

บทที่ 1

บทนำ

1. หลักการและเหตุผล

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

ในกระบวนการดำเนินงานของทุกองค์กร ล้วนมีปัจจัยเสี่ยงที่อาจส่งผลกระทบต่อเป้าหมายหรือการดำเนินงานขององค์กร ความเสี่ยงเหล่านี้เกิดจากความไม่แน่นอนในหลายมิติ จึงจำเป็นต้องมีการจัดการความเสี่ยงอย่างเป็นระบบและมีประสิทธิภาพ โดยเริ่มจากการระบุปัจจัยเสี่ยงที่มีผลกระทบต่อการดำเนินงาน จากนั้นจึงวิเคราะห์โอกาสและผลกระทบที่อาจเกิดขึ้น พร้อมจัดลำดับความสำคัญของปัจจัยเสี่ยงเหล่านั้น เมื่อทราบถึงปัจจัยเสี่ยงที่มีความสำคัญแล้วจึงต้องกำหนดแนวทางในการจัดการอย่างเหมาะสม โดยคำนึงถึงคุณค่าและประสิทธิภาพในการดำเนินการเพื่อลดความเสี่ยงให้เหลืออยู่ในระดับที่องค์กรสามารถยอมรับได้

2. วัตถุประสงค์

วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกาญจนบุรี เพื่อวัตถุประสงค์ต่อไปนี้

1. เพื่อให้ผู้บริหารและบุคลากรทุกระดับมีความรู้และความเข้าใจในกระบวนการและขั้นตอนของการบริหารความเสี่ยงและการควบคุมภายในอย่างถูกต้อง โดยสามารถนำความรู้ที่ได้ไปประยุกต์ใช้ในการทำงานได้อย่างมีประสิทธิภาพและสามารถรับมือกับความเสี่ยงที่อาจเกิดขึ้นได้อย่างเหมาะสม

2. เพื่อให้แผนการบริหารความเสี่ยงเป็นเครื่องมือที่ช่วยบุคลากรในการปฏิบัติงานได้อย่างเป็นระบบ สอดคล้องกับเป้าหมาย 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 ในกรณีของ ศูนย์เทคโนโลยีสารสนเทศ 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 (สต.) 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 เพื่อให้การ

ดำเนินงานเป็นไปตามเป้าหมายที่กำหนดและสนับสนุนการพัฒนามหาวิทยาลัยและชุมชนอย่างยั่งยืน
 ดังนั้น สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงนำหลักการบริหารความเสี่ยงมาดำเนินการ
 เพื่อให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศ สามารถบรรลุผลสำเร็จตามวัตถุประสงค์

4. ความหมายและคำจำกัดความของการบริหารความเสี่ยง

เพื่อให้เข้าใจความหมายและคำจำกัดความของการบริหารความเสี่ยงในบริบทของมหาวิทยาลัยราชภัฏกาญจนบุรี จำเป็นต้องทำความเข้าใจกับคำที่เกี่ยวข้องดังต่อไปนี้อย่างละเอียด

ความเสี่ยง (Risk)

ความเสี่ยงในบริบทของมหาวิทยาลัยราชภัฏกาญจนบุรีหมายถึง เหตุการณ์หรือสถานการณ์ที่มีความไม่แน่นอน ซึ่งอาจเกิดขึ้นในอนาคตและส่งผลกระทบต่อทั้งทางบวกและทางลบ หากเป็นความเสี่ยงทางลบ อาจทำให้เกิดความผิดพลาด ความเสียหาย หรือปัญหาอื่น ๆ ที่ขัดขวางการดำเนินงานของมหาวิทยาลัยและส่งผลให้ไม่สามารถบรรลุวัตถุประสงค์ที่ตั้งไว้ได้ 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 ความเสี่ยงนี้อาจส่งผลกระทบต่อทิศทางการพัฒนาของมหาวิทยาลัย ทำให้ไม่สามารถบรรลุวัตถุประสงค์ที่ตั้งไว้ได้ เช่น ความสำเร็จทางการศึกษา การบริการชุมชน หรือการยกระดับคุณภาพการศึกษาให้สอดคล้องกับมาตรฐานที่กำหนด

ความเสี่ยงด้านการปฏิบัติตามกฎหมาย/กฎระเบียบ/ข้อบังคับ (Compliance Risk)

มหาวิทยาลัยราชภัฏกาญจนบุรีจำเป็นต้องปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้อง การไม่สามารถปฏิบัติตามกฎระเบียบหรือการไม่สามารถปรับตัวให้ทันกับการเปลี่ยนแปลงของกฎหมาย อาจก่อให้เกิดปัญหาทางกฎหมายหรือส่งผลกระทบต่อการดำเนินงาน เช่น การไม่ปฏิบัติตามระเบียบการศึกษา

หรือการบริหารงานที่ไม่สอดคล้องกับข้อบังคับของกระทรวงการอุดมศึกษา 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 หรือการเปลี่ยนแปลงนโยบายภาครัฐที่กระทบต่อภาระเปิยของมหาวิทยาลัย 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 หรือแนวทางที่ชัดเจนในการลดความเสี่ยง ให้สอดคล้องกับสถานการณ์และบริบทเฉพาะขององค์กร การจัดการที่เหมาะสมนี้จะช่วยให้องค์กรสามารถลดความเสี่ยงได้อย่างมีประสิทธิภาพและเพิ่มโอกาสในการบรรลุเป้าหมายที่ตั้งไว้

ปัจจัยภายใน ประกอบด้วย

กลยุทธ์ (Strategy)

หมายถึง ความเหมาะสมของกลยุทธ์ในการตอบสนองต่อสถานการณ์ต่าง ๆ กลยุทธ์ที่มีประสิทธิภาพ จะช่วยให้องค์กรสามารถดำเนินการตามวัตถุประสงค์ได้ หากกลยุทธ์ไม่สอดคล้องกับสถานการณ์หรือการเปลี่ยนแปลงภายนอก อาจส่งผลให้การดำเนินงานประสบปัญหาและไม่บรรลุเป้าหมายที่ตั้งไว้

