รายงาน
แผนบริหารความเสี่ยงและการควบคุมภายใน
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกาญจนบุรี
ประจำปีงบประมาณ พ.ศ 2566
(รอบ 12 เดือน)

สำนักวิทยาบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏกาญจนบุรี

คำนำ

แผนบริหารความเสี่ยงและการควบคุมภายใน ประจำปีงบประมาณ 2566 ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปี 2566 จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานบริหารความเสี่ยงและการควบคุมภายใน เพื่อนำมาระบุและวิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้องค์กรบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่ เพื่อที่จะได้เลือกวิธีการที่เหมาะสม ในการบริหารความเสี่ยงเหล่านั้นได้อยู่ระดับที่องค์กรสามารถรองรับได้ และทำให้องค์กรบรรลุวัตถุประสงค์ได้ อย่างมีประสิทธิภาพมากขึ้น ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกาญจนบุรี หวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงและการควบคุมภายในฉบับนี้ จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศต่อไป

ศูนย์เทคโนโลยีสารสนเทศ
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏกาญจนบุรี
กันยายน 2566

บทที่ 1
บทนำ

1. หลักการและเหตุผล

การบริหารความเสี่ยงและการควบคุมภายในเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุมและวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์ คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อ การดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยง จากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการ ความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

2. วัตถุประสงค์

วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกาญจนบุรี เพื่อวัตถุประสงค์ต่อไปนี้

1. เพื่อให้ผู้บริหารและผู้ปฏิบัติงานทุกระดับ มีความรู้ความเข้าใจในหลักการ กระบวนการ และขั้นตอนการบริหารความเสี่ยงและการควบคุมภายในของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
2. เพื่อเป็นเครื่องมือให้บุคลากรปฏิบัติงานตามกระบวนการบริหารความเสี่ยง อย่างเป็นระบบและต่อเนื่อง สอดคล้องกับวิสัยทัศน์ พันธกิจ ยุทธศาสตร์ และกลยุทธ์ของสำนักฯ
3. เพื่อให้สำนักฯ มีการกำกับดูแลตนเองที่ดี ตามแนวพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี
4. เพื่อเป็นแนวทางในการติดตาม และประเมินผลการดำเนินงานของสำนักฯ ให้มีประสิทธิภาพและประสิทธิผล สามารถรับมือกับความเสี่ยงที่จะเกิดขึ้นในอนาคต

3. ความจำเป็นของการบริหารความเสี่ยงและการควบคุมภายใน

ประการแรก

พระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ 5) พ.ศ. 2545 มาตรา 3/1 บัญญัติว่า “การบริหารราชการต้องเป็นไปเพื่อประโยชน์สุขของประชาชน เกิดผลสัมฤทธิ์ต่อภารกิจของรัฐ ความมีประสิทธิภาพ ความคุ้มค่าในเชิงภารกิจแห่งรัฐ การลดขั้นตอนการปฏิบัติงาน การลดภารกิจและยุบเลิกหน่วยงานที่ไม่จำเป็น การกระจายภารกิจและทรัพยากรให้แก่ท้องถิ่น การกระจายอำนาจตัดสินใจ การอำนวยความสะดวกและการตอบสนองความต้องการของประชาชน มีผู้รับผิดชอบต่อผลของงาน การปรับปรุงคุณภาพการให้บริการ จึงเป็นแนวหนึ่งที่จำเป็นอย่างยิ่งเพื่อให้การบริหารราชการเป็นไปอย่างมีประสิทธิภาพและสามารถตอบสนองความต้องการของประชาชน ในการปฏิบัติหน้าที่ของส่วนราชการ ต้องใช้วิธีการบริหารกิจการบ้านเมืองที่ดี โดยเฉพาะอย่างยิ่งให้คำนึงถึงความรับผิดชอบของผู้ปฏิบัติราชการ การมีส่วนร่วมของประชาชน การเปิดเผยข้อมูล การติดตามตรวจสอบและประเมินผลการปฏิบัติราชการ ทั้งนี้ตามความเหมาะสมของแต่ละภารกิจ”

ประการที่สอง

พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. 2546 มาตรา 12 กำหนดว่า เพื่อประโยชน์ในการปฏิบัติราชการให้เกิดผลสัมฤทธิ์ ก.พ.ร. อาจเสนอต่อคณะรัฐมนตรีเพื่อกำหนดมาตรการกำกับการปฏิบัติราชการ โดยวิธีการจัดทำความตกลงเป็นลายลักษณ์อักษร หรือโดยวิธีการอื่นใดเพื่อแสดงความรับผิดชอบในการปฏิบัติราชการ และมาตรา 45 กำหนดให้ส่วนราชการจัดให้มีคณะผู้ประเมินอิสระดำเนินการประเมินผลการปฏิบัติราชการของส่วนราชการเกี่ยวกับผลสัมฤทธิ์ของภารกิจ คุณภาพการให้บริการ ความพึงพอใจของประชาชนผู้รับบริการ ความคุ้มค่าในภารกิจ ทั้งนี้ตามหลักเกณฑ์ วิธีการ และระยะเวลาที่ ก.พ.ร.กำหนด

ประการที่สาม

สำนักงานการตรวจเงินแผ่นดิน (สต.) ระเบียบว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน พ.ศ. 2544 กำหนดให้หน่วยรับตรวจหรือมหาวิทยาลัยราชภัฏกาญจนบุรี นำมาตรฐานการควบคุมภายในตามระเบียบฯ ไปใช้เป็นแนวทางการจัดวางระบบการควบคุมภายใน และประเมินผลการควบคุมภายในให้เกิดประสิทธิภาพและประสิทธิผล พร้อมรายงานต่อคณะกรรมการตรวจเงินแผ่นดินและผู้ที่เกี่ยวข้องทราบ

ประการที่สี่

พระราชบัญญัติการศึกษาแห่งชาติ พ.ศ. 2542 แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2545 ได้กำหนดจุดมุ่งหมายและหลักการของการจัดการศึกษาที่มุ่งเน้นคุณภาพและมาตรฐาน โดยกำหนดรายละเอียดไว้ในหมวด 6 มาตรฐานและการประกันคุณภาพการศึกษา ซึ่งประกอบด้วย “ระบบการประกันคุณภาพภายใน” และ “ระบบการประกันคุณภาพภายนอก” เพื่อใช้เป็นกลไกในการผดุงรักษาคุณภาพและมาตรฐานของสถาบันอุดมศึกษา และกำหนดให้สถานศึกษาทุกแห่งต้องได้รับการประเมินคุณภาพภายนอก อย่างน้อย 1 ครั้ง

ในทุกรอบ 5 ปี โดย “สำนักงานรับรองมาตรฐานและประเมินคุณภาพการศึกษา (องค์กรมหาชน) หรือเรียกชื่อย่อว่า “สมศ.”

ดังนั้น สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงต้องมีการประกันคุณภาพตามเกณฑ์ของสำนักงานคณะกรรมการการอุดมศึกษา โดยมหาวิทยาลัยทำหน้าที่ในการกำกับ ดูแลการดำเนินงานในสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ให้มีประสิทธิภาพและประสิทธิผล ปัจจัยที่จะทำให้องค์กรมีการบริหารจัดการที่มีคุณภาพ ได้แก่ ทรัพยากรบุคคล ระบบฐานข้อมูล การบริหารความเสี่ยง การบริหารการเปลี่ยนแปลง ฯลฯ เพื่อสัมฤทธิ์ผลตามเป้าหมายที่กำหนด โดยใช้หลักการบริหารจัดการบ้านเมืองและสังคมที่ดี

ประการสุดท้าย

เนื่องจากโลกมีการเปลี่ยนแปลงอย่างรวดเร็ว และสภาพแวดล้อมต่างๆ ทั้งเศรษฐกิจ สังคม การเมือง เทคโนโลยี นวัตกรรม และการแข่งขัน ทำให้องค์กรทั้งภาครัฐ และภาคเอกชนต้องปรับตัว และพร้อมสำหรับการเปลี่ยนแปลงเพื่อให้เกิดประสิทธิภาพ และประสิทธิผล ดังนั้น การดำเนินงานต่างๆ จึงต้องมีความรับผิดชอบต่อสังคม

ดังนั้น สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงนำหลักการบริหารความเสี่ยงมาดำเนินการเพื่อให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศ สามารถบรรลุผลสำเร็จตามวัตถุประสงค์

4. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

เพื่อให้เข้าใจความหมายและคำจำกัดความของการบริหารความเสี่ยง ควรทำความเข้าใจกับความหมายของคำที่เกี่ยวข้อง ต่อไปนี้

1. ความเสี่ยง (Risk) หมายถึง เหตุการณ์ที่มีความไม่แน่นอน ซึ่งมีโอกาสที่จะเกิดขึ้นในอนาคต และมีผลกระทบทั้งทางบวก และทางลบ หากเป็นทางลบจะก่อให้เกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ ทำให้การดำเนินงานของมหาวิทยาลัยฯ ไม่ประสบความสำเร็จตามวัตถุประสงค์ที่กำหนดไว้ จึงจำเป็นต้องพิจารณาโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์ และผลกระทบ (Impact) ที่จะได้รับ ความเสี่ยงสามารถจำแนกได้เป็นลักษณะ ดังนี้

- ความเสี่ยงด้านทรัพยากร (Resources Risk) หมายถึง ความเสี่ยงที่เกิดจากความไม่พร้อมหรือขาดประสิทธิภาพในการดำเนินงานด้านการเงิน งบประมาณ การควบคุมค่าใช้จ่าย ระบบสารสนเทศ ด้านอาคารสถานที่

- ความเสี่ยงด้านยุทธศาสตร์ หรือกลยุทธ์ (Strategic Risk) หมายถึง ความเสี่ยงที่เกิดจากการวางแผนกลยุทธ์หรือแผนปฏิบัติราชการ รวมถึงการนำไปปฏิบัติที่ไม่เหมาะสม หรือไม่สอดคล้องกับปัจจัยต่างๆ ทั้งที่เป็นปัจจัยภายในและภายนอกองค์กร ซึ่งอาจส่งผลกระทบต่อทิศทางการพัฒนา และการบรรลุตามเป้าหมายและวัตถุประสงค์ขององค์กร

- ความเสี่ยงด้านการปฏิบัติตามกฎหมาย/กฎระเบียบ/ข้อบังคับ (Compliance Risk) หมายถึง ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามกฎระเบียบ หรือข้อบังคับที่เกี่ยวข้องได้ หรือกฎระเบียบที่มีอยู่ไม่เหมาะสม เป็นอุปสรรคต่อการปฏิบัติงาน หรือไม่สามารถปฏิบัติได้ทันตามเวลาที่กำหนด และอาจมีผลต่อการลงโทษตามกฎหมายที่เกี่ยวข้อง ตลอดจนการปฏิบัติตามผลการปฏิบัติตามกฎระเบียบหรือข้อบังคับที่เกี่ยวข้อง

- ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk) หมายถึง ความเสี่ยงที่เกิดขึ้นในกระบวนการทำงานตามปกติทุกขั้นตอน ไม่ว่าจะเป็นเรื่องของกระบวนการการบริหารหลักสูตร การบริหารงานวิจัย ระบบงาน ระบบประกันคุณภาพ ว่ามีการดำเนินงานตามขั้นตอนอย่างถูกต้องเหมาะสม และมีระบบควบคุมตรวจสอบที่ดีเพียงใด ถ้าไม่ดีพอ องค์กรต้องหาวิธีในการจัดการไม่ให้ความเสี่ยงนั้นเกิดขึ้น มิฉะนั้นอาจจะส่งผลกระทบต่อความสำเร็จของการดำเนินงานตามแผนปฏิบัติราชการหรือแผนกลยุทธ์ขององค์กร

- ความเสี่ยงด้านบุคลากรและความเสี่ยงด้านธรรมาภิบาล (Human and Good Govemance Risk) หมายถึง ความเสี่ยงที่เกิดจากการขาดประสิทธิภาพในการกำหนดกรอบอัตรากำลังการสรรหาบุคลากร การบรรจุแต่งตั้ง การฝึกอบรม การโยกย้าย และไม่ได้จัดทำข้อกำหนดด้านจริยธรรมไว้อย่างชัดเจนในด้านต่าง ๆ

