ประจำปี 2568

แผนบริหารความเสี่ยง
และการควบคุมภายใน

งานศูนย์เทคโนโลยีสารสนเทศ
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏกาญจนบุรี

คำนำ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศได้จัดทำแผนบริหารความเสี่ยงและการควบคุมภายในประจำปีงบประมาณ 2568 ขึ้นเพื่อเป็นแนวทางในการบริหารจัดการความเสี่ยงอย่างมีระบบ โดยมีจุดมุ่งหมายหลักในการลดความเสี่ยงที่อาจเกิดขึ้นในกระบวนการดำเนินงานขององค์กร การบริหารความเสี่ยงถือเป็นสิ่งสำคัญที่ช่วยให้องค์กรสามารถตอบสนองต่อสถานการณ์ที่ไม่คาดคิดได้อย่างมีประสิทธิภาพ โดยแผนนี้ได้รับการออกแบบเพื่อตอบสนองต่อความท้าทายและความซับซ้อนที่เกิดขึ้นในกระบวนการบริหารจัดการทรัพยากรทั้งในด้านการปฏิบัติงานประจำวัน การให้บริการเทคโนโลยีสารสนเทศ และการพัฒนาบุคลากร แผนนี้จะประกอบไปด้วยขั้นตอนการระบุ วิเคราะห์ และประเมินความเสี่ยงที่เกี่ยวข้องกับกระบวนการดำเนินงาน ซึ่งรวมถึงการจัดการความยินยอม (Consent Management) เพื่อให้ข้อมูลส่วนบุคคลมีความชัดเจนและโปร่งใส รวมถึงการละเมิดความปลอดภัยของข้อมูล (Data Breach) ที่จำเป็นต้องมีการบริหารจัดการอย่างเข้มงวด เพื่อรักษาความไว้วางใจของผู้ใช้บริการและป้องกันการสูญเสียที่อาจเกิดขึ้น

ในส่วนของการใช้ระบบหรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดต (Outdated Software) ซึ่งเป็นความเสี่ยงที่สำคัญที่อาจเปิดช่องโหว่ให้กับการโจมตีจากแฮกเกอร์ องค์กรจึงต้องมีมาตรการรักษาความปลอดภัย เช่น การเข้ารหัสข้อมูลและการจัดการสิทธิการเข้าถึงข้อมูลอย่างเคร่งครัด นอกจากนี้การบริหารจัดการทรัพยากรบุคคล (Human Resource Management) ก็เป็นส่วนสำคัญในการลดความเสี่ยง เนื่องจากการขาดการฝึกอบรมหรือพัฒนาทักษะของบุคลากรอาจส่งผลให้การจัดการความเสี่ยงไม่ประสบผลสำเร็จ ดังนั้นการจัดอบรมและพัฒนาบุคลากรจึงมีความสำคัญในการสร้างความรู้และความสามารถในการจัดการความเสี่ยงอย่างมีประสิทธิภาพ แผนบริหารความเสี่ยงและการควบคุมภายในนี้จึงเป็นเครื่องมือสำคัญที่ช่วยให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศสามารถบรรลุเป้าหมายการดำเนินงานอย่างมั่นคงและยั่งยืน โดยการบริหารจัดการทรัพยากรภายในองค์กรอย่างเต็มประสิทธิภาพและลดความสูญเสียที่อาจเกิดขึ้นในอนาคต นอกจากนี้ยังเป็นการสนับสนุนให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศมีบทบาทสำคัญในการพัฒนาและสนับสนุนการดำเนินงานในมหาวิทยาลัยราชภัฏกาญจนบุรีให้ประสบความสำเร็จตามเป้าหมายที่กำหนดไว้

ศูนย์เทคโนโลยีสารสนเทศ

18 กันยายน 2567

สารบัญ

หน้า

บทที่ 1
บทนำ

1. หลักการและเหตุผล

การบริหารความเสี่ยงและการควบคุมภายในเป็นเครื่องมือเชิงกลยุทธ์ที่มีความสำคัญสูงสุดในการดำเนินงานขององค์กรตามหลักการการกำกับดูแลกิจการที่ดี โดยมีจุดประสงค์เพื่อสนับสนุนการบริหารงานและการตัดสินใจในด้านต่าง ๆ ขององค์กร อาทิเช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุมและการวัดผลการดำเนินงาน ตลอดจนการใช้ทรัพยากรอย่างมีประสิทธิภาพ ซึ่งจะช่วยลดความสูญเสียและลดความเสี่ยงที่จะทำให้เกิดความเสียหายแก่องค์กรได้อย่างมาก โดยเฉพาะในด้านเทคโนโลยีสารสนเทศซึ่งมีบทบาทสำคัญในการขับเคลื่อนการดำเนินงานขององค์กร การบริหารจัดการความเสี่ยงในด้านนี้จึงมีความจำเป็นอย่างยิ่ง เนื่องจากเทคโนโลยีสารสนเทศครอบคลุมตั้งแต่การจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย ไปจนถึงการดำเนินงานระบบเทคโนโลยีสารสนเทศต่าง ๆ

ในกระบวนการดำเนินงานของทุกองค์กร ล้วนมีปัจจัยเสี่ยงที่อาจส่งผลกระทบต่อเป้าหมายหรือการดำเนินงานขององค์กร ความเสี่ยงเหล่านี้เกิดจากความไม่แน่นอนในหลายมิติ จึงจำเป็นต้องมีการจัดการความเสี่ยงอย่างเป็นระบบและมีประสิทธิภาพ โดยเริ่มจากการระบุปัจจัยเสี่ยงที่มีผลกระทบต่อการ ดำเนินงาน จากนั้นจึงวิเคราะห์โอกาสและผลกระทบที่อาจเกิดขึ้น พร้อมจัดลำดับความสำคัญของปัจจัยเสี่ยงเหล่านั้น เมื่อทราบถึงปัจจัยเสี่ยงที่มีความสำคัญแล้วจึงต้องกำหนดแนวทางในการจัดการอย่างเหมาะสม โดยคำนึงถึงความคุ้มค่าและประสิทธิภาพในการดำเนินการเพื่อลดความเสี่ยงให้เหลืออยู่ในระดับที่องค์กรสามารถยอมรับได้

2. วัตถุประสงค์

วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกาญจนบุรี เพื่อวัตถุประสงค์ต่อไปนี้

1. เพื่อให้ผู้บริหารและบุคลากรทุกระดับมีความรู้และความเข้าใจในกระบวนการและขั้นตอนของการบริหารความเสี่ยงและการควบคุมภายในอย่างถูกต้อง โดยสามารถนำความรู้ที่ได้ไปประยุกต์ใช้ในการทำงานได้อย่างมีประสิทธิภาพและสามารถรับมือกับความเสี่ยงที่อาจเกิดขึ้นได้อย่างเหมาะสม

2. เพื่อให้แผนการบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยบุคลากรในการปฏิบัติงานได้อย่างเป็นระบบสอดคล้องกับเป้าหมาย ยุทธศาสตร์ และกลยุทธ์ของสำนักฯ รวมถึงการจัดการทรัพยากรอย่างคุ้มค่าและเกิดประโยชน์สูงสุดต่อองค์กร โดยลดผลกระทบที่อาจเกิดจากความเสี่ยงต่าง ๆ

3. เพื่อให้สำนักวิทยบริการฯ สามารถดำเนินงานตามแนวทางการกำกับดูแลที่ดี มีการควบคุมภายในที่โปร่งใส และสอดคล้องกับข้อกำหนดและมาตรฐานการบริหารจัดการที่ถูกต้องตามกฎหมายและระเบียบราชการ ทั้งนี้เพื่อเสริมสร้างความเชื่อมั่นในการบริหารงานขององค์กร

3. ความจำเป็นของการบริหารความเสี่ยงและการควบคุมภายใน

ข้อที่ 1 ตามพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ 5) พ.ศ. 2545 มาตรา 3/1 การบริหารราชการต้องมุ่งเน้นให้เกิดประโยชน์สุขต่อประชาชนและมีผลสัมฤทธิ์ในภารกิจของรัฐ ในกรณีของศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกาญจนบุรี การบริหารความเสี่ยงและการควบคุมภายในจึงมีความสำคัญอย่างยิ่งเพื่อให้กระบวนการทำงานด้านเทคโนโลยีสารสนเทศมีประสิทธิภาพสูงสุด โดยเฉพาะในด้านการให้บริการข้อมูล การจัดการระบบเครือข่าย และการสนับสนุนการดำเนินงานของมหาวิทยาลัยอย่างราบรื่นและมีความโปร่งใส นอกจากนี้ยังช่วยลดขั้นตอนที่ซับซ้อนและเพิ่มคุณภาพการบริการให้แก่คณาจารย์ นักศึกษา และบุคลากร

ข้อที่ 2 พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. 2546 มาตรา 12 ระบุว่า การบริหารงานราชการต้องมีการประเมินผลสัมฤทธิ์และการปฏิบัติงานที่โปร่งใส ก.พ.ร. สามารถกำหนดมาตรการเพื่อให้หน่วยงานภาครัฐรับผิดชอบต่อผลการดำเนินงาน ซึ่งศูนย์เทคโนโลยีสารสนเทศจำเป็นต้องบริหารจัดการความเสี่ยงและควบคุมภายในเพื่อให้มั่นใจว่าบริการด้านเทคโนโลยีสารสนเทศจะตอบสนองความต้องการของมหาวิทยาลัยและชุมชนได้อย่างมีประสิทธิภาพ และสามารถวัดผลการปฏิบัติงานได้อย่างชัดเจน

ข้อที่ 3 สำนักงานการตรวจเงินแผ่นดิน (สตง.) กำหนดระเบียบว่าด้วยมาตรฐานการควบคุมภายใน พ.ศ. 2544 ซึ่งเป็นข้อบังคับให้มหาวิทยาลัยราชภัฏกาญจนบุรีต้องปฏิบัติตามเพื่อตรวจสอบและประเมินผลการดำเนินงานของศูนย์เทคโนโลยีสารสนเทศ การปฏิบัติตามมาตรฐานเหล่านี้ช่วยให้ศูนย์สามารถจัดวางระบบควบคุมภายในที่มีประสิทธิภาพ พร้อมประเมินผลการดำเนินงานได้อย่างโปร่งใสและถูกต้อง ลดความเสี่ยงที่อาจเกิดขึ้นในกระบวนการทำงานด้านเทคโนโลยีสารสนเทศ เช่น การจัดการระบบเครือข่าย ความปลอดภัยของข้อมูล และการใช้ทรัพยากรไอทีอย่างเหมาะสม

ข้อที่ 4 พระราชบัญญัติการศึกษาแห่งชาติ พ.ศ. 2542 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2545 กำหนดให้สถาบันการศึกษาต้องมีระบบการประกันคุณภาพภายในและภายนอก เพื่อรักษามาตรฐานของการศึกษาและการให้บริการทางการศึกษา ศูนย์เทคโนโลยีสารสนเทศจึงต้องมีการบริหารความเสี่ยงและควบคุมภายในที่เข้มแข็ง เพื่อให้สามารถรักษามาตรฐานการให้บริการทางด้านไอที และสนับสนุนการดำเนินงานของมหาวิทยาลัยราชภัฏกาญจนบุรีได้ตามเกณฑ์การประเมินคุณภาพการศึกษาจากสำนักงานรับรองมาตรฐานและประเมินคุณภาพการศึกษา (สมศ.)