โครงสร้างองค์กร (Structure)

โครงสร้างองค์กรหมายถึงการจัดลำดับชั้นบังคับบัญชา การแบ่งหน้าที่ ความรับผิดชอบภายในหน่วยงาน การมีโครงสร้างที่เหมาะสมจะช่วยให้องค์กรดำเนินงานได้อย่างมีประสิทธิภาพ สามารถปรับตัวได้ตามพันธกิจ และบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพ

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 หรือภัยธรรมชาติล้วนส่งผลกระทบต่อการทำงานขององค์กร หากมีความไม่มั่นคงในสังคมหรือสภาพแวดล้อม เช่น ภัยธรรมชาติ องค์กรอาจต้องเผชิญกับความยากลำบากในการดำเนินธุรกิจ

ด้านการเมือง

การเปลี่ยนแปลงทางการเมืองส่งผลกระทบต่อความต่อเนื่องของนโยบายรัฐบาล หากนโยบายเปลี่ยนแปลงไปตามความไม่แน่นอนทางการเมือง องค์กรอาจต้องปรับเปลี่ยนกลยุทธ์หรือนโยบายการดำเนินงานให้สอดคล้องกับนโยบายใหม่

ด้านกฎหมาย

กฎหมายที่คลุมเครือหรือเปลี่ยนแปลงบ่อยครั้งเป็นความเสี่ยงต่อองค์กร เช่น กฎระเบียบที่ล่าช้าหรือไม่ทันกับการเปลี่ยนแปลง 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 ทั้งนี้ยังผลกระทบรุนแรง 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 มีแนวทางการจัดการความเสี่ยงดังนี้

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 หากการ

วิเคราะห์พบว่าต้นทุนในการจัดการความเสี่ยงสูงกว่าผลประโยชน์ที่ได้รับ องค์กรอาจเลือกที่จะยอมรับความเสี่ยง แต่ต้องติดตามความเสี่ยงนั้นอย่างใกล้ชิดและเตรียมมาตรการรองรับหากเกิดเหตุการณ์ขึ้น

4. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)

การหลีกเลี่ยงความเสี่ยงหมายถึงการหลีกเลี่ยงกิจกรรมหรือโครงการที่อาจนำไปสู่เหตุการณ์ความเสี่ยง โดยองค์กรอาจเลือกที่จะหยุด ยกเลิก หรือเปลี่ยนแปลงกิจกรรมเพื่อป้องกันไม่ให้เกิดความเสี่ยง การหลีกเลี่ยงเป็นวิธีการที่ใช้เมื่อต้องการลดความเสี่ยงอย่างเด็ดขาด แต่ควรคำนึงถึงความเป็นไปได้ในการดำเนินการในระยะยาว

กรณีที่มีความเสี่ยงเกิดจากปัจจัยภายใน ซึ่งอยู่ภายใต้การควบคุมของฝ่ายบริหาร การจัดการความเสี่ยงสามารถทำได้โดยการวางแผนการควบคุมที่เพียงพอ เช่น การเพิ่มประสิทธิภาพของการปฏิบัติตามกฎหมายระเบียบ และข้อบังคับ เพื่อลดโอกาสเกิดความเสียหายในด้านต่าง 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 รวมถึงการประเมินประสิทธิภาพของระบบควบคุมภายในและการบริหารความเสี่ยงที่กำหนดไว้อย่างต่อเนื่องและสม่ำเสมอ การติดตามประเมินผลนี้มีวัตถุประสงค์เพื่อให้มั่นใจว่าระบบควบคุมภายในและการบริหารความเสี่ยงมีความเพียงพอและเหมาะสม สามารถปฏิบัติได้จริง และปัญหาหรือข้อบกพร่องที่พบได้รับการแก้ไขอย่างถูกต้องและทันเวลาเพื่อป้องกันไม่ให้เกิดผลกระทบต่อการดำเนินงานขององค์กร

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

แผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏวชิรญาณบุรี ประจำปีงบประมาณ พ.ศ 2568

7.1 เป้าประสงค์เชิงแก้ปัญหา (Problematic Goal) หมายถึง เป้าหมายที่มุ่งเน้นการแก้ไขปัญหาที่องค์กรกำลังเผชิญ เช่น การปรับปรุงประสิทธิภาพ การลดต้นทุน หรือการแก้ไขปัญหาที่ส่งผลกระทบต่อการทำงาน

7.2 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

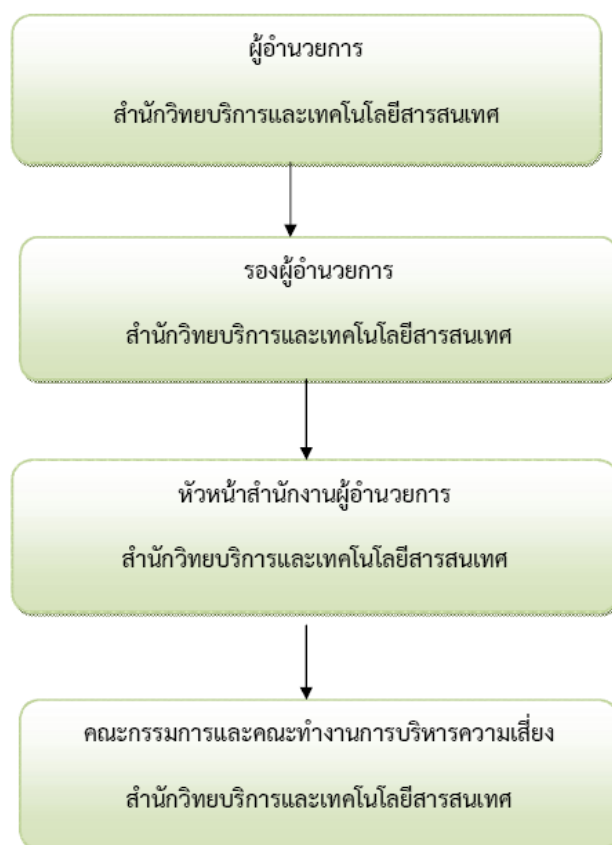
แผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏวชิรญาณบุรี ประจำปีงบประมาณ พ.ศ 2568

