บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในบทนี้จะกล่าวถึงทฤษฎีต่าง ๆ ที่นำมาใช้ในการทำวิทยานิพนธ์ ซึ่งประกอบด้วย หลักการการควบคุมภายใน (Internal Control) ภายใต้แนวคิดของ COSO (The Committee of Sponsoring Organization of the Treadway Commission) โดยเป็นการพัฒนากรอบการบริหารความเสี่ยงขององค์กรให้ชัดเจนขึ้น และเป็นการเชื่อมโยงระหว่างการควบคุมภายในกับการบริหารความเสี่ยง ซึ่งถือเป็นประเด็นหลักในการดำเนินการวิจัยนี้ นอกจากนี้ยังมีทฤษฎีเกี่ยวกับการวิเคราะห์ Why – Why ซึ่งใช้ในการวิเคราะห์และหาแผนจัดการความเสี่ยง ส่วนงานวิจัยที่เกี่ยวข้องได้นำเสนอไว้ในส่วนท้ายของบทนี้

2.1 การควบคุมภายใน (Internal Control) (ตลาดหลักทรัพย์แห่งประเทศไทย และสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย, 2548)

ความสำคัญในการบริหารจัดการองค์กร ได้แก่ การบริหารจัดการองค์กรให้บรรลุวัตถุประสงค์ที่ได้ตั้งไว้ โดยต้องอาศัยวัตถุประสงค์ การสร้างมาตรฐาน และกำหนดให้องค์กรมีขั้นตอนการดำเนินงานที่ดี ดังนั้น การควบคุมให้ระบบดำเนินการไปตามวัตถุประสงค์ จึงเป็นสิ่งที่มีความสำคัญตามมาและถูกเรียกว่า การควบคุมภายใน (Internal Control) ซึ่งมิใช่หมายถึงการควบคุมภายในเฉพาะทางด้านบัญชีและการเงินเท่านั้น ยังครอบคลุมไปถึงการควบคุมภายในด้านการบริหาร และการควบคุมภายในด้านการปฏิบัติงานในทุก ๆ หน่วย และทุก ๆ กระบวนการของการดำเนินงาน โดยมีวัตถุประสงค์เพื่อให้การบริหารจัดการองค์กรสามารถบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพและประสิทธิผล

ดังนั้น ผู้บริหารขององค์กรจึงจำเป็นต้องมีเครื่องมือในการสร้างความมั่นใจให้เกิดขึ้นได้ว่าองค์กรนั้นมีการควบคุมภายในที่ดี ซึ่งการจะสร้างความมั่นใจดังกล่าวให้เกิดขึ้นประกอบไปด้วยหลายวิธี หนึ่งวิธีดังกล่าวได้แก่ การตรวจสอบภายใน (Internal Auditing) ซึ่งเป็นกลไกอย่างหนึ่งในการติดตามกระบวนการควบคุมภายในขององค์กร (Monitoring Control) เพื่อให้การควบคุมภายในขององค์กรอยู่ในระดับที่สมเหตุสมผลและเหมาะสม ซึ่งท้ายสุดจะส่งผลให้องค์กรสามารถลดความเสี่ยงในการที่จะไม่สามารถบรรลุวัตถุประสงค์ลงได้

2.1.1 คำจำกัดความของการควบคุมภายใน

ในปี พ.ศ. 2535 คณะกรรมการที่เรียกว่า The Committee of Sponsoring Organisations of the Treadway Commission หรือ COSO ซึ่งเกิดจากการรวมตัวของสถาบันวิชาชีพ 5 แห่งในสหรัฐอเมริกา ได้แก่ สมาคมผู้สอบบัญชีรับอนุญาตแห่งสหรัฐอเมริกา (American Institute of Certified Public Accountants หรือ AICPA) สมาคมผู้ตรวจสอบภายใน (The Institute of Internal Auditors หรือ IIA) สมาคมผู้บริหารการเงิน (Financial Executives Institute หรือ FEI) สมาคมนักบัญชีแห่งสหรัฐอเมริกา (American Accounting Association หรือ AAA) และสมาคมนักบัญชีเพื่อการบริหาร (Institute of Management Accountants หรือ IMA) ได้ออกรายงานที่เรียกว่า COSO Internal Control Integrated Framework กำหนดความหมายและแม่บทของการควบคุมภายใน โดยได้ให้คำจำกัดความของการควบคุมภายในไว้ ดังต่อไปนี้

"การควบคุมภายใน" หมายถึง กระบวนการหรือขั้นตอนการทำงานที่เป็นผลมาจากการออกแบบโดยคณะกรรมการ ผู้บริหาร หรือบุคลากรอื่น ๆ ขององค์กร เพื่อก่อให้เกิดความมั่นใจได้อย่างสมเหตุสมผลว่าองค์กรจะสามารถบรรลุวัตถุประสงค์ได้

2.1.2 วัตถุประสงค์หลักของการควบคุมภายใน (ศิริ ตงศิริ, 2547)

วัตถุประสงค์หลักของการควบคุมภายในมี 3 ประการ คือ

1) ความมีประสิทธิผลและประสิทธิภาพของการดำเนินงาน (Effectiveness and Efficiency of Operations; O)
2) ความเชื่อถือได้ของรายงานทางการเงิน (Reliability of Financial Reporting; F)
3) การปฏิบัติตามกฎ ระเบียบ และนโยบายที่ใช้บังคับองค์กรนั้น ๆ (Compliance with Applicable Laws and Regulations; C)

2.1.3 ประโยชน์ที่มุ่งหวังได้จากการควบคุมภายใน

ประโยชน์ที่ได้จากการควบคุมภายใน ซึ่งก่อให้เกิดความเชื่อมั่นได้ในเรื่องต่อไปนี้

1) ความเชื่อถือได้และความถูกต้องของข้อมูลและรายงานทางการเงินและการปฏิบัติงาน
2) การปฏิบัติตามนโยบาย แผนงาน กระบวนการปฏิบัติงาน กฎหมาย และกฎระเบียบ
3) การดูแลป้องกันสินทรัพย์

4) การดำเนินงานอย่างประหยัดและมีประสิทธิภาพ

5) การบรรลุวัตถุประสงค์ขององค์กรและเป้าหมายของการดำเนินงานหรือโครงการ

2.1.4 **องค์ประกอบของมาตรฐานการควบคุมภายใน** (คณะกรรมการตรวจเงินแผ่นดิน, 2544)

มาตรฐานการควบคุมภายในประกอบด้วยองค์ประกอบ 5 ประการ ซึ่งผู้กำกับดูแลและฝ่ายบริหารจะต้องจัดให้มีในการดำเนินงานเพื่อให้บรรลุวัตถุประสงค์ของการควบคุมภายใน มีดังต่อไปนี้

1) **สภาพแวดล้อมของการควบคุม** (Control Environment)

"สภาพแวดล้อมของการควบคุม" หมายถึง ปัจจัยต่าง ๆ ซึ่งร่วมกันส่งผลให้มีการควบคุมขึ้นในหน่วยรับตรวจ หรือทำให้การควบคุมที่มีอยู่ได้ผลดีขึ้น หรือในทางตรงข้ามสภาพแวดล้อมอาจทำให้การควบคุมย่อหย่อนได้

ตัวอย่างปัจจัยที่เกี่ยวกับสภาพแวดล้อมของการควบคุมภายใน เช่น ปรัชญาและรูปแบบการทำงานของผู้บริหาร ความซื่อสัตย์และจริยธรรม ความรู้ ทักษะและความสามารถของบุคลากร โครงสร้างการจัดองค์กร การมอบอำนาจและหน้าที่ความรับผิดชอบ นโยบายและวิธีบริหารด้านบุคลากร เป็นต้น

ในการดำเนินการเกี่ยวกับสภาพแวดล้อมของการควบคุม ผู้กำกับดูแล ฝ่ายบริหาร และบุคลากรของหน่วยรับตรวจต้องสร้างบรรยากาศของการควบคุมเพื่อให้เกิดทัศนคติที่ดีต่อการควบคุมภายใน โดยส่งเสริมให้บุคลากรทุกคนในหน่วยรับตรวจเกิดจิตสำนึกที่ดีในการปฏิบัติงานในความรับผิดชอบ และตระหนักถึงความจำเป็นและความสำคัญของการควบคุมภายใน รวมทั้งดำรงรักษาไว้ซึ่งสภาพแวดล้อมของการควบคุมที่ดี

2) **การประเมินความเสี่ยง** (Risk Assessment)

"ความเสี่ยง" หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ซึ่งไม่พึงประสงค์ ที่ทำให้งานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนด

"การประเมินความเสี่ยง" หมายถึง กระบวนการที่ใช้ในการระบุและการวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยรับตรวจ รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยงหรือการบริหารความเสี่ยง

ในการดำเนินการเกี่ยวกับการประเมินความเสี่ยง ฝ่ายบริหารต้องประเมินความเสี่ยงทั้งจากปัจจัยภายในและภายนอกที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยรับตรวจอย่างพอเพียงและเหมาะสม

3) **กิจกรรมการควบคุม** (Control Activities)

"กิจกรรมการควบคุม" หมายถึง นโยบายและวิธีการต่าง ๆ ที่ฝ่ายบริหารกำหนดให้บุคลากรของหน่วยรับตรวจปฏิบัติเพื่อลดหรือควบคุมความเสี่ยงและได้รับการสนองตอบโดยมีการปฏิบัติตาม

ตัวอย่างกิจกรรมการควบคุม เช่น การสอบทานงาน การดูแลป้องกันทรัพย์สิน การแบ่งแยกหน้าที่งาน เป็นต้น

ในการดำเนินการเกี่ยวกับกิจกรรมการควบคุม ฝ่ายบริหารต้องจัดให้มีกิจกรรมการควบคุม ที่มีประสิทธิภาพและประสิทธิผล เพื่อป้องกันหรือลดความเสียหายที่อาจเกิดขึ้น และให้สามารถบรรลุวัตถุประสงค์ของการควบคุมภายใน สำหรับกิจกรรมการควบคุมในเบื้องต้นจะต้องแบ่งแยกหน้าที่งานภายในหน่วยรับตรวจอย่างเหมาะสม ไม่มอบหมายให้บุคคลใดบุคคลหนึ่งมีหน้าที่เป็นผู้รับผิดชอบปฏิบัติงานที่สำคัญหรืองานที่เสี่ยงต่อความเสียหายตั้งแต่ต้นจนจบ แต่ถ้ามีความจำเป็นให้กำหนดกิจกรรมการควบคุมอื่นที่เหมาะสมแทน

