การพัฒนาระบบ การประเมินผลการควบคุมภายในตามมาตรฐาน COSO
กรณีศึกษา : ฝ่ายเทคโนโลยีสารสนเทศ

รัตนา ไพรศรี

งานค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2552

The Development of Control Self Assessment System with COSO Standard

Case Study: Information Technology Department

Rattana Prisree

An Independent Study Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science (Computer and Communication Technology)

Department of Computer and Communication Technology

Graduate School, Dhurakij Pundit University

2009

กิตติกรรมประกาศ

งานค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงได้ด้วยดีนั้น ต้องขอขอบพระคุณอาจารย์ที่ปรึกษางานค้นคว้าอิสระ ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์ ที่กรุณา แนะนำความรู้และสิ่งที่เป็นประโยชน์อย่างเอนกประการในการช่วยปรับปรุงงานค้นคว้าอิสระฉบับนี้

ขอขอบพระคุณท่านอาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้แก่ข้าพเจ้า

ขอกราบขอบพระคุณบิดามารดา ญาติพี่น้องทุกคน และน้อมระลึกถึงผู้มีพระคุณทุกคนที่ทำให้ข้าพเจ้ามีวันนี้ และขออุทิศความดีทั้งหลายของงานค้นคว้าอิสระฉบับนี้แก่ ผู้มีพระคุณทุกท่าน

ผู้วิจัยหวังเป็นอย่างยิ่งว่า งานค้นคว้าอิสระฉบับนี้ จะเป็นประโยชน์กับผู้ที่ต้องการศึกษาด้านระบบการประเมินผลระบบการควบคุมภายในภายในองค์กร และหากมีข้อผิดพลาดประการใดในงานค้นคว้าอิสระฉบับนี้ ผู้วิจัยต้องกราบขออภัยเป็นอย่างสูงมา ณ ที่นี้ด้วย

รัตนา ไพรศรี

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

หัวข้องานค้นคว้าอิสระ การพัฒนาระบบการประเมินผลการควบคุมภายในตามมาตรฐาน COSO กรณีศึกษา : ฝ่ายเทคโนโลยีสารสนเทศ

ชื่อผู้เขียน รัตนา ไพรศรี

อาจารย์ที่ปรึกษางานค้นคว้าอิสระ ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์

สาขาวิชา เทคโนโลยีคอมพิวเตอร์และการสื่อสาร

ปีการศึกษา 2552

บทคัดย่อ

งานค้นคว้าอิสระ การพัฒนาระบบการประเมินผลการควบคุมภายในตามมาตรฐาน COSO กรณีศึกษา : ฝ่ายเทคโนโลยีสารสนเทศ เป็นการจัดทำระบบการจัดการความเสี่ยงในองค์กร โดยใช้ฝ่ายเทคโนโลยีสารสนเทศเป็นต้นแบบ ในการจัดทำการประเมินความเสี่ยงตามมาตรฐาน COSO เพื่อให้พนักงานในองค์การมีการจัดทำกระบวนการจัดการประเมินความเสี่ยง ใน 7 ขั้นตอนได้แก่ ขั้นตอนที่ 1 สภาพแวดล้อมการควบคุมภายใน ขั้นตอนที่ 2 การกำหนดวัตถุประสงค์ ขั้นตอนที่ 3 การระบุความเสี่ยง ขั้นตอนที่ 4 การประเมินความเสี่ยง ขั้นตอนที่ 5 การจัดการความเสี่ยง ขั้นตอนที่ 6 กิจกรรมการควบคุม และขั้นตอนที่ 7 การติดตามประเมินผล

การพัฒนาระบบในลักษณะการทำงานแบบ Client-Server ร่วมกับการทำงานในระบบ Web-based โดยนำเสนอผ่านทางระบบออนไลน์ที่ใช้งานภายในองค์กร เพื่อเผยแพร่ข้อมูลที่เกี่ยวข้องกับกระบวนการในการจัดทำการประเมินความเสี่ยง แนวทางในการจัดการความเสี่ยง ตามขั้นตอนมาตรฐานของ COSO โดยการประยุกต์ใช้โปรแกรมภาษา HTML (Hypertext Markup Language) ร่วมกับภาษาคริปท์ ASP (Active Server Page) และระบบจัดการฐานข้อมูล Microsoft Access

ผลจากการจัดทำหน้าเว็บเพจระบบการประเมินผลการควบคุมภายใน สามารถทำการประเมินผลการควบคุมภายในผ่านระบบต้นแบบการประเมินผลระบบการควบคุมภายใน และยังสามารถจัดการความเสี่ยงและสร้างแนวคิดในการจัดทำ และกระบวนการในการประเมินความเสี่ยงภายในระดับฝ่ายงานย่อย พนักงานในองค์เกิดการเรียนรู้ ตระหนักถึงความสำคัญของการบริหารความเสี่ยง โดยมีกรณีศึกษาของฝ่ายเทคโนโลยีสารสนเทศเป็นต้นแบบ

Independent Study Title The Development of Control Self Assessment System with COSO Standard
Case Study: Information Technology Department

Author Rattana Prisree

Independent Study Advisor Assistant Professor Dr.Pranot Boonchai-Apisit

Department Computer and Communication Technology

Academic Year 2009

ABSTRACT

An independent study, the Development of Control Self Assessment System with COSO Standard, Case Study: Information Technology Department, is a system of risk management in organizations using an Information Technology department as a model. In conducting COSO risk assessment standard to employees in organizations, there are risk assessment management processes in 7 steps, as follows: control the environment, set purposes, identify risk, assess risk, risk management, control activities, and evaluation tracking.

The development is based on Client/Server architecture and web technology, and implemented on organization Intranet. The system publishes information related to the processes conducting risk assessment, and an approach to risk management according to COSO standards. The application is developed by HTML (Hypertext Markup Language), ASP (Active Server Page), and Microsoft Access.

This independent study therefore looks at a main result is people within the organization have been involved in critical thinking. Expectations of events or risks that may arise, and identify how to manage these risks at a level appropriate or acceptable to help organization achieve the desired objectives. If the organization is managing risks effectively, it will contribute to achieve corporate objectives in both performance and efficiency.

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

บริษัทบริหารสินทรัพย์กรุงเทพพาณิชย์ จำกัด (บสก.) ตระหนักถึงความสำคัญในการดำเนินงานที่มีการกำกับดูแลกิจการที่ดี อันเป็นปัจจัยหลักในการเสริมสร้างองค์กรให้มีมาตรฐานการจัดการ และจริยธรรมทางธุรกิจที่ดี สร้างความเชื่อมั่นให้กับลูกค้าและสาธารณชน ว่ากระบวนการดำเนินงานของ บสก. มีความเป็นอิสระ โปร่งใส มีประสิทธิภาพและยุติธรรมต่อทุกฝ่ายที่เกี่ยวข้อง ซึ่งจะส่งผลให้ บสก. ได้รับการยอมรับว่ามีความน่าเชื่อถือและเป็นการส่งเสริมความเข้มแข็งในการดำเนินธุรกรรมของ บสก. และจะนำพาองค์กรให้สามารถบรรลุเป้าหมายของการเจริญเติบโตอย่างมั่นคงและยั่งยืนโดย บสก. ได้กำหนดหลักบรรษัทภิบาลไว้ 7 ประการ ดังนี้

1. มีความสำนึก และเข้าใจในหน้าที่ (Responsibility) มีความสามารถในการปฏิบัติหน้าที่ตามภารกิจได้เป็นอย่างดียิ่ง พร้อมกับการที่ต้องเรียนรู้สิ่งใหม่ๆ อยู่เสมอ มีความรักงาน มุ่งมั่นที่จะทำงานให้มีคุณภาพเกิดผลสำเร็จ ได้ผลงานที่มีคุณภาพยิ่งขึ้น

2. แสดงความยอมรับผิดและรับชอบต่อผลการปฏิบัติหน้าที่ (Accountability)

3. มีการปฏิบัติต่อผู้มีส่วนได้เสียงอย่างเท่าเทียมยุติธรรม (Equitable Treatment)

4. มีความโปร่งใสในการดำเนินงาน (Transparency) และการเปิดเผยข้อมูลอย่างพอเพียง สามารถอธิบายได้ ตรวจสอบได้

5. มีการกำหนดวิสัยทัศน์ (Vision) กลยุทธ์ และความมุ่งมั่นขององค์กร (Strategic Intent) ในการดำเนินการที่ชัดเจน โดยมุ่งเน้นให้สามารถบรรลุวัตถุประสงค์ขององค์กรในระยะยาว

6. มีการกำหนดแนวทางการปฏิบัติที่ดี ส่งเสริมการปฏิบัติอันเป็นเลิศ และการมีจริยธรรมที่ดีในการประกอบธุรกิจ (Promotion of Best Practices) รวมถึงสร้างวัฒนธรรมองค์กร (Corporate Culture) จริยธรรม (Code of Ethic and Business Conduct) และคุณธรรมอันรวมถึงความซื่อสัตย์ (Integrity) ในการปฏิบัติงาน

7. สำนึกในความรับผิดชอบที่พึงมีต่อสังคม (Social awareness)

บสก. เป็นองค์กร ที่มีความเชื่อมั่นว่าการมีระบบบริหารความเสี่ยงที่มีประสิทธิภาพและประสิทธิผลที่ดี จะมีส่วนช่วยผลักดันให้ การดำเนินการขององค์กร เป็นไปตามนโยบายของรัฐบาลและคณะกรรมการรัฐวิสาหกิจ เรื่องการวางแผนการบริหารกิจการที่ดี ดังนั้น บสก.ได้เล็งเห็นความสำคัญของการจัดทำระบบการบริหารจัดการความเสี่ยงโดยมีจุดมุ่งหมายที่จะบริหารจัดการความเสี่ยงขององค์กรให้เป็นไปตามแผนการบริหารจัดการความเสี่ยงที่ได้จัดทำขึ้น และสามารถนำไปปฏิบัติและประยุกต์ใช้งานได้จริงทั้งในระดับองค์กรและระดับหน่วยงาน พร้อมทั้งมีการวางกรอบนโยบายการดำเนินการด้านบริหารความเสี่ยงเพื่อให้มีการพัฒนางานด้านการบริหารความเสี่ยงอย่างยั่งยืนตามลำดับ การพัฒนางานด้านการบริหารความเสี่ยง

ซึ่งระเบียบคณะกรรมการตรวจเงินแผ่นดินว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน พ.ศ. 2544 กำหนดให้หน่วยงานของภาครัฐนำมาใช้ เพื่อปรับปรุงการควบคุมภายในให้มีประสิทธิผล และเหมาะสมกับสภาพแวดล้อมและความเปลี่ยนแปลงไปอยู่เสมอ โดยมาตรฐานดังกล่าวสามารถนำมาใช้เป็นแนวทางหนึ่งในการพิจารณาบริหารจัดความเสี่ยงภายในระดับฝ่ายงานย่อยไปจนถึงระดับองค์กรได้ ตามที่มาและความสำคัญของปัญหาดังกล่าวข้างต้นทำให้ผู้วิจัยสนใจทำการศึกษานำมาตรฐานดังกล่าวมาทำการพัฒนาเป็นระบบต้นแบบเพื่อประโยชน์ใช้งานภายในองค์กร

1.2 วัตถุประสงค์ของการวิจัย

วัตถุประสงค์ของการวิจัย มีดังต่อไปนี้

1. เพื่อสร้างเครื่องมือสำหรับการให้ความรู้งานด้านการจัดการความเสี่ยง แก่ผู้บริหารบริหารงานและปฏิบัติงานด้านบริหารความเสี่ยงของ บสก.
2. เพื่อสร้างเครื่องมือสำหรับการสื่อสารและสร้างความเข้าใจ ความสัมพันธ์ ตลอดจนเชื่อมโยงการบริหารความเสี่ยงกับกลยุทธ์ขององค์กร
3. เพื่อใช้สร้างเครื่องมือสำหรับกำหนดแนวทางการจัดการความเสี่ยง สำหรับหน่วยงานทุกระดับของ บสก.

1.3 ขอบเขตของการวิจัย

ขอบเขตของการวิจัย มีดังต่อไปนี้

1. จัดทำระบบต้นแบบการจัดการความเสี่ยงในองค์กร โดยใช้ฝ่ายเทคโนโลยีสารสนเทศเป็นต้นแบบ ในการจัดทำการประเมินความเสี่ยงตามมาตรฐาน COSO
2. จัดทำกระบวนการจัดการประเมินความเสี่ยง
3. สนับสนุนการการจัดการความเสี่ยงระดับส่วนงานย่อยในการจัดทำการประเมินความเสี่ยงผ่านทางระบบออนไลน์ขององค์กร

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับ มีดังต่อไปนี้

1. เป็นการพัฒนาระบบต้นแบบการประเมินผลการควบคุมภายใน เพื่อการประเมินความเสี่ยงภายในองค์กร
2. สร้างความตระหนักให้กับบุคคลในองค์กรถึงความสำคัญของการจัดการความเสี่ยง โดยใช้ฝ่ายเทคโนโลยีสารสนเทศเป็นกรณีศึกษา ให้มากขึ้น
3. การบันทึกข้อมูลและการส่งข้อมูลการประเมินผลการควบคุมภายใน ระหว่างสำนักงานใหญ่และสำนักงานจังหวัดมีความสะดวก เนื่องจากสามารถทำรายการผ่านระบบอินทราเน็ตขององค์กรได้
4. สามารถสร้างฐานข้อมูลเพื่อนำไปพัฒนาระบบงานด้านความเสี่ยงต่อไป

บทที่ 2
แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

2.1 บริษัทบริหารสินทรัพย์กรุงเทพพาณิชย์จำกัด (บสก.)

2.1.1 วิสัยทัศน์องค์กร

บสก.จะมุ่งสู่การเป็นองค์กรหลักในการบริหารจัดการสินทรัพย์ด้อยคุณภาพอย่างมีประสิทธิภาพและพึ่งพาตนเองได้ วิสัยทัศน์ของบสก. แบ่งได้หลักๆ ดังนี้

1. เป็นองค์กรหลักในการบริหารจัดการสินทรัพย์ด้อยคุณภาพ (NPL และ NPA)
2. เป็นองค์กรที่มีระบบการบริหารจัดการแบบธรรมาภิบาล
3. เป็นองค์กรที่มุ่งพัฒนาและส่งเสริมบุคลากรให้มีคุณภาพ
4. เป็นองค์กรที่มีส่วนร่วมในการพัฒนาเศรษฐกิจและสังคมไทย

บสก. มุ่งหวังที่จะเป็นเครื่องมือสำคัญของภาครัฐ ในการบริหารจัดการสินทรัพย์ด้อยคุณภาพ โดยมีส่วนช่วยเหลือลูกหนี้ และแก้ไขปัญหาสถาบันการเงิน ช่วยฟื้นฟูธุรกิจอสังหาริมทรัพย์ โดยการพัฒนาทรัพย์สินรอการขายที่มีศักยภาพ ให้เป็นสินค้าที่ได้มาตรฐานเป็นที่ต้องการของตลาดมากยิ่งขึ้น

บสก. มีความพร้อมที่จะเสนอตัวเข้าไปรับจัดการบริหารหนี้ด้อยคุณภาพจากสถาบันการเงินทุกแห่ง ให้สมกับเป็นองค์กร มืออาชีพในการบริหารจัดการ NPL/NPA และมุ่งมั่นที่จะก้าวสู่การเป็นบริษัทบริหารสินทรัพย์ที่ดีที่สุดแห่งหนึ่งของประเทศ

2.1.2 ความเป็นมา

บริษัทบริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด (บสก.) จัดตั้งขึ้นตามแผนฟื้นฟูระบบสถาบันการเงินของกระทรวงการคลัง ตามมติคณะรัฐมนตรีเมื่อวันที่ 14 สิงหาคม 2541 ซึ่งมีทุนจดทะเบียน 54,700 ล้านบาท ต่อมาลดทุนจดทะเบียนลงจากมูลค่าหุ้นละ 100 บาท เหลือหุ้นละ 25 บาท ทำให้ปัจจุบัน บสก. คงเหลือทุนจดทะเบียน 13,675 ล้านบาท โดยมีวัตถุประสงค์ในการจัดตั้งเพื่อบริหารจัดการสินทรัพย์ด้อยคุณภาพของธนาคารกรุงเทพฯ พาณิชย์การ จำกัด (มหาชน) (BBC) ซึ่ง บสก. ได้จดทะเบียนเป็นบริษัทจำกัด ตามประมวลกฎหมายแพ่งและพาณิชย์ และได้รับอนุญาตจากธนาคารแห่งประเทศไทยให้ประกอบกิจการเป็นบริษัทบริหารสินทรัพย์ ตามพระราชกำหนดบริษัทบริหารสินทรัพย์ พ.ศ. 2541 เมื่อวันที่ 28 มกราคม 2542 มีสถานภาพเป็นรัฐวิสาหกิจที่มีกองทุนเพื่อการฟื้นฟูและพัฒนาระบบสถาบันการเงินเป็นผู้ถือหุ้นโดยตรงของบริษัท

นอกจากภารกิจในการบริหารจัดการสินทรัพย์ด้อยคุณภาพของ BBC แล้ว บสก. ยังได้จดทะเบียนเพิ่มขอบเขตในการบริหารสินทรัพย์ด้อยคุณภาพของสถาบันการเงินอื่น การเป็นตัวแทนเรียกเก็บและชำระหนี้ตามพระราชกำหนดบรรษัทบริหารสินทรัพย์ไทย พ.ศ. 2544 และรับฝากดูแลบริหารจัดการเก็บรักษาทรัพย์สิน เอกสารการโอนสินทรัพย์หรือเอกสารอื่นใดในส่วนที่เกี่ยวข้องทั้งหมด นอกจากนั้น บสก. ยังเพิ่มขนาดสินทรัพย์โดยการรับซื้อ/รับโอนสินทรัพย์ด้อยคุณภาพ (NPL) จากสถาบันการเงินอื่นเพิ่มเติม ซึ่งในปัจจุบันมีสินทรัพย์ด้อยคุณภาพจากแหล่งที่มา 8 แห่ง คือ จากธนาคารกรุงเทพฯพาณิชย์ จำกัด (BBC) บริษัทบริหารสินทรัพย์ พญาไท จำกัด (PAMC) บริษัทบริหารสินทรัพย์ รัตนสิน จำกัด (RAM) ธนาคาร สแตนดาร์ดชาร์ดเตอร์ด นครธน จำกัด (มหาชน) (SCNB) ปัจจุบันเปลี่ยนชื่อเป็น ธนาคาร สแตนดาร์ดชาร์เตอร์ด (ไทย) จำกัด (มหาชน) (SCBT) ธนาคารอาคารสงเคราะห์ (GHB) ธนาคารไทยธนาคาร (BT) บรรษัทบริหารสินทรัพย์สถาบันการเงิน (AMC) และบริษัทบริหารสินทรัพย์ ออมทรัพย์ จำกัด (AMC-S) และยังมีทรัพย์สินรอการขาย (NPA) ที่อยู่ในความดูแลของ บสก. อีก 11,308 รายการ มูลค่า 37,391 ล้านบาท

เมื่อวันที่ 20 ธันวาคม 2548 คณะรัฐมนตรีได้มีมติให้ บรรษัทบริหารสินทรัพย์สถาบันการเงิน (บบส.) โอนขายสินทรัพย์หลัก ได้แก่ เงินลงทุนในลูกหนี้ ทรัพย์สินรอการขาย และเงินลงทุนในหลักทรัพย์ทั้งหมด ให้แก่ บสก. รวมทั้งให้ บสก. รับโอนพนักงานของ บบส. มายัง บสก. ตามความสมัครใจอีกด้วย การรวมกิจการครั้งนี้ ส่งผลให้องค์กรมีความแข็งแกร่งยิ่งขึ้น เนื่องจากได้รวมศักยภาพของพนักงานและระบบงานของทั้งสององค์กรไว้ด้วยกัน อีกทั้ง บสก. ยังมีสำนักงานต่างจังหวัดถึง 24 แห่งทั่วประเทศ ซึ่งจะเป็นเครือข่ายในการรองรับลูกค้าทั้งด้านการปรับโครงสร้างหนี้ และการจำหน่ายทรัพย์สินรอการขายอย่างครบวงจร

นับตั้งแต่ก่อตั้ง บสก. ขึ้นมาในปี 2542 สามารถสร้างผลงานได้สูงกว่าเป้าหมายที่วางไว้ โดยผลการดำเนินงานระหว่างปี 2542 – 2549 บสก. สามารถเจรจาปรับโครงสร้างหนี้จนได้ข้อยุติและมีผลเรียกเก็บที่เป็นเงินสด 57,973 ล้านบาท และรับโอนทรัพย์ชำระหนี้ 14,335 ล้านบาท รวมยอดผลการดำเนินงานทั้งสิ้น 72,308 ล้านบาท

บสก. มีความภูมิใจที่ได้เป็นหนึ่งในองค์กรของรัฐที่มีบทบาทสำคัญในการบริหารจัดการสินทรัพย์ด้อยคุณภาพในระบบสถาบันการเงิน ได้มีโอกาสช่วยเหลือลูกหนี้ที่สุจริตให้พ้นจากการเป็นหนี้ด้อยคุณภาพ อีกทั้ง ยังทำให้ธนาคารพาณิชย์สามารถทำธุรกรรมปกติต่อไปได้อย่างคล่องตัว และไม่ต้องพะวงกับการแก้ไขปัญหา NPL/NPA รวมทั้ง ธนาคารพาณิชย์ยังไม่จำเป็นต้องตั้งบริษัทบริหารสินทรัพย์ของตนเองให้เป็นภาระ เมื่อ NPL/NPA ได้รับการดูแลแก้ไข ก็จะส่งผลให้ระบบเศรษฐกิจโดยรวมสามารถขับเคลื่อนต่อไปข้างหน้าได้อย่างยั่งยืน

2.1.3 การกำกับดูแลที่ดี

บสก. ตระหนักถึงความสำคัญในการดำเนินงานที่มีการกำกับดูแลกิจการที่ดี อันเป็นปัจจัยหลักในการเสริมสร้างองค์กรให้มีมาตรฐานการจัดการ และจริยธรรมทางธุรกิจที่ดี สร้างความเชื่อมั่นให้กับลูกค้าและสาธารณชน ว่ากระบวนการดำเนินงานของ บสก. มีความเป็นอิสระ โปร่งใส มีประสิทธิภาพและยุติธรรมต่อทุกฝ่ายที่เกี่ยวข้อง ซึ่งจะส่งผลให้ บสก. ได้รับการยอมรับว่ามีความน่าเชื่อถือและเป็นการส่งเสริมความเข้มแข็งในการดำเนินธุรกรรมของ บสก. และจะนำพาองค์กรให้สามารถบรรลุเป้าหมายของการเจริญเติบโตอย่างมั่นคงและยั่งยืนต่อไป

โครงสร้างของ บสก. มีกลไกการตรวจสอบและถ่วงดุลอำนาจ มีการแบ่งอำนาจหน้าที่ระหว่าง คณะกรรมการบริษัท คณะกรรมการบริหาร และฝ่ายจัดการอย่างชัดเจน โดย บสก. ได้กำหนดหลักบรรษัทภิบาลไว้ 7 ประการ ดังนี้

1. มีความสำนึก และเข้าใจในหน้าที่ (Responsibility) มีความสามารถในการปฏิบัติหน้าที่ตามภารกิจได้เป็นอย่างดียิ่ง พร้อมกับการที่ต้องเรียนรู้สิ่งใหม่ๆ อยู่เสมอ มีความรักงาน มุ่งมั่นที่จะทำงานให้มีคุณภาพเกิดผลสำเร็จ ได้ผลงานที่มีคุณภาพยิ่งขึ้น

2. แสดงความยอมรับผิดและรับชอบต่อผลการปฏิบัติหน้าที่ (Accountability)

3. มีการปฏิบัติต่อผู้มีส่วนได้เสียอย่างเท่าเทียมยุติธรรม (Equitable Treatment)

4. มีความโปร่งใสในการดำเนินงาน (Transparency) และการเปิดเผยข้อมูลอย่างพอเพียง สามารถอธิบายได้ ตรวจสอบได้

5. มีการกำหนดวิสัยทัศน์ (Vision) กลยุทธ์ และความมุ่งมั่นขององค์กร (Strategic Intent) ในการดำเนินการที่ชัดเจน โดยมุ่งเน้นให้สามารถบรรลุวัตถุประสงค์ขององค์กรในระยะยาว

6. มีการกำหนดแนวทางการปฏิบัติที่ดี ส่งเสริมการปฏิบัติอันเป็นเลิศ และการมีจริยธรรมที่ดีในการประกอบธุรกิจ (Promotion of Best Practices) รวมถึงสร้างวัฒนธรรมองค์กร (Corporate Culture) จริยธรรม (Code of Ethic and Business Conduct) และคุณธรรมอันรวมถึงความซื่อสัตย์ (Integrity) ในการปฏิบัติงาน

7. สำนึกในความรับผิดชอบที่พึงมีต่อสังคม (Social awareness)

2.1.4 ลักษณะธุรกิจของบสก.

บริษัทบริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด (บสก.) Bangkok Commercial Asset Management Co., Ltd. (BAM) ก่อตั้งขึ้นตามพระราชกำหนด บริษัทบริหารสินทรัพย์ พ.ศ. 2541 โดยจดทะเบียนเป็นบริษัทบริหารสินทรัพย์ในวันที่ 1 เมษายน 2542 มีสถานะเป็นรัฐวิสาหกิจพิเศษที่มีกองทุนเพื่อการฟื้นฟูและพัฒนาระบบสถาบันการเงินเป็นผู้ถือหุ้นทั้งจำนวน บสก. เป็นสถาบันการเงินและนับเป็นบริษัทบริหารสินทรัพย์ในรูปแบบบริษัทจำกัดแห่งแรกในประเทศไทย

บสก. ได้กำหนดนโยบายและแนวทางการปฏิบัติงานขององค์กรไว้ ดังนี้ รับซื้อและรับโอนสินทรัพย์ด้อยคุณภาพจากสถาบันการเงินอื่นมาบริหารจัดการเพิ่มเติม สนับสนุนหรือมีส่วนร่วมกับหน่วยงานของรัฐในการแก้ไขปัญหาสินทรัพย์ด้อยคุณภาพ รวมถึงการบริหารจัดการทรัพย์สินรอการขาย จำหน่ายทรัพย์สินรอการขายและปรับปรุงระบบการบริหารจัดการทรัพย์ให้มีมาตรฐาน พัฒนาและปรับปรุงระบบงานภายในองค์กร

2.2 การบริหารความเสี่ยง (ไพร์ซวอเตอร์เฮาส์คูเปอร์ส,2547 : 1-23)

2.2.1 ภาพรวมของความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ที่มีโอกาสเกิดขึ้นได้ในอนาคตและอาจส่งผลในด้านลบที่ไม่ต้องการ ดังนั้นการตัดสินใจกระทำการใดๆ โดยไม่มีข้อมูล หรือไม่มีการวางแผนใดๆ จึงสามารถกล่าวได้ว่าเป็นการเสี่ยงตัดสินใจในสภาวะของความเสี่ยง

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การระบุความเสี่ยง (Risk Identification) หมายถึง การระบุความเสี่ยงที่องค์กรเผชิญอยู่หรือแฝงอยู่ในกระบวนการทำงาน ซึ่งจะต้องสามารถอธิบายถึงผลกระทบจากความเสี่ยงหรือลักษณะความเสียหายที่เกิดจากความเสี่ยงได้

การประเมินความเสี่ยง (Risk Assessment) หมายถึง การจำแนกและพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact)

- โอกาสที่จะเกิด (Likelihood) เป็นการพิจารณาความเป็นไปได้ที่จะเกิดเหตุการณ์ความเสี่ยงในห้วงเวลาหนึ่ง หรือจะเรียกว่าความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง
- ผลกระทบ (Impact) ระดับหรือขนาดของความรุนแรงของผลเสียที่เกิดขึ้นและมีผลกระทบต่อองค์กร

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่กำหนดขึ้นโดยคณะกรรมการผู้บริหารและพนักงานขององค์กรเพื่อใช้ในการกำหนดกลยุทธ์ของทั้งองค์กร กระบวนการบริหารความเสี่ยงถูกออกแบบมาเพื่อใช้ระบุความเสี่ยงหรือเหตุการณ์ที่อาจจะเกิดขึ้นในอนาคต ที่อาจมีผลกระทบต่อองค์กร และบริหารความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

ซึ่งจะช่วยให้มีความมั่นใจอย่างสมเหตุสมผลว่าองค์กรจะบรรลุวัตถุประสงค์ที่กำหนดไว้ ซึ่งการจัดการความเสี่ยงมีหลายวิธี ดังนี้

1. การยอมรับความเสี่ยง (Risk Acceptance) เป็นการยอมรับความเสี่ยงที่เกิดขึ้นเนื่องจากไม่คุ้มค่าในการจัดการควบคุมหรือป้องกันความเสี่ยง

2. การลด/การควบคุมความเสี่ยง (Risk Reduction) เป็นการปรับปรุงระบบการทำงานหรือการออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิด หรือลดผลกระทบ ให้อยู่ในระดับที่องค์กรยอมรับได้

3. การกระจายความเสี่ยง หรือการโอนความเสี่ยง (Risk Sharing) เป็นการกระจายหรือถ่ายโอนความเสี่ยงให้ผู้อื่นช่วยแบ่งความรับผิดชอบไป

4. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการจัดการกับความเสี่ยงที่อยู่ในระดับสูงมาก และหน่วยงานไม่อาจยอมรับได้ จึงต้องตัดสินใจยกเลิกโครงการ /กิจกรรมนั้นไป

การควบคุม (Control) หมายถึง นโยบาย แนวทาง หรือขั้นตอนปฏิบัติต่างๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ

1. การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก

2. การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อค้นพบข้อผิดพลาดที่เกิดขึ้นแล้ว

3. การควบคุมโดยการชี้แนะ (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ

4. การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

2.2.2 ประเภทความเสี่ยง

การจำแนกประเภทความเสี่ยงตามหลักเกณฑ์ของกระทรวงการคลัง สามารถแบ่งความเสี่ยงออกเป็น 4 ประเภท ดังนี้

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : S) เป็นความเสี่ยงที่เกี่ยวข้องในระดับยุทธศาสตร์ สามารถแบ่งได้ ดังนี้

1.1 Organizational Structure Risk ความเสี่ยงที่เกิดขึ้นจากการปฏิบัติงานอันเนื่องมาจากโครงสร้างองค์กรไม่เหมาะสม ซ้ำซ้อน หรือระบุขอบเขตหน้าที่ความรับผิดชอบไม่ชัดเจน เป็นอุปสรรคต่อการดำเนินธุรกิจ

1.2 Operational Strategic Risk ความเสี่ยงจากการดำเนินงานเกิดจากการวางกลยุทธ์ ประกอบด้วย

- Business Risk : ความเสี่ยงที่เกิดจากการวางกลยุทธ์ (ที่สอดคล้องกับสภาพแวดล้อมทางธุรกิจ ณ ขณะนั้น) แต่มีปัจจัยภายนอกที่เปลี่ยนแปลง ทำให้กลยุทธ์หรือการดำเนินธุรกิจในลักษณะดังกล่าวไม่เหมาะสม ได้แก่ ปัจจัยด้านนโยบายการเงิน การคลัง ภาวะเศรษฐกิจ สถานการณ์การเมือง คู่แข่ง กฎหมาย ภาษี หรือการเปลี่ยนแปลงข้อกำหนดกฎเกณฑ์

- Strategic Risk : ความเสี่ยงที่เกิดจากการวางกลยุทธ์ผิดพลาด ไม่เหมาะสมกับปัจจัยภายนอกที่ใช้พิจารณากำหนดกลยุทธ์

2. ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk : O) เป็นความเสี่ยงความเสี่ยงที่มีโอกาสเกิดความเสียหายโดยตรงหรือโดยอ้อม เนื่องจากการขาดระบบงาน การขาดการควบคุมที่ดี การจัดการภายในล้มเหลวจนทำให้เกิดความสูญเสีย และความผิดพลาดในการปฏิบัติงาน โดยมีสาเหตุต่างๆ ประกอบด้วย

2.1 People Risk ความเสี่ยงที่เกิดขึ้นจากการปฏิบัติงานอันเนื่องจากบุคลากร

- Incompetence : การขาดความรู้ความชำนาญในงานที่รับผิดชอบการ ขาดความสามารถในการทำงานเป็นทีม การละเลยไม่ให้ความสำคัญกับกลุ่มลูกค้า การขาดการทำงานแบบมืออาชีพ รวมทั้งการขาดความสามารถในการวิเคราะห์หรือใช้วิจารณญาณในการตัดสินใจ หรือตีความข้อมูลที่ใช้ในการปฏิบัติงานผิดพลาด ซึ่งทั้งหมดนี้อาจนำไปสู่การปฏิบัติงานที่ผิดพลาด

- Fraud : การทุจริตหรือกระทำผิดจรรยาบรรณ หรือใช้ตำแหน่งหน้าที่ ของตนเพื่อประโยชน์ส่วนตัว

- Human Error : ความผิดพลาดของพนักงานในการปฏิบัติงาน โดยมิได้มีเจตนาจะกระทำผิดหรือทุจริต

- HR Management : การบริหารทรัพยากรบุคคลไม่เหมาะสม เช่น การมีพนักงานมากหรือน้อยเกินไป การด้อยประสิทธิภาพในการสรรหา การมอบหมายไม่ตรงความสามารถ การขาดการอบรมให้พนักงานมีความเชี่ยวชาญหรือเพิ่มขีดความสามารถในการปฏิบัติงาน การขาดเครื่องมือในการสร้างแรงจูงใจและคงพนักงานที่มีความสามารถให้อยู่กับองค์กร การประเมินผลงานที่ไม่ยุติธรรม และค่าตอบแทนที่ไม่เหมาะสม การพึ่งพิงกับพนักงานหลัก (Reliance on Key Individuals)

- Resource Management : การบริหารทรัพยากรขององค์กรไม่เหมาะสม เช่น ไม่มีอุปกรณ์ที่ให้ความสะดวก หรือมีไม่เพียงพอต่อความจำเป็นในการปฏิบัติงาน อุปกรณ์ไม่อยู่ใน

สภาพที่ดีต่อการใช้งาน รวมทั้งการมีโครงสร้างพื้นฐานทางเทคโนโลยี (Technology Infrastructure) ที่ไม่เหมาะสมกับงานหรือล้าสมัย

2.2 Process เกิดจากระบบหรือขั้นตอนการปฏิบัติงาน

- Model/Methodology Error ความผิดพลาดในการพัฒนากำหนดสูตรการคำนวณต่างๆ เช่น อัตราส่วนทางการเงิน การประเมินมูลค่าหลักทรัพย์/ทรัพย์สิน/หนี้สิน และการประเมินมูลค่าหลักประกัน ตลอดจนข้อบกพร่องของวิธีการ/ขั้นตอนการทำงาน ซึ่งทำให้การปฏิบัติงานไม่มีประสิทธิภาพเพียงพอ

- Products/Services การออกแบบ/พัฒนาสินค้าและบริหารไม่ดีพอ สินค้า/บริการมีความซับซ้อนหรือมีข้อบกพร่อง ทำให้ลูกค้าไม่พึงพอใจ และอาจนำมาซึ่งต้นทุนของการให้บริการแก้ไขปัญหาให้แก่ลูกค้า หรือการชดเชยค่าเสียหายแก่ลูกค้า

- Legal/Regulatory เกิดจากการกำกับดูแลและกฎระเบียบที่องค์กร เผชิญอยู่ หากองค์กรวางแผนการปฏิบัติต่างๆ ไม่สอดคล้องกับข้อกำหนดของทางการ นอกจากนี้ยังรวมถึงความเสี่ยงจากการตีความข้อกฎหมาย และมี/ไม่มีกฎหมายที่เอื้ออำนวยต่อการดำเนินธุรกิจขององค์กร

- Communication การเข้าใจไม่ตรงกันในการสื่อข้อความ ทำให้ตีความผิดพลาด การสื่อสารที่ไม่ทั่วถึง ทุกกลุ่มงานหรือข้อมูลที่เผยแพร่ภายนอก ไม่ถูกต้อง ไม่สอดคล้องกันก่อให้เกิดความไม่น่าเชื่อถือ โดยเฉพาะกรณีที่มีการนำข้อมูลไปใช้อ้างอิง

- Inadequate systems & control การขาดมาตรฐาน/คู่มือ/รายละเอียดในการปฏิบัติงานรวมทั้งการขาดระบบการตรวจสอบ/การควบคุม/การรักษาความปลอดภัยที่ดีหรือมีแต่ไม่เพียงพอ

2.3 Technology Risk ความเสี่ยงที่เกิดขึ้นจากการปฏิบัติงานอันเนื่องจากเทคโนโลยี

- Security : การขาดระบบรักษาความปลอดภัยของข้อมูลหรือระบบคอมพิวเตอร์ หรือมีแต่ด้อยประสิทธิภาพ

- System Error/Failure ความผิดพลาด/ความสูญเสียของระบบ เนื่องจากอัคคีภัย ภัยธรรมชาติ ปัญหาด้านเทคนิค กระแสไฟฟ้าขัดข้อง ระบบ สูญเสียความสามารถบางส่วน/ทั้งหมด จากการทำลายของไวรัส คอมพิวเตอร์

- Programming Error ความผิดพลาด/ไม่สมบูรณ์ของโปรแกรมคอมพิวเตอร์ที่ใช้

- Telecommunication Error การขัดข้องของระบบการสื่อสาร เช่น เครือข่ายคอมพิวเตอร์ โทรศัพท์ โทรสาร เป็นต้น

- Information ข้อมูลสำหรับการปฏิบัติงานมีไม่เพียงพอ ไม่สมบูรณ์ ไม่ถูกต้อง หรือไม่มีความสำคัญเกี่ยวข้อง รวมถึงการมีระบบข้อมูลไม่ถูกต้อง ทำให้ไม่สามารถนำข้อมูลไปใช้ได้ หรือการมีหลายระบบที่แสดงข้อมูลในลักษณะแตกต่างกัน

3. ความเสี่ยงด้านการเงิน (Financial Risk : F) เป็นความเสี่ยงที่เกี่ยวข้องกับทางด้านการเงิน ประกอบด้วย

3.1 Market Risk ความเสี่ยงอันเกิดจากการเปลี่ยนแปลงมูลค่าหลักทรัพย์หรือพันธะสัญญาที่องค์กร ทำไว้ส่งผลให้ทรัพย์สิน หนี้สินหรือสัญญา ทั้งที่ปรากฏในงบดุลหรือนอกงบดุลมีมูลค่าสุทธิลดลง หรือส่งผลกระทบต่อการลงทุน (Investment) ขององค์กร ปัจจัยที่ส่งผลกระทบต่อความเสี่ยงทางด้านตลาด ประกอบด้วย

- การเปลี่ยนแปลงของอัตราดอกเบี้ย (Interest Rate Risk)
- การเปลี่ยนแปลงของอัตราแลกเปลี่ยนเงินตราต่างประเทศ (Foreign Exchange Risk)
- ความผันผวนของราคาหลักทรัพย์ (Investment Risk)
- ความผันผวนของอันดับความน่าเชื่อถือของผู้ออกหลักทรัพย์ อันส่งผลกระทบต่อ ราคาหลักทรัพย์ที่ลงทุน

3.2 Credit Risk ความเสี่ยงด้านเครดิต เป็นความเสี่ยงที่เกิดจากการที่คู่สัญญาไม่สามารถทำตามข้อตกลงที่ได้ทำไว้กับองค์กรได้เนื่องจากขาดความสามารถทางด้านการเงินซึ่งส่งผลเสียต่อองค์กรในที่สุด

3.3 Liquidity Risk ความเสี่ยงที่เป็นผลมาจากการที่องค์กร ไม่สามารถเปลี่ยนสินทรัพย์เป็นเงินสดได้ในราคาที่เหมาะสมตามเวลาที่ต้องการ อาจเนื่องจากมีตลาดรองรับสินทรัพย์นั้นไม่เพียงพอ หรือตลาดกำลังถูกแทรกแซงจากปัจจัยอื่น นอกจากนี้ยังหมายถึงความเสี่ยงที่องค์กร ขาดความสามารถชั่วคราวในการจัดหาเงินทุนมาชำระให้แก่คู่สัญญาในวันครบกำหนด

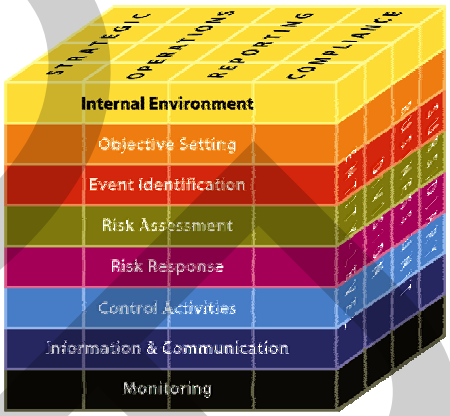
3.4 Budgeting Risk ความเสี่ยงจากความไม่เพียงพอของเงินงบประมาณ ฯลฯ

4. ความเสี่ยงด้านการปฏิบัติตามระเบียบและกฎหมาย (Compliance Risk : C) เป็นความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามระเบียบและกฎหมาย เช่น ระเบียบ กฎหมาย พระราชกฤษฎีกา ระเบียบข้อบังคับ ข้อกำหนดของทางการ นโยบายของรัฐ หรือองค์กรที่เกี่ยวข้อง เช่น ธนาคารแห่งประเทศไทย

4.1 Legal/Regulatory ความเสี่ยงที่เกิดจากการกำกับดูแลและกฎระเบียบที่องค์กรเผชิญอยู่ หากองค์กรวางแผนการปฏิบัติต่างๆ ไม่สอดคล้องกับข้อกำหนดของทางการ นอกจากนี้ยังรวมถึงความเสี่ยงจากการตีความข้อกฎหมาย และมี/ไม่มีกฎหมายที่เอื้ออำนวยต่อการดำเนินธุรกิจขององค์กร

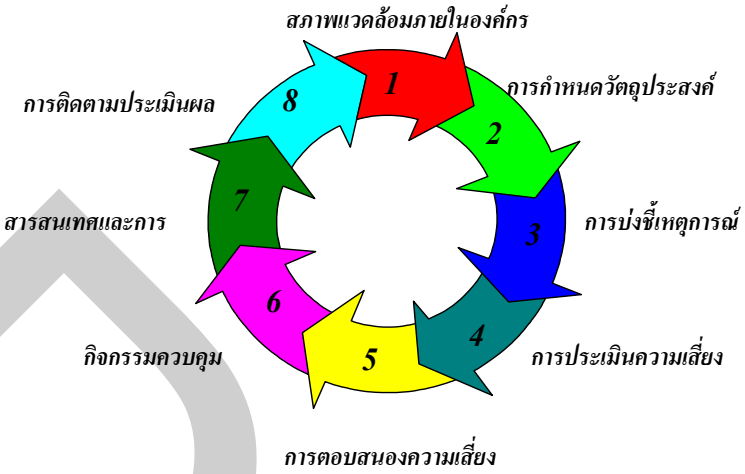
2.3 แนวคิดของ ERM และ COSO

การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management, ERM) คือ กระบวนการที่บุคลากรทั่วทั้งองค์กรได้มีส่วนร่วมในการคิด วิเคราะห์ และคาดการณ์ถึงเหตุการณ์หรือความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งการระบุแนวทางในการจัดการกับความเสี่ยงดังกล่าวให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้เพื่อช่วยให้องค์กรบรรลุในวัตถุประสงค์ที่ต้องการ ตามกรอบวิสัยทัศน์ และพันธกิจขององค์กร ภาพที่ 2.1 แสดงการบริหารความเสี่ยงระดับองค์กร



ภาพที่ 2.1 การบริหารความเสี่ยงระดับองค์กร

กรอบการบริหารความเสี่ยงองค์กรนั้น สามารถสะท้อนให้เห็นถึงนโยบายการบริหารจัดการ และการกำกับดูแลกิจการ ของแต่ละองค์กร โดยหากองค์กรมีการบริหารความเสี่ยงอย่างมีประสิทธิภาพจะส่งผลให้สามารถบรรลุวัตถุประสงค์องค์กร ทั้งในเชิงประสิทธิภาพและประสิทธิผลของงาน ภาพที่ 2.2 แสดงกรอบการบริหารความเสี่ยงตามมาตรฐาน Committee of Sponsoring Organizations of the Treadway Commission (COSO) ประกอบด้วยองค์ประกอบ 8 ประการ ซึ่งครอบคลุมแนวทางการกำหนดนโยบายการบริหารงาน การดำเนินงาน และการบริหารความเสี่ยง โดยมีรายละเอียดดังต่อไปนี้



