมการบริหาร

4) ตรวจสอบให้แน่ใจว่ามีการระบุความเสี่ยงในการปฏิบัติงานและจัดการอย่างเหมาะสมทั่วทั้งมหาวิทยาลัย

5) ตรวจสอบให้แน่ใจว่าได้ปฏิบัติตามข้อเสนอแนะและทิศทางของคณะกรรมการบริหาร ประธาน และผู้ตรวจสอบภายในและภายนอก ในส่วนที่เกี่ยวกับการบริหารความเสี่ยง

6) ให้ข้อมูลที่เพียงพอในเวลาที่เหมาะสมแก่คณะกรรมการผู้บริหารผ่านคณะกรรมการตรวจสอบและความเสี่ยงเกี่ยวกับสถานะของความเสี่ยงและแนวทางปฏิบัติและเสนอต่อความเสี่ยง

7) รับรองการมีอยู่ของมาตรฐานการปฏิบัติงานสำหรับการดำเนินการตามนโยบายและขั้นตอนการบริหารความเสี่ยง

8) จัดให้มีการทบทวนประจำปีของการดำเนินงานของศูนย์งบประมาณหน่วยธุรกิจ และหน่วยงานควบคุมที่เกี่ยวข้องกับการดำเนินการตามนโยบายและขั้นตอนการบริหารความเสี่ยง

9) ทบทวนนโยบายและขั้นตอนอย่างสม่ำเสมอเพื่อให้แน่ใจว่ายังคงมีประสิทธิภาพและเหมาะสม

4. กรรมการและผู้จัดการ (Directors and Managers) มีหน้าที่รับผิดชอบในการรวมการบริหารความเสี่ยงให้เข้ากับแนวทางการจัดการมาตรฐาน โดย

1) ระบุและกำหนดการดำเนินการที่เหมาะสมเพื่อจัดการกับความเสี่ยงในการปฏิบัติงานภายในขอบเขตความรับผิดชอบตามนโยบายและขั้นตอนของมหาวิทยาลัย

2) การดำเนินการเกี่ยวกับการบริหารความเสี่ยงตามคำสั่งของรองอธิการบดี

3) การรายงานเกี่ยวกับการจัดการความเสี่ยงที่เกิดขึ้นใหม่หรือความเสี่ยงคงเหลือที่มีนัยสำคัญ

5. ผู้อำนวยการฝ่ายบริการความเสี่ยงและการประกันภัย (Director, Risk and Insurance Services) ผู้อำนวยการฝ่ายบริการความเสี่ยงและการประกันภัยมีหน้าที่รับผิดชอบการบริหารความเสี่ยงโดยรวมของมหาวิทยาลัยและมีหน้าที่รับผิดชอบในส่วนของ

1) การพัฒนากรอบและนโยบายการบริหารความเสี่ยงที่ช่วยให้มหาวิทยาลัยสามารถจัดการความเสี่ยงได้อย่างมีโครงสร้างและส่งเสริมวัฒนธรรมการบริหารความเสี่ยงที่แข็งแกร่งที่มหาวิทยาลัยคาร์ลตัน

2) สร้างความมั่นใจว่าความเสี่ยงและโอกาสได้รับการยอมรับอย่างเป็นทางการจัดลำดับความสำคัญ และมอบหมายให้กับเจ้าของความเสี่ยงที่เหมาะสมทั่วทั้งมหาวิทยาลัย

3) สร้างความมั่นใจว่าเจ้าของความเสี่ยงได้มอบหมายให้ผู้จัดการที่เหมาะสมดูแลการดำเนินการตามมาตรการเพื่อลดความเสี่ยงและเพิ่มโอกาสในทุกที่ที่ทำได้

4) ติดตามและรายงานความคืบหน้าของการกระทำเหล่านั้น

5) ตรวจสอบให้แน่ใจว่าแผนบริหารความเสี่ยงได้รับการตรวจสอบและปรับปรุงอย่างสม่ำเสมอ

6) การรักษา/อัปเดตทะเบียนความเสี่ยงที่สำคัญ 10 อันดับแรก

7) ดำเนินการหรือจัดการศึกษาและฝึกอบรมการบริหารความเสี่ยงที่เหมาะสม

8) ให้นโยบายและกระบวนการแก่หน่วยงานเพื่อระบุ วิเคราะห์ และจัดการความเสี่ยง

9) จัดทำและจัดทำรายงานผู้ใช้ที่เกี่ยวข้องและทันเวลา

10) จัดทำรายงานสถานะการบริหารความเสี่ยงองค์กรประจำปี (วัดความคืบหน้า/ขั้นตอนต่อไป)

11) การจัดการโครงการจัดหาเงินทุนเพื่อความเสี่ยงของมหาวิทยาลัยโดยการจัดหาประกันที่เพียงพอเพื่อปกป้องทรัพย์สินทางกายภาพของมหาวิทยาลัยและความเสี่ยงที่อาจเกิดขึ้น

6. ฝ่ายตรวจสอบภายใน (Internal Audit) มีหน้าที่ในการ

1) ตรวจสอบประสิทธิผลของการดำเนินงานของกรอบการบริหารความเสี่ยงและทำเป็นข้อมูลเข้าในกระบวนการระบุความเสี่ยง

2) แนะนำการเปลี่ยนแปลงการควบคุม ซึ่งเมื่อดำเนินการแล้วจะช่วยลดความเสี่ยงที่ระบุได้อย่างมีประสิทธิภาพและประสิทธิผล

2.3.4 กระบวนการบริหารความเสี่ยง (risk management process)

กระบวนการจัดการความเสี่ยงระดับองค์กร (ERM) ของมหาวิทยาลัยคาร์ลตันได้รับการพัฒนาตามแนวทางการจัดการความเสี่ยง ISO 31000 โดยกระบวนการบริหารความเสี่ยงองค์กรของมหาวิทยาลัยคาร์ลตัน ถูกรวมเข้ากับวัฒนธรรมและแนวปฏิบัติของสถาบัน และปรับให้เข้ากับแนวปฏิบัติทางธุรกิจของมหาวิทยาลัย การดำเนินการตามกรอบนี้คาดว่าจะช่วยให้ผู้จัดการและผู้นำทางวิชาการสามารถ

1. ระบุโอกาสทางวิชาการและการวิจัยที่เป็นไปได้และยั่งยืน
2. สนับสนุนการตัดสินใจดำเนินการหรือยุติกิจกรรม

3. หลีกเลี่ยงโอกาสที่อาจทำให้มหาวิทยาลัยมีความเสี่ยงมากเกินไป
4. มั่นใจได้ในการส่งมอบบริการและผลิตภัณฑ์คุณภาพสูง

กระบวนการจัดการความเสี่ยงระดับองค์กรของมหาวิทยาลัยคาร์ลตัน ประกอบด้วยขั้นตอนต่อไปนี้

ขั้นตอนที่ 1 ตรวจสอบสภาพแวดล้อมภายในและภายนอก ในระยะนี้ มหาวิทยาลัยจะชี้แจงวัตถุประสงค์ ตลอดจนกำหนดปัจจัยภายในและภายนอกที่จะต้องพิจารณาเมื่อกำหนดขอบเขตและเกณฑ์ความเสี่ยงสำหรับขั้นตอนที่เหลือในกระบวนการนี้

ขั้นตอนที่ 2 การประเมินความเสี่ยง (risk assessment) ซึ่งเกี่ยวข้องกับ 3 ขั้นตอนหลัก คือ

1. การระบุความเสี่ยง (risk identification) คือ การสร้างรายการความเสี่ยงที่ครอบคลุมโดยพิจารณาจากเหตุการณ์ที่อาจป้องกัน เร่งรัด หรือชะลอความสำเร็จตามวัตถุประสงค์ของมหาวิทยาลัย กระบวนการระบุความเสี่ยงเกี่ยวข้องกับการระบุแหล่งที่มาของความเสี่ยง สาเหตุและผลกระทบ ความเสี่ยงถูกระบุผ่านกระบวนการต่าง ๆ รวมถึงที่คณะกรรมการบริหารความเสี่ยง แผนก/การประเมินความเสี่ยงด้านปฏิบัติการ การประเมินความเสี่ยงด้านสุขภาพและความปลอดภัย และการสัมภาษณ์ที่ดำเนินการโดยผู้อำนวยการฝ่ายบริการความเสี่ยงและการประกันภัย โดยความเสี่ยงที่ระบุจะถูกบันทึกไว้ใน 10 Key Enterprise Risk Register ซึ่งระบุความเสี่ยง 10 อันดับแรกที่มหาวิทยาลัยต้องเผชิญ เอกสารเกี่ยวกับความเสี่ยงประกอบด้วยคำอธิบายความเสี่ยง การระบุปัจจัยที่นำไปสู่ความเสี่ยง และการระบุผลกระทบที่อาจเกิดขึ้น

2. การวิเคราะห์ความเสี่ยง (risk analysis) เกี่ยวข้องกับกระบวนการทำความเข้าใจความเสี่ยงที่ระบุและให้ข้อมูลเพื่อประเมินความเสี่ยง การวิเคราะห์ความเสี่ยงเกี่ยวข้องกับการประเมินความเสี่ยง โดยกำหนดผลกระทบของความเสี่ยงที่ระบุและแนวโน้มที่จะเกิดขึ้นและเป็นกระบวนการที่เสร็จสิ้นโดยคณะกรรมการความเสี่ยง วัตถุประสงค์ของขั้นตอนนี้คือ การจัดลำดับความสำคัญของความเสี่ยงในระดับการจัดอันดับเพื่อให้ความสนใจมุ่งเน้นไปที่ความเสี่ยงที่สูงขึ้นเป็นหลัก ความเสี่ยงเล็กน้อยและไม่สำคัญมักจะได้รับการจัดการผ่านกระบวนการและขั้นตอนการปฏิบัติงานตามปกติ และอาจ

ไม่ต้องการการจัดการความเสี่ยงเพิ่มเติม อย่างไรก็ตาม เอกสารเหล่านี้มีความสำคัญในการจัดทำเอกสารเพื่อความสมบูรณ์ของการวิเคราะห์ความเสี่ยง

3. การประเมินความเสี่ยง (risk evaluation) เกี่ยวข้องกับการประเมินการยอมรับความเสี่ยงเทียบกับคำชี้แจงความเสี่ยงของมหาวิทยาลัย ควรพิจารณาถึงการบรรเทาผลกระทบที่มีอยู่ ค่าใช้จ่ายในการจัดการความเสี่ยงเพิ่มเติม นโยบายหรือข้อกำหนดทางกฎหมาย และข้อพิจารณาที่เกี่ยวข้องอื่น ๆ จากภายในบริบทของมหาวิทยาลัย

ขั้นตอนที่ 3 การจัดการความเสี่ยง (risk treatment) หลังจากระบุความเสี่ยงคงเหลือแล้ว จะต้องกำหนดกลยุทธ์การดำเนินการตามความเสี่ยง โดยมี 5 ตัวเลือก ได้แก่

1. หลีกเลี่ยง (avoidance) สิ่งนี้เกี่ยวข้องกับการลบแหล่งความเสี่ยง ดำเนินการเพื่อหลีกเลี่ยงหรือยุติกิจกรรมที่สร้างความเสี่ยง

2. บรรเทา (reduction) บรรเทาหรือจัดการความเสี่ยง การดำเนินการเพื่อลดโอกาสเสี่ยงหรือผลกระทบ หรือทั้งสองอย่าง

3. ถ่ายโอน (sharing) แบ่งปันความเสี่ยงกับบุคคลอื่นหรือฝ่ายอื่น มีการดำเนินการเพื่อลดความเสี่ยงหรือผลกระทบโดยการโอนหรือแบ่งปันความเสี่ยงบางส่วน เทคนิคการแบ่งปันความเสี่ยงทั่วไป เช่น การซื้อประกันการรวมความเสี่ยง การทำธุรกรรมป้องกันความเสี่ยง

4. ยอมรับ (acceptance) รักษาความเสี่ยงโดยการตัดสินใจอย่างมีข้อมูล ไม่มีการดำเนินการใด ๆ ที่จะส่งผลกระทบต่อแนวโน้มความเสี่ยงหรือผลกระทบ ซึ่งอาจรวมถึงการรับหรือเพิ่มความเสี่ยงเพื่อไล่ตามโอกาส

5. ใช้ประโยชน์จากความเสี่ยง (take advantage) ความเสี่ยงบางอย่างสามารถใช้ประโยชน์ได้ นั่นคือความเสี่ยงที่มีผลกระทบเชิงบวกต่อการบรรลุเป้าหมายของมหาวิทยาลัย ดังนั้น ควรใช้แหล่งข้อมูลเพิ่มเติมเพื่อใช้ประโยชน์จากโอกาสที่มีให้

ขั้นตอนที่ 4 การตรวจสอบและทบทวน (monitoring and review) ทั้งการติดตามและทบทวนควรเป็นส่วนที่วางแผนไว้ของกระบวนการบริหารความเสี่ยงและเกี่ยวข้องกับการตรวจสอบหรือเฝ้าระวังอย่างสม่ำเสมอ กระบวนการติดตามและทบทวน

ความเสี่ยงของมหาวิทยาลัยควรตรวจสอบให้แน่ใจว่า การควบคุมมีประสิทธิภาพและประสิทธิผล ทั้งในด้านการออกแบบและการดำเนินงาน เพื่อให้บรรลุเป้าหมายนี้ ผู้อำนวยการฝ่ายบริการความเสี่ยงและการประกันภัยจำเป็นต้องเตรียมการดังต่อไปนี้

1. รับข้อมูลเพิ่มเติมเกี่ยวกับกระบวนการจัดการความเสี่ยงระดับเดียวกัน เพื่อปรับปรุงความเสี่ยง

2. กระบวนการจัดการความเสี่ยง

3. วิเคราะห์และเรียนรู้บทเรียนจากเหตุการณ์ การเปลี่ยนแปลง แนวโน้ม ความสำเร็จและความล้มเหลว

4. ตรวจจับการเปลี่ยนแปลงในบริบทภายนอกและภายใน รวมถึงการเปลี่ยนแปลงเกณฑ์ความเสี่ยงและความเสี่ยงที่อาจต้องมีการแก้ไขการรักษาความเสี่ยงและการจัดลำดับความสำคัญ

5. ระบุความเสี่ยงที่เกิดขึ้นใหม่

เพื่อให้มั่นใจว่าการจัดการความเสี่ยงยังคงมีประสิทธิภาพและยังคงสนับสนุนแผนบูรณาการเชิงกลยุทธ์ของมหาวิทยาลัยคาร์ลตันต่อไป จึงมีการติดตามตรวจสอบกระบวนการบริหารความเสี่ยงองค์กรอย่างต่อเนื่อง โดยกลไกต่อไปนี้ใช้เพื่อให้ข้อมูลเกี่ยวกับประสิทธิภาพของกรอบการทำงานดังนี้

1. การรายงานกิจกรรมต่าง ๆ ที่สร้างขึ้นจากแผนกปฏิบัติการ

2. ทบทวนและตอบกลับข้อเสนอแนะจากผู้มีส่วนได้ส่วนเสียภายนอกหรือหน่วยงานกำกับดูแล

3. ผลตอบรับจากคณะกรรมการตรวจสอบและความเสี่ยง ผู้บริหารระดับสูง คณาจารย์ และพนักงาน

4. ความคิดเห็นที่ไม่เป็นทางการและเป็นทางการ ความคิดเห็นที่ร้องขอและไม่พึงประสงค์จากผู้มีส่วนได้ส่วนเสีย

5. การตรวจสอบเป็นระยะอย่างเป็นทางการดำเนินการโดยผู้อำนวยการฝ่ายบริการความเสี่ยงและการประกันภัยโดยใช้มาตรฐานอุตสาหกรรมและแบบจำลองที่มีวุฒิภาวะ

6. การทบทวนและผลการตรวจสอบภายใน

ขั้นตอนที่ 5 การสื่อสารและการให้คำปรึกษา (communication and consultation) โครงสร้างการรายงานสำหรับกระบวนการบริหารความเสี่ยงองค์กรในฐานะที่เป็นส่วนหนึ่งของกรอบการกำกับดูแลที่เข้มแข็งและเพื่อสนับสนุนการจัดการความเสี่ยงที่มหาวิทยาลัยคาร์ลตัน การรายงานข้อมูลความเสี่ยงในเวลาที่เหมาะสมและมีความหมายเป็นสิ่งสำคัญการรายงานความเสี่ยงที่สำคัญขององค์กรสนับสนุนการตัดสินใจและรับรองว่าความเสี่ยงได้รับการจัดการตามกรอบการบริหารความเสี่ยงรายงานการจัดการความเสี่ยงได้รับการปรับอย่างรอบคอบตามความต้องการของผู้ใช้ข้อมูลความเสี่ยง ข้อมูลต้องกระชับ ไม่คลุมเครือเป็นมาตรฐาน สอดคล้องกัน และรวมเข้ากับกระบวนการรายงานที่มีอยู่

2.4 Indiana University: IU – ประเทศสหรัฐอเมริกา

2.4.1 วัตถุประสงค์การบริหารความเสี่ยง (risk management objectives)

การดำเนินการของมหาวิทยาลัยอินเดียนากับการบริหารความเสี่ยงองค์กร เริ่มขึ้นอย่างเป็นทางการเมื่อ พ.ศ. 2555 ในขณะนั้นสมาชิกหลายคนของคณะกรรมการมูลนิธิมหาวิทยาลัยอินเดียนาเป็นผู้บริหารในองค์กรท้องถิ่น การบริหารความเสี่ยงองค์กรนำมาใช้ในทศวรรษที่ผ่านมา สมาชิกเหล่านี้เคยร้องขอให้ IU ดำเนินการสร้างโปรแกรม ERM ซ้ำแล้วซ้ำเล่า เนื่องจากประสบการณ์เชิงบวกของพวกเขาในองค์กรของตนเอง

COSO ERM Framework ถูกนำมาใช้เป็นกรอบการบริหารความเสี่ยงของมหาวิทยาลัยอินเดียนา เนื่องจากสมาชิกคณะกรรมการหลายคนคุ้นเคยกับ COSO ERM Framework ผู้ตรวจสอบภายในของมหาวิทยาลัยมีความคุ้นเคยกับกรอบการควบคุมภายในของ COSO ที่เกี่ยวข้อง และมีแหล่งข้อมูลมากมายจากที่ปรึกษาและโลกธุรกิจเกี่ยวกับวิธีการนำโปรแกรม ERM มาใช้

COSO ERM ถูกมองว่าเป็นแนวทางในการสร้างโครงสร้างที่ครอบคลุมซึ่งจะช่วยให้ผู้บริหารมหาวิทยาลัยสามารถจัดการกับความเสี่ยงและโอกาสสูงสุดในภารกิจและกลยุทธ์และวัตถุประสงค์ขององค์กรในขณะที่ยังช่วยให้การดำเนินงานของมหาวิทยาลัยยอมรับความเสี่ยงได้ เครื่องมือการจัดการเพื่อจัดการความเสี่ยงและโอกาสของหน่วยธุรกิจเจ้าภาพความเสี่ยงสามารถยกระดับให้กับกระบวนการ ERM ได้อย่างง่ายดาย ความเสี่ยงใด ๆ ที่พวกเขาระบุในพื้นที่ของตนเองที่ส่งผลต่อวัตถุประสงค์ของมหาวิทยาลัยโดยรวม

2.4.2 กรอบการบริหารความเสี่ยง (risk management framework)

ใน พ.ศ. 2555 คณะกรรมการได้อนุมัติโครงสร้างการบริหารความเสี่ยงองค์กรเบื้องต้น รวมถึงบทบาทและความรับผิดชอบ และปฏิบัติตามกรอบงาน COSO ERM คณะกรรมการบริหารความเสี่ยงองค์กร (ERMC) ซึ่งประกอบด้วยสมาชิกของทีมผู้บริหารของมหาวิทยาลัยเริ่มประชุมทุกเดือน ประการแรก ERMC ระบุหน้าที่ทางธุรกิจ 18 ส่วนหรือพื้นที่เสี่ยงที่ต้องทำงานได้ดีเพื่อให้ IU สามารถบรรลุภารกิจและวัตถุประสงค์เชิงกลยุทธ์ได้ และมอบหมายเจ้าภาพความเสี่ยงให้กับแต่ละพื้นที่ความเสี่ยง โดยทั่วไปแล้ว เจ้าภาพความเสี่ยงจะอยู่ที่ระดับรองประธานหรือผู้อำนวยการ

เจ้าภาพความเสี่ยงแต่ละรายต้องผ่านกระบวนการระบุความเสี่ยงที่เป็นเวลา 90 นาทีกับหัวหน้าเจ้าหน้าที่ความเสี่ยง เพื่อระบุความเสี่ยงระดับองค์กร 3-5 อันดับแกในพื้นที่นั้น ซึ่งเป็นความเสี่ยงที่อาจทำให้ IU ไม่บรรลุภารกิจขององค์กรและวัตถุประสงค์หลัก เจ้าภาพความเสี่ยงจะร่างความเสี่ยงเหล่านั้นไว้ในเอกสารรายงาน รวมถึงการประเมินความเป็นไปได้และผลกระทบ และคำอธิบายของการบรรเทาผลกระทบในอดีต ปัจจุบัน และอนาคตตามที่ต้องการ จากนั้นเจ้าภาพความเสี่ยงแต่ละคนจะเข้าร่วมการประชุม ERMC เพื่อหารือเกี่ยวกับรายงานของตน การสนทนา 1 ชั่วโมงของ ERMC กับเจ้าภาพความเสี่ยงแต่ละรายเป็นส่วนที่มีค่าที่สุดของการนำ ERM ไปปฏิบัติจริง ไม่เพียงแต่มีการพูดคุยถึงความเสี่ยงและประสิทธิผลของการบรรเทาผลกระทบเท่านั้น แต่หลายครั้งการสนทนาเกี่ยวกับความเสี่ยงเหล่านี้พัฒนาเป็นบทสนทนาเกี่ยวกับความเป็นไปได้ในการเปลี่ยนความเสี่ยงเหล่านั้นให้เป็นโอกาส

การอภิปรายส่งผลให้มีการดำเนินการที่เป็นไปได้อย่างน้อย 3 อย่าง ดังนี้

1. ERMC ยอมรับรายงานของเจ้าภาพความเสี่ยงเพื่อเป็นตัวแทนความเสี่ยงที่ถูกต้องและมีระดับการบรรเทาความเสี่ยงที่เหมาะสม

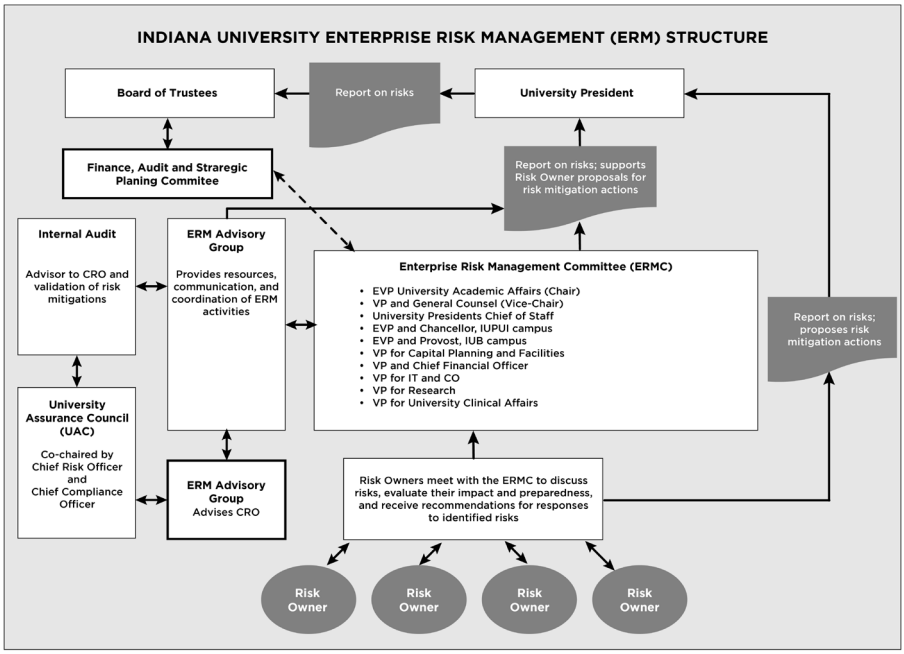
2. ERMC ตัดสินใจที่จะติดตามความเสี่ยงอย่างน้อย 1 อย่าง ซึ่งมักจะเป็นสถานการณ์ที่มีการวางแผนบรรเทาผลกระทบ แต่ยังอยู่ระหว่างดำเนินการหรือยังไม่ได้เริ่ม เจ้าภาพความเสี่ยงต้องรายงานกลับเป็นระยะเกี่ยวกับความคืบหน้าและประสิทธิผลของการบรรเทาผลกระทบ