ข้อที่ 5 การเปลี่ยนแปลงอย่างรวดเร็วในเทคโนโลยีดิจิทัลทำให้ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกาญจนบุรี ต้องเตรียมพร้อมรับมือกับความเสี่ยงที่เกิดจากปัจจัยภายนอก เช่น การพัฒนาทางเทคโนโลยี การโจมตีทางไซเบอร์ และการบริหารจัดการทรัพยากรที่มีความซับซ้อน การบริหารความเสี่ยงอย่างมีประสิทธิภาพจะช่วยให้ศูนย์ฯ สามารถปรับตัวและรองรับการเปลี่ยนแปลงได้อย่างเหมาะสม เพื่อให้การดำเนินงานเป็นไปตามเป้าหมายที่กำหนดและสนับสนุนการพัฒนามหาวิทยาลัยและชุมชนอย่างยั่งยืน

ดังนั้น สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงนำหลักการบริหารความเสี่ยงมาดำเนินการ เพื่อให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศ สามารถบรรลุผลสำเร็จตามวัตถุประสงค์

4. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

เพื่อให้เข้าใจความหมายและคำจำกัดความของการบริหารความเสี่ยงในบริบทของมหาวิทยาลัยราชภัฏกาญจนบุรี จำเป็นต้องทำความเข้าใจกับคำที่เกี่ยวข้องดังต่อไปนี้อย่างละเอียด

ความเสี่ยง (Risk)

ความเสี่ยงในบริบทของมหาวิทยาลัยราชภัฏกาญจนบุรีหมายถึง เหตุการณ์หรือสถานการณ์ที่มีความไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคตและส่งผลกระทบทั้งทางบวกและทางลบ หากเป็นความเสี่ยงทางลบ อาจทำให้เกิดความผิดพลาด ความเสียหาย หรือปัญหาอื่น ๆ ที่ขัดขวางการดำเนินงานของมหาวิทยาลัย และส่งผลให้ไม่สามารถบรรลุวัตถุประสงค์ที่ตั้งไว้ได้ การบริหารความเสี่ยงในมหาวิทยาลัยจำเป็นต้องพิจารณาทั้งโอกาสที่จะเกิดเหตุการณ์ (Likelihood) และผลกระทบที่อาจเกิดขึ้น (Impact) ซึ่งสามารถแบ่งความเสี่ยงได้เป็นหลายประเภทที่เกี่ยวข้องกับการดำเนินงานของมหาวิทยาลัย ดังนี้

ความเสี่ยงด้านทรัพยากร (Resources Risk)

ความเสี่ยงด้านทรัพยากรของมหาวิทยาลัยราชภัฏกาญจนบุรีเกิดจากการขาดความพร้อมหรือการจัดการทรัพยากรที่ไม่เพียงพอ เช่น การบริหารจัดการงบประมาณที่ไม่เหมาะสม การควบคุมค่าใช้จ่ายที่ไม่รัดกุม รวมถึงความเสี่ยงที่เกิดจากการขาดอุปกรณ์และทรัพยากรด้านเทคโนโลยีสารสนเทศซึ่งเป็นสิ่งสำคัญในการสนับสนุนการเรียนการสอน การวิจัย และการบริการแก่ชุมชน หากไม่มีการจัดการที่มีประสิทธิภาพ การขาดแคลนทรัพยากรอาจส่งผลกระทบต่อการดำเนินงานของมหาวิทยาลัย

ความเสี่ยงด้านยุทธศาสตร์หรือกลยุทธ์ (Strategic Risk)

ความเสี่ยงนี้เกี่ยวข้องกับการวางแผนยุทธศาสตร์หรือการดำเนินงานที่ไม่สอดคล้องกับเป้าหมายของมหาวิทยาลัยราชภัฏกาญจนบุรี เช่น การวางแผนพัฒนามหาวิทยาลัยที่ไม่เหมาะสม หรือการไม่ปรับแผนให้สอดคล้องกับการเปลี่ยนแปลงในสภาพแวดล้อมภายนอก ความเสี่ยงนี้อาจส่งผลต่อทิศทางการพัฒนาของมหาวิทยาลัย ทำให้ไม่สามารถบรรลุวัตถุประสงค์ที่ตั้งไว้ได้ เช่น ความสำเร็จทางการศึกษา การบริการชุมชน หรือการยกระดับคุณภาพการศึกษาให้สอดคล้องกับมาตรฐานที่กำหนด

ความเสี่ยงด้านการปฏิบัติตามกฎหมาย/กฎระเบียบ/ข้อบังคับ (Compliance Risk)

มหาวิทยาลัยราชภัฏกาญจนบุรีจำเป็นต้องปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้อง การไม่สามารถปฏิบัติตามกฎระเบียบหรือการไม่สามารถปรับตัวให้ทันกับการเปลี่ยนแปลงของกฎหมายอาจก่อให้เกิดปัญหาทางกฎหมายหรือส่งผลกระทบต่อการดำเนินงาน เช่น การไม่ปฏิบัติตามระเบียบการศึกษาหรือการบริหารงานที่ไม่สอดคล้องกับข้อบังคับของกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัย และนวัตกรรม ความเสี่ยงนี้อาจนำไปสู่การถูกลงโทษหรือการสูญเสียสิทธิประโยชน์ทางกฎหมาย

ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk)

ความเสี่ยงที่เกิดจากกระบวนการทำงานปกติภายในมหาวิทยาลัย เช่น การบริหารจัดการหลักสูตร การจัดการงานวิจัย การประกันคุณภาพการศึกษา และการบริการนักศึกษา หากขั้นตอนการปฏิบัติงานไม่ได้รับการควบคุมที่ดีเพียงพอหรือเกิดความผิดพลาดในกระบวนการ อาจส่งผลให้การดำเนินงานไม่เป็นไปตามแผนและเกิดผลกระทบต่อคุณภาพการศึกษาหรือการบริการที่มหาวิทยาลัยมุ่งหวัง เช่น การส่งมอบการเรียนการสอนที่ไม่ได้มาตรฐาน การประเมินคุณภาพที่ไม่สอดคล้องกับเกณฑ์ สมศ. หรือความล่าช้าในกระบวนการต่าง ๆ

ความเสี่ยงด้านบุคลากรและธรรมาภิบาล (Human and Good Governance Risk)

มหาวิทยาลัยราชภัฏกาญจนบุรีต้องการบุคลากรที่มีคุณภาพในการสนับสนุนการดำเนินงาน ความเสี่ยงในด้านนี้เกิดจากการขาดประสิทธิภาพในการสรรหาบุคลากร การบรรจุแต่งตั้งที่ไม่สอดคล้องกับความต้องการของมหาวิทยาลัย รวมถึงการขาดแผนการพัฒนาบุคลากรที่ชัดเจน นอกจากนี้ ความเสี่ยงด้านธรรมาภิบาลยังเกี่ยวข้องกับการกำกับดูแลและการบริหารงานที่ไม่โปร่งใส ซึ่งอาจส่งผลให้การบริหารงานขาดความเชื่อมั่นและไม่สามารถสร้างสภาพแวดล้อมการทำงานที่ยั่งยืนได้

ความเสี่ยงจากเหตุการณ์ภายนอก (External Environment Risk)

ความเสี่ยงจากปัจจัยภายนอกมหาวิทยาลัยที่มหาวิทยาลัยราชภัฏกาญจนบุรีไม่สามารถควบคุมได้ เช่น การเปลี่ยนแปลงทางเศรษฐกิจ สังคม การเมือง และเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็ว เช่น การเกิดภาวะวิกฤตเศรษฐกิจที่ส่งผลต่อการจัดสรรงบประมาณ หรือการเปลี่ยนแปลงนโยบายภาครัฐที่กระทบต่อกฎระเบียบของมหาวิทยาลัย ความเสี่ยงเหล่านี้อาจทำให้มหาวิทยาลัยไม่สามารถดำเนินการตามแผนงานที่วางไว้ได้ และต้องปรับตัวอย่างรวดเร็วเพื่อรับมือกับการเปลี่ยนแปลง

ความเสี่ยงด้านอื่น ๆ (Other Risks)

ความเสี่ยงด้านอื่น ๆ ในบริบทของมหาวิทยาลัยราชภัฏกาญจนบุรี ได้แก่ ความเสี่ยงที่เกิดจากการไม่สามารถดำเนินงานได้ตามแนวทางหรือมาตรฐานของมหาวิทยาลัย ความเสี่ยงเหล่านี้อาจเกิดขึ้นจากปัจจัยเฉพาะตัวของมหาวิทยาลัย เช่น การขาดแคลนทรัพยากร ความล่าช้าในการตัดสินใจ หรือการเปลี่ยนแปลงภายในที่ไม่สามารถรับมือได้ทัน

2. ปัจจัยเสี่ยง (Risk Factor) หมายถึง สาเหตุหรือที่มาของความเสี่ยงที่อาจทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์ตามแผนหรือขั้นตอนการดำเนินงานที่กำหนดไว้ ปัจจัยเสี่ยงสามารถมาจากทั้งปัจจัยภายในและภายนอกองค์กร ซึ่งอาจส่งผลต่อการดำเนินงานในหลากหลายรูปแบบ เช่น ความไม่แน่นอนทางเศรษฐกิจ ความเปลี่ยนแปลงทางเทคโนโลยี หรือข้อบกพร่องในกระบวนการทำงานขององค์กรเอง

องค์กรควรทำการระบุสาเหตุที่แท้จริงของปัจจัยเสี่ยงเหล่านี้ เพื่อสามารถวิเคราะห์และหาวิธีจัดการความเสี่ยงได้อย่างถูกต้อง โดยควรกำหนดกลยุทธ์ มาตรการ หรือแนวทางที่ชัดเจนในการลดความเสี่ยงให้สอดคล้องกับสถานการณ์และบริบทเฉพาะขององค์กร การจัดการที่เหมาะสมนี้จะช่วยให้องค์กรสามารถลดความเสี่ยงได้อย่างมีประสิทธิภาพและเพิ่มโอกาสในการบรรลุเป้าหมายที่ตั้งไว้

ปัจจัยภายใน ประกอบด้วย

กลยุทธ์ (Strategy)

หมายถึง ความเหมาะสมของกลยุทธ์ในการตอบสนองต่อสถานการณ์ต่าง ๆ กลยุทธ์ที่มีประสิทธิภาพจะช่วยให้องค์กรสามารถดำเนินการตามวัตถุประสงค์ได้ หากกลยุทธ์ไม่สอดคล้องกับสถานการณ์หรือการเปลี่ยนแปลงภายนอก อาจส่งผลให้การดำเนินงานประสบปัญหาและไม่บรรลุเป้าหมายที่ตั้งไว้

โครงสร้างองค์กร (Structure)

โครงสร้างองค์กรหมายถึงการจัดลำดับขั้นบังคับบัญชา การแบ่งหน้าที่ ความรับผิดชอบภายในหน่วยงาน การมีโครงสร้างที่เหมาะสมจะช่วยให้องค์กรดำเนินงานได้อย่างมีประสิทธิภาพ สามารถปรับตัวได้ตามพันธกิจ และบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิผล

ระบบ (System)

การดำเนินงานในองค์กรต้องมีระบบที่ถูกต้องและเหมาะสม ไม่ว่าจะเป็นระบบการคัดเลือกสรรหาบุคลากร ระบบการประเมินผล ระบบการพิจารณาความดีความชอบ ระบบการเงิน ระบบการผลิตบัณฑิต ระบบการจัดซื้อจัดจ้าง และระบบสารสนเทศ การมีระบบที่ดีจะช่วยให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและลดความเสี่ยงต่าง ๆ

รูปแบบการบริหารจัดการ (Style)

การบริหารจัดการต้องมีความยืดหยุ่นและสอดคล้องกับสภาพแวดล้อมที่เปลี่ยนแปลงอยู่ตลอดเวลา รูปแบบการบริหารที่เหมาะสมจะช่วยให้องค์กรสามารถปรับตัวได้ทันต่อการเปลี่ยนแปลงและสามารถบริหารทรัพยากรได้อย่างมีประสิทธิภาพ

บุคลากร (Staff)

บุคลากรต้องมีศักยภาพและสมรรถนะที่เหมาะสมกับงานที่ได้รับมอบหมาย บุคลากรที่มีคุณภาพจะช่วยให้องค์กรสามารถดำเนินงานได้อย่างราบรื่นและบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพ

ทักษะ (Skill)

ทักษะขององค์กรและบุคลากรต้องมีความเหนือกว่า หรือเทียบเท่ากับคู่แข่ง หากทักษะด้อยกว่าคู่แข่ง อาจทำให้องค์กรสูญเสียความสามารถในการแข่งขันในตลาดและอุตสาหกรรม

ค่านิยม (Share Value)

ค่านิยมร่วมของบุคลากรภายในองค์กรเป็นสิ่งที่ช่วยสนับสนุนให้การดำเนินงานเป็นไปตามทิศทางที่กำหนด หากค่านิยมของบุคลากรสอดคล้องกับเป้าหมายและการเปลี่ยนแปลงในสภาพแวดล้อม องค์กรจะสามารถปรับตัวและพัฒนาได้อย่างต่อเนื่อง

ปัจจัยภายนอก ประกอบด้วย

ด้านเศรษฐกิจ

ปัจจัยทางเศรษฐกิจมีผลต่อการดำเนินงานขององค์กร เช่น ราคาน้ำมัน อัตราแลกเปลี่ยน อัตราดอกเบี้ย อัตราว่างงาน และตลาดหุ้น ปัจจัยเหล่านี้ส่งผลต่อค่าใช้จ่าย การจัดการงบประมาณ และความสามารถในการแข่งขัน

ด้านสังคมและสิ่งแวดล้อม

ความเปลี่ยนแปลงด้านประชากร ความขัดแย้งทางสังคม ภัยสงคราม หรือภัยธรรมชาติล้วนส่งผลกระทบต่อการดำเนินงานขององค์กร หากมีความไม่มั่นคงในสังคมหรือสภาพแวดล้อม เช่น ภัยธรรมชาติ องค์กรอาจต้องเผชิญกับความยากลำบากในการดำเนินธุรกิจ

ด้านการเมือง

การเปลี่ยนแปลงทางการเมืองส่งผลกระทบต่อความต่อเนื่องของนโยบายรัฐบาล หากนโยบายเปลี่ยนแปลงไปตามความไม่แน่นอนทางการเมือง องค์กรอาจต้องปรับเปลี่ยนกลยุทธ์หรือนโยบายการดำเนินงานให้สอดคล้องกับนโยบายใหม่