2. เพื่อให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศสามารถลดขนาดของความเสียหายที่จะเกิดขึ้นในอนาคตให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยทำให้สามารถควบคุมและตรวจสอบได้อย่างมีประสิทธิภาพ

2. โครงสร้างการบริหารความเสี่ยง

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีโครงสร้างการบริหารความเสี่ยง



3. บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการและคณะทำงานบริหารความเสี่ยง

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ กำหนดให้การบริหารความเสี่ยงเป็นความรับผิดชอบร่วมกันของผู้บริหารและบุคลากรทุกระดับ เพื่อให้กระบวนการบริหารความเสี่ยงดำเนินไปอย่างเป็นระบบและต่อเนื่อง บทบาทหน้าที่และความรับผิดชอบหลักของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีดังนี้

แผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏวชิรญาณบุรี ประจำปีงบประมาณ พ.ศ 2568

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. ระบุและรายงานความเสี่ยงที่ตรวจพบในงานที่รับผิดชอบต่อผู้บังคับบัญชา เพื่อให้มีการจัดการที่เหมาะสม
	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 ซึ่งประกอบด้วย การวิเคราะห์ความเสี่ยงในแง่ของโอกาสที่จะเกิดขึ้น (Likelihood) และความรุนแรงของผลกระทบที่จะตามมา (Impact) การประเมินนี้ต้องอิงตามเกณฑ์มาตรฐานที่กำหนดไว้ เพื่อให้สามารถจัดลำดับความสำคัญของความเสี่ยงได้อย่างมีประสิทธิภาพ ความเสี่ยงที่มีโอกาสเกิดขึ้นสูงและมีผลกระทบรุนแรงจะต้องได้รับการจัดการก่อน ขณะที่ความเสี่ยงที่มีโอกาสเกิดขึ้นต่ำและผลกระทบน้อยอาจได้รับการจัดการในลำดับ

แผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏวชิรสุพรรณบุรี ประจำปีงบประมาณ พ.ศ 2568

ถัดไป การประเมินความเสี่ยงอย่างถูกต้องจะช่วยให้การตัดสินใจจัดการความเสี่ยงเป็นไปอย่างเหมาะสม

4. การจัดทำแผนบริหารความเสี่ยง

หลังจากประเมินความเสี่ยงแล้ว ขั้นตอนต่อไปคือการจัดทำแผนบริหารความเสี่ยง ซึ่งเป็นการกำหนดมาตรการหรือแผนปฏิบัติการที่ชัดเจนในการจัดการกับความเสี่ยงที่ได้รับการระบุอยู่ในระดับสูงหรือสูงมาก แผนนี้ต้องออกแบบมาเพื่อควบคุมและลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ การจัดทำแผนบริหารความเสี่ยงต้องคำนึงถึงคุณค่าในด้านค่าใช้จ่ายและต้นทุนที่ใช้ในการดำเนินการ เช่น การฝึกอบรมบุคลากร การปรับปรุงระบบงาน หรือการติดตั้งเทคโนโลยีที่สามารถช่วยลดความเสี่ยง นอกจากนี้ การตัดสินใจเลือกวิธีการจัดการความเสี่ยงควรพิจารณาประโยชน์ที่จะได้รับการดำเนินการตามมาตรการเหล่านั้นด้วย

5. การรายงานและติดตามผล

ขั้นตอนนี้เป็นการรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงต่อฝ่ายบริหาร เพื่อให้รับทราบถึงความก้าวหน้าและปัญหาที่เกิดขึ้นในการบริหารความเสี่ยง นอกจากนี้ การติดตามผลจะช่วยให้มั่นใจว่าแผนการบริหารความเสี่ยงที่ได้กำหนดไว้กำลังถูกดำเนินการอย่างมีประสิทธิภาพ การติดตามต้องเป็นไปอย่างต่อเนื่อง เพื่อให้สามารถปรับปรุงและแก้ไขปัญหาที่เกิดขึ้นได้ทันเวลา การรายงานต้องครอบคลุมข้อมูลเกี่ยวกับความเสี่ยงที่ยังคงอยู่ ผลของการจัดการความเสี่ยง และข้อเสนอแนะสำหรับการปรับปรุงแผนการบริหารความเสี่ยงในอนาคต

6. การประเมินผลบริหารความเสี่ยง

เป็นการประเมินผลการดำเนินการบริหารความเสี่ยงทั้งหมดในแต่ละปี เพื่อให้มั่นใจว่าองค์กรมีการจัดการความเสี่ยงอย่างเหมาะสม เพียงพอ และมีประสิทธิผล คณะทำงานวิเคราะห์และจัดทำแผนบริหารความเสี่ยงของมหาวิทยาลัยจะทำหน้าที่ประเมินมาตรการและกลไกควบคุมความเสี่ยงที่มีอยู่เพื่อตรวจสอบว่ามาตรการเหล่านั้นสามารถลดและควบคุมความเสี่ยงได้จริงหรือไม่ หากพบว่าความเสี่ยงยังคงอยู่ในระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องหามาตรการเพิ่มเติมเพื่อปรับปรุงการควบคุมความเสี่ยง