4) **สารสนเทศและการสื่อสาร** (Information and Communications)

"สารสนเทศ" หมายถึง ข้อมูลข่าวสารทางการเงิน และข้อมูลข่าวสารอื่น ๆ เกี่ยวกับการดำเนินงานของหน่วยรับตรวจ ไม่ว่าจะเป็นข้อมูลจากแหล่งภายในหรือภายนอก

ในการดำเนินการเกี่ยวกับสารสนเทศและการสื่อสาร ฝ่ายบริหารต้องจัดให้มีสารสนเทศอย่างเพียงพอและสื่อสารให้ฝ่ายบริหารและบุคลากรอื่น ๆ ที่เหมาะสมทั้งภายในและภายนอกหน่วยรับตรวจ ซึ่งจำเป็นต้องใช้สารสนเทศนั้นในรูปแบบที่เหมาะสมและทันเวลา

5) **การติดตามประเมินผล** (Monitoring)

"การติดตามประเมินผล" หมายถึง กระบวนการประเมินคุณภาพการปฏิบัติงานและประเมินประสิทธิผลของการควบคุมภายในที่วางไว้อย่างต่อเนื่องและสม่ำเสมอ โดยการติดตามผลระหว่างการปฏิบัติงาน (Ongoing Monitoring) และการประเมินผลเป็นรายครั้ง (Separate Evaluation) ซึ่งแยกเป็นการประเมินการควบคุมด้วยตนเอง (Control Self – Assessment) เช่น การประเมินการควบคุมโดยกลุ่มผู้ปฏิบัติงานภายในส่วนงานนั้น ๆ และการ

ประเมินการควบคุมอย่างเป็นอิสระ (Independent Assessment) เช่น การประเมินผลการควบคุมภายในโดยผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอก เป็นต้น

ในการดำเนินการเกี่ยวกับการติดตามประเมินผล ฝ่ายบริหารต้องจัดให้มีการติดตามประเมินผล โดยการการติดตามผลในระหว่างการปฏิบัติงาน และการประเมินผลเป็นรายครั้งอย่างต่อเนื่องและสม่ำเสมอ เพื่อให้ความมั่นใจว่า

- ระบบการควบคุมภายในที่วางไว้เพียงพอ เหมาะสม มีประสิทธิภาพและมีการปฏิบัติจริง
- การควบคุมภายในดำเนินไปอย่างมีประสิทธิผล
- ข้อตรวจพบจากการตรวจสอบและการสอบทานอื่น ๆ ได้รับการปรับปรุงแก้ไขอย่างเหมาะสมและทันเวลา
- การควบคุมภายในได้รับการปรับปรุงแก้ไขให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป

2.1.5 ประเภทของการควบคุมภายใน

การควบคุมภายในแบ่งตามลักษณะของของวิธีการควบคุมได้ 5 ประเภท ดังนี้

1) **การควบคุมแบบป้องกัน** (Preventive Controls) เป็นการป้องกันจากสิ่งที่ไม่ต้องการให้เกิดขึ้นในองค์กร

2) **การควบคุมแบบค้นหา** (Detective Controls) เป็นการค้นหาสิ่งที่ไม่ถูกต้องในองค์กร

3) **การควบคุมแบบแก้ไข** (Corrective Controls) เป็นการแก้ไขปัญหาที่ตรวจพบ

4) **การควบคุมแบบสั่งการ** (Directive Controls) เป็นการส่งเสริมสิ่งที่ต้องการให้เกิดขึ้นในองค์กร

5) **การควบคุมแบบทดแทน** (Compensating Controls) เป็นการควบคุมที่ช่วยทดแทนหรือชดเชยการควบคุมที่ขาดหาย

2.1.6 การควบคุมภายในเฉพาะอย่าง

จากประโยชน์ของการควบคุมภายในที่ทำให้เกิดความเชื่อมั่น 5 ประการ และจากวิธีการควบคุมภายใน 5 ประเภทที่กล่าวในข้างต้น ก่อให้เกิดรูปแบบเฉพาะอย่างของวิธีการควบคุม ซึ่งจำแนกเป็นพวก ๆ ได้ดังนี้

1) การควบคุมด้านองค์กร (Organization Controls)
2) การควบคุมด้านการปฏิบัติงาน (Operation Controls)
3) การควบคุมด้านการจัดการบุคลากร (Controls for Personnel Management)
4) การควบคุมโดยการสอบทาน (Review Controls)
5) สถานประกอบการ สิ่งอำนวยความสะดวก เครื่องใช้ และอุปกรณ์ต่าง ๆ (Facilities and Equipment)

2.1.7 การวางแผนการตรวจสอบแบบ Risk – Based Audit Plan

การวางแผนการตรวจสอบแบบ Risk – based Audit Plan หมายถึง การวางแผนการตรวจสอบโดยนำการประเมินความเสี่ยงมาเป็นเครื่องมือ เพื่อกำหนดลำดับกิจกรรมการตรวจสอบและความถี่ในการตรวจสอบในแต่ละกิจกรรมการตรวจสอบ ดังนั้นผู้ตรวจสอบจึงจำเป็นต้องมีหลักเกณฑ์และวิธีการที่ดี

2.1.7.1 ประโยชน์ของการวางแผนการตรวจสอบแบบ Risk – based Audit Plan

1) ทำให้ทุกกิจกรรมขององค์กรได้รับการตรวจสอบอย่างครบถ้วนตามผลการประเมินความเสี่ยง กิจกรรมที่มีความเสี่ยงสูงจะได้รับการตรวจสอบบ่อยครั้งกว่ากิจกรรมที่มีความเสี่ยงต่ำกว่า ซึ่งเป็นการใช้ทรัพยากรที่มีอยู่อย่างมีประสิทธิภาพและประสิทธิผล

2) ทำให้ผู้ตรวจสอบเข้าใจกิจกรรมและกระบวนการของหน่วยงานที่จะตรวจสอบก่อนเข้าตรวจสอบ สามารถประเมินความเสี่ยงของแต่ละกิจกรรมในเบื้องต้น เพื่อระบุขอบเขตของงานหรือระบบงานที่มีความเสี่ยง และอาจพบปัญหาในการปฏิบัติงาน

3) ทำให้เกิดการประสานงานและให้ความร่วมมือที่ดีจากผู้รับการตรวจสอบ เนื่องจากต้องมีการขอข้อมูลในการประเมินความเสี่ยงจากผู้รับการตรวจสอบ

4) ทำให้ทราบขอบเขต ปริมาณงาน และจำนวนอัตรากำลังที่ต้องการในกิจกรรมการตรวจสอบ สามารถใช้เป็นแนวทางในการจัดทำแผนอัตรากำลังและงบประมาณทั้งในปีปัจจุบันและอนาคต

5) ใช้เป็นเครื่องมือในการควบคุมกิจกรรมการตรวจสอบ ทำให้สามารถบริหารงานตรวจสอบได้อย่างมีประสิทธิภาพมากขึ้น

6) แสดงถึงการปฏิบัติงานตรวจสอบภายในตามมาตรฐานสากลการปฏิบัติงานวิชาชีพการตรวจสอบภายใน ซึ่งทำให้งานของผู้ตรวจสอบเป็นที่ยอมรับมากขึ้นจากผู้บริหารและผู้รับการตรวจสอบ

2.2 การบริหารความเสี่ยง (Risk Management)

สามารถอธิบายความหมายของความเสี่ยง ระบบบริหารความเสี่ยงและจำแนกแบ่งประเภทความเสี่ยง ได้ดังนี้

2.2.1 ความหมายของความเสี่ยง (ธารชุดา อมรเพชรกุล, 2546)

คำว่า ความเสี่ยง (Risk) นั้น มีผู้ให้นิยามไว้หลายแบบด้วยกัน ดังนี้

1) โอกาสการเกิดของเหตุการณ์ที่ไม่พึงประสงค์ (Undesirable Event) ภายในระยะเวลาหรือภายในสภาวะแวดล้อมที่ระบุขึ้น อาจพิจารณาได้ในลักษณะของความถี่ (Frequency) ของเหตุการณ์ไม่พึงประสงค์ที่เกิดขึ้นในช่วงเวลาหนึ่ง หรือความน่าจะเป็น (Probability) ที่จะเกิดเหตุการณ์ไม่พึงประสงค์นั้นขึ้นอีกครั้งหลังจากที่เคยเกิดมาแล้ว (วิริยา รัตนสุวรรณ, 2544)

2) โอกาสที่จะเกิดเหตุการณ์ซึ่งจะมีผลกระทบต่อวัตถุประสงค์ สามารถวัดได้จากผลกระทบที่ตามมา (Consequences) และความเป็นไปได้ในการเกิด (Likelihood) หรือกล่าวโดยง่ายว่า ความเสี่ยงคือ สิ่งใดก็ตามที่เกิดขึ้นแล้วจะทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์ที่ตั้งไว้ได้ (Siri Thongsiri, 2003)

3) โอกาสหรือเหตุการณ์ที่จะส่งผลกระทบทำให้วัตถุประสงค์เบี่ยงเบนไป หรือก่อให้เกิดความเสียหาย และสามารถเกิดขึ้นได้ตลอดเวลา (บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) และ สำนักตรวจสอบภายในและฝ่ายพัฒนาบุคลากร, 2545)

4) ความเป็นไปได้ของโอกาสที่จะเกิดเหตุการณ์ขึ้น และผลกระทบที่เป็นสาระสำคัญจากเหตุที่เกิดขึ้น (สุพจน์ โกสิยะจินดา, 2541)

จากความหมายต่าง ๆ ของความเสี่ยงข้างต้น ทำให้เราสามารถสรุปลักษณะของความเสี่ยงได้ 4 ประการ กล่าวคือ

- เป็นเหตุการณ์หรือโอกาสในการเกิดเหตุการณ์
- มีผลกระทบกับวัตถุประสงค์
- ก่อให้เกิดความเสียหาย ไม่เป็นที่ต้องการ
- มีความไม่แน่นอน ไม่ทราบว่าจะเกิดขึ้นเมื่อใด