3. ERMC ขอให้รวมความเสี่ยงเพิ่มเติม การดำเนินการเพิ่มเติมที่จะเกิดขึ้น หรือมุมมองที่แตกต่างเพื่อนำมาพิจารณา ซึ่งมักเกิดขึ้นในสถานการณ์ที่ความเสี่ยงจำเป็นต้องมีหลายหน่วยงานทางธุรกิจเพื่อทำงานร่วมกัน ซึ่ง ERMC เรียกว่าเป็นความเสี่ยงข้ามสายงาน

ในกรณีดังกล่าว Chief Risk Officer (CRO) หรือ Chief Compliance Officer (CCO) จะรวบรวมผู้เชี่ยวชาญที่เหมาะสมเพื่อวิเคราะห์ปัญหาและเสนอแผนกลับไปที่ ERMC เมื่อยอมรับแผนแล้ว การดำเนินการจะย้ายไปยังขั้นตอนการตรวจสอบ ในบางกรณี เจ้าภาพความเสี่ยงถูกขอให้พิจารณาความเสี่ยงจากมุมมองที่ต่างออกไป ทำให้ต้องมีการประเมินแผนการบรรเทาความเสี่ยงอีกครั้งเพื่อเปลี่ยนความเสี่ยงให้เป็นโอกาส

หลังจากตรวจสอบพื้นที่เสี่ยงทั้ง 18 ด้านแล้ว ERMC จะประเมินความเสี่ยงที่รวบรวมไว้ทั้งหมดเกี่ยวกับโอกาสและความรุนแรงของมาตรการผลกระทบ 6 ประการ และเลือกความเสี่ยงขององค์กรที่สำคัญที่จะมุ่งเน้นในปีที่จะมาถึง ท่ามกลางรูปแบบอื่น ๆ ของการวิเคราะห์ ความเสี่ยงที่สำคัญขององค์กรเหล่านี้ถูกวางแผนกับแผนกลยุทธ์ของสถาบันในปัจจุบัน และกลุ่มของผู้เชี่ยวชาญเฉพาะเรื่องจะถูกเรียกประชุมเพื่อทำการวิเคราะห์ Bow Tie เพื่อระดมความคิดถึงสาเหตุ ผลที่ตามมา และการบรรเทาปัญหาที่อาจเกิดขึ้น

นอกจากนี้กระบวนการยังได้วิเคราะห์สภาพแวดล้อม (environmental scan) ในทุก ๆ เดือน เพื่อช่วยให้พวกเขาตามทันแนวโน้ม ความเสี่ยง และโอกาสที่อาจส่งผลกระทบต่อ IU ในอนาคต การรับรู้ความเสี่ยงและแนวโน้มที่เพิ่มขึ้นนี้ช่วยปรับปรุงการตัดสินใจทั้งในระยะสั้นและระยะยาว รายงานที่ส่งไปยังคณะกรรมการมูลนิธิมักได้รับบ่อยขึ้นในช่วงปีเริ่มต้นของโครงการ นอกจากนี้ฝ่ายตรวจสอบภายในยังใช้ประโยชน์จากข้อมูล ERM ในกระบวนการประเมินความเสี่ยงประจำปีซึ่งใช้ในการสร้างแผนการตรวจสอบสำหรับปีถัดไป และทำให้แน่ใจว่าแผนการตรวจสอบประจำปีครอบคลุมพื้นที่ความเสี่ยงด้าน ERM รวมถึงแผนลดความเสี่ยงด้าน ERM ที่เพิ่งสร้างเสร็จ หลายครั้งที่เจ้าภาพความเสี่ยงสามารถใช้ผลการประเมินความเสี่ยงด้านการตรวจสอบภายในประจำปีนี้เพื่อเสริมข้อมูลในรายงาน ERM ของตน อย่างน้อยก็สำหรับความเสี่ยงที่ตรวจสอบได้ เจ้าภาพความเสี่ยงจะได้รับแจ้งในระหว่างกระบวนการ ERM ให้รวมความเสี่ยงที่ไม่สามารถตรวจสอบได้ (โดยทั่วไปคือความเสี่ยงด้านชื่อเสียงและเชิงกลยุทธ์) ในการประเมิน ERM นอกจากนี้ฝ่ายตรวจสอบภายในได้เปลี่ยนรูปแบบการรายงานของคณะกรรมการเพื่อให้ตรงกับคำศัพท์ ERM และพื้นที่เสี่ยง



รูปที่ 13 โครงสร้างการบริหารความเสี่ยงทั่วทั้งองค์กรของ Indiana University

2.4.3 กระบวนการบริหารความเสี่ยง (risk management process)

มหาวิทยาลัยอินเดียนาไม่ได้เริ่มต้นด้วยการทำงานตามลำดับในแต่ละองค์ประกอบของลูกบาศก์ COSO แต่ผู้นำจะวิเคราะห์ว่าพวกเขาต้องการคุณค่าใดจากกระบวนการและตัดสินใจว่าส่วนใดทำงานได้ดีที่สุดสำหรับสถาบันในช่วงเริ่มต้นของการดำเนินการจากด้านหน้าของลูกบาศก์ COSO ERM ในรูปที่ 14 IU ตัดสินใจที่จะใช้ส่วนประกอบต่าง ๆ ให้ได้มากที่สุด เนื่องจากองค์ประกอบทั้งแปดนี้เป็นรากฐานสำหรับโปรแกรมการจัดการความเสี่ยงที่ครบถ้วนสมบูรณ์ อย่างไรก็ตาม องค์ประกอบบางอย่าง (การตั้งค่าวัตถุประสงค์ การระบุเหตุการณ์การประเมินความเสี่ยง การตอบสนองต่อความเสี่ยงและการตรวจสอบ) ได้นำไปใช้ในเชิงลึกมากกว่าองค์ประกอบอื่น ๆ (สภาพแวดล้อมภายใน กิจกรรมการควบคุม และข้อมูลและการสื่อสาร)

รูปที่ 14 ลูกบาศก์ COSO

สำหรับด้านบนสุดของลูกบาศก์ COSO มหาวิทยาลัยได้ปรับแต่งหมวดหมู่วัตถุประสงค์ COSO ให้เหมาะสมกับสภาพแวดล้อมของอุดมศึกษา แทนที่จะใช้กลยุทธ์ (strategy) การปฏิบัติงาน (operations) การรายงาน (reporting) และการปฏิบัติตามข้อกำหนด (compliance) แต่ IU ใช้กลยุทธ์ (strategy) การปฏิบัติงาน (operations) การเงิน (finance) การปฏิบัติตามข้อกำหนด (compliance) และชื่อเสียง (reputation) ในขณะที่ตระหนักดีถึงการโต้เถียงเกี่ยวกับการเรียกความเสี่ยงจากชื่อเสียงว่าเป็นหมวดหมู่ของวัตถุประสงค์ (หลายคนยืนยันว่าชื่อเสียงนั้นเป็นผลมาจากการเกิดความเสี่ยง) ในที่สุดผู้บริหารของ IU ก็ตัดสินใจจัดหมวดหมู่ดังกล่าวเพราะชื่อเสียง ผ่านการรับรอง การจัดอันดับ สถิติของรัฐบาล และประเภทอื่น ๆ ของการทบทวนที่เป็นกุญแจสู่ความสำเร็จหรือความล้มเหลวในระบบอุดมศึกษา สิ่งสำคัญคือต้องแน่ใจว่าเจ้าภาพความเสี่ยงได้พิจารณาและวิเคราะห์ความเสี่ยงประเภทนี้อย่างชัดเจนในระดับองค์กร

2.5 University of Otago: UO – ประเทศนิวซีแลนด์

2.5.1 วัตถุประสงค์การบริหารความเสี่ยง (risk management objectives)

เพื่อสรุปความมุ่งมั่นและแนวทางการบริหารความเสี่ยงของมหาวิทยาลัย มหาวิทยาลัยโอทาโกได้กำหนดแนวทางในการบูรณาการ แนวทางการบริหารความเสี่ยงทั่วทั้งมหาวิทยาลัย และส่งเสริมสภาพแวดล้อมที่บุคลากรรับผิดชอบในการบริหารความเสี่ยง โปรแกรมการจัดการความเสี่ยงแบบมีโครงสร้างจะให้ผลลัพธ์ที่เป็นประโยชน์หลายประการในด้านต่อไปนี้

1. ปรับปรุงการวางแผนเชิงกลยุทธ์ผ่านการระบุภัยคุกคามต่อภารกิจของมหาวิทยาลัย

2. ส่งเสริมแนวทางเชิงรุกในประเด็นที่น่าจะมีผลกระทบต่อวัตถุประสงค์เชิงกลยุทธ์และการดำเนินงานของมหาวิทยาลัย

3. ปรับปรุงคุณภาพของการตัดสินใจ โดยจัดให้มีวิธีการที่มีโครงสร้างสำหรับการสำรวจภัยคุกคาม โอกาส และการจัดสรรทรัพยากร

นโยบายการจัดการความเสี่ยงนี้ใช้กับบุคลากรทุกคนและทุกสาขาของหน่วยงานมหาวิทยาลัย ซึ่งรวมถึงกิจกรรมทางวิชาการ การวิจัย การบริหาร โครงการ และกิจกรรมเชิงพาณิชย์ ในกรณีที่มีการพัฒนานโยบายหรือขั้นตอนการบริหารความเสี่ยงโดยละเอียดมากขึ้นเพื่อให้ครอบคลุมพื้นที่เฉพาะของการดำเนินงานของมหาวิทยาลัย (เช่น การประกันภัย สุขภาพและความปลอดภัย กิจกรรมเชิงพาณิชย์) นโยบายเหล่านั้นควรปฏิบัติตามคำแนะนำที่มีรายละเอียดอยู่ในนโยบายนี้ โดยคณะกรรมการที่เกี่ยวข้องมีหน้าที่กำหนดกรอบและกระบวนการของนโยบายการบริหารความเสี่ยงของตนเอง และจะจัดทำรายงานเกี่ยวกับความเสี่ยงต่อรองอธิการบดีและคณะกรรมการตรวจสอบและความเสี่ยงตามคำขอและทุกต้นปีปฏิทิน

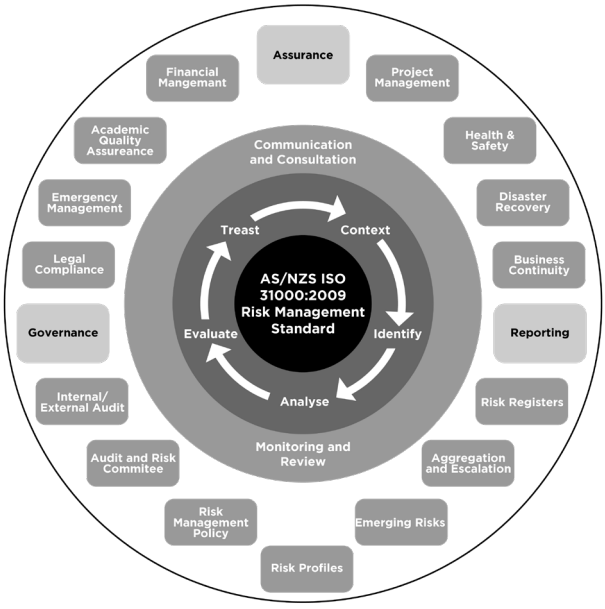
2.5.2 กรอบการบริหารความเสี่ยง (risk management framework)

กรอบการบริหารความเสี่ยง เป็นพื้นฐานสำหรับการพัฒนาและดำเนินการตามกิจกรรมที่ประสานกันเพื่อตอบสนองต่อความเสี่ยงที่อาจส่งผลต่อความสามารถของมหาวิทยาลัยในการบรรลุภารกิจและวัตถุประสงค์เชิงกลยุทธ์ โดยกรอบการบริหารความเสี่ยงจะสรุปแผน ความสัมพันธ์ ความรับผิดชอบ ทรัพยากร กระบวนการ และ

กิจกรรมที่จำเป็นต้องดำเนินการเพื่อจัดการความเสี่ยง ซึ่งกรอบนี้ยึดตามมาตรฐานการจัดการความเสี่ยงของออสเตรเลีย/นิวซีแลนด์ AS/NZS ISO 31000:2009 ซึ่งกำหนดไว้ดังนี้

1. วิธีการสำหรับการระบุ การประเมิน และการจัดการความเสี่ยง
2. ความรับผิดชอบในการบริหารความเสี่ยงทั่วทั้งมหาวิทยาลัย
3. ความรับผิดชอบในการกำกับดูแลกิจการที่ดี
4. กลไกในการรายงานข้อมูลความเสี่ยงอย่างเป็นทางการ

องค์ประกอบสำคัญของกรอบงานสรุปไว้ในแผนภาพต่อไปนี้



รูปที่ 15 กรอบการบริหารความเสี่ยงของ University of Otago

กรอบการทำงานนี้ใช้กับธุรกิจทุกด้านของมหาวิทยาลัย ซึ่งรวมถึงกิจกรรมทางวิชาการ การวิจัย การบริหาร โครงการ และกิจกรรมเชิงพาณิชย์ หน่วยงานมีหน้าที่รับผิดชอบในกิจกรรมการบริหารความเสี่ยงของตนเองและจัดทำรายงานสถานะความเสี่ยงต่อคณะกรรมการตรวจสอบและความเสี่ยงของมหาวิทยาลัยเป็นประจำทุกปีและตามคำขอของคณะกรรมการ

เชื่อมโยงการจัดการความเสี่ยงกับกระบวนการวางแผนของมหาวิทยาลัย – ให้แนวทางที่มีโครงสร้างในการระบุและจัดการความเสี่ยงที่อาจส่งผลกระทบต่อวัตถุประสงค์เชิงกลยุทธ์และการดำเนินงานของมหาวิทยาลัยดังนี้

1. ปรับปรุงคุณภาพของการตัดสินใจโดยจัดให้มีวิธีการและแนวทางในการสำรวจภัยคุกคามและโอกาส

2. สนับสนุนวัฒนธรรมการเปิดกว้างที่ส่งเสริมให้บุคลากรระบุความเสี่ยงและตอบสนองอย่างเหมาะสม

3. ส่งเสริมวัฒนธรรมความเป็นเลิศด้านบรรษัทภิบาลที่แข็งแกร่งและมีจริยธรรม

4. ให้การรับรองแก่รองอธิการบดีและสภาว่ามีการจัดการความเสี่ยงที่สำคัญ

5. ช่วยให้มั่นใจว่าผู้ผลิตและผู้รับเหมาตระหนักถึงความคาดหวังของมหาวิทยาลัยเกี่ยวกับความเสี่ยง

ทั้งนี้การกำกับดูแลความเสี่ยง (risk governance) หมายถึง วัฒนธรรมและการจัดการที่มหาวิทยาลัยพัฒนาขึ้นเพื่อจัดการความเสี่ยง เพื่อให้บรรลุภารกิจและวัตถุประสงค์เชิงกลยุทธ์ ซึ่งรวมถึงความเป็นผู้นำ ความรับผิดชอบ การกำกับดูแล และเป็นส่วนสำคัญของความรับผิดชอบในการกำกับดูแลโดยรวมของมหาวิทยาลัย ในส่วนของการกำกับดูแลความเสี่ยงประกอบไปด้วยองค์ประกอบดังนี้

1. ระดับความเสี่ยงที่ยอมรับได้ (risk appetite) ความเสี่ยงที่ยอมรับได้ของมหาวิทยาลัย คือ มุมมองร่วมกันของสภา คณะกรรมการ และทีมผู้นำอาวุโส และอ้างอิงถึงประเภทและปริมาณความเสี่ยงที่มหาวิทยาลัยเตรียมพร้อมที่จะยอมรับหรือหลีกเลี่ยงเพื่อให้บรรลุวัตถุประสงค์เชิงกลยุทธ์ ยิ่งไปกว่านั้น คำแถลงความเสี่ยงมีอิทธิพลและเป็นแนวทางในการตัดสินใจ ชี้แจงเจตนาเชิงกลยุทธ์ และช่วยให้มั่นใจว่าตัวเลือกต่าง ๆ สอดคล้องกับความสามารถและความสามารถของมหาวิทยาลัย ในการดำเนินตามวิสัยทัศน์ พันธกิจ และวัตถุประสงค์เชิงกลยุทธ์ มหาวิทยาลัยจะยอมรับระดับความเสี่ยงตามสัดส่วนของผลประโยชน์ที่คาดว่าจะได้รับ และผลกระทบหรือแนวโน้มที่จะเกิดความเสียหาย

โดยมหาวิทยาลัยต้องการความเสี่ยงสูงในบริบทของ

1) จัดการชื่อเสียงในฐานะมหาวิทยาลัยที่เน้นการวิจัยในระดับนานาชาติ

2) ส่งเสริมการคิดอย่างมีวิจารณญาณและความเป็นอิสระทางปัญญา

แต่มหาวิทยาลัยต้องการความเสี่ยงในระดับที่ต่ำในเรื่องของ

1) ชื่อเสียงหรือความเสียหายที่สำคัญทางการเงิน

2) เรื่องเป็นอันตรายต่อนักเรียน เจ้าหน้าที่ ผู้ร่วมงาน หรือผู้มาเยือน

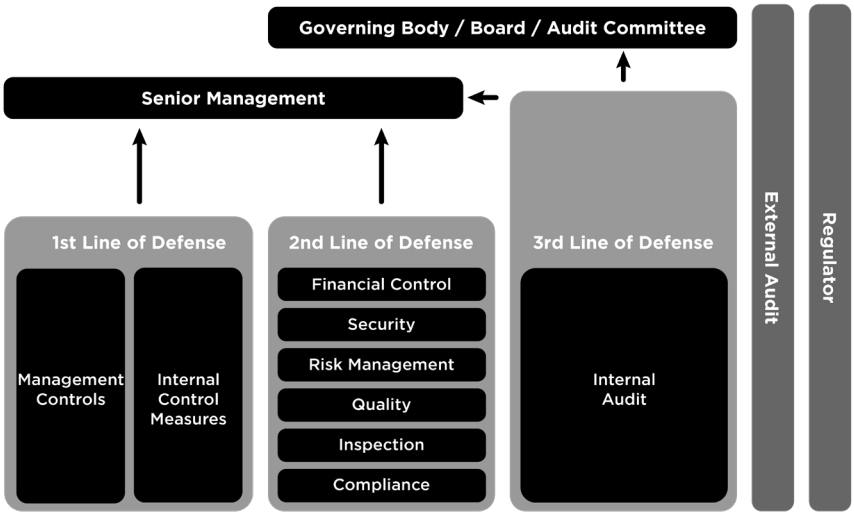
3) การกระทำหรือผลลัพธ์ที่ผิดกฎหมายหรือผิดจรรยาบรรณ

2. โมเดลสามด่านป้องกัน (Three Lines of Defense Model) โมเดลนี้ได้รับการออกแบบมาเพื่อให้แน่ใจว่าการจัดการความเสี่ยงมีประสิทธิภาพและโปร่งใส โดยการทำให้ความรับผิดชอบชัดเจน ทั้งสามสายงานมีบทบาทที่แตกต่างกันในการกำกับดูแลและในการกำกับดูแลของมหาวิทยาลัย สภา คณะกรรมการ และผู้บริหารระดับสูงเป็นผู้มีส่วนได้ส่วนเสียหลักที่ทำหน้าที่โดยสายงานที่จัดตั้งขึ้น และอยู่ในฐานะที่จะมั่นใจได้ว่าแนวป้องกันทั้งสามนั้นสะท้อนให้เห็นในกระบวนการควบคุมการจัดการความเสี่ยงของมหาวิทยาลัย

1) ด่านป้องกันแรก (1st line of defense) เกี่ยวข้องกับการดำเนินงานของมหาวิทยาลัย โดยเกี่ยวข้องโดยตรงกับการจัดการด้านวิชาการและการปฏิบัติงาน ซึ่งมีความรับผิดชอบในการประเมิน ควบคุม และลดความเสี่ยงโดยตรง

2) ด่านป้องกันที่สอง (2nd line of defense) ประกอบด้วยหน้าที่กำกับดูแลและสนับสนุน เช่น การบริหารความเสี่ยง การปฏิบัติตามข้อกำหนด คุณภาพ การเงิน

3) ด่านป้องกันที่สาม (3rd line of defense) การตรวจสอบภายในการตรวจสอบจากภายนอก หน่วยงานกำกับดูแล และผู้ให้บริการด้านการรับรอง ซึ่งเป็นอิสระจากแนวป้องกันที่หนึ่งและที่สอง



รูปที่ 16 โมเดลสามด่านป้องกัน (Three Lines of Defense Model)

3. คณะกรรมการตรวจสอบและคณะกรรมการความเสี่ยง (Audit & Risk Committee) ในการประชุมแต่ละครั้งของคณะกรรมการตรวจสอบและบริหารความเสี่ยงจะมีการจัดทำรายงานสถานะระดับสูงและความเห็นเกี่ยวกับการบริหารความเสี่ยงเป็นส่วนหนึ่งของการรายงานมาตรฐานต่อคณะกรรมการ นอกจากนี้ความเสี่ยงที่ประเมินว่าสูงหรือรุนแรงจะรายงานต่อคณะกรรมการผ่านทางทะเบียนความเสี่ยงองค์กร ซึ่งจะรวมความเสี่ยงที่สำคัญและรวมจากทะเบียนย่อยที่เก็บจัดการไว้สำหรับแผนก โครงการ สุขภาพและความปลอดภัย และการปฏิบัติตามกฎหมาย

4. นโยบายการบริหารความเสี่ยง (Risk Management Policy) นโยบายการบริหารความเสี่ยงจะระบุถึงเจตนารมณ์ของมหาวิทยาลัยในส่วนที่เกี่ยวกับการบริหารความเสี่ยงและอธิบายการจัดการและความคาดหวังในการกำกับดูแล ให้คำแนะนำและช่วยชี้แจงความคาดหวังเกี่ยวกับทัศนคติ ความตระหนัก และความรับผิดชอบที่เกี่ยวข้องกับการบริหารความเสี่ยง สำเนานโยบายการบริหารความเสี่ยงอยู่ในคลังนโยบายบนเว็บไซต์ของมหาวิทยาลัย

2.5.3 บทบาทและความรับผิดชอบในการบริหารความเสี่ยง (roles & responsibilities)

มหาวิทยาลัยโอทาโกมีบุคคล กลุ่มบุคคล หรือหน่วยงานที่เกี่ยวข้องในการบริหารความเสี่ยงตามกรอบการบริหารความเสี่ยงให้เป็นระบบและมีประสิทธิผลดังต่อไปนี้

1. สภามหาวิทยาลัย (University Council) มีความรับผิดชอบโดยรวมสำหรับการบริหารความเสี่ยง รวมถึงความรับผิดชอบในการกำกับดูแลกิจกรรมการบริหารความเสี่ยงต่อคณะกรรมการตรวจสอบความเสี่ยง และความรับผิดชอบในการดำเนินการตามกรอบการบริหารความเสี่ยงต่อรองอธิการบดี

2. ฝ่ายตรวจสอบภายใน (Internal Audit) ทำหน้าที่

1) ทบทวนความเพียงพอและประสิทธิผลของกรอบการบริหารความเสี่ยงและกระบวนการบริหารความเสี่ยงที่เกี่ยวข้องอย่างสม่ำเสมอ

2) รายงานผลต่อคณะกรรมการตรวจสอบและบริหารความเสี่ยง

3. เจ้าภาพความเสี่ยง (Risk Owners) ทำหน้าที่

1) ติดตามสถานะความเสี่ยงที่ได้รับมอบหมาย

2) ให้คำแนะนำแก่เจ้าของทะเบียนความเสี่ยงเกี่ยวกับความเหมาะสมของการตอบสนองต่อความเสี่ยงและมาตรการควบคุม

3) ยืนยันว่ามาตรการควบคุมและบรรเทาความเสี่ยงอยู่ในสถานที่และทำงานอย่างมีประสิทธิภาพ

4. เจ้าภาพในการดำเนินการ (Action Owners) ทำหน้าที่

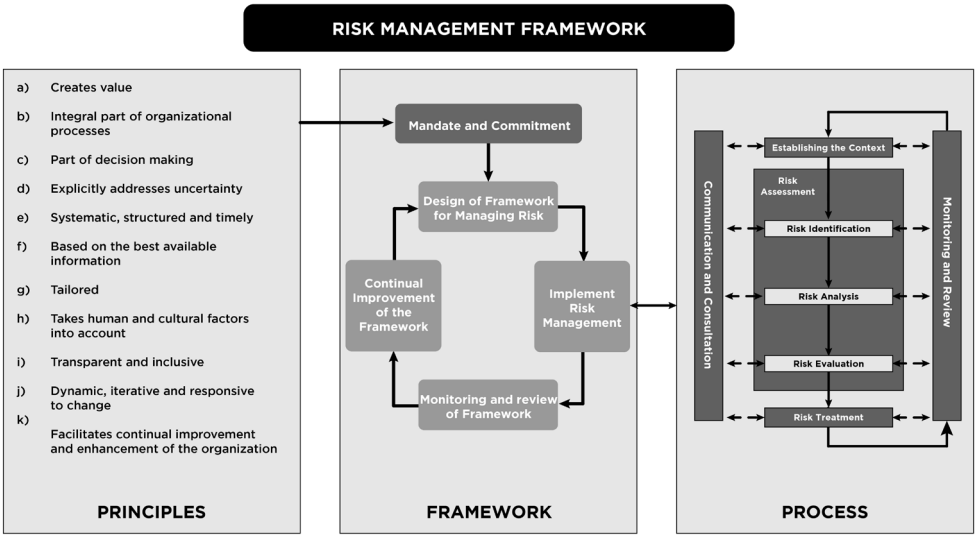
1) แจ้งเจ้าภาพความเสี่ยงในประเด็นที่เกี่ยวข้องกับการดำเนินการตามที่ได้รับมอบหมาย