- ความเสี่ยงจากเหตุการณ์ภายนอก (External Environment Risk) หมายถึง ความเสี่ยงที่เกิดขึ้นจากสภาพแวดล้อมที่มีการเปลี่ยนแปลงตลอดเวลา และอาจส่งผลกระทบทำให้องค์กรไม่สามารถดำเนินการสำเร็จตามเป้าหมาย

- ความเสี่ยงด้านอื่นๆ (Other Risk) ตามบริบทของสถาบัน หมายถึง ความเสี่ยงที่เกิดขึ้นจากความไม่สามารถดำเนินการได้ตามแนวทางของมหาวิทยาลัย

2. ปัจจัยเสี่ยง (Risk Factor) หมายถึง สาเหตุของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ตามขั้นตอนการดำเนินงานที่กำหนดไว้ ทั้งปัจจัยภายในและภายนอก ซึ่งองค์กรควรระบุสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดกลยุทธ์/มาตรการ/แนวทางในการลดความเสี่ยงได้อย่างถูกต้อง เหมาะสมกับสถานการณ์และบริบทขององค์กร

ปัจจัยภายใน ประกอบด้วย

1) กลยุทธ์ (Strategy) เหมาะสมกับสถานการณ์เพียงใด

2) โครงสร้างองค์กร (Structure) ที่หน่วยงานและระดับขั้นการบังคับบัญชาที่เหมาะสมที่จะประกอบพันธกิจให้สำเร็จตามวัตถุประสงค์ขององค์กรเพียงใด

3) ระบบ (System) การดำเนินงานมีระบบที่ถูกต้องเหมาะสมเพียงใด (ระบบการคัดเลือกสรรหา ระบบการประเมินผล ระบบการพิจารณาความดีความชอบ ระบบการเงิน ระบบการผลิต (บัณฑิต) ระบบการจัดซื้อจัดจ้าง ระบบสารสนเทศ)

4) รูปแบบการบริหารจัดการ (Style) เหมาะสมสอดคล้องกับสภาพแวดล้อมที่เปลี่ยนแปลงอยู่ตลอดเวลาเพียงใด

5) บุคลากร (Staff) มีศักยภาพ (สมรรถนะ) เหมาะสมกับงานที่ได้รับมอบหมายเพียงใด

6) ทักษะ (Skill) ขององค์กรและบุคลากรเมื่อเทียบกับคู่แข่งแล้วเหนือกว่าหรือด้อยกว่า

7) ค่านิยม (Share Value) ค่านิยมร่วมของบุคลากร มีส่วนสนับสนุนให้องค์กรสามารถปรับไปตามสภาพแวดล้อม

ปัจจัยภายนอก ประกอบด้วย

1) ด้านเศรษฐกิจ ได้แก่ ราคาน้ำมัน ความผันผวนของอัตราแลกเปลี่ยน อัตราดอกเบี้ย อัตราว่างงาน และตลาดหุ้น

2) ด้านสังคมและสิ่งแวดล้อม ได้แก่ การเปลี่ยนแปลงด้านประชากร ความขัดแย้งในสังคม การก่อความไม่สงบ ภัยสงคราม ภัยธรรมชาติ เป็นต้น

3) ด้านการเมือง ส่งผลต่อความต่อเนื่องในนโยบายรัฐบาล

4) ด้านกฎหมาย ได้แก่ ความคลุมเครือของกฎหมายที่เกี่ยวข้อง การเปลี่ยนแปลงกฎระเบียบต่างๆ ความไม่มั่นใจในการบังคับใช้กฎหมาย กฎหมายไม่ครอบคลุม กฎ ระเบียบ ข้อบังคับที่ล้าหลัง ไม่ทันการเปลี่ยนแปลง

5) ด้านเทคโนโลยี ได้แก่ ความก้าวหน้าของเทคโนโลยีที่ส่งผลต่อความสามารถในการแข่งขันขององค์กร

3. การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง และการวิเคราะห์เพื่อจัดลำดับความเสี่ยงที่จะมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร โดยการประเมินจากโอกาสที่จะเกิดเหตุการณ์ (Likelihood) และผลกระทบ (Impact) จากเหตุการณ์ความเสี่ยง

- โอกาสที่จะเกิดเหตุการณ์ (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง

- ผลกระทบ (Impact) หมายถึง ปริมาณของความรุนแรงความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์หรือความเสี่ยง

- ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่จะได้จากการประเมินโอกาส และผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 4 ระดับ คือ ความเสี่ยงสูงมาก ความเสี่ยงสูง ความเสี่ยงปานกลาง ความเสี่ยงน้อย

4. การจัดการความเสี่ยง (Risk Response) หมายถึง แนวทางในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์หรือความเสี่ยง หรือลดผลกระทบความเสียหายจากเหตุการณ์ความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ (Risk Acceptance) โดยการเลือกแนวทางที่จะจัดการกับความเสี่ยงนั้น เปรียบเทียบกับประโยชน์

ที่จะได้รับว่าเหมาะสมและคุ้มค่าหรือไม่ กรณีเป็นความเสี่ยงที่เกิดจากปัจจัยภายนอกซึ่งไม่สามารถควบคุมได้ การป้องกันหรือลดความเสี่ยงกระทำได้ ดังนี้

1) การลดความรุนแรงของความเสี่ยง (Risk Reduction) หรือลดความเป็นไปได้ในการเกิดความเสี่ยง คือ ความพยายามลดความเสี่ยงโดยการเพิ่มเติม หรือเปลี่ยนแปลงขั้นตอนบางส่วนของกิจกรรมหรือโครงการที่จะนำไปสู่เหตุการณ์ที่เป็นความเสี่ยง หรือลดความน่าจะเป็นที่เหตุการณ์ที่เป็นความเสี่ยงจะเกิดขึ้น โดยมีการเตรียมความพร้อมของบุคลากร เครื่องมือ อุปกรณ์ต่างๆ ด้วยการดำเนินการให้มีการฝึกอบรมบุคลากรให้มีความรู้ความเข้าใจ การกำหนดให้ผู้จัดซื้อจัดจ้าง ผู้ตรวจรับ ผู้รับมอบงานแยกออกจากกัน หรือลดระดับความรุนแรงของผลกระทบเมื่อเหตุการณ์ที่เป็นความเสี่ยงเกิดขึ้น ด้วยการติดตั้งเครื่องดับเพลิง การสำรองข้อมูล (Back up) เป็นระยะๆ มีการบันทึกข้อมูลสำรอง

2) การแบ่งปันความเสี่ยง (Risk Sharing) คือ การถ่ายทอดความเสี่ยงให้ผู้อื่น/หน่วยงานอื่นร่วมกันรับผิดชอบ เมื่อเกิดเหตุการณ์ความเสี่ยงขึ้นจะต้องรับผลกระทบร่วมกัน ซึ่งการแบ่งรับความเสี่ยงไม่ได้เป็นการลดความเสี่ยงที่จะเกิดขึ้น แต่เป็นการรับประกันว่าเมื่อเกิดความเสียหายแล้ว องค์กรจะได้รับการชดใช้จากผู้อื่น เช่น การทำประกัน (Insurance) การทำสัญญา (Contracts) การรับประกัน (Warranties) การจ้างผู้ดำเนินการภายนอก

3) การยอมรับความเสี่ยง (Risk Acceptance) คือ การรับความเสี่ยงไว้จัดการเองภายในหน่วยงาน หากทำการวิเคราะห์แล้วเห็นว่าไม่มีวิธีการจัดการความเสี่ยงที่เหมาะสม เนื่องจากต้นทุนการจัดการความเสี่ยงสูงกว่าประโยชน์ที่จะได้รับ แต่ควรมีมาตรการติดตามอย่างใกล้ชิดเพื่อรองรับผลที่จะเกิดขึ้น

4) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การปฏิเสธและหลีกเลี่ยงโอกาสที่จะเกิดความเสี่ยง โดยการหยุด ยกเลิก หรือเปลี่ยนแปลงกิจกรรมหรือโครงการที่จะนำไปสู่เหตุการณ์ที่เป็นความเสี่ยงไปสู่เป้าหมายที่วางไว้ได้ กรณีเป็นความเสี่ยงเกี่ยวกับการควบคุมภายใน ที่เกิดจากปัจจัยภายในซึ่งอยู่ภายใต้การควบคุมของฝ่ายบริหาร การป้องกันหรือลดความเสี่ยงกระทำได้โดยจัดให้มีกิจกรรมการควบคุมอย่างเพียงพอและเหมาะสม เพื่อลดมูลเหตุของแต่ละโอกาสที่องค์กรจะเกิดความเสียหาย ทั้งในรูปแบบของตัวเงินและไม่ใช่ตัวเงิน เช่น ชื่อเสียง การฟ้องร้องจากการไม่ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ ประสิทธิภาพ ประสิทธิผล หรือความคุ้มค่า

5. การบริหารความเสี่ยง (Enterprise Risk Management) หมายถึง การบริหารปัจจัย และควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่างๆ เพื่อลดมูลเหตุของแต่ละโอกาสที่องค์กรจะเกิดความเสียหาย โดยให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างเป็นระบบ โดยคำนึงถึงการบรรลุพันธกิจ (ภารกิจ) ยุทธศาสตร์ เป้าประสงค์ กลยุทธ์ และชื่อเสียงขององค์กรเป็นสำคัญ โดยได้รับการสนับสนุนและการมีส่วนร่วมในการบริหารความเสี่ยงจากหน่วยงานทุกระดับทั่วทั้งองค์กร

6. การติดตามประเมินผล หมายถึง กระบวนการประเมินคุณภาพการปฏิบัติงานและประเมินประสิทธิผลของการควบคุมภายในที่กำหนดไว้อย่างต่อเนื่องและสม่ำเสมอ เพื่อให้เกิดความมั่นใจว่า ระบบการควบคุมภายใน การบริหารความเสี่ยงที่กำหนดไว้มีความเพียงพอเหมาะสม มีการปฏิบัติการจริง ข้อบกพร่องที่พบได้รับการแก้ไขอย่างเหมาะสมและทันเวลา

7. เป้าประสงค์ขององค์กร (Goal) หมายถึง ความต้องการที่ผู้วางยุทธศาสตร์หรือผู้บริหารต้องการให้เกิดขึ้นตามที่คาดหวังไว้ โดยทั่วไปจะกำหนดให้มีลักษณะกว้างๆ ทั้งในเชิงแก้ปัญหา (Problematic Goal) และเชิงพัฒนา (Development Goal)

8. การควบคุมภายใน (Control) คือ กระบวนการ (Process) ปฏิบัติงานที่ฝ่ายบริหารและบุคลากรของหน่วยงานจัดให้มีขึ้น เพื่อควบคุมการปฏิบัติงานของหน่วยงานให้มีประสิทธิภาพ และประสิทธิผล ซึ่งการควบคุมภายในส่วนใหญ่จะออกมาในรูปแบบของนโยบาย แนวทาง กฎ ระเบียบ ข้อบังคับ คู่มือหรือขั้นตอนการปฏิบัติต่างๆ เพื่อลดความเสี่ยง (Risk) ที่จะเกิดขึ้น

บทที่ 2
แนวทางการบริหารความเสี่ยงและการควบคุมภายใน

การบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประกอบด้วย

1. นโยบาย วัตถุประสงค์ของการบริหารความเสี่ยง
2. โครงสร้างการบริหารความเสี่ยง
3. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการและคณะทำงานบริหารความเสี่ยง

1. นโยบาย วัตถุประสงค์ของการบริหารความเสี่ยงและการควบคุมภายใน

1.1 นโยบายการบริหารความเสี่ยง

ผู้บริหารให้นโยบายบริหารความเสี่ยงตามภารกิจหลักของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ และต้องเป็นไปตามแนวทาง/นโยบายบริหารความเสี่ยงดังนี้