ภาพที่ 2.2 กรอบการบริหารความเสี่ยงตามมาตรฐาน COSO

1. สภาพแวดล้อมภายในองค์กร (Internal Environment) ของการควบคุมภายในองค์กรเป็นองค์ประกอบที่สำคัญ ในการกำหนดกรอบบริหารความเสี่ยง ประกอบด้วยปัจจัยหลายประการ ได้แก่ โครงสร้างและวัฒนธรรมขององค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติงานบุคลากร กระบวนการทำงาน ระบบสารสนเทศ ระเบียบ เป็นต้น สภาพแวดล้อมภายในองค์กรประกอบเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงขององค์กรเพื่อนำไปปฏิบัติให้บังเกิดผลอย่างจริงจัง สำหรับสภาพแวดล้อมภายในองค์กรนั้น ควรคำนึงถึงปัจจัยสำคัญที่จะช่วยส่งผลให้การบริหารความเสี่ยงสามารถดำเนินการได้สำเร็จประกอบด้วย โครงสร้างองค์กร โดยการเพิ่มคณะกรรมการดูแลรับผิดชอบงานด้านการบริหารความเสี่ยง เพื่อทำหน้าที่กำหนดนโยบายและบริหารจัดการงานบริหารความเสี่ยงได้ตามเป้าหมายที่องค์กรวางไว้ สภาพแวดล้อมภายในองค์กรที่ผู้บริหารสามารถพบและมีโอกาสเผชิญกับความเสี่ยงในลักษณะต่างๆ มาจากหลายปัจจัยประกอบด้วย

1.1 ความเสี่ยงจากการดำเนินงาน ได้แก่ พนักงานไม่มีประสบการณ์ การพัฒนาผลิตภัณฑ์ไม่มีประสิทธิภาพ การทุจริตของพนักงานและผู้บริหาร การปฏิบัติผิดกฎระเบียบข้อบังคับ

1.2 ความเสี่ยงจากการมอบอำนาจ การกระจายอำนาจภายในองค์กร สามารถเพิ่มประสิทธิภาพในการทำงานให้สะดวกรวดเร็ว แต่อาจสร้างปัญหาในการทำงาน ได้แก่ ภาวะผู้นำของผู้รับมอบอำนาจ การมอบอำนาจหรือการมอบวงเงินไม่เหมาะสมกับสถานการณ์ เครื่องมือสร้างแรงจูงใจในการปฏิบัติงานไม่เพียงพอต่ออำนาจที่ได้รับ

1.3 ความเสี่ยงจากเทคโนโลยีที่เปลี่ยนแปลง ส่งผลให้อาจเกิดปัญหาต่อการดำเนินการขององค์กร ได้แก่ การปรับเปลี่ยนอุปกรณ์คอมพิวเตอร์และโปรแกรมใหม่ การเปลี่ยนแปลงขั้นตอนการทำงาน การพัฒนาผลิตภัณฑ์ใหม่ การปลดระวางเครื่องมือและโปรแกรมเก่า การจัดการฐานข้อมูล

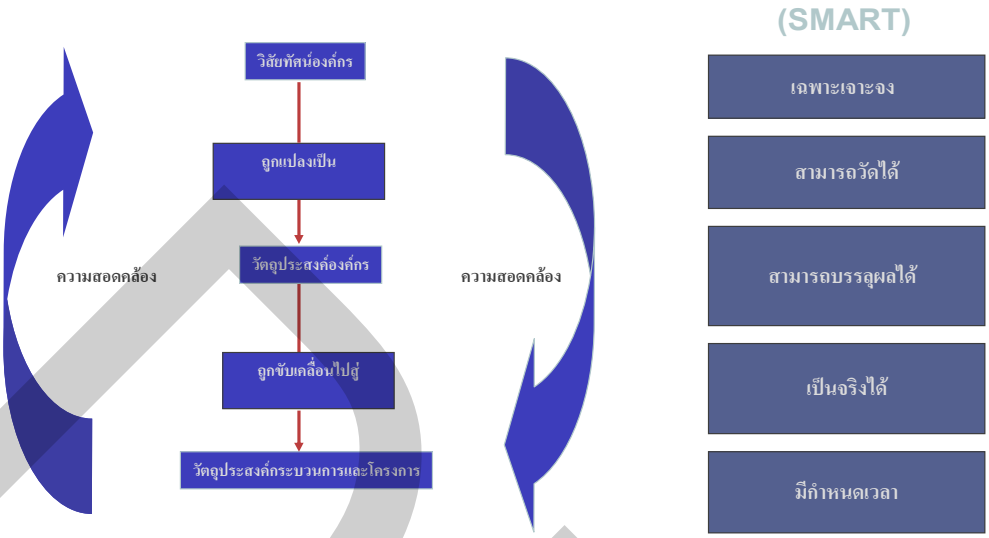
1.4 ความเสี่ยงจากการตัดสินใจทำธุรกิจ ซึ่งอาจก่อให้เกิดความเสี่ยงในเรื่องต่างๆ ได้แก่ การเพิ่มช่องทางในการจำหน่ายสินค้า การพัฒนาผลิตภัณฑ์หรือบริการใหม่ การแสวงหาตลาดกลุ่มใหม่ การสร้างภาพลักษณ์ทางการค้า

1.5 ความเสี่ยงทางการเงิน การบริหารจัดการทางการเงินมีความสำคัญต่อการดำเนินการภายในองค์กรอย่างยิ่ง เนื่องจากเป็นจุดยุทธศาสตร์สำคัญที่มีผลต่อการดำเนินการขององค์กร ผู้บริหารจะให้ความสนใจต่อความเสี่ยงในเรื่องต่างๆ ได้แก่ การบริหารสภาพคล่อง การวางแผนงบประมาณ รายงานทางการเงิน รายงานทางการบัญชี

ความเสี่ยงที่เกิดจากสภาพแวดล้อมภายในองค์กร เป็นเพียงตัวอย่างของความเสี่ยงที่มีโอกาสเกิดขึ้นและมีผลกระทบก่อให้เกิดความเสียหายต่อองค์กร แต่ไม่ว่าความเสี่ยงที่มีโอกาสเกิดขึ้นนั้นจะมาจากสาเหตุใดก็ตาม ปัจจัยที่เป็นผลกระทบสำคัญของความเสี่ยงภายในองค์กร มาจากสาเหตุหลัก 2 ประการ คือ คนและระบบ

ดังนั้นหากผู้บริหารสามารถคัดเลือกบุคลากรที่มีความสามารถตรงตามสายงาน ซื่อสัตย์ และมีความรับผิดชอบ รวมถึงมีการวางแผนและกำหนดแนวทางในการทำงานที่เป็นระบบ จะสามารถบริหารจัดการงานด้านความเสี่ยงได้อย่างมีประสิทธิภาพ

2. การกำหนดวัตถุประสงค์ (Objective Setting) ที่ชัดเจนขององค์กรนั้น เป็นขั้นตอนเริ่มต้นสำหรับกระบวนการบริหารความเสี่ยง ในการกำหนดวัตถุประสงค์ควรจัดทำเป็นลายลักษณ์อักษรอย่างชัดเจน มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่หน่วยงานยอมรับได้ รวมทั้งควรมีการสื่อสารให้แก่ทุกหน่วยงานรับทราบ เพื่อให้มีความเข้าใจที่ตรงกัน แนวทางในการกำหนดวัตถุประสงค์สามารถใช้การกำหนดวัตถุประสงค์แบบ SMART ดังภาพที่ 2.3 โดยประกอบด้วย



ภาพที่ 2.3 การกำหนดวัตถุประสงค์แบบ SMART

Specific มีความเฉพาะเจาะจง สอดรับกับ model ธุรกิจหลัก

Measurable สามารถวัดได้ทั้งเชิงปริมาณและคุณภาพ

Attainable สามารถปฏิบัติให้บรรลุผลได้

Relevant มีความสอดคล้องกับวัตถุประสงค์และเป้าหมายขององค์กร

Timely มีกรอบระยะเวลาที่แน่นอน

สามารถใช้การกำหนดวัตถุประสงค์แบบ SMART เพื่อเป็นแนวทางในการกำหนดวัตถุประสงค์ขององค์กร ซึ่งจะทำให้การบริหารงานและการดำเนินงานสอดคล้องกับวิสัยทัศน์องค์กร วัตถุประสงค์ไว้ 2 ระดับ คือ

2.1 การกำหนดวัตถุประสงค์ระดับองค์กร เป็นการนำวัตถุประสงค์และเป้าหมายจากแผนวิสาหกิจขององค์กร โดยทำการระบุสถานะปัจจุบันของการดำเนินงานตามเป้าหมายเพื่อให้มีการวิเคราะห์ความเสี่ยงในอันที่จะทำให้ไม่สามารถบรรลุวัตถุประสงค์ที่กำหนด

2.2 การกำหนดวัตถุประสงค์ระดับกลุ่มภารกิจ/โครงการ เป็นการกำหนดวัตถุประสงค์และเป้าหมายตามพันธกิจของแต่ละกลุ่มภารกิจ เพื่อนำไปสู่การวิเคราะห์ความเสี่ยงที่จะทำให้พันธกิจของกลุ่มภารกิจ ไม่บรรลุผลตามวัตถุประสงค์ที่วางไว้

3. การบ่งชี้เหตุการณ์ หรือการระบุปัจจัยเสี่ยง (Risk Identification) การบ่งชี้เหตุการณ์หรือการระบุความเสี่ยง เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งในส่วนของปัจจัยเสี่ยงที่เกิดจากภายในและภายนอกองค์กร ผู้ประเมินควรทำความเข้าใจ และทราบถึงวัตถุประสงค์หรือเป้าหมายที่ชัดเจนของงานแต่ละงาน และเหตุการณ์ใดหรือกิจกรรมใดของกระบวนการปฏิบัติงาน ที่จะทำให้ไม่บรรลุวัตถุประสงค์ของงานที่วางไว้ รวมถึงการทำความเข้าใจเกี่ยวกับกิจกรรมที่ปฏิบัติอย่างรอบคอบชัดเจนเพื่อให้ผู้บริหารสามารถพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจจะเกิดขึ้นได้เป็นอย่างดี ตารางที่ 2.1 แสดงตัวอย่างการระบุปัจจัยเสี่ยง

ตารางที่ 2.1 ตัวอย่างการระบุปัจจัยเสี่ยง

ความเสี่ยง	ปัจจัยเสี่ยง		ผลกระทบ	
	ภายนอก	ภายใน	ทางตรง	ทางอ้อม
ความเสี่ยงแต่ละลักษณะที่มีโอกาสเกิดขึ้น - ความล่าช้าของโครงการ - การเกิดอัคคีภัย - ระบบล่มข้อมูลสารสนเทศสูญหาย - ความเสียหายจากการทุจริตของพนักงาน	เกิดจากธรรมชาติหรือบุคคลอื่นหรือนโยบายจากหน่วยงานอื่นที่ไม่สามารถควบคุมได้ แต่สามารถติดตามความเคลื่อนไหวเพื่อหาวิธี ป้องกันได้ เช่น - ฝนตกหนัก - การเปลี่ยนแปลงนโยบายของรัฐบาล - การเปลี่ยนแปลงพฤติกรรมของลูกค้า - การก่อวินาศกรรม/ลอบวางระเบิด	เกิดจากนโยบายการทำงาน หรือบุคลากรภายในองค์กรสามารถควบคุมแก้ไขได้ เช่น - เจ้าหน้าที่ไม่มีประสบการณ์ และขาดแรงจูงใจในการทำงาน - กฎระเบียบ เคร่งครัดมากเกินไปทำให้งานล่าช้า - ระบบ IT ล่าช้า ไม่ทันสมัย ใช้งานยาก - ความขัดแย้งภายในหน่วยงาน	เกิดขึ้นทันที เช่น - มีการปรับลดเงินเดือนเนื่องจากทำงานผิดพลาดและล่าช้า - ข้อมูลในการทำงานได้รับความเสียหาย - สูญเสียทรัพย์สิน / รายได้เนื่องจากการทุจริต	เกิดขึ้นภายหลัง เช่น - การฟ้องร้อง - องค์กรเสื่อมเสียชื่อเสียง - ครอบครัวของผู้เสียชีวิตจากการก่อวินาศกรรมเกิดความลำบาก

การระบุความเสี่ยงให้ระบุโดยพิจารณาตามเหตุแห่งความเสี่ยง (Sources of Risk) ที่อาจส่งผลกระทบต่อวัตถุประสงค์/เป้าหมายของโครงการหรือกิจกรรม หรือสร้างความเสียหายทั้งทางตรงและทางอ้อมอย่างมีนัยสำคัญ ในการวิเคราะห์ความเสี่ยงควรเน้นที่จะระบุปัจจัยเสี่ยงและเหตุการณ์ความเสียหายที่เกี่ยวข้องกับกิจกรรมสำคัญ ทั้งนี้ไม่คำนึงถึงมาตรการควบคุมความเสี่ยงที่มีอยู่ในปัจจุบัน โดยครอบคลุมทั้งความเสี่ยงที่อยู่และไม่อยู่ภายใต้การควบคุมหรือความรับผิดชอบของหน่วยงาน

- ความเสี่ยงจากลักษณะธุรกิจ (Inherent Risk) เป็นความเสี่ยงที่มีอยู่โดยธรรมชาติในธุรกิจหรืองานแต่ละอย่าง เมื่อใดก็ตามที่ตัดสินใจที่จะทำธุรกิจหรืองานนั้นๆ ก็ย่อมมีความเสี่ยงเกิดขึ้น

- ความเสี่ยงที่เหลืออยู่ (Residual Risk) เป็นความเสี่ยงที่เหลืออยู่หลังจากที่ได้ดำเนินการจัดให้มีจุดควบคุมความเสี่ยงนั้นแล้ว

แนวทางที่สามารถใช้ในการระบุความเสี่ยง แสดงดังภาพที่ 2.4 โดยมีรายละเอียดดังต่อไปนี้

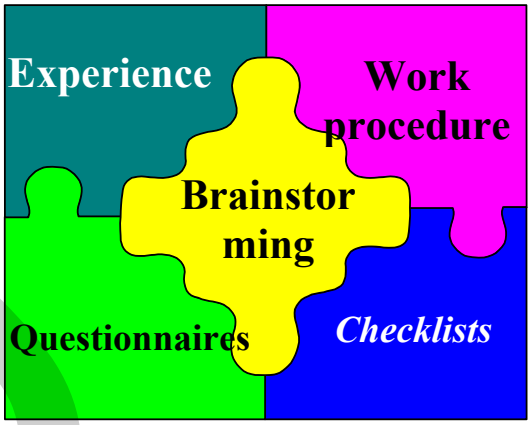
3.1 การใช้ประสบการณ์ของผู้ประเมินในการระบุเหตุการณ์ที่เคยเกิดขึ้น (Experience) หรือพิจารณาแล้วว่ามีโอกาสที่จะเกิดขึ้นได้ หรือใช้การเก็บข้อมูลเกี่ยวกับปัญหา/ข้อผิดพลาดในกระบวนการทำงานที่เคยเกิดขึ้นในอดีต และได้มีการบันทึกไว้ หรือเป็นข้อมูลที่บันทึกอยู่ในระบบคอมพิวเตอร์สามารถนำมาใช้เป็นแนวทางและเป็นข้อมูลเบื้องต้นได้

3.2 การใช้คู่มือปฏิบัติงาน (Work Procedure Manual) เพื่อลำดับขั้นตอนของกระบวนการทำงาน และพิจารณาว่าในแต่ละขั้นตอนอาจจะเกิดเหตุการณ์ต่าง ๆ ซึ่งอาจจะทำให้กิจกรรมนั้น ๆ หยุดชะงัก หรือผิดพลาดจนก่อให้เกิดความเสียหายขึ้นได้หรือไม่

3.3 การระดมความคิด (Brainstorming Group) จากพนักงานที่มีส่วนเกี่ยวข้องกับกิจกรรมดังกล่าว ทั้งภายในและภายนอกหน่วยงาน เพื่อร่วมกันพิจารณาว่ามีเหตุการณ์ใดบ้างที่เกิดขึ้นแล้วส่งผลกระทบเสียหายต่องานที่ดูแล

3.4 การใช้แบบสอบถามความคิดเห็น (Questionnaires) ไปยังผู้รับผิดชอบกิจกรรมต่างๆ ว่ามีปัญหาข้อผิดพลาด หรือความเสี่ยงในลักษณะใด ก่อให้เกิดความเสียหายแต่การสอบถามควรกระทำกับเจ้าหน้าที่ที่เกี่ยวข้องโดยตรง ซึ่งเป็นผู้ทราบข้อมูลต่าง ๆ อย่างแท้จริง

3.5 การใช้แบบตรวจสอบรายการ (Checklists) โดยผู้บริหาร และพนักงานในหน่วยงานสามารถตรวจสอบวิธีการทำงาน ขั้นตอนการทำงาน และมาตรฐานการทำงานตาม Checklist ที่จัดทำได้ด้วยตนเอง และควรกำหนดระยะเวลาในการประเมินผลภายในหน่วยงานด้วย Checklist ที่ชัดเจน เช่น ทุก 3 เดือน 6 เดือน หรือ 12 เดือน



ภาพที่ 2.4 แนวทางในการระบุความเสี่ยง

ในการเลือกใช้แหล่งข้อมูลหรือวิธีการใดในการระบุความเสี่ยงนั้น อาจแตกต่างกันในแต่ละหน่วยงานและแต่ละมูลเหตุความเสี่ยงโดยขึ้นกับลักษณะงานและวิธีปฏิบัติงานของหน่วยงาน ความเสี่ยงและเหตุแห่งความเสี่ยงควรครอบคลุมในเรื่องต่อไปนี้

3.1 ความเสียหายหรือเหตุการณ์ ที่อาจมีผลกระทบในเชิงลบต่อองค์กร

3.2 ความไม่แน่นอนที่อาจมีผลต่อการบรรลุวัตถุประสงค์และกลยุทธ์ขององค์กร

3.3 เหตุการณ์ที่อาจทำให้องค์กรสูญเสียโอกาสในการสร้างรายได้หรือสร้างโอกาสทางธุรกิจหรือการได้รับการยอมรับการหน่วยงานภายนอก

3.4 ความเสี่ยงที่อาจเกิดขึ้นทุกด้าน เช่น ความเสี่ยงด้านกลยุทธ์ การเงิน บุคลากร การดำเนินงาน ชื่อเสียง กฎหมาย ภาษีอากร ระบบงาน และสิ่งแวดล้อม เป็นต้น

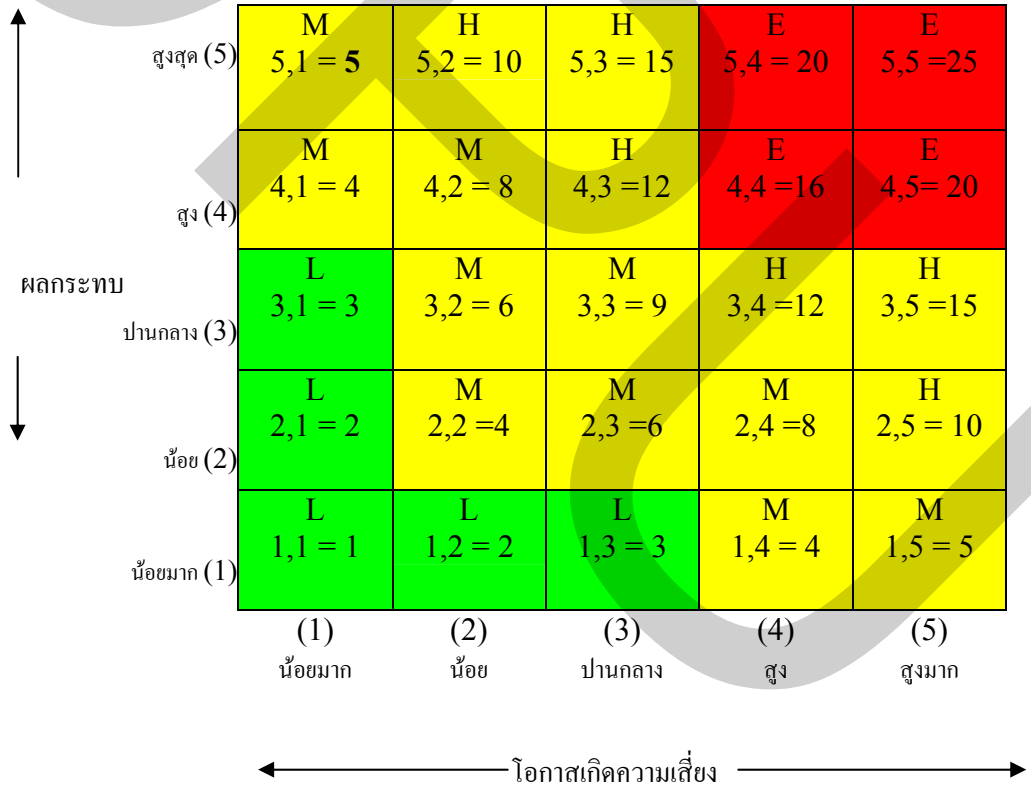
3.5 ความเสี่ยงที่อาจเกิดขึ้นจากสาเหตุทั้งจากปัจจัยภายในและภายนอกองค์กร

4. การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยงเป็นกระบวนการที่ควรดำเนินการหลังจากองค์กรทำการระบุความเสี่ยงแล้ว การประเมินความเสี่ยงประกอบด้วย 2 มิติ คือ โอกาสที่อาจเกิดขึ้น (Likelihood) และผลกระทบจากความเสี่ยง (Impact) ดังนั้นในการประเมินความเสี่ยง ผู้ประเมินควรระบุลักษณะของความเสียหายจากความเสี่ยงที่มีโอกาสเกิดขึ้นอย่างชัดเจน เพื่อให้ทราบถึงผลกระทบที่เกิดขึ้น และเป็นข้อมูลในการประเมินระดับความรุนแรงของความเสี่ยง ที่อาจจะส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร ทั้งนี้เพื่อสามารถกำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสมต่อไป

4.1 ขั้นตอนการประเมินความเสี่ยงนั้น ประกอบด้วยการดำเนินการ 5 ขั้นตอน ได้แก่

4.1.1 การกำหนดเกณฑ์ประเมินความเสี่ยง เป็นขั้นตอนกำหนดเกณฑ์การประเมินความเสี่ยง 2 มิติ คือ โอกาสที่จะเกิดความเสี่ยง โดยสามารถกำหนดได้ทั้งเกณฑ์ในเชิงปริมาณและเชิงคุณภาพ และ ระดับความรุนแรงของผลกระทบ แบ่งเป็นในด้านต่างๆ เช่น ด้านมูลค่าความเสียหาย ด้านชื่อเสียง ด้านเวลา และด้านความสำเร็จ เพื่อกำหนดระดับความเสี่ยง (Degree of Risks) ของความเสี่ยงแต่ละเหตุการณ์ต่อไป

4.1.2 การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นขั้นตอนการนำโอกาสที่จะเกิดความเสี่ยง และระดับความรุนแรงของผลกระทบ เพื่อกำหนดระดับความเสี่ยง ของความเสี่ยงแต่ละเหตุการณ์ตามเกณฑ์มาตรฐานที่กำหนด โดยให้ความสำคัญต่อความเสี่ยงที่มีผลกระทบสูง และมีโอกาสเกิดความเสี่ยงสูง เพื่อจัดการความเสี่ยงดังกล่าวก่อน ภาพที่ 2.5 แสดงการกำหนดระดับความเสี่ยง และตารางที่ 2.2 แสดงคำอธิบายของการกำหนดระดับความเสี่ยง



ภาพที่ 2.5 การกำหนดระดับความเสี่ยง

ตารางที่ 2.2 คำอธิบายของการกำหนดระดับความเสี่ยง

ระดับความเสี่ยง	ผลกระทบ	โอกาสที่จะเกิดความเสียหาย	คำอธิบายผลลัพธ์	กลยุทธ์ที่ต้องการ (ตัวอย่างเท่านั้น)
สูงสุด (Extreme) E	สูงสุด	สูงมาก	เป็นความเสี่ยงที่ไม่ควรยอมให้เกิดความเสียหายทางอย่างรุนแรง	กำหนดให้ผู้รับผิดชอบพิจารณากำหนดมาตรการลด/ป้องกันโดยเร่งด่วนเพื่อลดระดับความเสี่ยงให้อยู่ในระดับ M หรือ L
สูง (High) H	ปานกลางถึงสูง	ปานกลาง - มาก	เกิดการหยุดชะงักในการดำเนินธุรกิจ	กำหนดผู้รับผิดชอบต้องให้ความสำคัญ และดำเนินการให้ระดับความเสี่ยงลดลงอยู่ในระดับ M หรือ L
ปานกลาง (Medium) M	น้อยถึงปานกลาง	น้อย-ปานกลาง	บางครั้งไม่สามารถควบคุมการหยุดชะงักได้ภายในเวลาที่กำหนด	กำหนดผู้รับผิดชอบความเสี่ยงพิจารณาจัดให้มีมาตรการควบคุมความเสี่ยงเพื่อลดระดับของความเสี่ยงให้อยู่ในระดับ L
ต่ำ (Low) L	น้อยมากถึงน้อย	โอกาสเกิดขึ้นน้อยมาก-น้อย	ผลกระทบต่ำ แต่ถ้าไม่ควบคุมอาจเกิดความเสียหายได้เล็กน้อย	หากการลด/ควบคุมความเสี่ยงไม่คุ้มกับประโยชน์ที่ได้รับอาจไม่จำเป็นต้องจัดหามาตรการการลด/ควบคุมความเสี่ยงเพิ่มเติมแต่จะต้องติดตามสถานะความเสี่ยงอย่างสม่ำเสมอเพื่อให้แน่ใจว่าความเสี่ยงดังกล่าวอยู่ในระดับที่ยอมรับได้

4.1.3 การวิเคราะห์ความเสี่ยง หลังจากที่มีการประเมินโอกาสและผลกระทบของความเสี่ยงแล้ว ขั้นตอนต่อไปของการดำเนินการ คือ การวิเคราะห์ความเสี่ยง เพื่อทำให้ทราบว่าความเสี่ยงใดเป็นความเสี่ยงสูงสุดที่ควรเร่งบริหารจัดการความเสี่ยงนั้นก่อนเป็นลำดับแรก โดยทั่วไปในการบริหารความเสี่ยงของหน่วยงานและขององค์กร ควรเลือกงานที่มีความเสี่ยงสูงสุด 3-5 ลำดับแรกมาดำเนินการก่อน แล้วจึงค่อยพิจารณาดำเนินการกับงานที่มีความเสี่ยงในลำดับรองลงไป

4.1.4 การจัดลำดับความเสี่ยง เมื่อหน่วยงานสามารถกำหนดระดับความเสี่ยงได้แล้ว สำหรับขั้นตอนไปของการประเมินความเสี่ยงคือ การจัดลำดับความเสี่ยง เพื่อให้หน่วยงานสามารถจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของหน่วยงาน และสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดยพิจารณาจากความสัมพันธ์ระหว่าง โอกาสที่จะเกิดความเสี่ยง และผลกระทบของความเสี่ยง ซึ่งการประเมินความเสี่ยง ควรดำเนินการ ก่อนการจัดการความเสี่ยง (Inherent Risk) และหลังจากที่มีการจัดการความเสี่ยง (Residual Risk) อย่างสม่ำเสมอ

4.1.5 การประเมินมาตรการควบคุมความเสี่ยง (Risk Control) เป็นขั้นตอนในกระบวนการบริหารความเสี่ยง ซึ่งควรดำเนินการหลังจากที่องค์กรหรือหน่วยงานได้มีการประเมินโอกาสและผลกระทบของความเสี่ยง รวมถึงการจัดลำดับความเสี่ยงเรียบร้อยแล้ว ทั้งนี้เพื่อเป็นเครื่องมือในการช่วยควบคุมความเสี่ยงหรือปัจจัยเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กรหรือหน่วยงาน ซึ่งจะทำให้องค์กรหรือหน่วยงานสามารถดำเนินการได้บรรลุวัตถุประสงค์ได้ตามที่วางไว้

4.2 การกำหนดมาตรการควบคุมความเสี่ยงของแต่ละองค์กรจะมีมาตรฐานที่แตกต่างกันไป ขึ้นกับดุลยพินิจและประสบการณ์ของผู้บริหาร งบประมาณด้านการบริหารความเสี่ยง รวมถึงระดับความเสี่ยงที่ยอมรับได้ของแต่ละองค์กร โดยสามารถแบ่งออกเป็น 4 มาตรการดังนี้

4.2.1 การควบคุมเพื่อการป้องกัน (Preventive Control) เป็นมาตรการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาด เช่น การกำหนดนโยบาย การจัดโครงสร้างองค์กร การแบ่งแยกหน้าที่ การควบคุมการเข้าถึงเอกสาร ข้อมูล ทรัพย์สิน เป็นต้น

4.2.2 การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นมาตรการควบคุมที่กำหนดขึ้นเพื่อค้นพบข้อผิดพลาดในการทำงาน เช่น การสอบทาน การวิเคราะห์ การยืนยันยอด การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

4.2.3 การควบคุมโดยการชี้แนะ (Directive Control) เป็นมาตรการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดผลสำเร็จของงานตามวัตถุประสงค์ที่วางไว้ เช่น การสร้างแรงจูงใจในการทำงาน การบริหารงานอย่างเอาใจใส่ของผู้บังคับบัญชา เป็นต้น

4.2.4 การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นมาตรการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้น หรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำในอนาคต เช่น การสำรองข้อมูลสำคัญขององค์กรในที่ปลอดภัย การซ้อมหนีไฟกรณีเกิดเพลิงไหม้ในอาคาร เป็นต้น

ความเสี่ยงคงเหลือ (Residual Risk) เป็นจุดเริ่มต้นของการกำหนดความเสี่ยงในระดับที่ยอมรับได้สำหรับองค์กร ในการเผชิญกับความเสี่ยงจากการดำเนินกิจกรรมหรือธุรกิจ (Inherent Risk) ให้ทราบระหว่างระดับความเสี่ยงนั้นสูงกว่าระดับการควบคุม (Control Score) ในสถานการณ์เช่นนี้บ่งชี้ให้เห็นว่าความเสี่ยงคงเหลือ นั้นมีค่าสูงกว่า โดยพิจารณาจากสมการที่ 2.1

ความเสี่ยงคงเหลือ = ความเสี่ยงจากการดำเนินกิจกรรมหรือธุรกิจ – มาตรการควบคุม (2.1)

การลดระดับความเสี่ยงคงเหลือ สามารถกระทำได้โดยการเพิ่มระดับมาตรการควบคุมที่มีประสิทธิผลมากยิ่งขึ้น หรือการหลีกเลี่ยงการดำเนินกิจกรรมหรือธุรกิจที่ทำให้เกิดความเสี่ยง ความเสี่ยงนั้นๆ จากสมการข้างต้น องค์กรสามารถกำหนดระดับความเสี่ยง (Risk Score) และระดับการควบคุม (Control Score) ได้อย่างเหมาะสม ตารางที่ 2.3 แสดงเกณฑ์ในการยอมรับความเสี่ยง

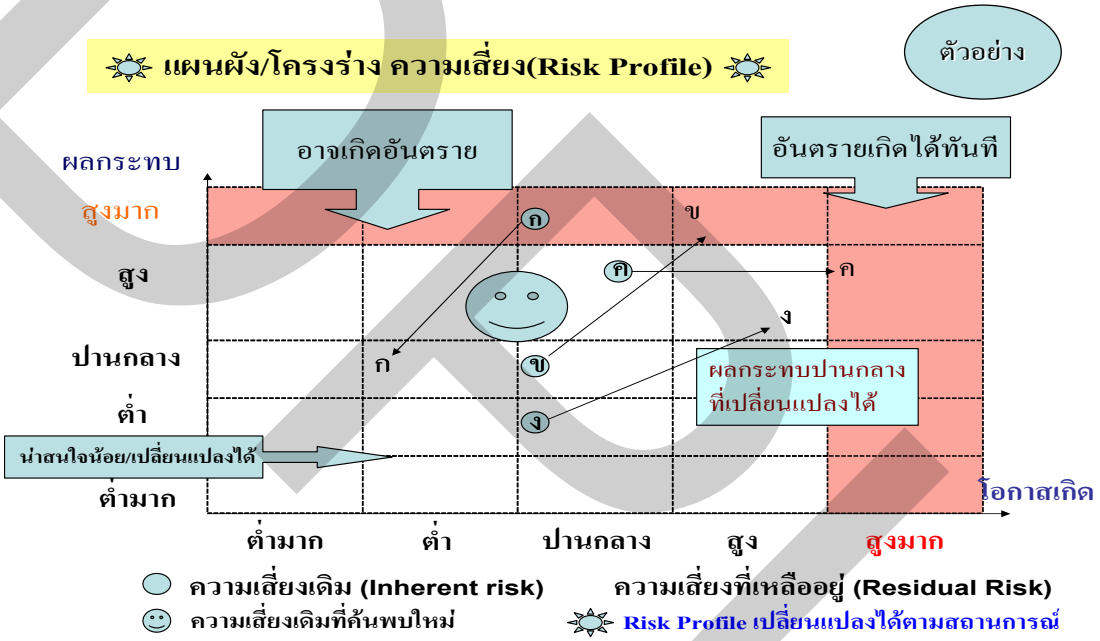
ตารางที่ 2.3 เกณฑ์ในการยอมรับความเสี่ยง

ระดับความเสี่ยง	แทนด้วยแถบสี	กลยุทธ์ที่ต้องการ (ตัวอย่างเท่านั้น)
สูงสุด (Extreme) E	**แดง**	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที
สูง (High) H	**ส้ม**	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ต่อไป
ปานกลาง (Medium) M	**เหลือง**	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ต่อไป
ต่ำมาก (Low) L	เขียว	ระดับที่สามารถยอมรับได้ โดยไม่ต้องมีการควบคุม และไม่ต้องจัดการอะไรเพิ่มเติม

เมื่อมีการประเมินมาตรการควบคุมความเสี่ยงแล้ว หากปัจจัยเสี่ยงที่พิจารณาแล้วว่าสามารถดำเนินการภายใต้การยอมรับของผู้บริหารระดับสูงและภายในงบประมาณที่วางไว้ ก็

สามารถวางแผนการบริหารจัดการความเสี่ยง เพื่อป้องกันหรือลดความเสี่ยงของงานหรือโครงการต่อไป

5. การจัดการความเสี่ยง (Risk Response) การจัดการความเสี่ยงเป็นขั้นตอนการระบุทางเลือกสำหรับการจัดการความเสี่ยง เพื่อนำแผนดังกล่าวไปปฏิบัติ หลังจากผู้ประเมินได้ผลการจัดระดับความรุนแรงของความเสี่ยงแล้ว ผู้ประเมินควรคัดเลือกความเสี่ยงที่มีระดับความรุนแรงสูงสุดตามลำดับมาจำนวนหนึ่ง เพื่อจัดให้มีมาตรการควบคุมความเสี่ยง และพิจารณาจัดการความเสี่ยง ตามลำดับความสำคัญ ดังแสดงดังภาพที่ 2.6



ภาพที่ 2.6 ตัวอย่างแผนผัง/โครงร่างความเสี่ยง

สำหรับแนวทางการจัดการความเสี่ยง อาจมีมากกว่า 1 แนวทาง ตัวอย่าง เช่น ความเสี่ยงที่มีโอกาสเกิดความเสียหายสูง เนื่องจากไม่มีกระบวนการตรวจสอบการทำงาน และพนักงานไม่มีความรู้ความชำนาญ หน่วยงานอาจเลือกจัดการกับความเสี่ยง โดยกำหนดมาตรการควบคุมการทำงาน หรือเพิ่มงบประมาณอบรมพนักงาน เพื่อลดโอกาสที่จะเกิดความเสียหาย

ในกรณีที่มีมาตรการควบคุมการทำงานแล้วแต่ยังเกิดเหตุการณ์ความเสียหาย หน่วยงานอาจพิจารณาทบทวนความเหมาะสมของมาตรการควบคุมการทำงานและปรับปรุงให้มีประสิทธิภาพมากขึ้น

กรณีเหตุการณ์ที่สร้างความเสียหายอย่างร้ายแรงต่อฐานะการเงิน และผลการดำเนินงาน ซึ่งอาจเกิดจากปัจจัยที่ไม่สามารถควบคุมได้ เช่น ไฟไหม้ หรือภัยธรรมชาติ อาจใช้วิธีการทำ

ประกันภัย หรือการจัดทำแผนรองรับ (Contingency Plan) เพื่อลดความเสียหายในระดับหนึ่ง สำหรับความเสี่ยงที่มีระดับความเสี่ยงต่ำ และเป็นความเสี่ยงที่ยอมรับได้ หน่วยงานควรติดตามดูแลและทบทวนเป็นประจำอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าความเสี่ยงดังกล่าวอยู่ในระดับที่ยอมรับได้

กลยุทธ์เพื่อจัดการความเสี่ยง (4T's Strategies)

5.1 Take การยอมรับ/ดำรงความเสี่ยง (Risk Acceptance) ถ้าความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้ โดยอาจไม่ต้องวางแผนจัดการความเสี่ยงนั้น แต่ต้องมีเหตุผลที่ดีเพียงพอ

5.2 Treat การลด/ควบคุมความเสี่ยง (Risk Reduction/Risk Control) โดยการหากิจกรรมควบคุมเพื่อลดความเสี่ยง เช่น การออกแบบระบบการควบคุมภายใน การแก้ไขปรับปรุงการทำงาน เพื่อป้องกันหรือจำกัดผลกระทบ

5.3 Terminate การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการตัดสินใจที่จะไม่เข้าไปเกี่ยวข้องกับสถานการณ์ความเสี่ยงนั้นหรือยุติการดำเนินกิจกรรมที่ก่อให้เกิดความ เช่น ยกเลิกขั้นตอนงานที่ไม่จำเป็นและมีโอกาสเกิดความเสี่ยง

5.4 Transfer การกระจาย/ถ่ายโอนความเสี่ยง (Risk Sharing/Risk Transfer) เป็นการถ่ายโอนความรับผิดชอบหรือภาระของการสูญเสียให้กับบุคคลอื่นหรือหน่วยงานอื่นจัดการแทน เช่น การทำประกันภัย การทำสัญญาป้องกันความเสี่ยง เป็นต้น

การระบุทางเลือกในการจัดการความเสี่ยง ซึ่งการจัดการความเสี่ยงในแต่ละวิธีอาจเหมาะสมกับสถานการณ์บางสถานการณ์เท่านั้น และการจัดการกับความเสี่ยงหนึ่งๆ อาจมีแนวทางได้มากกว่า 1 แนวทาง วิธีจัดการความเสี่ยงสามารถแบ่งออกได้เป็น 2 แนวทางหลัก ได้แก่ การลดโอกาสที่จะเกิดเหตุการณ์ความเสียหาย และการลดขนาดผลกระทบของความเสียหาย

ก่อนที่จะดำเนินการระบุทางเลือกในการจัดการความเสี่ยง หน่วยงานควรทราบวัตถุประสงค์ว่าต้องการควบคุมความเสี่ยงไปในทิศทางใด/ลักษณะใด โดยดูจากแผนภาพแสดงระดับความรุนแรงของความเสี่ยง (Risk Matrix) ประกอบเช่น ความเสี่ยงที่มีโอกาสที่จะเกิดเหตุการณ์ความเสียหายสูง แต่มีระดับความเสียหายต่ำ (อยู่ด้านล่าง - ด้านขวาของ Matrix) ก็ควรคัดเลือกแนวทางควบคุมที่มุ่งเน้นการลดโอกาส เป็นต้น ตารางที่ 2.4 แสดงตัวอย่างวิธีการจัดการความเสี่ยงโดยมีรายละเอียดดังต่อไปนี้

ตารางที่ 2.4 ตัวอย่างวิธีการจัดการความเสี่ยง

วิธีการจัดการความเสี่ยง	ตัวอย่างการดำเนินการ
- การลดโอกาสที่จะเกิดเหตุการณ์ความเสียหาย (Reduce Likelihood)	- จัดให้มีการสอบทานข้อกำหนด และวิธีปฏิบัติ - กำหนดให้มีขั้นตอนการควบคุม และการตรวจสอบ - จัดให้มีการพัฒนาและวิจัยด้านเทคโนโลยี - จัดให้มีการฝึกอบรม - การปรับปรุงกระบวนการทำงาน
- การลดผลกระทบ (Reduce Impact)	- จัดทำ Contingency Plan หรือ Business Continuity Plan - จัดทำแผนจัดการวิกฤต (Crisis Management) - การกระจายการกระจุกตัว (Diversification)
- การถ่ายโอนความเสี่ยง (Risk Transfer)	เป็นการถ่ายโอนความเสี่ยงให้องค์กรอื่น ได้แก่ การทำสัญญา การทำประกัน เป็นต้น
- การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)	เป็นการหลีกเลี่ยงหรือยุติการดำเนินกิจกรรมที่ก่อให้ เกิดความเสี่ยงที่มีระดับความรุนแรงที่ไม่อาจยอมรับได้ (Unacceptable Risk) ซึ่งการดำเนินการดังกล่าวสามารถทำได้ในทางปฏิบัติ
- การยอมรับ/ดำรงความเสี่ยง (Risk Acceptance)	เป็นแผนดำเนินการจัดสรรเงินทุนที่เหมาะสม เพื่อรองรับความเสียหายที่อาจเกิดขึ้นจากความเสี่ยงที่คงเหลือ อยู่ภายหลังการจัดการความเสี่ยงตามวิธีข้างต้นแล้ว หรือเป็นความเสี่ยงที่มีต้นทุนที่ใช้ในการจัดการไม่คุ้มกับผลประโยชน์ที่จะได้รับ หรือเป็นความเสี่ยงที่สำนัก/ส่วนงาน/องค์กร ไม่สามารถยุติ/หลีกเลี่ยงความเสี่ยงดังกล่าวได้

5.1 การลดโอกาสที่จะเกิดความเสียหาย (Reduce Likelihood) เป็นมาตรการควบคุมความเสี่ยง (Risk Control) ที่จัดการปัจจัยที่ก่อให้เกิดความเสียหายโดยตรงโดยมุ่งลดโอกาสที่จะเกิดเหตุการณ์ความเสียหาย เหมาะกับลักษณะงานที่ต้องปฏิบัติบ่อยครั้งหรือปฏิบัติเป็นประจำ เช่น

- การใช้ระบบงานอัตโนมัติ (Automation) ทดแทนกระบวนการที่ใช้คน (Manual) เป็นผู้กระทำซึ่งจะเหมาะสมกับลักษณะงานที่ต้องปฏิบัติซ้ำๆ จำนวนมาก (Routine work)
- การปรับปรุงกระบวนการทำงาน เพื่อลดความซับซ้อน (Complexity)
- การมีระบบตรวจจับ (Detection) และป้องกัน (Prevention) การกระทำทุจริต

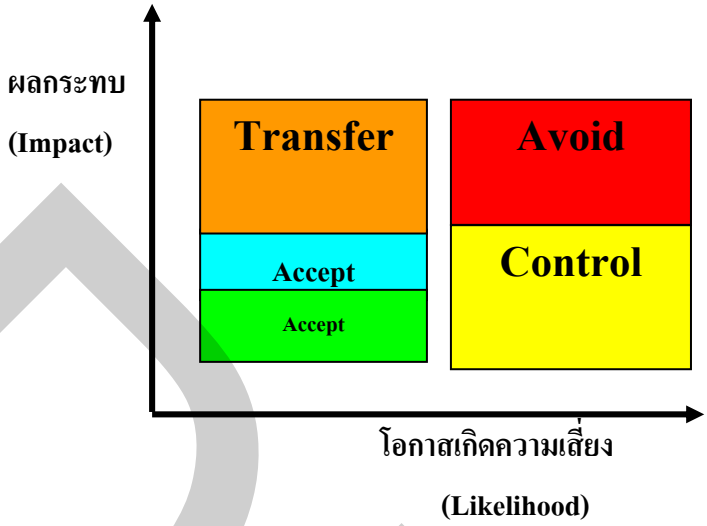
- การกำหนดให้มี Checklist เพื่อตรวจสอบความถูกต้องครบถ้วนในการทำงาน

