สารบัญ

หน้า

การบริหารจัดการความเสี่ยงด้านสารสนเทศ
สำนักคอมพิวเตอร์

จากภารกิจของสำนักคอมพิวเตอร์ มหาวิทยาลัยราชภัฏนครราชสีมา และความจำเป็นของการใช้งานเทคโนโลยีสารสนเทศในยุคปัจจุบัน จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานนั้นเกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น การบริหารจัดการความเสี่ยงของสำนักคอมพิวเตอร์จึงมีวัตถุประสงค์เพื่อเป็นแนวทางที่ใช้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัยด้วยการคาดการณ์ล่วงหน้าในกรณีที่ความเสี่ยงนั้นอาจเกิดขึ้นจริง และนำแนวทางจัดการความเสี่ยงนี้ไปใช้ในดำเนินการ

ความหมายของการบริหารความเสี่ยงด้านสารสนเทศ

ความเสี่ยง (Risk) **หมายถึง** เหตุการณ์หรือการกระทำที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 4 ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่ยอมรับได้ ซึ่งการจัดการความเสี่ยงอาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

หลักการวิเคราะห์ ประเมิน และจัดทำความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (Committee of Sponsoring Organization of the Tread way Commission) มีดังนี้

1. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
2. การระบุความเสี่ยงต่าง ๆ (Event Identification)
3. การประเมินความเสี่ยง (Risk Assessment)
4. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
5. กิจกรรมการบริหารความเสี่ยง (Control Activities)
6. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
7. การติดตามผลและเฝ้าระวังความเสี่ยงต่าง ๆ (Monitoring)

วัตถุประสงค์

1. เพื่อให้การจัดการภายในสำนักคอมพิวเตอร์ มีประสิทธิภาพ และมีความยืดหยุ่นในการปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศสมัยใหม่ รวมทั้งลดโอกาสที่จะก่อให้เกิดความเสียหายที่ไม่ต้องการกับระบบสารสนเทศ

2. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของสำนักคอมพิวเตอร์

3. เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ

4. เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และการเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

5. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

ขอบเขตการดำเนินการ

เป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในความรับผิดชอบของสำนักคอมพิวเตอร์

การประเมินความเสี่ยง (Risk assessment)

การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของสำนักคอมพิวเตอร์สามารถแยกประเภทความเสี่ยงแต่ละด้านเป็น 4 ประเภท ดังนี้

ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ อันอาจเกิดจากการถูกโจมตีจากไวรัส หรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