2) จัดการและจัดสรรทรัพยากรเพื่อให้แน่ใจว่าการดำเนินการบรรเทาผลกระทบที่พวกเขารับผิดชอบได้ดำเนินการและเสร็จสิ้นภายในกรอบเวลาที่ระบุ

3) อัปเดตความเสี่ยงที่ได้รับมอบหมายในทะเบียนความเสี่ยงที่อยู่ใน OURDrive เมื่อเกิดขึ้นหรือในเวลาที่รายงานรายไตรมาสต่อคณะกรรมการตรวจสอบและคณะกรรมการความเสี่ยง

2.5.4 กระบวนการบริหารความเสี่ยง (risk management process)

กระบวนการบริหารความเสี่ยงของมหาวิทยาลัย สามารถสรุปได้ดังรูปที่ 17 ซึ่งมาจากมาตรฐานการจัดการความเสี่ยง AS/NZS ISO 31000:2009 หลักการของการบริหารความเสี่ยงรวมอยู่ในกรอบการทำงานที่ใช้กระบวนการที่มีโครงสร้างสำหรับการระบุ การจัดการ และการสื่อสารความเสี่ยง



รูปที่ 17 กรอบการบริหารความเสี่ยงของ University of Otago

ขั้นตอนที่ 1 กำหนดบริบท (establishing the context) คือ การกำหนดบริบทภายนอก ภายใน และการจัดการความเสี่ยง ซึ่งกระบวนการที่เหลือจะเกิดขึ้น อ้างอิงหมวดหมู่ความเสี่ยง เช่น ข้อกำหนดทางกฎหมายหรือข้อบังคับ และวัตถุประสงค์ที่จะบรรลุ เครื่องมือและทรัพยากรในขั้นตอนนี้ ได้แก่

1. แผนปฏิบัติการหรือยุทธศาสตร์
2. ข้อมูลทางการเงิน
3. ข้อมูลผู้มีส่วนได้ส่วนเสีย
4. ผู้เชี่ยวชาญเฉพาะเรื่อง

5. เวิร์กชอป
6. หมวดหมู่ความเสี่ยง

ขั้นตอนที่ 2 การระบุความเสี่ยง (risk identification) เป็นการระบุตำแหน่ง เวลา สาเหตุที่เหตุการณ์สามารถป้องกันได้ หรือล่าช้า หรือเพิ่มประสิทธิภาพการบรรลุวัตถุประสงค์เชิงปฏิบัติการหรือเชิงกลยุทธ์ เครื่องมือและทรัพยากรในขั้นตอนนี้ ได้แก่

1. หมวดหมู่ความเสี่ยง
2. รายงาน การตรวจสอบ และบทวิจารณ์
3. ข้อมูล/แนวโน้มในอดีต
4. ข้อมูลผู้มีส่วนได้ส่วนเสีย
5. ผู้เชี่ยวชาญเฉพาะเรื่อง
6. เวิร์กชอป

ขั้นตอนที่ 3 การวิเคราะห์ความเสี่ยง (risk analysis) คือ การวิเคราะห์ความเสี่ยงที่ระบุเพื่อกำหนดระดับความเสี่ยงโดยธรรมชาติ ระบุและประเมินการควบคุมที่มีอยู่ ทบทวนความเป็นไปได้และการจัดอันดับผลกระทบเพื่อวัดระดับความเสี่ยงที่เหลือ เครื่องมือและทรัพยากรในขั้นตอนนี้ ได้แก่

1. ตารางการจำแนกความเสี่ยง
2. เมทริกซ์ความเสี่ยง

ขั้นตอนที่ 4 การประเมินความเสี่ยง (risk evaluation) คือ การประเมินความเสี่ยงโดยเปรียบเทียบระดับความเสี่ยงที่พบในระหว่างกระบวนการวิเคราะห์ความเสี่ยงกับประเภทความเสี่ยงที่กำหนดไว้ พิจารณาทรัพยากรที่จำเป็นในการจัดการหรือติดตามความเสี่ยง เครื่องมือและทรัพยากรในขั้นตอนนี้ ได้แก่

1. การประเมินต้นทุน/ผลประโยชน์
2. คำชี้แจงความเสี่ยง
3. หมวดหมู่ความเสี่ยง

ขั้นตอนที่ 5 การจัดการความเสี่ยง (risk treatment) คือ การพัฒนาและใช้กลยุทธ์/การควบคุมและแผนปฏิบัติการเฉพาะเพื่อบรรเทา/ติดตามความเสี่ยง เครื่องมือและทรัพยากรในขั้นตอนนี้ ได้แก่

1. ทะเบียนความเสี่ยง
2. แผนการจัดการความเสี่ยง
3. แผนฉุกเฉิน

ขั้นตอนที่ 6 การสื่อสารและให้คำปรึกษา (communicate and consult) คือ กระบวนการต่อเนื่องในการติดตามและทบทวนประสิทธิภาพของขั้นตอนทั้งหมดในกระบวนการบริหารความเสี่ยง สื่อสารและปรึกษากับผู้มีส่วนได้ส่วนเสียภายในและภายนอก เครื่องมือและทรัพยากรในขั้นตอนนี้ ได้แก่

1. ผู้มีส่วนได้ส่วนเสีย
2. แผนการสื่อสาร
3. เวิร์กชอป
4. บทสัมภาษณ์

ขั้นตอนที่ 7 การติดตามและทบทวน (monitor and review) คือ กระบวนการต่อเนื่องในการติดตามและตรวจสอบประสิทธิภาพของขั้นตอนทั้งหมดในกระบวนการบริหารความเสี่ยง ติดตาม บันทึก และรายงานเกี่ยวกับความเสี่ยงและประสิทธิผลของมาตรการการจัดการเพื่อให้แน่ใจว่าสถานการณ์ที่เปลี่ยนแปลงจะไม่เปลี่ยนลำดับความสำคัญ เครื่องมือและทรัพยากรในขั้นตอนนี้ ได้แก่

1. รายงาน การตรวจสอบ และบทวิจารณ์
2. ทะเบียนความเสี่ยง

2.6 University of Adelaide: UA – ประเทศออสเตรเลีย

2.6.1 วัตถุประสงค์การบริหารความเสี่ยง (risk management objectives)

การบริหารความเสี่ยงของมหาวิทยาลัยแอดิเลด สอดคล้องกับมาตรฐานสากล ISO 31000: 2018 Risk Management โดยมหาวิทยาลัยนี้ใช้หลักการบริหารความเสี่ยงตามที่กำหนดไว้ในมาตรฐาน ซึ่งให้คำแนะนำเกี่ยวกับลักษณะของการจัดการความเสี่ยงที่มีประสิทธิผลการสื่อสารคุณค่าและอธิบายความตั้งใจและวัตถุประสงค์ของมหาวิทยาลัยได้เป็นอย่างดี โดยสามารถสรุปหลักการของการบริหารความเสี่ยงได้ดังนี้

1. กรอบและกระบวนการควรได้รับการปรับเปลี่ยนให้เหมาะสมกับระดับความเสี่ยงที่องค์กรต้องเผชิญ

2. การมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียอย่างเหมาะสมและทันเวลาเป็นสิ่งที่จำเป็น

3. จำเป็นต้องมีแนวทางที่มีโครงสร้างและครอบคลุม

4. การบริหารความเสี่ยงเป็นส่วนสำคัญของกิจกรรมขององค์กรทั้งหมด กิจกรรมการบริหารความเสี่ยงจะต้องสอดคล้องกับกิจกรรม/วัตถุประสงค์เชิงกลยุทธ์

5. การบริหารความเสี่ยงจะต้องเป็นแบบพลวัต (dynamic) และคาดการณ์ได้ สามารถตรวจจับ รับทราบ และตอบสนองต่อการเปลี่ยนแปลง

6. การบริหารความเสี่ยงต้องใช้ข้อมูลที่ดีที่สุดที่มีอยู่

7. ปัจจัยด้านมนุษย์และวัฒนธรรมมีอิทธิพลต่อการจัดการความเสี่ยงทุกด้าน ซึ่งควรได้รับการพิจารณา

8. การจัดการความเสี่ยงต้องได้รับการปรับปรุงอย่างต่อเนื่องผ่านการเรียนรู้และประสบการณ์

2.6.2 กรอบการบริหารความเสี่ยง (risk management framework)

กรอบการบริหารความเสี่ยงของมหาวิทยาลัยถูกออกแบบมาโดยมีวัตถุประสงค์คือ

1. เชื่อมโยงข้อบังคับหรือข้อบัญญัติกับกระบวนการ ซึ่งข้อบังคับดังกล่าวมาจากพระราชบัญญัติของมหาวิทยาลัยแอดิเลดและสภา แสดงและดูแลโดยคณะกรรมการประจำและคณะกรรมการการจัดการต่าง ๆ เช่น คณะกรรมการกำกับการปฏิบัติตามข้อกำหนดและความเสี่ยง (Audit Compliance and Risk Committee) และคณะกรรมการบริหารความเสี่ยงมหาวิทยาลัย (University Risk Management Committee)

2. ตระหนักถึงอิทธิพลและความคาดหวังของผู้ให้ทุนภายนอก หน่วยงานกำกับดูแล ผู้ตรวจสอบบัญชี และผู้ทำงานร่วมกันในการวิจัย ผ่านความเสี่ยงขององค์กรและการปฏิบัติงาน และโปรแกรมการตรวจสอบภายใน เพื่อเชื่อมโยงความคาดหวังและแรงบันดาลใจเหล่านั้นกับสิ่งที่มหาวิทยาลัยทำ

3. มีอิทธิพลต่อวัฒนธรรมที่มีอยู่เพื่อจัดการความเสี่ยงและโอกาสได้ดียิ่งขึ้น โดยคำนึงถึงสภาพแวดล้อมทางเศรษฐกิจ สังคม กฎระเบียบ การเมือง และการแข่งขันทั้งในระดับท้องถิ่น ระดับภูมิภาค และระดับสากล โดยสอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์ของมหาวิทยาลัย

4. กำหนดขอบเขตที่เหมาะสมสำหรับการรับความเสี่ยง โดยกำหนดระดับความเสี่ยงขององค์กรและระดับความเบี่ยงเบนความเสี่ยง (risk tolerance)

ทั้งนี้กรอบการบริหารความเสี่ยงของมหาวิทยาลัยแอดิเลด ประกอบด้วย 7 องค์ประกอบ ดังนี้

1. นโยบายการบริหารความเสี่ยง (risk management policy) เกี่ยวข้องกับการกำหนดหลักการ นโยบาย ขั้นตอน ความรับผิดชอบต่าง ๆ ของสถาบันและส่วนบุคคล ความต้องการและโครงสร้าง นโยบายนี้เกี่ยวข้องกับอำนาจนิติบัญญัติและบทบาทของสภามหาวิทยาลัย ซึ่งแสดงถึงความมุ่งมั่นเชิงกลยุทธ์ของมหาวิทยาลัยในการสร้างวัฒนธรรมการบริหารความเสี่ยงซึ่งทำให้การระบุโอกาสในการเกิดความเสี่ยงและจัดการเป็นไปอย่างมีประสิทธิภาพ

2. ความเสี่ยงที่ยอมรับได้ (risk appetite statement) บ่งบอกถึงความเสี่ยงที่ยอมรับได้ของมหาวิทยาลัยและระดับความทนทานต่อความเสี่ยง โดยมหาวิทยาลัยใช้คำจำกัดความสำหรับความเสี่ยงที่ยอมรับได้และการทนทานต่อความเสี่ยงที่กำหนดไว้ในมาตรฐาน ISO 31000:2018

1) risk appetite ปริมาณความเสี่ยงที่มหาวิทยาลัยยินดียอมรับหรือคงไว้เพื่อให้บรรลุเป้าหมาย

2) risk tolerance ระดับความเบี่ยงเบนความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์เฉพาะหรือจัดการประเภทของความเสี่ยง ความเสี่ยงที่ยอมรับได้เป็นตัวกำหนดความเสี่ยงโดยทั่วไป และระดับความเสี่ยงที่ยอมรับได้เป็นการบอกให้ทราบถึง

(1) ความคาดหวังในการบรรเทาและติดตามความเสี่ยงเฉพาะประเภท

(2) ขอบเขตและเกณฑ์สำหรับการรับความเสี่ยงที่ยอมรับได้

(3) การดำเนินการแก้ไขที่จะดำเนินการเมื่อถึงขีดการยอมรับได้หรือการละเมิด

risk appetite ของมหาวิทยาลัยได้รับการสื่อสารผ่านกระบวนการวางแผนเชิงกลยุทธ์เป็นหลัก โดยในการพิจารณาความเสี่ยงนั้น มหาวิทยาลัยจำเป็นต้องสร้างสมดุลระหว่างวิธีการที่ชาญฉลาดและแข็งแกร่งในการลดความเสี่ยง และเพื่อให้มีความยืดหยุ่นเพียงพอในการส่งเสริมจิตวิญญาณของผู้ประกอบการซึ่งมีส่วนอย่างมากต่อความสำเร็จของมหาวิทยาลัย

3. วิธีการจัดการความเสี่ยง (risk management methodology) เกี่ยวข้องกับการกำหนดโครงร่างของกระบวนการ เพื่อเป็นแนวทาง ชี้นำ และช่วยเหลือทุกคนให้เกิดความเข้าใจอันดีและนำกระบวนการประเมินความเสี่ยงมาใช้อย่างสม่ำเสมอ

4. ทะเบียนความเสี่ยงของมหาวิทยาลัย (University Risk Register) คือ คลังข้อมูลหลักสำหรับบันทึกและติดตามความเสี่ยง รวมถึงข้อเสนอแนะ/การดำเนินการที่ตกลงร่วมกันระหว่างผู้ตรวจสอบ หน่วยงานกำกับดูแล ผู้ประกันตน และหน่วยงานที่เกี่ยวข้อง

5. ศูนย์ความเสี่ยงของมหาวิทยาลัย (University Risk Center) ประกอบด้วย Director, Risk Services (Anne Hill) และ General Counsel and Executive Director, Legal and Risk (Céline McInerney) ในสาขากฎหมายและความเสี่ยงแผนกปฏิบัติการของมหาวิทยาลัย ซึ่งมีหน้าที่หลักในการอำนวยความสะดวกและสนับสนุนมหาวิทยาลัยในด้านการบริหารความเสี่ยง

6. คณะกรรมการบริหารความเสี่ยงของมหาวิทยาลัย (University Risk Management Committee) ซึ่งจัดประชุมโดยประธานเจ้าหน้าที่ฝ่ายปฏิบัติการและรับผิดชอบการประสานงานโดยรวมของการบริหารความเสี่ยงภายในมหาวิทยาลัยและรายงานประจำปีต่อฝ่ายบริหาร

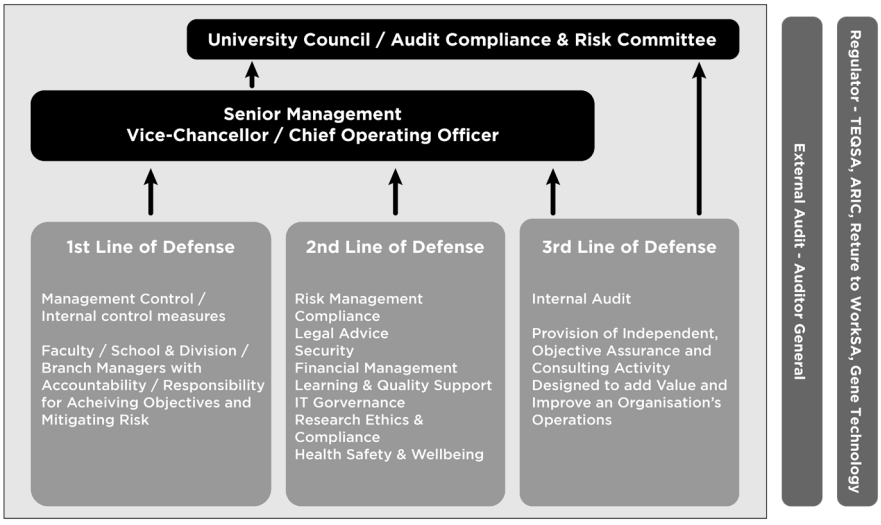
7. การติดตาม ตรวจสอบ ทบทวน และรายงานอย่างสม่ำเสมอ (regular monitoring, review and reporting) เกี่ยวข้องกับการยืนยันว่าการบริหารความเสี่ยงมีความเกี่ยวข้อง พิสูจน์ได้ มีประสิทธิภาพ และสนับสนุนวัตถุประสงค์ของธุรกิจ

เพื่อให้แน่ใจว่ากรอบการบริหารความเสี่ยงของมหาวิทยาลัยมีประสิทธิภาพ สภาและฝ่ายบริหารระดับสูงจำเป็นต้องพึ่งพาฟังก์ชันการติดตามและรับรองภายในมหาวิทยาลัย โดยใช้กระบวนการเรื่องโมเดลสามด่านป้องกัน (Three Lines of Defense Model) ในการอธิบายความสัมพันธ์ระหว่างหน้าที่เหล่านี้และทำหน้าที่เป็นแนวทางในการแบ่งความรับผิดชอบ

1. ด่านป้องกันแรก (1st line of defence) ทำหน้าที่เป็นเจ้าของและจัดการความเสี่ยง ได้แก่ คน กระบวนการ และเทคโนโลยี

2. ด่านป้องกันที่สอง (2nd line of defence) การจัดการและการกำกับดูแล ซึ่งทำหน้าที่กำกับดูแลและเชี่ยวชาญในการบริหารความเสี่ยงและการปฏิบัติตามข้อกำหนด

3. ด่านป้องกันที่สาม (3rd line of defence) การตรวจสอบภายใน ทำหน้าที่ให้การประกันโดยอิสระ



รูปที่ 18 กระบวนการเรื่องแนวทางการป้องกัน 3 ชั้น (Three Lines of Defense Model)

2.6.3 บทบาทและความรับผิดชอบในการบริหารความเสี่ยง (roles & responsibilities)

มหาวิทยาลัยแอดิเลดมีบุคคล กลุ่มบุคคล หรือหน่วยงานที่เกี่ยวข้องในการบริหารความเสี่ยงตามกรอบการบริหารความเสี่ยงให้เป็นระบบและมีประสิทธิผลดังต่อไปนี้

1. สภามหาวิทยาลัย (Council) หน่วยงานกำกับดูแลของมหาวิทยาลัย ทำหน้าที่ดูแลและติดตามการประเมินและการจัดการความเสี่ยงตามภาระหน้าที่ตามกฎหมายที่กำหนดไว้ในพระราชบัญญัติ

2. คณะกรรมการด้านความเสี่ยง (Standing Committees) ซึ่งจัดตั้งโดยสภา มีหน้าที่ในการดูแลและติดตามความเสี่ยงด้านวิชาการ วัฒนธรรม การเงิน ทรัพย์สิน การตรวจสอบ การปฏิบัติตามข้อกำหนด และความเสี่ยงทางกฎหมาย

3. รองอธิการบดีและประธานเจ้าหน้าที่ฝ่ายปฏิบัติการ (Vice-Chancellor and Chief Operating Officer (COO)) ทำหน้าที่ในการจัดการความเสี่ยง รวมถึงการวางแผน การตัดสินใจ การรายงาน และความรับผิดชอบต่าง ๆ

จากระดับการจัดการสูงสุดนี้ แต่ละแผนกซึ่งนำโดยรองอธิการบดีและ CEO จะทำงานร่วมกับคณะและหน่วยงานการบริหารต่าง ๆ เพื่อให้ความเสี่ยงได้รับการจัดการเชิงกลยุทธ์และเชิงปฏิบัติการ สำหรับหน่วยงานที่ควบคุมของมหาวิทยาลัย คณะกรรมการและผู้บริหารระดับสูงของแต่ละหน่วยงานมีหน้าที่รับผิดชอบในการจัดการความเสี่ยง การบริหารความเสี่ยงจึงเป็นความรับผิดชอบร่วมกันในคณะกรรมการกำกับดูแล ผู้บริหารและบุคลากร หน้าที่ความรับผิดชอบของผู้มีส่วนเกี่ยวข้องกับความเสี่ยงมีดังนี้

1. บุคลากรภายในมหาวิทยาลัยทั้งหมด มีหน้าที่

1) ใช้หลักการบริหารความเสี่ยงและกระบวนการเพื่อคาดการณ์และตอบสนองต่อการเปลี่ยนแปลงสถานการณ์และเหตุการณ์

2) รายงานความเสี่ยงที่รุนแรงและสูง (ประเมินโดยอ้างอิงจากตารางความเสี่ยงของมหาวิทยาลัย) ไปยังเจ้าภาพความเสี่ยงที่เกี่ยวข้องเพื่อการยกระดับและการจัดการที่เหมาะสม

3) มีส่วนร่วมในกิจกรรมการบริหารความเสี่ยงตามคำสั่งของมหาวิทยาลัยเกี่ยวกับบุคลากรซึ่งมีหน้าที่รับผิดชอบหลักรวมถึงการจัดการความเสี่ยงบางอย่าง

2 เจ้าภาพความเสี่ยง (Risk Owners) (ทั้งฝ่ายวิชาการและบริหาร) และหน่วยงานควบคุมที่เกี่ยวข้อง (คณะกรรมการและประธานเจ้าหน้าที่บริหารหรือผู้จัดการทั่วไป) มีหน้าที่

1) ส่งเสริมและสนับสนุนสภาพแวดล้อมที่การจัดการความเสี่ยงได้รับการยอมรับว่าเป็นความรับผิดชอบร่วมกัน

2) ตรวจสอบให้แน่ใจว่าหลักการและแนวปฏิบัติของการบริหารความเสี่ยงได้รับการสื่อสารและฝังอยู่ในแนวทางปฏิบัติเชิงกลยุทธ์ เชิงปฏิบัติการ และกระบวนการวางแผน

3) ก่อนที่จะได้รับอนุมัติให้ดำเนินการตามข้อเสนอ โครงการ แผนงาน ให้มั่นใจว่าการประเมินความเสี่ยงเสร็จสิ้น เพียงพอ และจะต้องอยู่ภายใต้การทบทวนอย่างต่อเนื่อง

4) ตรวจสอบให้แน่ใจว่าความเสี่ยงที่ได้รับการจัดอันดับว่าสูงมากหรือสูงจะถูกส่งต่อไปยัง Director Risk Services เพื่อบันทึกลงในทะเบียนความเสี่ยงของมหาวิทยาลัย

5) ถ่ายทอดความเสี่ยงใหม่ ๆ ที่ถือว่ามีความเสี่ยงสูงหรือรุนแรงส่งไปยังหน่วยงาน/ผู้จัดการ ที่เหมาะสม และผู้อำนวยการฝ่ายบริการความเสี่ยง

6) ติดตามและจัดการความเสี่ยง เพื่อให้ชัดเจนว่าใครเป็นผู้รับผิดชอบ มีการควบคุม จัดการความเสี่ยงเป็นปัจจุบันและมีประสิทธิภาพ และความเสี่ยงที่รุนแรงและสูงจะได้รับการเอาใจใส่อย่างเหมาะสมและมีการยกระดับอย่างรอบคอบ

7) สำหรับหน่วยงานที่ควบคุม ให้รายงานประจำปีต่อผู้อำนวยการฝ่ายบริการความเสี่ยงตามกำหนดเวลาและลักษณะที่กำหนด เพื่อรายงานต่อคณะกรรมการประจำมหาวิทยาลัยที่เกี่ยวข้อง

3. ผู้อำนวยการ (Director) ฝ่ายบริการความเสี่ยง (สาขากฎหมายและความเสี่ยง ฝ่ายปฏิบัติการมหาวิทยาลัย) มีหน้าที่

1) ประสานงานกิจกรรมการบริหารความเสี่ยงของมหาวิทยาลัยตามแนวทางปฏิบัติ นโยบายและกรอบการบริหารความเสี่ยง

2) จัดการทะเบียนความเสี่ยงของมหาวิทยาลัย (University Risk Register)