5.2 การลดขนาดของความเสียหาย (Reduce Impact) เป็นมาตรการจัดการความเสี่ยงโดยมุ่งลดขนาดความเสียหายที่เกิดขึ้นแล้ว เหมาะกับความเสี่ยงที่เกิดจากปัจจัยภายนอกที่ควบคุมได้ยาก หน่วยงานผู้ประเมินอาจจะใช้วิธีการกระจายความเสี่ยงหรือไม่ให้เกิดการกระจุกตัวของความเสี่ยง (Diversification) เช่น การจำกัดขนาดของธุรกรรมหรือปริมาณธุรกรรมโดยรวมไว้ในระดับต่ำ แต่หากความเสี่ยงอยู่นอกเหนือความสามารถที่จะควบคุม หรือไม่สามารถลดการกระจุกตัวได้ อาจจะเลือกการจัดการความเสี่ยงโดยการจัดทำแผนดำเนินการ/แผนฉุกเฉิน เพื่อรองรับความเสียหาย และลดผลกระทบจากเหตุการณ์ดังกล่าว เช่น

- จัดทำ Contingency Plan หรือ Business Continuity Plan เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่องในช่วงเกิดเหตุการณ์ความเสียหาย และอยู่ระหว่างการแก้ไขเพื่อให้กลับสู่สภาพการดำเนินงานตามปกติได้เร็วที่สุด

- จัดทำแผนจัดการกับวิกฤตทางธุรกิจ เมื่อเกิดเหตุการณ์ความเสียหาย (Effective Crisis Management Plan) เป็นวิธีการที่เหมาะกับการจัดการปัญหา หรือการหยุดชะงักทางธุรกิจอันเกิดจากเหตุการณ์ที่ไม่ได้คาดคิด ซึ่งส่งผลกระทบต่อชื่อเสียง/ภาพพจน์ขององค์กรอย่างรุนแรงและอาจไม่สามารถควบคุมได้

หากหน่วยงานดำเนินการควบคุมความเสี่ยงตามวิธีการข้างต้นแล้ว พบว่า ความเสี่ยงยังคงเหลืออยู่ อาจพิจารณาจัดการความเสี่ยงดังกล่าว โดยการถ่ายโอนความเสี่ยง (Transfer) บางส่วน/ทั้งหมดให้องค์กรภายนอกที่สามารถจัดการความเสี่ยงข้างต้นได้ดีกว่า หรือหลีกเลี่ยงความเสี่ยง (Terminate/Avoid) หรือยอมรับความเสี่ยง (Take/Accept/Retain) โดยขึ้นอยู่กับว่าความเสี่ยงที่เหลืออยู่นั้นมีระดับโอกาสและระดับความเสียหายเป็นอย่างไร ทั้งนี้การเลือกวิธีจัดการความเสี่ยงให้พิจารณาเปรียบเทียบค่าใช้จ่ายกับผลประโยชน์ที่จะได้รับ (Cost-Benefit Analysis) ได้แก่ การถ่ายโอน การหลีกเลี่ยง และการยอมรับ ดังภาพที่ 2.7 โดยมีรายละเอียดดังต่อไปนี้



ภาพที่ 2.7 วิธีการจัดการความเสี่ยง

5.1 การถ่ายโอนความเสี่ยง (Risk Transfer) เป็นการถ่ายโอนความรับผิดชอบหรือภาระของการสูญเสียให้กับบุคคลอื่น เช่น การทำประกันภัย การทำสัญญาป้องกันความเสี่ยง เป็นต้น แต่ในขณะเดียวกันก็ก่อให้เกิดความเสี่ยงจากคู่สัญญาไม่สามารถปฏิบัติตามภาระผูกพัน (Counterparty Risk) ซึ่งเป็นสิ่งที่หน่วยงานควรคำนึงในการคัดเลือกวิธีการจัดการกับความเสี่ยง

5.2 การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการตัดสินใจที่จะไม่เข้าไปเกี่ยวข้องกับสถานการณ์ความเสี่ยงนั้น หรือยุติการดำเนินกิจกรรมที่ก่อให้เกิดความเสี่ยง

5.3 การยอมรับ/ดำรงความเสี่ยง (Risk Acceptance) สำหรับกิจกรรมที่ไม่สามารถทำการถ่ายโอนความเสี่ยง หรือยกเลิกกิจกรรมนั้น หน่วยงานจำเป็นต้องยอมรับความเสี่ยงที่อาจเกิดขึ้น แต่ควรพิจารณามาตรการป้องกันความเสี่ยงเพิ่มเติม เช่น การจัดสรรเงินทุนสำรองที่เหมาะสม เพื่อรองรับความเสียหายที่อาจเกิดขึ้นจากความเสี่ยงที่คงเหลืออยู่ภายหลังการจัดการความเสี่ยงตามวิธีดังกล่าวข้างต้นแล้ว

เมื่อหน่วยงานทำการประเมินมาตรการควบคุมความเสี่ยง และทราบความเสี่ยงที่ยังเหลืออยู่ รวมถึงทราบกลยุทธ์และทางเลือกในการจัดการความเสี่ยงที่ระบุข้างต้นแล้วนั้น ควรพิจารณาความเป็นไปได้และค่าใช้จ่ายของแต่ละทางเลือกเพื่อการตัดสินใจเลือกมาตรการจัดการความเสี่ยงและดำเนินการอย่างเป็นระบบ ดังนี้

5.1 พิจารณาว่าจะยอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

5.2 เปรียบเทียบความคุ้มค่าของต้นทุนในการจัดการความเสี่ยง (Cost) กับผลประโยชน์ (Benefit) ที่จะได้รับจากมาตรการดังกล่าว

5.3 พิจารณาติดตามผลการบริหารความเสี่ยงในงวดปีงบประมาณก่อน ที่ยังไม่ได้ดำเนินการหรืออยู่ระหว่างดำเนินการ เพื่อนำมาบริหารความเสี่ยงตามกระบวนการดังกล่าวข้างต้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญ ซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนการปฏิบัติราชการของหน่วยงาน ควรนำมาระบุการควบคุมในแผนบริหารความเสี่ยง

5.4 กำหนดวิธีการควบคุมความเสี่ยงในแผนบริหารความเสี่ยงอย่างเป็นลายลักษณ์อักษรและควรจัดให้มีการสื่อสารและประชาสัมพันธ์ให้พนักงาน รับทราบและปฏิบัติตามแผนการจัดการความเสี่ยงอย่างทั่วถึงทั้งองค์กร

6 กิจกรรมควบคุม (Control Activities) กิจกรรมการควบคุม คือ นโยบายและกระบวนการปฏิบัติงาน ที่จะช่วยให้ผู้บริหารมีความมั่นใจว่าการปฏิบัติงานและการประกอบกิจกรรมของหน่วยงาน มีการดำเนินงานที่สอดคล้องกับเป้าหมายกลยุทธ์ขององค์กร เป็นกิจกรรมที่สามารถช่วยป้องกันและบ่งชี้ให้เห็นความเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ขององค์กร

สำหรับกิจกรรมการควบคุมนั้นแต่ละองค์กร จะมีวิธีการที่แตกต่างกันออกไปขึ้นกับนโยบายในการบริหารและดำเนินงาน ประเภทของธุรกิจ สภาพแวดล้อมภายในองค์กร และวัฒนธรรมขององค์กร แต่ถึงแม้วิธีการควบคุมจะมีความแตกต่างกันในแต่ละองค์กร กิจกรรมการการควบคุมเป็น 4 ประเภท ตามที่ระบุไปแล้ว ข้างต้น คือ การควบคุมเพื่อการป้องกัน การการควบคุมเพื่อให้ตรวจพบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

เมื่อมีการพิจารณาวัตถุประสงค์ของกิจกรรมการควบคุมตามมาตรฐานและแนวคิดของ COSO พบว่ามีวัตถุประสงค์หลัก 3 ประการ คือ

6.1 ประสิทธิภาพและประสิทธิผลของการดำเนินงาน ที่สอดคล้องกับเป้าหมายและวิสัยทัศน์ขององค์กร สำหรับ บสก. ซึ่งเป็นองค์กรที่มียุทธศาสตร์ในการบริหารสินทรัพย์ด้อยคุณภาพ จึงต้องกำหนดให้มีแผนโครงการ และแผนการดำเนินการ รวมถึงกำหนดให้มีกิจกรรมที่ส่งเสริมงานบริหารสินทรัพย์ พัฒนาคุณภาพสินทรัพย์ และจำหน่ายทรัพย์ และให้ความสำคัญต่อกิจกรรมการควบคุมงานประเภทดังกล่าวมากเป็นพิเศษ เพื่อเสริมสร้างสภาพคล่องของ บสก.

6.2 ความเชื่อถือได้ของรายงานการเงิน เนื่องจากรายงานทางการเงินเป็นเครื่องมือสำคัญที่แสดงให้เห็นสถานะของบริษัท ซึ่งมีความเกี่ยวข้องที่จะสร้างความเชื่อมั่นต่อสาธารณชนถึงความเข้มแข็งของบริษัท ที่เกิดจากการวางนโยบาย การดำเนินการ และการควบคุมติดตามผลที่ดี

6.3 การปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง ปัจจุบันภาครัฐให้ความสำคัญต่อการปฏิบัติตามระเบียบข้อบังคับ เพื่อให้เกิดการดูแลบริหารบ้านเมืองที่ดี การควบคุมภายในจึงเข้ามามีบทบาทสำคัญที่จะควบคุมการดำเนินการให้เป็นไปตามกฎระเบียบที่วางไว้

แต่อย่างไรก็ตามกิจกรรมการควบคุมเป็นเพียงเครื่องมือที่จะช่วยให้เกิดการปฏิบัติตามกรอบแนวทางที่วางไว้ หากพนักงานในองค์กรไม่ให้ความร่วมมือ ก็จะไม่สามารถทำให้การบริหารความเสี่ยงขององค์กรประสบความสำเร็จได้ตามเป้าหมาย ดังนั้นการที่จะสร้างให้ระบบกิจกรรมการควบคุมสำเร็จนั้น จะต้องอาศัยพนักงานที่มีความรับผิดชอบเพื่อปฏิบัติหน้าที่ดังกล่าว

7. สารสนเทศและการสื่อสาร (Information & Communication) ระบบสารสนเทศและการสื่อสารเป็นส่วนสำคัญที่จะช่วยให้การบริหารความเสี่ยงภายในองค์กรมีการดำเนินการได้สำเร็จ เนื่องจากสารสนเทศและการสื่อสารจะเป็นเครื่องมือที่ผู้บริหารสามารถใช้ในการถ่ายทอดนโยบายการกำกับดูแลและติดตามผลสำเร็จของการดำเนินงาน ภาพที่ 2.8 แสดงความสัมพันธ์ระหว่างสารสนเทศและการสื่อสารกับระบบการบริหารความเสี่ยง การมีระบบสารสนเทศที่ดีนั้น ควรจัดให้มีระบบสารสนเทศที่ประกอบด้วย

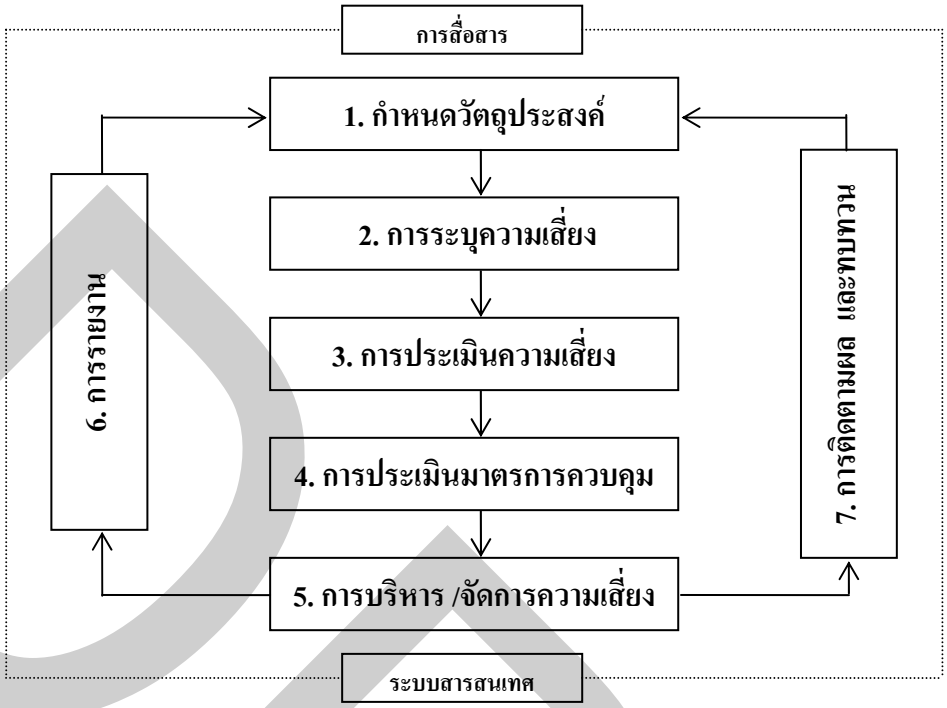
7.1 มีการควบคุมสิทธิ์ของผู้ใช้งาน โดยแบ่งออกเป็นลำดับขั้นตามความรับผิดชอบและประเภทของงาน

7.2 มีระบบสำรองข้อมูลเพื่อป้องกันปัญหาระบบล่ม หรือเกิดเหตุสุดวิสัยที่ส่งผลต่อข้อมูลสำคัญขององค์กร

7.3 มีระบบงานที่สามารถเชื่อมโยงระหว่างหน่วยงาน สามารถบริหารจัดการการใช้ข้อมูลร่วมกันได้อย่างมีประสิทธิภาพ

7.4 มีหน่วยงานสำรองที่มีอุปกรณ์และระบบที่สามารถให้หน่วยงานสำคัญสามารถเข้าปฏิบัติงานได้ทันที หากเกิดเหตุการณ์ฉุกเฉิน เช่น ไฟไหม้ ตึกถล่ม เป็นต้น

7.5 มีระบบการจัดการสินทรัพย์ที่สามารถตอบสนองความต้องการของผู้ใช้งาน วิธีการใช้งานไม่ยากซับซ้อน เพื่อให้สะดวกต่อการปฏิบัติงานต่อไป



ภาพที่ 2.8 ความสัมพันธ์ระหว่างสารสนเทศและการสื่อสารกับระบบการบริหารความเสี่ยง

8. การติดตามประเมินผล (Monitoring) เพื่อให้กลไกการบริหารความเสี่ยงมีประสิทธิภาพและประสิทธิผลที่สมบูรณ์ ควรจัดให้มีระบบการติดตามที่มีความต่อเนื่องอย่างสม่ำเสมอ และเป็นวงจรการประเมินผลที่ทุกหน่วยงานทราบและสามารถดำเนินการเมื่อถึงรอบระยะเวลาการติดตามประเมินผลที่กำหนด เช่น 6 เดือน หรือ ทุกสิ้นปีงบประมาณ โดยใช้วิธีการสร้างระบบการรายงานสถานะความเสี่ยงให้ชัดเจน รวมถึง ความถี่ของการติดตามและจัดทำรายงานรูปแบบรายงาน ตลอดจนวิธีการนำเสนอรายงานต่อผู้บริหาร นอกจากนี้ ควรกำหนดให้มีรายงานในกรณีที่มีเหตุการณ์พิเศษเกิดขึ้น (Exception Reports) เช่น เหตุการณ์ที่ไม่เกิดขึ้นบ่อย แต่ผลกระทบสูงและมีนัยสำคัญ

วัตถุประสงค์สำคัญในการติดตามประเมินผล เพื่อ

8.1 ประเมินคุณภาพและความเหมาะสมของการจัดการความเสี่ยง

8.2 ติดตามผลการจัดการความเสี่ยงที่ได้ดำเนินการไปแล้วหรืออยู่ระหว่างดำเนินการ ว่าบรรลุผลตามวัตถุประสงค์ของการบริหารความเสี่ยงที่วางไว้หรือไม่

8.3 รวจสอบความคืบหน้าของมาตรการควบคุม ว่าสามารถลดโอกาสหรือผลกระทบของเหตุการณ์ความเสี่ยงให้อยู่ในระดับที่ยอมรับได้หรือไม่

การติดตามประเมินผลนั้น หน่วยงานสามารถใช้รายงานบริหารความเสี่ยงเป็นเครื่องมือช่วยในการติดตามประเมินผลได้อย่างเป็นทางการ โดยหน่วยงานสามารถดำเนินการตามแผนการบริหารจัดการความเสี่ยงที่ได้ผล และพิจารณายกเลิกหรือปรับปรุงดำเนินการตามแผนการจัดการความเสี่ยงที่ยังมีข้อบกพร่อง นอกจากนี้แต่ละหน่วยงานอาจมีการจัดทำรายงานการติดตามประเมินผลสำหรับใช้ในหน่วยงานเป็นพิเศษ เช่น การจัดทำ Checklist สำหรับใช้ในหน่วยงานและกำหนดความถี่ในการติดตามเองภายในหน่วยงาน ซึ่งจัดเป็นการติดตามประเมินผลอย่างไม่เป็นทางการ โดยสามารถแบ่งรูปแบบการติดตามประเมินผลของ บสก. ออกเป็น 2 รูปแบบ ประกอบด้วย

8.1 การติดตามผลอย่างเป็นทางการ เป็นการติดตามผลรายครั้ง ตามรอบระยะเวลาที่กำหนด เช่น ทุก 6 เดือนหรือทุกสิ้นปีงบประมาณ โดยใช้แบบฟอร์ม และรายงานตามแบบที่กำหนด

8.2 การติดตามผลอย่างไม่เป็นทางการ เป็นการติดตามผลระหว่างการปฏิบัติงานซึ่งเป็นการติดตามการทำงานในระดับกิจกรรมที่แต่ละหน่วยงานปฏิบัติตามหน้าที่งานประจำวัน เช่น การอนุมัติสินเชื่อ การจัดทำแผนงาน การตรวจสอบเงินสด การตรวจสอบรายงานของผู้บังคับบัญชา เป็นต้น

การรายงานความเสี่ยงเป็นขั้นตอนสำคัญในกระบวนการบริหารความเสี่ยง เพื่อเป็นหลักฐานในการแสดงการวิเคราะห์ ประเมิน และจัดการความเสี่ยงขององค์กร ทั้งนี้เพื่อให้มีการพิจารณาว่ามีความเสี่ยงที่ยังคงเหลืออยู่หรือไม่ และความเสี่ยงดังกล่าวมีระดับความเสี่ยงและมีระดับความรุนแรงที่จะส่งผลต่อการบรรลุวัตถุประสงค์ขององค์กรมากน้อยเพียงใด ในการจัดทำรายงานความเสี่ยงนั้นให้เสนอผู้บังคับบัญชาตามลำดับสายงาน และนำเสนอต่อผู้บริหารสูงสุดขององค์กรในการพิจารณาอนุมัติดำเนินการและสั่งการเพื่อจัดการความเสี่ยงนั้น

สำหรับวัตถุประสงค์ การจัดทำรายงานการบริหารความเสี่ยง ได้แก่ เพื่อให้ผู้บริหารทราบ และตระหนักถึงความเสี่ยงขององค์กร/หน่วยงาน ที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร และพิจารณาแก้ไขได้อย่างทันท่วงที เพื่อให้มั่นใจว่า ความเสี่ยงได้รับการจัดการตามแผนงานที่วางไว้ และเพื่อประเมินว่าแผนการจัดการความเสี่ยงยังสามารถใช้ดำเนินการในสถานการณ์ปัจจุบัน

2.4 องค์ประกอบในระบบงานคอมพิวเตอร์ (วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล, 2548 : 52)

การทำงานด้านระบบงานคอมพิวเตอร์ โดยปกติแล้วมีองค์ประกอบทั่วไปอยู่ 4 อย่างคือ อุปกรณ์คอมพิวเตอร์ โปรแกรม บุคลากร และข้อมูล นอกเหนือจากนั้นแล้ว ยังกล่าวได้ว่ามีอีกหนึ่งองค์ประกอบที่สำคัญคืองานบริการ ซึ่งแต่ละอย่างมีรายละเอียดดังนี้

2.4.1 อุปกรณ์คอมพิวเตอร์ (Hardware) (วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล, 2548 : 110-136)

เป็นอุปกรณ์ที่จับต้อง สัมผัสและสามารถมองเห็นได้อย่างเป็นรูปธรรม ฮาร์ดแวร์ของคอมพิวเตอร์จะมีแบบที่ติดตั้งอยู่ภายในตัวเครื่องคอมพิวเตอร์ (เช่น ซีพียู เมนบอร์ด แรม) และติดตั้งอยู่ภายนอกเครื่องคอมพิวเตอร์ (เช่น คีย์บอร์ด เมาส์ จอภาพ เครื่องพิมพ์) รวมทั้งอุปกรณ์ใช้งานทางด้านระบบเครือข่าย เมื่อใดก็ตามที่ฮาร์ดแวร์ตัวใดตัวหนึ่งเสียหาย หรือไม่สามารถใช้งานได้ ก็สามารถเปลี่ยนหรือซ่อมแซมได้รวมไปถึงอุปกรณ์ที่เกี่ยวข้องกับการใช้งานร่วมกับคอมพิวเตอร์ ซึ่งจะทำงานประสานกันตั้งแต่การป้อนข้อมูลเข้า (input) การประมวลผล (process) และการแสดงของผลลัพธ์ (output) ตามระบบการทำงานของคอมพิวเตอร์ ซึ่งสามารถแบ่งออกได้เป็น 4 ประเภทหลัก ๆ ดังนี้

1. อุปกรณ์นำข้อมูลเข้า (Input Device) เป็นอุปกรณ์ที่เกี่ยวข้องกับการนำข้อมูล หรือชุดคำสั่งเข้ามายังระบบเพื่อให้คอมพิวเตอร์ทำการประมวลผลต่อไปได้ ซึ่งอาจเป็นตัวเลข ตัวอักษร ภาพ กราฟิก เสียง หรือวิดีโอ

2. หน่วยเก็บข้อมูลสำรอง (Secondary Storage Device) จัดเป็นอุปกรณ์ที่ใช้เก็บบันทึกผลลัพธ์ ข้อมูลหรือกลุ่มคำสั่งต่างๆเพื่อไว้ใช้สำหรับในอนาคต ในปัจจุบันนี้มีสื่อที่ผลิตมาสำหรับใช้เก็บข้อมูลสำรองหลากหลายชนิด ซึ่งสามารถแบ่งตามรูปแบบของสื่อที่เก็บได้ดังนี้

2.1 สื่อเก็บข้อมูลแบบจานแม่เหล็ก (Magnetic Disk Device) มีหลายประเภทได้แก่ ฟล็อปปี้ดิสก์ (Floppy disks) หรือฮาร์ดดิสก์ (Hard disks) เป็นอุปกรณ์เก็บบันทึกข้อมูลที่มีโครงสร้างคล้ายกับดิสเก็ตต์ แต่จุข้อมูลมากกว่าและมีความเร็วในการเข้าถึงข้อมูลสูงกว่า ส่วนใหญ่จะถูกติดตั้งภายในเครื่องคอมพิวเตอร์เพื่อใช้สำหรับเก็บตัวโปรแกรมระบบปฏิบัติการ รวมถึงโปรแกรมประยุกต์อื่น ๆ

2.2 สื่อเก็บข้อมูลแบบแสง (Optical Storage Device) นับเป็นสื่อเก็บข้อมูลสำรองที่ได้รับความนิยมมากในปัจจุบัน ซึ่งใช้หลักการทำงานของแสงเข้ามาช่วย การจัดเก็บข้อมูลจะคล้ายกับแผ่นจานแม่เหล็กแต่ต่างกันที่การแบ่งวงของแทรค จะแบ่งเป็นลักษณะคล้ายรูปก้นหอย และเริ่มเก็บบันทึกข้อมูลจากส่วนด้านในออกมาด้านนอก มีหลายประเภทได้แก่ CD แบบ Read และ Write CD-ROM DVD เป็นต้น

2.3 สื่อเก็บข้อมูลแบบเทป (Tape Device) เป็นอุปกรณ์บันทึกข้อมูลที่เหมาะสำหรับการสำรองข้อมูล(backup) ซึ่งเก็บข้อมูลได้ในจำนวนมาก มีลักษณะการเข้าถึงข้อมูลแบบเรียงลำดับต่อเนื่องกันไป (sequential access) โดยเทปที่ใช้ในการเก็บข้อมูล มีการผลิตขึ้นมาหลากหลายขนาดแตกต่างกันไป เช่น DAT หรือ DDS (Digital Audio Tape หรือ Digital Data Storage) มีความจุข้อมูลอยู่ที่ 2-240 GB DLT (Digital Linear Tape) มีความจุข้อมูลอยู่ที่ 20-229 GB LTO (Linear Tape-Open) มีความจุข้อมูลอยู่ที่ 100-200 GB

3. อุปกรณ์แสดงผลลัพธ์ (Output Device) เป็นอุปกรณ์ที่ใช้ในการแสดงผลลัพธ์ที่ได้จากการประมวลผลของคอมพิวเตอร์ โดยผลลัพธ์ที่แสดงออกมา จะมีทั้งข้อมูล ตัวอักษร ภาพนิ่ง ภาพเคลื่อนไหว หรือเสียง ซึ่งแบ่งประเภทได้ดังนี้

3.1 อุปกรณ์แสดงผลหน้าจอ (Display Device) เป็นอุปกรณ์สำหรับการแสดงผลในรูปแบบภาพกราฟิกใช้กับคอมพิวเตอร์ประเภทพีซี ทั่วไป ซึ่งปัจจุบันมีขนาดบาง เบา สะดวกในการเคลื่อนย้าย และยังไม่เปลืองพื้นที่สำหรับการทำงาน

3.2 อุปกรณ์สำหรับพิมพ์งาน (Printing Device) เป็นอุปกรณ์การแสดงผลที่แสดงออกมาให้อยู่ในรูปแบบข้อมูล รายงาน หรือรูปภาพ ซึ่งสามารถจับต้องหรือเก็บรักษาไว้ได้อย่างถาวร ซึ่งมีแบบที่เป็น เครื่องพิมพ์แบบเลเซอร์ (Laser Printer) เป็นเครื่องพิมพ์ที่ได้คุณภาพของงานที่มีความละเอียดสูงมาก และพิมพ์ได้เร็ว หรือเครื่องพิมพ์แบบอิงค์เจ็ต (Ink - jet Printer) เป็นเครื่องพิมพ์ที่มีการทำงานโดยอาศัยน้ำหมึกพ่นลงไปบนกระดาษตรงจุดที่ต้องการและสามารถเลือกใช้ได้ทั้งหมึกสีและขาวดำ

4. อุปกรณ์ทางด้านระบบเครือข่าย

4.1 ตัวรวมสาย (Hub) เป็นอุปกรณ์ที่จำเป็นในการเชื่อมต่อทางระบบเครือข่าย ซึ่งทำให้เครื่องคอมพิวเตอร์ทุกเครื่องส่งสัญญาณถึงกันได้หมด

4.2 อุปกรณ์เลือกเส้นทาง (Router) เป็นอุปกรณ์ที่ใช้ในการเลือกเส้นทางการสื่อสารเพื่อเชื่อมต่อวงจรเครือข่ายท้องถิ่น (LAN) มีเซิร์ฟเวอร์เป็นเสมือนสถานีบริการ เพื่อรองรับผู้ใช้งานด้านคอมพิวเตอร์จำนวนมากในองค์กร router เป็นอุปกรณ์ทำงานคล้าย bridge แต่จะสามารถเชื่อมต่อระบบที่ใช้สื่อ หรือสายสัญญาณต่างชนิดกันได้ เช่น เชื่อมต่อ Ethernet LAN ที่ส่งข้อมูลด้วยสาย UTP (Unshielded Twisted Pair) เข้ากับอีเทอร์เน็ตอีกเครือข่ายซึ่งที่สำคัญยังทำหน้าที่เลือกหรือกำหนดเส้นทางที่จะส่งข้อมูล ระหว่างเครือข่ายและแปลงข้อมูลให้เหมาะสมกับการนำส่ง

4.3 อุปกรณ์ควบคุมการรับ-ส่งข้อมูลในระบบเครือข่ายไร้สาย (Access Point) จะใช้คลื่นความถี่วิทยุ นิยมใช้สำหรับเครือข่ายระยะใกล้ (LAN) ปัจจุบัน access point 1 จุด สามารถรองรับคอมพิวเตอร์เครือข่ายได้ตั้งแต่ 10-255 เครื่อง

2.4.2 โปรแกรม (Software) (วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล, 2548 : 52-53)

เป็นองค์ประกอบทางนามธรรมที่ไม่สามารถจับต้อง หรือสัมผัสได้เหมือนกับฮาร์ดแวร์ ซอฟต์แวร์เป็นส่วนของโปรแกรมคอมพิวเตอร์ที่มีการบรรจุคำสั่ง เพื่อให้คอมพิวเตอร์สามารถทำงานได้ตามที่ผู้ใช้ต้องการ และระบบคอมพิวเตอร์จะไม่สามารถทำงานได้หากปราศจากชุดคำสั่งที่เขียนไว้เหล่านี้ ซึ่งซอฟต์แวร์แบ่งได้เป็น 2 ประเภทใหญ่ๆ คือ

1. ซอฟต์แวร์ระบบ (System Software) เป็นซอฟต์แวร์กลุ่มที่ทำหน้าที่ควบคุมระบบการทำงานของเครื่องคอมพิวเตอร์ ซึ่งในกลุ่มประเภทนี้เป็นที่รู้จักกันเป็นอย่างดีคือระบบปฏิบัติการ (Operating System) เช่น วินโดวส์ (Microsoft Windows) และลีนุกซ์ (Linux) เป็นต้น

2. ซอฟต์แวร์ประยุกต์ (Application Software) เป็นกลุ่มของซอฟต์แวร์ที่สามารถติดตั้งได้ในภายหลังทั้งนี้ขึ้นอยู่กับความเหมาะสมและการประยุกต์ใช้งานเป็นหลัก โดยอาจมีบริษัทผู้ผลิตขึ้นมาเพื่อจำหน่ายโดยตรงทั้งที่ให้เลือกใช้ฟรี ซื้อ ทำเอง หรือจ้างเขียนโดยเฉพาะ

2.4.3 บุคลากร (People) (วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล, 2548 : 54-59)

บุคลากรที่เกี่ยวข้องกับคอมพิวเตอร์ เป็นองค์ประกอบอีกอย่างหนึ่งที่สำคัญมาก เพราะหากบุคลากรไม่มีความรู้ความเข้าใจในการใช้งานเกี่ยวกับระบบคอมพิวเตอร์ ก็จะทำให้การใช้งานไม่มีประสิทธิภาพหรือไม่ได้ผลลัพธ์ตามเป้าหมาย กลุ่มบุคลากรที่เกี่ยวข้องทั้งหมดแบ่งออกได้เป็น 3 กลุ่มด้วยกันคือ

1. กลุ่มผู้ใช้งานทั่วไป (User) เป็นผู้ใช้งานระดับล่างซึ่งไม่จำเป็นต้องมีความเชี่ยวชาญ ก็สามารถใช้งานได้โดยศึกษาจากคู่มือการปฏิบัติงานหรือคู่มือใช้งานโปรแกรมที่นำมาใช้ หรืออาจต้องเข้ารับการอบรมบ้าง เพื่อให้สามารถใช้งานได้ บุคลากรกลุ่มนี้มีจำนวนมากที่สุดในหน่วยงาน และลักษณะงานมักเกี่ยวข้องกับการใช้งานคอมพิวเตอร์ทั่วไป เช่น งานธุรการ งานป้อนข้อมูล เป็นต้น

2. กลุ่มผู้เชี่ยวชาญ (Computer Technician) ส่วนใหญ่มักจะเป็นบุคลากรที่มีความชำนาญทางด้านเทคนิคโดยเฉพาะเช่น ช่างเทคนิคคอมพิวเตอร์ ซึ่งมีหน้าที่หลักคือการแก้ปัญหาที่เกิดขึ้นกับระบบในหน่วยงานให้สามารถใช้งานได้ตามปกติ นักวิเคราะห์ระบบจะมีหน้าที่ในการวิเคราะห์ความต้องการของผู้ใช้ในหน่วยงานว่าต้องการระบบโปรแกรมหรือลักษณะงานแบบไหน อย่างไร เพื่อจะพัฒนาระบบงานให้ตรงกับความต้องการมากที่สุด นักเขียนโปรแกรมจะทำการสร้างระบบงานตามที่นักวิเคราะห์ระบบได้ออกแบบมาเพื่อให้ระบบนั้นสามารถใช้งานได้จริง

3. กลุ่มผู้บริหาร (CIO – Chief Information Officer) ในหน่วยงานขนาดใหญ่ที่ต้องอาศัยเทคโนโลยีคอมพิวเตอร์ขับเคลื่อนงานธุรกิจในองค์กร อาจต้องมีบุคลากรในตำแหน่ง CIO ซึ่งทำหน้าที่กำหนดทิศทาง นโยบายและแผนงานทางคอมพิวเตอร์ในองค์กรทั้งหมดว่าควรเป็นไปในรูปแบบใด

2.4.4 ข้อมูล (Information) (วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล, 2548 : 60)

ข้อมูลเป็นองค์ประกอบที่สำคัญที่ใช้สำหรับการประมวลผลซึ่งการทำงานของระบบด้านคอมพิวเตอร์ จะเกี่ยวข้องกับข้อมูลตั้งแต่การนำข้อมูลเข้า จนกลายเป็นข้อมูลที่สามารถใช้ประโยชน์ต่อได้หรือที่เรียกว่า สารสนเทศ ข้อมูลสำหรับการนำมาประมวลผลด้วยคอมพิวเตอร์นั้นจะได้มาจากแหล่งข้อมูลที่มีแหล่งกำเนิดของข้อมูลที่อยู่ภายในองค์กรทั่วไป ข้อมูลที่ได้มานั้นอาจมาจากพนักงานหรือมีอยู่แล้วในองค์กร เช่น รายชื่อพนักงาน รายชื่อสมาชิกห้องสมุด รายชื่อทรัพยากรของห้องสมุด รายงานการใช้ระบบห้องสมุดอัตโนมัติ เป็นต้น

2.4.5 งานบริการ (Service)

นอกเหนือจากองค์ประกอบทั้ง 4 อย่างข้างต้นแล้ว ในปัจจุบันยังมีงานบริการซึ่งเป็นอีกองค์ประกอบหนึ่ง ที่สามารถกล่าวได้ว่าเป็นส่วนสำคัญต่อระบบงานทางด้านคอมพิวเตอร์ โดยมีส่วนเกี่ยวข้องกับระบบงานต่างๆ ที่มีให้บริการแก่ผู้ใช้งานภายในองค์กร แบ่งเป็นกลุ่มได้ดังนี้

1. Computing Service เป็นบริการที่เกี่ยวข้องกับโปรแกรมการใช้งาน ที่ผู้ใช้ได้รับจากระบบงานต่างๆ เช่น ระบบงานด้านไปรษณีย์อิเล็กทรอนิกส์ (E-mail) ระบบในการจัดหาหรือสั่งซื้อหนังสือ (Acquisition) ระบบจัดเก็บทรัพยากรภายในห้องสมุด (Cataloging) ระบบให้บริการยืม คืนหนังสือ (Circulation) ระบบสำรองข้อมูลห้องสมุดอัตโนมัติ (System Administration) เป็นต้น

2. Communication Service เป็นบริการที่เกี่ยวข้องกับทางด้านเครือข่าย ที่ผู้ใช้บริการได้ใช้ประโยชน์จากการใช้งานเครือข่าย เช่น ผู้ใช้บริการสามารถใช้เครือข่ายเพื่อที่จะเข้าถึงระบบงานหรือสามารถที่จะค้นหาข้อมูลที่ต้องการจากแหล่งข้อมูลทางด้านอินเทอร์เน็ตต่างๆ รวมไปถึงการส่งไปรษณีย์อิเล็กทรอนิกส์ได้

3. Technical Service เป็นบริการที่เกี่ยวข้องกับทางด้านเทคนิคเช่น ระบบทำความเย็น ระบบระบายอากาศภายในห้องปฏิบัติการเครื่องแม่ข่าย การมีระบบด้านจ่ายไฟฟ้าสำรอง และระบบสำรองกระแสไฟฟ้า (UPS) เพื่อให้งานบริการสามารถดำเนินงานได้อย่างต่อเนื่อง และมีความปลอดภัย

2.5 มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

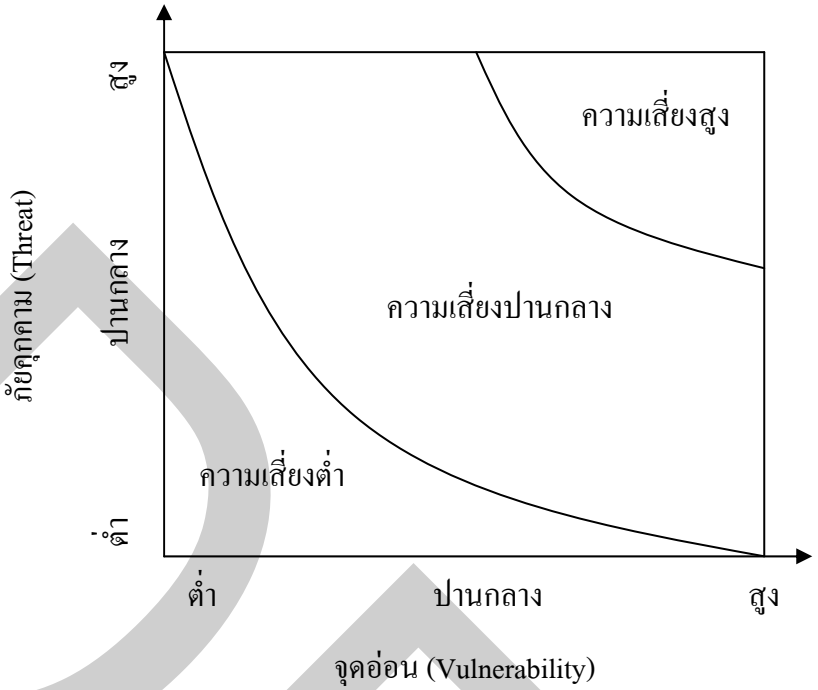
ในประเทศไทย คณะทำงาน คณะอนุกรรมการความมั่นคงภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ถูกจัดตั้งขึ้นตามพระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้นำเอามาตรฐาน ISO 17799 มาเป็นแนวทางในการกำหนดมาตรฐานการรักษาความปลอดภัยทางด้านอิเล็กทรอนิกส์ โดยมีการปรับเปลี่ยนให้มีความเหมาะสมกับสภาวะแวดล้อม และสถานการณ์ทางด้านเทคโนโลยีสารสนเทศในประเทศไทย และปัจจุบัน มาตรฐาน ISO 17799 ได้มี

การปรับปรุงถึงฉบับ Second Edition ซึ่งการจัดทำหนังสือ “มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2) ประจำปี 2549” โดยมีข้อมูลแหล่งที่มาจาก http://www.thaicert.nectec.or.th/event/SecurityStandard/SecurityStandardV2-2549.pdf จะมีเนื้อหาที่สอดคล้องกับมาตรฐานสากล ISO/IEC 17799 ซึ่งในปัจจุบันมาตรฐาน ISO/IEC 17799:2000 ได้รับการปรับปรุงให้ทันสมัยมากยิ่งขึ้น โดยให้มีความสอดคล้องกับเนื้อหาใหม่ ของมาตรฐาน ISO/IEC 17799:2005 ที่ได้รับการปรับปรุงเพิ่มเติม ซึ่งประกอบด้วยมาตรการป้องกันทั้งหมด 133 ข้อ ภายใต้ 39 วัตถุประสงค์ และเพื่อให้มีความเหมาะสมสำหรับการนำไปใช้เป็นแนวทางการศึกษาเพื่อสร้างความมั่นคงปลอดภัย อีกทั้งยังช่วยเอื้อประโยชน์เป็นอย่างมาก ให้กับภารกิจด้านการเสริมสร้างความมั่นคงปลอดภัย ให้กับระบบสารสนเทศต่าง ๆ ขององค์กรทั้งภาครัฐและเอกชน

2.5.1 การบริหารความเสี่ยงเพื่อการรักษาความปลอดภัย (จตุชัย แพงจันทร์, 2550 : 39-40)

การรักษาความปลอดภัยของข้อมูลเป็นกระบวนการในเชิงรุกเพื่อบริหารความเสี่ยง แต่ที่ผ่านมาโดยส่วนใหญ่แล้ว การรักษาความปลอดภัยนั้น จะเป็นแบบเชิงรับ กล่าวคือ องค์กรจะรอให้มีเหตุการณ์เกิดขึ้นก่อนแล้วค่อยหาวิธีการที่จะป้องกันเหตุการณ์นั้น ซึ่งการทำในลักษณะเช่นนี้อาจเกิดความเสียหายกับองค์กรมากเกินคาดก็ได้ โดยการจัดการในเชิงรุกนั้น เป็นขั้นตอนที่ทำก่อนที่จะเกิดเหตุการณ์ขึ้น ถ้าการรักษาความปลอดภัยนั้นเป็นแบบเชิงรับ ค่าใช้จ่ายสำหรับระบบการรักษาความปลอดภัยนั้น ไม่สามารถประเมินได้ อย่างไรก็ตามค่าความเสียหายเมื่อเกิดเหตุการณ์นั้นไม่สามารถทราบได้จนกว่าจะเกิดเหตุการณ์ขึ้นก่อน และเนื่องจากองค์กรไม่ได้เตรียมการไว้ล่วงหน้าก่อนที่จะเกิดเหตุการณ์ จึงทำให้ไม่สามารถทราบได้ถึงความเสียหายจากเหตุการณ์นั้น ดั้งนั้นความเสี่ยงขององค์กรไม่อาจทราบได้จนกว่าจะเกิดเหตุการณ์ขึ้นจริงๆ ซึ่งการรักษาด้านความปลอดภัยนั้นจะมีส่วนเกี่ยวข้องกับการบริหารความเสี่ยงอย่างใกล้ชิด ถ้าไม่มีความเข้าใจเกี่ยวกับความเสี่ยงขององค์กรแล้ว การใช้ทรัพยากรขององค์กรเพื่อการรักษาความปลอดภัยนั้นอาจมากเกินความจำเป็นหรือน้อยกว่าที่ควรจะเป็นก็ได้ นอกจากนี้การประเมินความเสี่ยงก็อาจใช้เป็นพื้นฐาน สำหรับการประเมินค่าของทรัพย์สินขององค์กรไปพร้อมกันได้ด้วย

ความเสี่ยง (Risk) เป็นพื้นฐานที่ทำให้ต้องมีการรักษาความปลอดภัย (Security) ความเสี่ยงคือ ความเป็นไปได้ที่มีการสูญเสียบางสิ่งที่ปกป้องอยู่ ถ้าไม่มีความเสี่ยงก็ไม่จำเป็นต้องมีการรักษาความปลอดภัย เมื่อมีการประเมินความเสี่ยง จึงมีความจำเป็นที่จะต้องเข้าใจถึงจุดอ่อนหรือช่องโหว่ (Vulnerability) และภัยคุกคาม (Threat) ขององค์กร เมื่อรวมจุดอ่อนเข้ากับภัยคุกคาม ก็จะกลายเป็นความเสี่ยง ถ้าไม่มีจุดอ่อนก็จะไม่มีความเสี่ยงหรือถ้าไม่มีภัยคุกคามก็จะไม่มีความเสี่ยงเช่นกัน ภาพที่ 2.9 แสดงความสัมพันธ์ระหว่างความเสี่ยง จุดอ่อน และภัยคุกคาม