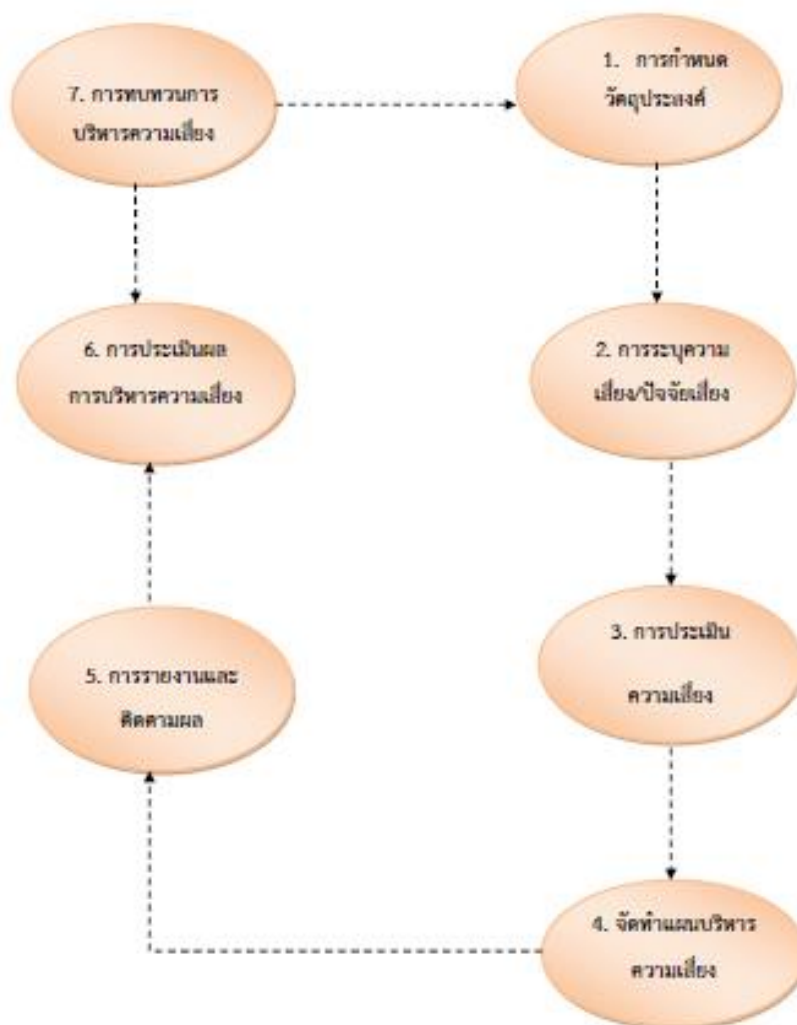
7. การทบทวนการบริหารความเสี่ยง

ขั้นตอนสุดท้ายคือการทบทวนกระบวนการบริหารความเสี่ยงในทุกขั้นตอน เพื่อปรับปรุงและพัฒนาระบบให้ดียิ่งขึ้น การทบทวนนี้เป็นการตรวจสอบว่ามาตรการที่นำมาใช้นั้นมีประสิทธิภาพในการลดความเสี่ยงและป้องกันปัญหาได้จริงหรือไม่ รวมถึงการตรวจสอบว่ากระบวนการบริหารความเสี่ยงนั้นยังคงสอดคล้องกับการเปลี่ยนแปลงของสภาพแวดล้อมทั้งภายในและภายนอกองค์กรหรือไม่ การทบทวนนี้จะช่วยให้การบริหารความเสี่ยงมีความยั่งยืนและตอบสนองต่อการเปลี่ยนแปลงได้ดียิ่งขึ้น

แผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏวชิรญาณบุรี ประจำปีงบประมาณ พ.ศ 2568

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 เป้าหมายเหล่านี้ควรสอดคล้องกับพันธกิจที่กำหนดไว้ และเชื่อมโยงกับทิศทางการดำเนินงานในทุกระดับ

3. กำหนดกิจกรรมที่สนับสนุนวัตถุประสงค์ขององค์กร

เพื่อให้วัตถุประสงค์ในระดับองค์กรสามารถบรรลุได้อย่างมีประสิทธิภาพ จำเป็นต้องกำหนดกิจกรรมหรือโครงการที่ชัดเจนและสอดคล้องกับวัตถุประสงค์เหล่านั้น กิจกรรมที่ถูกกำหนดขึ้นจะต้องสามารถสนับสนุนการบรรลุวัตถุประสงค์ในระดับองค์กร และช่วยสร้างความชัดเจนในกระบวนการทำงาน

4. กำหนดวัตถุประสงค์ในระดับกิจกรรม

เมื่อมีกิจกรรมที่ชัดเจนแล้ว จะต้องกำหนดวัตถุประสงค์เฉพาะสำหรับแต่ละกิจกรรม วัตถุประสงค์ในระดับกิจกรรมนี้จะต้องสอดคล้องและสนับสนุนวัตถุประสงค์ในระดับองค์กร การกำหนดวัตถุประสงค์ในระดับกิจกรรมช่วยให้การดำเนินงานในแต่ละส่วนชัดเจนและสามารถระบุความเสี่ยงที่อาจเกิดขึ้นได้อย่างครบถ้วน

ประเภทของวัตถุประสงค์

วัตถุประสงค์ของการบริหารความเสี่ยงสามารถแบ่งออกได้เป็น 2 ระดับ คือ

1. วัตถุประสงค์ในระดับองค์กร

วัตถุประสงค์ในระดับองค์กรเป็นวัตถุประสงค์หลักของการดำเนินงานที่ครอบคลุมภาพรวมของทั้งองค์กร ซึ่งสอดคล้องกับแผนปฏิบัติราชการประจำปีและแผนปฏิบัติราชการ 4 ปี วัตถุประสงค์นี้มีความสำคัญในการกำหนดทิศทางและเป้าหมายที่องค์กรต้องการบรรลุในระยะยาว วัตถุประสงค์

เหล่านี้มักเกี่ยวข้องกับการดำเนินงานในภาพรวม เช่น การพัฒนาองค์กร การเพิ่มประสิทธิภาพการดำเนินงาน และการสร้างความยั่งยืนในเชิงกลยุทธ์

2. วัตถุประสงค์ในระดับกิจกรรม

วัตถุประสงค์ในระดับกิจกรรมเป็นวัตถุประสงค์ที่มีความเฉพาะเจาะจงมากขึ้น เพื่อสนับสนุนการบรรลุวัตถุประสงค์ในระดับองค์กร วัตถุประสงค์ในระดับกิจกรรมจะถูกกำหนดขึ้นสำหรับแต่ละกิจกรรมหรือโครงการที่องค์กรดำเนินการ การกำหนดวัตถุประสงค์ในระดับกิจกรรมจะช่วยให้สามารถระบุความเสี่ยงและปัจจัยที่จะมีผลต่อความสำเร็จของกิจกรรมได้อย่างชัดเจน วัตถุประสงค์ในระดับกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กรเพื่อให้ทุกส่วนมีการเชื่อมโยงกันอย่างเป็นระบบ