ดังนั้น เราจึงอาจสรุปความหมายของความเสี่ยงได้เป็น "โอกาสหรือเหตุการณ์ที่ไม่พึงประสงค์ ที่จะส่งผลกระทบต่อวัตถุประสงค์ ก่อให้เกิดความเสียหายและสามารถเกิดขึ้นได้ตลอดเวลา"

2.2.2 **ประเภทของความเสี่ยง** (ธารซุดา อมรเพชรกุล, 2546)

บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) และสำนักงานตรวจสอบภายในและฝ่ายพัฒนาบุคลากร (2545) จำแนกประเภทความเสี่ยงออกเป็น 2 ประเภทใหญ่ ๆ โดยอาศัยปัจจัยแหล่งกำเนิดเป็นเกณฑ์ ดังนี้

ความเสี่ยงที่เกิดจากปัจจัยภายใน

- *Operational Risk* เกิดจากขั้นตอนและอุปกรณ์ในการปฏิบัติงาน
- *Human Resource Risk* เกิดจากตัวบุคลากรผู้ปฏิบัติงาน
- *Financial Risk* เกิดจากความไม่พร้อมในเรื่องงบประมาณ การเงิน
- *Strategic Risk* เกิดจากกลยุทธ์ และนโยบายในการบริหารงาน

ความเสี่ยงที่เกิดจากปัจจัยภายนอก

- *Competitive Risk* เกิดจากสภาวะการแข่งขัน บริษัทคู่แข่ง
- *Supplier / Customer Risk* เกิดจากบริษัทคู่ค้า และผู้ส่งมอบงานให้เรา
- *Regulatory / Legal Risk* เกิดจากกฎหมาย กฎระเบียบราชการ
- *Economic / Political Risk* เกิดจากสภาวะเศรษฐกิจและการเมือง

นอกจากนี้ การนิคมอุตสาหกรรมแห่งประเทศไทย (กนอ.) ได้แบ่งประเภทของความเสี่ยงออกเป็น 4 ด้าน ตามรูปแบบ S-F-O-C ดังนี้

1) **ความเสี่ยงด้านกลยุทธ์** (Strategic Risk) คือ ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ แผนดำเนินงานและการนำไปปฏิบัติไม่เหมาะสมหรือไม่สอดคล้องกับปัจจัยภายในและสภาพแวดล้อมภายนอก อันส่งผลกระทบต่อรายได้ หรือการดำรงอยู่ของกิจการ

2) **ความเสี่ยงด้านการเงิน** (Financial Risk) คือ ความเสี่ยงที่เกิดจากความไม่พร้อมในเรื่องงบประมาณ การเงิน เช่น ความผิดพลาดจากการเบิกจ่าย สภาพคล่องทางการเงิน เป็นต้น

3) **ความเสี่ยงด้านการปฏิบัติงาน** (Operational Risk; O) คือ ความเสี่ยงที่เกิดจากการปฏิบัติงานทุก ๆ ขั้นตอน โดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน อุปกรณ์ เทคโนโลยีสารสนเทศ บุคลากรในการปฏิบัติงาน เป็นต้น

ทั้งนี้ ไม่นับรวมความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการเงิน และความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ ซึ่งความไม่เพียงพอหรือความล้มเหลวที่เกิดขึ้นจากปัจจัยทั้ง 3 ปัจจัยข้างต้น เป็นสาเหตุที่ก่อให้เกิดความเสี่ยงด้านการปฏิบัติงานขึ้นได้ เช่น การทุจริต ความไม่เพียงพอหรือความไม่ถูกต้องของข้อมูลเพื่อการตัดสินใจ การหยุดชะงักหรือการขัดข้องของระบบคอมพิวเตอร์ เป็นต้น และอาจก่อให้เกิดความเสียหายต่อการดำเนินงานของหน่วยงานได้ (ชุมนุมสหกรณ์ออมทรัพย์แห่งประเทศไทย จำกัด หรือ ชสอ.)

ความเสี่ยงด้านปฏิบัติการ จำแนกออกได้ดังนี้

(1) **ความเสี่ยงจากการทุจริต**

(1.1) ความเสี่ยงจากการทุจริตจากภายใน เป็นความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายในองค์กร เพื่อให้ผลประโยชน์ที่เกิดขึ้นจากการทุจริตดังกล่าว ตกแก่พวกพ้องของตนเอง เช่น การปลอมแปลงเช็ค การปลอมแปลงเอกสาร การยักยอก หรือ การรับสินบน เป็นต้น

(1.2) ความเสี่ยงจากการทุจริตจากภายนอก เป็นความเสี่ยงที่เกิดจากการทุจริตของบุคคลภายนอกองค์กร แต่ก่อให้เกิดความเสียหายโดยตรงต่อหน่วยงาน เช่น การปลอมแปลงเช็ค การปลอมแปลงเอกสารทางการเงิน การฉ้อโกง เป็นต้น

(2) **ความเสี่ยงด้านบุคลากร** เป็นความเสี่ยงที่เกิดขึ้นจากกระบวนการจ้างงานที่ไม่เหมาะสม การจ่ายค่าตอบแทนหรือการปฏิบัติต่อพนักงานอย่างไม่เป็นธรรม ซึ่งอาจก่อให้เกิดการฟ้องร้อง การลาออก การหยุดงานประท้วง หรือการทำงานอย่างเฉื่อยชาล่าช้าได้ และการสรรหาบุคลากร ซึ่งอาจมีความรู้ ความสามารถ หรือมีคุณสมบัติไม่เพียงพอกับการปฏิบัติงาน นอกจากนี้ ยังรวมถึงความปลอดภัยในสถานที่ ซึ่งเป็นความเสี่ยงที่เกิดขึ้นเนื่องจากการกำหนดมาตรการรักษาความปลอดภัยในการปฏิบัติงาน และการควบคุมสภาพแวดล้อมในการปฏิบัติงานที่ไม่เพียงพอ จนส่งผลกระทบต่อสุขภาพของพนักงาน อันเนื่องมาจากโรคภัย หรือได้รับบาดเจ็บจากอุบัติเหตุอันเนื่องมาจากการปฏิบัติงานได้

(3) **ความเสี่ยงด้านความปลอดภัยของทรัพย์สิน** เป็นความเสี่ยงที่ก่อให้เกิดความเสียหายแก่ทรัพย์สินของหน่วยงาน อันเนื่องมาจากอุบัติภัยต่าง ๆ เช่น อุบัติเหตุ อัคคีภัย ภัยธรรมชาติ การทำลายทรัพย์สิน การจลาจล การก่อความไม่สงบทางการเมือง การก่อวินาศภัย เป็นต้น

(4) **ความเสี่ยงจากการขัดข้อง และหยุดชะงักของระบบงาน และระบบคอมพิวเตอร์** เป็นความเสี่ยงที่เกิดขึ้นจากระบบงานที่ผิดปกติ หรือการหยุดทำงานของระบบงานด้านต่าง ๆ เช่น ความไม่สอดคล้องกัน หรือความแตกต่างของระบบงานที่เกิดจากการควบรวมกิจการ ความบกพร่องของระบบงานคอมพิวเตอร์และระบบเครือข่าย รวมถึงการใช้เครื่องมือและเทคโนโลยี ที่ไม่เหมาะสมล้าสมัย และไม่มีประสิทธิภาพ เป็นต้น

(5) **ความเสี่ยงจากความปลอดภัยของข้อมูลสารสนเทศ** (Information Security Risk) เป็นความเสี่ยงที่เกิดขึ้นจากข้อมูลสำคัญสูญหาย ถูกขโมย หรือการเข้าถึงข้อมูลโดยไม่มีอำนาจ (Hacker) ลับลอบเข้าสู่ระบบข้อมูลคอมพิวเตอร์ อันอาจทำให้ข้อมูลชั้นความลับหรือข้อมูลทางธุรกิจของหน่วยงานเสียหายได้

(6) **ความเสี่ยงจากกระบวนการทำงาน** เป็นความเสี่ยงที่เกิดขึ้นจากความผิดพลาดในวิธีปฏิบัติงาน (Methodology) ความผิดพลาดของระบบการปฏิบัติงาน หรือความผิดพลาดจากการปฏิบัติงานของเจ้าหน้าที่ เช่น การขาดความรู้ความเข้าใจในการปฏิบัติงานและการใช้งานระบบคอมพิวเตอร์ของพนักงาน การปรับปรุงกระบวนการทำงานที่ไม่เหมาะสม เป็นต้น

4) **ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ** (Compliance Risk) คือ ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามกฎระเบียบหรือกฎหมายที่เกี่ยวข้องได้ หรือกฎระเบียบหรือกฎหมายที่มีอยู่ไม่เหมาะสม หรือเป็นอุปสรรคต่อการปฏิบัติงาน

2.2.3 **สาเหตุของการเกิดความเสี่ยง** (การนิคมอุตสาหกรรมแห่งประเทศไทย, 2548)

สาเหตุของการเกิดความเสี่ยงอาจเกิดจากปัจจัยหลัก 2 ปัจจัย คือ

1) **ปัจจัยภายใน** เช่น นโยบายของผู้บริหาร ความซื่อสัตย์ จริยธรรม คุณภาพของบุคลากร การเปลี่ยนแปลงระบบงาน ความเชื่อถือได้ของระบบสารสนเทศ การเปลี่ยนแปลงผู้บริหารและเจ้าหน้าที่บ่อยครั้ง การควบคุมกำกับดูแลไม่ทั่วถึง และการไม่ปฏิบัติตามกฎหมายระเบียบหรือข้อบังคับของหน่วยงาน เป็นต้น

2) **ปัจจัยภายนอก** เช่น กฎหมาย ระเบียบ ข้อบังคับของทางราชการ การเปลี่ยนแปลงทางเทคโนโลยี หรือสภาวะแวดล้อมทั้งทางเศรษฐกิจ และการเมือง เป็นต้น

2.2.4 ระบบบริหารความเสี่ยง (Risk Management System)