1) ให้มีการบริหารความเสี่ยงทั่วทั้งองค์กรแบบบูรณาการ โดยมีการจัดการอย่างเป็นระบบและต่อเนื่อง

2) ให้มีการกำหนดกระบวนการบริหารความเสี่ยงที่เป็นระบบมาตรฐานเดียวกันทั่วทั้งองค์กร

3) ให้มีการติดตามประเมินผลการบริหารความเสี่ยงและมีการทบทวนปรับปรุงอย่างสม่ำเสมอ

4) ให้มีการนำเทคโนโลยีสารสนเทศมาใช้เพื่อการจัดการที่ดี

5) ให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของการดำเนินงานตามปกติ

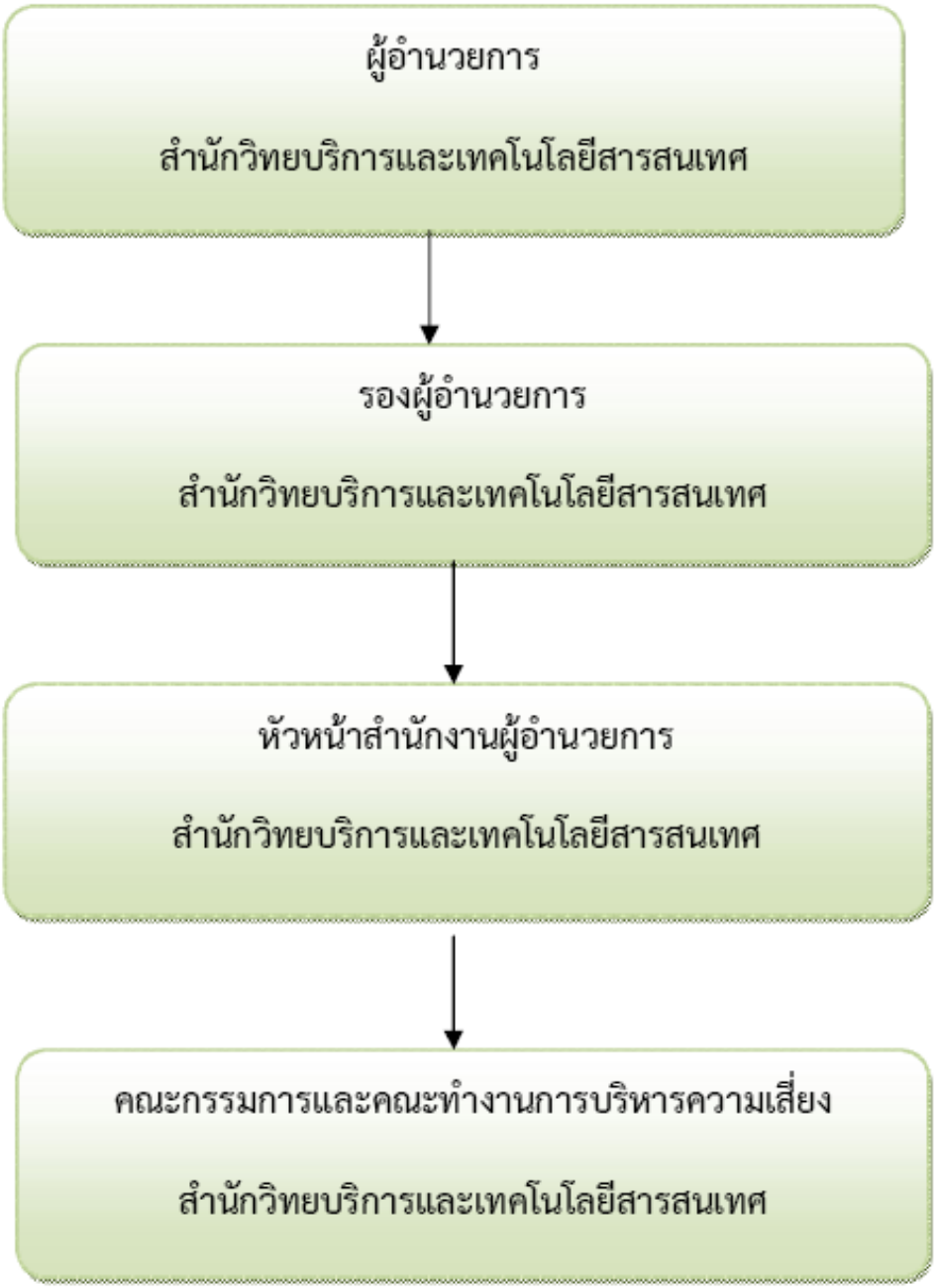
1.2 วัตถุประสงค์ของการบริหารความเสี่ยง

1) เพื่อช่วยเพิ่มประสิทธิภาพของการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์และนโยบายแล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงานหรือดำเนินงานตามแผนที่กำหนดไว้

2) เพื่อให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศ สามารถลดขนาดของความเสียหายที่จะเกิดขึ้นในอนาคตให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ ควบคุมได้ และตรวจสอบได้

2. โครงสร้างการบริหารความเสี่ยง

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีโครงสร้างการบริหารความเสี่ยง



3. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการและคณะทำงานบริหารความเสี่ยง

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ กำหนดให้การบริหารความเสี่ยงเป็นความรับผิดชอบร่วมกันของผู้บริหารและบุคลากรทุกระดับเพื่อให้มีการปฏิบัติอย่างเป็นระบบและต่อเนื่อง บทบาทหน้าที่และความรับผิดชอบหลักของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงของสำนักวิทยบริการและเทคโนโลยีสารสนเทศมีดังนี้

ผู้ที่เกี่ยวข้อง	หน้าที่และความรับผิดชอบ
1. คณะกรรมการบริหารความเสี่ยง	1. พิจารณากำหนดนโยบายและระบบบริหารความเสี่ยง รวมทั้งแผนการดำเนินการบริหารความเสี่ยงขององค์กร 2. ติดตามและพิจารณาผลการดำเนินการบริหารความเสี่ยงตั้งแต่กระบวนการระบุความเสี่ยง วิเคราะห์ปัจจัยเสี่ยง ประเมิน จัดการ ติดตามและรายงานอย่างเป็นระบบ 3. ให้การสนับสนุนโดยการจัดให้มีการแนะนำกระบวนการบริหารความเสี่ยงแก่บุคลากรฝ่ายต่างๆ ภายในหน่วยงานตลอดจนติดตามให้มีการปฏิบัติอย่างต่อเนื่องและสม่ำเสมอ 4. ให้ข้อเสนอแนะกำหนดนโยบาย แนวทางในการบริหารความเสี่ยงและเพื่อเสนอต่อมหาวิทยาลัย
2. คณะทำงานบริหารความเสี่ยง	1. ดำเนินการวิเคราะห์และระบุปัจจัยเสี่ยงที่อาจจะส่งผลกระทบหรือสร้างความเสียหาย หรือความล้มเหลวหรือลดโอกาสที่จะบรรลุเป้าหมายขององค์กร รวมทั้งจัดลำดับความสำคัญของปัจจัยเสี่ยงในแต่ละด้าน 2. ดำเนินการจัดทำแผนการบริหารความเสี่ยงในแต่ละด้าน ทั้งระดับองค์กรและระดับกิจกรรม 3. กำหนดแนวทางรวมทั้งข้อเสนอแนะในการปรับปรุงแผนบริหารความเสี่ยง

บทที่ 3
กระบวนการบริหารความเสี่ยงและการควบคุมภายใน

กระบวนการบริหารความเสี่ยง เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดระดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงาน หรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยง โดยกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ ซึ่งกระบวนการดังกล่าวนี้จะสำเร็จได้ต้องมีการสื่อสารให้คนในองค์กรมีความรู้ความเข้าใจในเรื่องบริหารความเสี่ยงในทิศทางเดียวกัน ตลอดจนมีการจัดทำระบบสารสนเทศ เพื่อใช้ในการวิเคราะห์ประเมินความเสี่ยง ทั้งนี้สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีกระบวนการและขั้นตอนการบริหารความเสี่ยง 7 ขั้นตอนดังนี้

1. การกำหนดวัตถุประสงค์ เป็นการกำหนดวัตถุประสงค์และกลยุทธ์ที่ชัดเจนของแผนงาน โครงการ/กิจกรรมตามแผนปฏิบัติราชการประจำปีและแผนปฏิบัติราชการของมหาวิทยาลัย

2. การระบุความเสี่ยง เป็นการระบุเหตุการณ์ใดๆ ทั้งที่มีผลดี และผลเสียต่อการบรรลุวัตถุประสงค์ โดยต้องระบุไว้ด้วยเหตุการณ์นั้นจะเกิดขึ้นที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร

3. การประเมินความเสี่ยง เป็นการวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยพิจารณาจากการประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood) และความรุนแรงของผลกระทบจากเหตุการณ์ความเสี่ยง (Impact) โดยอาศัยเกณฑ์มาตรฐานที่กำหนดไว้ ทำให้การตัดสินใจจัดการกับความเสี่ยงเป็นไปอย่างเหมาะสม

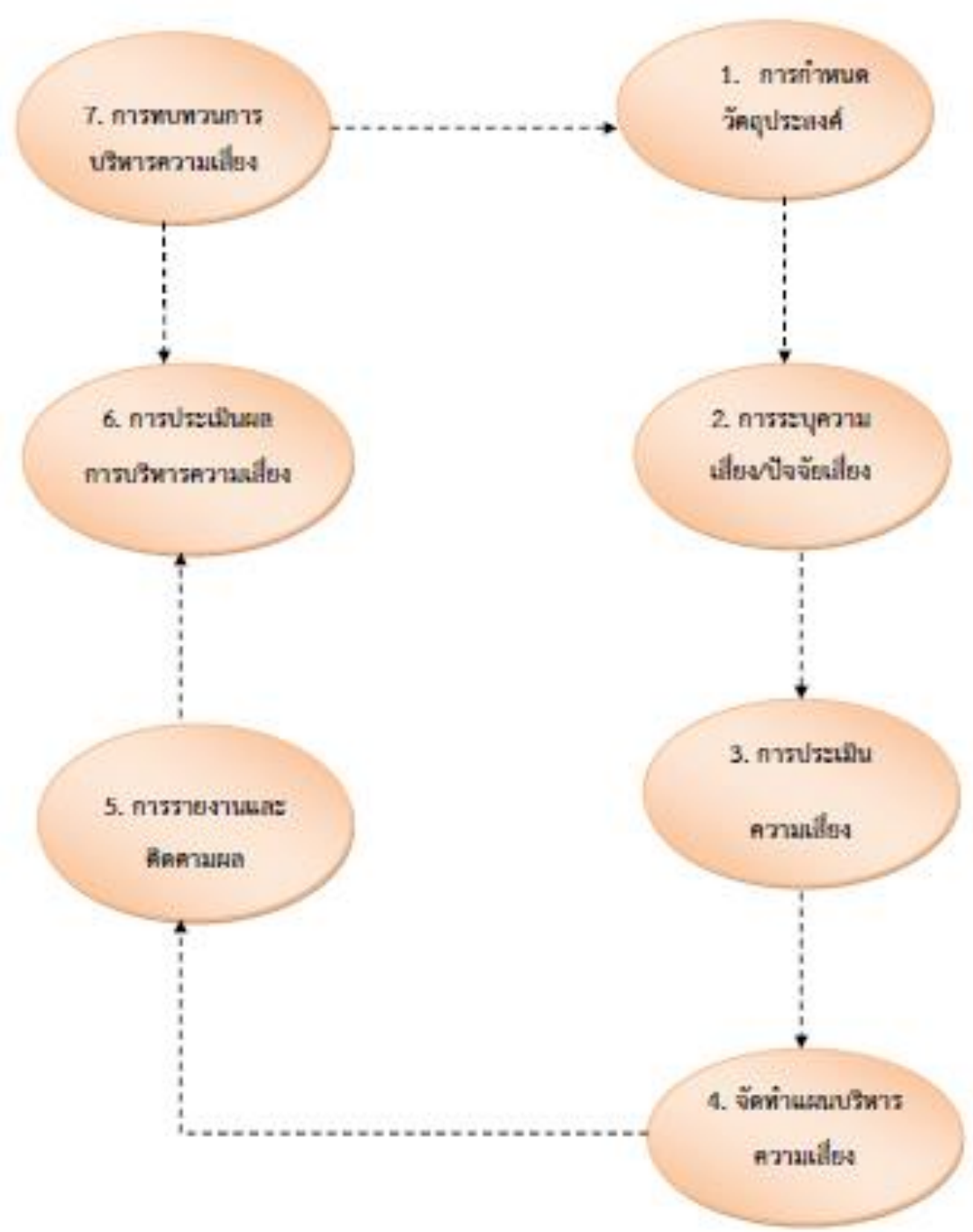
4. การจัดทำแผนบริหารความเสี่ยง เป็นการกำหนดมาตรการ หรือแผนปฏิบัติการในการจัดการและควบคุมความเสี่ยงที่สูง และสูงมากนั้นให้ลดลง ให้อยู่ในระดับที่ยอมรับได้ สามารถปฏิบัติได้จริงและควรต้องพิจารณาถึงความคุ้มค่าในด้านค่าใช้จ่ายและต้นทุนที่ต้องใช้ลงทุนในการกำหนดมาตรการหรือแผนปฏิบัติการนั้นหรือประโยชน์ที่จะได้รับด้วย

