การบริหารความเสี่ยง

ของฐานข้อมูลสารสนเทศศูนย์บริการวิชาการ

กลยุทธ์ในการจัดการความเสี่ยง

การวิเคราะห์ ประเมินโอกาสที่จะเกิดขึ้นของความเสี่ยงและผลกระทบ

แผนการบริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศ

ปัจจัยที่ทำให้ระบบบริหารความเสี่ยงสำเร็จ

สารบัญ

เรื่อง **หน้า**

คำนำ

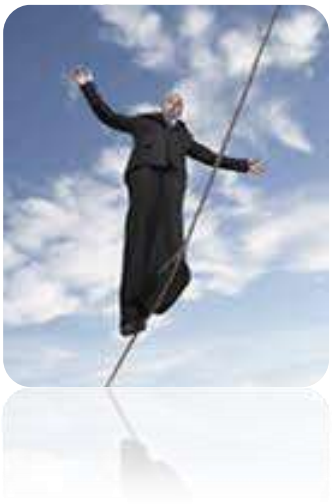
ศูนย์บริการวิชาการ มหาวิทยาลัยขอนแก่น มีการบริหารงานโดย รศ.ดร.อำนวย คำตื้อ ผู้อำนวยการศูนย์บริการวิชาการและคณะ มีภารกิจหลักด้านการบริการวิชาการแก่สังคม และเป็นศูนย์กลางในการพัฒนาทรัพยากรมนุษย์ ให้บริการและถ่ายทอดเทคโนโลยี สร้างชุมชนต้นแบบแห่งการพัฒนาที่เป็นแบบอย่าง ประสานงานสร้างเครือข่ายอุตสาหกรรม และมุ่งส่งเสริมในการพัฒนากลุ่มประเทศอนุภูมิภาคลุ่มน้ำโขง จากการดำเนินงานดังกล่าวต้องใช้ข้อมูลสารสนเทศเป็นกลไกในการบริหารจัดการด้านต่าง ๆ จึงจำเป็นต้องมีมาตรการในการบริหารความเสี่ยงของฐานข้อมูลสารสนทศ โดยเฉพาะการควบคุมทั้งระบบข้อมูลสารสนเทศ ระบบเครือข่ายเน็ตเวิร์ค ทั้งในด้านของ Hardware และ Software ซึ่งระบบการควบคุมจำเป็นต้องพัฒนาไปพร้อมกับการพัฒนาของเทคโนโลยีที่เกิดขึ้นอย่างรวดเร็วและเป็นไปอย่างเป็นระบบและเหมาะสม ศูนย์บริการวิชาการ ได้มอบหมายให้ส่วนสารสนเทศจัดทำการบริหารความเสี่ยงของฐานข้อมูลสารสนเทศ เพื่อเตรียมความพร้อมและรองรับสถานการณ์เสี่ยงที่จะเกิดขึ้นกับระบบฐานข้อมูล กำหนดมาตรการ และมีแผนการบริหารความเสี่ยงของฐานข้อมูลสารสนเทศ ในการป้องกันความเสียหายที่จะเกิดขึ้นจากภาวะความเสี่ยงต่าง ๆ เพื่อให้ระบบฐานข้อมูลสารสนเทศของศูนย์บริการวิชาการสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ

ส่วนสารสนเทศ

ศูนย์บริการวิชาการ มหาวิทยาลัยขอนแก่น

การบริหารความเสี่ยงของฐานข้อมูลสารสนเทศศูนย์บริการวิชาการ มหาวิทยาลัยขอนแก่น
ประจำปีงบประมาณ 2553
(ระหว่างวันที่ 1 ตุลาคม2552 - กันยายน 2553)

1. นิยามเกี่ยวข้องกับความเสี่ยง



ความเสี่ยง หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และส่งผลกระทบและความเสียหายหรือความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จต่อเป้าหมาย และวัตถุประสงค์ที่กำหนด

ข้อมูล (Data) หมายถึง ข้อเท็จจริงต่าง ๆ ซึ่งอาจแสดงเป็นตัวเลข ตัวหนังสือ หรือสัญลักษณ์ ข้อเท็จจริงเหล่านี้เป็นสิ่งที่เก็บรวบรวมมาโดยยังไม่ผ่านการประมวลผล หรือการวิเคราะห์จัดกระทำ จึงทำให้ส่วนมากไม่มีความหมายที่สมบูรณ์พอที่จะนำไปใช้ประกอบการตัดสินใจได้

สารสนเทศ (Information) หมายถึง ข้อมูลที่ผ่านการประมวลหรือการวิเคราะห์ด้วยวิธีการต่าง ๆ จนอยู่ในรูปแบบที่มีความหมาย สามารถนำไปใช้ประกอบการตัดสินใจหรือนำไปใช้ในเรื่องต่าง ๆ ได้ตามวัตถุประสงค์

ระบบสารสนเทศ (Information System) หมายถึง กระบวนการเก็บรวบรวมข้อมูล การประมวลข้อมูลให้อยู่ในรูปสารสนเทศที่เป็นประโยชน์สูงสุด และการจัดเก็บรักษาอย่างมีระบบเพื่อสะดวกต่อการนำไปใช้ สารสนเทศที่ถูกจัดเก็บอย่างเห็นระบบจะสามารถนำไปใช้สนับสนุนการบริหารและการตัดสินใจทั้งในระดับปฏิบัติ ระดับกลุ่มงาน หรือระดับบริหาร

ระบบฐานข้อมูล (Database System) หมายถึง การจัดเก็บข้อมูลที่มีความสัมพันธ์กันมาจัดเก็บในที่เดียวกัน ซึ่งแต่เดิมถูกจัดเก็บอยู่ในแต่ละแฟ้มข้อมูลเป็นระบบแฟ้มข้อมูล ฐานข้อมูลมีความจำเป็นในการแก้ปัญหาต่างๆ ที่เกิดขึ้นจากระบบแฟ้มข้อมูล ได้แก่ ความซ้ำซ้อนของข้อมูล ความขัดแย้งของข้อมูลความยากในการแก้ไขและบำรุงรักษา การผูกติดกับข้อมูล การกระจายของข้อมูล และการใช้ประโยชน์จากข้อมูลลดลง เพื่อประโยชน์ในการใช้งานตามวัตถุประสงค์ของหน่วยงาน