ระบบบริหารความเสี่ยง (Risk Management System) หมายถึง กระบวนการที่จัดทำขึ้นอย่างเป็นระบบ เพื่อลดความเสียหายที่อาจจะเกิดขึ้นเนื่องจากไม่บรรลุวัตถุประสงค์ที่ตั้งไว้ ให้อยู่ในระดับที่สามารถยอมรับได้

2.2.5 ขั้นตอนการจัดทำระบบบริหารความเสี่ยง

ระบบบริหารความเสี่ยงตามโครงสร้างการบริหารความเสี่ยงของมหาวิทยาลัย Queensland University of Technology (QUT) ซึ่งอิงตามมาตรฐานการบริหารความเสี่ยง AS/NZS 4360:1999 ของประเทศออสเตรเลียและประเทศนิวซีแลนด์ที่ใช้อยู่ในปัจจุบัน (Queensland University of Technology, Online) ประกอบด้วย 6 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 การทบทวนสภาพองค์กร (Establish the Context)

สิ่งสำคัญที่จะต้องจัดให้มีขึ้นก่อนการจัดการความเสี่ยง คือ การทำความเข้าใจถึงสภาพการดำเนินงานขององค์กร เพื่อช่วยในการระบุและกำหนดขอบเขตของสิ่งที่ส่งผลกระทบหรือมีอิทธิพลต่อองค์กร ทั้งที่มาจากปัจจัยภายในและภายนอกองค์กร เช่น การเงิน การดำเนินงาน สภาพการแข่งขัน การเมือง ภาพลักษณ์ สังคม ลูกค้า วัฒนธรรม กฎหมาย เป็นต้น นอกจากนี้จะต้องมีการกำหนดระดับการจัดการความเสี่ยงด้วยว่าจะดำเนินการถึงระดับใด เช่น ระดับองค์กร (Corporate Level) ระดับส่วน (Division Level) หรือระดับโครงการ (Project Level) เป็นต้น จากนั้นจึงกำหนดประเภทความเสี่ยงที่จะดำเนินการ เช่น ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงด้านการดำเนินงาน (Operational Risk) ความเสี่ยงด้านการปฏิบัติต่อกฎระเบียบ (Compliance Risk) หรือความเสี่ยงด้านชื่อเสียง (Reputational Risk) เป็นต้น

ขั้นตอนที่ 2 การระบุความเสี่ยง (Identify Risks)

ขั้นตอนนี้เป็นการระบุความเสี่ยงและโอกาสทั้งหมดที่เป็นไปได้ที่อาจส่งผลกระทบต่อวัตถุประสงค์ขององค์กร ส่วน หรือโครงการ ด้วยเครื่องมือต่าง ๆ อย่างเหมาะสม เช่น การระดมสมองร่วมกัน การตรวจติดตาม ประสบการณ์ส่วนบุคคลหรือขององค์กร เทคนิคการวิเคราะห์ระบบ การทบทวนการออกแบบระบบ การวิเคราะห์ประวัติและความล้มเหลว การวิเคราะห์ SWOT การออกแบบสอบถาม เป็นต้น แล้วนำผลที่ได้ไปวิเคราะห์และประเมินความเสี่ยงต่อไป

ขั้นตอนที่ 3 การวิเคราะห์ความเสี่ยง (Analyze Risks)

การวิเคราะห์ความเสี่ยงประกอบด้วย 3 ขั้นตอน ดังนี้

◈ **การประเมินระดับความเสี่ยง** (Inherent Risk) เป็นการประเมินระดับความเสี่ยงแต่ละตัวภายใต้สถานการณ์ปกติ ก่อนที่จะมีการจัดการความเสี่ยง ซึ่งประกอบด้วยปัจจัยที่สำคัญ 2 ปัจจัย ดังนี้

- *โอกาสในการเกิดความเสี่ยง (Likelihood)* ซึ่งอธิบายถึงความน่าจะเป็นหรือความถี่ที่จะเกิดความเสี่ยงนั้น โดยอาจกำหนดให้มีคะแนนอยู่ระหว่าง A-E ดังความหมายในตารางต่อไปนี้

ตารางที่ 2.1 การกำหนดระดับคะแนนของโอกาสในการเกิดความเสี่ยง

ระดับคะแนน	โอกาสเกิด	คำอธิบาย
A	มากที่สุด (Almost Certain)	คาดว่าจะเกิดขึ้นในสถานการณ์ส่วนใหญ่
B	มาก (Likely)	สามารถเกิดขึ้นได้ในสถานการณ์ปกติ
C	ปานกลาง (Possible)	อาจเกิดขึ้นได้บ้าง บางโอกาส
D	น้อย (Unlikely)	สามารถเกิดขึ้นได้เป็นครั้งคราว
E	น้อยมาก (Rare)	อาจเกิดขึ้นได้เฉพาะสถานการณ์ผิดปกติเท่านั้น

- *การประเมินความรุนแรงของผลกระทบที่เกิดขึ้น (Consequences)* คือผลลัพธ์ของเหตุการณ์แห่งความสูญเสีย การบาดเจ็บ ความเสียหาย หรือผลประโยชน์ที่ได้รับ โดยอาจกำหนดให้มีคะแนนอยู่ระหว่าง 1 - 5 ดังความหมายในตารางต่อไปนี้

ตารางที่ 2.2 การกำหนดระดับคะแนนความรุนแรงของผลกระทบที่เกิดขึ้น

ระดับคะแนน	ความรุนแรงที่เกิดขึ้น	คำอธิบาย
1	น้อยมาก (Insignificant)	ไม่มีการบาดเจ็บ, สูญเสียทางการเงินน้อย
2	น้อย (Minor)	มีการบาดเจ็บเล็กน้อย, สูญเสียทางการเงินปานกลาง, มีผลกระทบภายในองค์กร
3	ปานกลาง (Moderate)	ต้องได้รับการรักษาจากแพทย์, สูญเสียทางการเงินค่อนข้างมาก, มีผลกระทบกับลูกค้าภายนอก
4	มาก (Major)	บาดเจ็บสาหัส, สูญเสียทางการเงินมาก, สูญเสียความสามารถในการผลิต
5	มากที่สุด (Catastrophic)	เสียชีวิต, สูญเสียทางการเงินมหาศาล, มีผลกระทบถึงขั้นหายนะ

หลังจากที่ได้ให้คะแนนโอกาสในการเกิดความเสี่ยงและความรุนแรงของผลกระทบที่เกิดขึ้นแล้ว ต่อไปจะนำคะแนนทั้งสองมาเทียบกัน เพื่อพิจารณาระดับความเสี่ยง ดังตารางต่อไปนี้

ตารางที่ 2.3 การเทียบคะแนนเพื่อพิจารณาระดับความเสี่ยง

โอกาสในการเกิดความเสี่ยง	**ความรุนแรงของผลกระทบที่เกิดขึ้น**				
	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (A)	H	H	E	E	E
Likely (B)	M	H	H	E	E
Possible (C)	L	M	H	E	E
Unlikely (D)	L	L	M	H	E
Rare (E)	L	L	M	H	H

เมื่อ E: Extreme Risk H: High Risk

M: Moderate Risk L: Low Risk

◈ **การประเมินความเพียงพอของระบบหรือการควบคุมความเสี่ยงเดิมที่มีอยู่** เป็นการพิจารณาถึงความพร้อมและประสิทธิผลของระบบหรือการควบคุมความเสี่ยงเดิมที่มีอยู่ เพื่อเป็นแนวทางในการตัดสินใจว่าระบบหรือการควบคุมความเสี่ยงเดิมที่มีอยู่นั้นสมควรได้รับการปรับปรุง แก้ไข หรือเปลี่ยนไปใช้ระบบอื่นหรือไม่

สำหรับการประเมินความเพียงพอของระบบหรือการควบคุมความเสี่ยงเดิมที่มีอยู่นั้นอาจประเมินด้วยวิธีการตรวจติดตาม การศึกษาถึงประวัติหรือความน่าจะเป็นในการล้มเหลว เป็นต้น ส่วนประสิทธิผลของการนำไปปฏิบัติต่อความเสี่ยงอาจกำหนดให้มีการประเมินดังตารางต่อไปนี้

ตารางที่ 2.4 การประเมินประสิทธิผลของระบบหรือการควบคุมความเสี่ยงเดิมที่มีอยู่

ระดับ	**คำอธิบาย**
ดีเลิศ (Excellent)	ดีเยี่ยม ไม่ต้องมีการปรับปรุง
ดี (Good)	นำไปปฏิบัติแล้วได้ผลเป็นอย่างดี แต่มีบางส่วนต้องปรับปรุง
พอใช้ได้ (Fair)	ดีพอสมควร นำไปปฏิบัติแล้วได้ผลไม่ค่อยดีนัก
แทบจะไม่ดี (Marginal)	ไม่ได้นำไปปฏิบัติอย่างเคร่งครัด และไม่สอดคล้องกับความเสี่ยงที่ระบุ
แย่ / ยังไม่มีระบบ (Poor / Non-Existent)	

◈ **การประเมินความเสี่ยงที่อาจจะยังคงอยู่** (Residual Risk) เป็นการประเมินระดับความเสี่ยงที่อาจจะยังคงอยู่หลังจากที่ได้มีการจัดทำระบบหรือการควบคุมความเสี่ยงไว้แล้ว สำหรับการประเมินความเสี่ยงนั้นให้พิจารณาจากตารางที่ 2.2 2.3 และ 2.4 ตามลำดับ

ขั้นตอนที่ 4 การประเมินความเสี่ยง (Evaluate Risks)

เป็นขั้นตอนการประเมินความเสี่ยงที่อาจจะยังคงอยู่ ว่าสามารถยอมรับได้หรือไม่ พร้อมทั้งระบุเหตุผล ซึ่งจะต้องมีการกำหนดเกณฑ์ในการยอมรับหรือไม่สามารถยอมรับความเสี่ยงไว้ก่อนล่วงหน้า โดยทั่วไปแล้ว เหตุผลที่ต้องยอมรับความเสี่ยง ได้แก่

- ผลการประเมินความเสี่ยงที่อาจจะยังคงอยู่จากตารางที่ 2.4 มีความเสี่ยงอยู่ที่ระดับต่ำ
- ไม่สามารถหาแนวทางหรือวิธีการที่เหมาะสมเพื่อจัดการความเสี่ยงนั้นได้
- ต้นทุนของการจัดการความเสี่ยงสูงกว่าผลตอบแทนที่จะได้รับ
- โอกาส (Opportunities) มีความสำคัญมากกว่าภัยคุกคาม (Threats)