ภาพที่ 2.9 ความสัมพันธ์ระหว่างความเสี่ยง จุดอ่อน และภัยคุกคาม

จุดอ่อนหรือช่องโหว่ (Vulnerability) เป็นช่องทางที่สามารถใช้สำหรับการโจมตีได้ ซึ่งจุดอ่อนหรือช่องโหว่ อาจมีอยู่ภายในระบบคอมพิวเตอร์และเครือข่าย โดยเป็นช่องทางโอกาสที่ให้ผู้ไม่ประสงค์ดี สามารถเจาะเข้าระบบหรือเครือข่ายได้ จุดอ่อนนั้นมีหลายระดับขึ้นอยู่กับความยากง่ายและระดับของความชำนาญทางด้านเทคนิคที่จะสามารถใช้ประโยชน์จากมันได้ นอกจากนี้ผลกระทบที่เกิดขึ้น จากการใช้ประโยชน์จากจุดอ่อนดังกล่าวก็จะนับรวมเข้าไปด้วย ยกตัวอย่างเช่น จุดอ่อนประเภทที่ง่ายต่อการเจาะเข้า ซึ่งอาจเป็นเพราะสคริปต์ (Script) ที่ใช้สำหรับเจาะเข้าระบบนั้นหาได้ง่าย และเมื่อทำสำเร็จผู้บุกรุกสามารถควบคุมระบบได้ทั้งหมด จุดอ่อนประเภทนี้ก็จะจัดว่ามีความอันตรายในระดับสูง ในทางตรงกันข้ามถ้าเป็นจุดอ่อนประเภทที่ต้องใช้ความชำนาญสูง และอาจต้องใช้ทรัพยากรจำนวนมากในการเจาะเข้าระบบ ถ้าเจาะเข้าระบบได้แล้ว แต่ได้ข้อมูลที่ไม่ถือว่าสำคัญมากนัก จุดอ่อนประเภทเหล่านี้ก็ถือได้ว่ามีอันตรายในระดับต่ำ จุดอ่อนนั้นไม่ได้มีกับเฉพาะระบบคอมพิวเตอร์ และระบบเครือข่ายเท่านั้นแต่จะรวมถึงทางด้านกายภาพ พนักงานและข้อมูล หรือทรัพย์สิน ที่ไม่ได้อยู่ในรูปแบบอิเล็กทรอนิกส์ด้วย

ภัยคุกคาม (Threat) เป็นสิ่งที่อาจเกิดขึ้นและมีอันตรายต่อทรัพย์สินขององค์กร ภัยคุกคามนั้นประกอบด้วย 3 ส่วนคือ

1. เป้าหมาย (Target) เป้าหมายของการโจมตีในที่นี้ หมายถึง องค์ประกอบด้านต่าง ๆ ของการรักษาความปลอดภัยที่กล่าวถึงคือ ความลับ ความคงสภาพ และความพร้อมใช้งาน ซึ่งภัยคุกคามแต่ละด้านนั้นขึ้นอยู่กับเหตุผลหรือแรงจูงใจ

ความลับ (Confidentiality) ในการรักษาความลับของข้อมูลต่างๆ ภายในหน่วยงาน ซึ่งอาจกระทำได้หลากหลายวิธีด้วยกัน ไม่ว่าจะเป็น การกำหนดสิทธิ์การเข้าถึงข้อมูล เนื่องจากข้อมูลมีความสำคัญและไม่สามารถเปิดเผยให้รับทราบโดยทั่วกันได้และจะเป็นเป้าหมายก็ต่อเมื่อความลับของข้อมูลถูกเปิดเผยต่อผู้ที่ไม่ได้รับอนุญาต ซึ่งในกรณีเช่นนี้ก็เกิดขึ้นเนื่องจากบางคนอาจต้องการทราบข้อมูลที่ห้ามคนอื่นทราบ เช่น ความลับทางราชการ ความลับทางธุรกิจ และข้อมูลส่วนบุคคล เป็นต้น อย่างไรก็ตามข้อมูลที่เป็นข้อมูลส่วนบุคคลที่เก็บไว้โดยเฉพาะในองค์กรทางธุรกิจ ก็อาจจะกลายเป็นเป้าหมายได้เช่นกัน

ความคงสภาพ (Integrity) เป็นความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล โดยจำเป็นต้องให้มีการกำหนดมาตรการ หรือแนวทางในการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล เพื่อไว้ป้องกันความผิดพลาด หรือการเข้าแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต ซึ่งจะตกเป็นเป้าหมายเมื่อภัยคุกคามนั้นพยายามที่จะเปลี่ยนแปลงข้อมูล ผู้บุกรุกในกรณีนี้พยายามที่จะเปลี่ยนแปลงข้อมูลของคนอื่น หรือหลอกลวงให้เชื่อว่าข้อมูลที่ให้ไปถูกต้อง

ความพร้อมใช้งาน (Availability) เป็นความพร้อมสำหรับผู้มีสิทธิ์ในการเข้าถึงข้อมูลในระบบต่างๆ ของหน่วยงาน ต้องสามารถเข้าใช้ข้อมูลได้ในช่วงเวลาที่ต้องการอย่างต่อเนื่อง โดยไม่เกิดเหตุขัดข้อง ซึ่งจะเป็นเป้าหมายเมื่อมีการโจมตีแบบปฏิเสธการให้บริการ โดยการโจมตีนี้ก็อาจมีเป้าหมายเป็นข้อมูลระบบที่ให้บริการข้อมูล หรือเป็นโครงสร้างข้อมูลขององค์กร ซึ่งในการโจมตีนั้นอาจมีเป้าหมายเพื่อทำลายคุณสมบัติของข้อมูล และทรัพย์สินทางด้านสารสนเทศทั้ง 3 ด้านคือ ความลับ ความคงสภาพ และความพร้อมใช้งาน

2. ผู้โจมตี (Agent) เป็นผู้ที่กระทำการใด ๆ ที่ก่อให้เกิดผลทางด้านลบกับองค์กร โดยต้องสามารถเข้าถึงระบบ สถานที่ หรือข้อมูลที่ต้องการ ซึ่งองค์ประกอบที่สำคัญของการเข้าถึงคือโอกาส โอกาสนั้นเกิดขึ้นกับสถานที่หรือเครือข่ายได้เช่น เพียงแค่พนักงานเปิดประตูทิ้งไว้

ผู้โจมตีนั้นจำเป็นต้องมีความรู้หรือข้อมูลเกี่ยวกับเป้าหมาย เช่น บัญชีผู้ใช้ รหัสผ่าน ที่อยู่หรือหมายเลขไอพี ระบบรักษาความปลอดภัย เป็นต้น ผู้โจมตียิ่งมีข้อมูลเกี่ยวกับเป้าหมายมากเท่าใด ยิ่งทำให้ผู้โจมตีมีความรู้เกี่ยวกับจุดอ่อน หรือช่องโหว่ของเป้าหมายมากขึ้นเท่านั้น และผู้โจมตีก็ยิ่งมีโอกาสที่จะรู้วิธีในการใช้ประโยชน์จากจุดอ่อนเหล่านั้นได้ง่าย

ผู้โจมตีนั้นต้องมีแรงจูงใจที่จะกระทำต่อเป้าหมาย ซึ่งแรงจูงใจเป็นคุณสมบัติที่สำคัญที่ควรพิจารณาเพราะจะเป็นสิ่งที่บอกถึงเป้าหมายหลัก สิ่งที่ต้องควรพิจารณาประกอบด้วย ความท้าทาย ความอยากได้ และความตั้งใจที่จะทำอันตรายต่อองค์กรหรือบุคคลใดบุคคลหนึ่ง

ภัยคุกคามเกิดขึ้นเมื่อ ผู้โจมตีมีความรู้เกี่ยวกับเป้าหมายที่ต้องการ และสามารถเข้าถึงได้ด้วยแรงจูงใจ ซึ่งผู้โจมตีอาจเป็นบุคคลดังต่อไปนี้

พนักงาน ซึ่งสามารถเข้าถึงระบบ และมีความรู้ทางด้านที่เกี่ยวกับระบบ เพราะเป็นสิ่งที่จำเป็นสำหรับการทำงาน

พนักงานเก่า ซึ่งคุ้นเคยกับระบบเป็นอย่างดี เนื่องจากคุ้นเคยโดยการทำงานที่นั่นมาก่อน บางบริษัทหรือองค์กรนั้นอาจมีกระบวนการที่ยังหละหลวมอยู่ และเมื่อพนักงานออกจากงาน ทำให้พนักงานเก่าบางคนที่ออกไปแล้วอาจยังมีสิทธิ์ที่จะสามารถเข้าถึงระบบได้

แฮคเกอร์ เป็นบุคคลที่มีแรงจูงใจที่จะทำอันตรายให้บริษัทเสมอ จะด้วยความสามารถในระดับใดก็แล้วแต่ แฮคเกอร์นั้นอาจจะมีหรือไม่มีความรู้ หรือมีข้อมูลเกี่ยวกับระบบ และเครือข่ายขององค์กรก็ได้ การเข้าถึงระบบนั้นอาจผ่านช่องโหว่ หรือจุดอ่อนที่ระบบยังคงมีอยู่ได้

ศัตรูหรือคู่แข่ง เป็นกลุ่มที่ต้องการจะรู้ข้อมูลขององค์กรเสมอ เช่นคู่แข่งทางด้านการค้าอาจต้องการทำลายศักยภาพของคู่แข่งเพื่อให้ได้เปรียบทางด้านการค้า

3. เหตุการณ์ (Event) เป็นวิธีการที่ผู้โจมตีอาจทำอันตรายต่อองค์กร เช่น แฮคเกอร์อาจทำอันตรายโดยการแก้ไขหน้าเว็บไซท์ขององค์กร ได้แก่

- การบุกรุกเข้าห้องควบคุมโดยไม่ได้รับอนุญาต
- การทำลายระบบโดยไม่ได้ตั้งใจ
- การเจาะเข้าระบบโดยไม่ได้รับอนุญาต
- การแก้ไขข้อมูลที่สำคัญทั้งที่ตั้งใจและไม่ตั้งใจ
- การใช้บัญชีผู้ใช้ในทางที่ผิด หรือเกินกว่าที่ได้รับอนุญาต

2.5.2 กระบวนการในการรักษาความปลอดภัยข้อมูล (จตุชัย แพงจันทร์, 2550 : 45-67)

เป็นกระบวนการที่ต้องทำอย่างต่อเนื่อง ประกอบด้วย 5 ขั้นตอนหลักดังนี้คือ

1. การประเมินความเสี่ยง (Risk Assessment) เพื่อแนะนำแนวทางที่ใช้ในการประเมินภัยคุกคาม และความเสี่ยงขององค์กร เพื่อตอบคำถามต่าง ๆ เช่น ต้องการจะปกป้องอะไรบ้าง ใครหรืออะไรที่เป็นภัยคุกคาม จุดอ่อน หรือช่องโหว่ หรือจะเกิดความเสียหายมากน้อยเท่าใดเมื่อถูกโจมตีจุดอ่อน หรือช่องโหว่เหล่านั้น หรือมูลค่าทรัพย์สินขององค์กรมีอะไรบ้างและเท่าไร และจะป้องกันหรือแก้ไขช่องโหว่ หรือจุดอ่อนได้อย่างไร

ผลที่ได้จากการประเมินความเสี่ยง คือข้อแนะนำเกี่ยวกับวิธีป้องกัน เพื่อปกป้องความลับ ความคงสภาพ และความพร้อมใช้งาน และยังคงสามารถทำงานและให้บริการได้ปกติ การประเมินความเสี่ยงสามารถทำได้ โดยการใช้ทรัพยากรภายในหรือภายนอกก็ได้และต้องอาศัยความร่วมมือกันในทุกฝ่าย ถ้าไม่ได้รับความร่วมมือ อาจทำให้การประเมินความเสี่ยงไม่ได้ผลหรือไม่มีประสิทธิภาพ ซึ่งขั้นตอนที่สำคัญของการประเมินความเสี่ยงมี 6 ข้อดังนี้คือ

1.1 การกำหนดขอบเขต เป็นขั้นตอนที่สำคัญที่สุดของกระบวนการ ในการประเมินความเสี่ยง เนื่องจากขอบเขตเป็นสิ่งที่กำหนดว่าอะไรที่จะทำหรือไม่ทำในระหว่างการประเมิน และเป็นการระบุว่าอะไรที่จะปกป้อง ความสำคัญของสิ่งที่พยายามจะปกป้อง และจะต้องปกป้องถึงระดับไหน และละเอียดเพียงใด นอกจากนี้การกำหนดขอบเขต ยังเกี่ยวข้องกับว่าระบบใด หรือแอพพลิเคชันใดที่จะถูกประเมินบ้าง

1.2 เก็บรวบรวมข้อมูล ขั้นตอนนี้เป็นการรวบรวมนโยบาย และระเบียบปฏิบัติที่มีประกาศใช้อยู่ในปัจจุบันและบอกได้ว่าอะไรที่หายไปหรือไม่ได้มีการเก็บไว้ในรูปแบบของเอกสาร การสัมภาษณ์ หรือสนทนากับบุคคลหลักๆ ขององค์กรซึ่งอาจช่วยให้ได้ข้อมูลเกี่ยวกับด้านนี้ได้

1.3 วิเคราะห์นโยบายและระเบียบปฏิบัติ สำหรับการทบทวน และวิเคราะห์นโยบายและระเบียบปฏิบัติขององค์กรที่ประกาศใช้งานในปัจจุบัน เป็นการตรวจสอบดูว่าองค์กรนั้นจัดอยู่ในระดับใดของมาตรฐานความปลอดภัย มาตรฐานความปลอดภัยที่นิยมคือ ISO 17799 (BS 7799) อีกทั้งควรตรวจสอบว่า ส่วนใดขององค์กรที่ไม่ได้ตามมาตรฐาน และควรจะวิเคราะห์ดูว่ามีความจำเป็นที่จะต้องทำให้ได้ตามมาตรฐานหรือไม่ เนื่องจากมาตรฐานทางด้านการรักษาความปลอดภัยนั้นมีอยู่ค่อนข้างมากและส่วนใหญ่จะเป็นมาตรฐานที่ใช้กับองค์กรทั่วไปโดยมาตรฐานเหล่านี้อาจไม่ได้มีการคำนึงถึงลักษณะเฉพาะของแต่ละองค์กร ดังนั้น บางมาตรฐานก็ไม่จำเป็น แต่สำหรับบางองค์กรก็อาจต้องทำมากกว่าที่มาตรฐานกำหนดก็ได้

1.4 วิเคราะห์ภัยคุกคาม (Threat Analysis) เพื่อพิจารณาความเป็นไปได้ของการเกิดภัยคุกคามจึงต้องพิจารณาจากแหล่งกำเนิดภัยคุกคาม ความอ่อนแอไม่มั่นคง และการควบคุมที่มีอยู่ โดยสามารถพิจารณาได้จาก ภัยคุกคามโดยธรรมชาติ ภัยคุกคามโดยมนุษย์ หรือภัยคุกคามจากสภาพแวดล้อม ซึ่งการศึกษาข้อมูลในอดีต ข้อมูลของปัญหา รายงานระบบรักษาความปลอดภัย ยังช่วยให้สามารถระบุแหล่งกำเนิดของภัยคุกคามที่ก่อให้เกิดอันตรายได้อีกด้วย

1.5 วิเคราะห์จุดอ่อนหรือช่องโหว่ (Vulnerability Analysis) มีจุดประสงค์ก็เพื่อเป็นการทดสอบสถานภาพขององค์กร ในปัจจุบันว่าล่อแหลมต่อการถูกโจมตี หรือถูกทำลายมากน้อยแค่ไหน หรือเป็นการทดสอบการรักษาความลับ ความคงสภาพ และความพร้อมใช้งานของข้อมูลที่สำคัญ

ขององค์กร และนอกจากนี้ยังเป็นการทดสอบว่าเครื่องมือหรือระบบที่ใช้สำหรับป้องกัน และรักษาความปลอดภัยนั้น มีประสิทธิภาพเพียงพอหรือไม่

1.6 ประเมินความเสี่ยง กระบวนการรักษาความปลอดภัยของข้อมูล มีการเริ่มต้น ที่การประเมินความเสี่ยงหรือการประเมินสถานการณ์ การประเมินความเสี่ยงนั้น จะตอบคำถามที่ว่าอยู่ตรงไหน และกำลังจะไปที่ไหน การประเมินค่าความเสี่ยงนั้น จะรวมถึงการประเมินมูลค่าของทรัพย์สินประเภทข้อมูลขององค์กร ค่าความเสี่ยงของภัยและช่องโหว่ หรือจุดอ่อนของระบบที่อาจทำให้เกิดภัยกับข้อมูลเหล่านั้นได้ และความเสี่ยงโดยรวมขององค์กร ซึ่งเป็นขั้นตอนที่สำคัญ เนื่องจากถ้าไม่ทราบสถานการณ์ปัจจุบันเกี่ยวกับความเสี่ยงต่อองค์กรก็ไม่สามารถติดตั้ง และใช้งานเครื่องมือสำหรับป้องกัน และรักษาความปลอดภัยให้ทรัพย์สินขององค์กรได้ และในการประเมินควรคำนึงถึงปัจจัยต่าง ๆ ที่มีส่วนเกี่ยวข้องดังนี้

1.6.1 การประเมินค่านั้นสามารถทำได้ โดยทำตามขั้นตอนการบริหารความเสี่ยง หลังจากที่สามารถระบุความเสี่ยงต่อภัยและค่าความเสียหายจากภัยนั้นแล้ว ก็สามารถจะเลือกใช้เครื่องมือหรือระบบป้องกันที่เหมาะสม และมีประสิทธิภาพเพื่อป้องกันภัยต่าง ๆ เหล่านั้นได้ โดยจุดมุ่งหมายของการประเมินค่าความเสี่ยงภัยของข้อมูลนั้นประกอบด้วย

- เพื่อประเมินค่าของทรัพย์สินประเภทข้อมูล
- เพื่อประเมินค่าความเสี่ยงภัยที่มีต่อความลับ ความคงสภาพ และความพร้อมใช้งานของทรัพย์สินข้อมูล
- เพื่อตรวจสอบและค้นหาจุดอ่อน หรือช่องโหว่ของระบบในขณะนั้น
- เพื่อประเมินความเสี่ยงขององค์กรที่เกี่ยวกับทรัพย์สินประเภทข้อมูล
- เพื่อแนะนำวิธีปฏิบัติต่อข้อมูล สำหรับช่วยลดความเสี่ยง ให้อยู่ในระดับที่สามารถยอมรับได้
- เพื่อใช้เป็นข้อมูลที่เกี่ยวข้องกับการวางรากฐาน ใช้ในการสร้างระบบการรักษาความปลอดภัย

1.6.2 การประเมินสถานการณ์ในปัจจุบันขององค์กรนั้น แบ่งออกได้ดังนี้

- การวิเคราะห์ความเสี่ยงอยู่ในระดับระบบ (System-Level Vulnerability) เป็นการประเมินเพื่อหาจุดอ่อนของคอมพิวเตอร์แต่ละเครื่องที่ใช้งานในองค์กร ซึ่งเป็นการตรวจสอบระบบเพื่อให้ทราบว่าระบบดังกล่าว สามารถบังคับให้เป็นไปตามนโยบายการรักษาความปลอดภัยในขณะนั้นหรือไม่

- การวิเคราะห์ความเสี่ยงที่อยู่ในระดับของเครือข่าย (Network-Level risk Assessment) เป็นการประเมินค่าความเสี่ยงต่อภัยต่าง ๆ ของระบบคอมพิวเตอร์ และเครือข่าย ทั่วทั้งองค์กร รวมถึงโครงสร้างระบบการจัดการข้อมูลขององค์กร

- การวิเคราะห์ความเสี่ยงในระดับขององค์กร (Organization-Wide Risk Assessment) เป็นการวิเคราะห์และประเมินความเสี่ยงของทั้งองค์กรโดยรวม เพื่อที่จะระบุถึงภัยต่อข้อมูลขององค์กรโดยตรง เพื่อวิเคราะห์และค้นหาจุดอ่อนของการปฏิบัติ และการจัดการข้อมูลขององค์กร โดยจะต้องเก็บข้อมูลที่จัดเก็บในทุกรูปแบบ ไม่ว่าจะเป็นการจัดเก็บทางด้านกายภาพ เช่น บนกระดาษ หรือในรูปแบบของอิเล็กทรอนิกส์ในระบบคอมพิวเตอร์

- การตรวจสอบ (Audit) จะเป็นการตรวจสอบที่เกี่ยวกับนโยบายทางด้านการรักษาความปลอดภัย และตรวจวิเคราะห์ว่าองค์กรได้ปฏิบัติ หรือมีการบังคับใช้นโยบายเหล่านั้นหรือไม่

- การทดสอบเจาะเข้าระบบ (Penetration Test) จะเป็นการทดสอบการเจาะเข้าระบบ เพื่อทดสอบความสามารถขององค์กรในการตอบโต้ต่อการบุกรุก โดยการทดสอบประเภทนี้ควรทำกับเฉพาะองค์กรที่มีระบบการรักษาความปลอดภัยค่อนข้างแข็งแกร่ง เพราะการทดลองเจาะเข้าระบบอาจสร้างความเสียหายให้องค์กรได้

1.6.3 ในการประเมินองค์กรนั้น ควรเก็บรวบรวมข้อมูลจาก 3 แหล่ง คือ พนักงาน เอกสาร และจากการสำรวจตามสภาพจริง ต้องมีการสัมภาษณ์พนักงานที่ทำงานเกี่ยวกับด้านการรักษาความปลอดภัย และผู้ที่เข้าใจและรู้เรื่องเกี่ยวกับลักษณะงานขององค์กรนั้น ๆ การสัมภาษณ์ทั้งผู้บริหารและพนักงานที่ปฏิบัติงานจริง ก็จะได้ข้อมูลที่ต่างมุมกัน ในการสัมภาษณ์นั้นไม่ควรทำให้ผู้ที่ถูกสัมภาษณ์นั้นรู้สึกเหมือนว่าตัวเองกำลังถูกตรวจสอบอยู่ โดยก่อนสัมภาษณ์ควรอธิบายให้ผู้ที่ถูกสัมภาษณ์นั้นเข้าใจถึงจุดประสงค์ของการประเมิน และอธิบายได้ว่าผลที่ได้นั้นจะมีส่วนช่วยในการป้องกัน และรักษาความปลอดภัยให้ทรัพย์สินขององค์กรได้อย่างไร นอกจากนี้ควรอธิบายว่าข้อมูลที่ได้จากการสัมภาษณ์นั้นจะไม่ระบุชื่อของผู้ให้สัมภาษณ์ หรือจะไม่มีผลในด้านลบต่อผู้ที่ถูกสัมภาษณ์โดยตรง

2. กำหนดนโยบาย (Policy) นโยบายและระเบียบปฏิบัติจัดเป็นขั้นตอนต่อไป หลังจากที่ได้ประเมินสถานการณ์ด้านความเสี่ยงไปแล้ว นโยบายและระเบียบปฏิบัตินับเป็นสิ่งที่จะกำหนดถึงระดับความปลอดภัยขององค์กรที่คาดหวังไว้ และเป็นสิ่งที่กำหนดงานที่ต้องทำ ในระหว่างขั้นตอนการติดตั้งระบบด้านการรักษาความปลอดภัย ถ้าไม่มีนโยบายก็จะไม่มีแผนสำหรับองค์กร ที่จะทำให้การรักษาความปลอดภัยขององค์กรมีประสิทธิภาพได้ อย่างน้อยที่สุดนโยบายและระเบียบการปฏิบัติดังต่อไปนี้ควรมีในแต่ละองค์กรสำหรับขั้นตอนการรักษาความปลอดภัย

2.1 นโยบายข้อมูล (Information Policy) ควรกำหนดว่าข้อมูลแบบใด ที่มีความสำคัญ และข้อมูลเหล่านี้ซึ่งประกอบด้วยการจัดเก็บ การถ่ายโอน และการทำลาย นโยบายนี้จะเป็นสิ่งที่เป็นพื้นฐานเพื่อตอบคำถามว่า ทำไมจึงต้องมีการรักษาความปลอดภัย

2.2 นโยบายการรักษาความปลอดภัย (Security Policy) มีการกำหนดเกี่ยวกับระบบที่ควบคุมทางด้านเทคนิคคอมพิวเตอร์ต่าง ๆ

2.3 นโยบายการใช้งาน (Usage Policy) มีการกำหนดนโยบายขององค์กรเกี่ยวกับการใช้งานคอมพิวเตอร์ที่ถูกต้องและเหมาะสม

2.4 นโยบายการสำรอง (Backup Policy) มีการกำหนดความจำเป็น ที่มีส่วนเกี่ยวข้องกับการสำรองระบบคอมพิวเตอร์

2.5 ระเบียบปฏิบัติเมื่อเกิดเหตุการณ์ (Incident Handling Procedure) มีการกำหนดด้านจุดมุ่งหมายและขั้นตอนเกี่ยวกับการจัดการกับเหตุการณ์ที่เกิดขึ้นเกี่ยวกับข้อมูล

2.6 ระเบียบปฏิบัติที่เกี่ยวกับการบริหารจัดการบัญชีของผู้ใช้ (Account Management Procedure) มีการกำหนดขั้นตอนการปฏิบัติ เมื่อต้องเพิ่มบัญชีผู้ใช้ใหม่ และการลบทิ้งบัญชีผู้ใช้ที่ไม่ได้ใช้งานแล้ว

2.7 แผนการฟื้นฟูหลังภัยร้ายแรง (Disaster Recovery Plan) มีการกำหนดแผนสำหรับฟื้นฟูหรือกู้ระบบคอมพิวเตอร์คืนหลังจากที่เกิดภัยธรรมชาติหรือภัยที่เกิดจากมนุษย์

ในการลำดับการกำหนดนโยบาย ถ้าองค์กรยังไม่มีนโยบายใด ๆ เลย ควรเลือกที่จะกำหนดนโยบายใดก่อน คำตอบนั้นขึ้นอยู่กับความเสี่ยงขององค์กรในขณะนั้น ถ้าการป้องกันข้อมูลเป็นสิ่งที่มีความเสี่ยงสูงแล้ว ก็ควรเริ่มพัฒนานโยบายข้อมูลก่อน ในขณะที่ถ้าความเสี่ยงเกี่ยวกับการสูญเสียธุรกิจ อันเนื่องมาจากการขาดแผนการสำหรับฟื้นฟูหลังภัยธรรมชาติ นโยบายการฟื้นฟูหลังภัยร้ายแรงก็ควรเป็นจุดเริ่มต้น อีกปัจจัยหนึ่งที่ควรพิจารณาก็คือ ระยะเวลาสำหรับการวางเอกสารนโยบายเหล่านั้น แผนการฟื้นฟูจากภัยร้ายแรง มีแนวโน้มที่จะใช้ระยะเวลานาน เนื่องจากต้องมีรายละเอียดค่อนข้างมาก และจะเกี่ยวกับหลายหน่วยงานย่อย และบุคลากรมากหรือบางทีอาจจะต้องเกี่ยวข้องกับบริษัทข้างนอกซึ่งอาจต้องจ้างเข้ามาเพื่อช่วยในการทำระบบสำรองเพื่อใช้สำหรับกู้ระบบคอมพิวเตอร์ทั้งหมดคืนหากเกิดปัญหาขึ้น

นโยบายหนึ่งที่ควรกำหนดขึ้นในช่วงแรก ๆ ของกระบวนการคือนโยบายทางด้านข้อมูล นโยบายข้อมูลจะเป็นสิ่งที่กำหนดพื้นฐานว่าข้อมูลขององค์กรมีความสำคัญอย่างไร และมีวิธีป้องกันอย่างไร นอกจากนี้นโยบายจะเป็นตัวที่กำหนดการฝึกอบรม สำหรับพนักงานเพื่อให้ทราบวิธีปฏิบัติและปฏิบัติต่อข้อมูลอย่างระมัดระวัง

อย่างไรก็ตามเป็นไปได้ที่อาจจะมีการเขียนหลาย ๆ นโยบายขึ้นพร้อมกัน เนื่องจากแต่ละนโยบายอาจจะเกี่ยวข้องกับบุคลากรที่ต่างกันเล็กน้อย ยกตัวอย่างเช่น ผู้ดูแลระบบอาจต้องมีส่วนเกี่ยวข้องกับนโยบายการรักษาความปลอดภัยมากกว่านโยบายด้านข้อมูล ในกรณีนี้หน่วยงานรักษาความปลอดภัยอาจเป็นหน่วยงานแม่ที่ควรต้องดำเนินการทำนโยบายการรักษาความปลอดภัย หรือฝ่ายบุคคลอาจต้องเกี่ยวข้องกับนโยบายการใช้งาน และนโยบายการจัดการเกี่ยวกับบัญชีผู้ใช้มากกว่านโยบายการสำรองระบบ การกำหนดนโยบายนั้นก็อาจเริ่มจากการร่างหัวข้อเรื่องคร่าว ๆ หรือนโยบายคร่าว ๆ ก็ได้

โดยส่วนใหญ่ฝ่ายการรักษาความปลอดภัยนั้นอาจเริ่มจากนโยบายเล็ก ๆ ที่จะต้องเขียนข้อความไม่เยอะและไม่เกี่ยวข้องกับหลายหน่วยงานหรือบุคลากรมากนัก ซึ่งอาจเป็นโอกาสสำหรับฝ่ายรักษาความปลอดภัยที่จะเริ่มเรียนรู้และเข้าใจวิธีที่จะสร้างนโยบายอื่น ๆ

ในการปรับปรุงนโยบายที่มีใช้อยู่แล้ว ถ้าองค์กรมีนโยบายและระเบียบปฏิบัติอยู่แล้ว ก็เป็นสิ่งที่ได้เปรียบอย่างไรก็ตามนโยบายและระเบียบปฏิบัติเหล่านี้อาจต้องมีการปรับปรุงให้มีความทันสมัย ถ้าฝ่ายรักษาความปลอดภัยเป็นหน่วยงานที่สร้างนโยบายและระเบียบปฏิบัติเหล่านั้นก็อาจเริ่มจากการรวบรวมคณะที่จัดทำนโยบายนั้น โดยเริ่มพิจารณาจากเอกสารที่มีอยู่แล้ว และวิเคราะห์ว่ามีจุดด้อยตรงไหน

ถ้าเอกสารนั้นเขียนโดยบุคคล หรือคณะบุคคลที่ยังทำงานอยู่ในองค์กรนั้น บุคคลหรือคณะนั้น ควรมีส่วนร่วมในการปรับปรุงนโยบายให้ทันสมัยด้วย อย่างไรก็ตามฝ่ายการรักษาความปลอดภัย ควรเป็นหน่วยงานหลักที่ควบคุมกระบวนการปรับปรุงนี้ โดยกระบวนการก็ควรจะเริ่มจากเอกสารที่มีอยู่และค่อยพิจารณาจุดด้อยของนโยบายเหล่านั้น

ในกรณีที่คณะที่จัดทำนโยบายไม่ได้อยู่ในองค์กรนั้นแล้ว โดยส่วนใหญ่การเริ่มต้นจากศูนย์อาจเป็นสิ่งที่ง่ายกว่า พิจารณาว่าใครควรเกี่ยวข้องด้วย และเชิญเข้าร่วมกระบวนการปรับปรุงหรือพัฒนาใหม่ และควรแจ้งให้คณะทราบว่าทำไมเอกสารเก่าจึงไม่เพียงพอ

3. การติดตั้งระบบป้องกัน (Implementation) ในการบังคับใช้นโยบายสำหรับการรักษาความปลอดภัยให้ได้ผลนั้นต้องเกี่ยวข้องกับการจัดหาเครื่องมือ เทคนิค และระบบควบคุมการเข้าถึงทางกายภาพ พร้อมทั้งอาจต้องจ้างเจ้าหน้าที่รักษาความปลอดภัยเพิ่ม การบังคับใช้นั้นอาจต้องมีการคอนฟิกระบบใหม่ซึ่งอาจไม่ได้อยู่ในการควบคุม และดูแลของฝ่ายรักษาความปลอดภัย ในกรณีนี้ในการติดตั้งซอฟต์แวร์ระบบการรักษาความปลอดภัยนั้นต้องเกี่ยวข้องกับผู้ดูแลระบบ และผู้ดูแลเครือข่ายด้วย โดยต้องมีการตรวจสอบดูว่าการติดตั้งแต่ละระบบนั้นมีผลต่อสภาพแวดล้อมโดยรวมอย่างไร และมีผลกระทบต่อระบบควบคุมอื่นอย่างไร เช่น การเพิ่มระบบการรักษาความปลอดภัยทางด้านกายภาพนั้นอาจมีผลทำให้ความจำเป็นในการเข้ารหัสข้อมูลนั้นน้อยลง หรือในทางกลับกัน

หรือการติดตั้งไฟร์วอลล์ อาจจะช่วยลดช่องโหว่หรือจุดอ่อนของระบบได้ทันที ซึ่งแนวทางในการออกแบบและติดตั้งระบบเพื่อรักษาความปลอดภัยมีแนวทางต่าง ๆ ดังนี้

3.1 ระบบรายงานการรักษาความปลอดภัย ระบบนี้จะเป็นกลไก ที่ช่วยให้ฝ่ายรักษาความปลอดภัยทราบถึงการปฏิบัติตามนโยบายของพนักงานทั่วไป และเป็นสิ่งที่ใช้ติดตามทางด้านสถานภาพในปัจจุบัน ที่เกี่ยวกับจุดอ่อนโดยรวมขององค์กรด้วย การรายงานนั้นอาจเป็นแบบใช้มือหรืออาจเป็นแบบอัตโนมัติ โดยส่วนใหญ่จะใช้ทั้งสองวิธีควบคู่กันไป

3.2 การเฝ้าระวังการใช้งานระบบ การมอนิเตอร์การใช้งานระบบ จัดว่าเป็นกลไกที่ใช้สำหรับการตรวจสอบการปฏิบัติตามนโยบายการใช้งานของพนักงานซึ่งอาจจะรวมถึงซอฟต์แวร์ที่ใช้มอนิเตอร์การใช้งานอินเทอร์เน็ต จุดมุ่งหมายของการมอนิเตอร์ก็เพื่อตรวจดูว่าพนักงานคนใดที่ชอบฝ่าฝืนนโยบายขององค์กรบ่อย ๆ บางซอฟต์แวร์อาจสามารถป้องกันการเข้าถึงได้และเก็บล็อกเกี่ยวกับความพยายามที่จะฝ่าฝืนไว้ ซอฟต์แวร์บางตัวอาจสามารถลบเกมที่ติดตั้งบนเครื่องได้ หรืออาจเก็บล็อกเกี่ยวกับการติดตั้งโปรแกรมใหม่เข้าไปในระบบก็ได้

3.3 การสแกนช่องโหว่ระบบ การสแกนระบบเพื่อค้นหาจุดอ่อนได้กลายเป็นหัวข้อที่สำคัญเกี่ยวกับการรักษาความปลอดภัย การติดตั้งระบบปฏิบัติการโดยดีฟอลต์นั้นจะมี โพรเซสที่ไม่จำเป็นต้องถูกติดตั้งด้วย และรวมถึงจุดอ่อนและช่องโหว่ด้วย ในขณะที่การตรวจสอบเพื่อค้นหาจุดอ่อนและช่องโหว่ของระบบนั้นเป็นเรื่องที่ง่ายเมื่อใช้เครื่องมือที่มีในปัจจุบัน แต่การแก้ปัญหานั้นเป็นเรื่องที่ยากและต้องใช้เวลา

สำหรับฝ่ายทางด้านการรักษาความปลอดภัย ต้องคอยติดตามว่า มีระบบที่ติดตั้งในเครือข่ายจำนวนเท่าไร และแต่ละระบบมีจุดอ่อนหรือช่องโหว่ใดบ้าง และต้องคอยตรวจสอบเป็นประจำ การรายงานเกี่ยวกับจุดอ่อนหรือช่องโหว่นั้น ต้องแจ้งให้ผู้ดูแลระบบแก้ไขหรือทำการป้องกัน ถ้ามีการติดตั้งระบบใหม่ควรแจ้งให้ทุกฝ่ายทราบเพื่อจะได้สแกนและป้องกันก่อนที่จะถูกเจาะเข้าระบบ

3.4 การปฏิบัติตามนโยบาย การบังคับให้เป็นไปตามนโยบายในด้านการรักษาความปลอดภัยนั้นเป็นเรื่องที่ต้องใช้เวลาพอสมควร การตรวจสอบว่ามีการปฏิบัติตามนโยบายนั้นมี 2 วิธี คือแบบอัตโนมัติและแบบที่ไม่อัตโนมัตินั้นผู้รักษาความปลอดภัยต้องคอยตรวจสอบทุกระบบเพื่อดูว่ามีการฝ่าฝืนนโยบายหรือระเบียบหรือไม่ โดยอาจตรวจสอบล็อกไฟล์ หรืออาจใช้เครื่องมืออื่นเพื่อมอนิเตอร์เหตุการณ์ต่าง ๆ ที่เกิดขึ้นในระบบ วิธีนี้เป็นวิธีที่ใช้เวลามากและมีโอกาสที่จะเกิดข้อผิดพลาดสูง บางองค์กรอาจสุ่มเลือกบางระบบเพื่อสแกน วิธีนี้อาจช่วยลดเวลาในการทำงานแต่ก็เป็นวิธีที่ไม่สมบูรณ์

ในปัจจุบันมีซอฟต์แวร์หลายชุดที่สามารถทำงานแบบอัตโนมัติ การติดตั้งนั้นอาจใช้เวลาและค่อนข้างยุ่งยาก แต่เมื่อติดตั้งเสร็จซอฟต์แวร์ก็จะตรวจสอบการปฏิบัติตามนโยบายได้

ภายในเวลาที่ไม่นานนัก การติดตั้งนั้นต้องอาศัยความช่วยเหลือจากผู้ดูแลระบบเนื่องจากต้องติดตั้งกับทุกระบบที่มีกลไกนี้เพื่อที่จะตรวจสอบการปฏิบัติตามนโยบายอย่างเคร่งครัด และจะรายงานให้ผู้ดูแลระบบทราบตามช่วงเวลาที่กำหนด

3.5 ระบบพิสูจน์ทราบตัวตน (Authentication Systems) จะเป็นกลไกที่ใช้ตรวจสอบผู้ใช้ที่ต้องการล็อกอินเข้าใช้งานระบบ หรือเครือข่าย นอกจากนี้ยังเป็นกลไกสำหรับตรวจสอบการเข้าสถานที่ที่ต้องห้ามด้วย ในการตรวจสอบเพื่อพิสูจน์ทราบนั้นอาจต้องใช้รหัสผ่าน สมาร์ทการ์ด หรือไบโอเมติกก็ได้ ทุกระบบที่ใช้งานภายในองค์กรควรต้องมีระบบพิสูจน์ตัวตน นั่นหมายความว่าผู้ใช้แต่ละคนต้องได้รับการฝึกอบรม เพื่อใช้งานระบบพิสูจน์ตัวตนนี้ ถ้าไม่ได้รับการฝึกอบรมการใช้งานที่ดีอาจใช้เวลานี้ไปทำงานอย่างอื่น ดังนั้น ถ้ามีการเปลี่ยนแปลงระบบในการพิสูจน์ทราบใหม่ก็จำเป็นที่จะต้องจัดอบรมให้ผู้ใช้ก่อน

ระบบพิสูจน์ทราบตัวตนจะมีผลกระทบกับทุกระบบขององค์กร ไม่ควรติดตั้งและใช้งานระบบพิสูจน์ทราบตัวตนก่อนโดยที่ไม่ได้วางแผนล่วงหน้าก่อน ผู้ดูแลและรักษาความปลอดภัยควรทำงานร่วมกับผู้ดูแลระบบ เพื่อให้การติดตั้งและใช้งานระบบพิสูจน์ทราบตัวตนให้เป็นไปอย่างราบรื่นไม่ติดขัด

3.6 การติดตั้งระบบรักษาความปลอดภัย สำหรับการใช้งานอินเทอร์เน็ตนั้น จัดเป็นระบบที่ต้องใช้ไฟร์วอลล์ และ VPN (Virtual Private Network) ซึ่งอาจต้องเปลี่ยนโครงสร้างของเครือข่าย บางทีสิ่งที่สำคัญที่สุดเกี่ยวกับการรักษาความปลอดภัยอินเทอร์เน็ตก็คือ ตำแหน่งของการติดตั้งระบบควบคุมการเข้าถึง เช่น ไฟร์วอลล์ซึ่งต้องติดตั้งระหว่างอินเทอร์เน็ตและเครือข่ายภายใน ถ้าไม่มีระบบป้องกันนี้ ระบบที่อยู่ภายในเครือข่ายก็อาจจะถูกเปิด ให้สามารถถูกโจมตีได้ตลอดเวลา การติดตั้งไฟร์วอลล์นั้นไม่ใช่เป็นเรื่องที่ง่าย ซึ่งบางครั้งอาจรบกวนการใช้งานอินเทอร์เน็ต ของผู้ใช้ภายในด้วย

ทั้งนี้การปรับเปลี่ยนโครงสร้างของเครือข่ายนั้น นับเป็นสิ่งที่ต้องทำควบคู่ไปกับการติดตั้งไฟร์วอลล์และระบบควบคุมการใช้งานอื่น โดยในการติดตั้งระบบนี้ไม่ควรที่จะทำจนกว่าการออกแบบโครงสร้างพื้นฐานของเครือข่าย เสร็จสมบูรณ์แล้ว เพื่อที่จะได้สามารถกำหนดขนาดและประสิทธิภาพของไฟร์วอลล์ ให้เหมาะสมกับปริมาณข้อมูลที่ต้องวิ่งผ่านไฟร์วอลล์ และเพื่อที่จะได้สามารถกำหนดกฎการควบคุมของไฟร์วอลล์เพื่อให้เป็นไปตามนโยบายที่วางไว้

VPN นับเป็นส่วนที่สำคัญสำหรับระบบด้านการรักษาความปลอดภัยให้อินเทอร์เน็ต ในขณะที่ VPN ป้องกันข้อมูลที่วิ่งผ่านอินเทอร์เน็ตโดยมีการเข้ารหัสข้อมูลไว้ นอกจากนี้ VPN ยังช่วยขยายเครือข่ายขององค์กรได้ด้วย

3.7 ระบบตรวจจับและป้องกันการบุกรุก IDS (Intrusion Detection System) เป็นระบบเตือนภัยของเครือข่ายสัญญาณเตือนขโมย เป็นระบบที่ใช้สำหรับการตรวจจับผู้ไม่ประสงค์ดีที่พยายามจะบุกรุกเข้าสถานที่ต้องห้าม IDS ก็ทำงานคล้ายกัน โดยจะแยกแยะได้ระหว่างการเข้าถึงส่วนของเครือข่ายที่ต้องห้ามที่ได้รับอนุญาตหรือเป็นการเข้ามาโดยผิดปกติ IDS นั้นมีหลายประเภท การเลือกใช้งานนั้นก็ขึ้นอยู่กับความเสี่ยงและทรัพยากรที่มีอยู่ขององค์กร IDS อาจต้องใช้ทรัพยากรค่อนข้างมากจากฝ่ายรักษาความปลอดภัย

ระบบตรวจจับการบุกรุกที่รู้จักกันมากที่สุดคือ ซอฟต์แวร์ป้องกันไวรัส ซึ่งซอฟต์แวร์นี้ควรต้องติดตั้งลงในคอมพิวเตอร์ทุกเครื่องรวมถึงเซิร์ฟเวอร์ด้วย ซอฟต์แวร์ป้องกันไวรัสเป็น IDS ที่ใช้ทรัพยากรน้อยที่สุด และ IDS อื่น ๆ ยังประกอบด้วยประเภทต่าง ๆ เช่น การตรวจสอบล็อกไฟล์ด้วยมือ การตรวจสอบล็อกไฟล์แบบอัตโนมัติ Host-based IDS และ Network-based IDS

การตรวจสอบล็อกไฟล์ด้วยมืออาจเป็นวิธีที่อาจได้ผลดี แต่เป็นวิธีที่ใช้เวลามากและมีโอกาสที่จะเกิดข้อผิดพลาดได้สูง โดยธรรมชาติแล้ว คนจะไม่สามารถตรวจสอบล็อกไฟล์ได้อย่างมีประสิทธิภาพเท่าที่ควร เนื่องจากอาจมีจำนวนมากเกินความสามารถ ซอฟต์แวร์ที่ใช้ตรวจวิเคราะห์ล็อกไฟล์แบบอัตโนมัตินั้นอาจเป็นทางออกที่ดีกว่า การติดตั้ง IDS นั้นก็ไม่ควรทำจนกว่าจะได้ระบุพื้นที่ที่เป็นเขตที่มีความเสี่ยงสูง