ด้านกฎหมาย

กฎหมายที่คลุมเครือหรือเปลี่ยนแปลงบ่อยครั้งเป็นความเสี่ยงต่อองค์กร เช่น กฎระเบียบที่ล้าหลังหรือไม่ทันกับการเปลี่ยนแปลง กฎหมายที่ไม่ครอบคลุม หรือการบังคับใช้กฎหมายที่ไม่ชัดเจน ปัจจัยเหล่านี้สามารถสร้างอุปสรรคต่อการดำเนินงานขององค์กรและทำให้เกิดความไม่แน่นอน

ด้านเทคโนโลยี

ความก้าวหน้าของเทคโนโลยีมีผลต่อความสามารถในการแข่งขันขององค์กร หากองค์กรไม่สามารถปรับตัวให้ทันกับการเปลี่ยนแปลงทางเทคโนโลยีได้ อาจทำให้สูญเสียโอกาสในการแข่งขัน

3. การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการในการระบุและวิเคราะห์ความเสี่ยง เพื่อจัดลำดับความสำคัญของความเสี่ยงที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร การประเมินนี้พิจารณาจากสองปัจจัยหลัก คือ โอกาสที่จะเกิดเหตุการณ์ (Likelihood) และผลกระทบ (Impact) ที่อาจเกิดขึ้นจากเหตุการณ์ความเสี่ยง

โอกาสที่จะเกิดเหตุการณ์ (Likelihood) หมายถึง ความถี่หรือโอกาสที่เหตุการณ์ความเสี่ยงจะเกิดขึ้น ซึ่งอาจเกิดจากปัจจัยต่าง ๆ เช่น ปัจจัยภายในองค์กรหรือสภาพแวดล้อมภายนอก โอกาสเกิดนี้สามารถประเมินได้จากประวัติที่ผ่านมา หรือลักษณะของเหตุการณ์ที่มีโอกาสเกิดขึ้นในอนาคต

ผลกระทบ (Impact) หมายถึง ความรุนแรงหรือขนาดของความเสียหายที่จะเกิดขึ้นหากเหตุการณ์ความเสี่ยงนั้นเกิดขึ้นจริง ผลกระทบอาจวัดได้จากผลเสียต่อทรัพยากร การดำเนินงาน ความสามารถในการแข่งขันขององค์กร หรือชื่อเสียง ทั้งนี้ยิ่งผลกระทบรุนแรง ความเสี่ยงนั้นจะได้รับการจัดลำดับให้มีความสำคัญมากขึ้น

ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะหรือระดับของความเสี่ยงที่ได้จากการประเมินทั้งโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง โดยแบ่งออกเป็น 4 ระดับ ได้แก่

1) ความเสี่ยงสูงมาก (Very High Risk) หมายถึง ความเสี่ยงที่มีโอกาสเกิดขึ้นบ่อยและมีผลกระทบสูงมากต่อการดำเนินงานขององค์กร

2) ความเสี่ยงสูง (High Risk) หมายถึง ความเสี่ยงที่มีโอกาสเกิดขึ้นค่อนข้างบ่อยและมีผลกระทบมาก

3) ความเสี่ยงปานกลาง (Moderate Risk) หมายถึง ความเสี่ยงที่มีโอกาสเกิดขึ้นบ้างและมีผลกระทบปานกลาง

4) ความเสี่ยงน้อย (Low Risk) หมายถึง ความเสี่ยงที่มีโอกาสเกิดขึ้นน้อยและมีผลกระทบต่ำ

4. การจัดการความเสี่ยง (Risk Response) หมายถึง แนวทางการบริหารจัดการเพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ความเสี่ยงให้อยู่ในระดับที่องค์กรสามารถยอมรับได้ (Risk Acceptance) การจัดการความเสี่ยงนี้ต้องคำนึงถึงความเหมาะสมและความคุ้มค่าในการเลือกวิธีการจัดการ โดยเฉพาะในกรณีที่ความเสี่ยงเกิดจากปัจจัยภายนอกที่องค์กรไม่สามารถควบคุมได้ มีแนวทางการจัดการความเสี่ยง ดังนี้

1) การลดความรุนแรงของความเสี่ยง (Risk Reduction) การลดความเสี่ยงสามารถทำได้โดยการเปลี่ยนแปลงขั้นตอนหรือปรับปรุงกระบวนการบางส่วนในกิจกรรมหรือโครงการ เพื่อลดโอกาสการเกิดเหตุการณ์ความเสี่ยง หรือเพื่อบรรเทาความรุนแรงของผลกระทบเมื่อเกิดเหตุการณ์ ตัวอย่างเช่น การฝึกอบรมบุคลากรเพื่อเพิ่มความรู้ความเข้าใจ การแยกหน้าที่ระหว่างผู้จัดซื้อจัดจ้างกับผู้ตรวจรับ การสำรองข้อมูล (Back up) อย่างสม่ำเสมอ หรือการติดตั้งเครื่องดับเพลิงเพื่อลดความเสียหายจากเหตุการณ์ที่อาจเกิดขึ้น

2) การแบ่งปันความเสี่ยง (Risk Sharing) การแบ่งปันความเสี่ยงหมายถึงการถ่ายโอนความเสี่ยงบางส่วนให้กับหน่วยงานหรือบุคคลอื่น ๆ เพื่อร่วมรับผิดชอบเมื่อเกิดเหตุการณ์ความเสี่ยง แม้ว่าการแบ่งปันจะไม่สามารถลดโอกาสการเกิดเหตุการณ์ได้ แต่ช่วยให้มั่นใจว่าเมื่อเกิดความเสียหาย องค์กรจะได้รับการชดใช้ ตัวอย่างการแบ่งปันความเสี่ยง เช่น การทำประกัน การทำสัญญาที่กำหนดความรับผิดชอบร่วมกัน หรือการจ้างผู้ดำเนินการภายนอก

3) การยอมรับความเสี่ยง (Risk Acceptance) การยอมรับความเสี่ยงเกิดขึ้นเมื่อองค์กรตัดสินใจที่จะจัดการความเสี่ยงภายในหน่วยงานเอง หากการวิเคราะห์พบว่าต้นทุนในการจัดการความเสี่ยงสูงกว่าผลประโยชน์ที่ได้รับ องค์กรอาจเลือกที่จะยอมรับความเสี่ยง แต่ต้องติดตามความเสี่ยงนั้นอย่างใกล้ชิดและเตรียมมาตรการรองรับหากเกิดเหตุการณ์ขึ้น

4) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การหลีกเลี่ยงความเสี่ยงหมายถึงการหลีกเลี่ยงกิจกรรมหรือโครงการที่อาจนำไปสู่เหตุการณ์ความเสี่ยง โดยองค์กรอาจเลือกที่จะหยุด ยกเลิกหรือเปลี่ยนแปลงกิจกรรมเพื่อป้องกันไม่ให้เกิดความเสี่ยง การหลีกเลี่ยงเป็นวิธีการที่ใช้เมื่อต้องการลดความเสี่ยงอย่างเด็ดขาด แต่ควรคำนึงถึงความเป็นไปได้ในการดำเนินการในระยะยาวกรณีที่ความเสี่ยงเกิดจากปัจจัยภายใน ซึ่งอยู่ภายใต้การควบคุมของฝ่ายบริหาร การจัดการความเสี่ยงสามารถทำได้โดยการวางแผนการควบคุมที่เพียงพอ เช่น การเพิ่มประสิทธิภาพของการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับเพื่อลดโอกาสเกิดความเสียหายในด้านต่าง ๆ ทั้งในรูปแบบตัวเงินและชื่อเสียงขององค์กร

5) การบริหารความเสี่ยง (Enterprise Risk Management) หมายถึง กระบวนการที่ครอบคลุมการบริหารจัดการปัจจัยเสี่ยง และการควบคุมกิจกรรมต่าง ๆ ในการดำเนินงานขององค์กร เพื่อลดสาเหตุและโอกาสที่จะเกิดความเสียหาย โดยมุ่งให้ระดับความเสี่ยงและผลกระทบที่จะเกิดขึ้นอยู่ในระดับที่องค์กรสามารถยอมรับได้ กระบวนการนี้ต้องประเมิน ควบคุม และตรวจสอบได้อย่างเป็นระบบ การบริหารความเสี่ยงมีวัตถุประสงค์หลักคือการป้องกันผลกระทบที่จะทำให้การบรรลุพันธกิจ ยุทธศาสตร์ เป้าประสงค์ และกลยุทธ์ขององค์กรต้องหยุดชะงัก นอกจากนี้ การบริหารความเสี่ยงยังมีส่วนสำคัญในการรักษาและส่งเสริมชื่อเสียงขององค์กร

องค์กรต้องให้ความสำคัญกับการสนับสนุนและการมีส่วนร่วมจากหน่วยงานทุกระดับ เพื่อให้การบริหารความเสี่ยงดำเนินไปอย่างมีประสิทธิภาพ ซึ่งจะช่วยให้องค์กรสามารถเผชิญและจัดการกับความเสี่ยงที่อาจเกิดขึ้นได้อย่างเหมาะสม

6) การติดตามประเมินผล หมายถึง กระบวนการที่ใช้ในการตรวจสอบและประเมินคุณภาพของการปฏิบัติงาน รวมถึงการประเมินประสิทธิผลของระบบควบคุมภายในและการบริหารความเสี่ยงที่กำหนดไว้อย่างต่อเนื่องและสม่ำเสมอ การติดตามประเมินผลนี้มีวัตถุประสงค์เพื่อให้มั่นใจว่าระบบควบคุมภายในและการบริหารความเสี่ยงมีความเพียงพอและเหมาะสม สามารถปฏิบัติได้จริง และปัญหาหรือข้อบกพร่องที่พบได้รับการแก้ไขอย่างถูกต้องและทันเวลาเพื่อป้องกันไม่ให้เกิดผลกระทบต่อการดำเนินงานขององค์กร

7) เป้าประสงค์ขององค์กร (Goal) หมายถึง ความต้องการหรือผลลัพธ์ที่ผู้วางยุทธศาสตร์หรือผู้บริหารองค์กรต้องการให้เกิดขึ้นตามที่คาดหวัง โดยเป้าประสงค์ขององค์กรจะถูกกำหนดในลักษณะที่ครอบคลุมและกว้างขวาง เพื่อให้สะท้อนถึงวิสัยทัศน์ขององค์กร ซึ่งมักแบ่งออกเป็นสองประเภทหลัก คือ

- **เป้าประสงค์เชิงแก้ปัญหา (Problematic Goal)** หมายถึง เป้าหมายที่มุ่งเน้นการแก้ไขปัญหาที่องค์กรกำลังเผชิญ เช่น การปรับปรุงประสิทธิภาพ การลดต้นทุน หรือการแก้ไขปัญหาที่ส่งผลกระทบต่อการดำเนินงาน

- **เป้าประสงค์เชิงพัฒนา (Development Goal)** หมายถึง เป้าหมายที่มุ่งเน้นการพัฒนาหรือสร้างความก้าวหน้าให้กับองค์กร เช่น การขยายธุรกิจ การเพิ่มประสิทธิภาพในการทำงาน หรือการพัฒนาทักษะและศักยภาพของบุคลากร

8) การควบคุมภายใน (Control) หมายถึง กระบวนการปฏิบัติงานที่ฝ่ายบริหารและบุคลากรในหน่วยงานจัดให้มีขึ้นเพื่อควบคุมการดำเนินงานขององค์กรให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล การควบคุมภายในมักแสดงออกมาในรูปแบบของนโยบาย แนวทางปฏิบัติ กฎ ระเบียบ ข้อบังคับ คู่มือ หรือขั้นตอนการปฏิบัติต่าง ๆ เพื่อช่วยลดความเสี่ยงที่อาจเกิดขึ้นในกระบวนการทำงาน การควบคุมเหล่านี้มีบทบาทสำคัญในการป้องกันข้อผิดพลาด การทุจริต และการบริหารจัดการที่ไม่เหมาะสม อีกทั้งยังช่วยให้มั่นใจว่าการดำเนินงานของหน่วยงานเป็นไปตามเป้าหมายและมาตรฐานที่กำหนด

บทที่ 2
แนวทางการบริหารความเสี่ยงและการควบคุมภายใน

การบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประกอบด้วย

1. นโยบาย วัตถุประสงค์ของการบริหารความเสี่ยง
2. โครงสร้างการบริหารความเสี่ยง
3. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการและคณะทำงานบริหารความเสี่ยง

1. นโยบาย วัตถุประสงค์ของการบริหารความเสี่ยงและการควบคุมภายใน

1.1 นโยบายการบริหารความเสี่ยง

ผู้บริหารของสำนักวิทยบริการและเทคโนโลยีสารสนเทศกำหนดนโยบายการบริหารความเสี่ยงให้สอดคล้องกับภารกิจหลักขององค์กร และให้เป็นไปตามแนวทางการบริหารความเสี่ยง ดังนี้