ขั้นตอนที่ 5 การปฏิบัติต่อความเสี่ยง (Treat Risks)

เป็นการกำหนดแนวทางที่เหมาะสมเพื่อจัดการและลดความเสี่ยงที่ไม่สามารถยอมรับได้ สามารถเลือกดำเนินการได้ 4 แนวทาง หรือเรียกง่าย ๆ ว่า 4T's Strategies ดังนี้

1) Take - **การยอมรับความเสี่ยง** (Risk Acceptance) คือ การยอมรับให้มีความเสี่ยงนั้น ๆ ปรากฏอยู่ เนื่องจากค่าใช้จ่ายในการจัดการหรือการสร้างระบบการควบคุมมีมูลค่าสูงกว่าผลลัพธ์ที่ได้จากการแก้ไขความเสียหายที่อาจเกิดขึ้น อย่างไรก็ตาม ควรกำหนดให้มีมาตรการในการจัดการเพื่อให้สามารถติดตามและดูแลความเสี่ยงนั้น ๆ ได้อย่างมีประสิทธิภาพ

2) Treat – **การลด/ควบคุมความเสี่ยง** (Risk Reduction/Control) คือ การลดโอกาสในการเกิดความเสี่ยงหรือความรุนแรงของผลกระทบที่เกิดขึ้นหรือลดทั้งคู่ ด้วยการออกแบบระบบการควบคุมภายใน การแก้ไขปรับปรุงองค์กร การแก้ไขปรับปรุงการปฏิบัติงานโดยการหากิจกรรมควบคุม (Control Activities) มาลดความเสี่ยง และการตรวจติดตาม

3) Terminate – **การหลีกเลี่ยงความเสี่ยง** (Risk Avoidance) คือ การหยุดดำเนินกิจกรรมที่ประกอบไปด้วยความเสี่ยงที่ไม่สามารถยอมรับได้ การเลือกดำเนินกิจกรรมอื่นที่สามารถยอมรับได้มากกว่า

4) Transfer – **การแชร์/ถ่ายโอนความเสี่ยง** (Risk Sharing/Transferring Spreading) คือ การแชร์หรือถ่ายโอนความเสี่ยงทั้งหมดหรือเพียงบางส่วนไปยังส่วนอื่น (Party) ที่

มั่นใจได้ว่ามีความสามารถในการควบคุมความเสี่ยงได้เป็นอย่างดี เพื่อลดความสูญเสียที่อาจจะเกิดขึ้น

ขั้นตอนที่ 6 การติดตามและการสอบทาน (Monitoring and review)

เป็นขั้นตอนที่มีความจำเป็นขั้นตอนหนึ่งของกระบวนการจัดการความเสี่ยง ซึ่งทำหน้าที่สอบทานและประเมินผลการจัดการความเสี่ยงอย่างสม่ำเสมอ เพื่อทำให้มั่นใจว่าระบบควบคุมความเสี่ยงสามารถปรับเปลี่ยนได้ทันและสอดคล้องต่อเงื่อนไขต่าง ๆ ที่เปลี่ยนแปลงไป พร้อมทั้งรายงานผลให้ฝ่ายบริหารรับทราบทันที หากพบว่าความเสี่ยงอยู่ระดับสูง เพื่อดำเนินการเสนอแผนจัดการความเสี่ยง

2.2.6 **กรอบการบริหารความเสี่ยงขององค์กรตามแนวทางของ** The Committee of Sponsoring Organisations of the Treadway Commission **หรือ** COSO (ไพร้วอเตอร์เฮาส์คูเปอร์ส, 2547)

ในเดือนกันยายน พ.ศ. 2535 COSO ได้พัฒนากรอบการบริหารความเสี่ยงขององค์กรขึ้นมา โดยการปรับปรุงเพิ่มเติมจากกรอบการควบคุมภายในเดิมที่มีอยู่และเพิ่มองค์ประกอบที่เป็นขั้นตอนของการประเมินความเสี่ยงให้ชัดเจนขึ้น ซึ่งเรียกว่า Enterprise Risk Management หรือ ERM กรอบการบริหารความเสี่ยงใหม่ของ COSO นี้จึงเป็นการเชื่อมโยงระหว่างการควบคุมภายในกับการบริหารความเสี่ยงที่เป็นสากลและเป็นที่ยอมรับในปัจจุบัน

COSO ได้ให้คำนิยามของ ERM ไว้ว่าเป็น "is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (พสุ เดชะรินทร์, 2548)

จากคำนิยามข้างต้นมีความหมายที่ซ่อนไว้ซึ่งสามารถแตกออกเป็นข้อ ๆ เพื่อความเข้าใจ ซึ่งจะได้ว่าการบริหารความเสี่ยงทั่วทั้งองค์กร หรือ ERM เป็น (พสุ เดชะรินทร์, 2548)

1) กระบวนการไม่ใช่ตัวผลลัพธ์
2) เป็นสิ่งที่ได้รับผลกระทบจากบุคลากรทั่วทั้งองค์กร
3) ใช้ในกรอบการบริหารกลยุทธ์ขององค์กร
4) ใช้ได้ทั่วทั้งองค์กร
5) ระบุหรือคาดการณ์ในสิ่งที่อาจจะเกิดขึ้นในอนาคตที่จะส่งผลกระทบต่อองค์กร
6) บริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

7) เป็นการสร้างความมั่นใจ

8) มีเป้าหมายเพื่อบรรลุวัตถุประสงค์ขององค์กร

กล่าวคือการบริหารความเสี่ยงทั่วทั้งองค์กรเป็น "กระบวนการที่บุคลากรทั่วทั้งองค์กรได้มีส่วนร่วมในการคิด วิเคราะห์ และคาดการณ์ถึงเหตุการณ์หรือความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งการระบุแนวทางในการจัดการกับความเสี่ยงดังกล่าวให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ เพื่อช่วยให้องค์กรบรรลุในวัตถุประสงค์ที่ต้องการ"

จากกรอบการควบคุมภายในเดิมของ COSO มีการขยายความเพิ่มเติมในองค์ประกอบที่ 2 คือ การประเมินความเสี่ยง (Risk Assessment) โดยเพิ่มอีก 3 องค์ประกอบ ซึ่งประกอบด้วย การกำหนดวัตถุประสงค์ (Objective Setting) การบ่งชี้เหตุการณ์ (Event Identification) และการตอบสนองต่อความเสี่ยง (Risk Response) รวมเป็น 8 องค์ประกอบ และเพิ่มวัตถุประสงค์หลักอีก 1 ประการ คือ วัตถุประสงค์เชิงกลยุทธ์ (Strategic Objective) การเปรียบเทียบกรอบการควบคุมภายในเดิมและกรอบการบริหารความเสี่ยงใหม่ของ COSO แสดงได้ดังรูปที่ 2.1

COSO 1 "Internal Control – Integrated Framework"

COSO 2 "Enterprise Risk Management – Integrated Framework"

รูปที่ 2.1 กรอบการควบคุมภายในเดิมและกรอบการบริหารความเสี่ยงใหม่ของ COSO

กรอบการบริหารความเสี่ยงตามแนวทางของ COSO ประกอบด้วยองค์ประกอบ 8 ประการ ซึ่งสัมพันธ์กับการดำเนินธุรกิจและกระบวนการบริหารงาน ดังนี้

- สภาพแวดล้อมภายในองค์กร (Internal Environment)
- การกำหนดวัตถุประสงค์ (Objective Setting)
- การบ่งชี้เหตุการณ์ (Event Identification)
- การประเมินความเสี่ยง (Risk Assessment)

- การตอบสนองความเสี่ยง (Risk Response)
- กิจกรรมการควบคุม (Control Activities)
- สารสนเทศและการติดต่อสื่อสาร (Information and Communication)
- การติดตามผล (Monitoring)

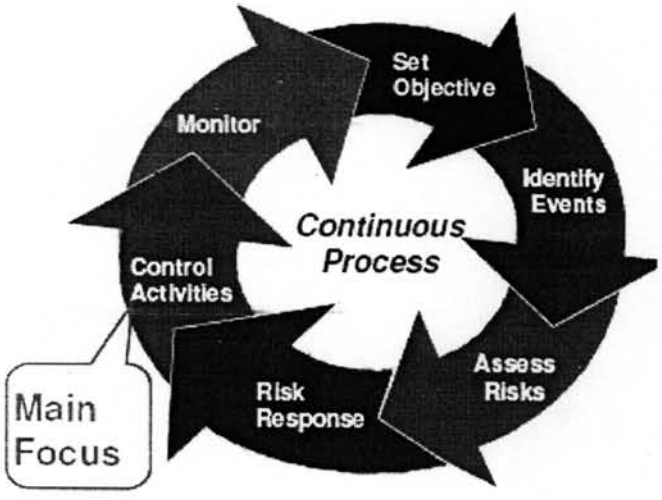
➢ **สภาพแวดล้อมภายในองค์กร** (Internal Environment)

สภาพแวดล้อมภายในองค์กรเป็นพื้นฐานที่สำคัญสำหรับกรอบการบริหารความเสี่ยง สภาพแวดล้อมนี้มีอิทธิพลต่อการกำหนดกลยุทธ์และเป้าหมายขององค์กร การกำหนดกิจกรรม การบ่งชี้ ประเมิน และจัดการความเสี่ยง ซึ่งจะเป็นการสร้างลักษณะภายในองค์กร (Tone of Organization) ที่มีอิทธิพลต่อการตระหนักถึงการควบคุมภายในของบุคลากรในองค์กร และเป็นพื้นฐานของทุกองค์ประกอบของการควบคุมภายใน โดยมีปัจจัยที่สำคัญประกอบไปด้วย (วิชัย กิตติวิทยากุล, 2548)

- ปรัชญา ความเชื่อและวัฒนธรรมในการบริหารความเสี่ยง
- บทบาทของคณะกรรมการในการกำกับดูแลการบริหารความเสี่ยง
- จรรยาบรรณ
- ความรู้ ความสามารถของบุคลากร
- การกำหนดอำนาจหน้าที่และความรับผิดชอบขององค์กร