3.8 การเข้ารหัสข้อมูลหรือเอ็นคริพชัน (Encryption) จะเป็นวิธีที่ใช้ปกป้องความลับ (Confidentiality) ของข้อมูลกลไกในการเข้ารหัสข้อมูลนั้นอาจใช้สำหรับป้องกันข้อมูลในระหว่างที่ส่งผ่านเครือข่าย หรือระหว่างที่จัดเก็บในอุปกรณ์การจัดเก็บข้อมูล เช่น ฮาร์ดดิสก์ เป็นต้น ในการเลือกใช้การเข้ารหัสแต่ละวิธีมี 2 สิ่งที่ต้องพิจารณาคือ อัลกอริธึม (Algorithms) และการบริหารคีย์ (Key Management) โดยสิ่งหนึ่งที่ควรคำนึงถึงเมื่อจะใช้งานการเข้ารหัสคือกระบวนการในการเข้ารหัสข้อมูลนั้นอาจทำให้การไหลของข้อมูลช้าลง ดังนั้น จึงไม่มีความจำเป็นที่ต้องเข้ารหัสทุก ๆ ข้อมูลที่มี

3.8.1 อัลกอริธึม เมื่อติดตั้งระบบการเข้ารหัสข้อมูลแล้วนั้น จุดประสงค์ของการเข้ารหัสข้อมูลนั้น จะเป็นสิ่งที่กำหนดการเลือกอัลกอริธึม การเข้ารหัสแบบไพรเวทคีย์เอ็นคริพชัน (Private Key Encryption) จะทำงานเร็วกว่าพับลิกคีย์เอ็นคริพชัน (Public Key Encryption) อย่างไรก็ตามไพรเวทคีย์เอ็นคริพชันไม่สามารถใช้สำหรับการพิสูจน์ตัวตน เช่น ดิจิตอลซิกเนเจอร์ (Digital Signature) ได้ ซึ่งในการเลือกอัลกอริธึมนั้นควรเลือกที่เป็นที่รู้จักดี ซึ่งได้มีการทดสอบอย่างเปิดเผยมาแล้วว่ามีประสิทธิภาพที่ดี เพราะถ้าใช้อัลกอริธึมที่ไม่รู้จักกับระบบนั้นอาจมีช่องโหว่หรือจุดอ่อนในตัวก็ได้

3.8.2 การบริหารคีย์ ในการติดตั้งกลไกในการเข้ารหัสข้อมูลนั้น จะมีบางส่วนที่เกี่ยวข้องกับการจัดการคีย์ สำหรับการเข้ารหัสแบบจุดต่อจุด (Point-to-Point) ซึ่งโดยส่วนใหญ่จะใช้

การเข้ารหัสแบบไพรเวทเอ็นคริพชันนั้น ระบบจะต้องมีการอัพเดตคีย์เป็นประจำซึ่งส่วนระบบที่ต้องใช้การเข้ารหัสแบบพับลิกคีย์เอ็นคริพชัน จำเป็นต้องมีการแจกจ่ายใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ไปยังผู้ใช้จำนวนมากทำให้ปัญหาที่เกิดขึ้นนั้นยุ่งยากกว่า เมื่อต้องติดตั้งระบบนี้ควรต้องกำหนดให้มีเวลาสำหรับทดสอบการจัดการคีย์ด้วย ซึ่งข้อควรระวังอย่างหนึ่งคือโปรแกรมทดลองนั้นส่วนใหญ่จะมีข้อกำหนดเกี่ยวกับจำนวนผู้ใช้ ในขณะที่เมื่อติดตั้งใช้งานจริงนั้น จะเกี่ยวข้องกับผู้ใช้จำนวนที่มากกว่ามาก

3.9 การรักษาความปลอดภัยทางด้านกายภาพนั้น ส่วนใหญ่มักจะถูกให้แยกออกจากการรักษาความปลอดภัยข้อมูลหรือทางด้านการสื่อสาร การติดตั้งระบบกล้องวงจรปิด กุญแจ การ์ดรูดหรือยามนั้น โดยส่วนใหญ่จะไม่เป็นที่เข้าใจโดยเจ้าหน้าที่รักษาความปลอดภัยข้อมูล ถ้าในกรณีอย่างนี้ควรหาความช่วยเหลือจากภายนอก เนื่องจากระบบรักษาความปลอดภัยทางด้านกายภาพนั้นจะมีผลกระทบต่อพนักงาน คล้ายกับระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์ เมื่อติดตั้งกล้องวงจรปิด หรือการที่ต้องใช้การ์ดรูดเข้ารูดออกจากที่ทำงาน พนักงานต้องการเวลาในการที่จะปรับตัวให้เข้ากับสภาพแวดล้อมใหม่นี้ เมื่อองค์กรกำหนดให้พนักงานทุกคน ต้องติดป้ายแสดงตนเมื่อพนักงานทำหาย องค์กรก็ต้องกำหนดระเบียบปฏิบัติเมื่อบัตรเกิดหาย ไม่เช่นนั้นก็อาจเป็นช่องโหว่หรือจุดอ่อนของระบบได้

ระเบียบปฏิบัติที่ถูกต้องนั้นต้องรวมขั้นตอน หรือวิธีในการพิสูจน์ทราบ ให้แน่ชัดว่าบุคคลที่กำลังพยายามจะเข้ามานั้นเป็นผู้ที่ได้รับอนุญาตจริง การพิสูจน์ตัวตนแบบนี้อาจรวมถึงการที่บัตรมีรูปถ่าย เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยสามารถตรวจสอบได้ บางองค์กรอาจใช้วิธีการพิสูจน์ตัวตนแค่การเซ็นชื่อเท่านั้น ซึ่งนี่อาจเปิดโอกาสให้ผู้ไม่หวังดีสามารถบุกรุกเข้าสถานที่ได้ง่าย

เมื่อติดตั้งระบบรักษาความปลอดภัยทางด้านกายภาพแล้ว ก็ควรจะพิจารณาศูนย์ข้อมูลเป็นพื้นที่ที่ต้องให้ความสำคัญเป็นพิเศษ ศูนย์ข้อมูลนั้นควรมีระบบป้องกันที่หนาแน่น และควรติดตั้งระบบป้องกันไฟไหม้ ระบบควบคุมอุณหภูมิ และระบบสำรองไฟฟ้าที่ดี การติดตั้งระบบเหล่านี้อาจต้องมีการปรับปรุงพื้นที่อย่างมาก การติดตั้งระบบ UPS ใหม่ อาจจำเป็นต้องปิดระบบชั่วคราวซึ่งต้องมีการวางแผนล่วงหน้าอย่างดี

3.10 คณะทำงาน เมื่อได้มีการติดตั้งระบบป้องกัน และรักษาความปลอดภัยใหม่นั้นจะต้องมีเจ้าหน้าที่ที่ดูแลอย่างเหมาะสม บางระบบอาจต้องมีผู้ดูแลระบบอยู่ตลอดเวลา เช่น ระบบพิสูจน์ทราบตัวตน ไฟร์วอลล์ และ IDS เป็นต้น กลไกอื่นอาจต้องมีผู้รับผิดชอบที่จะดำเนินการต่อเมื่อมีเหตุการณ์เกิดขึ้น เช่น การสแกนหาจุดอ่อนของระบบ ซึ่งเมื่อมีการพบจุดอ่อนหรือช่องโหว่ก็จำเป็นต้องให้ผู้ดูแลระบบแก้ไขจุดอ่อนดังกล่าว

ในการฝึกอบรมให้พนักงานนั้น จำเป็นที่ต้องมีเจ้าหน้าที่ที่ถนัดทางด้านนี้ อย่างน้อยที่สุดเจ้าหน้าที่รักษาความปลอดภัยก็ควรจะต้องเข้ามามีส่วนร่วมในการฝึกอบรมเพื่อตอบข้อซักถามต่าง ๆ ที่อาจมีจากพนักงาน ซึ่งเป็นสิ่งที่จำเป็น ถึงแม้ว่าผู้ที่บรรยายจะเป็นเจ้าหน้าที่จากฝ่ายบริหารบุคคล

ประเด็นสุดท้ายที่สำคัญเกี่ยวกับเจ้าหน้าที่คือ ความรับผิดชอบทางด้านการรักษาความปลอดภัยองค์กรนั้นควรถือเป็นหน้าที่และความรับผิดชอบของพนักงานทุกคนในองค์กร นอกจากนี้ควรมีคณะทำงานที่รับผิดชอบทางด้านนี้โดยเฉพาะ เพื่อทำหน้าที่ในการพัฒนานโยบาย ที่เกี่ยวข้องกับการรักษาความปลอดภัย และการบังคับใช้นโยบายเหล่านั้น ซึ่งคณะนี้อาจตั้งเป็นฝ่ายรักษาความปลอดภัย โดยความรับผิดชอบนั้นควรจะตกอยู่กับหัวหน้าฝ่าย

4. การฝึกอบรม (Training) เนื่องจากองค์กรไม่สามารถ ที่จะป้องกันข้อมูลที่สำคัญขององค์กรได้โดยการปราศจากความร่วมมือจากพนักงานขององค์กรทุกคน การจัดการฝึกอบรมเพื่อให้มีรับทราบนั้น ก็เป็นการแจ้งข้อมูลที่จำเป็นให้พนักงานแต่ละคนทราบ การฝึกอบรมนั้นอาจจัดเป็นการประชุมหรือการตีพิมพ์ผ่านสื่อต่าง ๆ ขององค์กร เช่น วารสาร หรือปิดประกาศในที่ต่าง ๆ วิธีที่ดีที่สุดคือ การใช้ทั้ง 3 วิธีควบคู่กันไป และจะต้องทำเป็นประจำด้วย โดยผู้ที่มีส่วนเกี่ยวข้องในการฝึกอบรมมีดังต่อไปนี้

4.1 พนักงาน อาจจะต้องมีการฝึกอบรมเพื่อทำความเข้าใจและทราบว่าการรักษาความปลอดภัยมีความสำคัญอย่างไร นอกจากนี้ควรแจ้งให้ทราบว่าข้อมูลใดมีความสำคัญและเป็นความลับขององค์กร และต้องช่วยกันปกป้องข้อมูลเหล่านั้นไม่ให้รั่วไหลออกไป การฝึกอบรมนั้นจะช่วยให้พนักงานทั่วไปรับทราบข้อมูลที่ควรทราบ รู้วิธีจัดการเกี่ยวกับรหัสผ่าน และช่วยป้องกันจากการถูกโจมตี โดยการฝึกอบรมนั้นควรเป็นแบบสั้น ๆ ควรใช้เวลาประมาณ 1-2 ชั่วโมง พนักงานใหม่ควรได้รับการฝึกอบรมนี้ โดยกำหนดให้เป็นส่วนหนึ่งของการปฐมนิเทศ ส่วนพนักงานเก่าก็ควรได้รับการฝึกอบรมนี้อย่างน้อย 2 ปีต่อครั้ง

4.2 ผู้ดูแลระบบ การฝึกอบรมนั้นก็เป็นสิ่งสำคัญและจำเป็นสำหรับผู้ดูแลระบบด้วย ผู้ดูแลระบบควรปรับความรู้ให้ทันสมัยอยู่เสมอ เช่น เทคนิคการเจาะระบบแบบต่าง ๆ หรือภัยที่อาจเกิดขึ้นได้ และการติดตั้งแพตซ์เพื่อป้องกันการโจมตีใหม่ ๆ การฝึกอบรมประเภทนี้ควรจัดให้มีบ่อยครั้ง เช่น ประมาณเดือนละครั้งและควรมีการเชิญผู้ที่เชี่ยวชาญทางด้านนี้โดยเฉพาะมาฝึกอบรม การฝึกอบรมประเภทนี้อาจจัดให้เป็นส่วนหนึ่งของการประชุมประจำของผู้ดูแลระบบเพื่อช่วยลดเวลา

นอกจากนี้เจ้าหน้าที่รักษาความปลอดภัย ควรจะมีการส่งข้อมูลใหม่ ๆ ที่เกี่ยวกับการรักษาความปลอดภัย ให้ผู้ดูแลระบบทราบทันทีที่ได้รับทราบ แทนที่จะรอแจ้งในที่ประชุม การทำ

เช่นนี้ก็เป็นการช่วยเพิ่มความสัมพันธ์และการทำงานร่วมกันอย่างมีประสิทธิภาพ ระหว่างเจ้าหน้าที่รักษาความปลอดภัยและผู้ดูแลระบบ

4.3 นักพัฒนาแอพพลิเคชัน การฝึกอบรมสำหรับนักพัฒนาโปรแกรมหรือนักพัฒนาแอพพลิเคชันนั้น ควรเป็นส่วนหนึ่งที่เพิ่มจากการฝึกอบรมพนักงานทั่วไป โดยส่วนที่เพิ่มขึ้นมานั้นควรเป็นเรื่องเกี่ยวกับเทคนิคการเขียนโปรแกรมอย่างไรเพื่อให้มีความปลอดภัย นอกจากนี้ก็ควรจะอธิบายถึงเหตุผลและหน้าที่ของฝ่ายรักษาความปลอดภัย ในระหว่างที่ได้มีการพัฒนา กระบวนการรักษาความปลอดภัย

สำหรับโครงการใหม่ฝ่ายรักษาความปลอดภัยนั้น ควรที่จะมีส่วนร่วม ในระหว่างการออกแบบด้วย ซึ่งเป็นการเปิดโอกาส ให้ฝ่ายการรักษาความปลอดภัยได้มีการพิจารณาเกี่ยวกับ เรื่องความปลอดภัย ก่อนที่จะผลิตในระหว่างการอบรมนั้น ควรจะอธิบายให้นักพัฒนาโปรแกรมทราบถึงคุณค่าของความปลอดภัยในช่วงต้นของการผลิตซอฟต์แวร์

4.4 ผู้บริหาร ถ้าผู้บริหารไม่สนับสนุนก็จะไม่มีระบบการรักษาความปลอดภัยสำหรับในองค์กร ดังนั้นคณะผู้บริหารควรได้รับรายงานสถานภาพและความก้าวหน้าเกี่ยวกับโครงการติดตั้งระบบการรักษาความปลอดภัย การเสนอผู้บริหารนั้นควรรวมกับเรื่องอื่นเข้าไปด้วย เช่น การตลาด การศึกษา เป็นต้น ในการเสนอหรือรายงานผู้บริหารประจำนั้นควรมีการรวมเกี่ยวกับผลที่ได้จากการประเมินสถานการณ์ปัจจุบัน และความก้าวหน้าของแต่ละโครงการด้วย ถ้าเป็นไปได้ควรมีมาตรฐานการวัดที่ออกมาเป็นตัวเลข เพื่อบ่งบอกถึงระดับความปลอดภัยขององค์กร หรือการรายงานนั้นควรมีตัวเลขทางด้านสถิติด้วย เช่น จำนวนช่องโหว่ของแต่ละระบบ หรือจำนวนครั้งที่มีการฝ่าฝืนนโยบายหรือมีความพยายามที่จะเจาะเข้าระบบ ในระหว่างการเสนอผู้บริหารนั้น ควรจะนำข้อมูลที่ฝึกอบรมพนักงานทั่วไปให้ทราบด้วยเพื่อเป็นการเตือนผู้บริหารให้ทราบถึงความรับผิดชอบที่มีต่อองค์กร

4.5 คณะเจ้าหน้าที่ฝ่ายรักษาความปลอดภัย ก็ควรปรับปรุงความรู้เกี่ยวกับการรักษาความปลอดภัยเป็นประจำเพื่อจะได้สามารถให้บริการกับองค์กรได้ การฝึกอบรมข้างนอกก็เป็นส่วนที่สำคัญ แต่ทั้งนี้การเชิญวิทยากรหรือผู้เชี่ยวชาญจากภายนอกมาให้บริการภายในก็เป็นสิ่งที่จำเป็นเช่นกัน นอกจากนี้การผลัดกันเสนอข้อมูลเกี่ยวกับเทคนิคหรือเทคโนโลยีใหม่ ๆ ก็เป็นสิ่งที่อาจช่วยได้ เช่น เจ้าหน้าที่แต่ละคนอาจได้รับมอบหมาย เพื่อให้เสนอเรื่องที่เกี่ยวกับการรักษาความปลอดภัย โดยอาจเป็นเรื่องที่ชอบหรือกำลังเป็นที่สนใจ หรือเป็นเรื่องที่เจ้าหน้าที่ส่วนใหญ่ ยังขาดความรู้และชำนาญ หรือความสามารถอยู่

5. การตรวจสอบ (Audit) จัดว่าเป็นขั้นตอนสุดท้าย ในกระบวนการรักษาความปลอดภัย หลังจากที่ได้ประเมินสถานการณ์ขององค์กร แล้วก็กำหนดนโยบายและระเบียบปฏิบัติ ติดตั้งระบบรักษาความปลอดภัยที่จำเป็น ฝึกอบรมเจ้าหน้าที่และพนักงานทั่วไป และท้ายสุดคือการตรวจสอบว่า

มีการฝ่าฝืนนโยบายและระเบียบปฏิบัติหรือไม่ เมื่อกล่าวถึงการตรวจสอบที่เกี่ยวกับด้านการรักษาความปลอดภัยนั้น มักจะหมายถึง การตรวจสอบ 3 ประเภทดังต่อไปนี้

5.1 การตรวจสอบการปฏิบัติตามนโยบาย (Policy Adherence Audit) เป็นเรื่องหลักของการตรวจสอบองค์กร ซึ่งได้มีนโยบายที่กำหนดเกี่ยวกับการรักษาความปลอดภัยขององค์กรแล้ว การตรวจสอบจะตอบคำถามองค์กรนั้นว่า มีระดับความปลอดภัย ตามที่ได้คาดหวังไว้หรือไม่ การตรวจสอบนั้นอาจทำโดยเจ้าหน้าที่ภายในเอง หรืออาจเป็นบุคลากรที่มีความชำนาญจากภายนอก มาตรวจสอบก็ได้ ไม่ว่ากรณีใด ๆ ก็ตามการตรวจสอบนั้นไม่สามารถทำได้ถ้าไม่ได้รับความร่วมมือจากคณะผู้ดูแลระบบ

การตรวจสอบการปฏิบัติตามนโยบายนั้น ไม่ควรที่จะเน้นในเฉพาะระบบคอมพิวเตอร์เท่านั้น ควรให้ความสำคัญกับข้อมูลที่มีอยู่ในรูปแบบอื่นด้วย ควรตรวจสอบด้วยว่านโยบายข้อมูลนั้นมีการปฏิบัติตามเคร่งครัดแค่ไหน หรือเอกสารที่มีข้อมูลที่สำคัญมีการจัดเก็บหรือรับส่งอย่างไร

การตรวจสอบควรกระทำปีละครั้ง ในการตรวจสอบนั้น อาจทำโดยเจ้าหน้าที่จากฝ่ายรักษาความปลอดภัย หรืออาจจะเป็นการดีกว่าที่จะตั้งฝ่ายตรวจสอบต่างหาก หรืออาจจ้างบริษัทข้างนอก ซึ่งมีความชำนาญทางด้านนี้โดยเฉพาะมาทำงานให้ เพราะจะได้ตรวจสอบการทำงานของฝ่ายรักษาความปลอดภัยด้วย

5.2 การประเมินโครงการใหม่ สำหรับคอมพิวเตอร์และเครือข่าย นับเป็นเทคโนโลยีที่มีการเปลี่ยนแปลงตลอดเวลา ซึ่งจะทำให้ผลที่ได้จากการประเมินนั้นอาจล้าสมัยในไม่ช้า เนื่องจากจุดอ่อนหรือช่องโหว่เก่าอาจถูกป้องกันไว้หมดแล้วในระบบใหม่ แต่ก็อาจจะมีช่องโหว่ หรือจุดอ่อนใหม่ที่ยังไม่ได้ค้นพบก็ได้ ด้วยเหตุนี้การประเมินสถานการณ์ควรกระทำเป็นประจำ การประเมินทั้งระบบหรือองค์กรนั้น ควรกระทำปีละครั้งหรือสองปีครั้งก็ได้ และเมื่อมีโครงการที่ต้องติดตั้ง หรือพัฒนาระบบใหม่ ก็ควรจะมีการประเมินหรือตรวจทดลองระบบใหม่ก่อนทุกครั้งว่ามีความปลอดภัยมากน้อยแค่ไหนก่อนที่จะใช้งานจริง ซึ่งถ้าเป็นการพัฒนาระบบใหม่นั้น ก็ควรจะมีการตรวจสอบในระหว่างการออกแบบ เพื่อจะได้แก้ไขปัญหา ก่อนที่จะผลิตออกมาใช้งานจริง

5.3 การทดลองเจาะระบบ (Penetration Testing) สำหรับการทดลองเจาะระบบนั้นหลายครั้งที่การทดลองเจาะระบบนั้นจัดไว้ในช่วงของการประเมินสถานการณ์ การทดลองเจาะระบบนั้นคือการใช้เครื่องมือเพื่อทดลองเจาะระบบหรือองค์กรโดยใช้ประโยชน์จากจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักกันทั่วไป ซึ่งถ้าการเจาะระบบสำเร็จ ข้อมูลที่ได้จากการทดสอบนี้ คือทราบว่าองค์กรหรือระบบมีจุดอ่อน หรือช่องโหว่เพิ่มขึ้นอย่างน้อยหนึ่งจุด ถ้าการทดสอบเจาะเข้าระบบไม่เป็นผลสำเร็จ ผลที่ได้จากการทดสอบกณคือ ผู้ทดสอบไม่สามารถจะเจาะเข้าระบบผ่านทางจุดอ่อนนั้นได้ แต่ไม่ได้หมายความว่าจุดอ่อนของระบบนั้นไม่มี ซึ่งหลังจากที่องค์กรได้ประเมินสถานการณ์ แล้วทราบว่า

ระบบมีความเสี่ยงสูง ดังนั้นจึงตัดสินใจที่จะติดตั้งระบบควบคุมการเข้าถึงระบบ การทดสอบเจาะระบบก็อาจเป็นเครื่องมือที่ใช้ทดสอบระบบนี้ได้

การทดสอบเจาะระบบนั้นเหมาะสำหรับการตรวจสอบระบบควบคุมดังต่อไปนี้

- ความสามารถและประสิทธิภาพของ IDS ที่จะตรวจจับการบุกรุกได้
- ความเพียงพอของข้อมูลที่ให้พนักงานรับทราบในระหว่างการฝึกอบรม
- ข้อมูลที่ได้จากการเรียนรู้ระบบเครือข่ายผ่านระบบควบคุมต่าง ๆ
- ความเหมาะสมของระบบรักษาความปลอดภัยทางด้านกายภาพของที่ตั้งนั้น ๆ

การทดสอบจะเพื่อจุดประสงค์ใดก็ตาม ก่อนที่จะทดสอบนั้น ควรมีการวางแผนอย่างละเอียดรอบคอบ และจะต้องแจ้งให้องค์กรทราบล่วงหน้า นอกจากนี้องค์กรควรต้องกำหนดขอบเขตของการทดสอบ การทดสอบเจาะระบบจากภายนอกนั้น จะถูกจำกัดด้วยลิงค์ที่เชื่อมต่อจากภายนอกซึ่งอาจจะรวม หรืออาจจะไม่รวมถึงระบบหมุนโมเด็มก็ได้ นอกจากนี้ควรมีการทดสอบระบบรักษาความปลอดภัยทางด้านกายภาพด้วย โดยอาจจะให้บางคนพยายามที่จะบุกเข้าสถานที่ ที่มีการควบคุมขอบเขตในเรื่องของเวลาอาจเป็นช่วงเวลาทำงานหรืออาจจะเป็นช่วงนอกเวลาทำงานก็ได้ โดยอาจจะอนุญาตให้ผู้ทดสอบสามารถเข้าถึงระบบขององค์กรได้ องค์กรต่าง ๆ อาจเริ่มต้นกระบวนการรักษาความปลอดภัยจากการทดสอบเจาะเข้าระบบ การทำลักษณะนี้อาจจะไม่เกิดผลดีมากนัก เนื่องจากการทดสอบเจาะเข้าระบบนั้นอาจไม่ได้ข้อมูลที่เพียงพอเพื่อจัดการความเสี่ยงขององค์กร

การรักษาความปลอดภัยนั้นเกี่ยวกับการบริหารจัดการความเสี่ยง ถ้าระบบไม่มีความเสี่ยงก็ไม่จำเป็นต้องมีระบบการรักษาความปลอดภัย แต่ถ้าระบบมีความเสี่ยง ก็จำเป็นต้องรู้ว่าเสี่ยงมากน้อยแค่ไหน และต้องออกแบบและติดตั้งระบบอะไร เพื่อที่จะช่วยลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และงบประมาณที่ใช้ไปกับระบบการรักษาความปลอดภัยนั้น อย่างน้อยก็ไม่ควรจะเกินมูลค่าทรัพย์สินที่ต้องการปกป้อง และที่สำคัญคือไม่มากจนเกินความจำเป็น

การรักษาความปลอดภัยนั้นเป็นกระบวนการ โดยทุกคนจะต้องให้ความร่วมมือเป็นอย่างดี เพราะไม่เช่นนั้นข้อมูลอาจเล็ดลอดออกทางใดทางหนึ่งได้ กระบวนการรักษาความปลอดภัยนั้นประกอบด้วย 6 ขั้นตอนหลักคือ การประเมินความเสี่ยง การกำหนดนโยบาย การออกแบบและติดตั้งระบบ การรักษาความปลอดภัย การฝึกอบรมพนักงาน และการตรวจสอบ ซึ่งแต่ละขั้นตอนนั้นมีความจำเป็นและสำคัญทั้งสิ้น ควรจะกระทำอย่างต่อเนื่อง และปรับให้เข้ากับสถานการณ์และความเสี่ยงในตอนนั้น ๆ

2.5.3 กระบวนการจัดการประเมินความเสี่ยง

กระบวนการที่ใช้ในการจัดการประเมินความเสี่ยง มีขั้นตอนดังนี้

1. การประเมินความเสี่ยง คือการศึกษาว่าความเสี่ยงอยู่ในระดับสูงหรือต่ำ ต้องไปดูว่าองค์กรมีความเสี่ยงอะไรบ้าง ระดับความเสี่ยงเป็นอย่างไร ต้องแสดงให้ดูทั้งสูงและต่ำร่วมกัน ถ้าความเสี่ยงอยู่ในระดับต่ำก็สามารถยอมรับได้ แต่หากในขณะที่ความเสี่ยงอยู่ในระดับสูง ก็ต้องไปกำหนดแผนในการที่จะแก้ไขให้ดีขึ้น

2. กำหนดทางเลือกในการที่จะไปจัดการกับความเสี่ยง โดยการนำมาตรการควบคุมที่มีการเลือกมาจากมาตรการป้องกันในมาตรฐาน ISO 17799 ตัวอย่างเช่น ความเสี่ยงในรูปแบบหนึ่งที่จะต้องจัดการคือเรื่องของไวรัส นับเป็นภัยคุกคามอย่างหนึ่ง ซึ่งมาตรการที่ใช้ป้องกันไวรัสจะอยู่ในข้อใดข้อหนึ่ง ในทั้งหมด 133 ข้อ ที่ว่าด้วยเรื่องการจัดการไวรัส โดยการนำภัยคุกคามนี้ไปหาข้อเปรียบเทียบ เพื่อที่จะบอกได้ว่าไวรัสที่เป็นความเสี่ยงขององค์กร อยู่ภายใต้วัตถุประสงค์ใด และก็มาตรการข้อใดที่อยู่ในมาตรฐาน ISO 17799

สำหรับทางเลือกในการป้องกัน อาจมีได้หลากหลาย เช่น การมีรูปแบบที่องค์กรจะใช้ป้องกันไวรัสที่ดี น่าจะเป็นแบบ client-server คือมีเครื่องแม่ข่ายเครื่องหนึ่ง ซึ่งทำหน้าที่ปรับปรุงข้อมูลที่เป็นรายชื่อของไวรัสตัวใหม่ ๆ ที่เกิดขึ้นมาใหม่ มาเก็บไว้ที่ตัวเองแล้วกระจายรายชื่อเหล่านี้ให้กับเครื่องลูกข่าย เพื่อให้ข้อมูลรูปแบบของไวรัสมีความใหม่ ได้รับการปรับปรุงให้ทันสมัยทั่วถึงและเท่าเทียมกัน ซึ่งเมื่อเทียบกับการปรับปรุงรายชื่อไวรัสใหม่ ๆ ลักษณะแบบนี้ จะทำให้รายชื่อหรือรูปแบบของไวรัสแต่ละเครื่องไม่เท่ากัน เครื่องไหนที่ล้าสมัยก็จะไม่สามารถป้องกันตัวเองได้

ดังนั้นทางเลือกในการติดตั้งโปรแกรม จะเห็นได้เป็น 2 ทางเลือก ทางเลือกหนึ่งคือแบบ client-server และอีกแบบหนึ่งคือแบบ 1 เครื่องต่อ 1 โปรแกรม (stand alone) เพราะฉะนั้นจะต้องประเมินทางเลือก ในการที่จะจัดการกับความเสี่ยงจากทางเลือกทั้งสอง จะต้องพิจารณาถึงข้อดีและข้อเสีย และให้เลือกทางที่ดีที่สุดในการจัดการความเสี่ยง ซึ่งก็คือควรเลือกแบบ client-server ที่เป็นทางเลือกสุดท้าย ที่จะต้องไปทำแผนป้องกันขึ้นมา และเมื่อมีการจัดทำแผนการป้องกัน สำหรับภัยคุกคามนั้นขึ้นมาแล้ว ก็จะต้องมีการนำไปฝึกอบรมเพื่อสอนให้แก่ผู้ใช้งานได้ทราบ เพื่อให้ผู้ใช้เกิดความตระหนักและรู้ถึงวิธีการที่จะป้องกันตนเองจากภัยคุกคามเหล่านั้น ซึ่งจะช่วยทำให้ระดับความเสี่ยงของภัยคุกคามเหล่านั้นที่มีต่อองค์กรมีระดับลดลง อยู่ในระดับที่องค์กรสามารถยอมรับได้

การจัดระดับความเสี่ยง (Risk Prioritisation) โอกาสการเกิดภัยคุกคาม (Probability) คือ ระดับของโอกาสการเกิดภัยคุกคามในแต่ละจุดอ่อนนั้น ซึ่งอาจแบ่งเป็น 5 ระดับโดยคิดจากโอกาสการเกิดขึ้นตามช่วงเวลา ดังตารางที่ 2.5

ตารางที่ 2.5 ระดับของโอกาสในการเกิดภัยคุกคาม

Probability	**คำอธิบาย**	**ระดับ**
Catastrophic	เกิดขึ้นประจำ - มีโอกาสเกิดบ่อย อาจเกิดขึ้นเกือบทุกเดือน	5
Major	เกิดขึ้นบ่อยครั้ง - มีโอกาสเกิดหลายครั้งต่อปี	4
Moderate	เกิดขึ้นน้อย - มีโอกาสเกิดขึ้น ปีละครั้ง	3
Minor	เกิดขึ้นบ้าง - มีโอกาสเกิดยาก อาจเกิดได้ในรอบสามปี	2
Insignificant	เกิดขึ้นยาก - มีโอกาสเกิดยากมาก	1

ผลกระทบต่อทรัพย์สิน (Impact) คือ ระดับของผลกระทบและความรุนแรงที่เกิดขึ้นต่อข้อมูลและทรัพย์สินสารสนเทศขององค์กร สามารถแบ่งเป็น 4 ระดับ ดังตารางที่ 2.6

ตารางที่ 2.6 ระดับของผลกระทบและความเสียหายต่อทรัพย์สิน

Probability	**คำอธิบาย**	**ระดับ**
Very High	รุนแรงมาก - มีความเสียหายจะมีผลกระทบสูงมาก	5
High	รุนแรง - มีความเสียหายจะมีผลกระทบสูง	4
Medium	ปานกลาง - มีความเสียหายจะมีผลกระทบปานกลาง	3
Low	น้อย - มีความเสียหายจะมีผลกระทบต่ำ	2
Very Low	น้อยมาก	1

ค่าความเสี่ยง (Risk Value) คือ ค่าของความเสี่ยงโดยรวมทั้งหมด ที่เกิดขึ้นกับทรัพย์สินสารสนเทศในแต่ละรายการ ซึ่งคำนวณหาค่าได้จากสมการที่ 2.2

$$\text{Risk Value} = \text{Probability} * \text{Impact} \qquad (2.2)$$

ระดับค่าความเสี่ยงโดยรวมสามารถสรุปดังตารางที่ 2.7 โดยประกอบด้วย

ค่าความเสี่ยงที่สามารถยอมรับได้มีค่าตั้งแต่ 1-4

ค่าความเสี่ยงที่มีค่าปานกลางควรดำเนินการแก้ไขมีค่าตั้งแต่ 5-11

ค่าความเสี่ยงที่ต้องการแก้ไขอย่างเร่งด่วนมีค่าตั้งแต่ 12-25

ตารางที่ 2.7 ระดับของค่าความเสี่ยงโดยรวม

Probability / Impact	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Very Low (1)	1(1,1)	2(1,2)	5(1,3)	6(1,4)	11(1,5)
Low (2)	3(2,1)	4(2,2)	7(2,3)	8(2,4)	12(2,5)
Medium (3)	9(3,1)	10(3,2)	13(3,3)	14(3,4)	15(3,5)
High (4)	16(4,1)	17(4,2)	18(4,3)	22(4,4)	23(4,5)
Very High (5)	19(5,1)	20(5,2)	21(5,3)	24(5,4)	25(5,5)

2.6 ภาษาเอเอสพี (กิตติ ภักดีวัฒนะกุล, ไชยรัตน์ ปานปั้น 2548 : 2-4**)**

โปรแกรมภาษา ASP (Active Server Pages) เป็นอีกแนวทางหนึ่งสำหรับนักพัฒนา นอกจากจะมีขีดความสามารถในการสร้าง และพัฒนาระบบสารสนเทศบนเว็บผ่านระบบเครือข่ายอินเทอร์เน็ต/อินทราเน็ต โดยผ่านเครื่องมือประเภทเว็บบราวเซอร์ได้อย่างดีแล้ว ยังมีประสิทธิภาพสูงในการนำมาใช้งานร่วมกับฐานข้อมูลประเภทต่างๆ โดยสามารถที่จะสร้าง แก้ไข ค้นหา เรียกใช้งานหรือแสดงผลลัพธ์บนเว็บ อีกทั้งมีการใช้งานที่ง่ายอีกด้วย

วิธีการทำงานในรูปแบบของการใช้ ASP ร่วมกับ ActiveX Data Object (ADO) ซึ่งเป็นเทคโนโลยีใหม่ในการเข้าถึงฐานข้อมูลและข้อมูลจากแหล่งเก็บข้อมูลอื่นๆ ได้อย่างมีประสิทธิภาพ มีความยืดหยุ่นและง่ายต่อการใช้งาน

Active Server Pages เป็นซอฟต์แวร์สำหรับการพัฒนาเว็บแอพพลิเคชัน ซึ่งทำหน้าที่เป็นส่วนขยายของ ISAPI โดยถูกสร้างอยู่บนโครงสร้างพื้นฐานของ ISAPI เพื่อใช้รองรับการพัฒนาเซิร์ฟเวอร์ไซท์แอปพลิเคชั่น ทำให้การพัฒนาไดนามิกเว็บแอพพลิเคชันทำให้สะดวกขึ้น เอกสาร ASP สามารถมีได้ด้วยทั้งแท็ก HTML และเซิร์ฟเวอร์ไซท์สคริปต์ เมื่อเว็บเซิร์ฟเวอร์ได้รับ HTTP จากการเรียกใช้เอกสาร ASP เอกสาร/โปรแกรม ASP ก็จะสร้างไฟล์ผลลัพธ์เป็นเสมือนเอกสาร HTML (อยู่ในหน่วยความจำ) แล้วส่งกลับไปสู่ไคล์เอ็นต์โดยจะเป็นการรวมกันของ Static HTML และ HTML ที่ถูกสร้างขึ้นมาจากการใช้เซิร์ฟเวอร์สคริปต์ (Server Scrip) ทั้งนี้ URL ที่ใช้อ้างถึงเอกสาร ASP จะคล้ายกับการเรียกใช้ ISAPI และ CGI

สคริปต์โค้ดของ ASP จะถูกประมวลผลที่เซิร์ฟเวอร์ จากนั้นจึงส่งผลลัพธ์สุดท้ายของการทำงานซึ่งอยู่ในรูปแบบของ HTML ผ่านทางเครือข่ายอินเทอร์เน็ตและแสดงผลลัพธ์บนบราวเซอร์ของไคลเอ็นต์ โดยไม่คำนึงถึงชนิดของบราวเซอร์และแพลทฟอร์มนั้นๆ ประการที่

สำคัญคือสคริปต์โค้ดของโปรแกรม จะไม่ปรากฏหรือแสดงผลบนบนฝั่งบราวเซอร์ของไคลเอ็นต์ ทำให้ไม่สามารถคัดสำเนาหรือลอกเลียนแบบได้ นอกจากนี้ไคลเอ็นต์สคริปต์อื่นๆ เช่น JavaScript หรือ VBScript ยังไม่สามารถใช้งานร่วมหรือฝังอยู่ในเอกสาร ASP ได้อีกด้วย

แต่สำหรับการใช้งานสคริปต์ในเอกสาร ASP จะสามารถใช้สคริปต์ คือการทำงานของสคริปต์นั้นจะอยู่ที่เซิร์ฟเวอร์ หรือจะใช้ไคลเอ็นต์สคริปต์ คือการทำงานสคริปต์นั้นจะอยู่ที่บราวเซอร์ของผู้ใช้อย่างไรก็ตามการใช้งานไคลเอ็นต์สคริปต์บางภาษาอาจไม่สามารถทำงานกับบราวเซอร์บางชนิดได้ เช่น การใช้ VBScrip ในลักษณะของไคลเอ็นต์สคริปต์ในเอกสาร ASP จะไม่สามารถแสดงผลได้อย่างถูกต้องเมื่อใช้ Netscape บราวเซอร์ในการทำงานกับเอกสาร ASP นั้น

อ็อบเจ็คต่างๆ ใน ASP จะเชื่อมต่อกันได้โดยใช้สคริปต์ ซึ่งอ็อบเจ็คเหล่านี้จะซ่อนรายละเอียดของการทำงานที่ยุ่งยากไว้ ดังนั้นจึงทำให้การพัฒนา ทำง่ายขึ้น เช่น การใช้งาน Session ทำให้ ASP สามารถรองรับข้อมูลจากการทำงานของผู้ใช้แต่ละคนได้และสามารถใช้การรับส่งตัวแปรข้ามเพจได้จนกว่าผู้ใช้จะปิดบราวเซอร์ ซึ่งก่อนที่จะมีการใช้ ASP รองรับข้อมูลของผู้ใช้แต่ละคนเพื่อส่งไปยังเพจต่างๆ นั้น เป็นขั้นตอนที่ซับซ้อนในการสร้างโปรแกรม นอกจากนั้น ASP ยังสามารถเชื่อมต่อกับ Component Object Model (COM) ซึ่งอาจอยู่ใน Windows NT และผลิตภัณฑ์ของ BackOffice ตัวอื่น หรืออาจถูกสร้างโดยผู้ใช้เองหรือจากผู้ผลิตซอฟต์แวร์รายอื่น ๆ ตัวอย่าง เช่น อาจใช้ ASP ร่วมกับ ADO เพื่อใช้ในการเชื่อมต่อกับฐานข้อมูลที่ผ่าน Open Database Connectivity (ODBC) หรือ OLE DB หรืออาจใช้ ASP ร่วมกับ Business อ็อบเจ็คที่สร้างจาก Visual Basic หรือ Visual C++ สำหรับการทำงานที่ต้องการได้

การใช้ ASP มีข้อดีหลายประการสำหรับการใช้ ASP เพื่อพัฒนาเว็บแอพพลิเคชันดังนี้

1.ASP ช่วยเสริมการทำงานไคลเอ็นไซท์สคริปต์ ASP ไม่ใช่สิ่งที่แทนการใช้งานของไคลเอ็นไซท์สคริปต์ เพียงแต่เป็นการเสนอเครื่องมือที่ดีอีกอย่างหนึ่งสำหรับการพัฒนาเว็บไซท์

2.การพัฒนา ASP สามารถเรียนรู้ได้ง่าย สิ่งที่จำเป็นต้องใช้สำหรับการเริ่มต้นใช้งาน ASP คือ ภาษาสคริปต์ของเว็บซึ่งอาจเป็น VBScript หรือ JavaScript สำหรับใช้ในการจัดการกับเหตุการณ์ อ็อบเจ็ค และเมธอดต่างๆ ของ ASP

3.สามารถใช้งานกับทรัพยากรอื่นๆ ที่มีอยู่ในองค์กรได้ เช่น การเชื่อมต่อกับฐานข้อมูลชนิดต่างๆ เช่น Accesss ไปถึง SQL Server หรือ Oracle ได้ และสามารถเชื่อมต่ออ็อบเจ็คอื่นๆ ที่มีอยู่แล้วในระบบ เช่น ActiveX, COM และ DCOM ได้

4.การพัฒนา ASP ไม่ต้องใช้คอมไพล์เลอร์ เดิมการพัฒนาเว็บแอพพลิเคชันต้องอาศัยการคอมไพล์ซอร์สโปรแกรมเพื่อสร้างไฟล์สำหรับทำงาน (Executable) หลังจากที่แอพพลิเคชันถูกคอมไพล์แล้วจึงทำการคัดลอกไปที่ไดเร็กทอรี CGI ของเว็บเซิร์ฟเวอร์ เมื่อแก้ไขแอพพลิเค

ชันแม้เพียงเล็กน้อยก็จะต้องทำตามขั้นตอนข้างต้นใหม่ทั้งหมด แต่ด้วยการพัฒนาเว็บแอพพลิเคชัน โดยใช้ ASP ทำให้ไม่ต้องคอมไพล์แอพพลิเคชันหลังจากที่มีการแก้ไข เพียงจัดเก็บไฟล์ไว้เป็นชื่อเดิม เพื่อรองรับการเรียกใช้จากไคลเอ็นต์ได้ทันที

5.ASP สามารถซ่อนทรัพย์สินทางปัญญาขององค์กรได้ เนื่องจากโค้ด ของ ASP จะอยู่ที่เซิร์ฟเวอร์ ดังนั้นการทำงานของบราวเซอร์ ร่วมกับโค้ดที่อยู่บนเซิร์ฟเวอร์ เพื่อสร้างผลลัพธ์และถูกส่งกลับไปยังบราวเซอร์ โดยเป็นการส่งกลับไปเฉพาะผลลัพธ์ แต่ไม่ส่งโค้ดหรือวิธีการทำงานไปด้วย ซึ่งตรงข้ามกับการทำงานของไคลเอ็นต์สคริปต์ที่จะส่งโค้ดกลับไปยังบราวเซอร์ เพื่อนำไปทำงานร่วมกับข้อมูลของผู้ใช้ในการสร้างผลลัพธ์ซึ่งข้อมูลต่างๆ เหล่านี้สามารถถูกคัดลอกเลียนแบบได้โดยง่าย

2.7 งานวิจัยที่เกี่ยวข้อง

ไพร์ซวอเตอร์เฮาส์คูเปอร์ส (2004:4) ศึกษาเรื่อง แนวทางการบริหารความเสี่ยง มีความมุ่งมั่นสนับสนุนและพัฒนาการบริหารความเสี่ยงให้เกิดขึ้นอย่างต่อเนื่องในองค์กรต่างๆ ในประเทศไทย สืบเนื่องจากการประกาศกรอบสากลของการบริหารความเสี่ยงโดย COSO “Committee of Sponsoring Organizations of the Treadway Commission” เพื่อให้บริษัทจดทะเบียนและองค์กรต่างๆ ได้มีความเข้าใจในแนวทางการบริหารความเสี่ยงที่ถูกต้อง และสามารถนำไปประยุกต์ใช้ในองค์กรแต่ละแห่ง