แผนบริหารความเสี่ยง ด้านสารสนเทศ ปี 2559
สำนักคอมพิวเตอร์

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
1 ความเสี่ยงจากการถูกบุคคลอื่นเข้าถึงข้อมูลส่วนบุคคล	RIT01	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบรหัสผ่านของตนเองให้ผู้อื่นเข้าใช้งาน หรือ ทำงานแทน	การขาดความตระหนักในเรื่องความปลอดภัยด้านสารสนเทศ	ผู้ใช้งาน ระบบสารสนเทศ ระบบฐานข้อมูล
2 ความเสี่ยงของการนำอุปกรณ์กระจายสัญญาณที่ไม่ได้รับอนุญาตมาเชื่อมต่อในระบบเครือข่ายมหาวิทยาลัย	RIT02	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าถึงระบบเครือข่าย เช่น การนำ **Access Point** มาเชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัยโดยไม่ได้มีการตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกสามารถเชื่อมต่อเข้ากับระบบเครือข่ายของมหาวิทยาลัย ทำให้เกิดช่องโหวในระบบรักษาความปลอดภัย	การขาดความตระหนักในเรื่องความปลอดภัยของการเข้าถึงระบบเครือข่าย	ผู้ใช้งาน ผู้ดูแลระบบ ระบบสารสนเทศ ระบบฐานข้อมูล เครื่องคอมพิวเตอร์แม่ข่าย
3 ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง หรือไม่สม่ำเสมอ	RIT03	ความเสี่ยงจากภัย หรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหาย หรือ เมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศเกิดการสูญหาย และ การให้บริการสารสนเทศไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	การขาดแหล่งกำเนิดไฟฟ้าสำรอง	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์ ระบบฐานข้อมูล ระบบสารสนเทศ
4 ความเสี่ยงจากการถูกบุกโจมตีโดยผู้ประสงค์ร้าย	RIT04	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ประสงค์ร้าย เช่น แฮ็คเกอร์ แคร็กเกอร์ เป็นต้น หรือ การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม การโจมตีการให้บริการ **(**denial of services**/ DOS)**	การควบคุมการเข้าถึงและการใช้งานสารสนเทศ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
5 ความเสี่ยงจากการขาดบุคลากรผู้ปฏิบัติงาน	RIT05	ความเสี่ยงด้านการบริหารจัดการ	การขาดบุคลากรด้านสารสนเทศทำให้การทำงานหยุดชะงัก ทั้งจากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานและ จำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	การขาดความเข้าใจภาระงานด้านสารสนเทศ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
6 ความเสี่ยงจากการปรับนโยบายในการบริหารงาน	RIT06	ความเสี่ยงด้านการบริหารจัดการ	นโยบายการบริหารงานสารสนเทศเปลี่ยนแปลง ทำให้การดำเนินการโครงการต่างๆ ได้รับผลกระทบ	การขาดความเข้าใจความจำเป็นของงานด้านสารสนเทศ	ผู้ใช้งาน ผู้ดูแลระบบ อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
7 ความเสี่ยงของการขาดระบบสารสนเทศ	RIT07	ความเสี่ยงด้านการบริหารจัดการ	ข้อจำกัดของงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	การมีงบประมาณจำกัดของมหาวิทยาลัย	ผู้ใช้งาน ผู้ดูแลระบบ ระบบฐานข้อมูล ระบบสารสนเทศ
8 ความเสี่ยงจากเครื่องคอมพิวเตอร์หรือ อุปกรณ์ไม่สามารถทำงานได้	RIT08	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์ หรือ อุปกรณ์ชำรุด หรือ มีสมรรถนะไม่เพียงพอในการทำงาน	การขาดแผนการบำรุงรักษาอุปกรณ์และ เพิ่มประสิทธิภาพ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
9 ความเสี่ยงจากการสูญหายของข้อมูลสารสนเทศ	RIT09	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การขาดระบบการสำรองข้อมูลที่เหมาะสม ทำให้ไม่สามารถสำรองข้อมูลได้อย่างมีประสิทธิภาพ	ความเสียหายของข้อมูล	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
10 ความเสี่ยงจากขยายการให้บริการระบบเครือข่าย	RIT10	ความเสี่ยงด้านการบริหารจัดการ	การขาดการออกแบบและติดตั้งระบบเครือข่ายภายในอาคารที่ก่อสร้างใหม่	ความจำเป็นของการใช้งานระบบเครือข่าย	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย
11 ความเสี่ยงของการเกิดสาธารณภัย	RIT11	ความเสี่ยงจากภัย หรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ทำให้เกิดความเสียหายต่อการให้บริการสารสนเทศของมหาวิทยาลัย	การเตรียมการเพื่อรับสถานการณ์ หรือ การขาดระบบสำรองของสารสนเทศ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
12 ความเสี่ยงจากความไม่สงบในบ้านเมือง	RIT12	ความเสี่ยงจากภัย หรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรง หรือ ความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	การเตรียมการเพื่อรับสถานการณ์ หรือ การขาดระบบสำรองของสารสนเทศ	ผู้ดูแลระบบเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบฐานข้อมูล ระบบสารสนเทศ
13 ความเสี่ยงจากเครื่องคอมพิวเตอร์และอุปกรณ์สูญหาย	RIT13	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือ ชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือ การสูญหายของข้อมูลในเครื่องคอมพิวเตอร์นั้น	การควบคุมสินทรัพย์สารสนเทศ หรือ การขาดการรักษาความปลอดภัย ไม่เพียงพอ	ผู้ใช้งาน ผู้ดูแลระบบ เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย

การประมาณความเสี่ยง (Risk Estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณความเสี่ยง

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ซึ่งใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
5	สูงมาก	5 ครั้ง/ปี
4	สูง	4 ครั้ง/ปี
3	ปานกลาง	3 ครั้ง/ ปี
2	น้อย	2 ครั้ง/ปี
1	น้อยมาก	ไม่เกิน 1 ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	**ผลกระทบ**	**คำอธิบาย**
5	สูงมาก	ความเสียหายมากกว่า 10 ล้านบาท
4	สูง	ความเสียหายมากกว่า 5 แสนบาท ถึง 10 ล้านบาท
3	ปานกลาง	ความเสียหายมากกว่า 2.5 แสนบาท ถึง 5 แสน
2	น้อย	ความเสียหายมากกว่า 1 แสนบาท ถึง 2.5 แสน
1	น้อยมาก	ความเสียหายไม่เกิน 1 แสนบาท

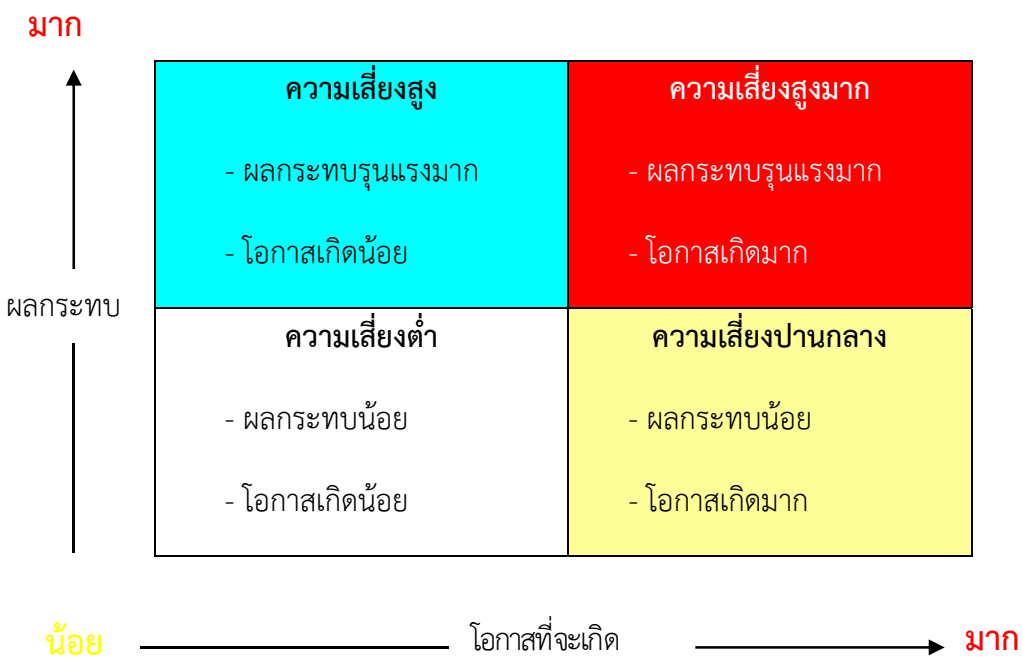
การประเมินค่าความเสี่ยง (Risk Evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมา ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้ ระดับความเสี่ยง เท่ากับ โอกาสในการเกิดเหตุการณ์ต่าง ๆ คูณ ความรุนแรงของเหตุการณ์ต่าง ๆ ซึ่งใช้เกณฑ์ในการจัดแบ่งดังนี้