ความเสี่ยงของระบบฐานข้อมูลสารสนเทศ หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่าหรือเหตุการณ์ซึ่งไม่พึงประสงค์ ที่ทำให้งานไม่ประสบความสำเร็จตามวัตถุประสงค์ และเป้าหมายที่กำหนด

การบริหารความเสี่ยง (Risk Management) เป็นการปฏิบัติควบคุมความเสี่ยง ประกอบด้วย การวางแผนความเสี่ยง การประเมินความเสี่ยงด้านต่าง ๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง และการตรวจสอบความเสี่ยงเพื่อหาว่าความเสี่ยงได้เปลี่ยนแปลงไปอย่างไร ทั้งจากปัจจัยภายในและภายนอกที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยรับตรวจอย่างเพียงพอ และเหมาะสม

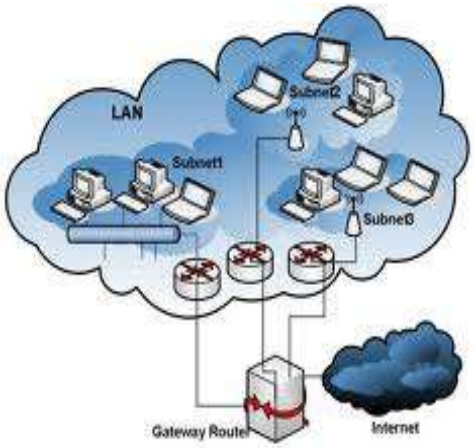


Fig. 1 A LAN comprises wired and wireless subnets.

การประเมินความเสี่ยง เป็นกระบวนการที่ใช้ระบุ และวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมหรือบริหารความเสี่ยง และ ขั้นตอนในการประเมินความเสี่ยงประเมินได้จากการระบุปัจจัยเสี่ยง ทั้งภายในและภายนอก, การวิเคราะห์ความเสี่ยงหาสาเหตุของความเสี่ยง และ การบริหารความเสี่ยง แก้ไขหรือควบคุมความเสี่ยง

2. กลยุทธ์ในการจัดการความเสี่ยง

1. Take (การยอมรับ) หมายถึง ยอมรับความเสี่ยงที่เกิดจากการปฏิบัติงานและภายใต้ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้

2. Treat (การลด) หมายถึง การดำเนินการเพิ่มเติมเพื่อลดโอกาสเกิดหรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

3. Terminate (การหลีกเลี่ยง) หมายถึง การดำเนินการเพื่อยกเลิกหรือหลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง ทั้งนี้หากทำการใช้กลยุทธ์นี้ อาจต้องทำการพิจารณาวัตถุประสงค์ว่าสามารถบรรลุได้หรือไม่เพื่อทำการปรับเปลี่ยนต่อไป