3) อำนวยความสะดวกในกระบวนการรายงานความเสี่ยงสำหรับหน่วยงานภายในและภายนอก/ผู้มีส่วนได้ส่วนเสีย

4. คณะกรรมการบริหารความเสี่ยงมหาวิทยาลัย (University Risk Management Committee) มีหน้าที่

1) ดูแลกิจการของมหาวิทยาลัยและกิจกรรมการบริหารความเสี่ยงด้านปฏิบัติการ

2) ให้คำแนะนำเกี่ยวกับกลยุทธ์ความเสี่ยง นโยบาย การจัดการและการเพิ่มระดับ

3) รายงานต่อรองอธิการบดี คณะกรรมการประจำที่เกี่ยวข้อง หน่วยงานภายนอก และผู้มีส่วนได้ส่วนเสียตามความจำเป็น

5. รองอธิการบดีมหาวิทยาลัย (Vice-Chancellor) ในฐานะผู้บริหารระดับสูงและประธานเจ้าหน้าที่บริหารของมหาวิทยาลัย รองอธิการบดี รวมทั้งอธิการบดี มีหน้าที่รับผิดชอบด้านมาตรฐานวิชาการ การจัดการ และการบริหารของมหาวิทยาลัย

6. สภามหาวิทยาลัย (University Council) สภามหาวิทยาลัยมีหน้าที่ตามกฎหมายในการกำกับดูแลและติดตามการประเมินและการจัดการความเสี่ยงทั่วทั้งมหาวิทยาลัย รวมถึงการดำเนินกิจการเชิงพาณิชย์ และในกิจกรรมทางวิชาการ กิจกรรมเชิงพาณิชย์ที่สำคัญ และหน่วยงานควบคุม

2.6.4 กระบวนการบริหารความเสี่ยง (risk management process)

กระบวนการและขั้นตอนที่อธิบายไว้ในส่วนนี้มีจุดมุ่งหมายเพื่อช่วยในการจัดการความเสี่ยง โดยคำนึงถึงสภาพแวดล้อมเฉพาะในมหาวิทยาลัย ซึ่งประกอบไปด้วย 5 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 กำหนดบริบท (establish the context) กำหนดบริบทโดยการระบุวัตถุประสงค์ของกิจกรรม จากนั้นพิจารณาตัวแปร (ภายในและภายนอก) ที่เกี่ยวข้องกับความเสี่ยงที่ต้องได้รับการจัดการ มีการใช้กระบวนการบริหารความเสี่ยงอย่างเท่าเทียมกันกับความเสี่ยงที่เกิดขึ้นในระดับองค์กรหรือระดับกลยุทธ์ ในระดับธุรกิจหรือการดำเนินงานประจำวัน หรือสำหรับโครงการใหม่ พันธมิตรทางธุรกิจ และการริเริ่มใหม่โดยโครงการ หุ้นส่วน หรือความคิดริเริ่มใด ๆ ที่เสนอควรพิจารณาความเสี่ยงอย่างจริงจังและจัดทำเอกสารการประเมินอย่างเป็นทางการตลอดวงจรชีวิตของกิจกรรมสำหรับกระบวนการในขั้นตอนการสร้างบริบท ประกอบไปด้วย

1. กำหนดขอบเขต (set the scope) สำหรับการประเมินความเสี่ยงโดยระบุสิ่งที่กำลังประเมิน เช่น เป็นหุ้นส่วนใหม่ เป็นโปรแกรมใหม่ เป็นโครงการใหม่ หรือการลงทุนใหม่หรือไม่

2. กำหนดวัตถุประสงค์แบบกว้าง (define the broad objectives) ระบุเหตุผลในการประเมินความเสี่ยง อาจเป็นการเปลี่ยนแปลงในกฎหมาย คำขอจากผู้ตรวจสอบภายนอกหรือหน่วยงานกำกับดูแล การเปลี่ยนแปลงการปฏิบัติงานหรือการทบทวน

3. ระบุผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง (identify the relevant stakeholders) เป้าหมายสำหรับกระบวนการที่ครอบคลุมอย่างเหมาะสมตั้งแต่เริ่มแรก คือ ตรวจสอบให้แน่ใจว่าได้ระบุพื้นที่ที่ได้รับผลกระทบหรืออาจได้รับผลกระทบ และค้นหาข้อมูลของพวกเขา ตรวจสอบให้แน่ใจว่าเหมาะสม มีการฝึกซ้อมการมอบอำนาจแม้ในระยะแรกนี้

4. รวบรวมข้อมูลเบื้องหลัง (gather background information) การมีข้อมูลที่ถูกต้องเป็นสิ่งสำคัญ ถามคนที่เหมาะสมและระบุข้อมูลที่มี บางครั้งการระบุข้อมูลที่ไม่พร้อมใช้งาน (ในทันที) อาจมีความจำเป็น

ขั้นตอนที่ 2 ระบุความเสี่ยง (identify the risk) เกี่ยวข้องกับการระบุแหล่งที่มาของความเสี่ยง พื้นที่ของผลกระทบ เหตุการณ์ (รวมถึงการเปลี่ยนแปลงในสถานการณ์) และสาเหตุและผลที่อาจเกิดขึ้น อธิบายปัจจัยเหล่านั้นที่อาจสร้าง ปรับปรุง ป้องกัน ลดระดับ เร่งความเร็ว หรือชะลอการบรรลุวัตถุประสงค์ของมหาวิทยาลัย ตั้งเป้าที่จะระบุปัญหาที่เกี่ยวข้องกับการไม่แสวงหาโอกาส ซึ่งถือเป็นความเสี่ยงที่เกิดจากการไม่ทำอะไรเลยและทำให้พลาดโอกาส

ขั้นตอนที่ 3 วิเคราะห์ความเสี่ยง (analyse the risk) เกี่ยวข้องกับการพัฒนาความเข้าใจโดยละเอียดเกี่ยวกับความเสี่ยง เมื่อระบุความเสี่ยงและบริบทแล้ว มีการอธิบายสาเหตุ ปัจจัยสนับสนุน และผลกระทบที่ตามมา ให้พิจารณาจุดแข็ง จุดอ่อนของระบบและกระบวนการที่มีอยู่ ซึ่งออกแบบมาเพื่อช่วยควบคุมหรือลดความเสี่ยง การรู้ว่าการควบคุมใดที่มีอยู่แล้วและมีผลหรือไม่ จะช่วยให้ระบุได้ว่าจำเป็นต้องดำเนินการใดเพิ่มเติม (ถ้ามี)

ขั้นตอนที่ 4 ประเมินความเสี่ยง (evaluate the risk) เป็นการตัดสินใจว่าความเสี่ยงเป็นที่ยอมรับหรือไม่เป็นที่ยอมรับ โดยใช้ความเข้าใจเกี่ยวกับความเสี่ยงในการตัดสินใจเกี่ยวกับการดำเนินการในอนาคต การตัดสินใจเกี่ยวกับการดำเนินการในอนาคตอาจรวมถึง

1. ไม่ดำเนินการหรือดำเนินกิจกรรม โครงการ หรือความคิดริเริ่ม
2. ปฏิบัติต่อความเสี่ยงอย่างจริงจัง
3. จัดลำดับความสำคัญของการดำเนินการที่จำเป็น หากความเสี่ยงซับซ้อนและจำเป็นต้องจัดการ
4. ยอมรับความเสี่ยง

ความเสี่ยงที่ยอมรับได้หรือไม่สามารถยอมรับได้นั้นเกี่ยวข้องกับความเต็มใจที่จะทนต่อความเสี่ยงนั้น คือความเต็มใจที่จะแบกรับความเสี่ยงหลังจากได้รับการปฏิบัติเพื่อให้บรรลุวัตถุประสงค์ที่ต้องการ ระดับที่ยอมรับได้ และความอดทนต่อความเสี่ยงนั้นมักจะแตกต่างกันไปตามช่วงเวลา คณะ สถาบัน สาขา และหน่วยงาน โดยความเสี่ยงจะถือว่ายอมรับได้หรือทนได้ หากมีการตัดสินใจที่จะไม่จัดการกับความเสี่ยง การยอมรับหรือทนต่อความเสี่ยงไม่ได้หมายความว่าความเสี่ยงนั้นไม่มีนัยสำคัญ ความเสี่ยงที่ถือว่ายอมรับได้หรือทนได้อาจยังคงต้องได้รับการตรวจสอบ เมื่อทำการประเมินความเสี่ยงโดยทั่วไปแล้วจะระบุถึงผลกระทบที่อาจเกิดขึ้นได้มากมาย

ขั้นตอนที่ 5 จัดการกับความเสี่ยง (treat the risk) คือ การตรวจสอบให้แน่ใจว่ามีการใช้กลยุทธ์ที่มีประสิทธิภาพเพื่อลดความถี่และความรุนแรงของความเสี่ยงที่ระบุ พัฒนาการดำเนินการและดำเนินการบำบัดที่มุ่งควบคุมความเสี่ยง เมื่อขั้นตอนการประเมินความเสี่ยงเสร็จสิ้น ให้ระบุทางเลือกในการจัดการ (หากมี) มิฉะนั้นจะถือเป็นการยอมรับความเสี่ยง หากมีทางเลือกในการจัดการและเหมาะสม ให้บันทึกตัวเลือกการจัดการเหล่านั้นไว้เป็นส่วนหนึ่งของแผนการจัดการความเสี่ยง

ตัวเลือกการจัดการที่ไม่ได้นำไปใช้กับแหล่งที่มาหรือสาเหตุของความเสี่ยงมักจะไม่ได้ผลและส่งเสริมความเชื่อที่ผิดพลาดภายในองค์กรว่าความเสี่ยงนั้นถูกควบคุม โดยกระบวนการในการจัดการกับความเสี่ยงมีดังต่อไปนี้

1. ตัดสินใจว่าจำเป็นต้องมีการจัดการเฉพาะหรือว่าสามารถจัดการความเสี่ยงได้อย่างเพียงพอในขั้นตอนการจัดการมาตรฐานและกิจกรรม กล่าวคือ ฝังการจัดการลงในการปฏิบัติหรือกระบวนการในแต่ละวัน ในการประเมินวิธีการจัดการที่สามารถนำมาใช้ได้จะเป็นประโยชน์ในการพิจารณาวิธีการที่แนวทางปฏิบัติมาตรฐานใช้อยู่แล้วเป็นตัวควบคุมหรือวิธีที่แนวทางปฏิบัติมาตรฐานเหล่านั้นสามารถปรับเปลี่ยนเพื่อควบคุมความเสี่ยงได้อย่างเพียงพอ

2. หาชนิดของการจัดการที่เหมาะสมสำหรับความเสี่ยงนี้ กำหนดเป้าหมายในการจัดการความเสี่ยงนี้โดยเฉพาะ คือหลีกเลี่ยงโดยสิ้นเชิง ลดโอกาสหรือผลที่ตามมา โอนความเสี่ยง (ให้กับบุคคลอื่น เช่น ผู้ประกันตนหรือผู้รับเหมา) หรือยอมรับระดับความเสี่ยงตามข้อมูลที่มีอยู่ ประเภทของการจัดการความเสี่ยงที่เลือกมักจะขึ้นอยู่กับลักษณะของความเสี่ยงและความอดทนต่อความเสี่ยงนั้น

3. ระบุและออกแบบตัวเลือกการจัดการที่ต้องการเมื่อทราบเป้าหมายของการจัดการ

4. ประเมินทางเลือกในการจัดการและประเมินความเป็นไปได้เมื่อเทียบกับความอดทนต่อความเสี่ยง เป็นการประเมินว่าการควบคุมที่เลือกดูเหมือนจะมีผลการจัดการที่ต้องการหรือไม่

1) การควบคุมจะก่อให้เกิดความเสี่ยงอื่น ๆ หรือไม่

2) การควบคุมมีประโยชน์หรือคุ้มค่าหรือไม่ ค่าใช้จ่ายในการดำเนินการควบคุมมีมากกว่าต้นทุนที่จะเกิดขึ้นจากเหตุการณ์ที่เกิดขึ้นโดยไม่มีการควบคุมหรือไม่ โดยรวมแล้วค่าใช้จ่ายในการดำเนินการควบคุมนั้นสมเหตุสมผลสำหรับความเสี่ยงนี้หรือไม่

5. จัดทำแผนการจัดการความเสี่ยง เมื่อระบุตัวเลือกการจัดการได้แล้ว ควรมีการเตรียมแผนการจัดการความเสี่ยง (หมายเหตุ สิ่งเหล่านี้สามารถสร้างขึ้นได้อย่างง่ายดายผ่านทะเบียนความเสี่ยงของมหาวิทยาลัยเพียงครั้งเดียวโดยความเสี่ยงจะถูกบันทึกไว้) แผนการจัดการควรระบุความรับผิดชอบในการดำเนินการ กรอบเวลาสำหรับการดำเนินการ ข้อกำหนดด้านงบประมาณหรือผลกระทบของทรัพยากร การวัดผลการปฏิบัติงาน และกระบวนการทบทวนตามความเหมาะสม กระบวนการทบทวนควรติดตามความคืบหน้าของการจัดการตามเหตุการณ์สำคัญในการดำเนินการ

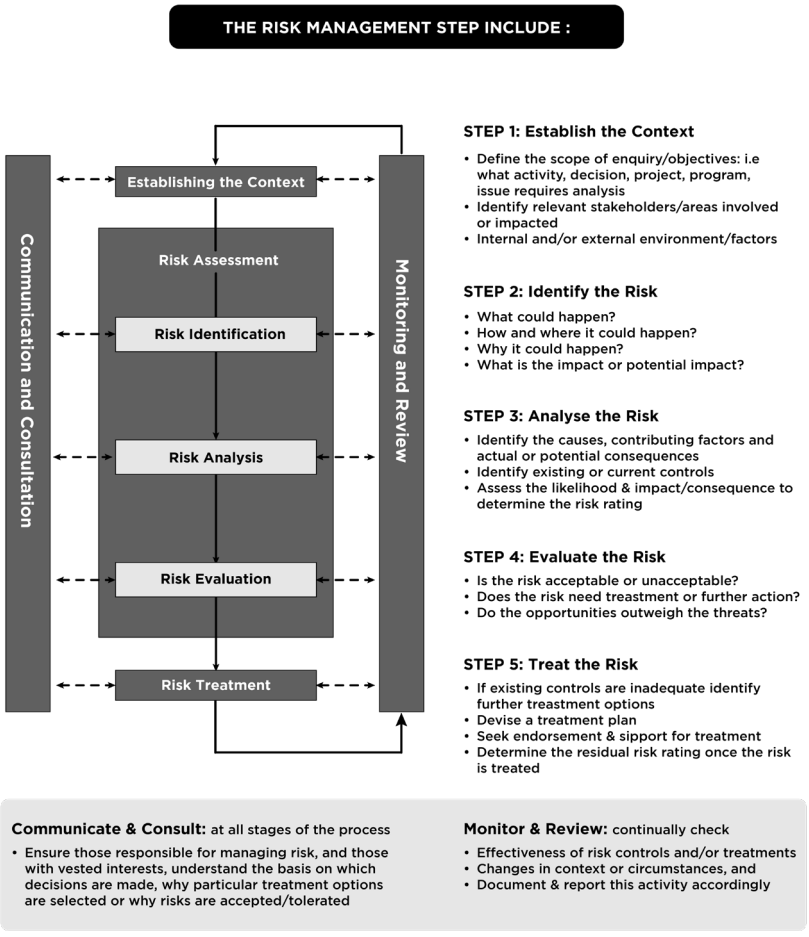
6. ดำเนินการจัดการความเสี่ยงที่ตกลงกันไว้ เมื่อมาตรการได้รับอนุมัติสำหรับการจัดหาทรัพยากร เงินทุน หรือการดำเนินการอื่น ๆ ได้รับการอนุมัติแล้ว การบำบัดควรดำเนินการโดยผู้ที่ระบุว่ามีหน้าที่รับผิดชอบในการดำเนินการดังกล่าว บุคคลที่ได้รับมอบหมายให้รับผิดชอบหลักสำหรับความเสี่ยงนั้นต้องรับผิดชอบต่อการจัดการความเสี่ยงในที่สุด

7. เมื่อความเสี่ยงได้รับการจัดการแล้ว ให้ประเมินระดับความเสี่ยงที่เหลือ แม้ว่าจะได้รับการปฏิบัติต่อความเสี่ยงและการควบคุมอยู่ในสถานที่แล้ว ความเสี่ยงก็อาจไม่ถูกขจัดออกไปโดยสิ้นเชิง ระดับความเสี่ยงที่เหลือหมายถึงโอกาสและผลที่ตามมาของความเสี่ยงที่เกิดขึ้นหลังการจัดการความเสี่ยง เมื่อนำไปใช้แล้ว การจัดการจะให้หรือปรับเปลี่ยนการควบคุม หากการควบคุมมีประสิทธิภาพ ระดับความเสี่ยงคงเหลือควรต่ำกว่าระดับความเสี่ยงเดิม ความเสี่ยงที่เหลือควรจัดทำเป็นเอกสาร ติดตาม

และตรวจสอบ หากเหมาะสม การจัดการต่อไปอาจจะรอบคอบ การมีความตระหนักดีถึงความเสี่ยงที่เหลืออยู่เป็นสิ่งสำคัญในการติดตามและตรวจสอบความเสี่ยงอย่างต่อเนื่อง

ขั้นตอนที่ 6 ติดตามและตรวจสอบ (monitor and review) คือ การติดตามการเปลี่ยนแปลง ที่มา และบริบทของความเสี่ยง ระดับของความเสี่ยงที่ยอมรับได้ และความเพียงพอของการควบคุม ตรวจสอบให้แน่ใจว่ามีกระบวนการในการตรวจสอบและรายงานความเสี่ยงอย่างสม่ำเสมอ และเพื่อให้แน่ใจว่ามีการทบทวนอย่างมีโครงสร้างและการรายงานอย่างสม่ำเสมอ แต่ละพื้นที่ควรได้รับการสนับสนุนให้ระบุกระบวนการที่ช่วยให้สามารถตรวจสอบความเสี่ยงที่สำคัญภายในพื้นที่ของตนได้ เนื่องจากสภาพแวดล้อมของมหาวิทยาลัยมีความหลากหลายและไม่หยุดนิ่ง จึงเป็นเรื่องสำคัญที่จะต้องตื่นตัวต่อความเสี่ยงที่เกิดขึ้นใหม่รวมถึงการติดตามความเสี่ยงที่ทราบ

ขั้นตอนที่ 7 สื่อสารและให้คำปรึกษา (communicate and consult) การสื่อสารและการปรึกษาหารือที่มีประสิทธิภาพเป็นสิ่งสำคัญ เพื่อให้แน่ใจว่าผู้ที่รับผิดชอบในการดำเนินการบริหารความเสี่ยงและผู้ที่มีส่วนได้ส่วนเสียเข้าใจพื้นฐานในการตัดสินใจและเหตุผลที่เลือกวิธีการจัดการที่มีความจำเพาะ สามารถสื่อสารและปรึกษากับผู้มีส่วนได้ส่วนเสียภายในและภายนอกในทุกขั้นตอนของกระบวนการบริหารความเสี่ยงได้ โดยเฉพาะอย่างยิ่งเมื่อมีการพิจารณาแผนในครั้งแรกและเมื่อจำเป็นต้องทำการตัดสินใจที่สำคัญ การจัดการความเสี่ยงได้รับการปรับปรุงผ่านการสื่อสารและการปรึกษาหารือที่มีประสิทธิภาพเมื่อทุกฝ่ายเข้าใจมุมมองของกันและกัน และมีส่วนร่วมอย่างแข็งขันในการตัดสินใจตามความเหมาะสม โดยวิธีการสื่อสารและการให้คำปรึกษาอาจรวมถึง 1) การจัดประชุม 2) การแจกแจงวาระ 3) การรายงานผล 4) การสื่อสารแบบออนไลน์และแพ็กเกจการเรียนรู้ 5) การชักนำ 6) จดหมายข่าว 7) รายการหมุนเวียน 8) แผนผังงาน 9) การอบรมความรู้และให้ความรู้แก่บุคลากร/อบรมบุคลากร



รูปที่ 19 ขั้นตอนการจัดการความเสี่ยง (Risk Management Process)

จากกรณีศึกษาของระบบบริหารความเสี่ยงของอุดมศึกษาในต่างประเทศทั้ง 6 มหาวิทยาลัยข้างต้น ผู้เขียนมีข้อสังเกตถึงองค์ประกอบร่วม (common component) ที่มหาวิทยาลัยทั้ง 6 แห่งมีร่วมกันสำหรับหลักการบริหารความเสี่ยงของสถาบันอุดมศึกษา จำแนกได้ 6 องค์ประกอบ ได้แก่ 1) ข้อกำหนดด้านการบริหารความเสี่ยงระดับชาติ 2) หลักธรรมาภิบาลในการบริหารมหาวิทยาลัย 3) กรอบการบริหารความเสี่ยงตามมาตรฐานสากล 4) โครงสร้างการกำกับการบริหารความเสี่ยง 5) กระบวนการบริหารความเสี่ยง และ 6) ผู้มีส่วนได้ส่วนเสียของการบริหารความเสี่ยง

ส่วนที่ 3

การบริหารความเสี่ยง ของสถาบันอุดมศึกษาในประเทศไทย กรณีศึกษา จุฬาลงกรณ์มหาวิทยาลัย

(Risk Management in Thai University Case of Chulalongkorn University)

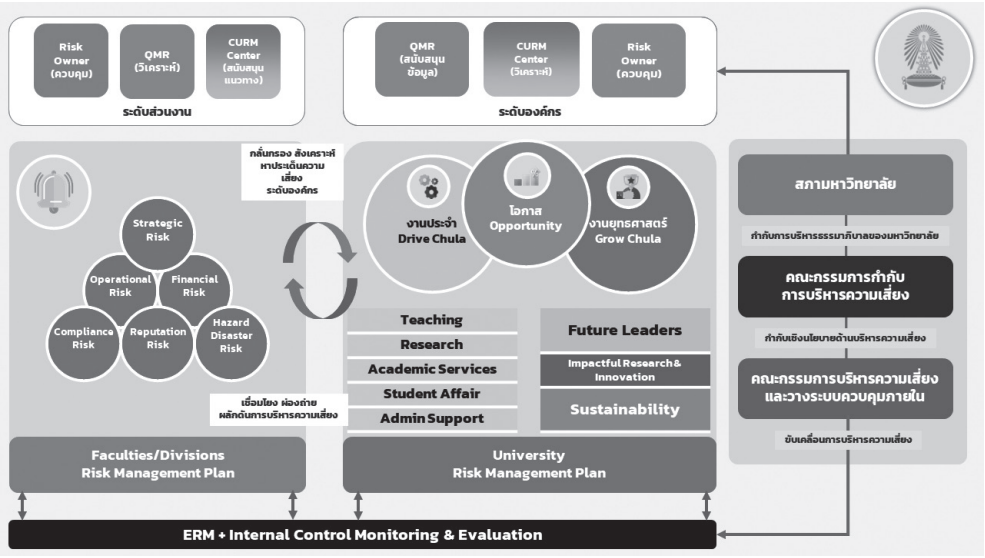
ในส่วนที่ 2 ได้มีการนำเสนอระบบบริหารความเสี่ยงของสถาบันอุดมศึกษาทั่วโลก เพื่อแสดงให้เห็นว่า การวางระบบบริหารความเสี่ยงเป็นเรื่องสำคัญที่มหาวิทยาลัยต่าง ๆ ได้ดำเนินการอันเป็นส่วนหนึ่งของการกำกับดูแลองค์กรที่ดี ทั้งนี้สำหรับมหาวิทยาลัยในประเทศไทย ในหนังสือเล่มนี้จะนำเสนอกรณีศึกษาของ **จุฬาลงกรณ์มหาวิทยาลัย** ซึ่งเป็นสถาบันอุดมศึกษาแห่งแรกของประเทศไทย มีการวางระบบโดยใช้กรอบการบริหารความเสี่ยงสากล COSO ERM 2017 เป็นพื้นฐาน ร่วมกับหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 และหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 โดยมีพัฒนาการของงานด้านบริหารความเสี่ยงอย่างต่อเนื่อง ทั้งในมิติของกระบวนการบริหารความเสี่ยง การสร้างเสริมวัฒนธรรมความเสี่ยง ตลอดจนการนำเทคโนโลยีดิจิทัลมาใช้สนับสนุนการบริหารความเสี่ยง ซึ่งผู้เขียน (ผู้แต่ง) เป็นผู้ปฏิบัติงานที่ศูนย์บริหารความเสี่ยง จุฬาลงกรณ์มหาวิทยาลัย จึงขอนำสิ่งที่ได้ดำเนินการที่มหาวิทยาลัยมาอธิบายในส่วนที่ 3 นี้