1. ให้มีการบริหารความเสี่ยงทั่วทั้งองค์กรแบบบูรณาการ โดยการจัดการความเสี่ยงอย่างเป็นระบบและต่อเนื่อง ครอบคลุมทุกส่วนขององค์กรเพื่อให้มั่นใจว่าความเสี่ยงจะถูกควบคุมในทุกขั้นตอนการดำเนินงาน
2. ให้กำหนดกระบวนการบริหารความเสี่ยงที่เป็นมาตรฐานเดียวกันทั่วทั้งองค์กร เพื่อให้ทุกหน่วยงานภายในองค์กรปฏิบัติตามหลักการเดียวกันและสอดคล้องกัน
3. ให้มีการติดตามและประเมินผลการบริหารความเสี่ยงอย่างสม่ำเสมอ พร้อมทั้งทบทวนและปรับปรุงกระบวนการบริหารความเสี่ยงตามความเหมาะสม เพื่อตอบสนองต่อการเปลี่ยนแปลงที่เกิดขึ้น
4. ส่งเสริมการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารความเสี่ยง เพื่อเพิ่มประสิทธิภาพและความแม่นยำในการจัดการและประเมินความเสี่ยง
5. ให้การบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการดำเนินงานปกติขององค์กร โดยรวมความเสี่ยงเข้ากับกิจกรรมในชีวิตประจำวัน เพื่อให้การจัดการความเสี่ยงเป็นไปอย่างต่อเนื่องและราบรื่น

1.2 วัตถุประสงค์ของการบริหารความเสี่ยง

1. เพื่อเพิ่มประสิทธิภาพในการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงที่อาจมีผลกระทบต่อการดำเนินงาน การกำหนดวัตถุประสงค์ และนโยบายขององค์กร การพิจารณาปัจจัยเหล่านี้ก่อนการปฏิบัติงานจะช่วยให้องค์กรสามารถป้องกันหรือลดความเสี่ยงได้ล่วงหน้า

2. เพื่อให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศสามารถลดขนาดของความเสียหายที่จะเกิดขึ้นในอนาคตให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยทำให้สามารถควบคุมและตรวจสอบได้อย่างมีประสิทธิภาพ

2. โครงสร้างการบริหารความเสี่ยง

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีโครงสร้างการบริหารความเสี่ยง

3. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการและคณะทำงานบริหารความเสี่ยง

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ กำหนดให้การบริหารความเสี่ยงเป็นความรัผบผิดชอบร่วมกันของผู้บริหารและบุคลากรทุกระดับ เพื่อให้กระบวนการบริหารความเสี่ยงดำเนินไปอย่างเป็นระบบและต่อเนื่อง บทบาทหน้าที่และความรับผิดชอบหลักของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีดังนี้

ตารางสรุปบทบาทหน้าที่และความรับผิดชอบหลักของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยง เพื่อให้การจัดการความเสี่ยงในสำนักวิทยบริการและเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ

ผู้ที่เกี่ยวข้อง	หน้าที่และความรับผิดชอบ
คณะกรรมการบริหารความเสี่ยง	1. กำหนดนโยบายและระบบบริหารความเสี่ยง รวมถึงวางแผนดำเนินการบริหารความเสี่ยงขององค์กร
	2. ติดตามและประเมินผลการบริหารความเสี่ยง ตั้งแต่การระบุความเสี่ยง การวิเคราะห์ ประเมิน และจัดการ รวมถึงการติดตามผลและรายงานความเสี่ยงอย่างเป็นระบบ
	3. สนับสนุนและให้คำแนะนำเกี่ยวกับกระบวนการบริหารความเสี่ยงแก่บุคลากรภายในองค์กร และติดตามให้มีการปฏิบัติอย่างต่อเนื่องและสม่ำเสมอ
	4. เสนอแนะนโยบายและแนวทางในการบริหารความเสี่ยงต่อมหาวิทยาลัย
คณะทำงานบริหารความเสี่ยง	1. วิเคราะห์และระบุปัจจัยเสี่ยงที่อาจก่อให้เกิดผลกระทบหรือความเสียหายต่อเป้าหมายขององค์กร รวมถึงจัดลำดับความสำคัญของปัจจัยเสี่ยงในแต่ละด้าน
	2. จัดทำแผนการบริหารความเสี่ยงทั้งในระดับองค์กรและระดับกิจกรรม เพื่อให้การดำเนินงานสอดคล้องกับความเสี่ยงที่ตรวจพบ
	3. เสนอแนวทางและข้อเสนอแนะในการปรับปรุงแผนบริหารความเสี่ยงให้มีประสิทธิภาพในการลดความเสี่ยงและป้องกันปัญหาในอนาคต
ผู้บริหารระดับสูงและหัวหน้าหน่วยงาน	1. นำแผนการบริหารความเสี่ยงไปปฏิบัติและสนับสนุนให้การบริหารความเสี่ยงในหน่วยงานเป็นไปตามทิศทางที่กำหนด
	2. ติดตามและรายงานความก้าวหน้าในการบริหารความเสี่ยง รวมถึงการปรับปรุงแผนการบริหารความเสี่ยงตามความจำเป็น
	3. ส่งเสริมให้บุคลากรภายในหน่วยงานเข้าใจบทบาทและหน้าที่ในการจัดการความเสี่ยง รวมถึงมีส่วนร่วมในกระบวนการบริหารความเสี่ยง
บุคลากรทุกระดับ	1. ปฏิบัติตามแนวทางและแผนบริหารความเสี่ยงที่กำหนด และร่วมมือในการป้องกันความเสี่ยงที่อาจเกิดขึ้นในกระบวนการทำงาน
	2. ระบุและรายงานความเสี่ยงที่ตรวจพบในงานที่รับผิดชอบต่อผู้บังคับบัญชาเพื่อให้มีการจัดการที่เหมาะสม
	3. ปฏิบัติตามมาตรการป้องกันและลดความเสี่ยงที่กำหนดไว้ในแผนการบริหารความเสี่ยง เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและลดความเสียหายที่อาจเกิดขึ้น

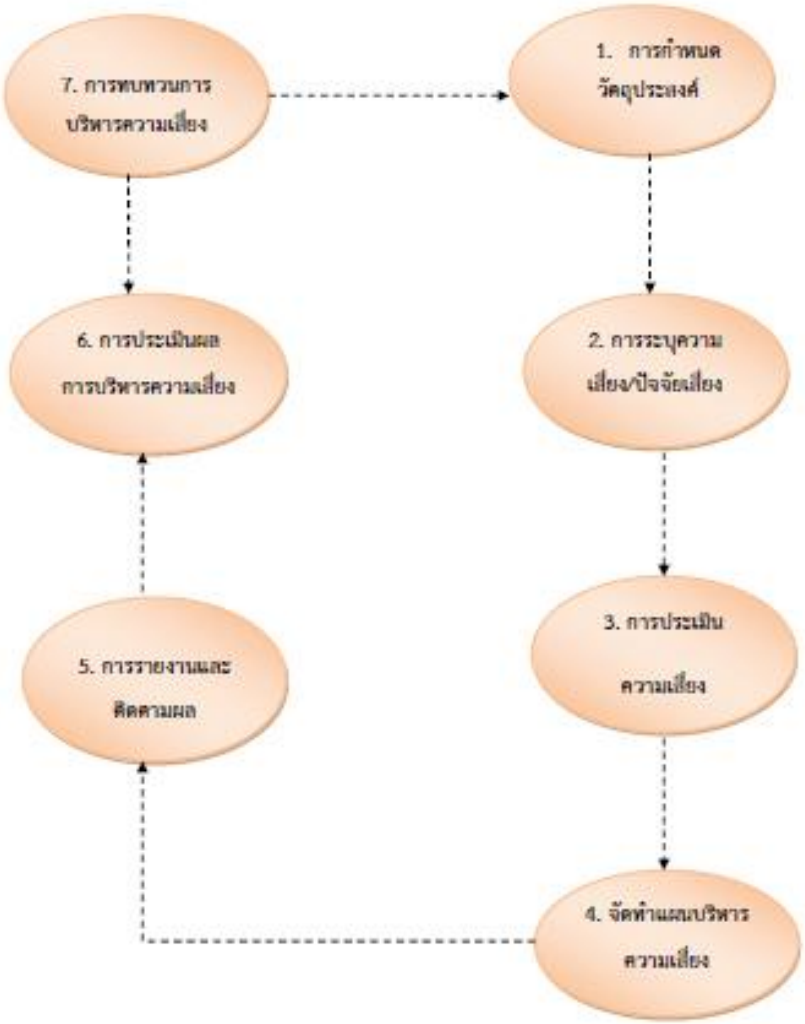
บทที่ 3
กระบวนการบริหารความเสี่ยงและการควบคุมภายใน

กระบวนการบริหารความเสี่ยง เป็นกระบวนการสำคัญที่ช่วยให้องค์กรสามารถระบุ วิเคราะห์ ประเมิน และจัดการความเสี่ยงที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กรหรือหน่วยงาน กระบวนการนี้ครอบคลุมถึงการกำหนดแนวทางการควบคุมเพื่อป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ การบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่องจำเป็นต้องได้รับความร่วมมือจากบุคลากรทุกระดับในองค์กร และต้องมีการสื่อสารให้ทุกคนเข้าใจในเรื่องของการบริหารความเสี่ยงในทิศทางเดียวกัน นอกจากนี้ ยังต้องจัดทำระบบสารสนเทศเพื่อใช้ในการสนับสนุนการวิเคราะห์และประเมินความเสี่ยงได้อย่างมีประสิทธิภาพ สำนักวิทยบริการและเทคโนโลยีสารสนเทศได้นำกระบวนการบริหารความเสี่ยงมาใช้ โดยมีขั้นตอนการดำเนินงาน 7 ขั้นตอนดังนี้

1. **การกำหนดวัตถุประสงค์** การกำหนดวัตถุประสงค์เป็นขั้นตอนแรกของการบริหารความเสี่ยง โดยต้องกำหนดวัตถุประสงค์และกลยุทธ์ที่ชัดเจนของแผนงาน โครงการ หรือกิจกรรมต่าง ๆ ตามแผนปฏิบัติราชการประจำปี รวมถึงต้องสอดคล้องกับวัตถุประสงค์ของมหาวิทยาลัย การกำหนดวัตถุประสงค์นี้เป็นพื้นฐานสำคัญที่จะนำไปสู่การวิเคราะห์ความเสี่ยงและการจัดการความเสี่ยงในขั้นตอนต่อไป การกำหนดวัตถุประสงค์ที่ชัดเจนจะช่วยให้การดำเนินงานเป็นไปในทิศทางที่ถูกต้องและสามารถประเมินความเสี่ยงได้อย่างแม่นยำ
2. **การระบุความเสี่ยง** หลังจากกำหนดวัตถุประสงค์ ขั้นตอนถัดมาคือการระบุความเสี่ยงที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ ความเสี่ยงสามารถแบ่งออกได้เป็นทั้งด้านบวกและด้านลบ ซึ่งต้องมีการวิเคราะห์ว่าเหตุการณ์ใดบ้างที่อาจเกิดขึ้นและมีโอกาสสร้างผลกระทบต่อการดำเนินงาน ต้องพิจารณาว่าความเสี่ยงอาจเกิดขึ้นที่ไหน เมื่อไหร่ และอย่างไร โดยการระบุความเสี่ยงนี้จำเป็นต้องใช้ข้อมูลจากหลายแหล่ง เช่น ประวัติความเสี่ยงในอดีต การวิเคราะห์สภาพแวดล้อมภายนอก และการสำรวจภายในองค์กร
3. **การประเมินความเสี่ยง** เมื่อระบุความเสี่ยงได้แล้ว จะเข้าสู่ขั้นตอนการประเมินความเสี่ยง ซึ่งประกอบด้วยการวิเคราะห์ความเสี่ยงในแง่ของโอกาสที่จะเกิดขึ้น (Likelihood) และความรุนแรงของผลกระทบที่จะตามมา (Impact) การประเมินนี้ต้องอิงตามเกณฑ์มาตรฐานที่กำหนดไว้ เพื่อให้สามารถจัดลำดับความสำคัญของความเสี่ยงได้อย่างมีประสิทธิภาพ ความเสี่ยงที่มีโอกาสเกิดขึ้นสูงและมีผลกระทบรุนแรงจะต้องได้รับการจัดการก่อน ขณะที่ความเสี่ยงที่มีโอกาสเกิดขึ้นต่ำและผลกระทบน้อยอาจได้รับการจัดการในลำดับถัดไป การประเมินความเสี่ยงอย่างถูกต้องจะช่วยให้การตัดสินใจจัดการความเสี่ยงเป็นไปอย่างเหมาะสม