4. Transfer (การร่วมจัดการ) หมายถึง การร่วมจัดการโดยแบ่งความเสี่ยงบางส่วนกับบุคคลหรือองค์กรอื่น

3. **หลักการและเหตุผล**

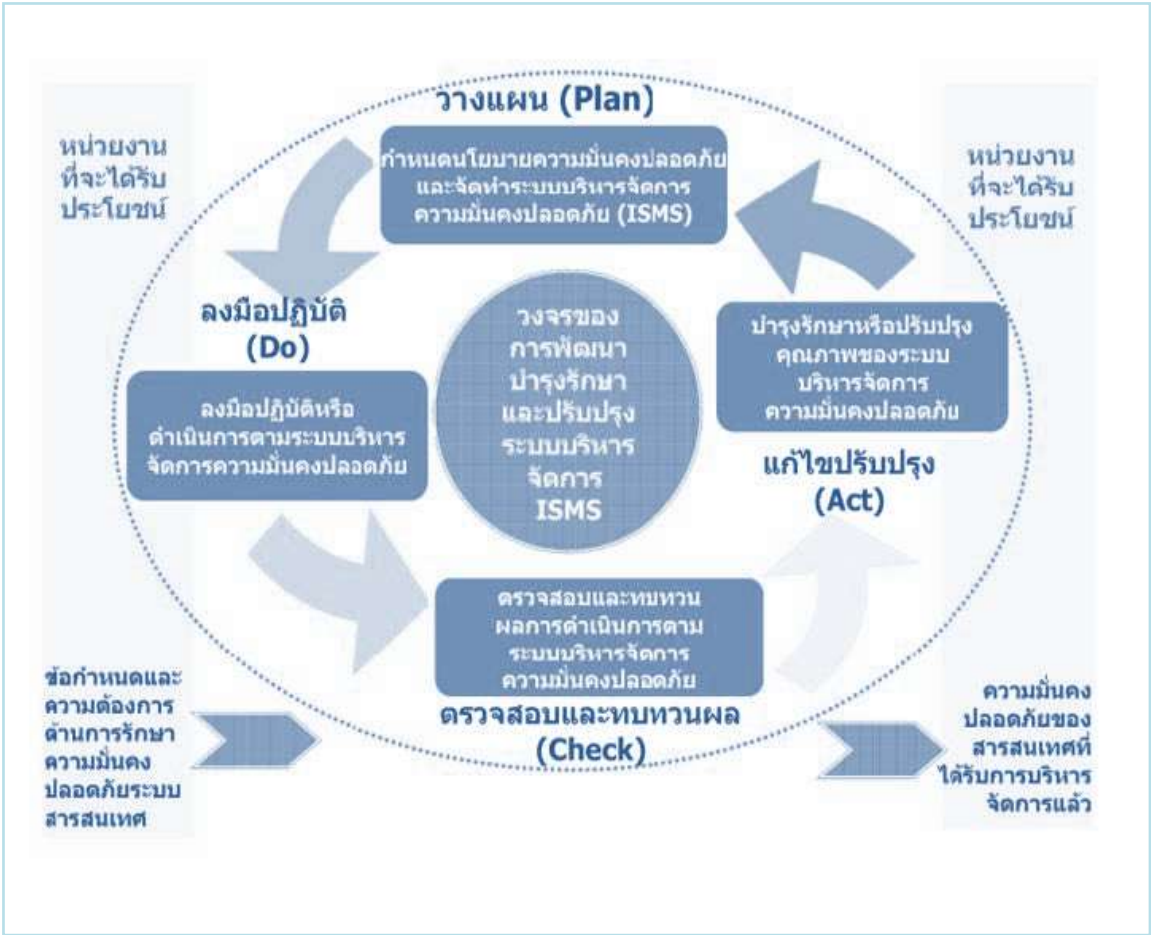
ศูนย์บริการวิชาการ มีภารกิจหลักด้านการบริการวิชาการแก่สังคม และเป็นศูนย์กลางในการพัฒนาทรัพยากรมนุษย์ ให้บริการและถ่ายทอดเทคโนโลยี สร้างชุมชนต้นแบบแห่งการพัฒนาที่เป็นแบบอย่าง ประสานงานการสร้างเครือข่ายอุตสาหกรรม และมุ่งส่งเสริมในการพัฒนากลุ่มประเทศอนุภูมิภาคลุ่มน้ำโขง จากการดำเนินงานที่กล่าวมานี้ ศูนย์บริการวิชาการได้มีการจัดเก็บข้อมูลจำนวนมากเพื่อการสนับสนุนการดำเนินงาน ดังนั้น ส่วนสารสนเทศจึงได้จัดทำฐานข้อมูลสารสนเทศที่สำคัญต่างๆของศูนย์บริการวิชาการ และวิเคราะห์ กลั่นกรองข้อมูลที่จำเป็นเพื่อใช้เป็นข้อมูลสารสนเทศเพื่อการบริหารจัดการของผู้บริหาร และเป็นข้อมูลสำหรับบุคลากรที่จะนำไปใช้ประโยชน์ใน การปฏิบัติ งาน ซึ่งได้แบ่งข้อมูลสารสนเทศออกเป็น 3 ด้าน ได้แก่ สารสนเทศเพื่อการบริหารจัดการ สารสนเทศเพื่อสนับสนุนการปฏิบัติงาน และสารสนเทศเพื่อให้บริการ โดยมีการให้บริการข้อมูลในระบบ Intranet และ Internet ซึ่งมีการบริหารจัดการเป็นระบบเครือข่าย ดังนั้น เพื่อเป็นการป้องกันความเสี่ยงที่จะเกิดขึ้นกับฐานข้อมูลสารสนเทศ จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการเตรียมการและวางแผนรองรับปัญหาเกี่ยวกับความเสี่ยงและภัยพิบัติต่าง ๆ ที่จะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศศูนย์บริการวิชาการ

4. **วัตถุประสงค์**

1) เพื่อเตรียมความพร้อม และรองรับสถานการณ์ฉุกเฉินที่จะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของศูนย์บริการวิชาการ
2) เพื่อกำหนดมาตรการในการป้องกันความเสียหายที่จะเกิดกับระบบฐานข้อมูลสารสนเทศจากภาวะความเสี่ยงต่างๆ
3) เพื่อให้ระบบงานฐานข้อมูลสารสนเทศของศูนย์บริการวิชาการ สามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ

5. กระบวนการบริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศ

ความเสี่ยง (Risk) เป็นสิ่งที่เกิดจากการรวมตัวกันของข้อจำกัด (Constraint) และความไม่แน่นอน (Uncertainly) การบริหารความเสี่ยง (Risk Management) เป็นการปฏิบัติการควบคุมความเสี่ยง ซึ่งจะประกอบด้วยการวางแผนความเสี่ยง การประเมินความเสี่ยงด้านต่าง ๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง การตรวจสอบความเสี่ยงว่าเป็นไปได้มากน้อยเพียงใด ส่วนสารสนเทศ จึงได้จัดทำแผนการบริหารความเสี่ยงของฐานข้อมูลสารสนเทศ วัตถุประสงค์เพื่อลดโอกาสที่จะเกิดความเสี่ยง พร้อมทั้งกำหนดมาตรการบริหารความเสี่ยง และได้นำกระบวนการ Plan Check Act หรือ PA มาประยุกต์ใช้ในกระบวนการจัดการความมั่นคงปลอดภัยของฐานข้อมูลสารสนเทศให้สอดคล้องกับมาตรการบริหารความเสี่ยงดังกล่าว ตามแสดงในรูป



แผนภาพแสดงวงจรการบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน P-D-C-A

6. การบริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศ

ขั้นตอนที่ 1 Identify หมายถึง การระบุความเสี่ยงและผลกระทบที่มีผลต่อข้อมูลสารสนเทศ

ขั้นตอนที่ 2 Analyze หมายถึง ประเมินถึงโอกาสที่จะเกิดขึ้นของความเสี่ยง และความรุนแรง ของผลกระทบ