กฤษฎา แก้วผุดผ่อง (2008:บทคัดย่อ) ศึกษาเรื่อง ระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กรตามมาตรฐานสากล BS 7799 กรณีศึกษา : สำนักหอสมุดมหาวิทยาลัยมหิดล ดำเนินการศึกษาและพัฒนาโดยใช้แนวทางมาตรฐานของอังกฤษที่เรียกว่า BS 7799 (British Standard) หรือมาตรฐาน สากล ISO/IEC 17799:2005 และ ISO/IEC 27001 ที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร ใช้แนวทางการประเมินความเสี่ยงมาประกอบการพิจารณาหาวิธีการหรือมาตรการเพื่อป้องกัน ลดความเสี่ยง และรักษาทรัพย์สินสารสนเทศที่มีค่าขององค์กร โดยมีจัดหมวดหมู่ของทรัพย์สินออกเป็น 5 หมวดคือ อุปกรณ์คอมพิวเตอร์ (Hardware) โปรแกรม (Software) บุคลากร (People) ข้อมูล (Information) และงานบริการ (Service) เพื่อทำการคำนวณหาค่าความเสี่ยงที่เกิดกับทรัพย์สินในแต่ละหมวด แล้วทำการจัดระดับของความเสี่ยง รวมไปถึงการศึกษาเพื่อค้นหาถึงจุดอ่อนของตัวข้อมูลและทรัพย์สินนั้นๆ ซึ่งเป็นสาเหตุที่ก่อให้เกิดปัญหาและภัยคุกคาม เพื่อนำความเสี่ยงที่เกินระดับที่องค์กรสามารถยอมรับได้ ไปดำเนินการควบคุมและแก้ไขความเสี่ยงโดยการออกเป็นมาตรการป้องกันเพื่อให้

บุคลากรในหน่วยงานปฏิบัติตาม รวมทั้งยังเป็นการกำหนดรูปแบบการรับมือในเรื่องความปลอดภัยได้อย่างมีระบบและมีประสิทธิภาพ

Oumeshsingh Sookdawoor (2005:บทคัดย่อ) ศึกษาเรื่อง นโยบายและแนวทางการปฏิบัติด้านการรักษาความปลอดภัยให้กับข้อมูลและสารสนเทศของบริษัทต่าง ๆ ที่ส่วนใหญ่มีความจำเป็นในการใช้งานทางด้านเทคโนโลยีสารสนเทศในพื้นที่ของมอริเชียส (Mauritius) การวิจัยครั้งนี้ มีวัตถุประสงค์ เพื่อหาแนวทางในการจัดทำการประเมินความเสี่ยงและการรักษาความปลอดภัย ให้กับสารสนเทศของธุรกิจ โดยใช้มาตรฐานที่เป็นสากลเช่น BS 7799 สำหรับแนวทางในการจัดทำนโยบายทางด้านการรักษาความปลอดภัยให้กับสารสนเทศขององค์กร และการนำนโยบายที่ได้สร้างขึ้นมาปฏิบัติใช้อย่างจริงจังให้เกิดผลและมีประสิทธิภาพ

กนกวรรณ วีระประสิทธิ์ (2009:บทคัดย่อ) ศึกษาเรื่อง การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ มีบทบาทสำคัญในการปกป้องข้อมูลและระบบเครือข่ายคอมพิวเตอร์ที่เป็นสินทรัพย์ขององค์กร และยังรวมถึงการปกป้อง “พันธกิจ” ขององค์กรให้รอดพ้นจากความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอีกด้วย ขั้นตอนในการบริหารจัดการความเสี่ยงควรจัดให้อยู่ในความรับผิดชอบหลักของฝ่ายเทคนิค ซึ่งมีผู้เชี่ยวชาญทางด้านเทคโนโลยีสารสนเทศเป็นผู้บริหารและฝ่ายบริหาร เพื่อความสามารถในการดำเนินพันธกิจขององค์กรให้บรรลุผลสำเร็จ

คณะกรรมการตรวจเงินแผ่นดิน (2004:บทคัดย่อ) ศึกษาเรื่อง การจัดทำรายงานการควบคุมภายในตามระเบียบคณะกรรมการตรวจเงินแผ่นดินว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน พ.ศ. 2544 เล่มที่ 2 (รายงานตามระเบียบฯ ข้อ 6) เพื่อเป็นแนวทางในการติดตามประเมินผลการปฏิบัติตามระบบการควบคุมภายในที่ใช้อยู่อย่างต่อเนื่องและสม่ำเสมอ เพื่อปรับปรุงแก้ไขการควบคุมภายในให้เป็นปัจจุบันและเหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไปอยู่เสมอ และการจัดทำรายงานตามระเบียบข้อ 6 ซึ่งได้ทำการศึกษาค้นคว้าจากเอกสารและวิธีปฏิบัติเกี่ยวกับการควบคุมภายในขององค์กรวิชาชีพต่างๆ ทั้งในภาครัฐและเอกชนทั่วโลก เช่น ได้นำวิธีการประเมินการควบคุมภายในของ COSO และของสำนักงานตรวจเงินแผ่นดินของสหรัฐอเมริกา (General Accounting Office หรือ GAO)

บทที่ 3
ระเบียบวิธีวิจัย

3.1 ขั้นตอนการดำเนินการวิจัย

ขั้นตอนการดำเนินการวิจัย มีดังต่อไปนี้

1. ศึกษาข้อมูลทางด้านการบริหารความเสี่ยงภายในองค์กร
2. ประเมินความเสี่ยงด้านสารสนเทศ เพื่อเป็นกรณีศึกษา
3. วิเคราะห์และออกแบบระบบต้นแบบ
4. จัดทำและทดสอบระบบต้นแบบ
5. สรุปผลการวิจัยและข้อเสนอแนะ
6. เรียบเรียงงานค้นคว้าอิสระ

3.2 อุปกรณ์และเครื่องมือที่ใช้ในการวิจัย

3.2.1 อุปกรณ์ฮาร์ดแวร์ที่จะนำมาใช้

1. เครื่องเซิร์ฟเวอร์
   - หน่วยประมวลผล Intel Xeon 2.4 GHz
   - หน่วยความจำ (RAM) 1 Gigabyte
   - ความจุของฮาร์ดดิสก์ 136 Gigabyte
   - จอภาพขนาด 15 นิ้ว
   - เม้าส์ และแป้นพิมพ์
2. เครื่องไคลเอนต์
   - เครื่องคอมพิวเตอร์ ระดับ Pentium IV 2.4 GHz
   - หน่วยความจำ (RAM) 256 Megabyte
   - ความจุของฮาร์ดดิสก์ 60 Gigabyte
   - จอภาพขนาด 15 นิ้ว
   - เม้าส์ และแป้นพิมพ์

3. เครื่องคอมพิวเตอร์โน้ตบุ๊ค

- ระดับ Pentium M 1.73 GHz
- หน่วยความจำ (RAM) 2 Gigabyte
- ความจุของฮาร์ดดิสก์ 60 Gigabyte
- จอภาพขนาด 15 นิ้ว
- เม้าส์ และแป้นพิมพ์

3.2.2 ซอฟต์แวร์ที่จะนำมาใช้

1. เครื่องเซิร์ฟเวอร์

- ระบบปฏิบัติการ Windows 2003 Server
- Appserv สำหรับจัดทำเว็บเซิร์ฟเวอร์ ใช้ Internet Information Services (IIS) 4.0 ขึ้นไป
- ระบบฐานข้อมูล Microsoft Access

2. เครื่องไคลเอนต์

- ระบบปฏิบัติการ Windows XP Professional
- เว็บเบราว์เซอร์ Internet Explorer 6.0

3.3 ระยะเวลาในการดำเนินการวิจัย

ระยะเวลาในการดำเนินการวิจัย สรุปได้ดังตารางที่ 3.1

ตารางที่ 3.1 ระยะเวลาในการดำเนินการวิจัย

ระยะเวลาดำเนินงาน (เดือน)	1	2	3	4	5	6	7	8	9	10	11	12
1. ศึกษาข้อมูลทางด้านการบริหารความเสี่ยงภายในองค์กร												
2. ประเมินความเสี่ยงด้านสารสนเทศ เพื่อเป็นกรณีศึกษา												
3. วิเคราะห์และออกแบบระบบต้นแบบ												
4. จัดทำและทดสอบระบบต้นแบบ												
5. สรุปผลการวิจัยและข้อเสนอแนะ												
6. เรียบเรียงงานค้นคว้าอิสระ												

3.4 สรุป

ขั้นตอนในการดำเนินการวิจัย ผู้วิจัยได้มีการแบ่งขั้นตอนที่จะศึกษาออกเป็น 6 ขั้นตอน ได้แก่ ศึกษาข้อมูลทางด้านการบริหารความเสี่ยงภายในองค์กร ขั้นตอนการประเมินความเสี่ยงด้านสารสนเทศ เพื่อเป็นกรณีศึกษา ขั้นตอนการวิเคราะห์และออกแบบระบบต้นแบบ ขั้นตอนการจัดทำและทดสอบระบบต้นแบบ ขั้นตอนการสรุปผลการวิจัยและข้อเสนอแนะ และขั้นตอนการเรียบเรียงงานค้นคว้าอิสระจะเริ่มดำเนินการไปพร้อม ๆ การจัดทำและทดสอบระบบ

บทที่ 4
ผลการวิเคราะห์และการออกแบบระบบ

เนื้อหาของบทนี้กล่าวถึง ผลการศึกษาด้านการจัดการความเสี่ยง ผลการวิเคราะห์ระบบ และผลการออกแบบระบบ โดยมีรายละเอียดดังต่อไปนี้

4.1 แนวทางในการจัดทำระบบบริหารความเสี่ยงของ บสก.

สำหรับแนวทางที่จะยกมาเป็นกรณีศึกษา เพื่อสร้างความเข้าใจเกี่ยวกับแนวทางการจัดทำระบบบริหารความเสี่ยงในคู่มือ เพื่อสร้างเสริมความรู้ความเข้าใจในการทำงานบริหารความเสี่ยงของ บสก. นั้น ผู้วิจัยนำแผนการปฏิบัติงานปี พ.ศ. 2552 มาเป็นกรณีศึกษาการจัดทำระบบบริหารความเสี่ยงที่สอดคล้องตามมาตรฐานของ COSO ทั้ง 8 องค์ประกอบดังนี้

1. สภาพแวดล้อมภายในองค์กร (Internal Environment)
2. การกำหนดวัตถุประสงค์ (Objective Setting)
3. การบ่งชี้เหตุการณ์ (Event Identification)
4. การประเมินความเสี่ยง (Risk Assessment)
5. การจัดการความเสี่ยง (Risk Response)
6. กิจกรรมควบคุม (Control Activities)
7. สารสนเทศและการสื่อสาร (Information & Communication)
8. การติดตามประเมินผล (Monitoring)

บสก. มีการวางแผนการปฏิบัติงาน (Action Plan) ประจำปี พ.ศ.2552 เพื่อตอบสนองต่อเป้าหมายทางยุทธศาสตร์ขององค์กร คือ มุ่งสู่การเป็นองค์กรที่ดูแลสินทรัพย์ด้อยคุณภาพ โดยพึ่งพาตนเองได้ ในการวางแผนดำเนินการเพื่อตอบสนองนโยบายดังกล่าว บสก.ได้มีการจัดทำแผนงานหลัก 8 แผนงาน ประกอบด้วย

1. แผนการบริหารจัดการลูกหนี้ด้อยคุณภาพ (NPL)
2. แผนการบริหารจัดการทรัพย์สินรอการขาย (NPA)
3. แผนการบริหารจัดการด้านการดำเนินคดี

4. แผนจัดเก็บเอกสารสำคัญ

5. แผนงานด้านข้อมูลและระบบงาน

6. แผนการบริหารบุคลากร

7. แผนการบริหารความเสี่ยง

8. แผนงานด้านการเงินและบัญชี

จากแผนงานที่ระบบทั้ง 8 แผนงาน จากข้อมูลการสอบถามและข้อมูลการวิเคราะห์และประเมินตนเอง ผู้วิจัยจึงขอยกด้านระบบเทคโนโลยีและสารสนเทศมาเป็นกรณีศึกษา สำหรับการจัดทำระบบบริหารความเสี่ยง ที่สอดคล้องตามมาตรฐานของ COSO ตามรายละเอียดที่นำเสนอข้างต้น โดยมีรายละเอียดดังนี้

4.1.1 ขั้นตอนที่ 1 สภาพแวดล้อมการควบคุมภายใน

การวิเคราะห์สภาพแวดล้อมการควบคุมอยู่บนหลักการของการวิเคราะห์ SWOT ขององค์กร จากการประเมินสภาพแวดล้อมภายในของ บสก. โดยสภาพแวดล้อมภายใน เป็นองค์ประกอบภายในองค์กรที่สำคัญซึ่งมีส่วนสนับสนุนและผลักดันงานด้านบริหารความเสี่ยงให้เกิดผลสำเร็จ ประกอบด้วย 4 ส่วนหลัก คือ

1. วัฒนธรรมภายในองค์กร ผู้บริหารของ บสก. ให้ความสำคัญและสนใจที่จะผลักดันงานด้านบริหารความเสี่ยงอย่างเต็มที่ จึงเป็นปัจจุบันสำคัญที่ทำให้งานด้านบริหารความเสี่ยงประสบความสำเร็จ ดังนั้นสิ่งที่ควรดำเนินการ คือผลักดันให้พนักงานในองค์กร ตระหนักและเห็นความสำคัญของงานบริหารความเสี่ยง เพื่อสนับสนุนให้เกิดระบบงานบริหารความเสี่ยงที่เป็นภาพรวมทั้งหมดของ บสก.

2. สถานที่ทำการของ บสก. แบ่งออกเป็น 2 ส่วน คือ สำนักงานใหญ่ จำนวน 26 ฝ่าย และภูมิภาคจำนวน 7 ภาค 24 สาขา จำเป็นต้องมีการจัดการบริหารความเสี่ยงอย่างเป็นระบบ และมีการติดตามงานอย่างสม่ำเสมอ

3. โครงสร้างองค์กร บสก. มีการปรับปรุงและเปลี่ยนแปลงโครงสร้างเพื่อรองรับการเปลี่ยนแปลงทางธุรกิจอย่างต่อเนื่อง จำเป็นต้องมีการกำหนดผู้รับผิดชอบงานด้านบริหารความเสี่ยงในแต่ละหน่วยงานอย่างชัดเจน

4. ปัจจุบันพื้นฐาน บสก. ให้ความสำคัญต่อการดูแลระบบสนับสนุนการปฏิบัติงานภายใน มีการจัดหาอุปกรณ์คอมพิวเตอร์ และระบบที่ช่วยสนับสนุนการทำงาน แต่ควรเพิ่มความเชื่อมั่นในเรื่องความปลอดภัยในเรื่องความถูกต้องของข้อมูล ผ่านระบบสารสนเทศมากขึ้น

4.1.2 ขั้นตอนที่ 2 การกำหนดวัตถุประสงค์

กระบวนการบริหารความเสี่ยงของ บสก. ให้มีการกำหนดวัตถุประสงค์ตามหลัก SMART คือมีความชัดเจนสามารถวัดผลได้ ปฏิบัติได้จริง น่าเชื่อถือ และมีกรอบระยะเวลาที่แน่นอน โดยทำการเปรียบเทียบวัตถุประสงค์เดิมที่ตั้งไว้กับตัวอย่างการกำหนดวัตถุประสงค์ตามหลัก SMART สรุปได้ดังตารางที่ 4.1

ตารางที่ 4.1 แผนงานที่ 5 งานด้านข้อมูลและระบบงาน

แผนโครงการย่อย	วัตถุประสงค์	วัตถุประสงค์ตามหลัก SMART
5.1 แผนพัฒนาระบบ IT เพื่อรองรับการปฏิบัติงานและกลยุทธ์องค์กร	เพื่อให้ระบบสารสนเทศสามารถรองรับการปฏิบัติงานได้โดยสะดวกและรวดเร็ว	เพื่อพัฒนาระบบ IT เพื่อรองรับระบบงานด้านธุรกิจ (Front Office) จำนวน 1 ระบบ และระบบงานด้านการสนับสนุน (Back Office) จำนวน 1 ระบบ ภายในปี 2552
5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง	เพื่อให้ระบบข้อมูลที่ถูกต้อง	เพื่อให้ฐานข้อมูลลูกหนี้และทรัพย์สินรอการขายมีความถูกต้องเป็นปัจจุบัน ภายใน 2 สัปดาห์หลังจากที่มีการเปลี่ยนแปลงของข้อมูล

4.1.3 ขั้นตอนที่ 3 การระบุความเสี่ยง

มีการพิจารณาขั้นตอนหรือกิจกรรมในแต่ละแผนงาน เพื่อระบุความเสี่ยงว่าเกิดจากสาเหตุใด เพื่อทราบถึงประเด็นที่ก่อให้เกิดความเสียหาย และมีผลกระทบต่องานที่เป็นอุปสรรคต่อความสำเร็จของงานตามวัตถุประสงค์ที่วางไว้ โดยในขั้นตอนของการระบุความเสี่ยงให้พิจารณาถึงปัจจัยเสี่ยงว่าเกิดจากปัจจัยใด ซึ่งประกอบไปด้วย ปัจจัยเสี่ยง 4 ด้านหลัก คือ ด้านกลยุทธ์ ด้านการดำเนินการ ด้านการเงิน และ ด้านกฎหมาย/ระเบียบ

ซึ่งในการพิจารณาถึงผลกระทบที่มีนัยสำคัญ แบ่งได้เป็น 9 ด้านหลัก คือ การเงิน/ทรัพย์สิน ลูกค้า บุคลากร การบริการ ชื่อเสียง ระยะเวลา ความสำเร็จ สิ่งแวดล้อม และชุมชน

ในกรณีแผนงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง สรุปปัจจัยเสี่ยงและผลกระทบได้ดังตารางที่ 4.2 และตารางที่ 4.3 มีขั้นตอนการดำเนินการประกอบด้วย

1. ให้ฝ่ายงานที่เกี่ยวข้อง Update ข้อมูลในระบบที่มีอยู่ให้ครบถ้วนถูกต้องทั้งข้อมูล NPL ข้อมูล NPA และข้อมูลคดี

2. จัดทำระบบการตรวจสอบแก้ไขเปลี่ยนแปลงข้อมูลในทุก Transaction

3. กำหนดฝ่ายงานที่มีอำนาจในการแก้ไขฐานข้อมูล

ตารางที่ 4.2 ระบุความเสี่ยงและผลกระทบด้านกลยุทธ์

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง					
ปัจจุบันเสี่ยง	ผลกระทบ				
	การเงิน/ทรัพย์สิน	การบริการ	บุคลากร	ระยะเวลา	ความสำเร็จ
ด้านกลยุทธ์					
5.2.1 การวางแผนการปรับปรุงฐานข้อมูลไม่เป็นไปตามแผนที่วางไว้				ดำเนินการล่าช้าเนื่องจากเสียเวลาในการตรวจสอบข้อมูลที่ถูกต้อง	ส่งผลกระทบต่องานการบริหารหนี้ NPL และ NPA

ตารางที่ 4.3 ระบุความเสี่ยงและผลกระทบด้านการดำเนินการ

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง					
ปัจจุบันเสี่ยง	ผลกระทบ				
	การเงิน/ทรัพย์สิน	การบริการ	บุคลากร	ระยะเวลา	ความสำเร็จ
ด้านการดำเนินการ					
5.2.2 ฝ่ายงานที่เกี่ยวข้องไม่ Update ข้อมูลให้ถูกต้องเป็นปัจจุบัน	การบันทึกบัญชีเกิดความผิดพลาดส่งผลกระทบต่อการบันทึกข้อมูลทางบัญชี		พนักงานไม่ทราบข้อมูลที่ถูกต้องเพื่อนำมาใช้ในการดำเนินการและติดตามงาน		ส่งผลกระทบต่องานการบริหารหนี้ NPL และ NPA

ตารางที่ 4.3 (ต่อ)

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง					
ปัจจุบันเสี่ยง	ผลกระทบ				
	การเงิน/ทรัพย์สิน	การบริการ	บุคลากร	ระยะเวลา	ความสำเร็จ
ด้านการดำเนินการ					
5.2.3 ไม่มีระบบ User Password เพื่อตรวจสอบ/แก้ไขข้อมูลตามลำดับชั้น			ไม่สามารถระบุตัวผู้ปฏิบัติงานกรณีเกิดปัญหาจากการดำเนินการหรือทุจริต		การบันทึกข้อมูลขาดระบบการตรวจสอบส่งผลให้เกิดความผิดพลาดของข้อมูล
5.2.4 ไม่มีระบบ Back up ข้อมูลสำรอง		ไม่สามารถตรวจสอบข้อมูลย้อนหลัง กรณีที่มีการบันทึกข้อมูลผิดพลาด			

4.1.4 ขั้นตอนที่ 4 การประเมินความเสี่ยง

เป็นขั้นตอนการนำปัจจัยความเสี่ยงที่ระบุมาประเมินความเสี่ยง ในด้านโอกาสและผลกระทบ เพื่อพิจารณาหาประเด็นความเสี่ยงที่เป็นความเสี่ยงสำคัญของ บสก. เพื่อนำมาบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพและเกิดประสิทธิผลสูงสุด แต่ทั้งนี้การให้คะแนนควรพิจารณาให้เหมาะสมกับข้อมูลของแต่ละฝ่ายงาน เพื่อให้การประเมินความเสี่ยงมีมาตรฐานตรงกับลักษณะของงานในแต่ละฝ่ายงาน

สำหรับการประเมินความเสี่ยงในด้านโอกาสและผลกระทบนั้น โดยปกติควรจะมีเกณฑ์ในการนำมาเป็นข้อมูลเพื่อใช้ในการกำหนด ซึ่งค่ามาตรฐานที่สามารถนำมากำหนดเกณฑ์การประเมินความเสี่ยง หรือใช้วิธีเปรียบเทียบจากค่ามาตรฐานที่มีการดำเนินการอยู่ในปัจจุบัน ซึ่งสามารถวัดได้เป็นระยะเวลา จำนวนครั้ง ซึ่งได้ทำการกำหนดเกณฑ์การประเมินความเสี่ยง สรุปได้ดังตารางที่ 4.4 และตารางที่ 4.5 ไว้ดังนี้

ตารางที่ 4.4 เกณฑ์การให้คะแนนค่าโอกาส โดยอ้างอิงจากค่ามาตรฐานด้านระยะเวลาและค่าสัดส่วน

โอกาส	
เรื่อง	คะแนน
จัดทำและปรับปรุงข้อมูลให้เป็นปัจจุบันภายใน 7 วัน	5
จัดทำและปรับปรุงข้อมูลให้เป็นปัจจุบันภายใน 8-10 วัน	4
จัดทำและปรับปรุงข้อมูลให้เป็นปัจจุบันภายใน 11-13 วัน	3
จัดทำและปรับปรุงข้อมูลให้เป็นปัจจุบันภายใน 14-16 วัน	2
จัดทำและปรับปรุงข้อมูลให้เป็นปัจจุบัน มากกว่า 16 วัน	1

ตารางที่ 4.5 เกณฑ์การให้คะแนนค่าผลกระทบ โดยอ้างอิงจากค่ามาตรฐานด้านจำนวนและค่าสัดส่วน

ผลกระทบ	
เรื่อง	คะแนน
จำนวนข้อมูลผิดพลาด 10% ขึ้นไป	5
จำนวนข้อมูลผิดพลาด 6-9%	4
จำนวนข้อมูลผิดพลาด 3-5%	3
จำนวนข้อมูลผิดพลาด 3%	2
จำนวนข้อมูลถูกต้องครบถ้วน	1

จากมติคณะกรรมการบริหารความเสี่ยง ของ บสก. ระดับความเสี่ยงที่ยอมรับได้ มีค่าสูงสุดเท่ากับ 11 และใช้โซนสี 4 สีในการแบ่งกลุ่มของความเสี่ยง ที่ต้องการการจัดการที่แตกต่างกัน ดังภาพที่ 4.1 โดยมีรายละเอียดดังนี้

1. สีเขียว ใช้การติดตาม ในระดับปกติมิให้ระดับความรุนแรงของผลกระทบเพิ่มขึ้นและมิให้โอกาสเพิ่มขึ้น

2. สีเหลือง ใช้การติดตามอย่างใกล้ชิดด้วยดัชนีเฝ้าระวัง เพื่อมิให้ระดับความรุนแรงของผลกระทบเพิ่มขึ้น

3. สีเขียว – เหลือง ใช้การติดตาม ในระดับที่สูงกว่าปกติมิให้ระดับความรุนแรงของผลกระทบเพิ่มขึ้นต่อไปและมิให้โอกาสเกิดเพิ่มขึ้น (ได้แก่ค่าความเสี่ยงที่ 8 และ 9) แม้ว่าจะเป็นส่วนที่อยู่ติดกับสีเขียว แต่หากประมาทอาจจะเพิ่มระดับไปสู่ค่าความเสี่ยงที่ 10 และ 11 ได้ง่าย

4. สีเหลือง – ส้ม ติดตามอย่างใกล้ชิดมากด้วยระบบสัญญาณเตือนภัยล่วงหน้ามิให้ระดับความรุนแรงของผลกระทบเพิ่มและมิให้โอกาสเกิดเพิ่มขึ้น (ได้แก่ค่าความเสี่ยงที่ระดับ 16 และ 17) ที่อยู่ติดกับสีเหลือง แต่มีโอกาสเพิ่มค่าไปเป็น 18 และ 19 ได้ง่าย

5. สีส้ม ทำแผนระดับสายงาน/ฝ่ายงาน เพื่อบริหารจัดการความเสี่ยงวางระบบการรายงานผลมิให้ผลกระทบเพิ่ม

6. สีแดง ทบทวนว่าจะระงับ/ยกเลิกกิจกรรมชั่วคราวหรือไม่

ประเมินความเสี่ยงในแต่ละปัจจัยเสี่ยงของแผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง โดยใช้แผนภูมิระดับความเสี่ยงองค์กร ดังภาพที่ 4.1 มาประเมินความเสี่ยงในด้านโอกาสและผลกระทบที่จะเกิดขึ้น ผลการประเมินความเสี่ยงในแต่ละปัจจัยเสี่ยงแสดงได้ดังตารางที่ 4.6 ดังนี้

Impact/ Consequences	**Likelihood / Frequency**				
	Very Low (1)	**Low (2)**	**Medium (3)**	**High (4)**	**Very High (5)**
Catastrophic (5)	19(S)	20(S)	21(S)	24(H)	25(H)
Major (4)	16(S)	17(S)	18(S)	22(H)	23(H)
Moderate (3)	8(M)	9(M)	13(S)	14(S)	15(S)
Minor (2)	3 (L)	4 (L)	7(M)	11(M)	12(S)
Insignificant (1)	1 (L)	2 (L)	5(M)	6(M)	10(M)

ภาพที่ 4.1 การจัดทำแผนภูมิระดับความเสี่ยงองค์กร

ตารางที่ 4.6 การประเมินความเสี่ยง

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง					
ปัจจัยเสี่ยง	ประเภทความเสี่ยง	รายละเอียดความสูญเสีย	โอกาส	ผลกระทบ	ระดับความเสี่ยง
5.2.1 การวางแผนการปรับปรุงฐานข้อมูลไม่เป็นไปตามแผนที่วางไว้	S	การดำเนินการล่าช้าเนื่องจากใช้เวลาในการตรวจสอบข้อมูลที่ถูกต้องส่งผลกระทบต่องานการบริหารหนี้ NPL และ NPA	3	4	18
5.2.2 ฝ่ายงานที่เกี่ยวข้องไม่ Update ข้อมูลให้ถูกต้องเป็นปัจจุบัน	O	พนักงานไม่ทราบข้อมูลที่ถูกต้องเพื่อนำมาใช้ในการดำเนินการและติดตามและอาจส่งผลกระทบต่อการบันทึกบัญชีผิดพลาด	2	3	9
5.2.3 ยังไม่มีระเบียบการกำหนดลำดับชั้นของผู้ใช้งาน User Password ในการบันทึก/แก้ไขข้อมูล	C	ทำให้ไม่มีการกำหนดตำแหน่งผู้รับผิดชอบการบันทึก/แก้ไขข้อมูลการควบคุมชั้นความลับของข้อมูลที่ชัดเจน	4	4	22
5.2.4 ยังขาดการทดสอบการนำข้อมูลที่ได้ Back up ข้อมูลสำรองมาใช้งาน	O	ขาดความเชื่อมั่นในการนำข้อมูลสำรองมาใช้งานย้อนหลังกรณีที่มีความผิดพลาดของข้อมูลที่ใช้ในการดำเนินการ	2	5	20

หมายเหตุ : ความเสี่ยงด้านกลยุทธ์ (Strategic Risk: S)

ความเสี่ยงด้านการปฏิบัติงาน (Operational Risk: O)

ความเสี่ยงด้านการเงิน (Financial Risk: F)

ความเสี่ยงด้านการปฏิบัติตามระเบียบ/กฎหมาย (Compliance Risk: C)

4.1.5 ขั้นตอนที่ 5 การจัดการความเสี่ยง

พิจารณาความเสี่ยงในระดับ สูงสุด 5 ลำดับแรก ซึ่งเป็นงานที่จะนำมาพิจารณาเพื่อหามาตรการจัดการความเสี่ยง ประกอบด้วย

งานที่มีความเสี่ยงสูงมาก (High Risk) จำนวน 1 งาน ได้แก่ แผนงาน 5.2.3 ยังไม่มีระเบียบการกำหนดลำดับชั้นของผู้ใช้งาน User Password ในการบันทึก/แก้ไขข้อมูล

งานที่มีความเสี่ยงที่มีนัยสำคัญรองลงมา (Significant Risk) จำนวน 2 งาน ได้แก่ แผนงาน 5.2.1 การวางแผนการปรับปรุงฐานข้อมูลไม่เป็นไปตามแผนที่วางไว้ และแผนงาน 5.2.4 ยังขาดการทดสอบการนำข้อมูลที่ได้ Back Up ข้อมูลสำรองมาใช้งาน

เมื่อ บสก. ได้ทำการประเมินความเสี่ยงของงานเรียบร้อยแล้ว จะดำเนินการพิจารณานำแผนงานที่มีนัยสำคัญทั้ง 3 แผนงาน มาพิจารณาจัดการความเสี่ยง เพื่อให้ความเสี่ยงดังกล่าวอยู่ในระดับที่ยอมรับได้ โดยมีวิธีการจัดการความเสี่ยง 4 วิธี คือ การยอมรับ การควบคุม การหลีกเลี่ยง และการถ่ายโอน ซึ่งผลการพิจารณาทางเลือกที่เหมาะสมเพื่อการจัดการความเสี่ยง ในแต่ละแผนงานแสดงได้ดังตารางที่ 4.7

ตารางที่ 4.7 ทางเลือกที่เหมาะสมเพื่อการจัดการความเสี่ยง

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง						
ปัจจัยเสี่ยง	ระดับความเสี่ยง	วิธีจัดการความเสี่ยง	รายละเอียดการจัดการ	ความคุ้มค่าของการจัดการ		ทางเลือกที่เหมาะสม
				ต้นทุน	ผลประโยชน์	
5.2.3 ยังไม่มีระเบียบการกำหนดลำดับชั้นของผู้ใช้งาน User Password ในการบันทึก/แก้ไขข้อมูล	สูงมาก	ยอมรับ	ไม่สามารถยอมรับ	-	-	ควบคุม
		ควบคุม	กำหนดให้มีผู้รับผิดชอบการจัดทำการบันทึก/แก้ไขข้อมูลและมีการตรวจสอบความถูกต้องจากผู้บังคับบัญชา	-	ควบคุมให้การบันทึก/แก้ไขข้อมูลมีความถูกต้อง สามารถตรวจสอบความผิดพลาดได้	
		หลีกเลี่ยง	ไม่สามารถหลีกเลี่ยงได้	-	-	
		ถ่ายโอน	มอบหมายให้ฝ่ายงานที่หน้าที่ในการออกระเบียบการใช้ระบบงานและชั้นความลับของระบบ	-	มีระเบียบในการกำหนดชั้นความความลับและการใช้งานระบบที่ชัดเจน	

ตารางที่ 4.7 (ต่อ)

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง						
ปัจจัยเสี่ยง	ระดับความเสี่ยง	วิธีจัดการความเสี่ยง	รายละเอียดการจัดการ	ความคุ้มค่าของการจัดการ		ทางเลือกที่เหมาะสม
				ต้นทุน	ผลประโยชน์	
5.2.1 การวางแผนการปรับปรุงฐานข้อมูลไม่เป็นไปตามแผนที่วางไว้	มีนัยสำคัญ	ยอมรับ	ไม่สามารถยอมรับ	-	-	ควบคุม
		ควบคุม	- สร้างระบบตรวจสอบการแก้ไขข้อมูลจากหน่วยงานที่เกี่ยวข้องให้มีความถูกต้องภายในระยะเวลาที่กำหนด - ให้มีการกำหนด Jointed KPI เพื่อทุกหน่วยงานร่วมรับผิดชอบงานด้านการปรับปรุงฐานข้อมูล NPL และ NPA	ขั้นตอนการปฏิบัติงานและปริมาณงานในแต่ละหน่วยงานเพิ่มขึ้น	บสก. มีฐานข้อมูล NPL และ NPA ที่เป็นปัจจุบัน ผู้บริหารสามารถนำข้อมูลมาใช้ประโยชน์ในการบริหารจัดการพอร์ตและดูแลสภาพคล่องได้อย่างมีประสิทธิภาพ	
		หลีกเลี่ยง	ไม่สามารถหลีกเลี่ยงได้	-	-	
		ถ่ายโอน	ไม่สามารถถ่ายโอนได้	-	-	

ตารางที่ 4.7 (ต่อ)

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง						
ปัจจัยเสี่ยง	ระดับความเสี่ยง	วิธีจัดการความเสี่ยง	รายละเอียดการจัดการ	ความคุ้มค่าของการจัดการ		ทางเลือกที่เหมาะสม
				ต้นทุน	ผลประโยชน์	
5.2.4 ยังขาดการทดสอบการนำข้อมูลที่ได้ Back up ข้อมูลสำรองมาใช้งาน	มีนัยสำคัญ	ยอมรับ	ไม่สามารถยอมรับ	-	-	ควบคุม
		ควบคุม	กำหนดให้มีผู้รับผิดชอบ การจัดทำระบบการสำรองข้อมูลทุกสิ้นวันทำการ และให้มีหน่วยงานตรวจสอบการปฏิบัติตามขั้นตอนอย่างถูกต้อง	เพิ่มขั้นตอนการปฏิบัติงานและมีต้นทุนค่าใช้จ่ายในการพัฒนาระบบและอบรมความรู้แก่พนักงาน	เพื่อกำหนดขั้นตอน และวิธีการในการนำข้อมูลสำรอง มาใช้งานอย่างมีประสิทธิภาพ	
		หลีกเลี่ยง	ไม่สามารถหลีกเลี่ยงได้	-	-	
		ถ่ายโอน	ไม่ควรมีการถ่ายโอนเนื่องจากข้อมูลบางประเภทเป็นจำเป็นต้องนำข้อมูลย้อนหลังมาใช้เพื่อการตรวจสอบ	-	-	

4.1.6 ขั้นตอนที่ 6 กิจกรรมการควบคุม

เมื่อได้ทราบแนวทางการจัดการความเสี่ยง โดยคัดเลือกแนวทางที่เหมาะสมที่สุด โดยคำนึงถึงต้นทุนและผลประโยชน์ที่จะได้รับอย่างคุ้มค่าที่สุด ให้มีการกำหนดกิจกรรมการควบคุมในแต่ละแผนงาน เพื่อเป็นเครื่องมือในการวางกรอบการดำเนินการ ลดความเสี่ยงของงานให้เป็นไปตามเป้าหมาย และให้มีการกำหนดระยะเวลาดำเนินการที่สอดคล้องกับแผนงาน และความเป็นไปได้ในการดำเนินการ พร้อมทั้งให้ระบุผู้รับผิดชอบเพื่อสามารถติดตามความคืบหน้าในการดำเนินการ ดังตารางที่ 4.8

ตารางที่ 4.8 การกำหนดกิจกรรมการควบคุมและกำหนดผู้รับผิดชอบ

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง					
ปัจจัยเสี่ยง	รายละเอียดความสูญเสียที่อาจเกิดขึ้น	แนวทางการจัดการ	กิจกรรมควบคุม	กำหนดเสร็จ/ระยะเวลา	ผู้รับผิดชอบ
5.2.1 การวางแผนการปรับปรุงฐานข้อมูลไม่เป็นไปตามแผนที่วางไว้	การดำเนินการล่าช้าเนื่องจากใช้เวลาในการตรวจสอบข้อมูลที่ถูกต้องส่งผลกระทบต่องานการบริหารหนี้ NPL และ NPA	- สร้างระบบตรวจสอบการแก้ไขข้อมูลจากหน่วยงานที่เกี่ยวข้องให้มีความถูกต้องภายในระยะเวลาที่กำหนด - ให้มีการกำหนด Jointed KPI เพื่อทุกหน่วยงานร่วมรับผิดชอบงานด้านการปรับปรุงฐานข้อมูล NPL และ NPA	- กำหนด Action Plan การจัดการให้มีระบบตรวจสอบการแก้ไขข้อมูลจากหน่วยงานที่เกี่ยวข้อง - ให้มีการกำหนด Jointed KPI เพื่อทุกหน่วยงานร่วมรับผิดชอบงานด้านการปรับปรุงฐานข้อมูล NPL และ NPA	มิ.ย. 52 เม.ย. 52	ฝ่ายเทคโนโลยีสารสนเทศ ทุกฝ่ายงาน

ตารางที่ 4.8 (ต่อ)

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง					
ปัจจัยเสี่ยง	รายละเอียดความสูญเสียที่อาจเกิดขึ้น	แนวทางการจัดการ	กิจกรรมควบคุม	กำหนดเสร็จ/ระยะเวลา	ผู้รับผิดชอบ
5.2.3 ยังไม่มีระเบียบการกำหนดลำดับชั้นของผู้ใช้งาน User Password ในการบันทึก/แก้ไขข้อมูล	ทำให้ไม่มีการกำหนดตำแหน่งผู้รับผิดชอบการบันทึก/แก้ไขข้อมูลการควบคุมชั้นความลับของข้อมูลที่ชัดเจน	กำหนดให้มีผู้รับผิดชอบการจัดทำการบันทึก/แก้ไขข้อมูลและมีการตรวจสอบความถูกต้องจากผู้บังคับบัญชา	- กำหนดให้มีระเบียบในกำหนดลำดับชั้นของผู้ใช้งาน User Password ในการบันทึก/แก้ไขข้อมูล - มีการควบคุมตรวจสอบโดยผู้บังคับบัญชาระดับหัวหน้า	ต.ค. 52 มิ.ย. 52	ฝ่ายพัฒนาองค์กรและบริหารความเสี่ยง ทุกฝ่ายงาน

ตารางที่ 4.8 (ต่อ)

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง					
ปัจจัยเสี่ยง	รายละเอียดความสูญเสียที่อาจเกิดขึ้น	แนวทางการจัดการ	กิจกรรมควบคุม	กำหนดเสร็จ/ระยะเวลา	ผู้รับผิดชอบ
5.2.4 ยังขาดการทดสอบการนำข้อมูลที่ได้ Back up ข้อมูลสำรองมาใช้งาน	ขาดความเชื่อมั่นในการนำข้อมูลสำรองมาใช้งานย้อนหลัง กรณีที่มีความผิดพลาดของข้อมูลที่ใช้ในการดำเนินการ	กำหนดให้มีผู้รับผิดชอบ การจัดทำระบบการสำรองข้อมูลทุกสิ้นวันทำการ และให้มีหน่วยงานตรวจสอบการปฏิบัติตามขั้นตอนอย่างถูกต้อง	- จัดทำขั้นตอนการปฏิบัติงานและกำหนดผู้รับผิดชอบ - จัดทำแผนงานการทดสอบการนำข้อมูลสำรองมา Recovery	มิ.ย. 52	ฝ่ายเทคโนโลยีสารสนเทศ

4.1.8 ขั้นตอนที่ 7 การติดตามประเมินผล

หลังจากที่มีการกำหนดกิจกรรมการควบคุมและผู้รับผิดชอบดำเนินการ ขั้นตอนที่จะทำให้ระบบบริหารความเสี่ยงประสบความสำเร็จอย่างยั่งยืนและเห็นเป็นรูปธรรม คือ มีการตรวจสอบและติดตามประเมินผลที่ดี จากผู้บริหารและพนักงานระดับหัวหน้า สำหรับวิธีการติดตามประเมินผลนั้นสามารถติดตามได้อย่างเป็นทางการและไม่เป็นทางการ สำหรับวิธีการติดตามประเมินผลอย่างเป็นทางการส่วนใหญ่จะติดตามผลผ่านรูปแบบของการรายงาน ซึ่งในแต่ละแผนมีการติดตามประเมินผลดังตารางที่ 4.9

ตารางที่ 4.9 การติดตามประเมินผลงานบริหารความเสี่ยง

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง			ปัจจัยเสี่ยง 5.2.1 การวางแผนการปรับปรุงฐานข้อมูลไม่เป็นไปตามแผนที่วางไว้			
หน่วยงานรับผิดชอบ ฝ่ายเทคโนโลยีสารสนเทศ			ระดับความเสี่ยง สูง			
วันที่ติดตาม			ผู้ตรวจสอบ			
กิจกรรมควบคุม	ความสำเร็จ	กำหนดเสร็จ	ผู้รับผิดชอบ	%ความคืบหน้า	ปัญหาอุปสรรคและแนวทางแก้ไข	แนวทางดำเนินการในอนาคต
- กำหนด Action Plan การจัดการให้มีระบบตรวจสอบการแก้ไขข้อมูลจากหน่วยงานที่เกี่ยวข้อง	กำหนด Action Plan การจัดให้มีระบบตรวจสอบแก้ไขข้อมูลจากหน่วยงานที่เกี่ยวข้องเรียบร้อย สามารถจัดทำแผนงานลุล่วงตามเป้าหมายที่วางไว้	มิ.ย. 52		50%	ยังไม่พบปัญหา	ให้มีระบบตรวจสอบ/จัดการข้อมูลตั้งแต่เริ่มต้นโดยไม่ต้องบันทึกข้อมูลโดยพนักงาน
- ให้มีการกำหนด Jointed KPI เพื่อทุกหน่วยงานร่วมรับผิดชอบงานด้านการปรับปรุงฐานข้อมูล NPL และ NPA	ดำเนินการได้ประมาณ 70% คงเหลือบางหน่วยงานที่ยังไม่ได้เจรจาเรื่องการกำหนด Jointed KPI	เม.ย. 52		70%	ยังเจรจาไม่ได้ครบทุกหน่วยงาน เนื่องจากผู้บริหารฝ่ายงานติดภาระกิจ	-

ตารางที่ 4.9 (ต่อ)

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง				ปัจจัยเสี่ยง 5.2.3 ยังไม่มีระเบียบการกำหนดลำดับชั้นของผู้ใช้งาน User Password ในการบันทึก/แก้ไขข้อมูล		
หน่วยงานรับผิดชอบ ฝ่ายเทคโนโลยีสารสนเทศ				ระดับความเสี่ยง สูง		
วันที่ติดตาม				ผู้ตรวจสอบ		
กิจกรรมควบคุม	ความสำเร็จ	กำหนดเสร็จ	ผู้รับผิดชอบ	%ความคืบหน้า	ปัญหาอุปสรรคและแนวทางแก้ไข	แนวทางดำเนินการในอนาคต
- กำหนดให้มีระเบียบในกำหนดลำดับชั้นของผู้ใช้งาน User Password ในการบันทึก/แก้ไขข้อมูล	มีระเบียบในกำหนดลำดับชั้นของผู้ใช้งาน User Password ในการบันทึก/แก้ไขข้อมูล	ต.ค. 52		80%	ยังไม่พบ	-
- มีการควบคุมตรวจสอบโดยผู้บังคับบัญชาระดับหัวหน้า	มีการลงนามการตรวจสอบโดยผู้บังคับบัญชาระดับหัวหน้า	มิ.ย. 52		100%	ไม่พบปัญหา	-

ตารางที่ 4.9 (ต่อ)