4. **การจัดทำแผนบริหารความเสี่ยง** หลังจากประเมินความเสี่ยงแล้ว ขั้นตอนต่อไปคือการจัดทำแผนบริหารความเสี่ยง ซึ่งเป็นการกำหนดมาตรการหรือแผนปฏิบัติการที่ชัดเจนในการจัดการกับความเสี่ยงที่ได้รับการระบุว่าอยู่ในระดับสูงหรือสูงมาก แผนนี้ต้องออกแบบมาเพื่อควบคุมและลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ การจัดทำแผนบริหารความเสี่ยงต้องคำนึงถึงความคุ้มค่าในด้านค่าใช้จ่ายและต้นทุนที่ใช้ในการดำเนินการ เช่น การฝึกอบรมบุคลากร การปรับปรุงระบบงาน หรือการติดตั้งเทคโนโลยีที่สามารถช่วยลดความเสี่ยง นอกจากนี้ การตัดสินใจเลือกวิธีการจัดการความเสี่ยงควรพิจารณาประโยชน์ที่จะได้รับจากการดำเนินมาตรการเหล่านั้นด้วย
5. **การรายงานและติดตามผล** ขั้นตอนนี้เป็นการรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงต่อฝ่ายบริหาร เพื่อให้รับทราบถึงความก้าวหน้าและปัญหาที่เกิดขึ้นในการบริหารความเสี่ยง นอกจากนี้ การติดตามผลจะช่วยให้มั่นใจว่าแผนการบริหารความเสี่ยงที่ได้กำหนดไว้กำลังถูกดำเนินการอย่างมีประสิทธิภาพ การติดตามต้องเป็นไปอย่างต่อเนื่อง เพื่อให้สามารถปรับปรุงและแก้ไขปัญหาที่เกิดขึ้นได้ทันเวลา การรายงานต้องครอบคลุมข้อมูลเกี่ยวกับความเสี่ยงที่ยังคงอยู่ ผลของการจัดการความเสี่ยง และข้อเสนอแนะสำหรับการปรับปรุงแผนการบริหารความเสี่ยงในอนาคต
6. **การประเมินผลบริหารความเสี่ยง** เป็นการประเมินผลการดำเนินการบริหารความเสี่ยงทั้งหมดในแต่ละปี เพื่อให้มั่นใจว่าองค์กรมีการจัดการความเสี่ยงอย่างเหมาะสม เพียงพอ และมีประสิทธิผล คณะทำงานวิเคราะห์และจัดทำแผนบริหารความเสี่ยงของมหาวิทยาลัยจะทำหน้าที่ประเมินมาตรการและกลไกควบคุมความเสี่ยงที่มีอยู่ เพื่อตรวจสอบว่ามาตรการเหล่านั้นสามารถลดและควบคุมความเสี่ยงได้จริงหรือไม่ หากพบว่าความเสี่ยงยังคงอยู่ในระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องหามาตรการเพิ่มเติมเพื่อปรับปรุงการควบคุมความเสี่ยง
7. **การทบทวนการบริหารความเสี่ยง** ขั้นตอนสุดท้ายคือการทบทวนกระบวนการบริหารความเสี่ยงในทุกขั้นตอน เพื่อปรับปรุงและพัฒนาระบบให้ดียิ่งขึ้น การทบทวนนี้เป็นการตรวจสอบว่ามาตรการที่นำมาใช้นั้นมีประสิทธิภาพในการลดความเสี่ยงและป้องกันปัญหาได้จริงหรือไม่ รวมถึงการตรวจสอบว่ากระบวนการบริหารความเสี่ยงนั้นยังคงสอดคล้องกับการเปลี่ยนแปลงของสภาพแวดล้อมทั้งภายในและภายนอกองค์กรหรือไม่ การทบทวนนี้จะช่วยให้การบริหารความเสี่ยงมีความยั่งยืนและตอบสนองต่อการเปลี่ยนแปลงได้ดียิ่งขึ้น

กระบวนการบริหารความเสี่ยงและการควบคุมภายใน



1. การกำหนดวัตถุประสงค์ (Set Objectives)

การกำหนดวัตถุประสงค์ในองค์กรเป็นขั้นตอนสำคัญที่ต้องดำเนินการอย่างรอบคอบและมีความเชื่อมโยงกันอย่างชัดเจนระหว่างวิสัยทัศน์ พันธกิจ และเป้าหมายเชิงกลยุทธ์ขององค์กร เพื่อให้ทุกระดับภายในองค์กรมีทิศทางการทำงานที่สอดคล้องกัน ตั้งแต่ระดับองค์กร หน่วยงาน จนถึงระดับกิจกรรมและบุคคล วัตถุประสงค์ขององค์กรต้องถูกกำหนดให้เชื่อมโยงกับผลลัพธ์ที่ต้องการ ไม่ใช่การอธิบายถึงวิธีการหรือกระบวนการ แต่เป็นเป้าหมายที่ต้องการบรรลุ ผลลัพธ์ที่ชัดเจนนี้จะช่วยให้องค์กรสามารถประเมินและจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

การกำหนดวัตถุประสงค์มีลำดับขั้นตอนที่ชัดเจนดังนี้

ขั้นตอนการกำหนดวัตถุประสงค์

1. **กำหนดพันธกิจขององค์กร** การกำหนดพันธกิจเป็นจุดเริ่มต้นสำคัญขององค์กร ซึ่งสะท้อนถึงภารกิจหลักที่องค์กรมุ่งเน้น พันธกิจควรชัดเจนและครอบคลุมทุกแง่มุมของการดำเนินงานขององค์กร เพื่อให้ทุกหน่วยงานมีความเข้าใจตรงกันในทิศทางการดำเนินงานที่ควรปฏิบัติ
2. **กำหนดวัตถุประสงค์ในระดับองค์กร** หลังจากกำหนดพันธกิจแล้ว จะต้องกำหนดวัตถุประสงค์ในระดับองค์กร ซึ่งเป็นภาพรวมของการดำเนินงานทั้งหมด วัตถุประสงค์ในระดับนี้จะถูกกำหนดตามแผนปฏิบัติราชการประจำปี และแผนปฏิบัติราชการ 4 ปี วัตถุประสงค์ในระดับองค์กรจะเป็นเส้นทางหลักที่องค์กรต้องการบรรลุ เป้าหมายเหล่านี้ควรสอดคล้องกับพันธกิจที่กำหนดไว้และเชื่อมโยงกับทิศทางการดำเนินงานในทุกระดับ
3. **กำหนดกิจกรรมที่สนับสนุนวัตถุประสงค์ขององค์กร** เพื่อให้วัตถุประสงค์ในระดับองค์กรสามารถบรรลุได้อย่างมีประสิทธิภาพ จำเป็นต้องกำหนดกิจกรรมหรือโครงการที่ชัดเจนและสอดคล้องกับวัตถุประสงค์เหล่านั้น กิจกรรมที่ถูกกำหนดขึ้นจะต้องสามารถสนับสนุนการบรรลุวัตถุประสงค์ในระดับองค์กร และช่วยสร้างความชัดเจนในกระบวนการทำงาน
4. **กำหนดวัตถุประสงค์ในระดับกิจกรรม** เมื่อมีกิจกรรมที่ชัดเจนแล้ว จะต้องกำหนดวัตถุประสงค์เฉพาะสำหรับแต่ละกิจกรรม วัตถุประสงค์ในระดับกิจกรรมนี้จะต้องสอดคล้องและสนับสนุนวัตถุประสงค์ในระดับองค์กร การกำหนดวัตถุประสงค์ในระดับกิจกรรมช่วยให้การดำเนินงานในแต่ละส่วนชัดเจนและสามารถระบุความเสี่ยงที่อาจเกิดขึ้นได้อย่างครบถ้วน

ประเภทของวัตถุประสงค์

วัตถุประสงค์ของการบริหารความเสี่ยงสามารถแบ่งออกได้เป็น 2 ระดับ คือ

1. **วัตถุประสงค์ในระดับองค์กร** วัตถุประสงค์ในระดับองค์กรเป็นวัตถุประสงค์หลักของการดำเนินงานที่ครอบคลุมภาพรวมของทั้งองค์กร ซึ่งสอดคล้องกับแผนปฏิบัติราชการประจำปีและแผนปฏิบัติราชการ 4 ปี วัตถุประสงค์นี้มีความสำคัญในการกำหนดทิศทางและเป้าหมายที่องค์กรต้องการบรรลุในระยะยาว วัตถุประสงค์เหล่านี้มักเกี่ยวข้องกับการดำเนินงานในภาพรวม เช่น การพัฒนาองค์กร การเพิ่มประสิทธิภาพการดำเนินงาน และการสร้างความยั่งยืนในเชิงกลยุทธ์
2. **วัตถุประสงค์ในระดับกิจกรรม** วัตถุประสงค์ในระดับกิจกรรมเป็นวัตถุประสงค์ที่มีความเฉพาะเจาะจงมากขึ้น เพื่อสนับสนุนการบรรลุวัตถุประสงค์ในระดับองค์กร วัตถุประสงค์ในระดับกิจกรรมจะถูกกำหนดขึ้นสำหรับแต่ละกิจกรรมหรือโครงการที่องค์กรดำเนินการ การกำหนดวัตถุประสงค์ในระดับ

กิจกรรมจะช่วยให้สามารถระบุความเสี่ยงและปัจจัยที่จะมีผลต่อความสำเร็จของกิจกรรมได้อย่างชัดเจน วัตถุประสงค์ในระดับกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร เพื่อให้ทุกส่วนมีการเชื่อมโยงกันอย่างเป็นระบบ

การกำหนดวัตถุประสงค์ที่ดี

วัตถุประสงค์ที่ดีควรมีลักษณะดังต่อไปนี้

- **Specific (ชัดเจน)** วัตถุประสงค์ต้องมีความชัดเจนและเฉพาะเจาะจง เพื่อให้ผู้ดำเนินการมีความเข้าใจตรงกันเกี่ยวกับสิ่งที่ต้องทำและเป้าหมายที่ต้องการบรรลุ
- **Measurable (วัดผลได้)** วัตถุประสงค์ควรสามารถวัดผลหรือประเมินผลได้ เพื่อให้ทราบถึงความก้าวหน้าและความสำเร็จของการดำเนินงาน การมีตัวชี้วัดที่ชัดเจนจะช่วยให้สามารถติดตามและประเมินผลการดำเนินงานได้อย่างมีประสิทธิภาพ
- **Achievable (ทำได้จริง)** วัตถุประสงค์ควรเป็นสิ่งที่สามารถทำได้จริงภายใต้ทรัพยากรที่มีอยู่และสภาพแวดล้อมที่เป็นอยู่ เพื่อให้การดำเนินงานมีความเป็นไปได้และไม่เป็นภาระที่เกินความสามารถ
- **Reasonable (สมเหตุสมผล)** วัตถุประสงค์ต้องมีความสมเหตุสมผลและเป็นไปได้ โดยคำนึงถึงทรัพยากร งบประมาณ และเวลาที่จำเป็นต้องใช้
- **Time constrained (มีกรอบเวลา)** วัตถุประสงค์ต้องมีการกำหนดกรอบเวลาที่ชัดเจนและเหมาะสม เพื่อให้การดำเนินงานมีทิศทางที่แน่นอนและสามารถติดตามความก้าวหน้าได้อย่างต่อเนื่อง

การใช้ตัวชี้วัด

หากหน่วยงานได้กำหนดตัวชี้วัด (Key Performance Indicators - KPI) และภารกิจหลักของงานไว้แล้ว ตัวชี้วัดเหล่านั้นสามารถนำมาใช้แทนการกำหนดวัตถุประสงค์ได้ ตัวชี้วัดจะช่วยให้สามารถวัดผลความสำเร็จและประสิทธิภาพของการดำเนินงานได้อย่างชัดเจน ตัวชี้วัดควรสอดคล้องกับวัตถุประสงค์ในแต่ละระดับ เพื่อให้การประเมินผลการดำเนินงานเป็นไปอย่างครบถ้วน

2. การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยงเป็นกระบวนการสำคัญในการบริหารความเสี่ยงขององค์กร เนื่องจากความเสี่ยงที่ไม่ได้ถูกระบุหรือระบุไม่ครบถ้วนจะส่งผลให้องค์กรไม่สามารถเตรียมการรับมือและป้องกันปัญหาที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ การระบุความเสี่ยงจึงเป็นการเริ่มต้นที่สำคัญในการบริหารความเสี่ยงทั้งหมด

โดยจะต้องมีการวิเคราะห์และจัดลำดับความเสี่ยงที่เกี่ยวข้องกับกิจกรรมหรือโครงการในทุกๆ ส่วนขององค์กร ทั้งนี้ การระบุความเสี่ยงจะช่วยให้องค์กรสามารถเตรียมการป้องกันล่วงหน้า รวมถึงวางมาตรการในการลดความเสี่ยงหรือจัดการผลกระทบที่อาจเกิดขึ้นได้

ความหมายของ "ความเสี่ยง" และ "ปัจจัยเสี่ยง"

1) ความเสี่ยง (Risk)

ความเสี่ยง หมายถึง เหตุการณ์หรือการกระทำที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งจะส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร ความเสี่ยงสามารถส่งผลทั้งด้านบวกและด้านลบ แต่โดยส่วนใหญ่แล้วมักเน้นไปที่ผลกระทบด้านลบที่อาจก่อให้เกิดความเสียหาย ความล้มเหลว หรือลดโอกาสในการบรรลุเป้าหมายขององค์กร

ตัวอย่างของความเสี่ยงอาจรวมถึงปัญหาทางการเงิน การละเมิดข้อบังคับ การเปลี่ยนแปลงเทคโนโลยีที่ไม่คาดคิด การบริหารจัดการที่ไม่เหมาะสม หรือการสูญเสียความสามารถในการแข่งขัน การระบุความเสี่ยงที่ครบถ้วนจะทำให้องค์กรสามารถวิเคราะห์และวางแผนจัดการความเสี่ยงได้อย่างเหมาะสม