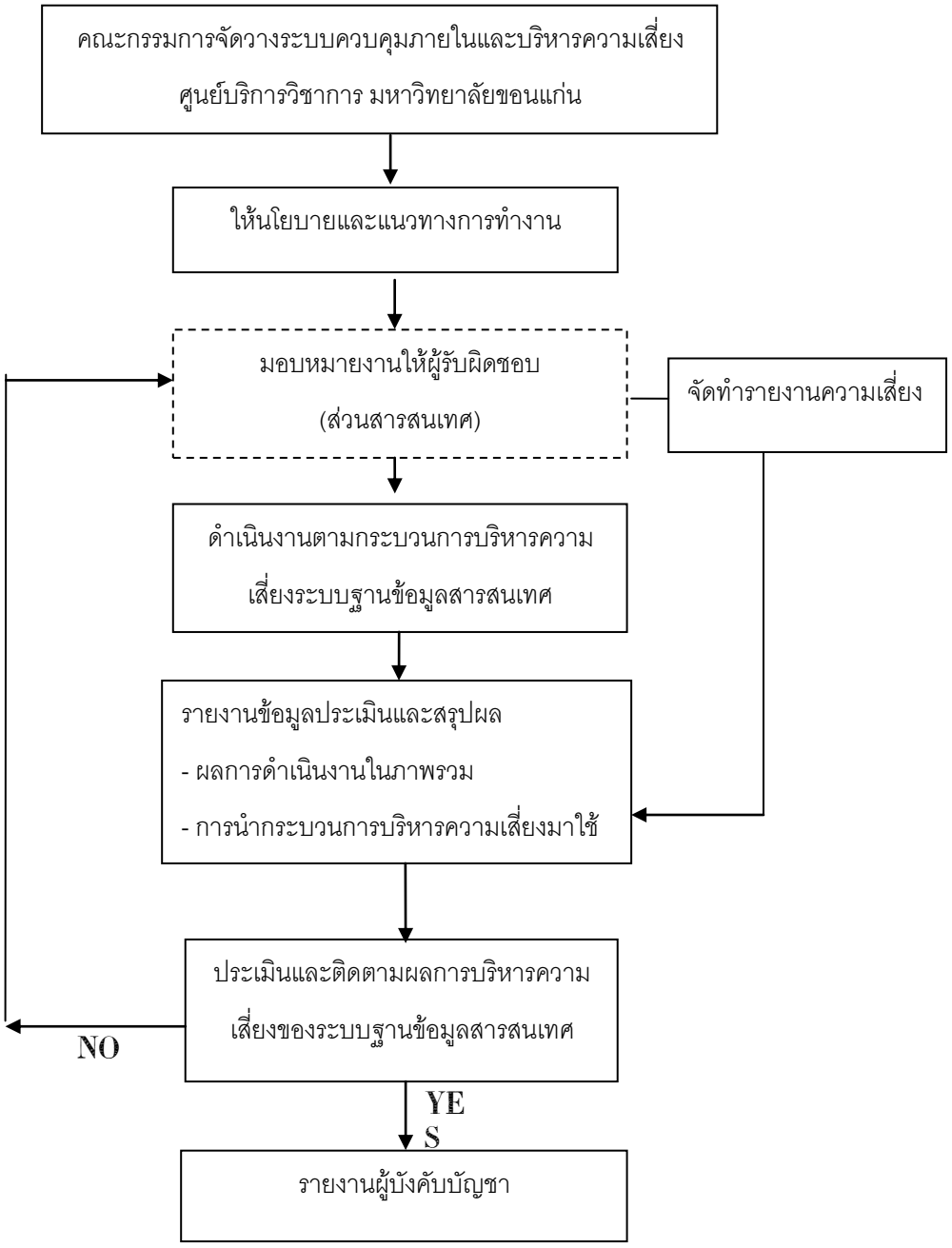
ขั้นตอนที่ 3 Plan หมายถึง การวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของ ความเสี่ยงให้บรรลุเป้าหมายหรือใกล้เคียงกับเป้าหมายที่กำหนด

ขั้นตอนที่ 4 Track หมายถึง การติดตามข้อมูลเพื่อทราบร่องรอยของความเสี่ยง

ขั้นตอนที่ 5 Control หมายถึง การติดตาม กำกับและตรวจสอบ การปฏิบัติการควบคุมความเสี่ยง

องค์ประกอบที่มีความสำคัญอีกประการหนึ่ง ที่เกี่ยวข้องในการบริหารการประเมินความเสี่ยง คือ การติดต่อสื่อสาร(Communicate) เพราะในการดำเนินการต่างๆ ต้องอาศัยการประสานงานกับทุกฝ่ายทั้งภายในและภายนอกหน่วยงาน เพื่อให้การดำเนินการในทุกขั้นตอนบรรลุผลตามเป้าหมาย มีความเข้าใจทางเลือกในการลดปัญหาความเสี่ยง ข้อมูลของความเสี่ยงในลักษณะต่างๆ และสามารถตัดสินใจได้ดีที่สุดภายใต้ข้อจำกัดของระบบพร้อมทำให้ระบบปฏิบัติการของส่วนสารสนเทศ สามารถนำไปใช้ประโยชน์ได้อย่างแท้จริง ศูนย์บริการวิชาการจึงได้จัดทำคำสั่งแต่งตั้งคณะ กรรมการจัดวางระบบควบคุมภายในและบริหารความเสี่ยง ศูนย์บริการวิชาการมหาวิทยาลัยขอนแก่น มีหน้าที่กำหนดนโยบายบริหารความเสี่ยง และระบุปัจจัยความเสี่ยงของศูนย์บริการวิชาการ จัดทำแผนบริหารความเสี่ยงและติดตามประเมินผล และจัดทำรายงานการควบคุมภายในศูนย์บริการวิชาการเสนอมหาวิทยาลัยขอนแก่นในด้านการ บริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศ นั้น ส่วนสารสนเทศ ได้รับมอบหมายให้ดำเนินการในการจัดทำ แผนและแนวทางในการบริการความเสี่ยง ปัจจัยเสี่ยง ระดับความรุนแรงของความเสี่ยง โอกาสและผลกระทบที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของศูนย์บริการวิชาการ และจัดทำแผนการบริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศ ประจำปี 2553

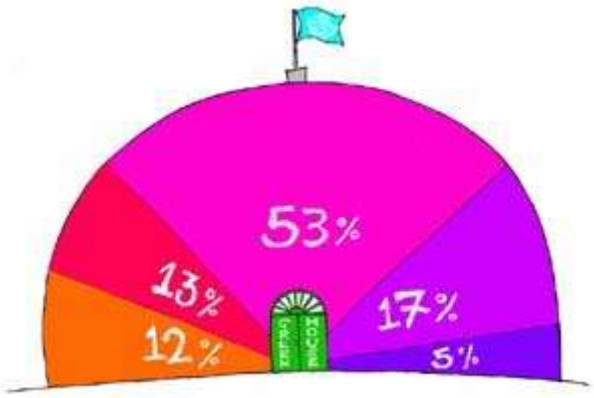
7. แผนผังแนวทางในการจัดทำรายงานการบริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศ



8. **การวิเคราะห์ ประเมินโอกาสที่จะเกิดขึ้นของความเสี่ยงและผลกระทบ**

1) โอกาส (Probability) ความเสี่ยงที่จะเกิดขึ้น ได้แก่ รวบรวมความเสี่ยง ซึ่งสามารถจำแนกเป็นกลุ่มใหญ่ ๆ จำแนกโอกาสตามระดับที่คาดว่าความเสี่ยงต่าง ๆ นั้นจะเกิดขึ้นต่อระบบระบบฐานข้อมูลสารสนเทศ

2) ผลกระทบ (Impact) จากผลการประเมินโอกาสของความเสี่ยงที่จะเกิดขึ้นต่อระบบฐานข้อมูล สารสนเทศ จะเห็นได้ว่าความเสี่ยงนั้นจะส่งผลกระทบตามมาและสร้างความเสียหายต่อระบบฐานข้อมูลสารสนเทศในหลายๆ ด้าน ซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกันไป เช่น โอกาสที่จะเกิดความเสี่ยงบ่อยแต่ความรุนแรงมีน้อย อาจจะทำให้ข้อมูลบางส่วนเกิดความเสียหายเล็กน้อย สามารถกู้กลับคืนได้ในเวลาอันรวดเร็ว หรือความเสี่ยงนั้นมีโอกาสเกิดน้อย แต่จะมีผลกระทบรุนแรงสร้างความเสียหายต่อระบบทั้งหมดได้ ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้นก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงานหรือองค์กรนั้น ๆ



9. **การวางแผนกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงและแนวทางปฏิบัติ**

ในการวางแผนเพื่อกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้นนั้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบของแต่ละหน่วยงานเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน / แก้ไข / ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามกลยุทธ์ที่วางแผนไว้ ดังนี้

10. การติดตามสภาวะที่อาจจะเกิดขึ้นของความเสี่ยง

ในขั้นตอนนี้เจ้าหน้าที่ผู้รับผิดชอบจะต้องมีการรวบรวม และรายงานข้อมูลของความเสี่ยงได้อย่างถูกต้องแม่นยำ ทั้งระยะเวลาและข้อมูลที่เกี่ยวข้อง เพื่อนำเสนอให้กับหน่วยงานได้อย่างชัดเจนและเข้าใจง่าย และจะได้มีการบันทึกไว้เป็นหลักฐาน เพื่อประโยชน์ในการเฝ้าติดตามความเสี่ยง /การป้องกัน /การควบคุม /แก้ไขความเสี่ยงที่จะเกิดขึ้นในโอกาสต่อไปได้ โดยลักษณะของความเสี่ยง (Risk attribute)จะเป็นเสมือนตัวชี้วัด (Indication) ของการวางแผนลดความเสี่ยง (Mitigation Plan) นั้นว่ามีผลสัมฤทธิ์หรือไม่ ขั้นตอนหรือวิธีการของแผนลดความเสี่ยงนี้ จะช่วยชี้ให้เห็นว่าการประเมินความเสี่ยงนั้นดำเนินไปอย่างถูกต้องและทันเวลาหรือไม่ ในขณะที่การเฝ้าติดตามลักษณะของความเสี่ยงนั้นจะชี้ให้เห็นว่าหากเป็นไปตามความคาดหมายอย่างถูกต้องแล้ว การประเมินผลความเสี่ยงที่ช่วยลดความเสี่ยงลงนั้น ย่อมที่จะสามารถลดผลกระทบหรือโอกาสการเกิดความเสี่ยงให้น้อยลง

11. ติดตาม กำกับและตรวจสอบการปฏิบัติการควบคุมความเสี่ยง

การติดตาม กำกับและตรวจสอบผลของการดำเนินการว่าได้มีการปฏิบัติจริงหรือไม่ตามรายการประเมินผลความเสี่ยงที่ได้กำหนดไว้ ทั้งนี้เจ้าหน้าที่ผู้ได้รับมอบหมายจะต้องมีการติดตามความเสี่ยงอย่างสม่ำเสมอ และมีการรายงานให้ผู้บังคับบัญชาทราบ เพื่อให้ทราบว่าจะมีปัญหาหรืออุปสรรคอะไรเกิดขึ้นหรือไม่ และถ้ามีอุปสรรคๆจะได้มีการแก้ไขปัญหาหรืออุปสรรคนั้นๆ เพื่อให้ทุกขั้นตอนได้ดำเนินไปตามแผนและบรรลุเป้าหมายในการควบคุมความเสี่ยงต่อไป

หมายเหตุ : เกณฑ์การให้คะแนนโอกาสที่จะเกิดและผลกระทบจากต่ำไปสูงคือ 1 ถึง 5

1. = รุนแรงน้อยที่สุด/โอกาสที่จะเกิดน้อยที่สุด
2. = รุนแรงน้อย/โอกาสที่จะเกิดน้อย
3. = รุนแรงปานกลาง/โอกาสที่จะเกิดปานกลาง
4. = รุนแรงมาก/โอกาสเกิดมาก
5. = รุนแรงมากที่สุด/โอกาสที่จะเกิดมากที่สุด

การวิเคราะห์ ประเมินโอกาสที่จะเกิดขึ้นของความเสี่ยงและผลกระทบของฐานข้อมูลสารสนเทศ ศูนย์บริการวิชาการ ประจำปีงบประมาณ 2553