➢ **กระบวนการบริหารความเสี่ยง** (Risk Management Process)

องค์กรที่นำกรอบการบริหารความเสี่ยงไปปฏิบัติได้อย่างประสบความสำเร็จ มีขั้นตอนที่สำคัญของการบริหารความเสี่ยงดังวงจรต่อไปนี้



รูปที่ 2.2 วงจรกระบวนการบริหารความเสี่ยง

1. **การกำหนดวัตถุประสงค์** (Objective Setting) การกำหนดวัตถุประสงค์ที่ชัดเจน คือ ขั้นตอนแรกสำหรับกระบวนการบริหารความเสี่ยง องค์กรควรมั่นใจว่าวัตถุประสงค์ที่กำหนดขึ้นมีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite) โดยทั่วไปวัตถุประสงค์และกลยุทธ์ควรได้รับการบันทึกเป็นลายลักษณ์อักษรและสามารพิจารณาในด้านต่าง ๆ ได้แก่ ด้านกลยุทธ์ ด้านปฏิบัติงาน ด้านการรายงาน และด้านการปฏิบัติตามกฎระเบียบต่างๆ

2. **การบ่งชี้เหตุการณ์** (Event Identification) การทำธุรกิจมักมีความไม่แน่นอนเกิดขึ้นมากมาย องค์กรไม่สามารถมั่นใจได้ว่าเหตุการณ์ใดเหตุการณ์หนึ่งจะเกิดขึ้นหรือไม่ หรือผลลัพธ์ที่เกิดขึ้นจะเป็นอย่างไร ในกระบวนการบ่งชี้เหตุการณ์ต้องพิจารณาปัจจัยเสี่ยงทุกด้านที่อาจเกิดขึ้นรวมถึงแหล่งความเสี่ยงทั้งจากภายในและภายนอกองค์กรด้วย

3. **การประเมินความเสี่ยง** (Risk Assessment) ขั้นตอนนี้เน้นการประเมินโอกาสและผลกระทบของเหตุการณ์ที่อาจเกิดขึ้นต่อวัตถุประสงค์ การเกิดเหตุการณ์ใดเหตุการณ์หนึ่งอาจส่งผลกระทบในระดับต่ำ แต่ถ้าเหตุการณ์เกิดขึ้นอย่างต่อเนื่องอาจมีผลกระทบในระดับสูงต่อวัตถุประสงค์ได้ โดยการประเมินความเสี่ยงประกอบด้วย 2 มิติ คือ โอกาสที่อาจเกิดขึ้นและผลกระทบที่เกิดขึ้น

4. **การตอบสนองความเสี่ยง** (Risk Response) เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้ว ผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้ โดยหลักการตอบสนองความเสี่ยงมี 4 ประการ ดังที่กล่าวมาแล้ว คือ การหลีกเลี่ยง (Avoid) การร่วมจัดการ (Share) การลด (Reduce) และการยอมรับ (Accept)

5. **กิจกรรมการควบคุม** (Control Activities) กิจกรรมการควบคุม คือ นโยบายและกระบวนการปฏิบัติงาน เพื่อให้มั่นใจได้ว่ามีการจัดการความเสี่ยง เนื่องจากแต่ละองค์กรมีการกำหนดวัตถุประสงค์และการนำไปปฏิบัติเป็นของเฉพาะองค์กร ดังนั้นกิจกรรมควบคุมจึงมีความแตกต่างกัน การควบคุมเป็นการสะท้อนถึงสภาพแวดล้อมภายในองค์กร ลักษณะธุรกิจ โครงสร้างและวัฒนธรรมองค์กร สิ่งสำคัญประการหนึ่งต่อกิจกรรมควบคุม คือ การกำหนดบุคลากรภายในองค์กรเพื่อรับผิดชอบการควบคุมนั้น

6. **การติดตามผล** (Monitoring) มีประเด็นที่สำคัญ ได้แก่

- การติดตามผลเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพและมีความเหมาะสม และการบริหารความเสี่ยงได้นำไปประยุกต์ใช้ในทุกระดับองค์กร
- ความเสี่ยงทั้งหมดที่มีผลกระทบสำคัญต่อการบรรลุวัตถุประสงค์ขององค์กรได้รับการรายงานต่อผู้บริหารที่รับผิดชอบ

➢ **สารสนเทศและการติดต่อสื่อสาร** (Information and Communication)

สารสนเทศเป็นสิ่งที่จำเป็นสำหรับองค์กรในการบ่งชี้ ประเมิน และจัดการความเสี่ยง ข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งภายนอกและภายในควรต้องได้รับการบันทึกและสื่อสารอย่างเหมาะสมทั้งในด้านรูปแบบและเวลา เพื่อช่วยให้บุคลากรที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพ มีการสื่อสารอย่างมีประสิทธิผล ซึ่งรวมถึงการแลกเปลี่ยนข้อมูลกับบุคคลภายนอก เช่น ลูกค้า ผู้จัดหาสินค้า ผู้ให้บริการ ผู้กำกับดูแล และผู้ถือหุ้น เป็นต้น

2.2.7 **ประโยชน์ของการบริหารความเสี่ยงที่มีประสิทธิภาพ** (วิชัย กิตติวิทยากุล, 2548)

ประโยชน์ของการบริหารความเสี่ยงมีดังต่อไปนี้

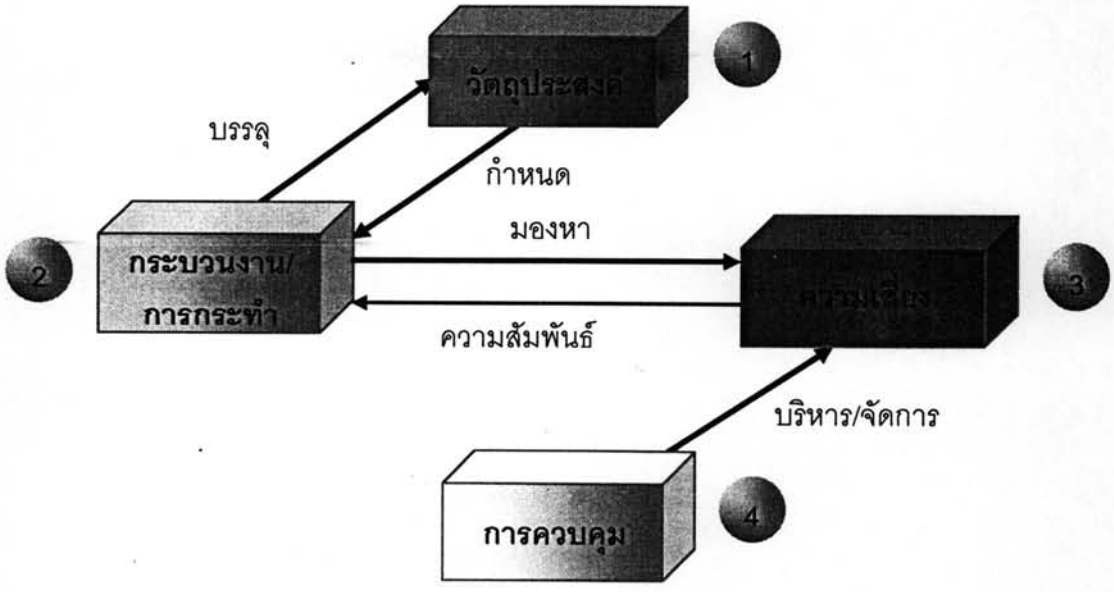
1) ช่วยให้องค์กรสามารถบริหารความเสี่ยงหรือเหตุการณ์ที่อาจจะเกิดขึ้นได้อย่างมีประสิทธิภาพ
2) ช่วยให้สามารถกำหนดแผนกลยุทธ์ และวัตถุประสงค์ที่สอดคล้องกับความเสี่ยงที่ยอมรับได้
3) ช่วยให้สามารถตัดสินใจและเลือกกลยุทธ์ในการบริหารความความเสี่ยงที่ดีขึ้น
4) บริหารความเสี่ยงในภาพรวมและทั่วทั้งองค์กร
5) สร้างโอกาสทางธุรกิจ
6) จัดสรรทรัพยากรได้ดีขึ้น
7) การดำเนินงานเป็นไปตามกฎหมาย
8) ระบบข้อมูลเพื่อการตัดสินใจดีขึ้น
9) ช่วยให้การวางแผนตรวจสอบภายในดีขึ้น

2.2.8 ความสัมพันธ์ระหว่างความเสี่ยง การควบคุมภายในและการตรวจสอบภายใน (ศิริ ตงศิริ, 2547)

ความสัมพันธ์ระหว่างความเสี่ยง การควบคุมภายในและการตรวจสอบภายใน มีดังต่อไปนี้

1) วัตถุประสงค์ใดที่ไม่มีการควบคุมจะไม่สำเร็จ
2) การควบคุมในจุดที่ไม่มีความเสี่ยง ทำให้เกิดการสูญเปล่าในการใช้ทรัพยากร
3) ถ้ามีความเสี่ยงต่ำ สามารถลดการควบคุมลงได้ แต่ผู้บริหารต้องยอมรับ
4) การตรวจสอบภายในที่ไม่พิจารณาความเสี่ยง และการควบคุมเป็นการตรวจสอบที่เสียเปล่า จึงต้องดูว่าจุดที่มีความเสี่ยง มีการควบคุมหรือไม่ ถ้ามีเพียงพอหรือไม่
5) ต้องรู้นโยบายกว้าง ๆ ในอนาคต เพื่อให้การควบคุมไปถูกทาง สอดคล้องกับนโยบายขององค์กร

จะเห็นได้ว่า การควบคุมภายในเป็นกระบวนการที่ต่อเนื่อง ซึ่งแทรกเข้าไปในกิจกรรมต่าง ๆ ขององค์กร และรวมอยู่ในวิธีการดำเนินธุรกิจอยู่แล้ว การขาดการควบคุมภายในที่ดีจึงเป็นการเปิดโอกาสให้เกิดความเสียหายอย่างใหญ่หลวง (ศิลปะพร ศรีจั่นเพชร, 2548) ดังนั้นจึงต้องสร้างการควบคุมภายในขึ้นมาเพื่อรับมือกับความเสี่ยง ความสัมพันธ์ของวัตถุประสงค์ กระบวนการ ความเสี่ยง และการควบคุมภายใน แสดงดังรูปที่ 2.3 (สุธนัย ประเสริฐสรรพ์, สไลด์)