จุฬาลงกรณ์มหาวิทยาลัยตระหนักถึงความสำคัญของการบริหารความเสี่ยงภายใต้สถานการณ์ไม่แน่นอน การพลิกโฉมของรูปแบบในการจัดการศึกษาและเรียนรู้ของมนุษย์ การวิวัฒนาการของเทคโนโลยีดิจิทัล การอุบัติขึ้นใหม่ของภัยต่าง ๆ ที่กระทบต่อการดำเนินพันธกิจ โดยถือว่าการบริหารความเสี่ยงเป็นองค์ประกอบที่สำคัญของทุกกระบวนการในการดำเนินพันธกิจที่มีการเชื่อมโยงทุกระดับ จึงได้กำหนดนโยบายการบริหารความเสี่ยงขึ้น เพื่อกระตุ้นให้ประชาคมตระหนักถึงความจำเป็นในการเตรียมความพร้อมรองรับความเสี่ยงและการเปลี่ยนแปลงที่ส่งผลต่อพันธกิจของมหาวิทยาลัย ผลักดันให้มหาวิทยาลัยมีการบริหารจัดการความเสี่ยงอย่างเป็นระบบ รอบคอบ กระชับ ชัดเจน เป็นไปในทิศทางเดียวกัน และเสริมสร้างวัฒนธรรมการทำงานที่คำนึงถึงความเสี่ยงอย่างเหมาะสม เอื้อต่อการเป็นองค์กรที่มีสมรรถนะสูงควบคู่กับการมีธรรมาภิบาล ผ่านการวิเคราะห์สภาพแวดล้อมทั้งภายในและภายนอกที่เปลี่ยนแปลงไปอันส่งผลถึงความเสี่ยงและโอกาสต่อมหาวิทยาลัยและส่วนงาน รวมทั้งวิเคราะห์ต้นเหตุ ตลอดจนการดำเนินงานที่จำกัดผลกระทบและโอกาสเกิดของความเสี่ยง การประเมินสถานการณ์จริงเพื่อวางแผนการบริหารความเสี่ยง

3.1 กลไกการบริหารความเสี่ยง จุฬาลงกรณ์มหาวิทยาลัย

จุฬาลงกรณ์มหาวิทยาลัยมีกระบวนการวิเคราะห์และประเมินความเสี่ยง เพื่อจัดทำกรอบความเสี่ยงระดับองค์กรที่สอดคล้องกับเป้าหมายหลักและแผนการดำเนินงานเป็นประจำทุกปี โดยทั่วไปโครงสร้างกรอบการบริหารความเสี่ยงในระดับมหาวิทยาลัยจะมีระบบควบคุมความเสี่ยงระดับองค์กรจากการแต่งตั้ง **คณะกรรมการบริหารความเสี่ยงและการวางระบบการควบคุมภายใน** ซึ่งมีหน้าที่นำนโยบายการบริหารความเสี่ยงจากสภามหาวิทยาลัยไปสู่การปฏิบัติ วิเคราะห์และวางระบบบริหารความเสี่ยงด้านต่าง ๆ ตามยุทธศาสตร์และพันธกิจหลักของมหาวิทยาลัย ประเมินผลกระทบและโอกาสที่อาจจะเกิดขึ้น กำหนดมาตรการหรือแผนปฏิบัติการ เพื่อดำเนินการหลีกเลี่ยง/ลดโอกาส/กระจายความเสี่ยงนั้น ๆ ตลอดจนทบทวนและประเมินผลมาตรการหรือแผนปฏิบัติการเพื่อปรับปรุงให้เหมาะสมและทันเวลา รวมทั้งรายงานผลการบริหารความเสี่ยงองค์กรต่อคณะกรรมการกำกับการบริหารความเสี่ยงรายไตรมาส

ขณะที่ **คณะกรรมการกำกับการบริหารความเสี่ยง** มีบทบาทกำหนดและทบทวนนโยบายกรอบการบริหารความเสี่ยงองค์กร กำกับดูแล และสนับสนุนให้มีการดำเนินงานด้านการบริหารความเสี่ยงและวางระบบควบคุมภายใน รวมทั้งพัฒนาระบบการจัดการบริหารความเสี่ยง เพื่อให้เกิดประสิทธิภาพอย่างต่อเนื่องในภาพรวม รวมถึงให้ข้อเสนอแนะแนวทาง ติดตาม และประเมินผลการบริหารความเสี่ยงของคณะกรรมการบริหารความเสี่ยงและการวางระบบการควบคุมภายใน พิจารณาอนุมัติรายงานแผนกรอบการบริหารความเสี่ยงระดับองค์กร เพื่อนำเสนอต่อสภามหาวิทยาลัยให้ทราบและรับข้อแนะนำ ซึ่งคณะกรรมการทั้งสองต่างมีหน้าที่สอบทานระบบการควบคุมภายในและระบบการบริหารความเสี่ยงระดับองค์กร สามารถอธิบายโครงสร้างและกระบวนการบริหารความเสี่ยงของมหาวิทยาลัย



รูปที่ 20 กลไกการบริหารความเสี่ยง จุฬาลงกรณ์มหาวิทยาลัย

นอกจากนี้คณะกรรมการกำกับการบริหารความเสี่ยงยังได้มีการประชุมร่วมกับคณะกรรมการตรวจสอบเพื่อแลกเปลี่ยนข้อมูลเชิงนโยบายสำหรับพัฒนาระบบการบริหารความเสี่ยงและควบคุมภายในของมหาวิทยาลัยที่ให้กระบวนการบริหารความเสี่ยงก่อให้เกิดประสิทธิภาพ (performance) และถูกต้องตามกฎระเบียบที่เกี่ยวข้อง (compliance) ทำให้ผลลัพธ์ของการบริหารความเสี่ยงสามารถสร้างคุณค่าแก่องค์กร

การเชื่อมโยงกลไกบริหารความเสี่ยงระดับองค์กรและระดับส่วนงานอย่างเป็นระบบ จุฬาลงกรณ์มหาวิทยาลัยมีการจัดตั้งศูนย์บริหารความเสี่ยง (University Risk Management Center: URM) เป็นศูนย์ระดับฝ่ายที่ขึ้นตรงต่ออธิการบดี มีภาระหน้าที่ในการศึกษา วิเคราะห์ และประเมินบริบทที่เป็นปัจจัยทั้งภายในและภายนอกที่มีการเปลี่ยนแปลง ไม่แน่นอน และส่งผลกระทบเชิงลบต่อการบรรลุเป้าหมายการดำเนินงานตามยุทธศาสตร์หรือภารกิจหลักที่สำคัญในระดับมหาวิทยาลัย สนับสนุนผู้บริหารในการจัดทำ ทบทวน และปรับปรุงแผนและมาตรการจัดการความเสี่ยงแบบบูรณาการ ร่วมกับระบบควบคุมภายในหรือระบบคุณภาพองค์กร ตลอดจนสนับสนุนและให้คำปรึกษาเกี่ยวกับงานในความรับผิดชอบแก่ส่วนงานและหน่วยงานต่าง ๆ ของมหาวิทยาลัย

3.2 การกำหนดกรอบบริหารความเสี่ยงระดับมหาวิทยาลัย

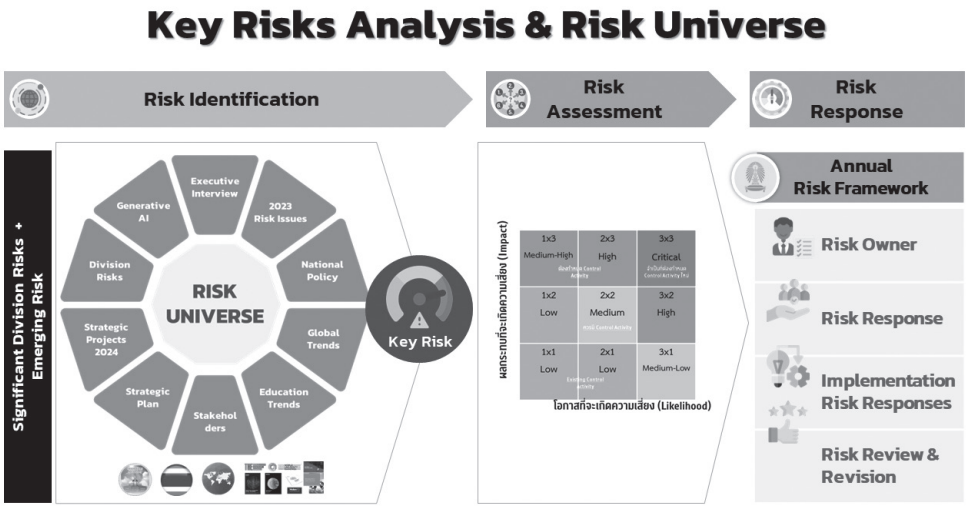
จุฬาลงกรณ์มหาวิทยาลัยได้กำหนดกรอบการดำเนินงานและกระบวนการบริหารความเสี่ยงที่สอดคล้องกับกรอบโครงสร้างการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management) ของ Committee of Sponsoring Organizations of the Treadway Commission (COSO ERM 2017) ที่เชื่อมโยงกับลักษณะความเสี่ยงด้านต่าง ๆ 6 ด้าน ได้แก่ strategic risk, financial risk, operation risk, compliance risk, reputation risk และ disaster risk

เพื่อให้ผู้ที่เกี่ยวข้องมีความเข้าใจหลักการบริหารความเสี่ยงและนำไปประยุกต์ใช้ได้อย่างเหมาะสม สำหรับความเสี่ยงในระดับองค์กรจะมีการกำกับผ่านคณะกรรมการบริหารความเสี่ยงและควบคุมภายใน คณะกรรมการกำกับการบริหารความเสี่ยงร่วมกับคณะกรรมการตรวจสอบ และสภามหาวิทยาลัยตามอำนาจและหน้าที่รับผิดชอบอย่างเป็นระบบ ส่วนความเสี่ยงในระดับส่วนงาน/หน่วยงานภายในมหาวิทยาลัยจะอยู่ภายใต้การกำกับดูแลของคณะกรรมการบริหารส่วนงานและผู้บริหารที่รับผิดชอบ โดยถือเป็นหน้าที่รับผิดชอบของทุกหน่วยงานในการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ พร้อมกับสร้างมูลค่าเพิ่มให้กับผู้มีส่วนได้ส่วนเสียของมหาวิทยาลัยที่สนองตอบเป้าหมายสำคัญ 3 ประการ คือ future leaders, impactful research and innovation และ sustainability ไปสู่การบรรลุวิสัยทัศน์ของจุฬาลงกรณ์มหาวิทยาลัย **“Innovations for Society”** ศูนย์บริหารความเสี่ยง จุฬาลงกรณ์มหาวิทยาลัย ได้ดำเนินการศึกษา วิเคราะห์และสังเคราะห์ข้อมูล จัดทำกรอบการบริหารความเสี่ยงระดับองค์กร โดยจำแนกกระบวนการเป็น 3 ระยะ คือ

ระยะที่ 1 การวิเคราะห์ประเด็นความเสี่ยง (key issues analysis) เริ่มต้นจากการวิเคราะห์วิสัยทัศน์ พันธกิจ เป้าหมาย และยุทธศาสตร์ของจุฬาลงกรณ์มหาวิทยาลัย นโยบายกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม และยุทธศาสตร์ชาติ 20 ปี การสัมภาษณ์ผู้บริหารระดับสูงของมหาวิทยาลัย คณะกรรมการสภามหาวิทยาลัย และผู้มีส่วนได้ส่วนเสียอื่น ๆ พร้อมทั้งวิเคราะห์สภาพแวดล้อมภายนอกองค์กร (external environment) จากข้อมูลทุติยภูมิจากแนวโน้มการเปลี่ยนแปลงระดับโลก หรือ Mega Trend รายงานการศึกษาวิจัยด้านการบริหารความเสี่ยงของสถาบันอุดมศึกษา ได้แก่ Deloitte PWC และ McKinsey & Company วิเคราะห์สภาพแวดล้อมภายนอกองค์กร

(internal environment) จากประเด็นความเสี่ยงที่สำคัญจากฐานข้อมูล (ERM Database) จากส่วนงาน/หน่วยงานต่าง ๆ ทั่วทั้งมหาวิทยาลัย

โดยกรอบการบริหารความเสี่ยงวิเคราะห์ตอบหลักการของกรอบมาตรฐานการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management) ของ Committee of Sponsoring Organizations of the Treadway Commission (COSO ERM 2017) โดยเน้นบูรณาการกับเป้าหมายและยุทธศาสตร์ของมหาวิทยาลัยทั้ง 3 ด้าน คือ future leaders, impactful research and innovation และ sustainability พร้อมกับเชื่อมโยงกับประเภทความเสี่ยงทั้ง 6 ด้านที่มหาวิทยาลัยกำหนด ได้แก่ strategic risk, financial risk, operation risk, compliance risk, reputation risk และ disaster risk โดยจัดทำในรูปแบบของ “Risk Universe”

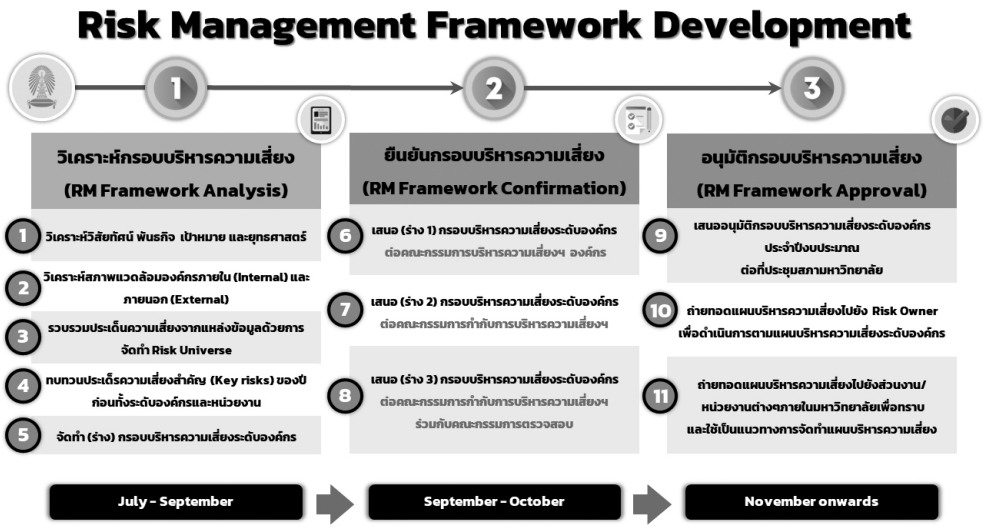


รูปที่ 21 ขั้นตอนการวิเคราะห์ประเด็นความเสี่ยงและการจัดทำ Risk Universe

ระยะที่ 2 ยืนยันกรอบการบริหารความเสี่ยง (risk management framework confirmation) โดยการประชุมแลกเปลี่ยนความคิดเห็นร่วมกับรองอธิการบดีผู้รับผิดชอบพันธกิจของมหาวิทยาลัยทุกด้าน ประกอบด้วยการพิจารณาการระบุความเสี่ยง การวิเคราะห์ปัจจัย/สาเหตุและผลกระทบของความเสี่ยง การวิเคราะห์ระดับความเสี่ยง และมอบหมาย

ผู้รับผิดชอบในแต่ละรายการความเสี่ยง (risk owners) ทำหน้าที่กำหนดแผนปฏิบัติการลดระดับความเสี่ยง/มาตรการในการจัดการความเสี่ยง (risk treatment action plan) ในชุดคณะกรรมการบริหารความเสี่ยงและการวางระบบการควบคุมภายใน (ทบทวน) จำนวน 3 รอบการประชุม และเสนอทบทวนให้ความเห็นต่อในชุดคณะกรรมการกำกับการบริหารความเสี่ยง (ทบทวน) จำนวน 3 รอบการประชุม และเสนอให้ความเห็นชอบต่อในการประชุมร่วมระหว่างคณะกรรมการตรวจสอบกับคณะกรรมการกำกับการบริหารความเสี่ยงสำหรับนำเสนอสภามหาวิทยาลัยต่อไป

ระยะที่ 3 อนุมัติกรอบการบริหารความเสี่ยง (risk management framework approval) เสนอพิจารณาเห็นชอบกรอบการบริหารความเสี่ยงระดับองค์กร จุฬาลงกรณ์-มหาวิทยาลัย ปีงบประมาณ 2564 ต่อสภามหาวิทยาลัยแล้ว เมื่อสภามหาวิทยาลัยพิจารณาเห็นชอบกรอบฯ แล้ว จึงนำแผนบริหารความเสี่ยงถ่ายทอดไปยัง risk owner และผู้ที่เกี่ยวข้องเพื่อดำเนินการบริหารความเสี่ยงให้อยู่ในระดับความเสี่ยงที่คาดการณ์หรือยอมรับได้ต่อไป โดยมีการติดตามผลการบริหารความเสี่ยงทุกรายไตรมาส



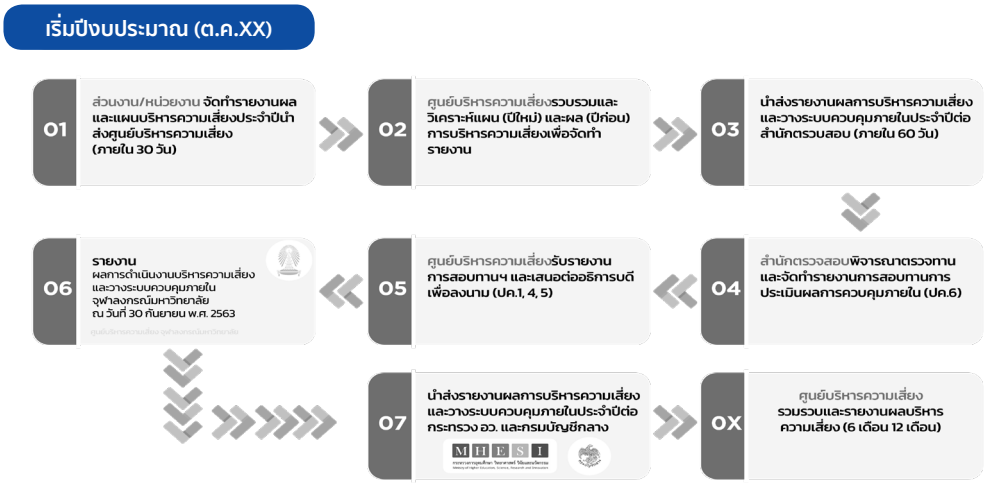
รูปที่ 22 กระบวนการจัดทำกรอบบริหารความเสี่ยงระดับองค์กร จุฬาลงกรณ์มหาวิทยาลัย

3.3 การดำเนินงานตามมาตรฐานการบริหารจัดการความเสี่ยงของจุฬาลงกรณ์มหาวิทยาลัย

ด้วยความตระหนักว่า การบริหารความเสี่ยงเป็นกลไกสำคัญในการพัฒนามหาวิทยาลัยให้เป็นองค์กรสมรรถนะสูงและมีธรรมาภิบาลในการบริหาร มหาวิทยาลัยดำเนินการบริหารจัดการความเสี่ยงและควบคุมภายในให้เป็นไปตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 โดยมีกระบวนการรายงานการบริหารความเสี่ยงและวางระบบควบคุมภายใน ตามมาตรฐานการบริหารจัดการความเสี่ยงดังนี้

มาตรฐานการบริหารจัดการความเสี่ยง	การดำเนินงานตามมาตรฐาน
1. จัดให้มีการบริหารจัดการความเสี่ยงเพื่อให้ความเชื่อมั่นอย่างสมเหตุสมผลแก่ผู้มีส่วนได้ส่วนเสียของมหาวิทยาลัยว่าได้ดำเนินการบริหารความเสี่ยงอย่างเหมาะสม	มีการแต่งตั้งคณะกรรมการกำกับการบริหารความเสี่ยง คณะกรรมการบริหารความเสี่ยง พร้อมจัดทำกรอบการบริหารความเสี่ยง นโยบายการบริหารความเสี่ยง และคู่มือเผยแพร่แก่ส่วนงานต่าง ๆ
2. ฝ่ายบริหารจัดให้มีสภาพแวดล้อมที่เหมาะสมต่อการบริหารจัดการความเสี่ยงภายในองค์กร	มีโครงการและกิจกรรมส่งเสริมความตระหนักและสร้างสภาพแวดล้อมในระดับองค์กรและบุคคล
3. มีการกำหนดวัตถุประสงค์เพื่อใช้ในการบริหารความเสี่ยงที่เหมาะสม รวมถึงมีการสื่อสารการบริหารจัดการความเสี่ยงของวัตถุประสงค์ด้านต่าง ๆ ต่อบุคคลที่เกี่ยวข้อง	มีการชี้แจงวัตถุประสงค์ของการบริหารความเสี่ยง สื่อสารกระบวนการบริหารความเสี่ยงผ่านช่องทางต่าง ๆ ตั้งแต่ผู้บริหาร บุคลากร นิสิต และผู้มีส่วนได้ส่วนเสียทุกระดับ
4. การบริหารความเสี่ยงต้องดำเนินการในทุกระดับของหน่วยงานของรัฐ	มีการดำเนินการบริหารความเสี่ยงตั้งแต่ระดับมหาวิทยาลัยและส่วนงานทุกระดับ
5. การบริหารความเสี่ยงอย่างน้อยต้องประกอบด้วยการระบุความเสี่ยง การประเมินความเสี่ยง และตอบสนองความเสี่ยง	มีขั้นตอนการบริหารความเสี่ยง ได้แก่ ระบุ ประเมิน ตอบสนอง ควบคุม ติดตามผล รวมทั้งวางระบบสารสนเทศ สื่อสาร และรายงานผลอย่างเป็นระบบ ตามกรอบ COSO ERM 2017

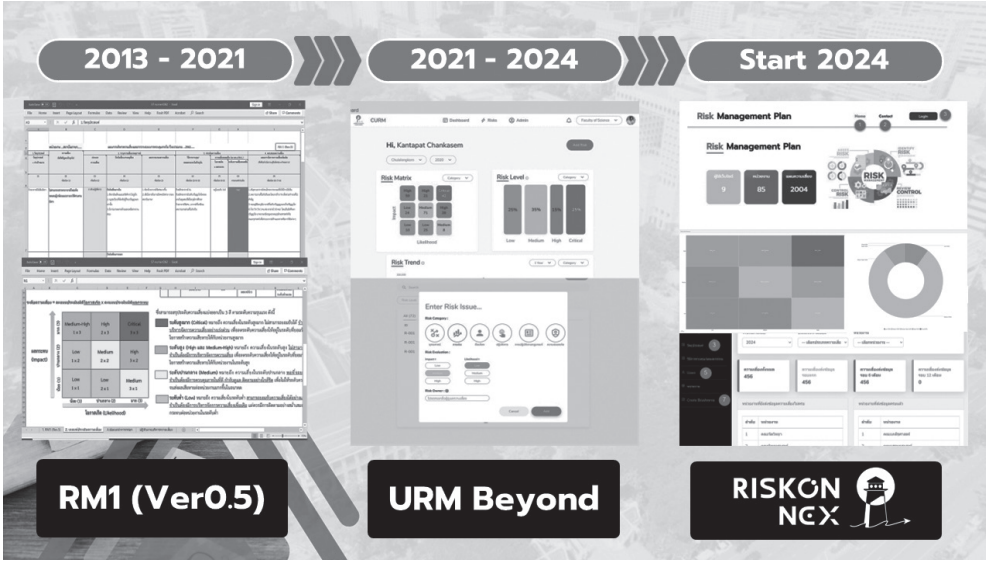
มาตรฐานการบริหารจัดการความเสี่ยง	การดำเนินงานตามมาตรฐาน
6. ต้องจัดทำแผนบริหารความเสี่ยงอย่างน้อยปีละครั้ง และต้องมีการสื่อสารแผนบริหารความเสี่ยงกับผู้ที่เกี่ยวข้องทุกฝ่าย	มีการจัดตั้งแผนบริหารความเสี่ยงระดับองค์กรและระดับส่วนงาน (89 ส่วนงาน) ในต้นปีงบประมาณ และปรับปรุงแผนบริหารความเสี่ยงตามสถานการณ์อย่างสม่ำเสมอ
7. ต้องมีการติดตามประเมินผลการบริหารความเสี่ยงและทบทวนแผนการบริหารความเสี่ยงอย่างสม่ำเสมอ	มีการติดตามประเมินผลและทบทวนการบริหารความเสี่ยงในทุกไตรมาส โดยมีการรายงานผลต่อสำนักตรวจสอบในไตรมาสที่ 2 และไตรมาสที่ 4
8. ต้องมีการรายงานการบริหารความเสี่ยงของหน่วยงานต่อผู้ที่เกี่ยวข้อง	มีการรายงานผลการบริหารความเสี่ยงต่อคณะกรรมการกำกับที่เกี่ยวข้อง สภามหาวิทยาลัย กระทรวงการอุดมศึกษาฯ และกระทรวงการคลัง และเผยแพร่ต่อสาธารณชนบนเว็บไซต์
9. นำเครื่องมือการบริหารความเสี่ยงที่เหมาะสมมาประยุกต์ใช้กับหน่วยงาน เพื่อให้การบริหารจัดการความเสี่ยงเกิดประสิทธิภาพสูงสุด	มีการนำมาตรฐานการบริหารความเสี่ยงสากลมาใช้ ได้แก่ COSO ERM 2017, COSO Fraud Risk 2016, McKinsey & Company Risk Culture Framework 2018