ที่มาของความเสี่ยง	ปัจจัยเสี่ยง	ผลกระทบ	โอกาสที่จะเกิด
1. ด้านบุคลากร	1) ด้านความปลอดภัย(Security) และการเข้าถึงข้อมูล (Access Risk)ของระบ บฐานข้อมูลสารสนเทศ อันเนื่องมาจาก ผู้ที่ไม่เกี่ยวข้องเข้ามาใช้ระบบฐานข้อมูลสารสนเทศ ซึ่งอาจสร้างความเสียหายแก่ระบบฐานข้อมูลสารสนเทศ	1) สร้างความเสียหายแก่ระบบฐานข้อมูล สารสนเทศ และระบบ Software ,Hard ware 2) สิ้นเปลืองงบประมาณในการจัดซื้อหรือซ่อมบำรุง 3) ระบบฐานข้อมูลไม่สามารถให้บริการได้	3
2. ความเสี่ยงอันเนื่องมาจากภัยพิบัติ (Contingency Plan)	1. กรณีกระแสไฟฟ้ามีปัญ หา (power supply failure or fluctuations) เช่น ไฟฟ้าตก ไฟฟ้าดับ (Blackout) ไฟฟ้ากระชาก (Spike) ไฟฟ้าเกิน (Surge) หรือ สัญญาณรบกวน (Noise)	1) อุปกรณ์จัดเก็บฐานข้อมูล (Server) เสียหาย 2) การเชื่อมโยงเครือข่ายล้มเหลว ระบบไม่สามารถใช้งานได้ 3) สิ้นเปลืองงบประมาณในการจัดซื้อและซ่อมบำรุง 4) เสียเวลาในการจัดทำฐานข้อมูลใหม่	4

แผนการบริหารความเสี่ยงของระบบฐานข้อมูลสารสนเทศศูนย์บริการวิชาการ ประจำปีงบประมาณ 2553

ประเด็น	การดำเนินงาน	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
1. ความเสี่ยงทางกายภาพ (Physical) 1) ด้านบุคลากร เพื่อป้องกันผู้ที่ไม่เกี่ยวข้องเข้ามาใช้ระบบฐานข้อมูลสารสนเทศ ซึ่งอาจสร้างความเสียหายแก่ระบบฐานข้อมูลสารสนเทศ	1. การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย ระบบฐานข้อมูลสารสนเทศ และอุปกรณ์ของผู้รับผิดชอบจะต้องทำการใส่บัญชีผู้ใช้ (Username) และ/หรือรหัสผ่าน (Password) เพื่อสร้างความปลอดภัยให้กับระบบปฏิบัติการและระบบเซิร์ฟเวอร์แม่ข่าย	ก.ย.52-ต.ค.53	ส่วนสารสนเทศ
2. ความเสี่ยงด้านความปลอดภัย (Security) และการเข้าถึงข้อมูล (Access Risk)ของระบ บฐานข้อมูลสารสนเทศ	1. กำหนดผู้รับผิดชอบ เช่น นักสารสนเทศ เจ้าหน้าที่ดูแลระบบ และเจ้าหน้าที่พัฒนาระบบงาน 2. ใส่บัญชีผู้ใช้(Username) และ รหัสผ่าน (Password) 3. กำหนดสิทธิให้ผู้ใช้แต่ละระดับ (Access rights) มีระบบรักษาความปลอดภัยและสามารถตรวจสอบผู้เข้าใช้ระบบได้ ดังนี้ - Guests คือกลุ่มผู้ใช้ทั่วไปสามารถอ่านข้อมูลได้อย่างเดียว - Users คือกลุ่มที่สามารถอ่านและแก้ไขข้อมูลได้โดยกำหนดขอบเขตการเข้าถึงข้อมูล - Admin คือผู้ดูแลระบบสามารถปรับปรุงแก้ไขได้ 4. จัดให้มีระบบสำรองฐานข้อมูล มีการจัดทำระบบสำรองข้อมูลไว้ตามวงรอบที่กำหนดไว้ โดยมีการจัดทำในระบบ Manual โดยมี	ก.ย.52-ต.ค.53	ส่วนสารสนเทศ

ประเด็น	การดำเนินงาน	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
	การกำหนดให้มีการสำรองข้อมูล (Backup) ฐานข้อมูล ตามระยะเวลา และติดตั้ง Soft ware Server Back Up เพื่อทำการสำรองข้อมูลให้ปลอดภัยและเหมาะสม 5. กำหนดมาตรการป้องกันไวรัส สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง มีวิธีการ ดังนี้ • ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม และอัพเดตข้อมูลไวรัสอยู่เสมอ • ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์ • ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆที่น่าไม่รู้ที่มา • อย่าเปิดไฟล์ E-Mail จากผู้ที่ไม่ทราบที่มา • มีการป้องกันจากการดาวน์โหลดจาก Internet • หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น		
3. ความเสี่ยงอันเนื่องมาจากภัย	1. กรณีกระแสไฟฟ้ามีปัญหา (power supply failure or fluctuations)	ก.ย.52-ต.ค.53	ส่วนสารสนเทศ

ประเด็น	การดำเนินงาน	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
พิบัติ Contingency Plan)	เช่น ไฟฟ้าตก ไฟฟ้าดับ (Blackout) ไฟฟ้ากระชาก (Spike) ไฟฟ้าเกิน (Surge) หรือ สัญญาณรบกวน (Noise) ซึ่งมีสาเหตุจากภัยทางธรรมชาติ เช่น ฝนตกหนัก ฝนฟ้าคะนอง พายุ ฟ้าผ่า เป็นต้น ให้รีบทำการบันทึกข้อมูล (Save) และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย (Safety) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นภายในสำนักงานด้วย 2. กรณีการเชื่อมโยงเครือข่ายล้มเหลว เจ้าหน้าที่ผู้รับผิดชอบจะต้องรีบรายงานให้ผู้บังคับบัญชาทราบ และดำเนินการประสานผู้ที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยด่วนที่สุด และให้ใช้การเชื่อมโยงเครือข่ายสำรองแทนการเชื่อมโยงหลักในระหว่างที่ดำเนินการแก้ไข ทั้งนี้หากมีเหตุจำเป็นที่ต้องใช้เวลามากกว่า 1 วัน ในการดำเนินการแก้ไข ให้ออกประกาศแจ้งแก่ผู้ใช้งานทราบ พร้อมกำหนดเวลาที่จะทำการแก้ไขเสร็จสิ้น 3. กรณีที่อุปกรณ์จัดเก็บข้อมูลเสียหายให้เจ้าหน้าที่ผู้รับผิดชอบ ทำการตรวจสอบเหตุแห่งความเสียหายนั้นในเบื้องต้น หากมีแนวทางที่จะทำการกู้คืนข้อมูลในอย่างเร่งด่วน ทั้งนี้อาจประสานงานขอความช่วยเหลือจากผู้ที่ชำนาญในเรื่อง และให้รายงานผู้บังคับบัญชา		
4. การทบทวนแผนเพื่อสร้างความ	1. จัดทำรายงานประเมินผลความเสี่ยงของระบบฐานข้อมูลสารสนเทศ	มี.ค.-ก.ย.53	ส่วนสารสนเทศ