รูปที่ 2.3 ความสัมพันธ์ของวัตถุประสงค์ กระบวนการ ความเสี่ยง และการควบคุมภายใน

2.2.9 **เกณฑ์การประเมินความเสี่ยงตามแนวทางของ** TRIS (Thai Rating and Information Services Co., Ltd.) (พรอนงค์ บุษราตระกูล, สไลด์) แบ่งเป็น 5 ระดับ ดังนี้

ระดับที่ 1

- มีแนวทางบริหารความเสี่ยงในเชิงรับ/ในระดับเบื้องต้น
- การบริหารความเสี่ยงยังไม่เป็นระบบ
- ไม่มีคณะทำงานเพื่อจัดการความเสี่ยงในรูปแบบบูรณาการ
- ไม่มีการจัดทำคู่มือการบริหารความเสี่ยง

ระดับที่ 2

- การบริหารความเสี่ยงของรัฐวิสาหกิจเป็นกลยุทธ์ระยะสั้น
- มีกระบวนการบริหารความเสี่ยงออกเป็นส่วนๆ
- มีการจัดทำคู่มือการบริหารความเสี่ยง
- ผลการบริหารความเสี่ยงที่เกิดขึ้นจริงด้อยกว่าแผนฯ และไม่ต่างจากอดีตที่ผ่านมาก่อนที่จะทำการบริหารความเสี่ยง

ระดับที่ 3

- มีการดำเนินงานครบถ้วนตามที่กำหนดในระดับที่ 2
- มีการบริหารความเสี่ยงที่เป็นกลยุทธ์หรือการดำเนินงานที่ต่อเนื่องทั้งองค์กร
- มีการบริหารความเสี่ยงแบบบูรณาการ
- มีการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดีตามที่กำหนด
- มีผลการบริหารความเสี่ยงที่เกิดขึ้นจริงไม่เป็นไปตามแผนฯ แต่ดีขึ้นจากอดีตที่ผ่านมาก่อนที่จะทำการบริหารความเสี่ยง

ระดับที่ 4

- มีการดำเนินงานครบถ้วนตามที่กำหนดในระดับที่ 3
- มีกลยุทธ์การบริหารความเสี่ยง เชื่อมโยงกับการกำหนดนโยบาย/กลยุทธ์การวางแผน/การลงทุนของรัฐวิสาหกิจ
- มีการสนับสนุนการบริหารเพื่อเพิ่มมูลค่าขององค์กร
- มีการทบทวนการบริหารความเสี่ยงอย่างสม่ำเสมอ และทำการปรับปรุงเมื่อจำเป็น

- มีผลการบริหารความเสี่ยงที่เกิดขึ้นจริงใกล้เคียงหรือดีกว่าแผนฯ และดีขึ้นจากอดีตที่ผ่านมาก่อนที่จะทำการบริหารความเสี่ยง
- มีการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดีตามที่กำหนด

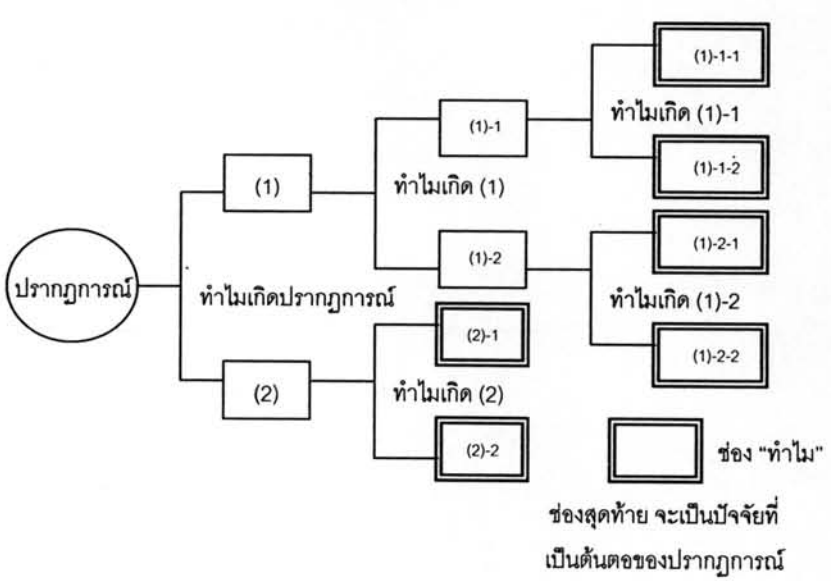
ระดับที่ 5

- มีการดำเนินงานครบถ้วนตามที่กำหนดในระดับที่ 4
- มีกระบวนการบริหารความเสี่ยง เป็นกิจกรรมประจำวัน และเป็นส่วนหนึ่งที่สำคัญของการพิจารณาผลตอบแทน
- มีการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดีตามที่กำหนด

2.3 การวิเคราะห์ Why – Why (Why – Why Analysis) (ฮิโตชิ โอกุระ และคณะ, 2545)

Why – Why Analysis เป็นเทคนิคการวิเคราะห์หาปัจจัยที่เป็นต้นเหตุให้เกิดปรากฏการณ์ที่เป็นระบบ มีขั้นตอน ไม่เกิดการตกหล่น ซึ่งไม่ใช่การคิดแบบคาดเดาหรือนั่งเทียน แต่อาศัยวิธีการระดมสมองจากผู้ที่มีความชำนาญ เป็นการถามว่าทำไมถึงเกิดปัญหานั้นซ้ำไปเรื่อย ๆ จนกว่าจะได้รากของปัญหา เพื่อนำมาโยงหาสาเหตุหลัก

การนำวิธีการวิเคราะห์ Why – Why นี้มาประยุกต์ใช้กับแผนผังต้นไม้เพื่อกระจายความเสี่ยงออกมาเพื่อหาปัจจัยเสี่ยงที่เป็นต้นเหตุแห่งความเสี่ยงที่จะนำไปสู่การกำหนดมาตรการควบคุมได้ต่อไป ตัวอย่างการอธิบายวิธีการวิเคราะห์ ค้นหาสาเหตุ เมื่อได้ปัจจัยที่เป็นต้นตอของปรากฏการณ์ แล้วจึงนำมาหามาตรการในการแก้ไข แสดงดังรูปที่ 2.4



รูปที่ 2.4 แผนภูมิอธิบายวิธีการคิดแบบ Why-Why Analysis

2.3.1 วิธีการมองปัญหาของ Why - Why Analysis

ก่อนทำ Why - Why Analysis ต้องตรวจสอบสถานที่จริงและดูสภาพงานจริง อันเป็นที่มาของปัญหา เพื่อสร้างความเข้าใจเกี่ยวกับรายละเอียดของปัญหาให้ถูกต้องชัดเจน และต้องทำความเข้าใจโครงสร้างและหน้าที่ของส่วนที่เป็นปัญหา อาจเขียนออกมาเป็นผังแสดงการไหลของงาน หรือภาพสเกตช์ของส่วนที่เป็นปัญหาก็ได้

แนวทางในการพิจารณาปัญหามี 2 แนวทาง คือ การมองปัญหาจากสภาพที่ควรจะเป็นและการมองปัญหาจากหลักเกณฑ์หรือทฤษฎี

1) **การมองปัญหาจากสภาพที่ควรจะเป็น** เป็นการมองปรากฏการณ์ที่เกิดขึ้นอย่างถี่ถ้วน แล้วกำหนดหัวข้อเงื่อนไขที่จำเป็น ซึ่งจะทำให้ปรากฏการณ์นั้นไม่เกิดขึ้น จากนั้นลองสำรวจหัวข้อเงื่อนไขแต่ละอันโดยดูจากของจริง แล้วทำการวิเคราะห์ต่อไปเฉพาะหัวข้อที่คิดว่าผิดปกติ

2) **การมองปัญหาจากหลักเกณฑ์หรือทฤษฎี** จะเป็นการวิเคราะห์สาเหตุของปรากฏการณ์อย่างครบถ้วนและทำให้พบต้นตอที่แท้จริงสูงกว่า

หมายเหตุ : การมองปัญหาจากหลักเกณฑ์หรือทฤษฎี ต้องอาศัยผู้ที่มีความรู้ความชำนาญในปัญหานั้นอย่างแท้จริง

2.3.2 ข้อควรระวังในการทำ Why-Why Analysis

ข้อควรระวังในการทำ Why-Why Analysis มีดังนี้

1) ข้อความที่ใช้เขียนตรงช่อง "ปรากฏการณ์" และช่อง "ทำไม" ต้องสั้นและกระชับ
2) หลังจากที่ทำ Why - Why Analysis แล้ว จะต้องยืนยันความถูกต้องตามหลักตรรกวิทยา โดยอ่านย้อนจาก "ทำไม" ช่องสุดท้ายกลับมายัง "ปรากฏการณ์" ได้
3) ให้ตรวจสอบดูว่า ปัจจัยหรือสาเหตุที่ทำให้เกิดเหตุการณ์ก่อนหน้านั้นได้ทำการหยิบยกขึ้นมาอย่างครบถ้วนหรือยัง โดยพิจารณาย้อนกลับว่า ถ้าปัจจัยนั้นไม่เกิดขึ้นแล้ว เหตุการณ์ก่อนหน้านั้นจะไม่เกิดขึ้นหรือไม่
4) ให้ถามว่า "ทำไม" ไปเรื่อย ๆ จนกว่าจะพบปัจจัยหรือสาเหตุที่สามารถเชื่อมโยงไปสู่การวางมาตรการป้องกันไม่ให้ปัญหาเกิดซ้ำอีก
5) ให้เขียนเฉพาะส่วนที่คิดว่าคลาดเคลื่อนไปจากสภาพปกติ (ผิดปกติ) เท่านั้น

6) ให้หลีกเลี่ยงการค้นหาสาเหตุที่มาจากสภาพจิตใจของคน เช่น ใจลอย เหนื่อย เป็นต้น

7) อย่าใช้คำว่า "ไม่ดี" ในประโยค

2.4 แผนผังกลุ่มเชื่อมโยงหรือแผนผังกลุ่มเครือญาติ (Affinity Diagram)