5. การรายงานและติดตามผล เป็นการรายงานและติดตามผลการดำเนินงานตามแผนการบริหารความเสี่ยงที่ได้ดำเนินการทั้งหมดตามลำดับให้ฝ่ายบริหารรับทราบ และให้ความเห็นชอบดำเนินงานตามแผนการบริหารความเสี่ยง

6. การประเมินผลบริหารความเสี่ยง เป็นการประเมินการบริหารความเสี่ยงประจำปีต่อคณะทำงานวิเคราะห์และจัดทำแผนบริหารความเสี่ยงของมหาวิทยาลัย เพื่อให้มั่นใจว่าองค์กรมีการบริหารความเสี่ยงเป็นอย่างเหมาะสม เพียงพอ ถูกต้องและมีประสิทธิผล มาตรการหรือกลไกควบคุมความเสี่ยงที่ดำเนินการสามารถลดและควบคุมความเสี่ยงที่เกิดขึ้นได้จริงและอยู่ในระดับที่ยอมรับได้หรือต้องจัดหามาตรการ หรือตัวควบคุมอื่นเพิ่มเติม เพื่อให้ความเสี่ยงที่ยังเหลืออยู่หลังมีการจัดการอยู่ในระดับที่ยอมรับได้ และให้องค์กรมีการบริหารความเสี่ยงอย่างต่อเนื่อง

7. การทบทวนการบริหารความเสี่ยง เป็นการทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงในทุกขั้นตอนเพื่อพัฒนาระบบให้ดียิ่งขึ้น

กระบวนการบริหารความเสี่ยงและการควบคุมภายใน



1. การกำหนดวัตถุประสงค์ (Set Objectives)

การกำหนดวัตถุประสงค์ภายในองค์กร จะต้องมีความสอดคล้องและเป็นไปในทิศทางเดียวกันกล่าวคือ วัตถุประสงค์ขององค์กรจะต้องสอดคล้องกับวิสัยทัศน์ พันธกิจ และทิศทางการดำเนินงานขององค์กร และจะต้องสอดคล้องกันตั้งแต่ระดับองค์กร หน่วยงาน กิจกรรม จนถึงระดับบุคคล เพื่อให้วัตถุประสงค์ในภาพรวมบรรลุเป้าประสงค์ ทราบขอบเขตการดำเนินงานในแต่ละระดับ และสามารถวิเคราะห์ความเสี่ยงที่จะเกิดขึ้นได้ครบถ้วน ดังนั้นวัตถุประสงค์จะแสดงให้เห็นถึง “ผลลัพธ์” ที่องค์กรต้องการจะบรรลุไม่ใช่การกล่าวถึง “กระบวนการ” ในการปฏิบัติงานซึ่งมีลำดับขั้นตอนดังนี้

1) กำหนดพันธกิจขององค์กร

2) กำหนดวัตถุประสงค์ในระดับองค์กรให้สอดคล้องกับพันธกิจที่กำหนดไว้

3) กำหนดกิจกรรมที่ทำให้บรรลุวัตถุประสงค์ในระดับองค์กร

4) กำหนดวัตถุประสงค์ในระดับกิจกรรม

วัตถุประสงค์ของการบริหารความเสี่ยงอาจแบ่งออกได้เป็น 2 ระดับ คือ

(1) วัตถุประสงค์ในระดับองค์กร เป็นวัตถุประสงค์ของการดำเนินงานในภาพรวมองค์กรตามแผนปฏิบัติราชการประจำปี และแผนการปฏิบัติราชการ 4 ปี

(2) วัตถุประสงค์ในระดับกิจกรรม เป็นวัตถุประสงค์ของการดำเนินงานที่เฉพาะเจาะจงลงไปสำหรับแต่ละกิจกรรมที่องค์กรกำหนด เพื่อให้บรรลุวัตถุประสงค์ขององค์กรซึ่งวัตถุประสงค์ของแต่ละกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร การกำหนดที่ชัดเจนช่วยให้การระบุและวิเคราะห์ความเสี่ยงที่จะเกิดขึ้นได้อย่างครบถ้วน ซึ่งวัตถุประสงค์ที่กำหนดขึ้นในแต่ละระดับ ควรมีการกำหนดเป้าหมายและตัวชี้วัดความสำเร็จที่ชัดเจนและสามารถวัดผลได้วัตถุประสงค์ที่ดีควรมีลักษณะดังนี้

Specific : มีการกำหนดเป้าหมายที่ชัดเจน

Measurable : สามารถวัดผลหรือประเมินผลได้

Achievable : สามารถปฏิบัติให้บรรลุผลได้

Reasonable : สมเหตุผล มีความเป็นไปได้

Time constrained : มีกรอบเวลาที่ชัดเจนและเหมาะสม

อย่างไรก็ตาม หากหน่วยงานมีการกำหนดตัวชี้วัดและภารกิจหลักของงานอยู่แล้ว ก็สามารถนำตัวชี้วัดและค่าเป้าหมายกำหนดไว้มาใช้แทนวัตถุประสงค์ก็ได้

2. การระบุความเสี่ยง (Risk Identification) ในการระบุความเสี่ยง ควรต้องทำความเข้าใจในความหมายของ “ความเสี่ยง” และ “ปัจจัยเสี่ยง” ก่อน

1) ความเสี่ยง หมายถึง เหตุการณ์/การกระทำใดๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว

หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจหลักที่กำหนด ในกฎหมายจัดตั้งส่วนราชการและเป้าหมายตามแผนปฏิบัติการ

การบริหารความเสี่ยง หมายถึง กระบวนการที่ใช้ในการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และการกำหนดแนวทางหรือมาตรการควบคุมเพื่อป้องกัน หรือลดความเสี่ยงเพื่อมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร

2) ปัจจัยเสี่ยง หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นเกิดขึ้นที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

ตัวอย่าง ปัจจัยเสี่ยง/ต้นเหตุ/สาเหตุของความเสี่ยง

- บรรยากาศทางจริยธรรม
- ความกดดันจากฝ่ายบริหาร
- ความรู้ ความสามารถของบุคลากร
- ราคา/มูลค่าของทรัพย์สิน
- ปริมาณการบันทึกรายการและจำนวนเอกสาร
- สภาพความจริงในการแข่งขัน
- ระเบียบต่างๆ ของทางราชการ
- ระบบข้อมูลสารสนเทศที่ประมวลด้วยคอมพิวเตอร์
- การกระจายของสถานที่ในการปฏิบัติงาน
- ความเพียงพอและประสิทธิผลของการควบคุมภายใน
- การเปลี่ยนแปลงองค์กร การปฏิบัติงาน เทคโนโลยี
- การตัดสินใจของฝ่ายบริหาร

3) การระบุความเสี่ยง เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องกับโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ โดยต้องคำนึงถึง

3.1) สภาพแวดล้อมภายนอกหน่วยงาน ซึ่งเป็นสิ่งที่ไม่อยู่ในความรับผิดชอบของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ และมหาวิทยาลัยราชภัฏกาญจนบุรี เช่น นโยบายภาครัฐ กฎหมาย ระเบียบข้อบังคับ

3.2) สภาพแวดล้อมภายในหน่วยงานสำนักวิทยบริการและเทคโนโลยีสารสนเทศ และมหาวิทยาลัยราชภัฏกาญจนบุรี เช่น รูปแบบบริหาร สั่งการ การมอบหมายอำนาจหน้าที่ความรับผิดชอบ โครงสร้างองค์กร ระเบียบข้อบังคับภายใน

วิธีการและเทคนิคในการระบุความเสี่ยง มีหลายวิธีซึ่งแต่ละหน่วยงานอาจเลือกใช้ได้ตามเหมาะสม ดังนี้

1) การระบุความเสี่ยงโดยการรวมกลุ่ม ระดมสมอง เพื่อให้ได้ความเสี่ยงที่หลากหลาย

2) การระบุความเสี่ยงโดยการใช้ checklist ในกรณีที่มีข้อจำกัดด้านงบประมาณและทรัพยากร

3) การระบุความเสี่ยงโดยการวิเคราะห์สถานการณ์จากการตั้งคำถาม “what – if”

4) การระบุความเสี่ยงโดยการวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอนที่สำคัญ

การระบุความเสี่ยง สามารถดำเนินการได้หลายวิธี เช่น จากการวิเคราะห์กระบวนการทำงาน การวิเคราะห์ทบทวนผลการปฏิบัติงานที่ผ่านมา การประชุมเชิงปฏิบัติการ การระดมสมอง การเปรียบเทียบกับองค์กรอื่น การสัมภาษณ์ แบบสอบถาม เป็นต้น

การระบุความเสี่ยงแบ่งเป็น 4 ประเภท ได้แก่

1) ความเสี่ยงเชิงยุทธศาสตร์ มีการวิเคราะห์ความเสี่ยงในด้านต่างๆ ที่อาจก่อให้เกิดการเปลี่ยนแปลงหรือการไม่บรรลุผลตามเป้าหมายในแต่ละประเด็นยุทธศาสตร์ของส่วนราชการ และดำเนินการวางมาตรการบริหารความเสี่ยงตาม 5 ขั้นตอนดังกล่าวข้างต้น

2) ความเสี่ยงด้านธรรมาภิบาล มีการวิเคราะห์ความเสี่ยงด้านธรรมาภิบาลที่จะเกิดขึ้นในกระบวนงานหลักขององค์กร เพื่อให้มั่นใจว่าการดำเนินการเป็นไปตามหลักธรรมาภิบาล เช่น ความมีประสิทธิภาพ ความคุ้มค่า ความโปร่งใสตรวจสอบได้ เป็นต้น รวมถึงมีการวิเคราะห์ความเสี่ยงในการกำกับดูแลตนเองที่ดีด้วย

“การกำกับดูแลตนเองที่ดี” (Organizational Governance) หมายถึง การจัดการเพื่อให้เกิดการควบคุม และการตรวจสอบการดำเนินการของส่วนราชการ รวมทั้งความรับผิดชอบในด้านต่างๆ ของผู้บริหารสูงสุดขององค์กร อาจรวมถึงการมีคณะกรรมการดำเนินการขององค์กร การติดตามและประเมินผลการดำเนินการของผู้บริหารสูงสุดขององค์กร การตรวจสอบด้านการเงิน การจัดการความเสี่ยง การเปิดเผยข้อมูลข่าวสาร และป้องกันและปราบปรามการทุจริตและประพฤติมิชอบ โดยมีการวิเคราะห์และจัดทำแผนบริหารความเสี่ยงในเรื่องการกำกับดูแลตนเองที่ดีด้านองค์กร เช่น การวิเคราะห์ความเสี่ยงในการดำเนินการที่อาจก่อให้เกิดการทุจริตและ/หรือละเว้นการปฏิบัติหน้าที่โดยมิชอบในการปฏิบัติราชการ และด้านการเงิน เป็นต้น และนำแผนดังกล่าวไปเป็นแนวทางปฏิบัติเพื่อให้เกิดประสิทธิภาพในการดูแลตนเองที่ดีและควบคุมการบริหารจัดการภายในองค์กร

3) ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของฐานข้อมูลและสารสนเทศ โดยต้องดำเนินการดังต่อไปนี้

(1) มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดความเสียหายในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบสารสนเทศ และการสำรองและกู้คืนข้อมูลจากความเสียหาย (Back up and Recovery)

(2) มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan)

(3) มีระบบรักษาความมั่นคงและปลอดภัยของระบบฐานข้อมูล (Security) เช่น ระบบ Anti-Virus ระบบไฟฟ้าสำรอง เป็นต้น

(4) มีการกำหนดสิทธิให้ผู้ใช้แต่ละระดับ (Access rights)

4) ความเสี่ยงด้านกระบวนการ ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของกระบวนการเพื่อสร้างคุณค่าเพื่อให้เป็นไปตามมาตรฐานการปฏิบัติงานที่กำหนดการบริหารความเสี่ยงของกระบวนการอาจนำแนวคิดในการออกแบบระบบควบคุมมาใช้ได้ ซึ่งระบบควบคุมกระบวนการมีปัจจัยสำคัญดังต่อไปนี้

(1) วัตถุประสงค์ของการควบคุม

(2) ความคุ้มค่าของการควบคุม

(3) ความทันการณ์ของการติดตามและบอกเหตุ

(4) ความสม่ำเสมอของกลไกการควบคุม

(5) การจูงใจผู้ปฏิบัติงาน

3. การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยง เป็นการนำปัจจัยเสี่ยงมาวิเคราะห์เพื่อประเมินโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบจากความเสี่ยง และจัดระดับความเสี่ยง โดยหน่วยงานอาจจะเชิญผู้ที่เกี่ยวข้องมาร่วมประชุมปรึกษาหารือร่วมกัน หรือกรณีที่เป็นเรื่องที่เกี่ยวข้องกับทุกคนและต้องการความคิดเห็นจากบุคคลจำนวนมากอาจจะพิจารณาใช้วิธีการเก็บข้อมูลจากแบบสอบถาม การประเมินความเสี่ยง ประกอบด้วย 4 ขั้นตอน คือ

3.1 การกำหนดเกณฑ์การประเมินมาตรฐาน

การประเมินโอกาสที่จะเกิดความเสี่ยง และระดับความรุนแรงของผลกระทบจากความเสี่ยง สามารถกำหนดเกณฑ์ได้ทั้งเกณฑ์ในเชิงปริมาณ และเชิงคุณภาพ ทั้งนี้ขึ้นอยู่กับข้อมูล สภาพแวดล้อมของหน่วยงานและดุลยพินิจการตัดสินใจของคณะกรรมการ คณะทำงาน และฝ่ายบริหารของหน่วยงาน โดยเกณฑ์ในเชิงปริมาณจะเหมาะกับหน่วยงานที่มีข้อมูลตัวเลขมาใช้ในการวิเคราะห์อย่างเพียงพอ สำหรับหน่วยงานที่มีข้อมูลที่ไม่สามารถระบุเป็นตัวเลขที่ชัดเจนให้กำหนดเกณฑ์เชิงคุณภาพ ดังนี้

3.1.1 ระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood)

หน่วยงานระบุตัวเลขระดับโอกาสที่จะเกิดความเสี่ยง (5-4-3-2-1) ซึ่งเป็นการประเมินความเป็นไปได้ที่จะเกิดเหตุการณ์หรือความเสี่ยง ผู้ประเมินของหน่วยงานควรเป็นผู้ที่มีความรู้ความชำนาญ และมีประสบการณ์ในเรื่องนั้นๆ สำหรับวิธีการเลือกตัวเลขระดับโอกาส (5-4-3-2-1) ของแต่ละปัจจัยความเสี่ยง ใช้วิธีวิเคราะห์ร่วมกันหากไม่สามารถหาข้อยุติได้ อาจใช้เสียงข้างมากในที่ประชุม หรือให้แต่ละคนเป็นผู้ให้คะแนนแล้วนำมาหาค่าเฉลี่ย

ตัวอย่างเกณฑ์ โอกาสที่จะเกิดความเสี่ยง (Measures of Likelihood)

ระดับคะแนน	โอกาสที่จะเกิดความเสี่ยง (Likelihood)	รายละเอียด (Description)
5	สูงมาก	เกิดขึ้นได้จากสภาพแวดล้อมปกติ (1 เดือนต่อ 1 ครั้ง หรือเกิดขึ้นทุกเดือน หรือมากกว่า 1 ครั้งใน 1 เดือน)
4	สูง	มีโอกาสเกิดเหตุการณ์ (1-6 เดือนต่อ 1 ครั้ง)
3	ปานกลาง	อาจเกิดขึ้นบางครั้ง (1 ปีต่อ 1 ครั้ง)
2	ต่ำ	อาจเกิดขึ้นบางครั้ง (2-3 ปีต่อ 1 ครั้ง)
1	ต่ำมาก	อาจเกิดขึ้นได้จากสภาพแวดล้อมที่พิเศษ (5 ปีหรือมากกว่า 5 ปีต่อ 1 ครั้ง)

3.1.2 ระดับความรุนแรงของผลกระทบ (Impact)

หน่วยงานระบุตัวเลขระดับความรุนแรงของผลกระทบ (5-4-3-2-1) ซึ่งเป็นการประเมินผลกระทบของการดำเนินงานในรูปของความเสียหายที่เกิดขึ้น และส่งผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยงาน ซึ่งความเสียหายที่เกิดขึ้นจะเป็นตัวเงิน หรือไม่ใช่ตัวเงิน ได้แก่ ผลกระทบด้านการเงิน ด้านเวลา ด้านชื่อเสียง ด้านลูกค้า/ผู้รับบริการ/นักศึกษา ด้านการดำเนินงาน ด้านความปลอดภัยของบุคลากร และด้านเทคโนโลยีสารสนเทศ

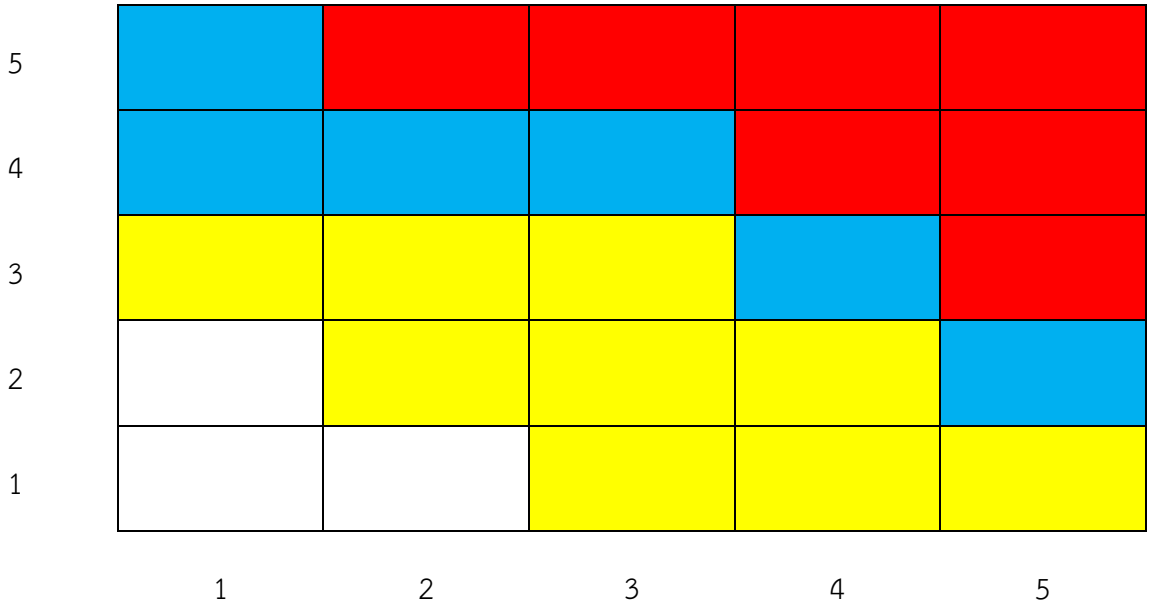
นอกจากนี้ หน่วยงานยังสามารถกำหนดระดับความรุนแรงของผลกระทบด้านอื่นๆ เพิ่มเติมได้ตามความเหมาะสม สำหรับวิธีการเลือกตัวเลขระดับความรุนแรงของผลกระทบ (5-4-3-2-1) ใช้วิธีการวิเคราะห์ร่วมกันหากไม่สามารถหาข้อยุติได้ อาจใช้เสียงข้างมากในที่ประชุม หรือให้แต่ละคนเป็นผู้ให้คะแนนแล้วนำมาหาค่าเฉลี่ย

ตัวอย่าง เกณฑ์ระดับความรุนแรงของผลกระทบ (Impact)

ระดับคะแนน	รายละเอียด	สูญเสียเงิน	สูญเสียทรัพย์สิน	การทำงานของบุคลากร	ชื่อเสียงและภาพลักษณ์	สูญเสียการปฏิบัติงาน
5	สูงมาก	มากกว่า 21% ของงบประมาณ	ทรัพย์สินเสียหายทั้งหมด	ถูกเลิกจ้าง/ออกจากงาน	มีการพาดหัวข่าวจากสื่อทั้งภายในและต่างประเทศ	มีผลแตกต่างจากตัวชี้วัด > 51%
4	สูง	16 – 20% ของงบประมาณ	ทรัพย์สินสูญเสียหรือเสียหายจำนวนมาก	ถูกลงโทษทางวินัย/ตัดเงินเดือน/ไม่ได้ขึ้นเงินเดือน	มีการเผยแพร่ข่าวในวงกว้างภายในประเทศและเผยแพรในวงจำกัดของสื่อต่างประเทศ	มีผลแตกต่างจากตัวชี้วัด 26-50%
3	ปานกลาง	11-15% ของงบประมาณ	ทรัพย์สินสูญเสียหรือเสียหายจำนวนมาก	ถูกทำทัณฑ์บน/บรรยากาศการปฏิบัติงานไม่เหมาะสม	มีการเผยแพร่ข่าวในหนังสือพิมพ์ในประเทศหลายฉบับ (2-5 วัน)	มีผลแตกต่างจากตัวชี้วัด 11-25%
2	ต่ำ	6-10% ของงบประมาณ	ทรัพย์สินสูญเสียหรือเสียหายน้อย	ไม่สะดวกต่อการปฏิบัติงานบ่อยครั้ง	มีการเผยแพร่ข่าวในวงจำกัดภายในประเทศ (1 วัน)	มีผลแตกต่างจากตัวชี้วัด 6-10%
1	ต่ำมาก	น้อยกว่า 5% ของงบประมาณ	เล็กน้อยหรือไม่กระทบกับทรัพย์สิน	ไม่สะดวกต่อการปฏิบัติงานนานๆ ครั้ง	ไม่มีการเผยแพร่ข่าว	มีผลแตกต่างจากตัวชี้วัดไม่เกิน 5%

3.1.3 ระดับของความเสี่ยง (Risk Matrix) กำหนดเกณฑ์ไว้ 4 ระดับ ได้แก่ สูงมาก สูง ปานกลาง และน้อย

เกณฑ์มาตรฐานระดับของความเสี่ยง (Degree of Risk Matrix)



โดย ระดับความเสี่ยงจำแนกตามสีใน Risk Assessment เป็น 4 ระดับดังนี้

ระดับความเสี่ยง

สูงมาก	สูง	ปานกลาง	ต่ำ

3.2 การประเมินโอกาสและผลกระทบของความเสี่ยง

เป็นการนำความเสี่ยงและปัจจัยแต่ละปัจจัยที่ระบุมาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงต่างๆ และประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงโดยใส่ลงในแผนภูมิความเสี่ยง เพื่อให้เห็นถึงระดับความเสี่ยง และผลกระทบที่แตกต่างกัน ทำให้สามารถกำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม ซึ่งจะช่วยให้หน่วยงานสามารถวางแผนและจัดสรรทรัพยากรได้อย่างถูกต้องภายในงบประมาณ กำลังคน หรือเวลาที่จำกัดโดยอาศัยเกณฑ์มาตรฐานที่กำหนดไว้ในข้อ 3.1.3