การบริหารความเสี่ยง คือกระบวนการที่ครอบคลุมการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และการกำหนดแนวทางในการควบคุมเพื่อลดความเสี่ยงที่อาจเกิดขึ้น โดยมีจุดมุ่งหมายเพื่อให้องค์กรสามารถบรรลุเป้าหมายตามที่กำหนดได้อย่างมีประสิทธิภาพ

2) ปัจจัยเสี่ยง (Risk Factors)

ปัจจัยเสี่ยง คือ ต้นเหตุหรือสาเหตุที่นำไปสู่ความเสี่ยง โดยต้องมีการระบุอย่างชัดเจนว่าความเสี่ยงนั้นเกิดจากสาเหตุอะไร เกิดขึ้นที่ไหน เมื่อใด และอย่างไร การระบุสาเหตุของความเสี่ยงที่แท้จริงจะทำให้องค์กรสามารถวิเคราะห์และกำหนดมาตรการในการจัดการความเสี่ยงได้อย่างเหมาะสม การระบุปัจจัยเสี่ยงที่ถูกต้องเป็นขั้นตอนสำคัญที่จะช่วยให้องค์กรสามารถวางแผนและเตรียมการรับมือกับความเสี่ยงในลักษณะต่างๆ ได้ดีขึ้น

ตัวอย่างปัจจัยเสี่ยงที่พบบ่อย

- **บรรยากาศทางจริยธรรม** ปัญหาที่เกิดจากการไม่ปฏิบัติตามหลักจริยธรรมของบุคลากรในองค์กร
- **ความกดดันจากฝ่ายบริหาร** การเร่งรัดหรือความกดดันจากผู้บริหารที่อาจนำไปสู่การตัดสินใจที่ไม่เหมาะสม
- **ความรู้และความสามารถของบุคลากร** บุคลากรขาดทักษะหรือความเชี่ยวชาญที่จำเป็นในการปฏิบัติงาน
- **มูลค่าทรัพย์สิน** ความเสี่ยงที่เกี่ยวข้องกับราคาหรือมูลค่าของทรัพย์สินที่อาจผันผวน
- **ปริมาณงานหรือเอกสาร** ความเสี่ยงที่เกิดจากการจัดการข้อมูลหรือเอกสารในปริมาณมาก ซึ่งอาจนำไปสู่ข้อผิดพลาด

- **การเปลี่ยนแปลงขององค์กร** การเปลี่ยนแปลงโครงสร้างหรือกระบวนการทำงานที่ส่งผลต่อการดำเนินงานปกติ
- **ระบบสารสนเทศ** ความเสี่ยงที่เกิดจากปัญหาทางเทคโนโลยี เช่น ระบบล่ม หรือการโจมตีทางไซเบอร์

3) การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยง เป็นกระบวนการที่บุคลากรในองค์กรร่วมกันวิเคราะห์และระบุปัจจัยเสี่ยงที่เกี่ยวข้องกับกิจกรรม โครงการ หรือการดำเนินงานต่างๆ เพื่อให้สามารถระบุเหตุการณ์ที่อาจเป็นความเสี่ยงและมีผลกระทบต่อการบรรลุเป้าหมายได้อย่างครบถ้วน การระบุความเสี่ยงจำเป็นต้องพิจารณาทั้งปัจจัยภายในและปัจจัยภายนอกที่อาจส่งผลกระทบต่อการดำเนินงาน

ปัจจัยที่ต้องคำนึงถึงในการระบุความเสี่ยง

- **สภาพแวดล้อมภายนอก** ปัจจัยภายนอกที่อยู่นอกเหนือการควบคุมขององค์กร เช่น นโยบายภาครัฐ กฎหมาย เศรษฐกิจ และสภาพการเมือง สิ่งเหล่านี้อาจมีผลกระทบต่อการดำเนินงานขององค์กรโดยตรงหรือทางอ้อม
- **สภาพแวดล้อมภายใน** ปัจจัยที่อยู่ภายใต้การควบคุมขององค์กร เช่น โครงสร้างองค์กร การมอบหมายอำนาจหน้าที่ ความสามารถของบุคลากร ระบบภายใน และการดำเนินงานในระดับหน่วยงาน การปรับปรุงสภาพแวดล้อมภายในให้มีประสิทธิภาพสูงสุดจะช่วยลดความเสี่ยงในการดำเนินงานได้

วิธีการระบุความเสี่ยงที่ใช้บ่อย

1. **การระดมสมอง (Brainstorming)** รวบรวมความคิดเห็นจากบุคลากรหลายฝ่ายเพื่อหาความเสี่ยงที่หลากหลาย
2. **การใช้รายการตรวจสอบ (Checklist)** ใช้รายการตรวจสอบเพื่อระบุความเสี่ยงในกรณีที่มีข้อจำกัดทางด้านงบประมาณหรือทรัพยากร
3. **การตั้งคำถาม “What-If”** การใช้คำถามที่สมมุติเหตุการณ์ที่อาจเกิดขึ้นเพื่อวิเคราะห์สถานการณ์ความเสี่ยง
4. **การวิเคราะห์กระบวนการทำงาน** ตรวจสอบขั้นตอนการทำงานที่สำคัญเพื่อระบุจุดเสี่ยงที่อาจเกิดขึ้นในกระบวนการทำงาน

การระบุความเสี่ยงสามารถทำได้หลายวิธี เช่น

- การวิเคราะห์กระบวนการทำงาน
- การทบทวนผลการดำเนินงานที่ผ่านมา
- การประชุมเชิงปฏิบัติการ (Workshop)

- การเปรียบเทียบกับองค์กรอื่น
- การสัมภาษณ์หรือใช้แบบสอบถาม

4) ประเภทของความเสี่ยง (Types of Risks)

การระบุความเสี่ยงสามารถแบ่งออกได้เป็น 4 ประเภทหลัก ดังนี้

1. ความเสี่ยงเชิงยุทธศาสตร์

ความเสี่ยงที่เกี่ยวข้องกับการดำเนินงานในเชิงยุทธศาสตร์ขององค์กร ซึ่งอาจก่อให้เกิดการเปลี่ยนแปลงหรือการไม่บรรลุเป้าหมายในแต่ละประเด็นยุทธศาสตร์ที่กำหนดไว้ ตัวอย่างเช่น ความเสี่ยงจากการเปลี่ยนแปลงนโยบายภาครัฐที่อาจส่งผลต่อการดำเนินงานขององค์กร

2. ความเสี่ยงด้านธรรมาภิบาล (Governance Risk)

ความเสี่ยงที่เกิดจากการไม่ปฏิบัติตามหลักธรรมาภิบาล ซึ่งอาจส่งผลกระทบต่อความโปร่งใส ความคุ้มค่า และความรับผิดชอบในการดำเนินงาน การบริหารธรรมาภิบาลที่ดีจะช่วยให้การดำเนินงานขององค์กรมีความโปร่งใส ตรวจสอบได้ และมีประสิทธิภาพ

3. ความเสี่ยงด้านเทคโนลยีสารสนเทศ

ความเสี่ยงที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เช่น ปัญหาจากการโจมตีทางไซเบอร์ ข้อมูลสูญหาย หรือระบบล่ม การบริหารความเสี่ยงในด้านนี้ต้องมีมาตรการรักษาความปลอดภัย เช่น การสำรองข้อมูล (Backup) การฟื้นฟูระบบ (Recovery) และการจัดการสิทธิ์ในการเข้าถึงข้อมูล (Access Control)

4. ความเสี่ยงด้านกระบวนการ (Process Risk)

ความเสี่ยงที่เกิดขึ้นจากการดำเนินงานในกระบวนการต่างๆ ขององค์กร เช่น การผลิต การบริการ การควบคุมคุณภาพ กระบวนการเหล่านี้มีความเสี่ยงในการไม่ปฏิบัติตามมาตรฐานหรือเป้าหมายที่กำหนด การบริหารความเสี่ยงด้านกระบวนการอาจรวมถึงการออกแบบระบบควบคุมที่เหมาะสม เพื่อให้การดำเนินงานเป็นไปตามมาตรฐานที่กำหนด

ปัจจัยสำคัญในการบริหารความเสี่ยงด้านกระบวนการ

1. **วัตถุประสงค์ของการควบคุม** การควบคุมกระบวนการต้องมีวัตถุประสงค์ที่ชัดเจนเพื่อป้องกันความเสี่ยง
2. **ความคุ้มค่าของการควบคุม** การลงทุนในมาตรการควบคุมต้องคุ้มค่ากับผลที่ได้
3. **ความทันการณ์ของการติดตาม** ระบบการติดตามต้องรวดเร็วและตอบสนองต่อเหตุการณ์ได้ทันท่วงที
4. **ความสม่ำเสมอของการควบคุม** การควบคุมต้องดำเนินการอย่างต่อเนื่องและมีความน่าเชื่อถือ
5. **การจูงใจผู้ปฏิบัติงาน** การสร้างแรงจูงใจให้บุคลากรปฏิบัติงานอย่างมีประสิทธิภาพ

การระบุความเสี่ยงเป็นขั้นตอนสำคัญที่ช่วยให้องค์กรสามารถวางแผนรับมือและจัดการกับความเสี่ยงได้อย่างรอบคอบ

3. การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยง เป็นการนำปัจจัยเสี่ยงมาวิเคราะห์เพื่อประเมินโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบจากความเสี่ยง และจัดระดับความเสี่ยง โดยหน่วยงานอาจจะเชิญผู้ที่เกี่ยวข้องมาร่วมประชุมปรึกษาหารือร่วมกัน หรือกรณีเป็นเรื่องที่เกี่ยวข้องกับทุกคนและต้องการความคิดเห็นจากบุคคลจำนวนมากอาจจะพิจารณาใช้วิธีการเก็บข้อมูลจากแบบสอบถาม 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 ผู้ประเมินของหน่วยงานควรเป็นผู้ที่มีความรู้ความชำนาญและมีประสบการณ์ในเรื่องนั้นๆ สำหรับวิธีการเลือกตัวเลขระดับโอกาส (5-4-3-2-1) ของแต่ละปัจจัยความเสี่ยงใช้วิธีวิเคราะห์ร่วมกันหากไม่สามารถหาข้อยุติได้ 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

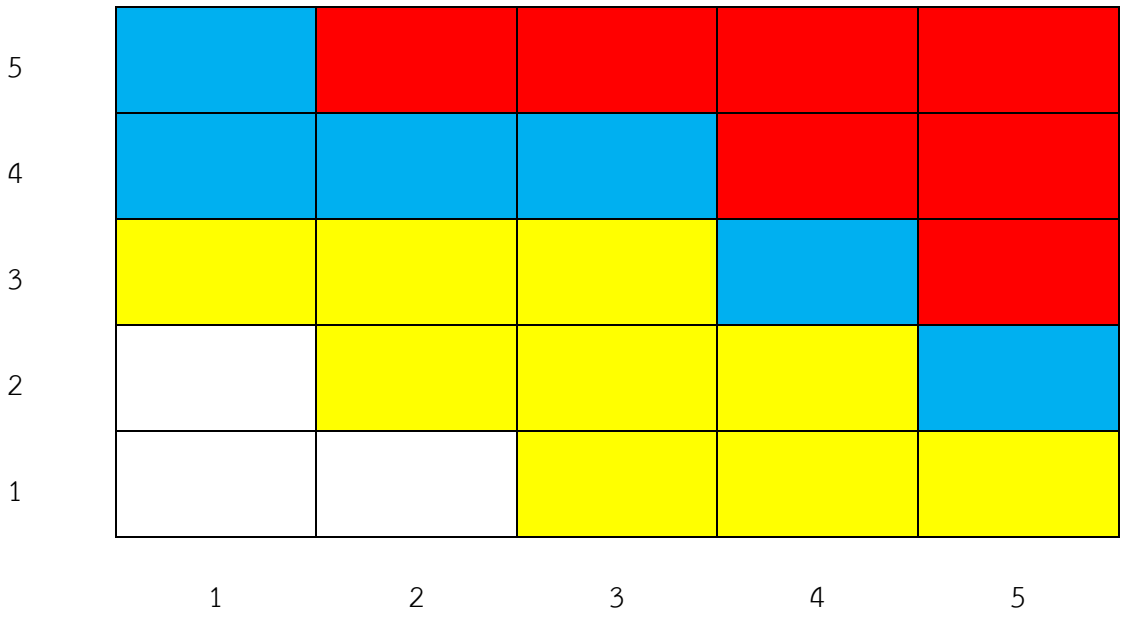
ตัวอย่าง เกณฑ์ระดับความรุนแรงของผลกระทบ (Impact)

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	มีการเผยแพร่ข่าวในวงกว้างภายในประเทศและเผยแพร่ในวงจำกัดของสื่อต่างประเทศ	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%

ระดับคะแนน	รายละเอียด	สูญเสียเงิน	สูญเสียทรัพย์สิน	การทำงานของบุคลากร	ชื่อเสียงและภาพลักษณ์	สูญเสียการปฏิบัติงาน
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)



โอกาสที่จะเกิดความเสี่ยง

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

ระดับความเสี่ยง	แทนด้วยสี	ความหมาย
น้อย	 สีขาว	Acceptable or Limited Focus ระดับที่ยอมรับได้ โดยไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