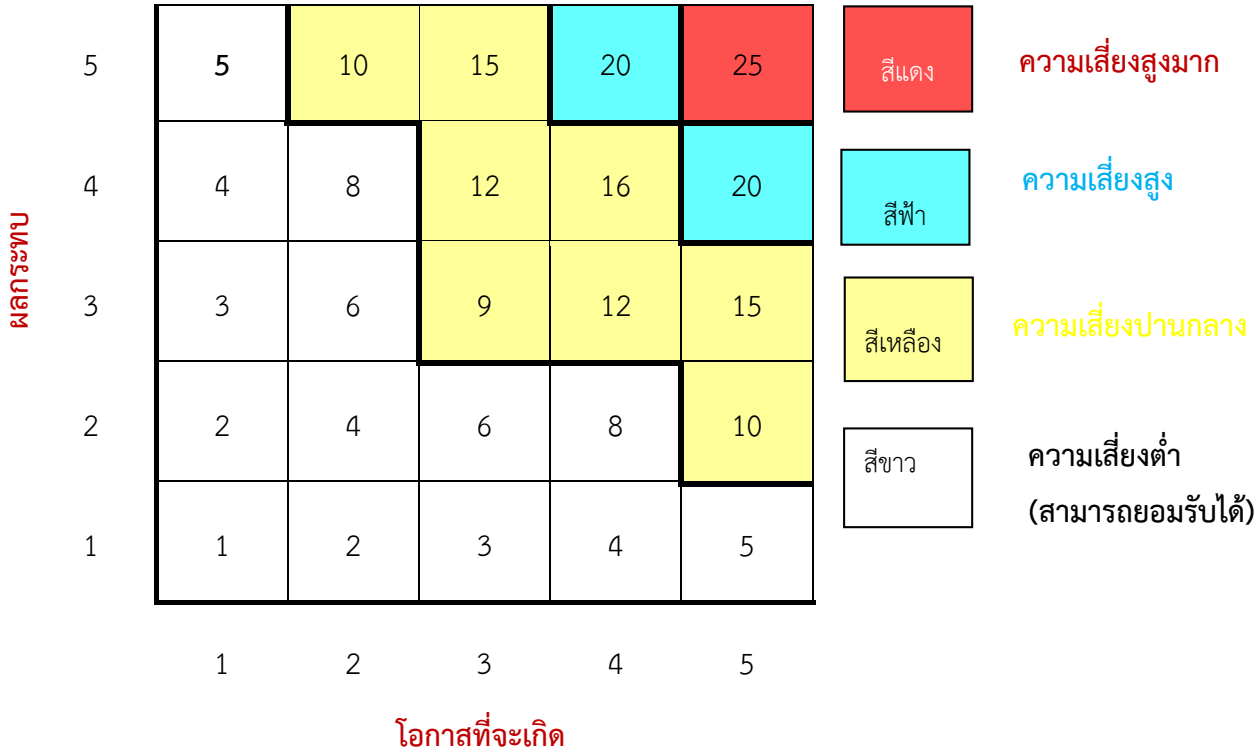
ระดับคะแนนความเสี่ยง	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
1 – 8	ต่ำ	ยอมรับความเสี่ยง	ขาว
9 – 16	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
17 – 24	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า
25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยง



การประเมินค่าความเสี่ยง



รายงานผลการวิเคราะห์ความเสี่ยง

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
1 ความเสี่ยงจากการถูกบุคคลอื่นเข้าถึงข้อมูลส่วนบุคคล	RIT01	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบรหัสผ่านของตนเองให้ผู้อื่นเข้าใช้งานหรือ ทำงานแทน	5	4	20
2 ความเสี่ยงของการนำอุปกรณ์กระจายสัญญาณที่ไม่ได้รับอนุญาตมาเชื่อมต่อในเครือข่ายมหาวิทยาลัย	RIT02	ความเสี่ยงจากผู้ปฏิบัติงาน	ผู้ใช้ขาดความระมัดระวังในการเข้าถึงระบบเครือข่าย เช่น การนำ Access Point มาเชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัยโดยไม่ได้มีการตั้งค่าการรักษาความปลอดภัย ทำให้เครื่องคอมพิวเตอร์ของบุคคลภายนอกสามารถเชื่อมต่อเข้ากับระบบเครือข่ายของมหาวิทยาลัย ทำให้เกิดช่องโหว่ในระบบรักษาความปลอดภัย	5	3	15