รูปที่ 23 กระบวนการดำเนินงานตามมาตรฐานการบริหารจัดการความเสี่ยง สำหรับหน่วยงานของรัฐ พ.ศ. 2562

3.4 การนำสารสนเทศและเทคโนโลยีมาใช้สนับสนุนงานบริหารความเสี่ยง

เพื่อให้การดำเนินงานในการบริหารความเสี่ยงระดับส่วนงาน และการดำเนินภารกิจของศูนย์บริหารความเสี่ยงด้านการส่งเสริมและสนับสนุนระบบการบริหารความเสี่ยงและควบคุมภายในให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล ศูนย์บริหารความเสี่ยงจึงได้พัฒนาระบบสนับสนุนการบริหารความเสี่ยงระดับส่วนงาน (URM Beyond) ขึ้น โดยเริ่มดำเนินงานภายใต้โครงการพัฒนาระบบสนับสนุนการบริหารความเสี่ยงระดับส่วนงาน ตั้งแต่ พ.ศ. 2563 เป็นต้นมา และพัฒนาอย่างต่อเนื่องจนถึงปัจจุบัน ใน พ.ศ. 2567 ได้พัฒนาระบบที่มีชื่อว่า “RisKonnex” เพื่อสนับสนุนในการดำเนินงานของส่วนงานและศูนย์บริหารความเสี่ยง ในการจัดทำแผนการประเมินความเสี่ยง การติดตามการดำเนินงานตามแผน และดัชนีชี้วัดความเสี่ยง (KRIs) การรวบรวม คัดกรอง วิเคราะห์ประมวลผล และจัดทำรายงานการบริหารความเสี่ยง รวมถึงการจัดการองค์ความรู้ด้านการบริหารความเสี่ยงของส่วนงาน ตลอดจนการใช้ข้อมูลสารสนเทศเพื่อการบริหารจัดการความเสี่ยงระดับส่วนงานและระดับองค์กรได้อย่างเป็นรูปธรรม



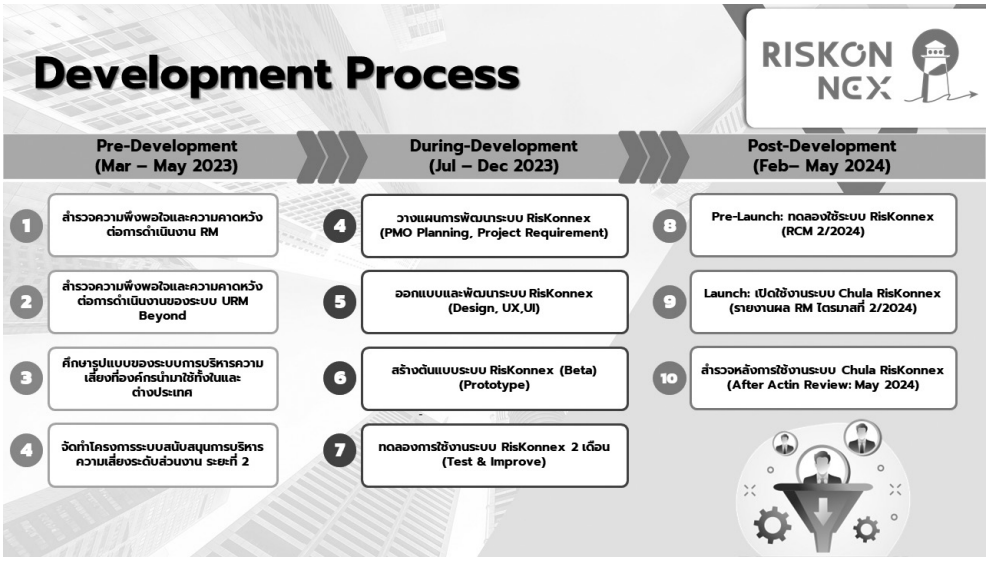
รูปที่ 24 การเปลี่ยนผ่านระบบบริหารความเสี่ยงสู่ระบบดิจิทัลของจุฬาลงกรณ์มหาวิทยาลัย

วัตถุประสงค์ของระบบสนับสนุนการบริหารความเสี่ยงระดับส่วนงาน ประกอบด้วย

1. พัฒนาระบบสนับสนุนการบริหารความเสี่ยงระดับส่วนงานให้มีความเหมาะสมและสอดคล้องกับกระบวนการบริหารจัดการความเสี่ยงของส่วนงานและการบริหารจัดการความเสี่ยงในภาพรวมของศูนย์บริหารความเสี่ยงมากยิ่งขึ้นในรูปแบบ Dashboard

2. สร้างกระบวนการระบุ ประเมิน ติดตามและประเมินผล และการยืนยันการส่งข้อมูลจากส่วนงานหน่วยงานต่าง ๆ ที่มีความทันสมัย สวยงาม และอำนวยความสะดวกให้แก่ผู้ใช้งานกลุ่มต่าง ๆ

3. ส่งเสริมการแลกเปลี่ยนข้อมูล (shared data) ด้านการบริหารความเสี่ยงระหว่างส่วนงาน/หน่วยงานภายในมหาวิทยาลัย นำผลงานการบริหารจัดการความเสี่ยงของส่วนงานที่สามารถรับมือกับความเสี่ยงได้ดีมาเป็นแบบอย่าง เพื่อศึกษาและประกอบการตัดสินใจพัฒนาแผนการบริหารจัดการกับความเสี่ยงในหน่วยงานตน



รูปที่ 25 กระบวนการพัฒนาระบบสนับสนุนการบริหารความเสี่ยงของจุฬาลงกรณ์มหาวิทยาลัย

จากผลการดำเนินงานที่ผ่านมา ระบบสามารถสร้างผลลัพธ์ให้จุฬาลงกรณ์มหาวิทยาลัยมีระบบสนับสนุนการบริหารความเสี่ยงระดับส่วนงานที่มีประสิทธิภาพเหมาะสมกับกระบวนการบริหารความเสี่ยงของส่วนงาน และบริหารจัดการความเสี่ยงในภาพรวมของศูนย์บริหารความเสี่ยง รวมถึงมีข้อมูลสารสนเทศความเสี่ยงของส่วนงานและรายงานสนับสนุนการตัดสินใจของผู้บริหารทั้งในระดับส่วนงานและมหาวิทยาลัย สอดคล้องกับทิศทางที่มหาวิทยาลัยต้องการมุ่งนำนวัตกรรมมาใช้เพิ่มประสิทธิภาพและประสิทธิผลตามหลักธรรมาภิบาล

ทั้งนี้นอกจากระบบสนับสนุนการบริหารความเสี่ยงระดับส่วนงานข้างต้นแล้ว จุฬาลงกรณ์มหาวิทยาลัยยังนำสารสนเทศและเทคโนโลยีอื่นจากหน่วยงานภายในมาใช้เป็นข้อมูลประกอบการสำหรับการบริหารความเสี่ยง เช่น ระบบ Chula Dashboard ซึ่งเป็นระบบสำหรับใช้ในการบริหาร วางแผนตัดสินใจ ติดตามงาน และนำเสนอข้อมูลสรุปผลการดำเนินงานและสถิติต่าง ๆ ของมหาวิทยาลัย คณะ และหน่วยงาน ทำให้ผู้บริหารและผู้ปฏิบัติงานที่เกี่ยวข้องในคณะ สถาบัน หน่วยงานต่าง ๆ ได้รับทราบข้อมูลได้โดยง่ายและรวดเร็ว อีกทั้งยังช่วยสื่อสารให้ประชาคมจุฬาฯ ระบบ Chula TUN-T ซึ่งเป็นระบบสำหรับใช้รายงาน แก้ไข ติดตามปัญหาต่าง ๆ ภายในมหาวิทยาลัย ระบบบริหารจัดการความปลอดภัย อาชีวอนามัยและสิ่งแวดล้อมในการทำงาน และระบบ Social Listening เพื่อติดตามสถานการณ์ด้านสื่อสังคมออนไลน์และข่าวสารเชิงลบของมหาวิทยาลัย เป็นต้น

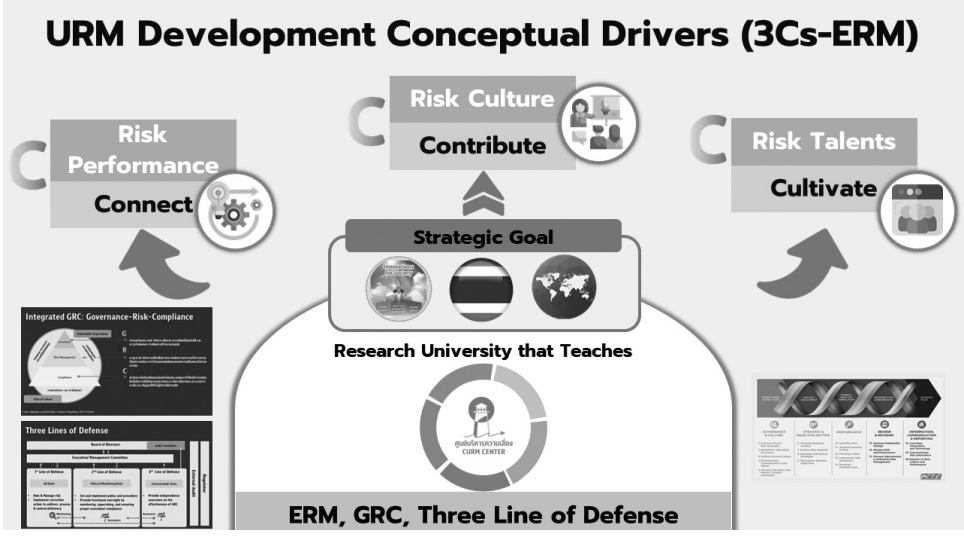
3.5 กระบวนการสร้างเสริมวัฒนธรรมความเสี่ยง (risk culture)

เพื่อให้การบริหารความเสี่ยงของจุฬาลงกรณ์มหาวิทยาลัยมีการดำเนินงานที่สอดรับกับองค์ประกอบที่ 1 ของกรอบการบริหารความเสี่ยง COSO ERM 2017 การกำกับดูแลและวัฒนธรรมองค์กร (governance & culture) ประกอบกับการปฏิบัติหน้าที่ในฐานะด่านที่สองของโมเดลสามด่าน (Three Lines Model) ของสมาคมผู้ตรวจสอบภายในสากล (IIA) ศูนย์บริหารความเสี่ยงจึงได้กำหนดทิศทางการสร้างเสริมวัฒนธรรมความเสี่ยงผ่านแนวคิด “3Cs-ERM” ประกอบด้วย

1. การเชื่อมสัมพันธ์ (connect) เน้นการสร้างความสัมพันธ์ภายในมหาวิทยาลัยเพื่อสร้างศักยภาพในการบริหารความเสี่ยงด้วยความร่วมมือ

2. การส่งเสริม (contribute) เน้นการขับเคลื่อนงานบริหารความเสี่ยงโดยใช้ยุทธศาสตร์ของมหาวิทยาลัยเป็นเป้าหมายสำคัญสำหรับการบริหารความเสี่ยงให้บรรลุเป้าหมายโดยการสร้างเสริมวัฒนธรรมที่เหมาะสม

3. การปลูกฝัง (cultivate) เน้นการพัฒนาศักยภาพของบุคลากรที่เกี่ยวข้องกับงานด้านบริหารความเสี่ยง ให้มีโอกาสในการพัฒนาสมรรถนะต่าง ๆ ทั้งองค์ความรู้ ทักษะ และทัศนคติที่มีต่อการบริหารความเสี่ยง



รูปที่ 26 ทิศทางการสร้างเสริมวัฒนธรรมความเสี่ยงผ่านแนวคิด “3Cs-ERM”

ภายใต้ทิศทางข้างต้นนั้น ศูนย์บริหารความเสี่ยงจึงได้กำหนดงานด้านสร้างเสริมวัฒนธรรมความเสี่ยง (risk culture) เป็นหนึ่งในพันธกิจหลักของหน่วยงาน แล้วได้ดำเนินโครงการ/กิจกรรมต่าง ๆ ให้แก่ประชาคมมหาวิทยาลัย เครือข่ายผู้ที่รับผิดชอบงานด้านบริหารความเสี่ยงในมิติต่าง ๆ ตามนโยบายที่คณะกรรมการกำกับการบริหารความเสี่ยง และคณะกรรมการบริหารความเสี่ยง และวางระบบควบคุมภายในมอบหมาย ดังนี้

1. โครงการคลินิกให้คำปรึกษาการจัดทำแผนบริหารความเสี่ยงระดับส่วนงาน (RM Clinic) เป็นโครงการฝึกอบรมเชิงปฏิบัติการด้านการวางแผนบริหารความเสี่ยงของส่วนงาน/หน่วยงาน ในลักษณะตามความต้องการและช่องว่างของการพัฒนางานด้านบริหารความเสี่ยงเฉพาะของส่วนงาน/หน่วยงาน โดยวัตถุประสงค์ของโครงการคือการอบรมให้ความรู้ ความเข้าใจ เตรียมพร้อมทำแผนบริหารความเสี่ยงของส่วนงานที่จะทำให้ท่านบริหารจัดการความเสี่ยงด้วยความมั่นใจ และเกิดประสิทธิผลในการบริหารความเสี่ยงองค์กรเพื่อให้บรรลุเป้าหมายที่องค์กรกำหนด

รูปที่ 27 ประมวลภาพโครงการคลินิกให้คำปรึกษาการจัดทำแผนบริหารความเสี่ยงระดับส่วนงาน (RM Clinic)

2. โครงการพัฒนาสมรรถนะด้านการบริหารความเสี่ยง (Risk Competency Development) เป็นโครงการที่มุ่งเน้นการให้ความรู้และพัฒนาทักษะแก่ประชาคมมหาวิทยาลัยและผู้ที่สนใจภายนอกมหาวิทยาลัย ในหัวข้อที่หลากหลายสำหรับเตรียมความพร้อมรับมือกับเหตุการณ์ความเสี่ยงในกรณีต่าง ๆ ที่อาจกระทบต่อมหาวิทยาลัย หรือเป็นเหตุการณ์เร่งด่วนที่ต้องวางแผนรับมือล่วงหน้า

รูปที่ 28 ประมวลภาพโครงการพัฒนาสมรรถนะด้านการบริหารความเสี่ยง

3. โครงการแลกเปลี่ยนเรียนรู้ผู้ประสานการขับเคลื่อนการบริหารความเสี่ยง (Risk Champion Meetup) เป็นโครงการแลกเปลี่ยนเรียนรู้เกี่ยวกับประสบการณ์และความคาดหวังเกี่ยวกับการบริหารความเสี่ยงเชิงปฏิบัติการจากส่วนงานในรูปแบบของการจัดการความรู้ (Knowledge Management: KM) เรียนรู้เรื่องราวและเทคนิคการทำงานด้านบริหารความเสี่ยงอย่างมีประสิทธิภาพจากส่วนงานภายในมหาวิทยาลัย และรับทราบแนวทางในการปรับปรุงและพัฒนากระบวนการดำเนินงาน และสนับสนุนการบริหารความเสี่ยงทั้งในระดับมหาวิทยาลัยและระดับส่วนงานให้เกิดประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

4. โครงการสำรวจข้อมูลด้านการบริหารความเสี่ยง (University Risk Management Study) เพื่อศึกษาสภาพปัจจุบัน ความเสี่ยง โอกาส แนวโน้ม และข้อเสนอแนะที่ใช้ในการสนับสนุนการบริหารความเสี่ยงและการขับเคลื่อนพันธกิจของมหาวิทยาลัยในมิติต่าง ๆ เช่น การสำรวจประสบการณ์และความคาดหวังเกี่ยวกับการดำเนินงานบริหารความเสี่ยง การสำรวจผลกระทบของปัญญาประดิษฐ์ประเภท Generative AI ต่อพันธกิจมหาวิทยาลัย การศึกษากลไกสนับสนุนการจัดการความเสี่ยงด้านชื่อเสียง เป็นต้น

ส่วนที่ 4

แนวโน้มความเสี่ยงในระบบอุดมศึกษา

(Risk Trends in Higher Education)

ท่ามกลางการเปลี่ยนแปลงของระบบอุดมศึกษาที่รวดเร็ว ผันผวน ซับซ้อน และยากที่จะคาดการณ์ได้เช่นในอดีต พฤติกรรรมและความคาดหวังของผู้มีส่วนได้ส่วนเสียที่ปรับเปลี่ยนไปตามสภาพของสังคม เป็นสาเหตุให้ความเสี่ยงเกิดขึ้นได้เสมอ อันส่งผลกระทบต่อการดำเนินพันธกิจของมหาวิทยาลัย โดยในส่วนนี้จะกล่าวถึงแนวโน้มความเสี่ยงในระบบอุดมศึกษาจากผลการสำรวจและวิเคราะห์จากสถาบันต่าง ๆ เพื่อใช้เป็นแนวทางสำหรับระบุความเสี่ยงและบริหารความเสี่ยงของสถาบันการศึกษาต่อไป โดยในส่วนนี้จะเป็นการรวบรวมบทความที่ผู้เขียนได้วิเคราะห์ สังเคราะห์ และเรียบเรียงสารสนเทศจากแหล่งต่าง ๆ และจากการปฏิบัติงานด้านบริหารความเสี่ยงมาถ่ายทอดเพื่อเป็นประโยชน์อีกครั้งหนึ่ง

4.1 แนวโน้มความเสี่ยงอุดมศึกษาหลังยุควิกฤต COVID-19

ปฏิเสธไม่ได้เลยว่า การระบาดของไวรัส COVID-19 เข้ามากระทบกิจกรรมต่าง ๆ ของมนุษย์และสังคมในหลายประเทศทั่วโลก ไม่ว่าจะเป็นการดำเนินธุรกิจเล็กใหญ่ การจ้างงานในระบบเศรษฐกิจ ความเป็นอยู่ของผู้คนในสังคม รวมทั้งการจัดการศึกษาด้วย ซึ่งทุกวันนี้ สถาบันอุดมศึกษาทั้งในต่างประเทศและของประเทศไทยเองต่างมีการปรับตัวเพื่อให้สามารถดำเนินภารกิจได้ภายใต้สถานการณ์การระบาดของไวรัส เงื่อนไขที่จำกัดหลากหลายประการและคาดการณ์ไม่ได้ว่าสถานการณ์นี้จะจบลงเมื่อไหร่ ศูนย์บริหารความเสี่ยง จุฬาลงกรณ์มหาวิทยาลัย ได้มีโอกาสศึกษาข้อมูลการคาดการณ์ที่เกี่ยวข้องกับผลกระทบและการเปลี่ยนแปลงที่มีความเป็นไปได้ว่าจะเกิดขึ้นในโลกของอุดมศึกษาในช่วงหลังการแพร่ระบาดของไวรัส COVID-19 เพื่อให้ผู้อ่านได้รับทราบและนำไปใช้คาดการณ์ความเสี่ยงที่อาจจะเกิดขึ้นแล้วมีผลกระทบต่อมหาวิทยาลัยและหน่วยงานของท่าน สามารถปรับตัวสำหรับคว้าโอกาสใหม่ ๆ จากแนวโน้มการเปลี่ยนแปลงที่จะเกิดขึ้น

แนวโน้มที่ 1 การเพิ่มขึ้นของชั้นเรียนและแพลตฟอร์มออนไลน์ เนื่องจากสถานการณ์ที่เกิดขึ้น มหาวิทยาลัยจำเป็นต้องปรับการเรียนการสอนเป็นรูปแบบออนไลน์เกือบจะ 100 เปอร์เซ็นต์ แบบอัตโนมัติ ดังนั้น ประสบการณ์ที่ได้ทำการเรียนการสอนแบบออนไลน์ในครั้งนี้จะทำให้เกิดการยอมรับในกระบวนการและเห็นประสิทธิภาพและประสิทธิผลของออนไลน์ที่มีต่อการศึกษายิ่งขึ้น ข้อกังวลและข้อโต้เถียงในจุดอ่อนของออนไลน์ได้รับการคลี่คลายเพื่อให้งานดำเนินต่อไปได้และปรับแก้ไขให้มีประสิทธิภาพมากขึ้น

แนวโน้มที่ 2 ระบบรับสมัครเข้าเรียนต่อรูปแบบเฉพาะสถาบัน การที่มหาวิทยาลัยปิดที่ทำการในช่วงการรับสมัครนิสิตนักศึกษาใหม่ทั่วโลก ทำให้ต้องเลื่อนกำหนดการที่เกี่ยวข้องกับการรับนิสิตนักศึกษาใหม่ไปอย่างไม่มีกำหนด แต่ยังคงมีมหาวิทยาลัยหลายแห่งที่ออกแบบระบบเทคโนโลยีมาใช้ให้การรับสมัครสามารถดำเนินการได้เป็นปกติ ไม่ว่าจะเป็นการลงทะเบียน การจัดส่งเอกสารออนไลน์ การปรับเกณฑ์การรับสมัครโดยเน้นการพิจารณาแฟ้มสะสมผลงาน (portfolio) การสัมภาษณ์ของระบบการประชุมทางไกล (teleconference) การสร้างระบบทดสอบมาตรฐานของสถาบันเองที่มีความคล่องตัวและแก้ปัญหาที่ไม่สามารถทดสอบผ่านระบบทดสอบกลางของประเทศหรือของสากลได้

แนวโน้มที่ 3 ความนิยมในหลักสูตรสาขาสุขภาพและสาธารณสุขที่เพิ่มสูงขึ้น เนื่องจากแนวหน้าที่ออกไปสู้รบกับสงครามโรค COVID-19 ในครั้งนี้ คือบุคลากรในระบบสาธารณสุข ไม่ว่าจะเป็นแพทย์ พยาบาล เภสัชกร นักเทคนิคการแพทย์ สาธารณสุขชุมชน ฯลฯ คุณค่าที่บุคลากรกลุ่มนี้สร้างขึ้นส่งผลให้สังคมทั่วโลกรู้สึกขอบคุณ ตระหนักในคุณค่าและความสำคัญของประเทศที่จำเป็นต้องผลิตบุคลากรกลุ่มนี้ให้เพียงพอในการดูแลรักษาผู้ป่วยทั้งในยามเหตุการณ์ปกติและยามที่มีโรคอุบัติใหม่เกิดขึ้น โดยนักวิเคราะห์ชี้ว่า หลังสถานการณ์การระบาดของไวรัส ตลาดของหลักสูตรการศึกษาในสาขาสุขภาพและสาธารณสุขจะเติบโตขึ้น อัตราการได้งานทำที่สูง โดยเฉพาะกับกลุ่มอาชีพผู้ช่วยแพทย์และนักเทคโนโลยีปฏิบัติการคลินิกที่ทำหน้าที่เป็นด่านแรกของการตรวจคัดกรองโรค การใช้เทคโนโลยีอุปกรณ์ทางการแพทย์มาใช้ในการตรวจหาเชื้อ และดูแลผู้ป่วยขั้นต้นก่อนถึงมือแพทย์ ซึ่งหลักสูตรนี้อาจจะใช้เวลาศึกษาเพียง 1-2 ปีเท่านั้น

แนวโน้มที่ 4 การลงทุนวิจัยด้านสุขภาพและสาธารณสุขที่สูงขึ้น การแพร่ระบาดของไวรัส COVID-19 ในประเทศต่าง ๆ ทั่วโลก ทำให้มหาวิทยาลัย ภาครัฐ และภาคเอกชนต่างระดมสรรพกำลังเพื่อแสวงหาแนวทางการป้องกัน รักษา และลดผลกระทบจากการระบาดในครั้งนี้ ผ่านการวิจัยและพัฒนาวัคซีนป้องกัน ยารักษาโรค นวัตกรรมตรวจคัดกรองการติดเชื้อที่มีความแม่นยำและรวดเร็ว รวมทั้งอุปกรณ์ทางการแพทย์ที่ช่วยส่งเสริมประสิทธิภาพในการดูแลผู้ป่วย จึงทำให้มหาวิทยาลัย ภาครัฐ และภาคเอกชนต่างจัดสรรงบประมาณเพื่อแสวงหาความรู้ สร้างระบบสาธารณสุขที่มีคุณภาพของประเทศและโลก