การกำหนดวัตถุประสงค์ที่ดี

วัตถุประสงค์ที่ดีควรมีลักษณะดังต่อไปนี้

- **Specific (ชัดเจน)** วัตถุประสงค์ต้องมีความชัดเจนและเฉพาะเจาะจง เพื่อให้ผู้ดำเนินการมีความเข้าใจตรงกันเกี่ยวกับสิ่งที่ต้องทำและเป้าหมายที่ต้องการบรรลุ
- **Measurable (วัดผลได้)** วัตถุประสงค์ควรสามารถวัดผลหรือประเมินผลได้ เพื่อให้ทราบถึงความก้าวหน้าและความสำเร็จของการดำเนินงาน การมีตัวชี้วัดที่ชัดเจนจะช่วยให้สามารถติดตามและประเมินผลการดำเนินงานได้อย่างมีประสิทธิภาพ
- **Achievable (ทำได้จริง)** วัตถุประสงค์ควรเป็นสิ่งที่สามารถทำได้จริงภายใต้ทรัพยากรที่มีอยู่และสภาพแวดล้อมที่เป็นอยู่ เพื่อให้การดำเนินงานมีความเป็นไปได้และไม่เป็นภาระที่เกินความสามารถ
- **Reasonable (สมเหตุสมผล)** วัตถุประสงค์ต้องมีความสมเหตุสมผลและเป็นไปได้ โดยคำนึงถึงทรัพยากร งบประมาณ และเวลาที่ต้องใช้
- **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** ความเสี่ยงที่เกิดจากการจัดการข้อมูลหรือเอกสารในปริมาณมากซึ่งอาจนำไปสู่ข้อผิดพลาด
- **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. ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

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** ระบบการติดตามต้องรวดเร็วและตอบสนองต่อเหตุการณ์ได้ทัน่วงที
4. **ความสม่ำเสมอของการควบคุม** การควบคุมต้องดำเนินการอย่างต่อเนื่องและมีความน่าเชื่อถือ
5. **การจูงใจผู้ปฏิบัติงาน** การสร้างแรงจูงใจให้บุคลากรปฏิบัติงานอย่างมีประสิทธิภาพ

การระบุความเสี่ยงเป็นขั้นตอนสำคัญที่ช่วยให้องค์กรสามารถวางแผนรับมือและจัดการกับความเสี่ยงได้อย่างรอบคอบ

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

3.1 การกำหนดเกณฑ์การประเมินมาตรฐาน

การประเมินโอกาสที่จะเกิดความเสี่ยง และระดับความรุนแรงของผลกระทบจากความเสี่ยง สามารถกำหนดเกณฑ์ได้ทั้งเกณฑ์ในเชิงปริมาณ และเชิงคุณภาพ ทั้งนี้ขึ้นอยู่กับข้อมูล สภาพแวดล้อมของ

หน่วยงานและดุลยพินิจการตัดสินใจของคณะกรรมการ 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	โอกาสที่จะเกิด ความเสี่ยง (Likelihood)	รายละเอียด (Description)
5	สูงมาก	เกิดขึ้นได้จากสภาพแวดล้อมปกติ (1 เดือนต่อ 1 ครั้ง หรือ เกิดขึ้นทุกเดือน 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 ปี ต่อ 1 ครั้ง)

3.1.2 ระดับความรุนแรงของผลกระทบ (Impact)

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

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

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/บรรยายภาศการปฏิบัติงานไม่เหมาะสม	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 ระดับของความเสี่ง (Risk Matrix) กำหนดเกณฑ์ไว้ 4 ระดับ ได้แก่ สูงมาก สูง ปานกลาง และน้อย

เกณฑ์มาตรฐานระดับของความเสี่ง (Degree of Risk Matrix)

5					
4					
3					
2					
1					
	1	2	3	4	5

โอกาสที่จะเกิดความเสี่ยง

โดย ระดับความเสี่งจำแนกตามสีใน Risk Assessment เป็น 4 ระดับดังนี้

ระดับความเสี่ง

สูงมาก	สูง	ปานกลาง	ต่ำ
--------	-----	---------	-----

3.2 การประเมินโอกาสและผลกระทบของความเสี่ง

เป็นการนำความเสี่ยงและปัจจัยแต่ละปัจจัยที่ระบุมาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงต่างๆ และประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงโดยใส่ลงในแผนภูมิความเสี่ยงเพื่อให้เห็นถึงระดับความเสี่ง และผลกระทบที่แตกต่างกัน ทำให้สามารถกำหนดมาตรการควบคุมความเสี่งได้อย่างเหมาะสม ซึ่งจะช่วยให้หน่วยงานสามารถวางแผนและจัดสรรทรัพยากรได้อย่างถูกต้องภายในงบประมาณ กำลังคน หรือเวลาที่จำกัดโดยอาศัยเกณฑ์มาตรฐานที่กำหนดไว้ในข้อ 3.1.3

แผนบริหารความเสี่ยงและการควบคุมภายใน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏวชิรญาณบุรี ประจำปีงบประมาณ พ.ศ 2568

คณะกรรมการประเมินของหน่วยงานควรเป็นผู้มีความรู้ความชำนาญและมีประสบการณ์ในเรื่องนั้นๆ สำหรับวิธีการให้คะแนนระดับการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยงนั้น ใช้การมีส่วนร่วมหากไม่สามารถหาข้อยุติได้ อาจใช้เสียงข้างมากในที่ประชุม หรือให้แต่ละคนเป็นผู้ให้คะแนนแล้วนำคะแนนนั้นมาหาค่าเฉลี่ย เป็นต้น ทั้งนี้ขั้นตอนการดำเนินการ ดังนี้