แผนดำเนินงาน 5.2 แผนปรับปรุงฐานข้อมูลลูกหนี้และทรัพย์รอการขาย (NPA) ให้สมบูรณ์และถูกต้อง				ปัจจัยเสี่ยง 5.2.4 ยังขาดการทดสอบการนำข้อมูลที่ได้ Back up ข้อมูลสำรองมาใช้งาน		
หน่วยงานรับผิดชอบ ฝ่ายเทคโนโลยีสารสนเทศ				ระดับความเสี่ยง สูง		
วันที่ติดตาม				ผู้ตรวจสอบ		
กิจกรรมควบคุม	ความสำเร็จ	กำหนดเสร็จ	ผู้รับผิดชอบ	%ความคืบหน้า	ปัญหาอุปสรรคและแนวทางแก้ไข	แนวทางดำเนินการในอนาคต
- จัดทำขั้นตอนการปฏิบัติงานและกำหนดผู้รับผิดชอบ	มีคู่มือขั้นตอนการปฏิบัติงานและกำหนดผู้รับผิดชอบที่ชัดเจน	มิ.ย. 52		70%	ไม่พบปัญหา	-
- จัดทำแผนงานการทดสอบการนำข้อมูลสำรองมา Recovery	มีแผนงานการทดสอบการนำข้อมูลสำรองมา Recovery ในปี 2552	เม.ย. 52		90%	ยังไม่มีการกำหนดฝ่ายงานที่จะเข้าร่วมทดสอบ	-

4.2 ผลการวิเคราะห์ระบบ

ในการศึกษาด้านการจัดการความเสี่ยง ที่เกิดขึ้นภายใน บสก. ได้ทำการแบ่งเป็นในแต่ละด้าน เพื่อจะค้นหาจุดอ่อนและปัญหาที่เกิดขึ้นจากจุดอ่อนเหล่านั้น ที่มีผลทำให้เกิดความเสี่ยงขึ้นในการดำเนินการไม่เป็นไปตามวัตถุประสงค์ขององค์กร ข้อมูลที่มีการนำมาวิเคราะห์ จะช่วยทำให้องค์กรได้ทราบถึง ระดับของความเสี่ยงโดยรวมที่เกิดขึ้น รวมไปถึงการกำหนดแนวทางในการจัดทำมาตรการป้องกันและแนวทางแก้ไข เพื่อเป็นการช่วยลดระดับของความเสี่ยงที่มีต่อองค์กรอยู่ในระดับที่สามารถยอมรับได้

ระบบที่ใช้ในการจัดการความเสี่ยง ซึ่งได้จัดทำขึ้น จะเก็บรวบรวมข้อมูลทั้งหมด ที่เกี่ยวข้องกับการประเมินผลการควบคุมภายใน (Control Self Assessment) กระบวนการในการจัดการความเสี่ยง เพื่อรวบรวมเป็นฐานข้อมูลในการพิจารณาความเสี่ยงขององค์กร และนำไปสู่การการจัดทำรายงานตามระเบียบคณะกรรมการตรวจเงินแผ่นดินว่าด้วยการกำหนดมาตรฐานการควบคุมภายในพ.ศ. 2544 ข้อ 6 สำหรับหน่วยงานสังกัดกระทรวงการคลัง ระบบที่จัดทำขึ้นจะอยู่ในรูปแบบของหน้าเว็บเพจ บุคลากรภายในสามารถเข้ามาศึกษาถึงแนวทางในการจัดการความเสี่ยง และยังเป็นช่องทางในการติดตามข่าวสาร กิจกรรม รวมทั้งบทความเกี่ยวกับการบริหารความเสี่ยง เพื่อเป็นการเผยแพร่ความรู้และสร้างความตระหนักในเรื่องการบริหารความเสี่ยงให้บุคคลากรในองค์กรได้

ภาพที่ 4.2 แสดง Use Case Diagram ระบบการจัดการความเสี่ยง โดยบุคลากรภายในที่ได้รับมอบหมายเป็นตัวแทนฝ่ายงานในเรื่องการบริหารความเสี่ยง สามารถบันทึกและแก้ไขข้อมูลด้านการจัดการความเสี่ยง ผ่านทางระบบเครือข่ายภายในองค์กรได้อย่างทั่วถึง ผ่านทางเครื่องคอมพิวเตอร์ที่ใช้งานภายใน

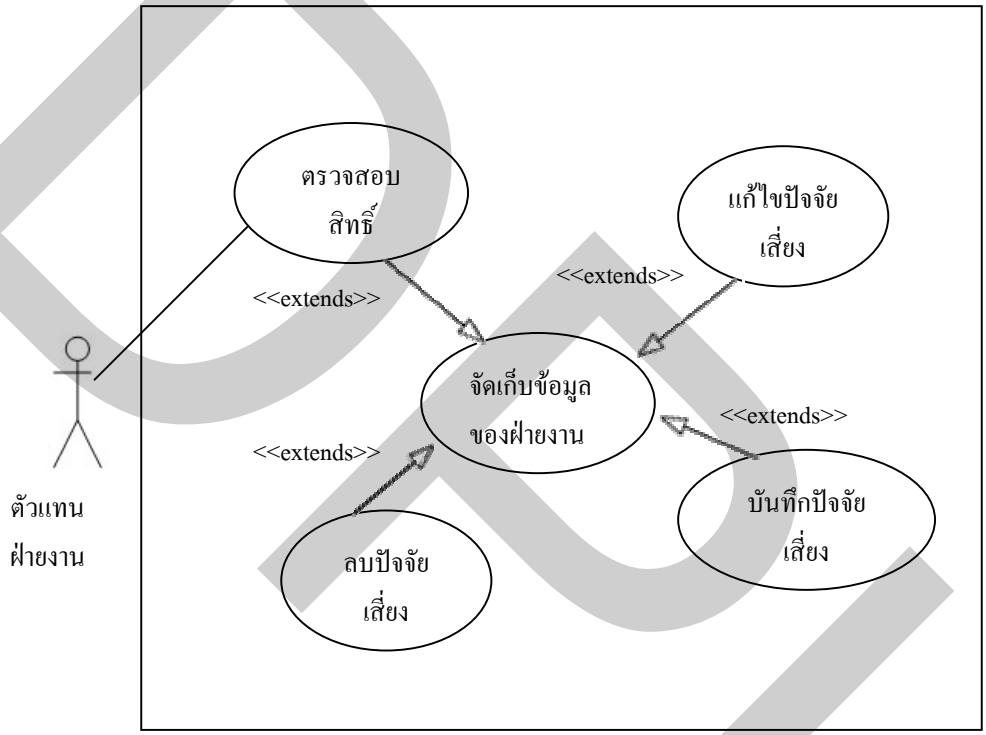
การประมวลผลข้อมูลของระบบจะเป็นลักษณะแบบ Web - based ที่มีการติดต่อส่งข้อมูลถึงกันระหว่างเครื่องคอมพิวเตอร์แต่ละเครื่องผ่านทางหน้าเว็บเพจ ซึ่งเป็นเครื่องมือหลักในการรับส่งข้อมูล โดยส่งข้อมูลผ่านทางโปรแกรมเว็บบราวเซอร์เช่น Internet Explorer การประมวลผลบนหน้าเว็บเพจ จะเกี่ยวข้องกับการส่งถ่ายข้อมูลระหว่างเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์ กับเครื่องคอมพิวเตอร์ที่เป็นฝ่ายเรียกใช้ข้อมูล (Client) ซึ่งประกอบด้วยขั้นตอนต่าง ๆ ดังนี้

1. ผู้ใช้จะส่งคำร้องขอไปยังเครื่องแม่ข่ายผ่านทางหน้าเว็บบราวเซอร์ โดยใช้โปรโตคอลแบบ HTTP

2. เครื่องแม่ข่ายเว็บเซิร์ฟเวอร์ รับคำร้องขอ แล้วค้นหาตำแหน่งของเว็บเพจที่ร้องขอ

3. เครื่องแม่ข่ายเว็บเซิร์ฟเวอร์ ทำการประมวลผลโค้ดภาษา และแปลงผลลัพธ์เป็นเอกสารในรูปภาษาเอเอสพี

4. เครื่องแม่ข่ายเว็บเซิร์ฟเวอร์ จะทำหน้าที่ส่งข้อมูลกลับไปยังเว็บบราวเซอร์ของเครื่องผู้เรียกใช้ข้อมูล (Client) ให้อยู่ในรูปแบบที่ใช้แสดงผลให้กับผู้ใช้สามารถอ่านได้



ภาพที่ 4.2 Use Case Diagram ระบบการจัดการความเสี่ยง

4.3 ผลการออกแบบระบบ

ในการออกแบบระบบจะกล่าวถึง 2 ส่วนคือ การออกแบบตารางจัดเก็บข้อมูล และการออกแบบหน้าเว็บเพจ โดยมีรายละเอียดดังนี้

4.3.1 การออกแบบตารางจัดเก็บข้อมูล

การออกแบบตารางจัดเก็บข้อมูลสำหรับการบริหารความเสี่ยงตามแนวทางมาตรฐาน COSO ประกอบไปด้วย 8 ตารางดังนี้

1. ตารางการระบุความเสี่ยง (ตารางที่ 4.10) เป็นการระบุปัจจัยเสี่ยงในกิจกรรม โครงการ เพื่อให้ทราบประเด็นที่จะก่อให้เกิดปัญหา มีโอกาสเกิดความเสียหาย และมีผลกระทบต่องานที่เป็นอุปสรรคต่อความสำเร็จของงานให้บรรลุวัตถุประสงค์

ตารางที่ 4.10 การระบุปัจจัยเสี่ยงในกิจกรรมในแต่ละแผนงานโครงการ

ลำดับ	ฟิลด์	ชนิด	ความกว้าง/รูปแบบ	หมายเหตุ
1	DP_ID	text	3	รหัสรายชื่อฝ่ายงาน
2	DP_Name	text	50	รายชื่อฝ่ายงาน
3	DP_Year	text	4	ปีที่ทำการประเมิน
4	Subject Risk ID	text	4	รหัสความเสี่ยงที่นำมาพิจารณา
5	Subject Risk	text	100	ความเสี่ยงที่นำมาพิจารณา
6	Object Risk	text	100	วัตถุประสงค์ของการควบคุม
7	Type Risk	text	100	ประเภทความเสี่ยง
8	Residual inside Risk	text	100	สาเหตุที่ทำให้เกิดความเสี่ยงปัจจัยภายใน
9	Residual Outside Risk	text	100	สาเหตุที่ทำให้เกิดความเสี่ยงปัจจัยภายนอก
10	Sources of Risks	text	100	เหตุแห่งความเสี่ยง
11	Impact Side	text	100	ผลกระทบต่อด้านต่างๆ ที่มีนัยสำคัญ
12	Impact Detail	text	200	อธิบายว่าจะกระทบอย่างไร

2. ตารางรายละเอียดการประเมินความเสี่ยง (ตารางที่ 4.11) เพื่อประเมินผลกระทบและโอกาส/ความถี่ที่จะเกิดความเสี่ยง เมื่อนำค่าที่ได้ไปเทียบกับแผนภูมิระดับความเสี่ยงองค์กร (Degree of Risks) ดังภาพที่ 4.1 เพื่อที่จะได้ค่าความเสี่ยงในเชิงปริมาณและคุณภาพ

ตารางที่ 4.11 การประเมินความเสี่ยง

ลำดับ	ฟิลด์	ชนิด	ความกว้าง/รูปแบบ	หมายเหตุ
1	DP_ID	text	3	รหัสรายชื่อฝ่ายงาน
2	DP_Year	text	4	ปีที่ทำการประเมิน
3	Subject Risk ID	text	4	รหัสความเสี่ยงที่นำมาพิจารณา
4	Impact	Number	Standard	ผลกระทบ
5	Likelihood	Number	Standard	โอกาส/ความถี่ที่จะเกิดความเสี่ยง
6	RISK MATRIX	text	20	RISK MATRIX
7	Quality	text	100	เชิงคุณภาพ (ต่ำ-สูงสุด)
8	Amount	Number	Standard	เชิงปริมาณ (1-25 คะแนน)

3. ตารางทางเลือกจัดการความเสี่ยง (ตารางที่ 4.12) ในการเลือกแนวทางการจัดการความเสี่ยงควรพิจารณาถึงความเพียงพอของการควบคุมเดิมที่มีอยู่ และยังมีจุดอ่อนที่ควรปรับปรุงเพิ่มเติม ซึ่งทั้ง 4 แนวทางการจัดการจะมีวิธีการจัดการ ต้นทุน และผลประโยชน์ที่ได้รับแตกต่างกัน ซึ่งผู้ประเมินต้องพิจารณาทั้ง 4 แนวทาง เพื่อเปรียบเทียบเลือกแนวทางที่เหมาะสม และสามารถดำเนินการได้

ตารางที่ 4.12 ทางเลือกจัดการความเสี่ยง

ลำดับ	ฟิลด์	ชนิด	ความกว้าง/รูปแบบ	หมายเหตุ
1	DP_ID	text	4	รหัสรายชื่อฝ่ายงาน
2	DP_Year	text	4	ปีที่ทำการประเมิน
3	Subject Risk ID	text	4	รหัสความเสี่ยงที่นำมาพิจารณา
4	Control of Use	text	200	การควบคุมที่มีอยู่
5	Estimate of Control	text	200	การประเมินผลการควบคุมที่มีอยู่
6	Weak Point	text	200	จุดอ่อนของการควบคุมที่มีอยู่
7	Terminate of Management	text	200	การจัดการ
8	Terminate Cost	Number	Standard	ต้นทุน
9	Terminate Use	text	200	ผลประโยชน์
10	Choice Control	text	100	ทางเลือกที่เหมาะสม

4. ตารางรายละเอียดการจัดการความเสี่ยง (ตารางที่ 4.13) กำหนดกิจกรรมของแต่ละแนวทางในการจัดการความเสี่ยง และกำหนดผู้รับผิดชอบและระยะเวลาการดำเนินการ

ตารางที่ 4.13 การจัดการความเสี่ยง

ลำดับ	ฟิลด์	ชนิด	ความกว้าง/รูปแบบ	หมายเหตุ
1	DP_ID	text	4	รหัสรายชื่อฝ่ายงาน
2	DP_Year	text	4	ปีที่ทำการประเมิน
3	Subject Risk ID	text	4	รหัสความเสี่ยงที่นำมาพิจารณา
4	Way of Management1	text	200	แนวทางการจัดการที่1
5	Way of Management1 Activity	text	200	กิจกรรม
6	Way of Management1 Schedule	text	200	กำหนดการ
7	Way of Management2	text	200	แนวทางการจัดการที่1
8	Way of Management2 Activity	text	200	กิจกรรม
9	Way of Management2 Schedule	text	200	กำหนดการ

5. ตารางการติดตามความเสี่ยง (ตารางที่ 4.14) ความถี่ในการติดตามถ้าความเสี่ยงสูงอาจติดตามเป็นรายเดือน ขึ้นอยู่ความเหมาะสม

ตารางที่ 4.14 การติดตามความเสี่ยง

ลำดับ	ฟิลด์	ชนิด	ความกว้าง	หมายเหตุ
1	DP_ID	text	4	รหัสรายชื่อฝ่ายงาน
2	DP_Year	text	4	ปีที่ทำการประเมิน
3	Subject Risk ID	text	4	รหัสความเสี่ยงที่นำมาพิจารณา
4	Result of Activity	text	100	ผลลัพธ์ของกิจกรรม
5	Interval of Process	text	100	ระยะเวลาดำเนินการ
6	Process%	Number	Standard	% ความคืบหน้า
7	Problem	text	200	ปัญหาอุปสรรค
8	Adjust	text	200	แนวทางแก้ไข

6. ตารางการประเมินผลการจัดการความเสี่ยง (ตารางที่ 4.15) หลังจากได้มีการติดตามการดำเนินการจัดการความเสี่ยงครบตามระยะเวลาที่กำหนด ควรต้องมีการประเมินผลการจัดการความเสี่ยงหลังจากได้มีการดำเนินการปฏิบัติตามแผนการจัดการความเสี่ยง กรณีความเสี่ยงลดลงอยู่ในระดับที่ยอมรับได้ (ระดับต่ำ หรือ ระดับปานกลาง) ก็อาจจะไม่ต้องมีการติดตามการจัดความเสี่ยงอีก แต่ควรจะต้องมีการเฝ้าระวังเพื่อไม่ให้เกิดระดับความเสี่ยงกลับมาสูงอีก แต่ถ้าความเสี่ยงยังอยู่ในระดับสูงอยู่ควรต้องมีการติดตามและประเมินผลการจัดการความเสี่ยงต่อไปเรื่อยๆ จนกว่าความเสี่ยงจะลดลง หรืออาจต้องมีการพิจารณาแนวทางการจัดการความเสี่ยงเพิ่มเติม

ตารางที่ 4.15 การประเมินผลการจัดการความเสี่ยง

ลำดับ	ฟิลด์	ชนิด	ความกว้าง/รูปแบบ	หมายเหตุ
1	DP_ID	text	4	รหัสรายชื่อฝ่ายงาน
2	DP_Year	text	4	ปีที่ทำการประเมิน
3	Subject Risk ID	text	4	รหัสความเสี่ยงที่นำมาพิจารณา
4	Impact after Management	Number	Standard	ระดับความเสียหายหลังจัดการความเสี่ยง
5	Likelihood after M	Number	Standard	โอกาสที่จะเกิดหลังจัดการความเสี่ยง
6	RISK MATRIX after	text	20	RISK MATRIX
7	Quality after	text	100	เชิงคุณภาพ (ต่ำ-สูงสุด)
8	Amount after	Number	Standard	เชิงปริมาณ (1-25 คะแนน)

7. ตารางการตรวจสอบสิทธิ์ผู้เข้าใช้งาน (ตารางที่ 4.16) โดยระบบจะแสดงข้อมูลเฉพาะของผู้ใช้งานเท่านั้น ซึ่งผู้ใช้งานสามารถบันทึกและแก้ไขข้อมูลได้

ตารางที่ 4.16 การตรวจสอบสิทธิ์ผู้เข้าใช้งาน

ลำดับ	ฟิลด์	ชนิด	ความกว้าง/รูปแบบ	หมายเหตุ
1	User_ID	text	15	กำหนดชื่อผู้ใช้งาน
2	Password	text	8	รหัสชื่อผู้ใช้งาน
3	Name_User	text	30	ชื่อผู้ใช้งาน
4	Surename	text	30	นามสกุลผู้ใช้งาน

8. ตารางข้อมูลแสดงความคิดเห็น (ตารางที่ 4.17) โดยจะเก็บข้อมูลคำถาม ข้อแสดงความคิดเห็น ของบุคลากรในองค์กับฝ่ายงานผู้รับผิดชอบดูแลระบบ (ฝ่ายพัฒนาองค์และบริหารความเสี่ยง)

ตารางที่ 4.17 ข้อมูลแสดงความคิดเห็น

ลำดับ	ฟิลด์	ชนิด	ความกว้าง/รูปแบบ	หมายเหตุ
1	ID	AutoNumber	Long Integer	หมายเลขกระทู้
2	ParentID	Number	Long Integer	หมายเลขหัวข้อกระทู้ที่ตอบ
3	Topics	Text	50	หัวข้อกระทู้
4	Data	Memo	-	เนื้อหาของกระทู้
5	User	Text	20	ชื่อผู้โพสกระทู้
6	Email	Text	50	อีเมลผู้โพสกระทู้
7	Date	Date/Time	-	วันที่และเวลาที่โพสกระทู้
8	Replies	Number	Long Integer	จำนวนคนที่ตอบกระทู้
9	LastUpdate	Date/Time	-	วันที่และเวลาล่าสุดที่ตอบกระทู้นั้นๆ

4.3.2 การออกแบบหน้าเว็บเพจ

สำหรับหน้าเว็บเพจที่จัดทำระบบการจัดการความเสี่ยงมีการแบ่งข้อมูลออกเป็น 4 ส่วน ดังนี้

1. ส่วนที่แสดงรายละเอียดข่าวสาร กิจกรรมเพื่อส่งเสริมความเข้าใจในเรื่องการบริหารความเสี่ยงให้กับบุคลากรภายในองค์กร

2. ส่วนในการให้ความรู้ในเรื่องการบริหารความเสี่ยง โดยจะกล่าวถึงความสำคัญและแนวคิดในการจัดการความเสี่ยง เพื่อให้ผู้ใช้ได้ศึกษาถึงกระบวนการในการจัดการความเสี่ยงและองค์ประกอบต่าง ๆ ที่มีส่วนเกี่ยวข้อง อย่างละเอียด

3. ส่วนที่เป็นระบบการประเมินผลระบบการควบคุมภายใน (Control Self Assessment) แบ่งแยกตามฝ่ายงานในส่วนนี้จะมีการแสดงรายละเอียดถึงการประเมินความเสี่ยงที่เกิดขึ้นในแต่ละปัจจัยเสี่ยงที่นำมา สามารถบันทึก แก้ไข และลบข้อมูลได้

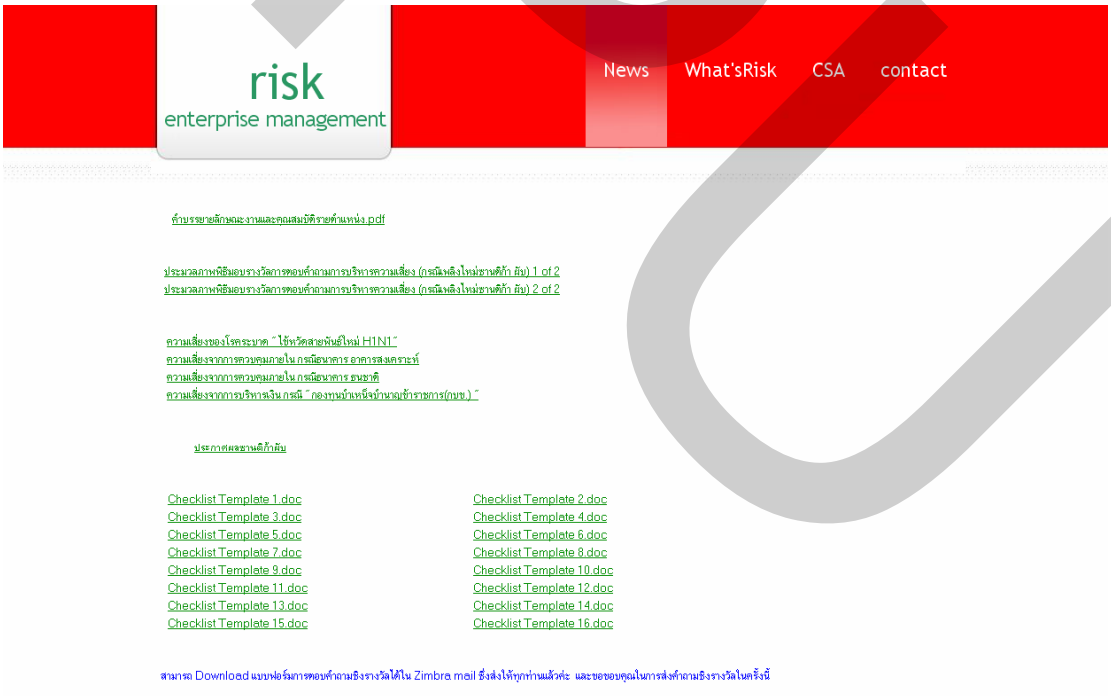
4. ส่วนแสดงการติดต่อกับฝ่ายพัฒนาองค์กรและบริหารความเสี่ยง คำถาม หรือข้อเสนอแนะเพื่อเป็นช่องทางในการแสดงความคิดเห็น เพราะบุคลากรในองค์กรมีทั้งส่วนที่อยู่ในส่วนสำนักงานใหญ่และส่วนสำนักงานจังหวัด

บทที่ 5
ผลการจัดทำและการทดสอบระบบ

เนื้อหาของบทนี้กล่าวถึงผลการจัดทำและการทดสอบการใช้งานระบบการประเมินผลการควบคุมภายในตามมาตรฐาน COSO กรณีศึกษา : ฝ่ายเทคโนโลยีสารสนเทศ โดยจัดทำและทดสอบตามการออกแบบหน้าเว็บเพจที่แบ่งออกเป็น 4 ส่วนได้แก่ การนำเสนอข่าวสารกิจกรรมในเรื่องการบริหารความเสี่ยง การให้ความรู้ในเรื่องการบริหารความเสี่ยง การใช้งานระบบการประเมินผลการควบคุมภายใน และช่องทางการติดต่อกับกลุ่มงานบริหารความเสี่ยง

5.1 การใช้งานเว็บเพจหน้าข้อมูลหลัก

เมื่อผู้ใช้งานคลิกที่เมนูด้านบนชื่อ News ดังภาพที่ 5.1 จะปรากฏหน้าเว็บเพจแสดงรายละเอียดที่เกี่ยวข้องกับข่าวสารการจัดกิจกรรมของกลุ่มงานบริหารความเสี่ยง



ภาพที่ 5.1 หน้าเว็บแสดงรายละเอียดข่าวสารกิจกรรมการบริหารความเสี่ยง

5.2 การให้ความรู้ในเรื่องการบริหารความเสี่ยง

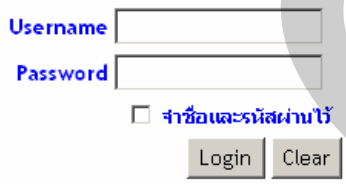
ภาพที่ 5.2 แสดงหน้าเว็บการนำเสนอทฤษฎีในเรื่องของการบริหารความเสี่ยงตามมาตรฐาน COSO เพื่อให้พนักงานในองค์กรเกิดความเข้าใจ และนำการบริหารความเสี่ยงไปใช้ในการปฏิบัติงาน

ภาพที่ 5.2 การให้ความรู้ในเรื่องการบริหารความเสี่ยง

5.3 การใช้งานระบบการประเมินผลการควบคุมภายใน

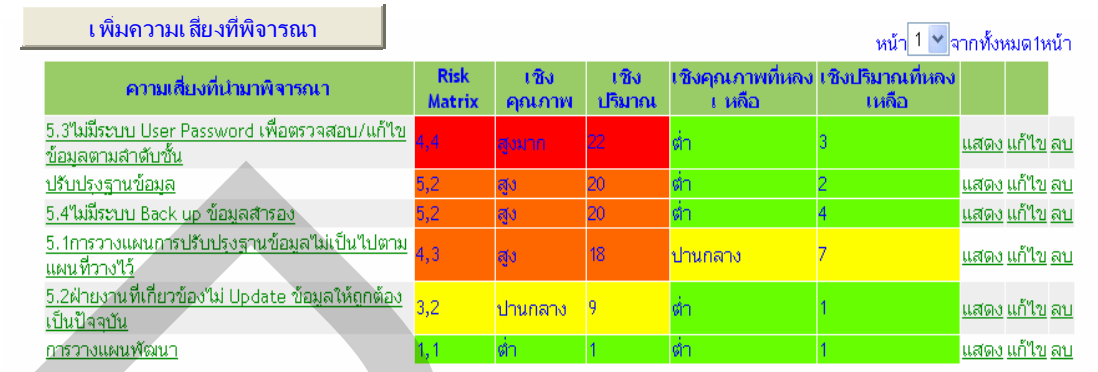
5.3.1 การตรวจสอบสิทธิ์

ผู้ใช้งานระบบต้องทำการใส่ Username และ Passsword ดังภาพที่ 5.3 ที่ผู้พัฒนาระบบเป็นผู้กำหนดให้ โดยกำหนดเป็น 1 ฝ่ายงาน 1 ผู้ใช้งานเนื่องจากการประเมินผลการควบคุมภายในจะเป็นการในระดับฝ่ายงานย่อย



ภาพที่ 5.3 การตรวจสอบสิทธิ์ก่อนการเข้าใช้งาน

เมื่อระบบได้ทำการตรวจสอบสิทธิผู้งานแล้ว ระบบจะแสดงหน้าจอดังภาพที่ 5.4 ซึ่งจะแสดงปัจจัยเสี่ยงทั้งหมดที่ได้เคยทำการบันทึกไว้


เพิ่มความเสี่ยงที่พิจารณา

หน้า 1 จากทั้งหมด 1 หน้า

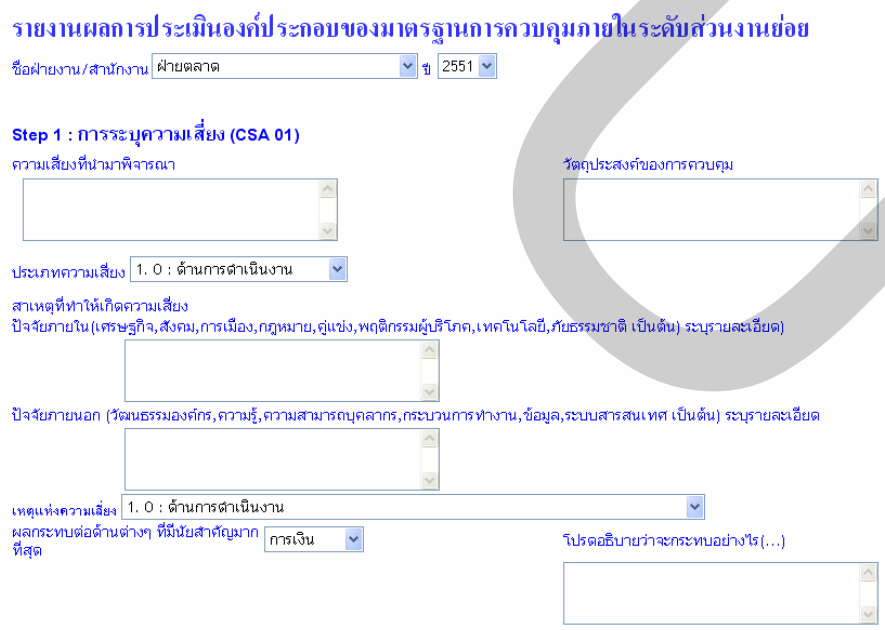
ความเสี่ยงที่นำมาพิจารณา	Risk Matrix	เชิงคุณภาพ	เชิงปริมาณ	เชิงคุณภาพที่หลงเหลือ	เชิงปริมาณที่หลงเหลือ		
5.3ไม่มีระบบ User Password เพื่อตรวจสอบ/แก้ไขข้อมูลตามลำดับชั้น	4,4	สูงมาก	22	ต่ำ	3	แสดง	แก้ไข ลบ
ปรับปรุงฐานข้อมูล	5,2	สูง	20	ต่ำ	2	แสดง	แก้ไข ลบ
5.4ไม่มีระบบ Back up ข้อมูลสำรอง	5,2	สูง	20	ต่ำ	4	แสดง	แก้ไข ลบ
5.1การวางแผนการปรับปรุงฐานข้อมูลไม่เป็นไปตามแผนที่วางไว้	4,3	สูง	18	ปานกลาง	7	แสดง	แก้ไข ลบ
5.2ฝ่ายงานที่เกี่ยวข้องไม่ Update ข้อมูลให้ถูกต้องเป็นปัจจุบัน	3,2	ปานกลาง	9	ต่ำ	1	แสดง	แก้ไข ลบ
การวางแผนพัฒนา	1,1	ต่ำ	1	ต่ำ	1	แสดง	แก้ไข ลบ

ภาพที่ 5.4 รายการความเสี่ยงที่นำมาพิจารณาที่ได้เคยบันทึกไว้

5.3.2 การบันทึก แก้ไข ลบ และแสดงรายการความเสี่ยง

จากภาพที่ 5.4 ผู้ใช้งานสามารถบันทึกเพิ่มรายการความเสี่ยงที่นำมาพิจารณา เพื่อประเมินผลการควบคุมภายใน ทั้ง 6 ขั้นตอน และยังสามารถแสดงรายละเอียด แก้ไข และลบแต่ละรายการได้ โดยมีรายละเอียดดังนี้

ขั้นตอนที่ 1 การระบุความเสี่ยงแสดงดังภาพที่ 5.5 ระบุฝ่ายงาน/สำนักงานที่ทำการบันทึกข้อมูล เพื่อทำการวิเคราะห์หาสาเหตุ และปัจจัยที่ทำให้เกิดความเสี่ยง

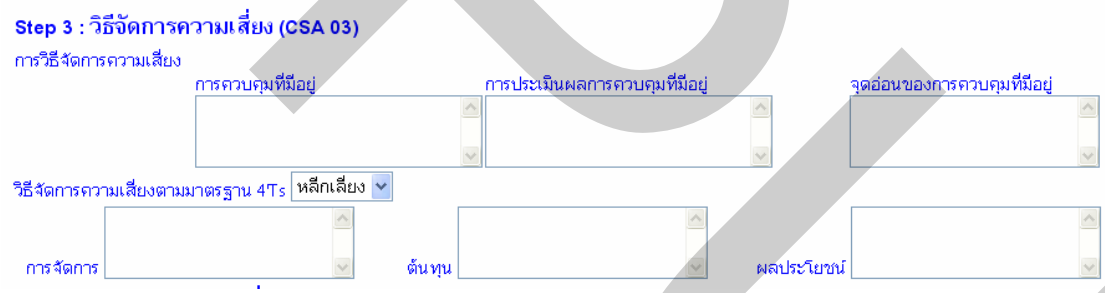


ภาพที่ 5.5 การบันทึกการประเมินผลระบบการควบคุมภายในของขั้นตอนที่ 1

ขั้นตอนที่ 2 การประเมินความเสี่ยง แสดงดังภาพที่ 5.6 เป็นการประเมินผลกระทบ และโอกาสที่จะเกิดความเสี่ยง ในเชิงคุณภาพและปริมาณ

ภาพที่ 5.6 การบันทึกการประเมินผลระบบการควบคุมภายในของขั้นตอนที่ 2

ขั้นตอนที่ 3 วิธีการจัดการความเสี่ยง แสดงดังภาพที่ 5.7 เป็นการวิเคราะห์วิธีในการจัดการกับความเสี่ยงที่คาดว่าจะเกิดขึ้น ประกอบด้วย 4 วิธี ได้แก่ หลีกเลี่ยง ยอมรับ ควบคุม หรือถ่ายโอน ซึ่งควรพิจารณาอธิบายในทุกๆ วิธี เพื่อหาวิธีการจัดการที่ดีและเหมาะสมที่สุด

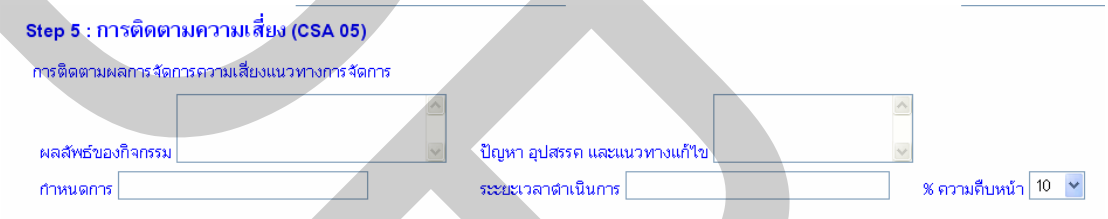


ภาพที่ 5.7 การบันทึกการประเมินผลระบบการควบคุมภายในของขั้นตอนที่ 3

ขั้นตอนที่ 4 การจัดการความเสี่ยง แสดงดังภาพที่ 5.8 เป็นการนำเสนอแนวทางในการจัดการความเสี่ยงโดยพิจารณาจากการควบคุมภายในที่มีอยู่ในปัจจุบันว่ามีความเสี่ยงเพียงพอ หรือต้องมีการจัดการความเสี่ยงเพิ่มเติม

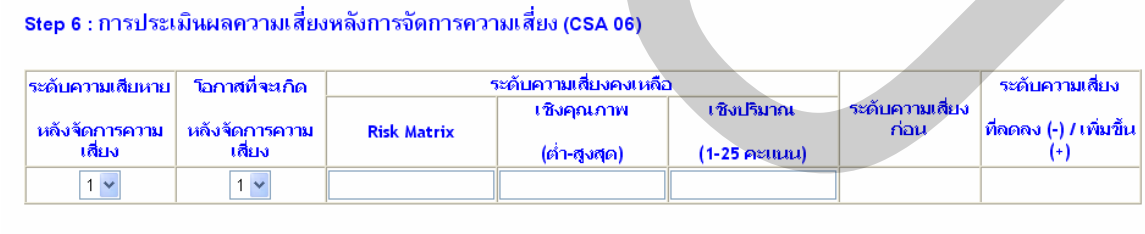
ภาพที่ 5.8 การบันทึกการประเมินผลระบบการควบคุมภายในของขั้นตอนที่ 4

ขั้นตอนที่ 5 การติดตามความเสี่ยง แสดงดังภาพที่ 5.9 เมื่อได้มีการกำหนดแนวทางการจัดการความเสี่ยงแล้วการติดตามวิธีปฏิบัติในการบริหารความเสี่ยง เมื่อครบตามระยะเวลาที่กำหนด ซึ่งอาจมีปัญหาและอุปสรรคที่เกิดขึ้น เพื่อนำไปปรับปรุงในครั้งต่อไป



ภาพที่ 5.9 การบันทึกการประเมินผลระบบการควบคุมภายในของขั้นตอนที่ 5

ขั้นตอนที่ 6 การประเมินผลความเสี่ยงหลังการจัดการความเสี่ยง แสดงดังภาพที่ 5.10 จะดำเนินการประเมินความเสี่ยง หลังจากที่ได้มีการจัดการความเสี่ยงแล้ว ความเสี่ยงยังคงหลงเหลืออยู่หรือลดลง



ภาพที่ 5.10 การบันทึกการประเมินผลระบบการควบคุมภายในของขั้นตอนที่ 6

5.3.3 การแสดงรายรายละเอียดสรุปการประเมินผลการควบคุมภายใน

ระบบจะแสดงรายละเอียดสรุปผลข้อมูลที่ได้บันทึกไว้ แสดงดังภาพที่ 5.11 พร้อมประเมินผลความเสี่ยงโดยการใช้ภูมิระดับความเสี่ยงองค์กร ดังภาพที่ 5.12

รายงานผลการประเมินองค์ประกอบของมาตรฐานการควบคุมภายในระดับส่วนงานย่อย

ฝ่ายงาน/สำนักงาน/ภาค :ฝ่ายเทคโนโลยีสารสนเทศ **ปี** : 2552

Step 1 : การระบุความเสี่ยง (CSA 01)	
ความเสี่ยงที่นำมาพิจารณา **5.3ไม่มีระบบ User Password เพื่อตรวจสอบ/แก้ไขข้อมูลตามลำดับชั้น**	วัตถุประสงค์ของการควบคุม **เพื่อให้ฐานข้อมูลลูกหนี้และทรัพย์สินรอการขายมีความถูกต้องเป็นปัจจุบัน ภายใน 2 สัปดาห์หลังจากที่มีการเปลี่ยนแปลงของข้อมูล**
ประเภทความเสี่ยง **3. C : ด้านกฎหมาย/ระเบียบ**	สาเหตุที่ทำให้เกิดความเสี่ยง **.1.2 O12 = การบริหารทรัพยากรบุคคลไม่เหมาะสม**
ปัจจัยภายใน(เศรษฐกิจ,สังคม,การเมือง,กฎหมาย,คู่แข่ง,พฤติกรรมผู้บริโภค,เทคโนโลยี,ภัยธรรมชาติ เป็นต้น) ระบุรายละเอียด) **บุคลากรไม่เพียงพอ**	
ปัจจัยภายนอก (วัฒนธรรมองค์กร,ความรู้,ความสามารถบุคลากร,กระบวนการทำงาน,ข้อมูล,ระบบสารสนเทศ เป็นต้น) ระบุรายละเอียด -	
ผลกระทบต่อด้านต่างๆ ที่มีนัยสำคัญมากที่สุด **บุคลากร**	โปรดอธิบายว่าจะกระทบอย่างไร(...) **ไม่สามารถระบุตัวผู้ปฏิบัติงาน กรณีเกิดปัญหาจากการดำเนินการหรือทุจริต**

ภาพที่ 5.11 รายละเอียดการประเมินผลระบบการควบคุมภายใน

Step 2 : การประเมินความเสี่ยง (CSA 02)				
ผลกระทบ(Impact)	โอกาส/ความถี่ที่จะเกิดความเสี่ยง(Likelihood)	RISKMATRIX	เชิงคุณภาพ(ต่ำ-สูง)	เชิงปริมาณ(1-25)
4	4	4,4	สูงมาก	22

Step 3 : วิธีจัดการความเสี่ยง (CSA 03)		
การควบคุมที่มีอยู่	การประเมินผลการควบคุมที่มีอยู่	จุดอ่อนของการควบคุมที่มีอยู่
-	-	-

วิธีจัดการความเสี่ยงตามมาตรฐาน 4Ts ทางเลือกที่เหมาะสม : **ควบคุม**

การจัดการ	ต้นทุน	ผลประโยชน์
กำหนดให้มีผู้รับผิดชอบการจัดทำการบันทึก/แก้ไขข้อมูลและมีการตรวจสอบความถูกต้องจากผู้บังคับบัญชา	-	ควบคุมให้การบันทึก/แก้ไขข้อมูลมีความถูกต้อง สามารถตรวจสอบความผิดพลาดได้

ภาพที่ 5.12 การประเมินผลความเสี่ยงโดยการใช้ภูมิระดับความเสี่ยงองค์กร

5.4 ช่องทางการติดต่อกับกลุ่มงานบริหารความเสี่ยง

ระบบได้จัดทำช่องทางในการติดต่อระหว่างพนักงานกับกลุ่มงานบริหารความเสี่ยง โดยมีหน้าจอเขียนกระทู้ ดังภาพที่ 5.9 สำหรับสอบถามติดต่อระหว่างพนักงานในองค์กร ข้อคิดเห็น หรือข้อสงสัยต่าง ๆ ในเรื่องการบริหารความเสี่ยง

ภาพที่ 5.13 หน้าเว็บแสดงช่องทางการติดต่อกับกลุ่มงานบริหารความเสี่ยง

บทที่ 6
สรุปผลการวิจัย

6.1 สรุปผลการวิจัย

การพัฒนาระบบการประเมินผลการควบคุมภายในตามมาตรฐาน COSO กรณีศึกษา : ฝ่ายเทคโนโลยีสารสนเทศ เป็นการจัดทำระบบการจัดการความเสี่ยงในองค์กร โดยใช้ฝ่ายเทคโนโลยีสารสนเทศเป็นต้นแบบ ในการจัดทำการประเมินความเสี่ยงตามมาตรฐาน COSO เพื่อให้พนักงานในองค์การมีการจัดทำกระบวนการจัดการประเมินความเสี่ยง ใน 7 ขั้นตอนได้แก่ ขั้นตอนที่ 1 สภาพแวดล้อมการควบคุมภายใน ขั้นตอนที่ 2 การกำหนดวัตถุประสงค์ ขั้นตอนที่ 3 การระบุความเสี่ยง ขั้นตอนที่ 4 การประเมินความเสี่ยง ขั้นตอนที่ 5 การจัดการความเสี่ยง ขั้นตอนที่ 6 กิจกรรมการควบคุม และขั้นตอนที่ 7 การติดตามประเมินผล

จากการศึกษารวบรวมข้อมูล การบริหารความเสี่ยงภายในองค์กร โดยมีการจัดทำในระดับส่วนงานย่อย ในทุกฝ่ายงาน เพื่อรวบรวมปัจจัยเสี่ยงที่จะเกิดขึ้นซึ่งมีผลให้ไม่เป็นไปตามวัตถุประสงค์ขององค์กร แล้วนำข้อมูลเหล่านี้มาทำการพัฒนาระบบการประเมินผลการควบคุมภายใน ตามมาตรฐาน COSO เพื่อให้ทุกฝ่ายงานในองค์กรทำการประเมินผลการควบคุมภายในของฝ่ายงาน และจัดส่งผลการประเมินผลการควบคุมภายใน ส่งให้กับฝ่ายงานพัฒนาองค์กรและบริหารความเสี่ยง ซึ่งจะเป็นผู้รวบรวมและสรุปเพื่อจัดทำรายงานเพื่อนำเสนอความเสี่ยงในส่วนขององค์กร ใช้รูปแบบของการพัฒนาระบบในลักษณะการทำงานแบบ Client-Server ร่วมกับการทำงานในระบบ Web-based โดยนำเสนอผ่านทางระบบออนไลน์ที่ใช้งานภายในองค์กร เพื่อเผยแพร่ข้อมูลที่เกี่ยวข้องกับกระบวนการในการจัดทำการประเมินความเสี่ยง แนวทางในการจัดการความเสี่ยง ตามขั้นตอนมาตรฐานของ COSO โดยการประยุกต์ใช้โปรแกรมภาษา HTML (Hypertext Markup Language) ร่วมกับภาษาคริปท์ ASP (Active Server Page) และระบบจัดการฐานข้อมูล Microsoft Access ดังนั้นเพื่อจะให้บุคลากรภายในองค์กร ตระหนักในเรื่องการบริหารความเสี่ยง และสามารถใช้งานระบบการประเมินผลการควบคุมภายใน ตามมาตรฐาน COSO ผ่านระบบอินทราเน็ตขององค์กรซึ่งมีความสะดวกทั้งฝ่ายงานที่เป็นผู้ใช้งาน (User) และฝ่ายงานฯ ผู้รวบรวมข้อมูล (Administator)

การจัดทำหน้าเว็บเพจ ระบบการประเมินผลการควบคุมภายในตามมาตรฐาน COSO กรณีศึกษา : ฝ่ายเทคโนโลยีสารสนเทศ เพื่อสนับสนุนการจัดการความเสี่ยงให้แก่ผู้ใช้งานในองค์กร ได้มีการนำข้อมูลที่ศึกษาและวิเคราะห์การประเมินความเสี่ยงในองค์กร เพื่อจัดทำหน้าเว็บเพจโดย

แบ่งข้อมูลออกเป็น 4 ส่วน ได้แก่ หน้าเว็บเผยแพร่ข้อมูลข่าวสารกิจกรรมการบริหารความเสี่ยง หน้าเว็บให้ความรู้ในเรื่องการบริหารความเสี่ยง หน้าเว็บเป็นข้อมูลหลักการประเมินผลระบบการควบคุมภายใน และหน้าเว็บสำหรับการแสดงความคิดเห็นติดต่อสื่อสารกับบุคลากรในองค์กร

ผลการทดสอบการจัดทำหน้าเว็บเพจระบบการประเมินผลระบบการควบคุมภายในสามารถสรุปได้ดังนี้

1. สามารถทำการประเมินผลการควบคุมภายในผ่านระบบการประเมินผลระบบการควบคุมภายใน ทำให้สามารถจัดการความเสี่ยงและสร้างแนวคิดในการจัดทำ และกระบวนการในการประเมินความเสี่ยงภายในระดับฝ่ายงานย่อย

2. สามารถสร้างความตระหนักให้กับบุคคลในองค์กรถึงความสำคัญของการบริหารความเสี่ยง โดยใช้ฝ่ายเทคโนโลยีสารสนเทศเป็นต้นแบบได้

6.2 อภิปรายผลการศึกษา

ผลการศึกษาพบว่า ผู้ใช้งานจากส่วนงานสำนักงานใหญ่ และสำนักงานต่างจังหวัดสามารถใช้งานระบบที่พัฒนาขึ้น จากการเชื่อมต่อระบบเครือข่ายภายในองค์กร และเครือข่ายอินเทอร์เน็ตผ่านทางหน้าเว็บบราวเซอร์ต่าง ๆ ได้เช่น Internet Explorer และ Firefox เป็นต้น การประมวลผลข้อมูลของระบบจะเป็นลักษณะแบบ Web-based ซึ่งมีการติดต่อส่งข้อมูลถึงกันระหว่างเครื่องคอมพิวเตอร์แต่ละเครื่องผ่านทางหน้าเว็บเพจ โดยการใช้โปรโตคอล แบบ HTTP เพื่อจะส่งคำร้องขอไปยังเครื่องแม่ข่ายผ่านทางเว็บบราวเซอร์ซึ่งช่วยทำให้องค์กร สามารถที่จะสร้างระบบบริหารจัดการความมั่นคงปลอดภัย ของสารสนเทศขึ้นมาได้อย่างมีประสิทธิภาพ

6.3 ข้อเสนอแนะ

ระบบที่จัดทำขึ้นในการวิจัยครั้งนี้ เป็นการรวบรวมการบริหารความเสี่ยงระดับส่วนงานย่อย ระบบยังขาดการจัดทำรายงานการบริหารความเสี่ยง ซึ่งบสก. เป็นหน่วยงานที่ต้องนำส่งรายงานการบริหารความเสี่ยงไปยังหน่วยงานภายนอก ซึ่งเป็นหน่วยงานภาครัฐ 2 หน่วยงาน คือ คณะกรรมการรัฐวิสาหกิจ และคณะกรรมการตรวจเงินแผ่นดิน ตามแบบรายงานที่คณะกรรมการรัฐวิสาหกิจ กำหนด และ การจัดทำรายงานผลประเมินระบบการควบคุมภายใน ตามระเบียบคณะกรรมการตรวจเงินแผ่นดิน ว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน พ.ศ.2544 (รายงานตามระเบียบฯ ข้อ 6)

ในส่วนของข้อมูลที่ได้จากการจัดทำการประเมินผลการควบคุมภายใน ยังสามารถนำไปเป็นฐานข้อมูลเพื่อพัฒนาเป็นระบบการเฝ้าระวังกิจกรรมความเสี่ยงที่มีความเสี่ยงสูง และจัดทำเป็นระบบประเมินความเสี่ยงในระดับองค์กรได้

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

หนังสือ

กิตติ ภักดีวัฒนะกุล และไชยรัตน์ ปานปั้น. (2543). **คัมภีร์ ASP ฉบับฐานข้อมูล**. กรุงเทพฯ: เคทีพี คอมพ์ แอนด์ คอนซัลท์.