แนวโน้มที่ 5 กระบวนการทำงานรูปแบบใหม่ ๆ ในมหาวิทยาลัย การเกิดสถานการณ์ในครั้งนี้ทำให้มหาวิทยาลัยทุกแห่งต้องมีค่าใช้จ่ายที่สูงขึ้นในขณะที่รายได้ลดลง คาดว่าเมื่อสถานการณ์จบลง มหาวิทยาลัยทั่วโลกคงมีการทบทวนโครงสร้างองค์กรและกระบวนการทำงานต่าง ๆ ภายใน โดยมีการนำเทคโนโลยีดิจิทัลเข้ามาใช้บริหารจัดการ การจ้างบุคคลภายนอก (outsource) ในการทำงานประจำเพื่อเพิ่มประสิทธิภาพ การลดต้นทุนการจ้างงานบุคลากรในตำแหน่งที่ไม่จำเป็น หรือมีการทดแทนด้วยเทคโนโลยี การปรับการเรียนการสอนแบบออนไลน์ทำให้ความจำเป็นต้องใช้บุคลากรบางตำแหน่งลดลงหรือเพิ่มขึ้น มีการนำระบบการประชุมทางไกลมาใช้ในการสื่อสารหรือประชุมงาน รวมทั้งการปรับเปลี่ยนการทำงานจากบ้าน (work from home) เป็นต้น

แนวโน้มที่ 6 การเลือกศึกษาต่อในประเทศต่างภูมิภาคลดลง คาดว่าหลังจากสถานการณ์การระบาดสามารถควบคุมได้แล้ว ในช่วงหลังจากนี้ 1-3 ปี ผู้ที่ต้องการศึกษาต่อต่างประเทศยังคงกังวลเกี่ยวกับการระบาดของเชื้อไวรัส COVID-19 รัฐบาลของประเทศที่มีการแพร่ระบาดยังคงมีมาตรการควบคุมการเดินทางและการเข้าออกของผู้คนในและต่างประเทศ การเดินทางไปศึกษาต่อจึงยังคงมีความเสี่ยงอยู่ ผู้ที่มีแผนศึกษาต่อในประเทศที่มีการแพร่ระบาดเหล่านั้นอาจปรับแผนการศึกษาต่อเพื่อลดความเสี่ยงและความกังวลส่วนตัวและครอบครัว ซึ่งอาจมีการเปลี่ยนประเทศที่จะเดินทางไปศึกษาต่อเป็นสถาบันที่ตั้งอยู่ในภูมิภาคเดียวกันที่มีชื่อเสียงและได้รับการจัดอันดับสูง หรือการศึกษาต่อในหลักสูตรนานาชาติของสถาบันภายในประเทศที่มีคุณภาพสูงแทน

รูปที่ 29 แนวโน้มอุดมศึกษาหลังยุควิกฤต COVID-19

4.2 แนวโน้มความเสี่ยงอุดมศึกษา : ผลวิเคราะห์จากรายงาน "Global Risks 2024"

ในช่วงต้นปี องค์กรระดับโลกหลายแห่งได้เผยแพร่ผลการวิเคราะห์และคาดการณ์ความเสี่ยงที่องค์กรทั่วโลกกำลังเผชิญอยู่ในแต่ละปีหรือในอนาคตที่ถูกคาดการณ์ทั้งในระยะสั้นและระยะยาว ข้อสังเกตที่พบจากรายงานต่าง ๆ เหล่านี้เป็นประโยชน์อย่างยิ่งต่อองค์กรที่กำลังจัดทำแผนบริหารความเสี่ยง โดยเฉพาะอย่างยิ่งในกระบวนการของ risk performance ที่จำเป็นต้องระบุความเสี่ยง (identify risks) ให้สอดคล้องกับวัตถุประสงค์และเป้าหมายเชิงกลยุทธ์ของแต่ละองค์กร ครั้งนี้จึงเป็นการวิเคราะห์ข้อมูลจากรายงานความเสี่ยงที่ถูกเผยแพร่โดยองค์กรระดับโลกในธีมของ "Global Risks 2024" จากรายงาน 5 ฉบับที่มีการเผยแพร่โดยองค์กรระดับโลก พร้อมเชื่อมโยงกับบริบทของอุดมศึกษาซึ่งเป็นหนึ่งในองค์กรที่ขณะนี้ได้รับผลกระทบจากการพลิกโฉม (disruption) ทั้งทางด้านเทคโนโลยี สิ่งแวดล้อม เศรษฐกิจ สังคม นโยบาย กฎระเบียบใหม่ ๆ และพฤติกรรมของมนุษย์ที่เปลี่ยนแปลงไป แต่ดูเหมือนว่าเป็นองค์กรที่ขยับหรือปรับตัวได้ช้าจนไม่สามารถก้าวทันการเปลี่ยนแปลงที่เกิดขึ้น โดยรายงานทั้ง 5 ฉบับประกอบด้วย

สรุปผลการคาดการณ์ความเสี่ยงที่โลกเผชิญอยู่ใน ค.ศ. 2024 และอนาคตมีอะไรบ้าง

เริ่มต้นที่รายงานฉบับแรกซึ่งเป็นสารสนเทศอ้างอิงให้แก่องค์กรต่าง ๆ ทั่วโลก อย่าง **รายงานความเสี่ยงโลกประจำปี 2567 (Global Risks Report 2024) โดย World Economic Forum (WEF)** ที่กล่าวถึงการเปลี่ยนแปลงทางเทคโนโลยี ความไม่แน่นอนทางเศรษฐกิจ การเปลี่ยนแปลงสภาพภูมิอากาศ และความขัดแย้ง เน้นบทบาทของการสำรวจการรับรู้ความเสี่ยงทั่วโลกและข้อมูลเชิงลึกจากผู้เชี่ยวชาญ ระบุความเสี่ยงด้านสิ่งแวดล้อม การแบ่งขั้วทางสังคม ความไม่แน่นอนทางเศรษฐกิจ ความก้าวหน้าทางเทคโนโลยี และพลวัตทางภูมิรัฐศาสตร์เป็นข้อกังวลหลัก และเน้นย้ำถึงความจำเป็นในการร่วมมือและกลยุทธ์ในท้องถิ่นเพื่อจัดการกับความเสี่ยงระดับโลก

รายงานฉบับที่สอง คือ **2024 Risk in Focus Survey Results โดย The Internal Audit Foundation (IIA)** คือ การสรุปผลการสำรวจความเสี่ยงจากมุมมองของผู้เชี่ยวชาญด้านการตรวจสอบภายในซึ่งระบุถึงความเสี่ยงในปัจจุบันและความเสี่ยงที่เกิดขึ้นใหม่ โดยระบุความเสี่ยงระดับโลก 3 อันดับแรก ได้แก่ ความปลอดภัยทางไซเบอร์ ทุนมนุษย์ และความต่อเนื่องทางธุรกิจ และคาดการณ์ความเสี่ยงที่เพิ่มขึ้นใน พ.ศ. 2024 เป็นต้นไป ได้แก่ การหยุดชะงักทางดิจิทัลและการเปลี่ยนแปลงสภาพภูมิอากาศ

รายงานฉบับที่สาม คือ **Allianz Risk Barometer 2024 โดย Allianz Commercial** รวมความคิดเห็นจากผู้ตอบแบบสอบถาม 3,069 ราย จากอุตสาหกรรมต่าง ๆ แสดงรายการความเสี่ยงระดับโลกที่สำคัญ ได้แก่ เหตุการณ์ทางไซเบอร์ การหยุดชะงักทางธุรกิจ ภัยพิบัติทางธรรมชาติ และการเปลี่ยนแปลงในกฎหมายและกฎระเบียบ นอกจากนี้ยังให้ความสำคัญเกี่ยวกับความเสี่ยงด้าน ESG Environmental (สิ่งแวดล้อม) Social (สังคม) และ Governance (ธรรมาภิบาล) การล้มละลาย การเปลี่ยนแปลงสภาพภูมิอากาศ ความเสี่ยงทางการเมือง การพัฒนาตลาด และการขาดแคลนแรงงานที่มีทักษะ โดยเน้นย้ำให้องค์กรทั่วโลกให้ความสำคัญกับเหตุการณ์ทางไซเบอร์ (cyber incidents) ว่าเป็นความเสี่ยงอันดับต้น ๆ ของโลกที่ต้องวางแผนรับมือ โดยในปีนี้ได้เพิ่มผลสำรวจความเสี่ยงในประเทศไทย ซึ่งเป็นปีแรกที่มีการเผยแพร่ข้อมูลในรายงานอีกด้วย

รายงานฉบับที่สี่ **Risk Trends in 2024 and Beyond โดย MNP Internal Audit Services** กล่าวถึงความสัมพันธ์ที่เกี่ยวโยงกันของความเสี่ยงในมิติต่าง ๆ รวมถึงการโจมตีทางไซเบอร์ การใช้ปัญญาประดิษฐ์ (AI) ในทางที่ผิด และข้อกังวลด้านความเป็นส่วนตัว การเปลี่ยนแปลงในกฎหมายและความจำเป็นในการบริหารความเสี่ยงที่ครอบคลุมในมิติต่าง ๆ การปรับตัวให้เข้ากับกฎระเบียบด้าน ESG และความท้าทายของการเปลี่ยนแปลงทางดิจิทัล ครอบคลุมหัวข้อต่าง ๆ เช่น การเปลี่ยนแปลงบุคลากร การประกันภัย ภาวะเศรษฐกิจ และความต้องการบริการเทคโนโลยีจากบุคคลที่สาม (third party) ที่เพิ่มขึ้น

รายงานฉบับสุดท้าย คือ **4Q23 Emerging Risks Report โดย Gartner** กล่าวถึงการมุ่งเน้นไปที่ความเสี่ยงต่าง ๆ รวมถึงความเสี่ยงจากการกระจุกตัวของคลาวด์ โดยมีลักษณะเฉพาะคือการพึ่งพาผู้ให้บริการคลาวด์รายใดรายหนึ่ง และความกังวลด้านความต่อเนื่องทางธุรกิจที่เพิ่มขึ้นเนื่องจากการหยุดชะงักที่อาจเกิดขึ้น กล่าวถึงผลกระทบของการตรวจสอบตามกฎระเบียบ ตัวเลือกผู้จำหน่ายที่จำกัด และการเข้าถึงไมโครโปรเซสเซอร์ขั้นสูง เน้นย้ำถึงผลกระทบจากการล็อกอินและอิทธิพลที่มีต่ออนาคตเทคโนโลยีขององค์กร โดยความเสี่ยงอุบัติใหม่ (emerging risk) ที่อยู่ในอันดับต้นยังคงไม่พ้นประเด็นของผลกระทบจากสภาพอากาศที่ร้อนขึ้น วิกฤตการณ์ทางเศรษฐกิจและการเงิน การเปลี่ยนแปลง เงื่อนไขทางการเมืองและภูมิรัฐศาสตร์ และการเปลี่ยนแปลงด้านตลาดแรงงานและกำลังคนในองค์กร

ความเสี่ยงจากการคาดการณ์ทั่วโลกแผ่ขยายมายัง Landscape ของอุดมศึกษาอย่างไรบ้าง

คงปฏิเสธไม่ได้ว่า โลกในทุกวันนี้ถูกเชื่อมโยงกันอย่างไร้พรมแดนด้วยเทคโนโลยีและนวัตกรรมการสื่อสารที่สะดวกรวดเร็ว พร้อมกับอัตราเร่งขององค์กรต่าง ๆ ทั่วโลกที่เพิ่มขึ้นอย่างทวีคูณด้วยพลังของปัญญาประดิษฐ์ (AI) ที่ถูกกล่าวถึงในทุกอุตสาหกรรมใน พ.ศ. 2023 ที่ผ่านมา ขยายต่อมาในปีนี้และอนาคต เห็นได้ชัดว่า ในบริบทของมหาวิทยาลัยได้รับผลกระทบอย่างยิ่งทั้งในเชิงบวกและเชิงลบ นอกจากนี้ผลการศึกษาของ Arthur D. Little, 2023 ในรายงาน The Future of Higher Education Report ยังแนะนำให้ผู้นำในมหาวิทยาลัยตระหนักและเตรียมรับมือกับการปรับตัวกับโลกที่กำลังเปลี่ยนแปลงการจัดการกับสภาพแวดล้อมของการเรียนรู้และการวิจัยแห่งอนาคตซึ่งมีผลต่อความอยู่รอดของมหาวิทยาลัย เนื่องจากเป็นพันธกิจหลักของมหาวิทยาลัยที่ส่งมอบ

คุณค่าทางวิชาการ แหล่งรายได้ และการพัฒนาประเทศ เมื่อทำการวิเคราะห์ผลการคาดการณ์ของรายงานความเสี่ยงระดับโลกทั้ง 5 ฉบับข้างต้นแล้ว สามารถสรุปประเด็นความเสี่ยงสำคัญของมหาวิทยาลัยที่ผู้บริหาร คณาจารย์ บุคลากร และผู้มีส่วนได้ส่วนเสียของมหาวิทยาลัยควรทำความเข้าใจและวางแนวทางในการบริหารความเสี่ยง ซึ่งแบ่งได้เป็น 7 ประเด็นความเสี่ยง มีรายละเอียดดังต่อไปนี้

7 ความเสี่ยงของมหาวิทยาลัย : ผลวิเคราะห์จาก “Global Risks Report 2024”

1. ความเสี่ยงทางเทคโนโลยีที่กำลังเกิดขึ้น (emerging technologies) สถาบันการศึกษาในระดับสูงควรตระหนักถึงการพัฒนาทางเทคโนโลยีอย่างรวดเร็ว โดยเฉพาะในด้าน AI และการเปลี่ยนแปลงทางดิจิทัล ความเสี่ยงที่เกี่ยวข้อง ได้แก่ ภัยคุกคามด้านความปลอดภัยทางไซเบอร์ การรั่วไหลของข้อมูล และความท้าทายในการติดตามการเปลี่ยนแปลงทางเทคโนโลยีอย่างรวดเร็ว

2. ความปลอดภัยทางไซเบอร์ (cybersecurity) ด้วยการพึ่งพาแพลตฟอร์มดิจิทัลที่เพิ่มขึ้น ความปลอดภัยทางไซเบอร์ยังคงเป็นปัญหาสำคัญ สถาบันต้องเสริมสร้างการป้องกันต่อการโจมตีทางไซเบอร์ แรนซัมแวร์ และภัยคุกคามดิจิทัลอื่น ๆ เพื่อปกป้องข้อมูลที่ละเอียดอ่อนและรับประกันการบริการการศึกษาที่ไม่มีการขัดจังหวะ

3. ความเสี่ยงด้านการเปลี่ยนแปลงสภาพอากาศและสิ่งแวดล้อม (climate change and environment) มหาวิทยาลัยและวิทยาลัยต้องพิจารณาถึงผลกระทบของการเปลี่ยนแปลงสภาพอากาศต่อการดำเนินงานและโครงสร้างพื้นฐาน รวมถึงการเตรียมพร้อมสำหรับเหตุการณ์สภาพอากาศที่รุนแรง และการรวมความยั่งยืนและความต่อเนื่องในการดำเนินงาน

4. การปรับตัวเข้ากับการเปลี่ยนแปลงของกฎหมายและระเบียบ (adaptation to legislation and regulation changes) กฎระเบียบใหม่ ๆ โดยเฉพาะที่เกี่ยวข้องกับความเป็นส่วนตัวและการป้องกันข้อมูล จะส่งผลต่อวิธีการที่สถาบันจัดการและรักษาข้อมูลของนักศึกษาและพนักงาน การปรับตัวเข้ากับการเปลี่ยนแปลงเหล่านี้เป็นสิ่งสำคัญเพื่อความสอดคล้องและการรักษาความไว้วางใจ หรือข้อตกลงใหม่ ๆ ที่เป็นระเบียบของการศึกษา การวิจัย หรือความร่วมมือที่มหาวิทยาลัยต้องเปิดเผยข้อมูลหรือส่งเสริมความเท่าเทียมที่มีความเป็นสากลมากยิ่งขึ้น

5. การเปลี่ยนแปลงทางสังคมและเศรษฐกิจ (societal and economic changes) มหาวิทยาลัยควรเตรียมพร้อมเพื่อรับมือกับความแตกต่างของความคิดทางสังคม การถดถอยทางเศรษฐกิจ และการเปลี่ยนแปลงโครงสร้างและพฤติกรรมของประชากร ซึ่งรวมถึงการตอบสนองต่อความต้องการ ความคาดหวังของนิสิตนักศึกษาที่หลากหลายและการปรับตัวเข้ากับการเปลี่ยนแปลงของตลาดแรงงาน และความเห็นต่อการศึกษาในระดับอุดมศึกษาที่แตกต่างไปจากเดิม

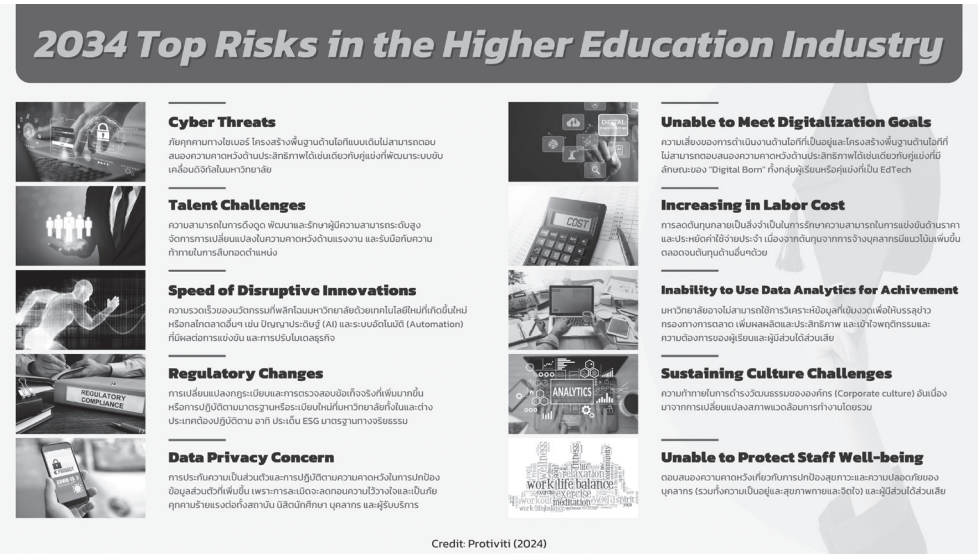
6. ความท้าทายด้านโลกาภิวัตน์และความเปลี่ยนแปลงทางภูมิรัฐศาสตร์ (globalization and geopolitical challenges) ในขณะที่ความตึงเครียดทางภูมิรัฐศาสตร์เพิ่มขึ้นในภูมิภาคต่าง ๆ ทั่วโลก มหาวิทยาลัยต้องเตรียมพร้อมสำหรับผลกระทบที่อาจเกิดขึ้นต่อความร่วมมือระหว่างประเทศ เช่น การเคลื่อนย้ายนิสิตนักศึกษา/อาจารย์ และการระดมทุนวิจัย

7. การขาดแคลนแรงงานที่มีทักษะ (skilled workforce shortages) มหาวิทยาลัยมีบทบาทสำคัญในการแก้ไขปัญหาการขาดแคลนแรงงานที่มีทักษะ แต่สิ่งที่พบคือมหาวิทยาลัยอาจเผชิญความเสี่ยงกับการขาดแคลนแรงงานที่จะเข้ามาร่วมทำงานในมหาวิทยาลัย ไม่ว่าจะเป็นอาจารย์ นักวิจัย หรือบุคลากรสนับสนุนที่มีทักษะสูง เนื่องจากสภาพการแข่งขันในตลาดแรงงานของคนเก่ง ค่าตอบแทน สวัสดิการ ระบบการทำงานที่ไม่รองรับพฤติกรรมการทำงานของคนยุคใหม่

ทั้ง 7 ความเสี่ยงนี้ น่าจะเป็นประโยชน์อย่างยิ่งกับมหาวิทยาลัยที่กำลังอยู่ระหว่างจัดทำแผนบริหารความเสี่ยง หรือที่ทำไว้อยู่แล้วก่อนหน้าอาจนำมาทบทวนเพื่อปรับปรุงได้ตามบริบทอุดมศึกษาที่เปลี่ยนแปลงไป เพราะการเชื่อมโยงกับบริบทอื่น ๆ ประกอบด้วยย่อมเป็นการวิเคราะห์ความเสี่ยงในมุม **“outside-in”** จะเป็นอีกเทคนิคหนึ่งที่สามารถนำมาใช้ระบุความเสี่ยงขององค์กรได้แม่นยำขึ้น และไม่ได้วิเคราะห์ความเสี่ยงจากมุมภายในมหาวิทยาลัยอย่างเดียวเท่านั้น เพราะโลกของอุดมศึกษาในทุกวันนี้จำเป็นต้องเชื่อมโยงกับสิ่งต่าง ๆ อย่างถ้วนทั่วทั้งในเชิงการบริหารความเสี่ยงและการขับเคลื่อนพันธกิจของมหาวิทยาลัยให้บรรลุเป้าหมายภายใต้สถานการณ์ที่ท้าทายและคาดเดาอะไรได้ไม่ง่ายเช่นในอดีตที่ผ่านมา

4.3 แนวโน้มความเสี่ยงอุดมศึกษาในอนาคตก่อน ค.ศ. 2034

ใน ค.ศ. 2024 เมื่อระบบอุดมศึกษาถูกพลิกโฉมด้วยการเข้ามาของปัญญาประดิษฐ์ประเภท Generative AI การเรียกร้องระดับโลกในด้านความยั่งยืน (sustainability) นำมาสู่การที่มหาวิทยาลัยทุกแห่งควรใส่ใจประเด็นด้านสิ่งแวดล้อม สังคม และการกำกับดูแล หรือ ESG มากขึ้น ประกอบกับวิกฤตทางเศรษฐกิจ สังคม ภูมิรัฐศาสตร์ที่รุนแรงมากยิ่งขึ้น ส่งผลให้มหาวิทยาลัยต้องให้ความสำคัญกับการบริหารความเสี่ยงท่ามกลางวิกฤตมากยิ่งขึ้น **รายงาน 2024 Top Risks in the Higher Education Industry โดย Protiviti** ระบุว่า 10 ความเสี่ยงที่ได้รับการสำรวจจากผู้บริหารในภาคอุดมศึกษาว่าเป็นความเสี่ยงสำคัญมีแนวโน้มจะเกิดขึ้นใน ค.ศ. 2034 หรืออีก 10 ปีข้างหน้า ประกอบด้วย



รูปที่ 30 แนวโน้มความเสี่ยงอุดมศึกษาในอนาคตก่อน ค.ศ. 2034

1. ภัยคุกคามทางไซเบอร์ (cyber threats) ภัยคุกคามทางไซเบอร์ โครงสร้างพื้นฐานด้านไอทีแบบเดิมไม่สามารถตอบสนองความคาดหวังด้านประสิทธิภาพได้เช่นเดียวกับคู่แข่งที่พัฒนาระบบขับเคลื่อนดิจิทัลในมหาวิทยาลัย

2. ความท้าทายด้านบุคลากรที่มีความสามารถสูง (talent challenges) ความสามารถในการดึงดูด พัฒนา และรักษาผู้มีความสามารถระดับสูง จัดการการเปลี่ยนแปลงในความคาดหวังด้านแรงงาน และรับมือกับความท้าทายในการสืบทอดตำแหน่ง

3. ความรวดเร็วของนวัตกรรมที่พลิกโฉม (speed of disruptive innovations) ความรวดเร็วของนวัตกรรมที่พลิกโฉมมหาวิทยาลัยด้วยเทคโนโลยีใหม่ที่เกิดขึ้นใหม่หรือกลไกตลาดอื่น ๆ เช่น ปัญญาประดิษฐ์ (AI) และระบบอัตโนมัติ (automation) ที่มีผลต่อการแข่งขันและการปรับโมเดลธุรกิจ

4. ความเปลี่ยนแปลงด้านกฎระเบียบ (regulatory changes) การเปลี่ยนแปลงกฎระเบียบและการตรวจสอบข้อเท็จจริงที่เพิ่มมากขึ้น หรือการปฏิบัติตามมาตรฐานหรือระเบียบใหม่ที่มหาวิทยาลัยทั้งในและต่างประเทศต้องปฏิบัติตาม เช่น ประเด็น ESG มาตรฐานทางจริยธรรม มาตรฐานคุณภาพหลักสูตร

5. ความกังวลด้านความเป็นส่วนตัวของข้อมูล (data privacy concern) การประกันความเป็นส่วนตัวและการปฏิบัติตามความคาดหวังในการปกป้องข้อมูลส่วนตัวที่เพิ่มขึ้น เพราะการละเมิดจะลดทอนความไว้วางใจและเป็นภัยคุกคามร้ายแรงต่อทั้งสถาบัน นิสิตนักศึกษา บุคลากร และผู้รับบริการ

6. การไม่สามารถบรรลุเป้าหมายการปรับเปลี่ยนทางดิจิทัล (unable to meet digitalization goals) ความเสี่ยงของการดำเนินงานด้านเทคโนโลยีสารสนเทศที่เป็นอยู่และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศที่ไม่สามารถตอบสนองความคาดหวังด้านประสิทธิภาพได้เช่นเดียวกับคู่แข่งที่มีลักษณะของ “Digital Born” ทั้งกลุ่มผู้เรียนหรือคู่แข่งที่เป็น EdTech