คณะกรรมการประเมินของหน่วยงานควรเป็นผู้มีความรู้ความชำนาญและมีประสบการณ์ในเรื่องนั้นๆ สำหรับวิธีการให้คะแนนระดับการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงนั้น ใช้การมีส่วนร่วมหากไม่สามารถหาข้อยุติได้ อาจใช้เสียงข้างมากในที่ประชุม หรือให้แต่ละคนเป็นผู้ให้คะแนนแล้วนำคะแนนนั้นมาหาค่าเฉลี่ย เป็นต้น ทั้งนี้มีขั้นตอนการดำเนินการ ดังนี้

1. ร่วมกันวิเคราะห์โอกาส/ความถี่ในการเกิดเหตุการณ์ต่างๆ ว่ามีโอกาส/ความถี่ที่จะเกิดขึ้นมากน้อยเพียงใด และเมื่อได้รับโอกาสแล้วให้นำไปใส่ในแผนบริหารความเสี่ยง

2. ร่วมกันวิเคราะห์ความรุนแรงของผลกระทบของความเสี่ยง ที่มีผลต่อมหาวิทยาลัย/หน่วยงานว่ามีระดับความรุนแรงหรือระดับความเสียหายเพียงใด และเมื่อได้รับผลกระทบแล้วให้นำมาใส่ในแผนบริหารความเสี่ยง

3.3 การวิเคราะห์ระดับของความเสี่ยง (Degree of Risk)

เป็นการพิจารณาความสัมพันธ์ของความถี่กับโอกาสที่จะเกิดความเสี่ยง และระดับความรุนแรงของผลกระทบตามเกณฑ์ความสามารถในการยอมรับความเสี่ยง ดังต่อนี้

ระดับความเสี่ยง	แทนด้วยสี	ความหมาย
สูงมาก	สีแดง	Intolerable or Immediate Attention Require/High Risk ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที
สูง	สีฟ้า	Intolerable or Attention Require/High Risk ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับพื้นที่ยอมรับได้ต่อไป
ปานกลาง	สีเหลือง	Tolerable but caution or Management Discretion/Medium Risk ระดับที่พอยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
น้อย	สีขาว	Acceptable or Limited Focus ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

ระดับความเสี่ยงที่นัยสำคัญที่ผู้บริหารควรให้ความสำคัญมากคือ ความเสี่ยงที่มีระดับสูงมาก และสูงเนื่องจากเป็นความเสี่ยงที่มหาวิทยาลัยไม่สามารถยอมรับได้ เพราะจะทำให้การดำเนินงานตามพันธกิจหลักไม่เป็นไป

ตามเป้าประสงค์ที่กำหนดไว้ และส่งผลกระทบต่อชื่อเสียงของมหาวิทยาลัย ระดับความเสี่ยงปานกลางแม้ว่าจะเป็นความเสี่ยงที่พอยอมรับได้ แต่ก็ต้องมีการควบคุมเพื่อไม่ให้เกิดความเสี่ยงมากขึ้นส่วนความเสี่ยงระดับน้อย ผู้บริหารไม่จำเป็นต้องเอาใจใส่มากนัก แต่ก็ไม่ควรละเลยโดยให้มีการดำเนินการควบคุมเท่าที่จำเป็นตามความเหมาะสม

3.4 การจัดลำดับความเสี่ยง

นำค่าระดับความเสี่ยงและผลกระทบมาจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อมหาวิทยาลัย คณะ/สำนัก/สถาบัน/ศูนย์/กอง/สาขาฯ เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับของความเสี่ยงที่เกิดจากความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยง (Likelihood) และผลกระทบของความเสี่ยง (Impact) ที่ประเมินได้ตามแผนภูมิความเสี่ยง โดยจัดเรียงลำดับจากระดับสูง ปานกลาง น้อย และเลือกความเสี่ยงที่มีระดับสูงมาก และหรือสูง มาจัดทำแผนการบริหาร/จัดการความเสี่ยงในขั้นตอนต่อไป

4. การจัดทำแผนบริหารความเสี่ยง การจัดทำแผนบริหารความเสี่ยงเป็นขั้นตอนของการบริหาร/จัดการความเสี่ยง โดยการนำกลยุทธ์ มาตรการหรือแผนงาน มาใช้ปฏิบัติในทุกหน่วยงานของมหาวิทยาลัย เพื่อลดโอกาสที่จะเกิดความเสียหายของผลกระทบที่อาจเกิดขึ้นจากความเสี่ยงในการดำเนินงานตามภารกิจต่างๆ รวมทั้งโครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยงหรือที่มีอยู่แต่ยังไม่เพียงพอและนำมาวางแผนจัดการควาเมสี่ยง

โดยในการวางแผนการจัดการความเสี่ยงต้องมีเป้าหมาย คือ

1) ลดโอกาสที่จะเกิดความเสี่ยงนั้น

2) ลดความรุนแรงของผลกระทบจากความเสี่ยงนั้น ในกรณีที่ความเสี่ยงนั้นเกิดขึ้น

3) เปลี่ยนลักษณะของผลลัพธ์ที่จะเกิดขึ้นของความเสี่ยงให้เป็นในรูปที่องค์กรหรือหน่วยงานต้องการหรือยอมรับได้

ทางเลือกในการจัดการความเสี่ยง แนวทางการจัดการความเสี่ยงมีหลายวิธี และสามารถปรับเปลี่ยนให้เหมาะสมกับสถานการณ์ ขึ้นอยู่กับดุลยพินิจของผู้รับผิดชอบ แต่อย่างไรก็ตามแนวทางการบริหารจัดการความเสี่ยงต้องคุ้มค่ากับการลดระดับผลกระทบความเสี่ยง

ทางเลือกหรือกลยุทธ์ในการจัดการความเสี่ยงแบ่งได้ 4 แนวทางหลักคือ

1) การยอมรับ (Take, Accept) หมายถึง การที่ความเสี่ยงนั้นสามารถยอมรับได้ภายใต้การควบคุมที่มีอยู่ในปัจจุบัน ซึ่งไม่ต้องดำเนินการใดๆ เช่น กรณีที่มีความเสี่ยงในระดับไม่รุนแรงและไม่คุ้มค่าที่จะดำเนินการใดๆ ให้ขออนุมัติหลักการรับความเสี่ยงไว้และไม่ดำเนินการใดๆ

2) การควบคุม (Treat) คือ ความเสี่ยงที่ยอมรับได้แต่ต้องมีการแก้ไขเกี่ยวกับการควบคุมที่มีอยู่ในปัจจุบัน เพื่อให้มีการควบคุมที่เพียงพอและเหมาะสม เช่น การปรับปรุงกระบวนการดำเนินงาน การจัดอบรมเพิ่มทักษะในการทำงานให้กับพนักงานและการจัดทำคู่มือการปฏิบัติงาน เป็นต้น

3) การยกเลิก (Terminate) หรือหลีกเลี่ยง (Avoid) คือ ความเสี่ยงที่ไม่สามารถยอมรับและต้องจัดการให้ความเสี่ยงนั้นไปอยู่นอกเงื่อนไขการดำเนินการ โดยมีวิธีการจัดการความเสี่ยงกลุ่มนี้ เช่น การหยุดการดำเนินงาน หรือกิจกรรมที่ก่อให้เกิดความเสี่ยงนั้นๆ การเปลี่ยนแปลงวัตถุประสงค์ในการดำเนินงาน การลดขนาดของงานที่จะดำเนินการหรือกิจกรรมลง เป็นต้น

4) การโอนความเสี่ยง (Transfer) หรือแบ่ง (Share) คือ ความเสี่ยงที่สามารถโอนไปให้ผู้อื่นได้ เช่น การทำประกันภัย/ประกันทรัพย์สินกับบริษัทประกัน การจ้างบุคคลภายนอกหรือการจ้างบริษัทประกัน การจ้างบุคคลภายนอกหรือการจ้างบริษัทภายนอกมาจัดการในงานบางอย่างแทน เช่น งานรักษาความปลอดภัย เป็นต้น ความเสี่ยงเพื่อกำหนดมาตรการ หรือแผนปฏิบัติการในการจัดการและควบคุมความเสี่ยงที่สูง (High) และสูงมาก (Extreme) นั้นให้ลดลง ให้อยู่ในระดับที่ยอมรับได้ สามารถปฏิบัติได้จริงและให้สามารถติดตามและประเมินผลการจัดการความเสี่ยงนั้นได้ รวมทั้งต้องพิจารณาถึงความคุ้มค่าในด้านค่าใช้จ่ายและต้นทุนที่ต้องใช้ลงทุนในการกำหนดมาตรการ หรือแผนปฏิบัติการนั้นกับประโยชน์ที่จะได้รับด้วย

5. การรายงานและติดตามผล หลังจากจัดทำแผนบริหารความเสี่ยงและมีการดำเนินงานตามแผนแล้วจะต้องมีการรายงานและติดตามผลเป็นระยะ เพื่อให้เกิดความมั่นใจว่าได้มีการดำเนินงานไปอย่างถูกต้องและเหมาะสมโดยมีเป้าหมายในการติดตามผล คือ เป็นการประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยง รวมทั้งติดตามผลการจัดการความเสี่ยงที่ได้มีการดำเนินการแล้วว่าบรรลุผลตามวัตถุประสงค์ของการบริหารความเสี่ยงหรือไม่ โดยหน่วยงานต้องสอบถามดูว่า วิธีการบริหารการจัดการความเสี่ยงใดมีประสิทธิภาพดีก็ให้ดำเนินการต่อไป หรือวิธีการบริหารจัดการความเสี่ยงใดควรปรับเปลี่ยน และนำผลการติดตามไปรายงานให้ฝ่ายบริหารทราบตามรายงานที่ได้กล่าวไว้ข้างต้น ทั้งนี้กระบวนการสอบถามหน่วยงานอาจกำหนดข้อมูลที่ติดตามหรืออาจทำ Check List การติดตาม พร้อมทั้งกำหนดความถี่ในการติดตามผล โดยสามารถติดตามผลได้ใน 2 ลักษณะคือ

1. การติดตามผลเป็นรายครั้ง (Separate Monitoring) เป็นการติดตาม ตามรอบระยะเวลาที่กำหนด เช่น ทุก 3 เดือน 9 เดือน หรือทุกสิ้นปี เป็นต้น

2. การติดตามผลในระหว่างการปฏิบัติงาน (Ongoing Monitoring) เป็นการติดตามผลที่รวมอยู่ในการดำเนินงานต่างๆ ตามปกติของหน่วยงาน

6. การประเมินผลการบริหารความเสี่ยง ผู้จัดทำระบบการจัดการความเสี่ยง จะต้องทำสรุปรายงานผลและประเมินผลการบริหารความเสี่ยงประจำปีต่อคณะทำงานวิเคราะห์และจัดทำแผนบริหารความเสี่ยงของมหาวิทยาลัย เพื่อให้มั่นใจว่ามหาวิทยาลัยมีการบริหารความเสี่ยงเป็นไปอย่างเหมาะสม เพียงพอ ถูกต้องและมีประสิทธิผล มาตรการหรือกลไกการควบคุมความเสี่ยง (Control Activity) ที่ดำเนินการสามารถลดและ

ควบคุมความเสี่ยงที่เกิดขึ้นได้จริงและอยู่ในระดับที่ยอมรับด้ หรือต้องจัดหามาตรการหรือตัวควบคุมอื่นเพิ่มเติม เพื่อให้ความเสี่ยงที่ยังเหลืออยู่หลังมีการจัดการ (Residual Risk) อยู่ในระดับที่ยอมรับได้ และให้องค์กรมีการบริหารความเสี่ยงอย่างต่อเนื่องจนเป็นวัฒนธรรมในการดำเนินงาน