1. ร่วมกันวิเคราะห์โอกาส/ความถี่ในการเกิดเหตุการณ์ต่างๆ ว่ามีโอกาส/ความถี่ที่จะเกิดขึ้นมากน้อยเพียงใด และเมื่อได้รับโอกาสแล้วให้นำไปใส่ในแผนบริหารความเสี่ยง
2. ร่วมกันวิเคราะห์ความรุนแรงของผลกระทบของความถี่ ที่มีผลต่อมหาวิทยาลัย/หน่วยงานว่ามีระดับความรุนแรงหรือระดับความเสียหายเพียงใด และเมื่อได้รับผลกระทบแล้วให้นำมาใส่ในแผนบริหารความเสี่ยง

3.3 การวิเคราะห์ระดับของความถี่ (Degree of Risk)

เป็นการพิจารณาความสัมพันธ์ของความถี่กับโอกาสที่จะเกิดความเสี่ยง และระดับความรุนแรงของผลกระทบตามเกณฑ์ความสามารถในการยอมรับความเสี่ยง ดังต่อไปนี้

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

ระดับความเสี่ยงที่น้อยสำคัญที่ผู้บริหารควรให้ความสำคัญมากคือ ความเสี่ยงที่มีระดับสูงมาก และสูงเนื่องจากเป็นความเสี่ยงที่มหาวิทยาลัยไม่สามารถยอมรับได้ เพราะจะทำให้การดำเนินงานตามพันธกิจหลักไม่เป็นไป

ตามเป้าประสงค์ที่กำหนดไว้ และส่งผลกระทบต่อชื่อเสียงของมหาวิทยาลัย ระดับความเสี่ยงปานกลางแม้ว่าจะเป็นความเสี่ยงที่พอยอมรับได้ แต่ก็ต้องมีการควบคุมเพื่อไม่ให้เกิดความเสี่ยงมากขึ้นส่วนความเสี่ยงระดับน้อยผู้บริหารไม่จำเป็นต้องเอาใจใส่มากนัก 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/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยงหรือที่มีอยู่แต่ยังไม่เพียงพอและนำมาวางแผนจัดการความเสี่ยง

โดยในการวางแผนการจัดการความเสี่ยงต้องมีเป้าหมาย คือ

- 1) ลดโอกาสที่จะเกิดความเสี่ยงนั้น
- 2) ลดความรุนแรงของผลกระทบจากความเสี่ยงนั้น ในกรณีที่ความเสี่ยงนั้นเกิดขึ้น
- 3) เปลี่ยนลักษณะของผลลัพธ์ที่จะเกิดขึ้นของความเสี่ยงให้เป็นในรูปที่องค์กรหรือหน่วยงานต้องการหรือยอมรับได้

ทางเลือกในการจัดการความเสี่ยง แนวทางการจัดการความเสี่ยงมีหลายวิธี และสามารถปรับเปลี่ยนให้เหมาะสมกับสถานการณ์ ขึ้นอยู่กับดุลยพินิจของผู้รับผิดชอบ แต่อย่างไรก็ตามแนวทางการบริหารจัดการความเสี่ยงต้องค้ำค้ำกับการลดระดับผลกระทบความเสี่ยง

ทางเลือกหรือกลยุทธ์ในการจัดการความเสี่ยงแบ่งได้ 4 แนวทางหลักคือ

- 1) การยอมรับ (Take, Accept) หมายถึง การที่ความเสี่ยงนั้นสามารถยอมรับได้ภายใต้การควบคุมที่มีอยู่ในปัจจุบัน ซึ่งไม่ต้องดำเนินการใดๆ เช่น กรณีที่มีความเสี่ยงในระดับไม่รุนแรงและไม่ค้ำค้ำที่จะดำเนินการใดๆ 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 วิธีการบริหารการจัดการความเสี่ยงใดมีประสิทธิภาพดีให้ดำเนินการต่อไป 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. การติดตามผลในระหว่างการทำงาน (Ongoing Monitoring) เป็นการติดตามผลที่รวมอยู่ในการดำเนินงานต่างๆ ตามปกติของหน่วยงาน

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

ควบคุมความเสี่ยงที่เกิดขึ้นได้จริงและอยู่ในระดับที่ยอมรับได้ 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	วิธีการจัดการความเสี่ยง	การควบคุมที่มีอยู่แล้ว	การควบคุมที่มีอยู่แล้วได้ผลหรือไม่	ระดับความเสี่ยง
1. การจัดการความยินยอม (Consent Management Risk)	1. ระบบการเก็บความยินยอมไม่มีความชัดเจนและไม่โปร่งใส	ควบคุมความเสี่ยง	○	○	สูง (20 คะแนน)
	2. ไม่สามารถพิสูจน์ได้ว่าได้รับความยินยอมจากเจ้าของข้อมูล	ควบคุมความเสี่ยง	○	○	สูง (20 คะแนน)
2. การละเมิดความปลอดภัยของข้อมูล (Data Breach Risk)	1. ขาดมาตรการรักษาความปลอดภัยทางข้อมูล เช่น การเข้ารหัสข้อมูล	ควบคุมความเสี่ยง	○	○	สูง (20 คะแนน)
	2. การใช้ระบบหรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดตเพื่อป้องกันการโจมตีทางไซเบอร์	ควบคุมความเสี่ยง	○	○	สูง (20 คะแนน)

หมายเหตุ ช่องการควบคุมที่มีอยู่แล้ว ใส่เครื่องหมาย ✓ = มีอยู่แล้ว , ○ = มีแต่ไม่สมบูรณ์ , ✕ = ไม่มี
ช่องการควบคุมที่มีแล้วได้ผลหรือไม่ ✓ = ได้ผลตามที่คาดหวัง , ○ = ได้ผลบ้างแต่ไม่สมบูรณ์ , ✕ = ไม่ได้ผลตามที่คาดหวัง