7. ต้นทุนด้านแรงงานที่เพิ่มขึ้น (increasing in labor cost) การลดต้นทุนกลายเป็นสิ่งจำเป็นในการรักษาความสามารถในการแข่งขันด้านราคาและประหยัดค่าใช้จ่ายประจำ เนื่องจากต้นทุนจากการจ้างบุคลากรมีแนวโน้มเพิ่มขึ้น ตลอดจนต้นทุนด้านอื่น ๆ ด้วย

8. ขาดความสามารถในการวิเคราะห์ข้อมูลเพื่อบรรลุเป้าหมาย (inability to use data analytics for achievement) มหาวิทยาลัยอาจไม่สามารถใช้การวิเคราะห์ข้อมูลที่เข้มงวดเพื่อให้บรรลุข่าวกรองทางการตลาด เพิ่มผลผลิตและประสิทธิภาพ และเข้าใจพฤติกรรมและความต้องการของผู้เรียนและผู้มีส่วนได้ส่วนเสีย

9. ความท้าทายในการดำรงวัฒนธรรม (sustaining culture challenges) ความท้าทายในการดำรงวัฒนธรรมขององค์กร (corporate culture) เนื่องมาจากการเปลี่ยนแปลงสภาพแวดล้อมการทำงานและพฤติกรรมของคนในองค์กรโดยภาพรวม

10. การไม่สามารถปกป้องสุขภาวะของบุคลากร (unable to protect staff well-being) ตอบสนองความคาดหวังเกี่ยวกับการปกป้องสุขภาวะและความปลอดภัยของบุคลากร (รวมทั้งความเป็นอยู่และสุขภาพกายและจิตใจ) และผู้มีส่วนได้ส่วนเสีย

กระบวนการสำรวจ Protiviti ทำโดยการสำรวจสมาชิกคณะกรรมการและผู้บริหาร 1,143 รายในอุตสาหกรรมต่าง ๆ และจากทั่วโลก โดยประเมินผลกระทบของความเสี่ยงเฉพาะ 36 ประการที่มีต่อองค์กรของตนในช่วง 12 เดือนข้างหน้าและในอีก 10 ปีข้างหน้า สำหรับภาคอุดมศึกษาก็ได้สำรวจเช่นเดียวกัน ข้อมูลเหล่านี้จะเป็นกรอบพื้นฐานให้กับมหาวิทยาลัยใช้ทบทวนหรือระบุความเสี่ยงใหม่เพื่อรับมือกับการเปลี่ยนแปลงของภาคอุดมศึกษาที่กำลังได้รับผลกระทบจากการเปลี่ยนแปลงทางเทคโนโลยี พฤติกรรม ทัศนคติต่อการเรียนรู้ คุณค่าของมหาวิทยาลัยที่ส่งมอบจากพันธกิจต่าง ๆ ซึ่งแตกต่างออกไปจากเดิมจนเข้าขั้นน่าเป็นห่วง

4.4 แนวโน้มความเสี่ยงอุดมศึกษาในยุค Generative AI

ปัจจุบันปฏิเสธไม่ได้ว่า AI เข้ามามีบทบาทอย่างมากกับการดำรงชีวิตและการดำเนินธุรกิจ ไม่เว้นแต่ในมหาวิทยาลัย ในปีนี้ ข่าวสารต่าง ๆ ทั้งในและต่างประเทศต่างพุ่งความสนใจไปยัง ChatGPT ซึ่งเป็นหนึ่งใน AI ที่ถูกนำมาใช้งานในมิติต่าง ๆ ของมหาวิทยาลัย โดยรายงานล่าสุดของ UNESCO ได้กล่าวว่า แนวทางหลัก ๆ ที่เป็นไปได้ ซึ่งมหาวิทยาลัยนำ ChatGPT มาประยุกต์ใช้แบ่งออกเป็น 4 แนวทาง คือ ด้านการจัดการเรียนการสอนและการเรียนรู้ (ทั้งในมุมของอาจารย์และมุมนิสิตนักศึกษา) ด้านการวิจัยและพัฒนาองค์ความรู้/นวัตกรรม ด้านการบริหารจัดการของมหาวิทยาลัย และด้านความร่วมมือกับสังคม (ตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสีย)

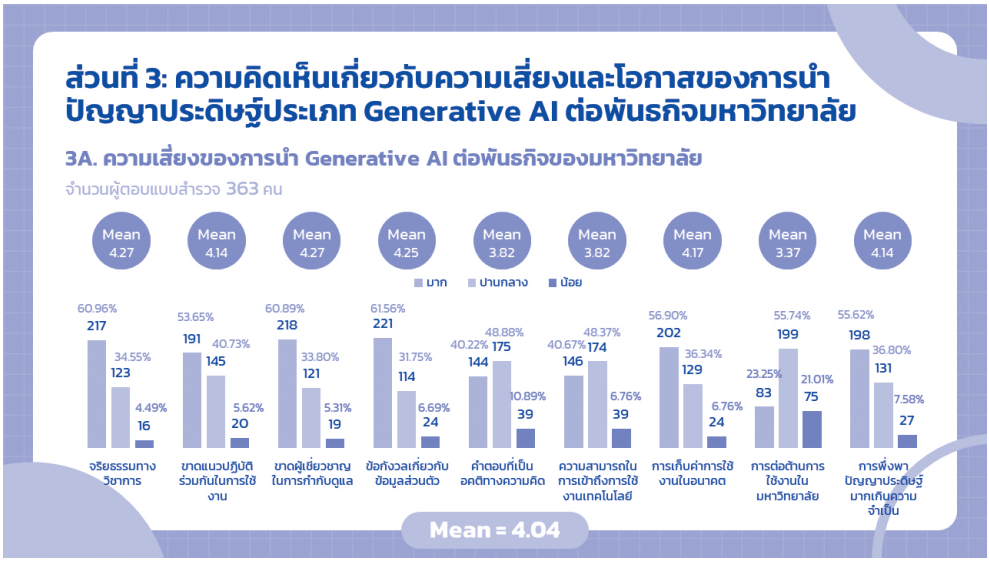
อย่างไรก็ดี ยังคงมีการถกเถียงกันอยู่ไม่น้อยในระดับผู้จัดทำนโยบาย ผู้บริหารมหาวิทยาลัย อาจารย์ นิสิตนักศึกษา เกี่ยวกับคุณประโยชน์และภัยที่เกิดขึ้นจากการใช้งาน ChatGPT และ/หรือ Generative AI อื่น ๆ ที่จะเข้ามามีบทบาทมากยิ่งขึ้นในรั้วมหาวิทยาลัย บ้างก็เห็นว่าเป็นโอกาส บ้างก็ว่าเป็นภัยคุกคาม ซึ่งในเชิงบวกเราคงได้เห็นกันมาบ้างแล้วว่า ChatGPT เป็นตัวช่วยที่สำคัญที่สนับสนุนการทำงานของมหาวิทยาลัยได้อย่างมีประสิทธิภาพ ทำให้การดำเนินพันธกิจต่าง ๆ เป็นไปอย่างรวดเร็วมากขึ้น (ในส่วนนี้เอง ผู้เขียนได้ลองใช้งานมาระยะหนึ่งแล้วมีความเห็นด้วยอย่างมาก) อย่างไรก็ตาม คงไม่อาจกล่าวได้ครบทั้งหมดว่าการใช้งานนั้นเป็นที่น่าพอใจ ได้คำตอบที่ถูกต้องทั้งหมดสำหรับนำไปใช้งานได้จริงแบบสำเร็จรูป ทั้งนี้ยังมีอีกหลายมิติที่ปัจจุบันและอนาคตอันใกล้ที่ AI จะเข้ามามีบทบาทและแทรกซึมกิจกรรมต่าง ๆ ภายในมหาวิทยาลัย ในฐานะผู้ที่เกี่ยวข้องกับมหาวิทยาลัยจึงไม่ควรละเลยเรื่องเหล่านี้ โดยความเสี่ยงที่อาจเกิดขึ้นจากการใช้งาน Generative AI ที่ต้องคำนึงถึงมีดังต่อไปนี้

1. จริยธรรมทางวิชาการ (academic integrity)
2. ขาดแนวปฏิบัติร่วมกันในการใช้งาน (lack of regulation)
3. ข้อกังวลเกี่ยวกับข้อมูลส่วนตัว (data privacy concerns)
4. คำตอบที่เป็นอคติทางความคิด (cognitive bias)
5. ความสามารถในการเข้าถึงการใช้งานเทคโนโลยี (accessibility)
6. การเก็บค่าการใช้งานในอนาคต (commercialization)
7. การต่อต้านการใช้งานในมหาวิทยาลัย (opposition)

8. ความเข้าใจที่ว่าเป็นแหล่งอ้างอิงที่แท้จริง (reference of truth)
9. การพึ่งพาการใช้งานที่มากเกินไป (overreliance)

จากความเสี่ยงข้างต้น การปฏิเสธการใช้งานเทคโนโลยีทั้งหมดคงจะไม่ได้ ในเมื่อนวัตกรได้พัฒนาเครื่องมือเหล่านี้มาสนับสนุนการทำงานและการใช้ชีวิตของผู้คนแล้ว แต่คำถามที่อาจจะต้องหาคำตอบ คือ จุดร่วม (common) และขอบเขต (scope) ของการใช้งานสิ่งเหล่านี้อยู่ตรงไหน เพราะคงไม่มีใครอยากเห็นว่า ในอนาคต เราอาจจะบกพร่องในทักษะการคิดเชิงวิพากษ์ (critical thinking) พึ่งพาแต่การใช้งานเครื่องมือในการแสวงหาคำตอบ เพราะต้องไม่ลืมว่าหากขาดองค์ความรู้ใหม่หรือการคิดวิเคราะห์ด้วยความสามารถของมนุษย์ ในอนาคต คำถาม/คำตอบใหม่ ๆ ที่เราใช้สอน AI เหล่านี้อาจจะวนอยู่กับเรื่องเดิม ๆ จนไม่อาจพัฒนาสิ่งใหม่ขึ้นมาก็เป็นได้

ซึ่งสอดคล้องกับ **“ผลสำรวจผลกระทบของปัญญาประดิษฐ์ประเภท Generative AI ต่อพันธกิจมหาวิทยาลัย” โดยศูนย์บริหารความเสี่ยง จุฬาลงกรณ์มหาวิทยาลัย** ในช่วงต้นปี พ.ศ. 2567 โดยการสำรวจผู้บริหาร บุคลากรสายวิชาการและสายสนับสนุน และนิสิตของจุฬาลงกรณ์มหาวิทยาลัย จำนวน 363 คน ซึ่งพบว่าความเสี่ยงของการนำปัญญาประดิษฐ์ประเภท Generative AI ต่อพันธกิจมหาวิทยาลัย คือ 1) จริยธรรมทางวิชาการ 2) ขาดความเชี่ยวชาญในการกำกับดูแลและการใช้งานอย่างถูกต้อง 3) การละเมิดข้อมูลส่วนบุคคล/หรือข้อมูลถูกเผยแพร่โดยไม่ได้รับอนุญาต 4) ต้นทุนจากการใช้งานปัญญาประดิษฐ์ นอกจากนี้ยังมีข้อเสนอแนะจากการสำรวจ เช่น ขาดการคิดสร้างสรรค์ด้วยตนเอง (originality) ส่งผลให้ขาดวิจารณญาณการนำผลลัพธ์จาก AI มาใช้โดยขาดการพิจารณาความถูกต้องและความคลาดเคลื่อนของข้อมูล การละเมิดลิขสิทธิ์จากผลลัพธ์ที่ AI สร้างขึ้น พึ่งพาการใช้งานปัญญาประดิษฐ์มากเกินไป



รูปที่ 31 ความเสี่ยงของการนำ Generative AI ต่อพันธกิจของมหาวิทยาลัย

อย่างไรก็ตาม จากแนวโน้มความเสี่ยงในระบบอุดมศึกษาข้างต้นนั้นแสดงให้เห็นว่าระบบอุดมศึกษากำลังเผชิญกับความท้าทายจากการเปลี่ยนแปลงที่เกิดขึ้นจากมิติทั้งในและนอกภูมิทัศน์ของอุดมศึกษา อาจเป็นได้ทั้งความเสี่ยงและโอกาสที่มหาวิทยาลัยควรตระหนักและวางแผนบริหารจัดการอย่างเป็นระบบทั้งในเชิงรุกและรับเพื่อให้สามารถบริหารจัดการสถาบันอุดมศึกษาให้ปรับเปลี่ยนพันธกิจและเป้าหมายได้ทันการณ์ สอดรับกับความคาดหวังและความต้องการที่สังคมมีต่ออุดมศึกษา และบริหารจัดการสถาบันให้สามารถส่งมอบคุณค่าได้อย่างยั่งยืน

บทส่งท้าย

จุดเริ่มต้นที่ทำให้ผู้เขียนเขียนหนังสือเล่มนี้ขึ้นมาคือ ความตั้งใจที่จะรวบรวมแนวคิด หลักการ และการดำเนินงานด้านการบริหารความเสี่ยงที่เกิดขึ้นในสถาบันอุดมศึกษา มาถ่ายทอดให้เกิดความเข้าใจและสามารถนำไปประยุกต์ใช้ได้ในการบริหารสถาบันอุดมศึกษา เนื่องจากปัจจุบันมีสื่อไม่มากนักที่กล่าวถึงเรื่องการบริหารความเสี่ยงเฉพาะเจาะจงในองค์กรอย่างสถาบันอุดมศึกษา ที่ในบางมิติมีโครงสร้างและพันธกิจที่ต่างออกไปจากองค์กรโดยทั่วไป เช่น การบริหารงานวิชาการและงานวิจัย การบริหารกิจการที่เกี่ยวกับนิสิตนักศึกษา การส่งมอบคุณค่าต่อสังคมด้วยงานบริการวิชาการ การเคารพในอิสระทางวิชาการ การบริหารจัดการที่เรื่องรายได้อาจมิใช่เป้าหมายสูงสุด เป็นต้น ท่ามกลางการเปลี่ยนแปลงอย่างพลิกโฉม (disrupt) ที่เกิดขึ้นทั้งจากเทคโนโลยีสมัยใหม่ การแทนที่ของปัญญาประดิษฐ์ ระบบเศรษฐกิจและสังคมที่ผันผวน วิกฤตการณ์สิ่งแวดล้อมทางธรรมชาติ การกีดกันและความขัดแย้งภูมิรัฐศาสตร์ เป็นสาเหตุให้มหาวิทยาลัยทั่วโลกเผชิญกับความเสี่ยงนานัปการ ซึ่งเป็นเรื่องท้าทายของผู้นำและผู้ปฏิบัติงานในมหาวิทยาลัยว่าจะสามารถปรับตัวให้อยู่ในสภาวะของความคล่องแคล่ว (agility) และสามารถล้มและฟื้นตัว (resilience) ได้อย่างไร

จากการทำงานด้านบริหารความเสี่ยงตั้งแต่ระดับคณะ ส่วนกลาง จนกระทั่งมีโอกาสดูภาพรวมทั้งระบบของมหาวิทยาลัย ประกอบกับได้มีโอกาสเป็นวิทยากรและที่ปรึกษาให้แก่มหาวิทยาลัยในประเทศไทยกว่า 30 แห่ง สิ่งที่พบคือ ความรู้ ความเข้าใจและการเห็นความสำคัญถึงคุณค่าของการบริหารความเสี่ยงนั้นยังคลาดเคลื่อน การระบุปัญหามาจัดทำแผนบริหารความเสี่ยง ความไม่ต่อเนื่องและจริงจังในการนำมาตรการควบคุมที่ออกแบบไว้ไปปฏิบัติใช้จริง หรือบางแห่งยังไม่ได้ริเริ่มงานด้านบริหารความเสี่ยง หนังสือเล่มนี้จึงเป็นเล่มแรกที่ผู้เขียนอยากจะรวบรวมองค์ความรู้ที่สำคัญ กรณีศึกษาของระบบบริหารความเสี่ยงนำไปใช้จริงในสถาบันอุดมศึกษาในต่างประเทศ ที่ผู้เขียนปฏิบัติงานอยู่สำหรับมหาวิทยาลัยในประเทศไทย พร้อมกับรวบรวมบทความที่ฉายภาพถึงแนวโน้มของความเสี่ยงสำคัญในมิติต่าง ๆ ที่มหาวิทยาลัยในปัจจุบันและอนาคตกำลังเผชิญ เพื่อสร้างความตระหนักให้กับผู้นำและผู้ปฏิบัติงานในมหาวิทยาลัยทุกท่านได้เห็นถึงคุณค่าของงานบริหารความเสี่ยง และปรับทัศนคติใหม่ว่า **“การบริหารความเสี่ยงเป็นเครื่องมือเชิงกลยุทธ์ที่จะทำให้มหาวิทยาลัยบรรลุเป้าหมาย”**

บรรณานุกรม

ณัฐชา ทวีแสงสกุลไทย. (2562). *วิศวกรรมคุณภาพและการจัดการ: เข็มทิศการปรับปรุงและสร้างนวัตกรรมอย่างต่อเนื่อง (Quality engineering and management: Guide to continual improvement and innovation).* สำนักพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

ศูนย์บริหารความเสี่ยง. (2566). *บทสรุปผู้บริหาร รายงานการบริหารความเสี่ยงระดับองค์กร ปีงบประมาณ 2566 และกรอบการบริหารความเสี่ยงระดับองค์กร ปีงบประมาณ 2567 จุฬาลงกรณ์มหาวิทยาลัย.*

ศูนย์บริหารความเสี่ยง. (2567). *รายงานผลสำรวจผลกระทบของปัญญาประดิษฐ์ประเภท Generative AI ต่อพันธกิจมหาวิทยาลัย 2024*. ศูนย์บริหารความเสี่ยง จุฬาลงกรณ์มหาวิทยาลัย.

Allianz. (2024). *Allianz Risk Barometer 2024.* https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024-Appendix.pdf

C. Ronald Kimberling. (2020, December 3). *Coronavirus presents new challenges and opportunities to higher education.* The Hill. https://thehill.com/opinion/education/486603-coronavirus-presents-new-challenges-and-opportunities-to-higher-education

Gartner. (2023). *4Q23 Emerging Risk Report.* https://www.gartner.com/en/audit-risk/trends/top-emerging-risk-trends-for-erm-leade

Joshua Kim. (2020, March 31). *Teaching and Learning After COVID-19*. Inside Higher Ed. https://www.insidehighered.com/digital-learning/blogs/learning-innovation/teaching-and-learning-after-covid-19

Marguerite Dennis. (2020, March 28). *How will higher education have changed after COVID-19?.* University World News. https://www.universityworldnews.com/post.php?story=20200324065639773

MNP. (2023). *Risk Trends in 2024 and Beyond.* https://www.mnp.ca/en/insights/directory/risk-trends-in-2024-and-beyond.

Protiviti. (2024). *2024 Top Risks in the Higher Education Industry*. https://www.protiviti.com/us-en/survey/executive-perspectives-top-risks

QS Global India Initiative. (2020, April 1). *How is COVID-19 Shaping the Higher Education Sector?.* https://www.qs.com/how-is-covid-19-shaping-the-higher-education-sector/

Rae Shaffer (2023, March 15). *How Will ChatGPT Impact Higher Education?* K16 Solutions. https://www.k16solutions.com/resources/k16-blog/how-will-chatgpt-impact-higher-education/

The Internal Audit Foundation. (2023). *Risk in Focus 2024 Global Summary.* https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/risk-in-focus-survey-results-global-summary-2024.pdf.

UNESCO. (2023). *ChatGPT and artificial intelligence in higher education: Quick start guide.* https://www.iesalc.unesco.org/wp-content/uploads/2023/04/ChatGPT-and-Artificial-Intelligence-in-higher-education-Quick-Start-guide_EN_FINAL.pdf

World Economic Forum. (2024). *Global Risks Report 2024.* https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.

ประวัติผู้เขียน

“อวิรุทธ์ ฉัตรมาลาทอง” ปัจจุบันทำงานประจำเป็นผู้อำนวยการศูนย์บริหารความเสี่ยง ที่จุฬาลงกรณ์มหาวิทยาลัย เป็นนักวิชาการในสาขาการอุดมศึกษาที่มีประสบการณ์ 10 ปี ในงานวิเคราะห์ยุทธศาสตร์ แผนงาน และบริหารความเสี่ยงของสถาบันอุดมศึกษา ซึ่งเห็นว่างานบริหารความเสี่ยงสามารถสร้างคุณค่าให้แก่องค์กรทั้งในสถานการณ์ปกติและสถานการณ์วิกฤต จึงเป็นนักเรียนรู้ศาสตร์และศิลป์ด้านบริหารความเสี่ยงเพิ่มเติม โดยนำเรื่องราวของ **“risk management”** และ **“higher education trends”** มาเผยแพร่ในเพจส่วนตัวชื่อว่า **“Knack Box”** มีเป้าหมายเพื่อส่งต่อเทคนิคและเรื่องราวขององค์กรต่าง ๆ ที่สามารถปรับตัวและสร้างโอกาสใหม่ ๆ จากการบริหารความเสี่ยง พร้อมทั้งนำ case study ขององค์กรต่าง ๆ ทั้งภาคธุรกิจและภาคการศึกษามาถ่ายทอดเพื่อสร้างแรงบันดาลใจแก่ผู้นำและผู้ที่สนใจให้สามารถนำองค์กรโดยใช้ความเสี่ยงสร้างโอกาส และยังเป็นวิทยากรและที่ปรึกษาด้านการวางระบบบริหารความเสี่ยง (risk management system) และสร้างเสริมวัฒนธรรมความเสี่ยง (risk culture) ให้แก่สถาบันการศึกษา ภาครัฐ และรัฐวิสาหกิจที่สนใจพัฒนากระบวนการบริหารความเสี่ยง

“อวิรุทธ์ ฉัตรมาลาทอง” ปัจจุบันยังมีอีกหนึ่งบทบาทในฐานะนักวิจัยเชิงนโยบายในหัวข้อต่าง ๆ เช่น การพัฒนาโมเดลของมหาวิทยาลัยแห่งการประกอบการ (Entrepreneurial University) การพัฒนาระบบนิเวศนวัตกรรมและการร่วมลงทุนในธุรกิจฐานนวัตกรรม การพัฒนาระบบพี่เลี้ยงธุรกิจนวัตกรรม (IDEs Mentoring System) และการวางกลไกบ่มเพาะความเป็นผู้ประกอบการและธุรกิจนวัตกรรมในมหาวิทยาลัย (University IDEs incubation) ซึ่งมีเป้าหมายเพื่อสนับสนุนการพัฒนาประเทศไทยสู่ประเทศที่ขับเคลื่อนด้วยธุรกิจนวัตกรรมที่สามารถเติบโตอย่างก้าวกระโดด

FREE

COURSE FREE

มี Certificate ให้!

ORGANIZATIONAL RISK MANAGEMENT

คอร์สเรียนออนไลน์ การบริหารความเสี่ยงองค์กร
เนื้อหาพัฒนาจากหลักวิชาการและประสบการณ์ปฏิบัติการด้านการบริหารความเสี่ยงและการวางระบบควบคุมภายในจริง...ภายในองค์กร
บนแพลตฟอร์มการเรียนรู้จากจุฬาลงกรณ์มหาวิทยาลัย

CHULA MOOC

อวิรุทธ์ ฉัตรมาลาทอง

ผู้อำนวยการศูนย์บริหารความเสี่ยง จุฬาลงกรณ์มหาวิทยาลัย
วิทยากรและที่ปรึกษาด้านการบริหารความเสี่ยงองค์กร

Learn Now

Contact me

- Facebook: https://www.facebook.com/knackboxx
- Tel: 0864161566
- Line: Knack88

KNACK BOX

Higher Education Risk Management

จัดการความเสี่ยงอย่างไร ให้มหาวิทยาลัยบรรลุเป้าหมาย

เล่มนี้เป็นคู่มือที่ทางผู้แต่งตั้งใจจัดทำขึ้นเพื่อแลกเปลี่ยนความรู้ แนวคิดพื้นฐานของการบริหารความเสี่ยงในอุดมศึกษาระบบบริหารความเสี่ยงที่ถูกใช้จริงในสถาบันอุดมศึกษาทั่วโลกตัวอย่างกรณีศึกษาการบริหารความเสี่ยง ตลอดจนรวบรวมแนวโน้มความเสี่ยงที่มหาวิทยาลัยต้องเผชิญ ท่ามกลางการเปลี่ยนแปลงในยุค New Normal ที่จะทำให้ผู้บริหาร และคนทำงานในมหาวิทยาลัยเข้าใจเรื่องบริหารความเสี่ยงมากยิ่งขึ้น

ISBN 978-616-6127-31-7
9 786166 127317
หมวดการศึกษา