ประเด็น	การดำเนินงาน	ระยะเวลาดำเนินการ	ผู้รับผิดชอบ
ปลอดภัยของระบบฐานข้อมูลสารสนเทศ	และการใช้ประโยชน์ระบบ สารสนเทศเพื่อเป็นข้อมูลประกอบการประเมินผล 2. ทบทวนแผนภายหลังจากที่ได้มีการนำวิธีการเพื่อลดความเสี่ยงมาใช้เพื่อทำการวิเคราะห์ความเสี่ยงและหาวิธีแก้ไขเพิ่มเติม		
5. การพัฒนาระบบฐานข้อมูลสารสนเทศ	1. ให้มีการพัฒนาระบบสารสนเทศของหน่วยงานอย่างต่อเนื่อง 2. พัฒนาด้าน Hardware, Software, Network และ People ware เพื่อเหมาะสมและเกิดประโยชน์สูงสุดกับการปฏิบัติงาน 3. มีมาตรการหรือแนวปฏิบัติในการรักษาความปลอดภัยระบบฐานข้อมูลสารสนเทศ 4. มีการมอบหมายเจ้าหน้าที่ดูแลระบบฐานข้อมูลสารสนเทศ	ก.ย.52-ต.ค.53	ส่วนสารสนเทศ
5. การติดตามเพื่อทราบสภาพวะความเสี่ยง	1. มีการติดตามความเสี่ยงอย่างสม่ำเสมอ และมีการรายงานให้ผู้บังคับบัญชาทราบ ถึงปัญหาหรืออุปสรรคเกิดขึ้นหรือไม่เพื่อให้ทุกขั้นตอนได้ดำเนินไปตามแผนและบรรลุเป้าหมาย	ส.ค.- ต.ค.53	ส่วนสารสนเทศ

มาตรการป้องกัน ควบคุม และจัดการความเสี่ยงของฐานข้อมูลสารสนเทศ

ส่วนสารสนเทศ ศูนย์บริการวิชาการ มีหน้าที่รับผิดชอบระบบฐานข้อมูลสารสนเทศ และมีเจ้าหน้าที่ปฏิบัติงานโดยตรงในการดูแลระบบ ป้องกัน ควบคุมและจัดการความเสี่ยงที่อาจเกิดขึ้น แยกออกเป็น 3 ด้าน คือ

1. ด้านความปลอดภัยของระบบฐานข้อมูลสารสนเทศ
2. ด้านระบบการรักษาความปลอดภัยของระบบเครือข่าย
3. ด้านจัดทำแผนแก้ไขปัญหาจากภัยพิบัติ

เพื่อเป็นการป้องกันมิให้เกิดความเสี่ยงของระบบฐานข้อมูลสารสนเทศศูนย์บริการวิชาการตามที่กล่าวมานั้น ส่วนสารสนเทศได้ดำเนินการวางระบบการควบคุมและการบริหารความเสี่ยง ดังนี้

1. **ด้านความปลอดภัยของระบบฐานข้อมูลสารสนเทศ**

ฐานข้อมูลสารสนเทศศูนย์บริการวิชาการ มีการใช้งานผ่านระบบเครือข่าย Intranet และ Internet โดยมีการบริหารจัดการ และปรับปรุงข้อมูลโดยเจ้าหน้าที่สารสนเทศ ซึ่งมีหน้าที่ดูแล รักษาความปลอดภัย และกำหนดสิทธิ์การเข้าถึงข้อมูลสารสนเทศ ดังนี้

1) ผู้ดูแลระบบ (Admin) สามารถดำเนินการ กำหนดผู้ใช้งาน, ถ่ายโอนข้อมูลระหว่างส่วนงานต่าง ๆ ไปยังเครื่องแม่ข่ายและกำหนดสิทธิ์การเข้าถึงข้อมูลสารสนเทศ
2) ผู้ปฏิบัติ (User) สามารถบันทึก / ลบ / แก้ไข ได้เฉพาะข้อมูลที่ตนเองรับผิดชอบของหน่วยงานเท่านั้น
3) ผู้ใช้งานทั่วไป สามารถเรียกดูรายงานได้อย่างเดียว

2. **ด้านระบบคอมพิวเตอร์และการรักษาความปลอดภัยระบบเครือข่าย**

1) มีระบบป้องกันหรือตรวจสอบตัวตนของผู้ใช้งานก่อนอนุญาตให้เข้าใช้ระบบ โดยระบบงานทุกระบบจะมีการตรวจสอบ User Name และ Password ของผู้เข้าใช้งานทุกครั้งเพื่อเป็นการรักษาความปลอดภัยของระบบสารสนเทศของหน่วยงาน
2) มีการควบคุมการแชร์ไฟล์ หรือข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์ โดยการกำหนดรหัสผ่านและกำหนดสิทธิในการแชร์ไฟล์ เพื่อลดการแพร่กระจายไวรัสและเป็นการรักษาความปลอดภัยของข้อมูลที่อยู่ในเครื่องเหล่านั้น