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	ระดับ ความเสี่ยง	แนวทาง/กิจกรรมการ ควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรม การควบคุม	ผู้รับผิดชอบ
1. การจัดการความยินยอม (Consent Management Risk)	1. ระบบการเก็บความยินยอมไม่ มีความชัดเจนและไม่โปร่งใส	สูง (20 คะแนน)	1. สร้างระบบการเก็บความ ยินยอมที่ชัดเจนและโปร่งใส	1. ระบบเก็บความยินยอมที่ สามารถตรวจสอบย้อนหลังได้	- รองอธิการบดี ดูแลงานเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ
	2. ไม่สามารถพิสูจน์ได้ว่าได้รับ ความยินยอมจากเจ้าของข้อมูล	สูง (20 คะแนน)	2. จัดทำการบันทึกและ จัดเก็บหลักฐานความ ยินยอมอย่างครบถ้วน	2. มีเอกสารหรือหลักฐานการ ยินยอมที่ครบถ้วนและสามารถ ตรวจสอบได้	- รองอธิการบดี ดูแลงานเทคโนโลยี (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. ใช้ระบบเข้ารหัสข้อมูล และการรักษาความปลอดภัยของข้อมูล	1. ข้อมูลถูกเข้ารหัสและมีมาตรการรักษาความปลอดภัยที่เหมาะสม	- รองอธิการบดี ผู้อำนวยการเทคโนโลยี (ผู้กำกับ) - ผอ. / รอง ผอ. เทคโนโลยีฯ
	2. การใช้ระบบหรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดตเพื่อป้องกันการโจมตีทางไซเบอร์	สูง (20 คะแนน)	2. อัปเดตซอฟต์แวร์และระบบรักษาความปลอดภัยอย่างสม่ำเสมอ	2. การอัปเดตซอฟต์แวร์อย่างต่อเนื่องและตรวจสอบประสิทธิภาพ	- รองอธิการบดี ผู้อำนวยการเทคโนโลยี (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. ระบบการเก็บความยินยอมไม่มี ความชัดเจนและไม่โปร่งใส	1. สร้างระบบการเก็บความยินยอมที่ ชัดเจนและโปร่งใส 2. พัฒนาและทดสอบเครื่องมือเก็บ ข้อมูลเพื่อบันทึกการยินยอมอย่าง ชัดเจน	1. ระบบเก็บความยินยอมที่สามารถ ตรวจสอบย้อนหลังได้ 2. เครื่องมือเก็บข้อมูลถูกนำมาใช้ใน องค์กรและมีบันทึกการยินยอมที่ ถูกต้องและโปร่งใส	-
	2. ไม่สามารถพิสูจน์ได้ว่าได้รับ ความยินยอมจากเจ้าของข้อมูล	1. จัดทำการบันทึกและจัดเก็บ หลักฐานความยินยอมอย่างครบถ้วน 2. มีการตรวจสอบความถูกต้องของ เอกสารความยินยอมทุกไตรมาส	1. มีเอกสารหรือหลักฐานการยินยอม ที่ครบถ้วนและสามารถตรวจสอบได้ 2. การตรวจสอบรายไตรมาสบ่งชี้ว่า หลักฐานมีความถูกต้องและทันสมัย	-
2. การละเมิดความปลอดภัย ของข้อมูล (Data Breach Risk)	1. ขาดมาตรการรักษาความ ปลอดภัยทางข้อมูล เช่น การ เข้ารหัสข้อมูล	1. ใช้ระบบเข้ารหัสข้อมูลและการ รักษาความปลอดภัยของข้อมูล 2. จัดตั้งทีม IT เพื่อตรวจสอบและ ประเมินความปลอดภัยข้อมูลราย ไตรมาส	1. ข้อมูลถูกเข้ารหัสและมีมาตรการ รักษาความปลอดภัยที่เหมาะสม 2. รายงานการตรวจสอบความ ปลอดภัยจากทีม IT ทุกไตรมาส	-

ความเสี่ยง	ปัจจัยเสี่ยง	แนวทาง/กิจกรรมการควบคุม	ตัวชี้วัดของแนวทาง/กิจกรรมการควบคุม	ผลการดำเนินงาน
	2. การใช้ระบบหรือซอฟต์แวร์ที่ไม่ได้รับการอัปเดตเพื่อป้องกันการโจมตีทางไซเบอร์	1. อัปเดตซอฟต์แวร์และระบบรักษาความปลอดภัยอย่างสม่ำเสมอ 2. ทำการทดสอบความปลอดภัยด้วยการเจาะระบบ (Penetration Testing) ทุกปี	1. การอัปเดตซอฟต์แวร์อย่างต่อเนื่องและตรวจสอบประสิทธิภาพ 2. รายงานการทดสอบ Penetration Testing ที่แสดงผลลัพธ์ความปลอดภัยที่สูงขึ้น	-

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

1. การจัดการความยินยอม (Consent Management Risk)

- ปัญหาที่พบ
.....
.....
- การดำเนินการ
.....
.....
- ผลการดำเนินการ
.....
.....

2. การละเมิดความปลอดภัยของข้อมูล (Data Breach Risk)

- ปัญหาที่พบ
.....
.....
- การดำเนินการ
.....
.....
- ผลการดำเนินการ
.....
.....

ผลการดำเนินงานโดยสรุป

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

จากการดำเนินการในข้างต้นที่กล่าวมาแล้วนั้น สามารถสรุปผลการดำเนินงานตามแผนบริหารความเสี่ยง และการควบคุมภายใน ประจำปีงบประมาณ 2568 สรุปผลดังแสดงในตารางต่อไปนี้

ความเสี่ยง	ปัจจัยเสี่ยง	โอกาสที่ จะ เกิดขึ้น	ผลกระทบ ความรุนแรง	ระดับ คะแนน ความเสี่ยง	ระดับ ความ เสี่ยง
1. การจัดการความ ยินยอม (Consent Management Risk)	- ระบบการเก็บความ ยินยอมไม่มีความชัดเจน และไม่โปร่งใส				
	- ไม่สามารถพิสูจน์ได้ว่า ได้รับความยินยอมจาก เจ้าของข้อมูล				
2. การละเมิดความ ปลอดภัยของข้อมูล (Data Breach Risk)	- ขาดมาตรการรักษา ความปลอดภัยทางข้อมูล เช่น การเข้ารหัสข้อมูล				
	- การใช้ระบบหรือ ซอฟต์แวร์ที่ไม่ได้รับ การอัปเดตเพื่อป้องกัน การโจมตีทางไซเบอร์				