คณะกรรมการตรวจเงินแผ่นดิน สำนักงานการตรวจเงินแผ่นดิน. (2004). **คำแนะนำ : การจัดทำรายงานการควบคุมภายใน ตามระเบียบคณะกรรมการตรวจเงินแผ่นดินว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน พ.ศ.2544**. กรุงเทพฯ : สำนักงานการตรวจเงินแผ่นดิน.

จตุชัย แพงจันทร์. (2550). **Master in Security**. นนทบุรี : ไอดีซีฯ.

พนิดา พานิชกุล. (2549).**คัมภีร์ Dreamweaver MX 2004** . กรุงเทพฯ : เคทีพี คอมพ์ แอนด์ คอนซัลท์.

มณีโชติ สมานไทย. (2544). **สร้างเว็บแอพพลิเคชัน ASP สำหรับผู้เริ่มต้น**. นนทบุรี: อินโฟเพรส.

วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล. (2548). **ความรู้เบื้องต้นเกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศ**. กรุงเทพฯ : โปรวิชั่น.

วิทยานิพนธ์

กฤษฎา แก้วผุดผ่อง. (2551). **ระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กร ระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กร**. วิทยานิพนธ์ปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศและการสื่อสาร. กรุงเทพฯ: มหาวิทยาลัยธุรกิจบัณฑิตย์.

สารสนเทศจากสื่ออิเล็กทรอนิกส์

กนกวรรณ วีระประสิทธิ์. (2552,มกราคม). การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ. สืบค้นเมื่อ 12 มีนาคม 2551, จาก **www.guru-ict.com/guru/files/ITRisk.doc.**

บริหารความเสี่ยง ในสถาบันวิทยาศาสตร์และเทคโนโลยีแห่งประเทศไทย. (2548, สิงหาคม). คู่มือการบริหารความเสี่ยง. สืบค้นเมื่อ 10 มกราคม 2551, จาก **www.tistr.or.th/tistr2006/code/tistrorg/report/file/risk20051012.pdf.**

ไพร้ซวอเตอร์เฮาส์คูเปอร์ส. (2547, สิงหาคม). แนวทางการบริหารความเสี่ยง. สืบค้นเมื่อ 5 กุมภาพันธ์ 2551, จาก **www.set.or.th/th/.../cg/.../RiskManagementHandbookThai_Final.pdf**.

ภาษาต่างประเทศ

DISSERTATIONS

Oumeshsingh Sookdawoor. (2005). **An investigation of information security policies and practices in Mauritius**. MSC. South Africa: University of South Africa.

Books

An Introduction to Computer Security.(1996). **The NIST Handbook**. NIST Special Publication.

Anonymous.(2009).**COSO Guidance/Monitoring Internal Control Systems**. Los Angeles, CA.

Gary S., Alice G. & Alexis F.(2002). **National Institute Standards and Technology Risk Management Guide for Information Management Systems**. Gaitherburg & Falls Church: National Institute Standards and Technology.

Guy M.Merritt, Preston G.Smith.(2002). **Proactive Risk Management.** Productivity Press.

Emmett J. Vaughan .(1996).**Risk Management (Hardcover).** John Wiley & Sons.

Laura H..(2009).**Internal Control Guidance Well Worth Your Time**. Montana.

Michel Crouhy, Dan Galai, Robert Mark. P.cm (2000).**Risk Management**. Mcgraw-Hill,United States of America.

Nottingham .(2004).**Enterprise Risk Management - Integrated Framework**. the Committee of Sponsoring Organizations of the Treadway Commission.

Richard M. Steinberg. Miles E.A. Everson. Frank J. Martens. Lucy E..

Ross S.(2004).**Enterprise Risk Management -- Integrated Framework**. AICPA.

Thomas R. P. (2005). **Information Security Risk Analysis**. Boca Raton, London, New York, Washington D.C.: Auerbach.

Wayne L.(1992).**Internal Control - Integrated Framework**. AICPA.

ภาคผนวก

ภาคผนวก

แบบสอบถาม เพื่อประกอบการประเมินผลการดำเนินงาน ด้านการควบคุมภายใน

ในการตรวจสอบมาตรการในการควบคุมภายในขององค์กร สามารถเก็บรวบรวมข้อมูลที่ต้องการศึกษาได้จาก ตัวอย่างแบบสอบถาม ประกอบการประเมินผลการดำเนินงาน ในแต่ละด้าน ได้แก่ สภาพแวดล้อมของการควบคุม การประเมินความเสี่ยง กิจกรรมการควบคุม สารสนเทศและการสื่อสาร การติดตามผลและการประเมินผล

แบบสอบถาม
เพื่อประกอบการประเมินผลการดำเนินงาน
ของ <u>บริษัทบริหารสินทรัพย์ กรุงเทพพาณิชย์ จำกัด</u>
ด้าน <u>การควบคุมภายใน</u>

<u>เกณฑ์การตอบแบบสอบถาม</u> - โปรดตอบแบบสอบถาม ในกรอบตารางใต้ข้อมูลหรือข้อซักถาม
- โปรดแนบสำเนาเอกสารที่เกี่ยวข้องกับการปฏิบัติงานนั้น ๆ

1. **สภาพแวดล้อมของการควบคุม** (Control Environment) พิจารณาจาก

1.1 ความสุจริตและความมีจรรยาบรรณของผู้บริหารและพนักงาน

• มีการจัดทำคู่มือ/การกำหนดจรรยาบรรณของผู้บริหารและพนักงาน หรือ มีการทบทวนและมีการปรับปรุง (ถ้าจำเป็น) หรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> ● มีการจัดทำคู่มือ/การกำหนดจรรยาบรรณของผู้บริหารแล้วเสร็จ เมื่อวันที่ xx/xx/ 25…. และประกาศใช้เมื่อวันที่ xx/xx/ 25…. ● (ถ้ามี) มีการทบทวนและปรับปรุงแล้ว เมื่อวันที่ xx/xx/ 25…. และประเด็นสำคัญที่มีการทบทวนและปรับปรุง พร้อมชี้แจงถึงการทบทวนและปรับปรุง

• มีการฝึกอบรม/กิจกรรม/การสื่อสารถึงการปฏิบัติหน้าที่ด้วยความสุจริตและจรรยาบรรณของผู้บริหารและพนักงาน หรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> ● จำนวนการฝึกอบรม (ครั้งต่อปี) ระดับผู้บริหารและพนักงาน และจำนวนผู้บริหารและพนักงานเข้าฝึกอบรมภายในปี ● การจัดฝึกอบรมฯ เฉพาะเรื่อง หรือเป็นหนึ่งในหัวข้อในการฝึกอบรมเรื่องอื่น ๆ ขององค์กร

• การจัดกิจกรรม/การประกวด/การรณรงค์/การสื่อสารภายในองค์กรอย่างไร ประเภท (ชื่อ) กิจการ/การประกวด/การรวบรวม ความถี่ของการจัดฯ ภายในปี

• มีการจัดทำแนวทางที่พึงปฏิบัติหรือมาตรฐานการปฏิบัติงานที่สำคัญ หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการระบุข้อที่พึงปฏิบัติ เช่น กรณีความขัดแย้งทางผลประโยชน์ กรณีใดที่ห้ามปฏิบัติอย่างเด็ดขาด • มีการชี้แจง/สื่อสารอย่างไรให้พนักงานภายในองค์กรรับทราบและปฏิบัติตามข้อกำหนด หรือการเซ็นรับทราบ (ถ้ามี)

• มีกำหนดบทลงโทษทางวินัยอย่างชัดเจนและเป็นลายลักษณ์อักษร หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการกำหนดบทลงโทษทางวินัยอย่างชัดเจนและเป็นลายลักษณ์อักษร • กรณีที่บุคลากรภายในองค์กรกระทำการที่เป็นการฝ่าฝืนนโยบาย กฎหมาย ระเบียบ แนวทางการปฏิบัติงาน หรือมีข้อกำหนดด้านจรรยาบรรณที่กำหนดไว้ มีขั้นตอน/กระบวนการอย่างไร • มีการสื่อสารให้ทราบเมื่อมีการรับตำแหน่งใหม่ (ตำแหน่งที่สำคัญ)

• มีบทลงโทษหากมีการฝ่าฝืน หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • ระดับถึง ความรุนแรงของการฝ่าฝืน • ความเสียหายของการกระทำผิด (มูลค่าความเสียหาย) • สถิติการฝ่าฝืนกระทำผิด

1.2 การมอบอำนาจและหน้าที่ความรับผิดชอบ

• มีการมอบหมายอำนาจหน้าที่ความรับผิดชอบ หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • การจัดทำคู่มือ/มติ/คำสั่งมอบหมายอำนาจหน้าที่แก่คณะกรรมการและผู้บริหารระดับสูงขององค์กร • การอบรม/สัมมนาเพื่อสร้างความเข้าใจหน้าที่ความรับผิดชอบแก่คณะกรรมการและผู้บริหารระดับสูงขององค์กร

• มีการมอบหมายอำนาจหน้าที่และความรับผิดชอบให้แก่บุคลากรในแต่ละตำแหน่งอย่างเหมาะสม หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการระบุอย่างชัดเจนถึงอำนาจหน้าที่และความรับผิดชอบของส่วนงานที่มีความสำคัญ เพื่อป้องกันความผิดพลาดและการปฏิบัติไม่ตรงกฎระเบียบ (Check & Balance)

• มีการกำหนดขอบเขตระดับของอำนาจในการอนุมัติหรือไม่ อย่างไร
แนวทางการตอบคำถาม: • การอนุมัติควรกำหนดขอบเขตระดับของอำนาจในการอนุมัติให้ชัดเจนเป็นลายลักษณ์อักษร และควรสื่อสารให้พนักงานภายในองค์กร

• มีระบบการติดตามงานระหว่างผู้บริหารระดับสูงกับระดับปฏิบัติการ หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีระบบการติดตามงานระหว่างผู้บริหารระดับสูงกับระดับปฏิบัติการ โดยเฉพาะหน่วยงานที่อยู่ห่างไกล ระบบการติดตาม ได้แก่ 1) รูปแบบรายงานที่เป็นทางการ 2) ขั้นตอนวิธีปฏิบัติชัดเจน 3) การดำเนินการกรณีมีปัญหาอุปสรรค และ 4) ความถี่ของการรายงาน

1.3 การกำหนดระเบียบข้อบังคับขององค์กร

• มีระเบียบ/นโยบายควบคุมการจัดซื้อและการบริหารทั่วไปหรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> • มีระเบียบ/นโยบายควบคุมการจัดซื้อและการบริหารทั่วไปที่ควรมีข้อกำหนดที่ชัดเจน อำนาจการอนุมัติการจัดซื้อและขั้นตอนจัดซื้อที่รัดกุมและตรวจสอบได้ เป็นต้น

1.4 ความรู้ ทักษะ และความสามารถของบุคลากร

• มีการจัดทำเอกสารกำหนดคุณลักษณะเฉพาะตำแหน่ง (Job Description) ของหน่วยงานที่เกี่ยวข้องหรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> • มีการจัดทำเอกสารกำหนดคุณลักษณะเฉพาะตำแหน่ง (Job Description) อย่างครบถ้วน (ตำแหน่งงานที่เกี่ยวข้องกับความเสี่ยง ตำแหน่งงานที่เกี่ยวข้องกับด้านการเงินและบัญชี)

• มีการฝึกอบรมและการพัฒนาบุคลากร การประเมินการฝึกอบรมและการพัฒนาบุคลากรมุ่งเน้นที่เกี่ยวข้องการควบคุมภายในโดยตรง หรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> • มีการฝึกอบรมและการพัฒนาบุคลากร การประเมินการฝึกอบรมและการพัฒนาบุคลากรมุ่งเน้นที่เกี่ยวข้องการควบคุมภายในโดยตรง ยกตัวอย่าง พนักงานที่ได้รับการมอบหมาย ควรได้รับอบรม/ศึกษากฎ ระเบียบ มติ ครม. ที่เกี่ยวข้อง และหนังสือแนะนำมาตรฐาน และการควบคุมภายในไปใช้ในเชิงปฏิบัติของคณะกรรมการตรวจเงินแผ่นดิน (คตง.) รวมทั้งการอบรมเรื่อง Control Self - Assessment เป็นต้น

2. การประเมินความเสี่ยง [1] (Risk Assessment)

2.1 องค์กรมีคณะทำงานหรือผู้รับผิดชอบเพื่อรับผิดชอบและติดตามในการบริหารจัดการความเสี่ยง ซึ่งโครงสร้างของคณะทำงานหรือผู้รับผิดชอบยังเป็นลักษณะเฉพาะกาล(เช่น คณะทำงานมีอายุ การทำงานเพียง 1 ปี หรือ มีการทำงานเฉพาะเรื่องเพื่อเสนอเข้าคณะกรรมการพิจารณาเป็นคราวไป เป็นต้น) และ/หรือยังไม่มีการทำงานที่เป็นรูปธรรมอย่างจริงจัง (ผลงานที่เป็นรูปธรรม ได้แก่ ผลงานที่นอกเหนือจากการประชุม เช่น การมีโครงการนำร่องในการพัฒนาระบบบริหารความเสี่ยง เป็นต้น)

• องค์กรมีการบริหารความเสี่ยงเป็นกลยุทธ์ระยะสั้นหรือไม่ อย่างไร • องค์กรมีโครงสร้างของคณะทำงานในการบริหารความเสี่ยง อย่างไร • ในปีบัญชี 2551 คณะทำงานการบริหารความเสี่ยง มีการทำงานที่เป็นรูปธรรม หรือมีการปฏิบัติการบริหารความเสี่ยงจริง หรือมีโครงการนำร่องใน การพัฒนาระบบบริหารความเสี่ยงอย่างไร
<u>แนวทางการตอบคำถาม:</u> กลยุทธ์ระยะสั้น เช่น โครงสร้างของคณะทำงานเป็นลักษณะเฉพาะกาล และ/หรือ ยังไม่มีการทำงานที่เป็นรูปธรรม (มีการปฏิบัติการบริหารความเสี่ยงจริง หรือมีโครงการนำร่องใน การพัฒนาระบบบริหารความเสี่ยง) การตอบคำถามให้ยกตัวอย่างโครงสร้างของคณะทำงานในการบริหารความเสี่ยง และผลงานของคณะทำงานใน ปี 2551

2.2 ไม่ปรากฏนโยบาย กลยุทธ์ หรือแผนงาน/โครงการที่แสดงถึงการดำเนินงานเพื่อให้การบริหารความเสี่ยงเป็นไปในระยะยาวหรือปลูกฝังอยู่ในองค์กร

• องค์กรมีนโยบาย/กลยุทธ์ หรือ แผนงาน/โครงการที่แสดงถึงการดำเนินการ เพื่อให้การบริหารความเสี่ยงเป็นไปในระยะยาวหรือปลูกฝังอยู่ในองค์กร อย่างไร
<u>แนวทางการตอบคำถาม:</u> องค์กรชี้แจงเกี่ยวกับนโยบาย/กลยุทธ์ หรือ แผนงาน/โครงการที่แสดงถึงการดำเนินการเพื่อให้การบริหารความเสี่ยงเป็นไปในระยะยาวหรือปลูกฝังอยู่ในองค์กร การตอบคำถามให้ยกตัวอย่างพร้อมหลักฐาน สำหรับนโยบาย/กลยุทธ์ หรือ แผนงาน/โครงการด้านการบริหารความเสี่ยงประกอบ

[1] ประเมินในหัวข้อการบริหารความเสี่ยง

3. กิจกรรมการควบคุม (Control Activities) พิจารณาจาก

3.1 การอนุมัติ พิจารณาจาก การกำหนดขอบเขตระดับของอำนาจในการอนุมัติให้ชัดเจนเป็นลายลักษณ์ของพนักงานทุกระดับและมีการสื่อสารให้พนักงานภายในองค์กรรับทราบ [2]

**** ประเมินในหัวข้อย่อย 1.1 สภาพแวดล้อมของการควบคุม****

3.2 การสอบทานงาน

• มีการสอบทานรายงานทางการเงินและรายงานผลการดำเนินงานที่มิใช่การเงินหรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการสอบทานรายงานทางการเงินและรายงานผลการดำเนินงานที่มิใช่การเงิน รวมทั้งข้อมูลข่าวสารอย่างสม่ำเสมอ เช่น รายเดือน รายไตรมาส และ ทุก 6 เดือน เป็นต้น • มีการพิจารณารายงานของผลการสอบทาน

• มีการสอบทานโดยผู้บริหารสูงสุดของหน่วยงาน และขององค์กร หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการสอบทานโดยผู้บริหารสูงสุด พิจารณาจากการที่ผู้บริหารสูงสุดมุ่งเน้นการบรรลุวัตถุประสงค์ขององค์กร เช่น การเปรียบเทียบผลการดำเนินงานกับผลงานในอดีตและเป้าหมายตามแผนงาน/ประมาณการ การเปรียบเทียบกับงบประมาณ การสอบทานโดยเปรียบเทียบกับข้อมูลคู่แข่ง และการกำหนดตัวชี้วัดความสำเร็จ เป็นต้น

3.3 การดูแลป้องกัน

• มีการจำกัดการเข้าถึงทรัพย์สินที่มีความเสี่ยง หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการจำกัดการเข้าถึงทรัพย์สินที่มีความเสี่ยง เช่น กำหนดระดับของพนักงานที่เข้าถึง กำหนดรหัสลับ เป็นต้น

[2] ประเมินในหัวข้อย่อย 1.1 สภาพแวดล้อมของการควบคุมภายใน

• มีการดูแลรักษาทรัพย์สินอย่างรัดกุมและเพียงพอ หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการดูแลรักษาทรัพย์สินอย่างรัดกุมและเพียงพอ เช่น ระบบรักษาความปลอดภัยโดยใช้การ์ดหรือแผงสัญญาณ การใช้รหัสผ่าน การจัดเวรยามรักษา เป็นต้น

• มีทะเบียนทรัพย์สิน หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการจัดทำทะเบียนทรัพย์สิน และให้มีการตรวจนับทรัพย์สินเทียบกับทะเบียน/หลักฐานทางบัญชี

• มีการจัดทำงบพิสูจน์ยอดเงินฝากธนาคาร หรือไม่ อย่างไร (สำหรับหน่วยงานที่มีหน้าที่เกี่ยวข้อง)**
แนวทางการตอบคำถาม: • มีการจัดทำงบพิสูจน์ยอดเงินฝากธนาคาร ยอดเงินสดรับจากการรับชำระหนี้ในทะเบียนเงินสดรับเท่ากับยอดรวมรับชำระหนี้ในบัญชีลูกหนี้รายตัว

3.4 การแบ่งแยกหน้าที่งาน

• มีการแบ่งแยกหน้าที่งาน เพื่อมิให้หน่วยงานหรือบุคคลเดียวกันปฏิบัติหน้าที่ทุกขั้นตอนหรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มี การแบ่งแยกหน้าที่ เพื่อมิให้หน่วยงานหรือบุคคลเดียวกันปฏิบัติหน้าที่ทั้ง 4 หน้าที่ทุกขั้นตอน ดังนี้ คือ 1) การอนุมัติรายการ/การให้ความเห็นชอบ 2) การประมวลผล/การบันทึกรายการ 3) การดูแลรักษาทรัพย์สินที่เกี่ยวข้อง 4) การดำเนินงาน • เช่น การจัดโครงสร้างให้ผู้บริหารในระดับสูงกว่าหน่วยปฏิบัติเป็นผู้มีอำนาจตัดสินใจจัดซื้อหรือ

อนุมัติ การจ่ายเงิน ฝ่ายบัญชีรับผิดชอบงานจดบันทึกรายการทางบัญชีทั้งหมด ฝ่ายการเงินรับผิดชอบรายรับรายจ่ายทั้งเงินสดและเงินฝากธนาคาร (หน้าที่งาน หมายถึง งานที่เสี่ยงต่อความเสียหาย)

• มีการขัดแย้งทางผลประโยชน์ส่วนตนหรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> • มีการขัดแย้งทางผลประโยชน์ส่วนตน โดยพิจารณาจากผู้บริหารที่มีบทบาทหน้าที่ และ/หรือความสัมพันธ์อื่นที่มีวัตถุประสงค์หรือผลประโยชน์ขัดแย้งกับบทบาทหน้าที่ในองค์กรและมีผลกระทบต่อผลประโยชน์ต่อองค์กร

3.5 การควบคุมระบบสารสนเทศ

• มีการควบคุมทั่วไปที่เกี่ยวกับกับการปฏิบัติเกี่ยวกับสารสนเทศของเฉพาะของฝ่ายงานหรือไม่อย่างไร
<u>แนวทางการตอบคำถาม:</u> • มีการควบคุมทั่วไปที่เกี่ยวกับกับการปฏิบัติงานของศูนย์ข้อมูล การจัดหา และดูแลรักษาซอฟต์แวร์ระบบงาน การรักษาความปลอดภัยในการเข้าถึงข้อมูลและระบบงานต่างๆ • การพัฒนาและดูแลรักษาระบบงานที่อยู่ในระบบสารสนเทศขององค์กร

• มีการควบคุมเฉพาะระบบงาน ที่เกี่ยวกับการควบคุมการประมวลของระบบงาน ของเฉพาะของฝ่ายงานหรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> • มีการควบคุมเฉพาะระบบงานที่เกี่ยวกับการควบคุมการประมวลของระบบงาน เพื่อให้เกิดความมั่นใจว่าข้อมูลที่ผ่านมาสู่ระบบงานดังกล่าวได้รับการบันทึก การประมวลผล และรายงานอย่างถูกต้องและครบถ้วน

• มีการแบ่งแยกหน้าที่ในหน่วยงานอย่างเหมาะสม หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการแบ่งแยกหน้าที่ในหน่วยงานอย่างเหมาะสม โดยไม่มอบให้บุคลากรใดบุคลากรหนึ่งปฏิบัติงานเกี่ยวกับการประมวลผลข้อมูลที่สำคัญหรือความเสี่ยงต่อความเสียหาย กรณีการควบคุมทั่วไป และการควบคุมเฉพาะระบบ

3.6 การทำเอกสารอ้างอิง

• ระบบงานในที่มีความจำเป็น/สำคัญ มีการจัดทำหลักฐานเป็นเอกสารหรือหนังสือ หรือไม่อย่างไร
แนวทางการตอบคำถาม: • มีการจัดทำโครงสร้างการควบคุมภายใน การจัดทำคู่มือการปฏิบัติงานไว้ให้สมบูรณ์เพียงพอของ การปฏิบัติงานนั้น (คู่มือการอนุมัติรายการแนววิธีปฏิบัติงานที่ดี) เป็นต้น • มีการสอบทาน/ทบทวนเอกสารหลักฐานนั้นเป็นปัจจุบันเสมอ

3.7 การกระทบยอด

• มีการกระทบยอด หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • การกระทบยอด เช่น การเปรียบเทียบรายการในบัญชีทรัพย์สินที่มีอยู่ การเปรียบเทียบรายการในบัญชีกับข้อมูลที่ได้รับจากภายนอก และการเปรียบเทียบรายการในบัญชีกับทะเบียนคุม ซึ่งเมื่อมีการค้นพบผลต่างจากกระทบยอด ให้มีการดำเนินการแก้ไขผลต่างที่เกิดขึ้น

4. สารสนเทศและการสื่อสาร [3] (Information and Communications) การบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี ดังต่อไปนี้

- ฝ่ายบริหารจัดให้มีคณะทำงานหรือผู้รับผิดชอบด้าน IT และ ITG หรือไม่ อย่างไร (ทั้งนี้กรุณาแนบเอกสารเพิ่มเติม เกี่ยวกับการจัดตั้งคณะทำงานดังกล่าว และหน้าที่ความรับผิดชอบของคณะทำงาน)
- ในปีบัญชี 2551 ผลงานที่เป็นรูปธรรมของคณะทำงานหรือผู้รับผิดชอบด้าน IT และ ITG คืออะไร
- ในปีบัญชี 2551 ผลงานที่ Board มีการติดตามดูแลวิธีการที่ฝ่ายบริหารใช้ประโยชน์จาก IT เพื่อให้บรรลุวัตถุประสงค์ที่กำหนด คืออะไร
- ในปีบัญชี 2551 คณะกรรมการตรวจสอบมีการกำกับดูแลและติดตามการจัดการกระบวนการป้องกันความเสียหาย การปรับปรุงรวมถึงเสนอแนะแก่ฝ่ายตรวจสอบด้านการจัดการ อย่างไร (ทั้งนี้กรุณาแนบเอกสารเพิ่มเติม เกี่ยวกับรายงานการประชุมที่แสดงถึงการกำกับดูแลและติดตามการจัดการกระบวนการป้องกันความเสียหาย การปรับปรุงรวมถึงเสนอแนะแก่ฝ่ายตรวจสอบด้านการจัดการของคณะกรรมการตรวจสอบ ดังกล่าว)
- คณะกรรมการตรวจสอบทบทวน กฎบัตร (Charter) ของคณะกรรมการตรวจสอบในส่วนที่เกี่ยวข้องกับการจัดการด้าน IT เมื่อไร อย่างไร (ทั้งนี้กรุณาแนบเอกสารเพิ่มเติม เกี่ยวกับกฎบัตร (Charter) ของคณะกรรมการตรวจสอบ ประกอบการพิจารณา)
- ในปีบัญชี 2551 ความคืบหน้าในการติดตั้งระบบ e-DOC หรือปัญหาที่เกิดขึ้นกับการใช้งานของระบบ e-DOC ของ องค์กร เป็นอย่างไร
- คณะกรรมการและผู้บริหารระดับสูง มีการประเมินผลของวิธีการที่ฝ่ายบริหารใช้ในการจัดการกับความเสี่ยงและมาตรฐานการจัดการปัญหา ที่อาจเกิดขึ้นด้าน IT และ ITG หรือไม่ อย่างไร เช่น ระบบ ศูนย์คอมพิวเตอร์สำรองนอกสถานที่ทำการ (Off-site Back up) ที่ใช้งานได้ในปัจจุบัน มีระบบการดูแลสภาพแวดล้อมที่ดี มีมาตรฐาน (IT Security Room) ของศูนย์คอมพิวเตอร์หลัก มีระบบการจัดการดำเนินธุรกิจอย่างต่อเนื่อง (BCM – Business Continuity Management) ของงานหลักๆ ทั้งด้าน IT และ non - IT เป็นต้น
- คณะกรรมการและผู้บริหารระดับสูง จัดให้มีการจัดการกลยุทธ์ทางด้าน IT ของ องค์กรที่ดี เช่น การจัดตั้งคณะอนุกรรมการ การกำหนดกลยุทธ์ทางด้าน IT ที่เป็นรูปธรรมและสอดคล้องกับการบริหารความเสี่ยง เป็นต้น หรือไม่ อย่างไร
- ฝ่ายบริหารมีการประเมินศักยภาพ และความคุ้มค่าของการใช้ IT และการจัดการอย่างสม่ำเสมอ

[3] ประเมินในหัวข้อการบริหารจัดการสารสนเทศ

ทั้งทางด้านการเงินและมิใช่การเงิน เพื่อการตัดสินใจของคณะกรรมการและผู้บริหารระดับสูง ในเชิงวิเคราะห์เปรียบเทียบกับวัตถุประสงค์และเป้าหมาย หรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> องค์ประกอบของการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดีในระดับ 3 ครบถ้วน แนวทางการตอบ : พิจารณาจากตัวอย่างและหลักฐานของการที่ องค์กรมีองค์ประกอบของการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดีในระดับ 3 ครบถ้วน ซึ่งประกอบด้วย ● ฝ่ายบริหารจัดให้มีคณะทำงานหรือผู้รับผิดชอบด้าน IT และ ITG ● คณะกรรมการ มีการติดตามดูแลวิธีการที่ฝ่ายบริหารใช้ประโยชน์จาก IT เพื่อให้บรรลุวัตถุประสงค์ที่กำหนด ● คณะกรรมการตรวจสอบกำกับดูแลและติดตามการจัดการกระบวนการป้องกันความเสียหาย การปรับปรุงรวมถึงเสนอแนะแก่ฝ่ายตรวจสอบด้านการจัดการ IT ● คณะกรรมการตรวจสอบทบทวน กฎบัตร (Charter) ของคณะกรรมการตรวจสอบในส่วนที่เกี่ยวข้องกับการจัดการด้าน IT ● ระบบ e-DOC แล้วเสร็จ ● คณะกรรมการ องค์กรมีการประเมินผลฝ่ายบริหารในการจัดการกับความเสี่ยงและปัญหาที่อาจเกิดขึ้นทางด้าน IT เช่น มีศูนย์คอมพิวเตอร์สำรองนอกสถานที่ทำการ มีระบบการดูแลสภาพแวดล้อมที่ดี มีมาตรฐาน (IT Security Room) ของศูนย์คอมพิวเตอร์หลัก มีระบบข้อมูลสำรองไว้ในกรณีฉุกเฉิน มีระบบการจัดการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Management : BCM) ของงานหลักๆ ทุกด้าน เพื่อให้ความมั่นใจอย่างสมเหตุสมผลว่าธุรกิจจะไม่มีปัญหาในสถานการณ์ฉุกเฉินต่างๆ อย่างเป็นรูปธรรม เป็นต้น ● คณะกรรมการ องค์กรจัดให้มีการจัดการที่ดีถึงกลยุทธ์ทางด้าน IT ของ องค์กร เช่น การจัดตั้งคณะอนุกรรมการการกำหนดกลยุทธ์ทางด้าน IT (IT Strategy Committee) เป็นต้น ● ฝ่ายบริหารมีการประเมินศักยภาพของ IT และการจัดการอย่างสม่ำเสมอ ทั้งทางด้านการเงินและมิใช่การเงิน เช่น อัตราการเพิ่มของผลตอบแทนที่ได้จากการลงทุนทางด้าน IT และระยะเวลาของ การเปลี่ยนแปลงกระบวนการและระบบการทำงาน เป็นต้น

5. การติดตามผลและการประเมินผล (Monitoring) พิจารณาจาก

5.1 การติดตามผลในระหว่างการปฏิบัติงาน (Ongoing Monitoring)

• มีการกำหนดเป็นนโยบายให้การติดตามผลเป็นส่วนหนึ่งของการปฏิบัติงานประจำวันหรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> • มีนโยบายจากผู้บริหารระดับสูง ให้มีการติดตามผลการดำเนินงาน • มีการพิจารณารายงานติดตามผลฯ

• มีการติดตามและประเมินผลการควบคุมภายในหรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> • การติดตามและประเมินผลการควบคุมภายใน เช่น 1) ตามองค์ประกอบการควบคุมภายใน เช่น การติดตามผลของสภาพแวดล้อมของการควบคุม ความเสี่ยงและโอกาสจะเกิดความเสี่ยง กิจกรรมการควบคุม และสารสนเทศและ การสื่อสาร หรือ 2) ตามวัตถุประสงค์ของการควบคุม หรือ 3) ตามกิจกรรมการควบคุมเฉพาะด้าน หรือ 4) เฉพาะงานใดงานหนึ่ง หรือตามกิจกรรมการควบคุมโดยรวมขององค์กร

• มีการติดตามผลเป็นไปอย่างสม่ำเสมอและจัดทำรายงานติดตามผลและการประเมินผลของระบบการควบคุมภายในหรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> • มีการติดตามผลเป็นไปอย่างสม่ำเสมอและจัดทำรายงานติดตามผลและการประเมินผลของระบบการควบคุมภายในแบบรายเดือน รายไตรมาส ทุก 6 เดือน เป็นต้น โดยรายงานเสนอผู้บริหารที่รับผิดชอบควรมีสาระสำคัญประกอบ เช่น แสดงผลจากการเปรียบเทียบของผลงานเทียบกับเป้าหมาย เทียบกับผลงานในอดีต มีคำชี้แจงหรืออธิบายถึงความแตกต่างระหว่างผลงานและเป้าหมาย และผลงานในอดีต ระบุถึงหน่วยงานผู้รับผิดชอบ และการระบุแนวทางหรือวิธีการแก้ไขข้อบกพร่อง เป็นต้น

• มีการติดตามและรายงานผลตามข้อเสนอแนะ หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการติดตามและรายงานผลเมื่อมีการดำเนินงานตามข้อเสนอเสนอแนะหรือการแก้ไขข้อบกพร่อง

5.2 การประเมินผลเป็นรายครั้ง (Separate Evaluation)

1) มีการประเมินการควบคุมด้วยตนเอง (Control Self-Assessment : CSA) ของระบบการควบคุมหรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการกำหนดให้กลุ่มผู้ปฏิบัติงานในส่วนงานนั้นเข้ามามีส่วนร่วมในการประเมินการควบคุมภายในของส่วนงานนั้นๆ เพื่อประสิทธิผลด้านการดำเนินงาน การรายงานทางการเงิน และการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับและมติคณะรัฐมนตรี และการวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ 2) มีผู้บริหารและพนักงานที่เกี่ยวข้องในส่วนงานนั้น มีการประชุมกันเป็นกลุ่ม (Workshop Facilitation) เพื่อหารือกระบวนการที่ปฏิบัติอยู่ วัตถุประสงค์ของงาน ความเสี่ยง และประเมินการควบคุมภายในที่มีอยู่ในงานนั้น 3) มีแบบสอบถามทั่วไป หรือ แบบสอบถามเฉพาะงาน (Self-Assessment Questionnaire) การสัมภาษณ์ผู้ที่เกี่ยวข้อง 4) มีการอบรมเรื่องการประเมินการควบคุมด้วยตนเอง (Control Self-Assessment) การประเมินการควบคุมด้วยตนเองทั่วทั้งองค์กร

• มีการประเมินการควบคุมอย่างเป็นอิสระ (Independent Assessment) หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการประเมินการควบคุมอย่างเป็นอิสระ (Independent Assessment) เป็นการประเมินโดย 1) ผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอก หรือที่ปรึกษาภายนอก 2) การนำผลของการประเมินมาใช้ประโยชน์ เช่น เพื่อสนับสนุนให้องค์กรดำเนินงานให้บรรลุเป้าหมาย

5.3 ความรับผิดชอบของผู้บริหารต่อการติดตามประเมินผลของระบบการควบคุมภายในระดับองค์กรและระดับหน่วยงาน

• สำนักตรวจสอบภายในรายงานเกี่ยวกับความไม่มีประสิทธิผลของระบบการควบคุมภายในโดยตรงต่อคณะกรรมการตรวจสอบ และผู้บริหารระดับสูง ในส่วนที่เกี่ยวข้องกับฝ่ายงานท่านหรือไม่ อย่างไร
แนวทางการตอบคำถาม: • สำนักตรวจสอบภายในต้องรายงานเกี่ยวกับความไม่มีประสิทธิผลของระบบการควบคุมภายในโดยตรงต่อคณะกรรมการตรวจสอบ และผู้บริหารระดับสูงอย่างเพียงพอและทันกาล โดยเป็นรายงานประเมินระบบการควบคุมภายในระดับองค์กรและระดับหน่วยงาน และรายงานเป็นประจำรายไตรมาส

• กำหนดให้แต่ละหน่วยงานติดตามประเมินผล หรือไม่ อย่างไร
แนวทางการตอบคำถาม: • การติดตามผลถือเป็นส่วนหนึ่งของการปฏิบัติงานประจำวัน • สำนักตรวจสอบภายใน ติดตามผลการดำเนินงานด้านการควบคุมขององค์กร โดยประเมินระบบการควบคุมประจำปีและรายงานต่อผู้บริหารระดับสูง รวมถึง (ถ้ามี) การปรับปรุงระบบการควบคุมภายใน

• สำนักตรวจสอบภายในมีการแจ้งผลการติดตามต่อผู้รับผิดชอบ และผู้บังคับบัญชาที่เหนือผู้รับผิดชอบขึ้นไปอย่างน้อยหนึ่งระดับหรือไม่ อย่างไร
แนวทางการตอบคำถาม: • มีการกำหนดให้สำนักตรวจสอบภายในแจ้งผลการติดตามต่อผู้รับผิดชอบ และผู้บังคับบัญชาที่เหนือผู้รับผิดชอบขึ้นไปอย่างน้อยหนึ่งระดับ กรณีพบ จุดอ่อน ข้อบกพร่อง หรือปัญหาที่พบในระหว่างการติดตามผลอย่างต่อเนื่องและการประเมินรายครั้ง

• สำนักตรวจสอบภายในมีการแจ้งผลการติดตามต่อผู้บริหารฝ่ายงานในระดับที่มีอำนาจการตัดสินใจ กรณี ตรวจพบที่สำคัญ หรือไม่ อย่างไร

<u>แนวทางการตอบคำถาม:</u> • มีการกำหนดให้สำนักตรวจสอบภายในแจ้งผลการติดตามต่อผู้บริหารในระดับที่มีอำนาจการตัดสินใจ กรณี ตรวจพบที่สำคัญ

• หน่วยงานภายในองค์กรมีการดำเนินมาตรการที่กำหนดขึ้นเพื่อจัดการหรือแก้ไขปัญหาที่ได้รายงานให้แก่คณะกรรมการองค์กร หรือไม่ อย่างไร
<u>แนวทางการตอบคำถาม:</u> • มีการแก้ไขข้อบกพร่องที่ได้ตรวจสอบไว้ • มีการปรับเปลี่ยนในทางที่ดีขึ้น • มีการชี้แจงถึงเหตุผลที่ไม่จำเป็นต้องดำเนินการใดกับข้อตรวจพบและข้อเสนอแนะ

• เมื่อมีการติดตามผลแล้วมีจุดบกพร่องที่เป็นสาระสำคัญ ดำเนินการอย่างไร
<u>แนวทางการตอบคำถาม:</u> • ที่เกิดจากความบกพร่องการทำงานของบุคลากร ผู้บริหารควรมีบทลงโทษอย่างชัดเจนและระบุเป็นลายลักษณ์อักษร * จะประเมิน ความสุจริตและความมีจรรยาบรรณของผู้บริหาร

ลงชื่อ.....ผู้ตอบแบบสอบถาม

(.....)

ตำแหน่งงาน.....ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ.....

ประวัติผู้เขียน

ชื่อ-นามสกุล	นางสาวรัตนา ไพรศรี
ประวัติการศึกษา	ระดับปริญญาตรี ปริญญาครุศาสตรอุตสาหกรรมบัณฑิต (ค.อ.บ.) สาขาวิชาเทคโนโลยีคอมพิวเตอร์ ภาควิชาคอมพิวเตอร์ศึกษา คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ 2543
ตำแหน่งและสถานที่ทำงานปัจจุบัน	เจ้าหน้าที่ 6 ฝ่ายพัฒนาองค์กรและบริหารความเสี่ยง บริษัท บริหารสินทรัพย์กรุงเทพพาณิชย์ จำกัด ตั้งอยู่ที่ เลขที่ 99 ถนนสุรศักดิ์ แขวงสีสม เขตบางรัก จังหวัดกรุงเทพมหานคร
ประสบการณ์ทำงาน	เจ้าหน้าที่ตรวจสอบคอมพิวเตอร์ (Computer Audit)