7. การทบทวนการบริหารความเสี่ยง การทบทวนแผนบริหารความเสี่ยง เป็นการทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงทุกขั้นตอน เพื่อการปรับปรุงและพัฒนาแผนงานในการบริหารความเสี่ยงให้ทันสมัยและเหมาะสมกับการปฏิบัติงานจริงเป็นประจำทุกปี

บทที่ 4
การประเมินและวิเคราะห์ความเสี่ยงและการควบคุมภายใน

คณะกรรมการจัดทำแผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้ดำเนินการตามกระบวนการบริหารความเสี่ยง ตั้งแต่การระบุเหตุการณ์/สถานการณ์เสี่ยง การวิเคราะห์ความเสี่ยง และการจัดลำดับความเสี่ยง สรุปได้ดังนี้

ความเสี่ยง	ปัจจัยเสี่ยง	โอกาสที่จะเกิดขึ้น	ผลกระทบความรุนแรง	ระดับคะแนนความเสี่ยง	ระดับความเสี่ยง
1. การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ	1. เสี่ยงจากช่องโหว่ในด้านการนำโปรแกรม Open Source	5	5	25	สูงมาก
	2. เสี่ยงจากการเปิดใช้บริการบนระบบเครือข่ายที่ไม่จำเป็น	4	5	20	สูง
	3. เสี่ยงจากการไม่ต่ออายุลิขิตสิทธิ์การใช้งานของซอฟแวร์ระบบ	4	5	20	สูง
	4. ไม่มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ (vulnerability assessment)	5	5	25	สูงมาก
	5. ไม่มีการทดสอบเจาะระบบ (penetration test)	4	5	20	สูง
2. การสำรองข้อมูล (Data Backup)	1. มีการสำรองข้อมูลแต่ไม่เป็นไปตามระบบและกลไกการสำรองข้อมูล	4	5	20	สูง

ความเสี่ยง	ปัจจัยเสี่ยง	โอกาสที่จะเกิดขึ้น	ผลกระทบความรุนแรง	ระดับคะแนนความเสี่ยง	ระดับความเสี่ยง
	2. มีการดำเนินงานการสำรองข้อมูลแต่ไม่มีระบบหรือทะเบียนควบคุมการจัดเก็บและเรียกใช้งานสื่อบันทึกข้อมูลตามประเภทของสื่อที่จัดเก็บ	4	5	20	สูง
	3. ไม่มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้อง พร้อมใช้งาน และปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติ	4	5	20	สูง

การประเมินมาตรการควบคุมความเสี่ยงและการควบคุมภายใน

การประเมินมาตรการควบคุมความเสี่ยง โดยการนำปัจจัยเสี่ยงที่อยู่ในระดับความเสี่ยงสูง และสูงมาก มาประเมินการควบคุมความเสี่ยงและการควบคุมภายใน

ความเสี่ยง	ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	การควบคุมที่มีอยู่แล้ว	การควบคุมที่มีอยู่แล้วได้ผลหรือไม่	ระดับความเสี่ยง
1. การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ	1. เสี่ยงจากช่องโหว่ในด้านการนำโปรแกรม Open Source	ควบคุมความเสี่ยง	X	X	สูงมาก (25 คะแนน)
	2. เสี่ยงจากการเปิดใช้บริการบนระบบเครือข่ายที่ไม่จำเป็น	ควบคุมความเสี่ยง	O	O	สูง (20 คะแนน)
	3. เสี่ยงจากการไม่ต่ออายุลิขิตสิทธิ์การใช้งานของซอฟแวร์ระบบ	ควบคุมความเสี่ยง	O	O	สูง (20 คะแนน)
	4. ไม่มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ (vulnerability assessment)	ควบคุมความเสี่ยง	X	X	สูงมาก (25 คะแนน)
2. การสำรองข้อมูล (Data Backup)	1. มีการสำรองข้อมูลแต่ไม่เป็นไปตามระบบและกลไกการสำรองข้อมูล	ควบคุมความเสี่ยง	O	O	สูง (20 คะแนน)

ความเสี่ยง	ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	การควบคุมที่มีอยู่แล้ว	การควบคุมที่มีอยู่แล้วได้ผลหรือไม่	ระดับความเสี่ยง
	2. ไม่มีการตรวจทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้องพร้อมใช้งาน และปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติ	ควบคุมความเสี่ยง	✗	✗	สูง (20 คะแนน)

หมายเหตุ ช่องการควบคุมที่มีอยู่แล้ว ใส่เครื่องหมาย ✓ = มีอยู่แล้ว , O = มีแต่ไม่สมบูรณ์ , ✗ = ไม่มี
ช่องการควบคุมที่มีแล้วได้ผลหรือไม่ ✓ = ได้ผลตามที่คาดหมาย , O = ได้ผลบ้างแต่ไม่สมบูรณ์ , ✗ = ไม่ได้ผลตามที่คาดหมาย

แผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ประจำปีงบประมาณ พ.ศ. 2566

คณะกรรมการจัดทำแผนบริหารความเสี่ยง ได้มีการวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อพันธกิจ ตามแผนปฏิบัติราชการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ.2566 โดยนำพิจารณาระดับความเสี่ยงของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ที่มีค่าคะแนนในระดับสูง และสูงมาก มาบริหารจัดการความเสี่ยง รวมทั้งสิ้นจำนวน 2 ความเสี่ยง และ 6 ปัจจัยเสี่ยง รายละเอียดดังตารางต่อไปนี้

ความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผู้รับผิดชอบ
1. การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ	1. เสี่ยงจากช่องโหว่ในด้านการนำโปรแกรม Open Source	สูงมาก	1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการนำโปรแกรม Open Source	1. อบรมเชิงปฏิบัติ เรื่อง ภัยคุกคามบนระบบเครือข่าย 2. มาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการนำโปรแกรม Open Source	- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ

ความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผู้รับผิดชอบ
			2. มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ โดยผู้ให้บริการและผู้บริหาร ควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ให้ครอบคลุมทุกระบบงานอย่างสม่ำเสมอตามระดับความเสี่ยง สำหรับระบบบงานสำคัญควรจัดทำอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ	2. มีกระบวนการและเครื่องมือในการประเมินช่องโหว่	- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ
			3. มีการรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย		- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ
	2. เสี่ยงจากการเปิดใช้บริการบนระบบเครือข่ายที่ไม่จำเป็น	สูง	1. กำหนดมาตรฐานและระเบียบในการใช้บริการบนระบบเครือข่าย	มีมาตรฐานและระเบียบในการใช้บริการบนระบบเครือข่าย	- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ

ความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผู้รับผิดชอบ
	3. เสี่ยงจากการไม่ต่ออายุลิขิตสิทธิ์การใช้งานของซอฟแวร์ระบบ	สูง	1. ดำเนินต่ออายุลิขิตสิทธิ์การใช้งานของซอฟแวร์ระบบ	จัดทำการต่ออายุลิขิตสิทธิ์การใช้งานของซอฟแวร์ระบบ	- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ
	4. ไม่มีกระบวนการและเครื่องมือในการประเมินช่องโหว่	สูงมาก	1.จัดทำประกาศกฎระเบียบเกี่ยวกับเรื่องดูแลความปลอดภัยจากช่องโหว่ของการใช้บนเครือข่าย	มีประกาศกฎระเบียบเกี่ยวกับเรื่องดูแลความปลอดภัยจากช่องโหว่ของการใช้บนเครือข่าย	- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ
			2. กำหนดแนวทางเกี่ยวกับกระบวนการและเครื่องมือในการประเมินช่องโหว่	1.มีปฏิทินตารางการตรวจประเมินช่องโหว่ของตัวระบบ 2.จัดการซื้อโปรแกรม Nod32 antivirus	- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ

ความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผู้รับผิดชอบ
2. การสำรองข้อมูล (Data Backup)	1. มีการสำรองข้อมูลแต่ไม่เป็นไปตามระบบและกลไกการสำรองข้อมูล	สูง	กำหนดมาตรการการสำรองข้อมูลและกลไกการสำรองข้อมูล	1. มีปฏิทินตารางการการสำรองข้อมูลและกลไกการสำรองข้อมูล 2. มีการตรวจทานการสำรองข้อมูล 3. ติดตามประเมิลการสำรองข้อมูล จำนวน 2 ครั้ง (รอบ 6 เดือนและ 12 เดือน)	- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ
	2. ไม่มีการตรวจทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้องพร้อมใช้งาน และปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติ	สูง			- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ

รายงานผลการดำเนินการ

แผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2566

รอบ 9 เดือน

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
1. การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ	1. เสี่ยงจากช่องโหว่ในด้านการนำโปรแกรม Open Source	1. กำหนดมาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการนำโปรแกรม Open Source มาใช้	1. อบรมเชิงปฏิบัติ เรื่อง ภัยคุกคามบนระบบเครือข่าย	วันที่ 15 มิ.ย. 2566 ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกาญจนบุรี ได้ติดต่อไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thaicert) ขอรับคำปรึกษากรณีพบช่องโหว่การโจมตีเว็บไซต์ของหน่วยงานมหาวิทยาลัยราชภัฏกาญจนบุรี จำนวน 3 เว็บไซต์ ได้แก่ 1). เว็บไซต์คณะกรรมการบริหารมหาวิทยาลัยราชภัฏกาญจนบุรี (https://directors.kru.ac.th/) 2). เว็บไซต์สภามหาวิทยาลัยราชภัฏกาญจนบุรี (https://council.kru.ac.th/) และ 3. เว็บไซต์ระบบผลงานวิชาการ (https://success.kru.ac.th/) ทาง Thaicert จึงขอนัดเชิญประชุมเพื่อหารือเพื่อให้ความรู้และแนวทางเกี่ยวกับประเด็นการโจมตี

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
				เว็บไซต์ของหน่วยงาน มหาวิทยาลัยราชภัฏกาญจนบุรี วันที่ 23 มิ.ย. 2566 บริษัท เน็ทวัน เน็ทเวิร์ค โซลูชั่น จำกัด ร่วมกับบริษัท บริษัท ซังฟอร์ เทคโนโลยี (ประเทศไทย) จำกัด ได้อนุเคราะห์ติดตั้งอุปกรณ์ไฟร์วอลล์แอปพลิเคชันเว็บสำหรับกรองตรวจสอบและบล็อกการรับส่งข้อมูล และได้อบรมเชิงปฏิบัติการผ่านระบบออนไลน์ และให้ความรู้เกี่ยวด้านการเฝ้าระวังการโจมตีระบบเครือข่ายให้กับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ และการบริหารจัดการเรื่องการนำโปรแกรม Open Source มาติดตั้งในระบบเครือข่ายของมหาวิทยาลัยราชภัฏกาญจนบุรี
			2. มาตรฐานและระเบียบวิธีปฏิบัติการบริหารจัดการนำโปรแกรม Open Source	1.จัดการ Patch โปรแกรม Open Source บนเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ทุกตัว 2. ทำการ Update ระบบปฏิบัติการระบบปฏิบัติการลีนุกซ์ และระบบปฏิบัติการวินโดวเซิร์ฟเวอร์

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
				3. มีแนวทางในการบริการจัดการเซิร์ฟเวอร์และโปรแกรม Open Source ทั้งหมด 4. ตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายโดยทำการแยก Zone และกำหนดค่า policy ในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
		2. มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ โดยผู้ให้บริการและผู้บริหาร ควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหวให้ครอบคลุมทุกระบบงานอย่างสม่ำเสมอตามระดับความเสี่ยง สำหรับระบบงานสำคัญควรจัดทำอย่างน้อยปีละ 1	2. มีกระบวนการและเครื่องมือในการประเมินช่องโหว่	1. มีแนวทางในการตรวจสอบ ประเมินแอพพลิเคชั่น หรือเครื่องเซิร์ฟเวอร์ที่จะใช้งานจริงโดยการทำ penetration test 2. มีการตรวจสอบ ทดสอบ ประเมินระบบภัยคุกคามจากการโจมตีในระดับเครือข่าย และเครื่องเซิร์ฟเวอร์ 3. มีการติดตั้ง Antivirus แบบ EDR บนเครื่องคอมพิวเตอร์แม่ข่าย เพื่อทำงานร่วมกับอุปกรณ์การตรวจจับภัยคุกคามบนระบบเครือข่าย 4. มีแนวทางในการติดตั้งอุปกรณ์รักษาความปลอดภัยใน server โดยทำการสร้าง Zone สำหรับเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ทั้งที่เป็นแบบ open source และแบบที่พัฒนาขึ้นใช้งาน