บทที่ 5

การติดตามและประเมินผลตามแผนบริหารความเสี่ยงและการควบคุมภายใน

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

องค์ประกอบที่สำคัญของกระบวนการควบคุมและประเมินผล

1. การวัดและประเมินผล

○ กระบวนการย่อย 3 ขั้นตอน

▪ การเก็บรวบรวมข้อมูล

- ในขั้นตอนนี้จะมีการรวบรวมข้อมูลที่จำเป็นจากแหล่งต่าง ๆ เช่น รายงานการดำเนินงาน รายงานการตรวจสอบ และข้อเสนอแนะจากผู้ให้บริการ
- ข้อมูลจะต้องถูกจัดเก็บในรูปแบบที่เป็นระเบียบ เพื่อให้การเข้าถึงข้อมูลทำได้ง่าย

▪ การวิเคราะห์และประเมินผลข้อมูล

- ข้อมูลที่เก็บรวบรวมจะถูกนำมาวิเคราะห์เพื่อดูความสำเร็จในการดำเนินงานตามแผน เช่น การเปรียบเทียบกับเป้าหมายที่ตั้งไว้
- การวิเคราะห์นี้จะช่วยให้เห็นภาพรวมเกี่ยวกับประสิทธิภาพของมาตรการที่ใช้

▪ การเสนอผลการประเมิน

- ผลการวิเคราะห์จะต้องถูกจัดทำเป็นรายงาน โดยมีการแสดงข้อมูลที่สำคัญ เช่น จุดแข็ง จุดอ่อน และข้อเสนอแนะสำหรับการปรับปรุง
- รายงานจะถูกส่งไปยังผู้บริหารและบุคลากรที่เกี่ยวข้องเพื่อนำไปใช้ในการตัดสินใจและวางแผนในอนาคต

2. การติดตามระหว่างการปฏิบัติงาน

- ในระหว่างการดำเนินการตามแผนบริหารความเสี่ยง จะมีการติดตามจากผู้บริหารที่ได้รับมอบหมายเพื่อให้แน่ใจว่าการดำเนินงานเป็นไปตามแผน

- การติดตามนี้จะรวมถึงการจัดประชุมเพื่อตรวจสอบสถานะการดำเนินงาน และมีการสื่อสารระหว่างทีมงานเพื่อให้สามารถแก้ไขปัญหาที่เกิดขึ้นได้ทัน่วงที

3. การติดตามเป็นรายครึ่ง

- 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

1. PDPA (Personal Data Protection Act)

- คำอธิบาย
 - PDPA เป็นกฎหมายการป้องกันข้อมูลส่วนบุคคลที่มีผลบังคับใช้ในประเทศไทย โดยมุ่งเน้นการคุ้มครองสิทธิของบุคคลในการจัดการข้อมูลส่วนบุคคลของตนเอง
 - กฎหมายนี้กำหนดให้ผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูลต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- ความสำคัญ
 - PDPA ช่วยให้เจ้าของข้อมูลมีสิทธิในการเข้าถึงและควบคุมข้อมูลส่วนบุคคลของตน รวมถึงสิทธิในการขอให้ลบข้อมูลและตรวจสอบความถูกต้องของข้อมูล

2. ROPA (Record of Processing Activities)

- คำอธิบาย
 - ROPA คือเอกสารที่บันทึกข้อมูลเกี่ยวกับกิจกรรมการประมวลผลข้อมูลส่วนบุคคลขององค์กร โดยเฉพาะอย่างยิ่งสำหรับองค์กรที่อยู่ภายใต้ข้อบังคับของ PDPA
 - เอกสารนี้จะรวมถึงข้อมูลเกี่ยวกับประเภทของข้อมูลที่ถูกประมวลผล, วัตถุประสงค์ในการประมวลผล, วิธีการประมวลผล, และข้อมูลเกี่ยวกับผู้ควบคุมข้อมูล
- ความสำคัญ
 - ROPA ช่วยให้องค์กรสามารถแสดงความโปร่งใสในการจัดการข้อมูลส่วนบุคคล และเป็นเครื่องมือสำคัญในการปฏิบัติตามกฎหมาย PDPA

3. VS Scan (Vulnerability Scan)

- คำอธิบาย
 - VS Scan เป็นกระบวนการที่ใช้ในการตรวจสอบช่องโหว่ในระบบซอฟต์แวร์หรือโครงสร้างพื้นฐานขององค์กร โดยการใช้เครื่องมือเฉพาะเพื่อค้นหาช่องโหว่ที่อาจถูกโจมตีได้
 - การสแกนช่องโหว่จะทำการตรวจสอบระบบเครือข่าย อุปกรณ์ เซิร์ฟเวอร์ และแอปพลิเคชัน เพื่อค้นหาความเสี่ยงที่อาจเกิดขึ้น
- ความสำคัญ
 - การดำเนินการ VS Scan เป็นขั้นตอนสำคัญในการรักษาความปลอดภัยของข้อมูล และช่วยให้องค์กรสามารถจัดการกับช่องโหว่ที่อาจเป็นอันตรายได้ก่อนที่จะถูกโจมตีจริง

4. PenTest (Penetration Testing)

- คำอธิบาย

- PenTest หรือการทดสอบการเจาะระบบ เป็นกระบวนการที่ผู้เชี่ยวชาญด้านความปลอดภัยจะพยายามโจมตีระบบขององค์กร เพื่อหาช่องโหว่และตรวจสอบว่าระบบมีความปลอดภัยเพียงใด
- PenTest มักจะใช้เทคนิคและเครื่องมือที่คล้ายกับที่แฮกเกอร์ใช้ในการโจมตีระบบจริง
- **ความสำคัญ**
 - PenTest ช่วยให้องค์กรสามารถตรวจสอบความแข็งแกร่งของมาตรการรักษาความปลอดภัยและให้ข้อมูลที่มีค่าในการปรับปรุงระบบรักษาความปลอดภัยเพื่อป้องกันการโจมตีที่อาจเกิดขึ้นในอนาคต