ระดับความเสี่ยงที่นัยสำคัญที่ผู้บริหารควรให้ความสำคัญมากคือ ความเสี่ยงที่มีระดับสูงมาก และสูงเนื่องจากเป็นความเสี่ยงที่มหาวิทยาลัยไม่สามารถยอมรับได้ เพราะจะทำให้การดำเนินงานตามพันธกิจหลักไม่เป็นไปตามเป้าประสงค์ที่กำหนดไว้ 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) ที่ดำเนินการสามารถลดและควบคุมความเสี่ยงที่เกิดขึ้นได้จริงและอยู่ในระดับที่ยอมรับด้ หรือต้องจัดหามาตรการหรือตัวควบคุมอื่นเพิ่มเติม เพื่อให้ความเสี่ยงที่ยังเหลืออยู่หลังมีการจัดการ (Residual Risk) อยู่ในระดับที่ยอมรับได้ และให้องค์กรมีการบริหารความเสี่ยงอย่างต่อเนื่องจนเป็นวัฒนธรรมในการดำเนินงาน

7. การทบทวนการบริหารความเสี่ยง การทบทวนแผนบริหารความเสี่ยง เป็นการทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงทุกขั้นตอน เพื่อการปรับปรุงและพัฒนาแผนงานในการบริหารความเสี่ยงให้ทันสมัยและเหมาะสมกับการปฏิบัติงานจริงเป็นประจำทุกปี

บทที่ 4
การประเมินและวิเคราะห์ความเสี่ยงและการควบคุมภายใน

คณะกรรมการจัดทำแผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้ดำเนินการตามกระบวนการบริหารความเสี่ยงตั้งแต่การระบุเหตุการณ์/สถานการณ์เสี่ยง การวิเคราะห์ความเสี่ยง และการจัดลำดับความเสี่ยง สรุปได้ดังนี้

ความเสี่ยง	ปัจจัยเสี่ยง	โอกาสที่จะเกิดขึ้น	ผลกระทบความรุนแรง	ระดับคะแนนความเสี่ยง	ระดับความเสี่ยง
1. การจัดการความยินยอม (Consent Management Risk)	- ระบบการเก็บความยินยอมไม่มีความชัดเจนและไม่โปร่งใส	4	5	20	สูง
	- ไม่สามารถพิสูจน์ได้ว่าได้รับความยินยอมจากเจ้าของข้อมูล	4	5	20	สูง
2. การไม่จัดทำ ROPA อย่างครบถ้วน (Incomplete ROPA Documentation Risk)	- การไม่บันทึกกระบวนการประมวลผลข้อมูลทุกขั้นตอน	3	4	12	ปานกลาง
	- ขาดระบบตรวจสอบข้อมูลประมวลผลที่สามารถติดตามได้	3	4	12	ปานกลาง
3. การละเมิดความปลอดภัยของข้อมูล (Data Breach Risk)	- ขาดมาตรการรักษาความปลอดภัยทางข้อมูล เช่น การเข้ารหัสข้อมูล	4	5	20	สูง

ความเสี่ยง	ปัจจัยเสี่ยง	โอกาสที่จะเกิดขึ้น	ผลกระทบความรุนแรง	ระดับคะแนนความเสี่ยง	ระดับความเสี่ยง
	- การใช้ระบบหรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดตเพื่อป้องกันการโจมตีทางไซเบอร์	4	5	20	สูง
4. การไม่อัปเดต ROPA (Outdated ROPA Risk)	- ไม่มีการปรับปรุงข้อมูลการประมวลผลข้อมูลใหม่ใน ROPA อย่างสม่ำเสมอ	3	4	12	ปานกลาง
	- ขาดการรายงานหรือการตรวจสอบข้อมูลที่ไม่เป็นปัจจุบัน	3	4	12	ปานกลาง

การประเมินมาตรการควบคุมความเสี่ยงและการควบคุมภายใน

การประเมินมาตรการควบคุมความเสี่ยง โดยการนำปัจจัยเสี่ยงที่อยู่ในระดับความเสี่ยงสูง และสูงมาก มาประเมินการควบคุมความเสี่ยงและการควบคุมภายใน

ความเสี่ยง	ปัจจัยเสี่ยง	วิธีจัดการความเสี่ยง	การควบคุมที่มีอยู่แล้ว	การควบคุมที่มีอยู่แล้วได้ผลหรือไม่	ระดับความเสี่ยง
1. การจัดการความยินยอม (Consent Management Risk)	1. ระบบการเก็บความยินยอมไม่มีความชัดเจนและไม่โปร่งใส	ควบคุมความเสี่ยง	O	O	สูง (20 คะแนน)
	2. ไม่สามารถพิสูจน์ได้ว่าได้รับความยินยอมจากเจ้าของข้อมูล	ควบคุมความเสี่ยง	O	O	สูง (20 คะแนน)
2. การละเมิดความปลอดภัยของข้อมูล (Data Breach Risk)	1. ขาดมาตรการรักษาความปลอดภัยทางข้อมูล เช่น การเข้ารหัสข้อมูล	ควบคุมความเสี่ยง	O	O	สูง (20 คะแนน)
	2. การใช้ระบบหรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดตเพื่อป้องกันการโจมตีทางไซเบอร์	ควบคุมความเสี่ยง	O	O	สูง (20 คะแนน)

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

แผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ประจำปีงบประมาณ พ.ศ. 2568

คณะกรรมการจัดทำแผนบริหารความเสี่ยง ได้มีการวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อพันธกิจ ตามแผนปฏิบัติราชการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2568 โดยนำพิจารณาระดับความเสี่ยงของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ที่มีค่าคะแนนในระดับสูง และสูงมาก มาบริหารจัดการความเสี่ยง รวมทั้งสิ้นจำนวน 2 ความเสี่ยง และ 4 ปัจจัยเสี่ยง รายละเอียดดังตารางต่อไปนี้

ความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผู้รับผิดชอบ
1. การจัดการความยินยอม (Consent Management Risk)	1. ระบบการเก็บความยินยอมไม่มีความชัดเจนและไม่โปร่งใส	สูง (20 คะแนน)	1. สร้างระบบการเก็บความยินยอมที่ชัดเจนและโปร่งใส	1. ระบบเก็บความยินยอมที่สามารถตรวจสอบย้อนหลังได้	- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ
	2. ไม่สามารถพิสูจน์ได้ว่าได้รับความยินยอมจากเจ้าของข้อมูล	สูง (20 คะแนน)	2. จัดทำการบันทึกและจัดเก็บหลักฐานความยินยอมอย่างครบถ้วน	2. มีเอกสารหรือหลักฐานการยินยอมที่ครบถ้วนและสามารถตรวจสอบได้	- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ

ความเสี่ยง	ปัจจัยเสี่ยง	ระดับความเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผู้รับผิดชอบ
2. การละเมิดความปลอดภัยของข้อมูล (Data Breach Risk)	1. ขาดมาตรการรักษาความปลอดภัยทางข้อมูล เช่น การเข้ารหัสข้อมูล	สูง (20 คะแนน)	1. ใช้ระบบเข้ารหัสข้อมูลและการรักษาความปลอดภัยของข้อมูล	1. ข้อมูลถูกเข้ารหัสและมีมาตรการรักษาความปลอดภัยที่เหมาะสม	- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ
	2. การใช้ระบบหรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดตเพื่อป้องกันการโจมตีทางไซเบอร์	สูง (20 คะแนน)	2. อัปเดตซอฟต์แวร์และระบบรักษาความปลอดภัยอย่างสม่ำเสมอ	2. การอัปเดตซอฟต์แวร์อย่างต่อเนื่องและตรวจสอบประสิทธิภาพ	- รองอธิการบดีดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ

รายงานผลการดำเนินการ

แผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2568

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
1. การจัดการความยินยอม (Consent Management Risk)	1. ระบบการเก็บความยินยอมไม่มีความชัดเจนและไม่โปร่งใส	1. สร้างระบบการเก็บความยินยอมที่ชัดเจนและโปร่งใส	1. ระบบเก็บความยินยอมที่สามารถตรวจสอบย้อนหลังได้	1.1 แต่งตั้งคณะกรรมการเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เพื่อทำหน้าที่ตรวจสอบ ให้คำปรึกษา และกำกับดูแลกระบวนการจัดเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคล ให้เป็นไปตามหลักเกณฑ์ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
				1.2 จัดทำเอกสารแสดง กระบวนการจัดเก็บข้อมูลส่วนบุคคล โดยระบุรายละเอียด เกี่ยวกับรูปแบบของแบบฟอร์มที่ใช้ในการจัดเก็บ ระยะเวลา การเก็บรักษา และแนวทางการจัดการข้อมูลในแต่ละขั้นตอนอย่างชัดเจน

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
		2. พัฒนาและทดสอบเครื่องมือเก็บข้อมูลเพื่อบันทึกการยินยอมอย่างชัดเจน	2. เครื่องมือเก็บข้อมูลถูกนำมาใช้ในองค์กรและมีบันทึกการยินยอมที่ถูกต้องและโปร่งใส	2.1 นำโปรแกรมจัดเก็บและบริหารจัดการข้อมูลส่วนบุคคล (PDPA Management System) มาใช้ในองค์กรเพื่อเพิ่มประสิทธิภาพในการจัดเก็บ บริหารและตรวจสอบข้อมูลส่วนบุคคลให้เป็นระบบ สามารถติดตามและควบคุมการประมวลผลข้อมูลได้อย่างโปร่งใสและตรวจสอบได้
	2. ไม่สามารถพิสูจน์ได้ว่าได้รับความยินยอมจากเจ้าของข้อมูล	1. จัดทำการบันทึกและจัดเก็บหลักฐานความยินยอมอย่างครบถ้วน	1. มีเอกสารหรือหลักฐานการยินยอมที่ครบถ้วนและสามารถตรวจสอบได้	1.1 จัดทำแบบฟอร์มสำหรับการจัดเก็บเอกสารข้อมูลส่วนบุคคล โดยออกแบบให้มีความครบถ้วน ถูกต้อง และสอดคล้องกับวัตถุประสงค์ของการประมวลผลข้อมูลตลอดจนสามารถใช้เป็นหลักฐานแสดงการได้รับความยินยอมและการจัดการข้อมูลได้อย่างโปร่งใสและตรวจสอบได้
				1.2 นำโปรแกรมสำหรับจัดเก็บและบริหารจัดการข้อมูลส่วนบุคคล (PDPA–RoPA Management System) มาใช้ในองค์กรเพื่อรองรับการจัดเก็บกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities) และสนับสนุนการดำเนินงานให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
		2. มีการตรวจสอบความถูกต้องของเอกสารความยินยอมทุกไตรมาส	2. การตรวจสอบรายไตรมาสบ่งชี้ว่าหลักฐานมีความถูกต้องและทันสมัย	2. มีการตรวจสอบความถูกต้องของเอกสารความยินยอมทุกไตรมาส
2. การละเมิดความปลอดภัยของข้อมูล (Data Breach Risk)	1. ขาดมาตรการรักษาความปลอดภัยทางข้อมูล เช่น การเข้ารหัสข้อมูล	1. ใช้ระบบเข้ารหัสข้อมูลและการรักษาความปลอดภัยของข้อมูล	1. ข้อมูลถูกเข้ารหัสและมีมาตรการรักษาความปลอดภัยที่เหมาะสม	1.1 ระบบสารสนเทศที่จัดหาได้รับการพัฒนาตามแนวทางการเขียนโปรแกรมอย่างปลอดภัยของ OWASP (Open Web Application Security Project) เพื่อยกระดับความมั่นคงปลอดภัยของระบบ และลดความเสี่ยงจากช่องโหว่ทางไซเบอร์ที่อาจกระทบต่อข้อมูลส่วนบุคคล
				1.2 ดำเนินการติดตั้งระบบบริหารจัดการเว็บไซต์ (Web Hosting Control Panel) เช่น aaPanel เพื่อใช้ในการบริหารจัดการเว็บไซต์ที่พัฒนาด้วยระบบจัดการเนื้อหา (Content Management System: CMS) โดยระบบดังกล่าวรองรับการอัปเดตแพตช์ (Patch) อย่างต่อเนื่องและอัตโนมัติ เพื่อเสริมความมั่นคงปลอดภัยและลดความเสี่ยงจากช่องโหว่ในระบบ

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
				1.3 ดำเนินการจัดหาซอฟต์แวร์สำหรับการบริหารจัดการบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities Management: RoPA) ซึ่งเป็นองค์ประกอบพื้นฐานที่มีความสำคัญอย่างยิ่งต่อการ ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างถูกต้องและมีประสิทธิภาพ 1.4 จัดหาปรึกษาให้คำแนะนำและแนวทางการใช้งานซอฟต์แวร์ตามกระบวนการบริหารจัดการความมั่นคงปลอดภัยของข้อมูล ตามมาตรฐานสากล ISO/IEC 27001 เพื่อสนับสนุนการบริหารจัดการความเสี่ยงด้านสารสนเทศให้เป็นระบบ และสอดคล้องกับแนวปฏิบัติด้านความปลอดภัยขององค์กร
		2. จัดตั้งทีมเทคโนโลยีสารสนเทศ (IT) เพื่อตรวจสอบและประเมินความปลอดภัยข้อมูลรายไตรมาส	2. รายงานการตรวจสอบความปลอดภัยจากทีมเทคโนโลยีสารสนเทศ (IT) ทุกไตรมาส	2.1 คำสั่งแต่งตั้งคณะทำงานด้านความมั่นคงปลอดภัยทางเทคโนโลยี สารสนเทศ 2.2 รายงานผลการประเมินความเปราะบางของระบบ (Vulnerability Assessment: VA Scan)