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
		ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ		
		3. มีการรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมทั้งมีการติดตามการดำเนินการปรับปรุงแก้ไขและนำเสนอความคืบหน้าการดำเนินการต่อคณะกรรมการหรือผู้บริหารที่ได้รับมอบหมาย	รายงานผลการประเมินช่องโหว่ของระบบไปยังผู้รับผิดชอบ และรายงานต่อผู้บริหารสำนักหรือมหาวิทยาลัยฯ จำนวน 2 ครั้ง (รอบ 6 เดือน และ 12 เดือน)	รายงานการตรวจพบช่องโหว่ภายในระบบไปยังผู้รับผิดชอบ ผู้บริหารสำนักฯ และมหาวิทยาลัยทราบ
	2. เสี่ยงจากการเปิดใช้บริการบนระบบเครือข่ายที่ไม่จำเป็น	1. กำหนดมาตรฐานและระเบียบในการใช้บริการบนระบบเครือข่าย	มีมาตรการและระเบียบในการใช้บริการบนระบบเครือข่าย	กำลังดำเนินการกำหนดให้มีมาตรการในการให้บริการบนระบบเครือข่าย จำนวน 1 มาตรการ

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
	3. เสี่ยงจากการไม่ต่ออายุลิขิตสิทธิ์การใช้งานของซอฟแวร์ระบบ	1. ดำเนินต่ออายุลิขิตสิทธิ์การใช้งานของซอฟแวร์ระบบ	จัดทำการต่ออายุลิขิตสิทธิ์การใช้งานของซอฟแวร์ระบบ	ดำเนินการต่ออายุอายุลิขิตสิทธิ์ระบบป้องกันเครือข่าย ดังนี้ 1.ระบบป้องกันการโจมตีจากเครือข่ายภายนอก (Firewall) 2.ระบบ Web Application Firewall (WAF)
	4. ไม่มีกระบวนการและเครื่องมือในการประเมินช่องโหว่	1.จัดทำประกาศกฎระเบียบเกี่ยวกับเรื่องดูแลความปลอดภัยจากช่องโหว่ของการใช้บนเครือข่าย	มีประกาศกฎระเบียบเกี่ยวกับเรื่องดูแลความปลอดภัยจากช่องโหว่ของการใช้บนเครือข่าย	อยู่ระหว่างการดำเนินการ
		2. กำหนดแนวทางเกี่ยวกับกระบวนการและเครื่องมือในการประเมินช่องโหว่	1.จัดทำปฏิทินตารางการตรวจประเมินช่องโหว่ของเครื่องแม่ข่ายในการให้บริการระบบสารสนเทศ	1.ติดตั้งเครื่องมือในการประเมินช่องโหว่ เช่น endpoint security และ Nod32 Antivirus (Endpoint Protection) โดยติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายจำนวน 48 เครื่อง ที่ใช้งานบนระบบ windows server และ Linux server 2.รายงานช่องโหว่ของระบบไปยังผู้รับผิดชอบ และมหาวิทยาลัยทราบ พร้อมกับวิธีการแก้ปัญหาต่างๆ

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
				ที่เกิดกับระบบ
			2.จัดการซื้อโปรแกรม Nod32 antivirus	จัดซื้อโปรแกรม Nod32 Antivirus (Endpoint Protection) จำนวน 50 สิทธิการใช้งาน ระยะเวลา 3 ปี
2. การสำรองข้อมูล (Data Backup)	1. มีการสำรองข้อมูลแต่ไม่เป็นไปตามระบบและกลไกการสำรองข้อมูล	กำหนดมาตรการการสำรองข้อมูลและกลไกการสำรองข้อมูล	1. มีปฏิทินตารางการการสำรองข้อมูลและกลไกการสำรองข้อมูล	กำหนดตารางการสำรองข้อมูลดังนี้ 1.สำรองระบบสารสนเทศทั้งหมดลงบนอุปกรณ์สำรองข้อมูลแบบทันทีที่มีการปรับปรุงหรือแก้ไขข้อมูล 2. มีปฏิทินตารางการการสำรองข้อมูลและกลไกการสำรองข้อมูล
	2. ไม่มีการตรวจทานการสำรองข้อมูลเพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้อง พร้อมใช้งานและปลอดภัยตามมาตรฐานและ		2. มีการตรวจทานการสำรองข้อมูล	สำรองข้อมูลสารสนเทศทุกระบบลงในอุปกรณ์สำรองข้อมูล ดังนี้ 1.สำรองข้อมูลสารสนเทศด้วยโปรแกรม Veem Backup 2.สำรองข้อมูลสารสนเทศทั้งหมดลงบนอุปกรณ์จัดเก็บข้อมูลแบบภายนอก QNAP

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
	ระเบียบวิธีปฏิบัติ		3. ติดตามประเมินการสำรองข้อมูล จำนวน 2 ครั้ง (รอบ 6 เดือนและ 12 เดือน)	ติดตามประเมินการสำรองข้อมูล คือ 1. ศูนย์เทคโนโลยีสารสนเทศได้ทดสอบการกู้คืนข้อมูลสารสนเทศที่ได้สำรองข้อมูลข้างต้น พบว่าสามารถกู้คืนข้อมูลได้โดยใช้เวลาที่แต่กต่างกันขึ้นอยู่กับขนาดของไฟล์ข้อมูลที่ได้ทำการจัดเก็บไว้ และพบว่าข้อมูลที่ได้จากการกู้คืนนั้นมีความสมบูรณ์สามารถใช้งานได้จริง

ผลการดำเนินการตามแผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. 2566 โดยมีประเด็นความเสี่ยงทั้งสิ้น 2 ความเสี่ยง และ 6 ปัจจัยเสี่ยง มีผลการดำเนินการดังต่อไปนี้

ความเสี่ยงที่ 1 การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ มี 4 ปัจจัยเสี่ยง คือ 1) เสี่ยงจากช่องโหว่ในด้านการนำโปรแกรม Open Source 2) เสี่ยงจากการเปิดใช้บริการบนระบบเครือข่ายที่ไม่จำเป็น 3) เสี่ยงจากการไม่ต่ออายุลิขิตสิทธิ์การใช้งานของซอฟแวร์ระบบ 4) ไม่มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ (vulnerability assessment)

ความเสี่ยงที่ 2 การสำรองข้อมูล (Data Backup) มี 2 ปัจจัยเสี่ยง 1) มีการสำรองข้อมูลแต่ไม่เป็นไปตามระบบและกลไกการสำรองข้อมูล 2) ไม่มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้อง พร้อมใช้งาน และปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติ

ผลการดำเนินการ พบว่า

ความเสี่ยงที่ 1 ปัจจัยเสี่ยง 1. เสี่ยงจากช่องโหว่ในด้านการนำโปรแกรม Open Source ระดับคะแนนความเสี่ยง 16 ระดับความเสี่ยงสูง 2) เสี่ยงจากการเปิดใช้บริการบนระบบเครือข่ายที่ไม่จำเป็น ระดับคะแนนความเสี่ยง 16 ระดับความเสี่ยงสูง 3) เสี่ยงจากการไม่ต่ออายุลิขิตสิทธิ์การใช้งานของซอฟแวร์ระบบ ระดับคะแนนความเสี่ยง 16 ระดับความเสี่ยงสูง 4) ไม่มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ (vulnerability assessment) ระดับคะแนนความเสี่ยง 16 ระดับความเสี่ยงสูง

ความเสี่ยงที่ 2 ปัจจัยเสี่ยง 1) มีการสำรองข้อมูลแต่ไม่เป็นไปตามระบบและกลไกการสำรองข้อมูล ระดับคะแนนความเสี่ยง 9 ระดับความเสี่ยงปานกลาง และ 2) ไม่มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้อง พร้อมใช้งาน และปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติ ระดับคะแนนความเสี่ยง 9 ระดับความเสี่ยงปานกลาง

รายละเอียดดังได้แสดงในตาราง

ความเสี่ยง	ปัจจัยเสี่ยง	โอกาสที่จะเกิดขึ้น	ผลกระทบความรุนแรง	ระดับคะแนนความเสี่ยง	ระดับความเสี่ยง
1. การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ	1. เสี่ยงจากช่องโหว่ในด้านการนำโปรแกรม Open Source	4	4	16	สูง
	2. เสี่ยงจากการเปิดใช้บริการบนระบบเครือข่ายที่ไม่จำเป็น	4	4	16	สูง
	3. เสี่ยงจากการไม่ต่ออายุลิขิตสิทธิ์การใช้งานของซอฟแวร์ระบบ	4	4	16	สูง

ความเสี่ยง	ปัจจัยเสี่ยง	โอกาสที่จะเกิดขึ้น	ผลกระทบความรุนแรง	ระดับคะแนนความเสี่ยง	ระดับความเสี่ยง
	4. ไม่มีกระบวนการและเครื่องมือในการประเมินช่องโหว่ (vulnerability assessment)	4	4	16	สูง
2. การสำรองข้อมูล (Data Backup)	1. มีการสำรองข้อมูลแต่ไม่เป็นไปตามระบบและกลไกการสำรองข้อมูล	3	3	9	ปานกลาง
	2. ไม่มีการสอบทานการสำรองข้อมูล เพื่อให้มั่นใจว่ามีการสำรองข้อมูลครบถ้วนถูกต้องพร้อมใช้งาน และปลอดภัยตามมาตรฐานและระเบียบวิธีปฏิบัติ	3	3	9	ปานกลาง

บทที่ 5
การติดตามและประเมินผลตามแผนบริหารความเสี่ยงและการควบคุมภายใน

ในระหว่างที่นำมาตรการลดความเสี่ยงในแต่ละปัจจัยเสี่ยงไปปฏิบัตินั้น ในแต่ละช่วงเวลาต้องจัดทำรายงานผลการปฏิบัติงาน และจะต้องมีการควบคุม กำกับ ติดตามความก้าวหน้าของงาน หากพบปัญหาอุปสรรคต่างๆ เพื่อนำไปสู่การแก้ไข ตลอดจนมีการประเมินผลสำเร็จของแผนบริหารความเสี่ยงเพื่อเป็นข้อมูลย้อนกลับ (Feedback) เพื่อนำไปทบทวนประสิทธิภาพของแนวทางการบริหารความเสี่ยงในทุกขั้นตอน เพื่อการพัฒนาและนำไปสู่การปฏิบัติในปีต่อไป

กระบวนการควบคุมและประเมินผลตามแผนบริหารความเสี่ยง จะประกอบด้วย 3 องค์ประกอบที่สำคัญ ได้แก่

1. การวัดและประเมินผล จะประกอบด้วยกระบวนงานย่อย 3 ขั้นตอน ได้แก่ 1) การเก็บรวบรวมข้อมูล 2) การวิเคราะห์และประเมินผลข้อมูล 3) การเสนอผลการประเมิน การวัดและประเมินผลจะเป็นการประเมินผลความสำเร็จของการปฏิบัติงานตามแผนแต่ละรอบเวลาที่กำหนด

2. การติดตามระหว่างการปฏิบัติงาน เป็นการติดตามจากผู้บริหารที่ต้องรับผิดชอบตามที่ได้กำหนดไว้ในแผนบริหารความเสี่ยง

3. การติดตามเป็นรายครั้ง โดยคณะกรรมการบริหารความเสี่ยง จะได้มีการจัดทำแผนการติดตามและจัดทำรายงานผลการติดตาม 9 เดือน และ 12 เดือน ดังนี้

ครั้งที่ 1 ติดตามและรายงานผล ระหว่างเดือน มิถุนายน – กรกฎาคม 2566

ครั้งที่ 2 ติดตามและรายงานผล ระหว่างเดือน สิงหาคม – กันยายน 2566