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
3 ความเสี่ยงจากกระแสไฟฟ้าขัดข้องหรือไม่สม่ำเสมอ	RIT03	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหาย หรือ เมื่อกระแสไฟฟ้าขัดข้องทำให้เครื่องคอมพิวเตอร์แม่ข่ายถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศเกิดการสูญหาย และการให้บริการสารสนเทศไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ	5	2	10
4 ความเสี่ยงจากการถูกบุกรุกโดยประสงค์ร้าย	RIT04	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากผู้ปฏิบัติงาน	การบุกรุกโจมตีโดยผู้ประสงค์ร้าย เช่น แฮ็คเกอร์ แคร็กเกอร์ เป็นต้น หรือ การดักจับข้อมูล การส่งข้อมูล คำสั่งเจตนาร้าย การติดไวรัส หรือ การโจมตีการให้บริการ(denial of services)	2	4	8
5 ความเสี่ยงจากการขาดบุคลากรผู้ปฏิบัติงาน	RIT05	ความเสี่ยงด้านการบริหารจัดการ	การขาดบุคลากรด้านสารสนเทศทำให้การทำงานหยุดชะงัก ทั้งจากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานและจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	5	4	20
6 ความเสี่ยงจากการปรับนโยบายในการบริหารงาน	RIT06	ความเสี่ยงด้านการบริหารจัดการ	นโยบายการบริหารงานสารสนเทศเปลี่ยนแปลง ทำให้การดำเนินการโครงการต่างๆ ได้รับผลกระทบ	1	1	1
7 ความเสี่ยงของการขาดระบบสารสนเทศ	RIT07	ความเสี่ยงด้านการบริหารจัดการ	ข้อจำกัดของงบประมาณในการดำเนินการให้ระบบสารสนเทศสามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	5	4	20
8 ความเสี่ยงจากเครื่องคอมพิวเตอร์หรือ อุปกรณ์ไม่สามารถทำงานได้	RIT08	ความเสี่ยงด้านเทคนิค	เครื่องคอมพิวเตอร์ หรือ อุปกรณ์ชำรุด หรือ มีสมรรถนะไม่เพียงพอในการทำงาน	1	5	5
9 ความเสี่ยงจากการสูญหายของข้อมูลสารสนเทศ	RIT09	ความเสี่ยงด้านการบริหารจัดการ/ความเสี่ยงจากผู้ปฏิบัติงาน	การขาดระบบการสำรองข้อมูลที่เหมาะสม ทำให้ไม่สามารถสำรองข้อมูลได้อย่างมีประสิทธิภาพ	1	2	2

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
10 ความเสี่ยงจากขยายการให้บริการระบบเครือข่าย	RIT10	ความเสี่ยงด้านการบริหารจัดการ	การขาดการออกแบบและติดตั้งระบบเครือข่ายภายในอาคารที่ก่อสร้างใหม่	3	4	12
11 ความเสี่ยงของการเกิดสาธารณภัย	RIT11	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆทำให้เกิดความเสียหายต่อการให้บริการสารสนเทศของมหาวิทยาลัย	1	5	5
12 ความเสี่ยงจากความไม่สงบในบ้านเมือง	RIT12	ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน	การเกิดสถานการณ์ความรุนแรงหรือ ความไม่สงบเรียบร้อย จนทำให้บุคลากรสามารถปฏิบัติงานได้ตามปกติ	1	4	4
13 ความเสี่ยงจากเครื่องคอมพิวเตอร์และอุปกรณ์สูญหาย	RIT13	ความเสี่ยงด้านการบริหารจัดการ/ ความเสี่ยงจากผู้ปฏิบัติงาน	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือ การสูญหายของข้อมูลในเครื่องคอมพิวเตอร์นั้น	1	4	4