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
	2. การใช้ระบบหรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดตเพื่อป้องกันการโจมตีทางไซเบอร์	1. อัปเดตซอฟต์แวร์และระบบรักษาความปลอดภัยอย่างสม่ำเสมอ	1. การอัปเดตซอฟต์แวร์อย่างต่อเนื่องและตรวจสอบประสิทธิภาพ	1.1 ติดตั้งระบบบริหารจัดการเว็บไซต์ (Web Hosting Control Panel) เช่น aaPanel เพื่อใช้ในการบริหารจัดการเว็บไซต์ที่พัฒนาด้วยระบบจัดการ เนื้อหา (Content Management System: CMS) โดย ระบบดังกล่าวรองรับการอัปเดตแพตช์ (Patch) อย่าง ต่อเนื่องและอัตโนมัติ เพื่อเสริมความมั่นคงปลอดภัยและลดความเสี่ยงจากช่องโหว่ในระบบ
		2.ทำการทดสอบความปลอดภัยด้วยการเจาะระบบ (Penetration Testing) ทุกปี	2. รายงานการทดสอบ Penetration Testing ที่แสดงผลลัพธ์ความปลอดภัยที่สูงขึ้น	2.1.2 รายงานผลการทดสอบเจาะระบบ (Penetration Testing Report)

สรุปผลการดำเนินการตามแผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. 2568 โดยมีประเด็นความเสี่ยงทั้งสิ้น 2 ประเด็นความเสี่ยง คือ 1. การจัดการความยินยอม (Consent Management Risk) และ 2. การละเมิดความปลอดภัยของข้อมูล (Data Breach Risk) สามารถสรุปผลการดำเนินกิจกรรมตามแผนบริหารความเสี่ยงและการควบคุมภายในประจำปีงบประมาณ 2568 ดังนี้

1. **การจัดการความยินยอม (Consent Management Risk)**
    - **ปัญหาที่พบ**
        1. ระบบการจัดเก็บความยินยอมไม่มีความชัดเจน โปร่งใส และไม่สามารถพิสูจน์การได้รับความยินยอมจากเจ้าของข้อมูลได้อย่างเป็นรูปธรรม
    - **การดำเนินการ**
        1. จัดทำระบบการเก็บความยินยอมที่สามารถตรวจสอบย้อนหลังได้
        2. พัฒนาและทดสอบเครื่องมือจัดเก็บข้อมูลการยินยอม
        3. จัดทำแบบฟอร์มบันทึกความยินยอม พร้อมจัดเก็บหลักฐานไว้อย่างครบถ้วน
        4. ตรวจสอบความถูกต้องของเอกสารความยินยอมเป็นรายไตรมาส
        5. แต่งตั้งคณะกรรมการ DPO เพื่อให้คำปรึกษาและตรวจสอบกระบวนการจัดเก็บข้อมูล
        6. ใช้โปรแกรมบริหารจัดการข้อมูลส่วนบุคคล (PDPA/RoPA)
    - **ผลการดำเนินการ**
        1. มีการจัดเก็บข้อมูลการยินยอมที่สามารถตรวจสอบย้อนหลังได้
        2. เอกสารความยินยอมมีความครบถ้วน ถูกต้อง และมีการตรวจสอบตามรอบระยะเวลาที่กำหนด
        3. กระบวนการจัดเก็บข้อมูลมีความโปร่งใส และสามารถนำเสนอหลักฐานต่อผู้เกี่ยวข้องได้ทันที
    - **ผลการดำเนินงานโดยสรุป**
        1. การดำเนินการจัดการความยินยอมมีความก้าวหน้าอย่างชัดเจน โดยมีการพัฒนาระบบจัดเก็บที่สามารถตรวจสอบย้อนหลังได้ พร้อมทั้งมีการสนับสนุนจากเครื่องมือดิจิทัลและบุคลากรผู้รับผิดชอบเฉพาะด้าน (DPO) ทำให้กระบวนการจัดเก็บความยินยอมของหน่วยงานเป็นไปอย่างถูกต้องตามหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคล

2. **การละเมิดความปลอดภัยของข้อมูล (Data Breach Risk)**
    - **ปัญหาที่พบ**
        1. ขาดมาตรการด้านความมั่นคงปลอดภัยของข้อมูล เช่น การเข้ารหัส
        2. การใช้ระบบหรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดตเป็นประจำ
        3. ยังไม่มีระบบประเมินและติดตามความเสี่ยงที่เป็นรูปธรรม
    - **การดำเนินการ**
        1. ใช้ระบบสารสนเทศที่พัฒนาตามแนวทางการเขียนโปรแกรมอย่างปลอดภัยของ OWASP
        2. ติดตั้งระบบบริหารจัดการเว็บไซต์ (aaPanel) เพื่อบริหาร CMS และอัปเดต Patch อัตโนมัติ
        3. จัดหาซอฟต์แวร์ RoPA เพื่อรองรับการจัดเก็บกิจกรรมการประมวลผลข้อมูล
        4. ให้คำปรึกษาและดำเนินงานตามแนวทาง ISO/IEC 27001
        5. จัดตั้งทีม IT เพื่อดำเนินการตรวจสอบความปลอดภัยรายไตรมาส
        6. ดำเนินการทดสอบ VA Scan (Vulnerability Assessment) และ Penetration Testing เป็นประจำ
    - **ผลการดำเนินการ**
        1. ระบบมีการอัปเดตและเสริมความมั่นคงปลอดภัยอย่างต่อเนื่อง
        2. รายงานจากการทดสอบ Penetration Testing ระบุว่าระบบมีความปลอดภัยสูงขึ้น
        3. มีแนวทางบริหารจัดการความเสี่ยงที่สอดคล้องกับมาตรฐานสากล
    - **ผลการดำเนินงานโดยสรุป**
        1. หน่วยงานสามารถดำเนินการควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยข้อมูลได้อย่างเป็นระบบ โดยอาศัยเทคโนโลยีที่ทันสมัยและแนวทางตามมาตรฐานสากล ประกอบกับการจัดตั้งคณะทำงานเฉพาะทาง ส่งผลให้การป้องกันและตอบสนองต่อภัยคุกคามทางไซเบอร์มีประสิทธิภาพและสอดคล้องกับพันธกิจขององค์กร

จากการดำเนินการในข้างต้นที่กล่าวมาแล้วนั้น สามารถสรุปผลการดำเนินงานตามแผนบริหารความเสี่ยงและการควบคุมภายใน ประจำปีงบประมาณ 2568 สรุปผลดังแสดงในตารางต่อไปนี้

จากการดำเนินการในข้างต้นที่กล่าวมาแล้วนั้น สามารถสรุปผลการดำเนินงานตามแผนบริหารความเสี่ยงและการควบคุมภายใน ประจำปีงบประมาณ 2568 สรุปผลดังแสดงในตารางต่อไปนี้

ความเสี่ยง	ปัจจัยเสี่ยง	โอกาสที่จะเกิดขึ้น	ผลกระทบความรุนแรง	ระดับคะแนนความเสี่ยง	ระดับความเสี่ยง
1. การจัดการความยินยอม (Consent Management Risk)	- ระบบการเก็บความยินยอมไม่มีความชัดเจนและไม่โปร่งใส	1	5	5	ปานกลาง
	- ไม่สามารถพิสูจน์ได้ว่าได้รับความยินยอมจากเจ้าของข้อมูล	1	5	5	ปานกลาง
2. การละเมิดความปลอดภัยของข้อมูล (Data Breach Risk)	- ขาดมาตรการรักษาความปลอดภัยทางข้อมูล เช่น การเข้ารหัสข้อมูล	1	5	5	ปานกลาง
	- การใช้ระบบหรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดตเพื่อป้องกันการโจมตีทางไซเบอร์	2	5	10	ปานกลาง

บทที่ 5
การติดตามและประเมินผลตามแผนบริหารความเสี่ยงและการควบคุมภายใน

เมื่อมีการนำมาตรการลดความเสี่ยงไปปฏิบัติในแต่ละปัจจัยเสี่ยง องค์กรต้องมีการจัดทำรายงานผลการปฏิบัติงานในแต่ละช่วงเวลา การควบคุม กำกับ และติดตามความก้าวหน้าของงานเป็นสิ่งที่สำคัญ หากพบปัญหาหรืออุปสรรคใด ๆ จะต้องมีการแก้ไข นอกจากนี้ยังต้องมีการประเมินผลสำเร็จของแผนบริหารความเสี่ยงเพื่อเป็นข้อมูลย้อนกลับ (Feedback) สำหรับการทบทวนประสิทธิภาพของแนวทางการบริหารความเสี่ยงในทุกขั้นตอน เพื่อพัฒนาและนำไปสู่การปฏิบัติในปีถัดไป

องค์ประกอบที่สำคัญของกระบวนการควบคุมและประเมินผล

1. **การวัดและประเมินผล**
    - **กระบวนการย่อย 3 ขั้นตอน**
        - **การเก็บรวบรวมข้อมูล**
            - ในขั้นตอนนี้จะมีการรวบรวมข้อมูลที่จำเป็นจากแหล่งต่าง ๆ เช่น รายงานการดำเนินงาน รายงานการตรวจสอบ และข้อเสนอแนะจากผู้ใช้บริการ
            - ข้อมูลจะต้องถูกจัดเก็บในรูปแบบที่เป็นระเบียบ เพื่อให้การเข้าถึงข้อมูลทำได้ง่าย
        - **การวิเคราะห์และประเมินผลข้อมูล**
            - ข้อมูลที่เก็บรวบรวมจะถูกนำมาวิเคราะห์เพื่อดูความสำเร็จในการดำเนินงานตามแผน เช่น การเปรียบเทียบกับเป้าหมายที่ตั้งไว้
            - การวิเคราะห์นี้จะช่วยให้เห็นภาพรวมเกี่ยวกับประสิทธิภาพของมาตรการที่ใช้
        - **การเสนอผลการประเมิน**
            - ผลการวิเคราะห์จะต้องถูกจัดทำเป็นรายงาน โดยมีการแสดงข้อมูลที่สำคัญ เช่น จุดแข็ง จุดอ่อน และข้อเสนอแนะสำหรับการปรับปรุง
            - รายงานจะถูกส่งไปยังผู้บริหารและบุคลากรที่เกี่ยวข้องเพื่อนำไปใช้ในการตัดสินใจและวางแผนในอนาคต
2. **การติดตามระหว่างการปฏิบัติงาน**
    - ในระหว่างการดำเนินการตามแผนบริหารความเสี่ยง จะมีการติดตามจากผู้บริหารที่ได้รับมอบหมายเพื่อให้แน่ใจว่าการดำเนินงานเป็นไปตามแผน

- การติดตามนี้จะรวมถึงการจัดประชุมเพื่อตรวจสอบสถานะการดำเนินงาน และมีการสื่อสารระหว่างทีมงานเพื่อให้สามารถแก้ไขปัญหาที่เกิดขึ้นได้ทันท่วงที

3. **การติดตามเป็นรายครั้ง**
    - คณะกรรมการบริหารความเสี่ยงจะจัดทำแผนการติดตามเพื่อให้แน่ใจว่ามีการตรวจสอบและประเมินผลอย่างต่อเนื่อง โดยจะมีการจัดทำรายงานผลการติดตามในช่วงเวลา 9 เดือน และ 12 เดือน
    - **ตัวอย่างการติดตาม**
        - **ครั้งที่ 1** ติดตามและรายงานผลระหว่างเดือน มิถุนายน – กรกฎาคม 2568
        - **ครั้งที่ 2** ติดตามและรายงานผลระหว่างเดือน สิงหาคม – กันยายน 2568
    - การติดตามจะรวมถึงการประเมินสถานะของมาตรการที่นำมาใช้ และให้ข้อเสนอแนะแก่ผู้บริหารเกี่ยวกับการปรับปรุงที่จำเป็น

สรุป

กระบวนการควบคุมและประเมินผลตามแผนบริหารความเสี่ยงมีความสำคัญอย่างยิ่งในการสร้างความมั่นใจว่า มาตรการที่นำมาใช้จะมีประสิทธิภาพในการลดความเสี่ยง การติดตามและประเมินผลช่วยให้องค์กรสามารถปรับปรุงกระบวนการได้ตามความจำเป็น ข้อมูลที่ได้รับจากการประเมินผลยังสามารถนำไปใช้ในการวางแผนและพัฒนากลยุทธ์การบริหารความเสี่ยงในปีถัดไปได้อย่างมีประสิทธิภาพ