3) การป้องกันไวรัส ติดตั้งโปรแกรมตรวจจับไวรัสที่เครื่องคอมพิวเตอร์แม่ข่ายและลูกข่ายทุกเครื่อง พร้อมทั้งติดตั้งโปรแกรม Anti Spy ware ต่าง ๆ หรือการป้องกันไม่ให้ข้อมูลถูกทำลายเสียหาย และเป็นการรักษาความปลอดภัยของข้อมูลจากผู้บุกรุก นอกจากนี้ยังมีการแนะนำการตรวจสอบไวรัสและการกำจัดไวรัสให้กบเจ้าหน้าที่และบุคลากรเพื่อให้มีความรู้และสามารถปฏิบัติการป้องกันไวรัสที่จะเกิดขึ้นจากการปฏิบัติงาน ติดตั้งโปรแกรม Anti Virus และมีการปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ โดยกำหนดโปรแกรมสามารถ Update ตัวเองได้อย่างอัตโนมัติ

4) การสำรองข้อมูลและโปรแกรม (Back Up) มีการสำรองข้อมูล (Back Up) ฐานข้อมูลของระบบงานต่าง ๆ เก็บไว้ให้สามารถนำกลับมาใช้งานได้อย่างถูกต้องครบถ้วน

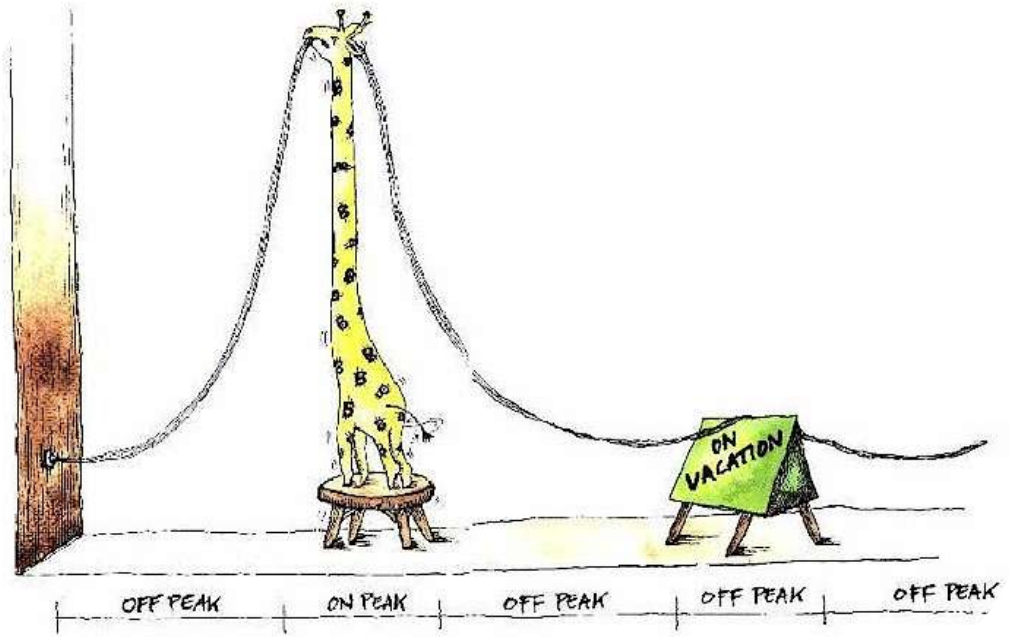
3. ด้านภัยพิบัติจากสถานการณ์ความไม่แน่นอน

1) ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า เช่น ไฟฟ้าตก ไฟฟ้าดับ (Blackout) ไฟฟ้ากระชาก (Spike) ไฟฟ้าเกิน (Surge) หรือ สัญญาณรบกวน (Noise) ซึ่งมีสาเหตุจากภัยทางธรรมชาติ เช่น ฝนตกหนัก ฝนฟ้าคะนอง พายุ ฟ้าผ่า เป็นต้น

2) กรณีไฟฟ้าดับ ให้รีบทำการบันทึกข้อมูล (Save) และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย (Safety) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นภายในสำนักงานด้วย

ปัจจัยที่ทำให้ระบบบริหารความเสี่ยงประสบผลสำเร็จ

1. แรงผลักดันจากผู้บริหารหน่วยงานที่ให้ความสนับสนุนทุกด้าน
2. เทคโนโลยีและสารสนเทศที่ช่วยในการจัดเก็บข้อมูล การส่งถ่ายข้อมูลและการตรวจสอบย้อนกลับได้อย่างรวดเร็ว
3. ความร่วมแรงร่วมใจของบุคลากรภายในศูนย์ บริการวิชาการ ที่จะผลักดันให้การบริหารความเสี่ยงประสบผลสำเร็จ



บทสรุป

ความจริงประการหนึ่งที่ควรทราบคือ เราไม่สามารถที่จะกำจัดความเสี่ยงให้หมดไปได้ทั้ง 100 % เราไม่อาจหลีกเสี่ยงความเสี่ยงได้เสมอไปในทุกสถานการณ์ แต่การ มีระบบบริหารความเสี่ยงจะช่วยในการค้นหา ลดระดับความรุนแรง การควบคุมและป้องกันความเสี่ยงต่าง ๆ ลงไปได้ระดับหนึ่ง อย่างน้อยก็ช่วยให้เรามีความตื่นตัวและปฏิบัติงานด้วยความระมัดระวังอยู่เสมอ ระบบบริหารความเสี่ยงของฐานข้อมูลสารสนเทศศูนย์บริการวิชาการนี้ นอกจากจะช่วยบริหารงานใน หน่วยงาน ให้มีประสิทธิภาพมากขึ้นแล้ว ยังสามารถประยุกต์ใช้กับงานอื่น ๆ ได้ การตระหนักถึงความผิดพลาดและเตรียมแผนรองรับก่อนที่จะเกิดขึ้น ย่อมดีกว่าการแก้ไขปัญ หาที่ปลายเหตุ ซึ่งอาจจะตัดสินใจผิดพลาดและไม่ทันต่อเหตุการณ์ทำให้เสียค่าใช้จ่ายและทรัพยากรโดยไม่จำเป็น

บุคลากรส่วนสารสนเทศ

นางวิภาดา มีแวว

หัวหน้าส่วนสารสนเทศ

นางสาวศิโรรัตน์ กุลวงศ์

เจ้าหน้าที่บริหารงานทั่วไป

นายประหยัด สืบเมืองซ้าย

นักสารสนเทศ