แผนผังกลุ่มเชื่อมโยงเป็นเครื่องมือที่มีประสิทธิภาพสูง สำหรับช่วยแก้ไขความสับสนและการนำปัญหามาสร้างเป็นภาพที่ชัดเจน แผนผังนี้ทำได้โดยการรวบรวมข้อเท็จจริงทั้งหลาย ความเห็นและความคิดเห็นในรูปแบบของข้อมูลที่เป็นคำพูดและสังเคราะห์เข้าด้วยกันเป็นแผนผังเดียว โดยมีขั้นตอนการทำเริ่มจากการกำหนดประเด็นปัญหาที่ต้องการระดมความคิด จากนั้นให้เขียนประโยคสั้น ๆ ที่มีความเกี่ยวข้องกับประเด็นปัญหานั้นลงในกระดาษ แล้วเมื่อได้ข้อมูลมากเพียงพอแล้ว จึงทำการจัดกลุ่มกระดาษที่มีความใกล้เคียงกันมาอยู่ด้วยกัน และเขียนหัวข้อของกลุ่มนั้น

2.5 เทคนิคที่ใช้ในการปรับปรุงงาน ECRS (Eliminate, Combine, Rearrange และ Simplify) (ประเวศ อัศวดากร และกิติศักดิ์ พลอยพานิชเจริญ, 2534)

ECRS คือ ตัวย่อจากภาษาอังกฤษ 4 คำ ที่ใช้เป็นหลักในการปรับปรุงงาน ซึ่งสร้างขึ้นจากการตรวจพิจารณาด้วย 5W2H เพื่อพิจารณาจุดประสงค์ของงาน ได้แก่

- Eliminate(E) คือการกำจัด กำจัดด้วยการไล่หาจุดประสงค์ อันทำให้สามารถกำจัดขั้นตอนที่ไม่จำเป็นออกได้ รูปแบบนี้มีประสิทธิผลสูงสุดในการปรับปรุงงาน
- Combine(C) คือการผสมผสาน โดยการผสมผสานองค์ประกอบของงานหลายประการเข้าด้วยกัน ช่วยให้ลดขั้นตอนของงานบางส่วนลงได้ และมีอยู่บ่อยที่พบว่าวิธีการใหม่ที่พบหลังจากการผสมผสานนี้ ทำให้งานทั้งระบบง่ายขึ้น
- Rearrange(R) คือการจัดลำดับใหม่ เป็นการโยกย้ายสับเปลี่ยนขององค์ประกอบของงาน อาจสร้างโอกาสกำจัดงานบางส่วนหรือโอกาสผสมผสานใหม่ก็ได้
- Simplify(S) คือการทำให้ง่าย เมื่อพิจารณาถึงการกำจัด การผสมผสาน และการจัดลำดับใหม่อย่างรอบคอบแล้ว พยายามจัดการองค์ประกอบของงานส่วนที่เหลืออยู่ให้เป็นงานที่ง่ายที่สุดเท่าที่จะทำได้

2.6 งานวิจัยที่เกี่ยวข้อง

พิชิต เทพวรรณ์ (2548) อธิบายการบริหารความเสี่ยงด้วยการควบคุมและตรวจสอบภายใน ซึ่งเป็นการบริหารแบบป้องกันและควบคุมความเสี่ยงที่จะเกิดขึ้น โดยอธิบายถึงประเภทความเสี่ยงและปัจจัยเสี่ยง ขั้นตอนการประเมินความเสี่ยง เกณฑ์การประเมินความเสี่ยง กลยุทธ์การบริหารความเสี่ยง และความสำคัญของการควบคุมและตรวจสอบภายในว่าอาจส่งผลกระทบต่อการดำเนินงานทั้งในกระบวนการปฏิบัติงานและพนักงานผู้ปฏิบัติงาน หากผู้บริหารนำมาใช้อย่างถูกต้องและเหมาะสม สามารถช่วยแก้ไขให้การบริหารความเสี่ยงของกิจการเกิดการบริหารและดำเนินงานขององค์กรเป็นไปอย่างมีประสิทธิภาพและประสิทธิผลโดยเกิดประโยชน์สูงสุดอย่างแท้จริง

นครินทร์ พลพินิจ (2547) ศึกษาความเสี่ยงในการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ของบริษัทกรณีศึกษา สำนัก Knowledge Management System บริษัท อุตสาหกรรมปิโตรเคมีกัลไทย จำกัด (มหาชน) เพื่อศึกษาโอกาสที่จะเกิดความเสี่ยงและความรุนแรงของความเสี่ยง พร้อมทั้งหา วิธีการควบคุมและจัดการระบบการให้บริการเครือข่ายคอมพิวเตอร์ให้มีประสิทธิภาพและประสิทธิผลสูงสุด โดยทำการศึกษาจากผู้ที่เกี่ยวข้องตั้งแต่ระดับบริหารจนถึงระดับปฏิบัติการ การ ซึ่งใช้แบบสอบถามเป็นเครื่องมือในการศึกษา จากผลการศึกษาสามารถแบ่งประเภทของความเสี่ยงเป็น 5 ประเภท คือ ความเสี่ยงด้านมนุษย์ ด้านระบบ/อุปกรณ์ ด้านสภาวะแวดล้อมและเงื่อนไขในการปฏิบัติงาน ด้านการบริหารจัดการ และด้านภารกิจ ในการประเมินความเสี่ยงด้วยโอกาสและความรุนแรงของความเสี่ยงนั้น จะได้ Risk Assessment Matrix โดยมีระดับความเสี่ยง 4 ระดับ จากนั้นพิจารณาระดับความเสี่ยง (Risk Ranking) ในแต่ละกลุ่มเปรียบเทียบกับเกณฑ์ที่กำหนดไว้ (Criteria) เพื่อกำหนดการปฏิบัติเพื่อควบคุมปัจจัยเสี่ยงก่อนหลังตามลำดับความสำคัญต่อไป

ญาณินี วจีประทับจิต (2547) นำแนวทางการบริหารความเสี่ยงมาประยุกต์ใช้ในการขยายการลงทุนในธุรกิจสำรวจและผลิตปิโตรเลียมในต่างประเทศ ของกรณีศึกษา บริษัท ปตท. สำรวจและผลิตปิโตรเลียม จำกัด (มหาชน) หรือ ปตท.สผ. โดยมีกระบวนการบริหารความเสี่ยง 5 ขั้นตอน ดังนี้ 1) การกำหนดวัตถุประสงค์ในการดำเนินงาน 2) การบ่งชี้ความเสี่ยง 3) การประเมินความเสี่ยง 4) การจัดการความเสี่ยง และ 5) การติดตามและประเมินผล โดยการสัมภาษณ์พนักงานในหน่วยงานที่มีส่วนเกี่ยวข้อง จากการศึกษาพบว่าสามารถแบ่งประเภทความเสี่ยงได้เป็น 5 ประเภท คือ ความเสี่ยงด้านการบริหารเชิงกลยุทธ์ ความเสี่ยงของประเทศที่จะเข้าไปลงทุน ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านการเงินและธุรกิจ และความเสี่ยงด้านเทคนิคและการดำเนินงาน ซึ่งมีความเสี่ยงที่อาจเกิดขึ้นทั้งหมด 24 รายการ โดยทำการประเมินจากโอกาสที่เหตุการณ์ความเสี่ยงนั้นจะเกิดขึ้นและผลกระทบที่มีต่อองค์กร ทำให้สามารถแบ่งกลุ่มความเสี่ยงตามโอกาสที่จะเกิด

และผลกระทบเป็น 3 กลุ่ม คือ กลุ่มที่มีโอกาสเกิดต่ำ กลุ่มที่มีโอกาสเกิดปานกลาง และกลุ่มที่มีโอกาสเกิดสูง จากนั้นนำความเสี่ยงในกลุ่มที่มีโอกาสเกิดสูงจำนวน 10 รายการ มาจัดทำรายงานตารางการตอบสนองต่อความเสี่ยง มาตรการติดตาม กิจกรรมควบคุม และกำหนดดัชนีชี้วัดความเสี่ยงหลักที่สำคัญ เพื่อใช้เป็นมาตรวัดหรือจุดเตือนภัยของระดับความเสี่ยงที่อาจกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร เพื่อให้ทราบว่ายังสามารถควบคุมความเสี่ยงนั้น ๆ ได้หรือไม่

วราพร อาสาพห์ประกิต (2547) พัฒนาระบบบริหารความเสี่ยงของโครงการการให้คำปรึกษาและติดตั้งระบบสารสนเทศ เพื่อใช้ป้องกันการเกิดเหตุการณ์ไม่พึงประสงค์ โดยมีกระบวนการบริหารความเสี่ยง ดังนี้ 1) การกำหนดและวางขอบเขตของโครงการ 2) การระบุความเสี่ยงภายในโครงการ 3) การค้นหาความเสี่ยงภายนอกโครงการ 4) การวิเคราะห์ปัจจัยเสี่ยง 5) การสร้างแผนจัดการความเสี่ยง และ 6) พัฒนาใบบันทึกข้อมูลความเสี่ยงเพื่อติดตามปัจจัยเสี่ยง การประเมินความเสี่ยงของโครงการ แบ่งเป็น 2 ส่วน คือ ปัจจัยภายในโครงการและปัจจัยภายนอกโครงการ โดยประเมินจากความรุนแรงและโอกาสในการเกิดความเสี่ยง พบว่า มีปัจจัยเสี่ยงทั้งจากภายในโครงการและภายนอกโครงการทั้งหมด 117 ความเสี่ยง และสรุปปัจจัยเสี่ยงต่าง ๆ เหลือ 27 ปัจจัยเสี่ยง แบ่งเป็นความเสี่ยงภายใน 13 ปัจจัย และความเสี่ยงภายนอก 14 ปัจจัย จากนั้นนำทุกปัจจัยเสี่ยงมาจัดลำดับและประเมินความเสี่ยงโดยผู้เชี่ยวชาญ ใช้เทคนิคการวิเคราะห์แขนงความบกพร่อง หรือ FTA (Fault Tree Analysis) เพื่อค้นหาสาเหตุของความเสี่ยง แล้วสร้างแผนควบคุมความเสี่ยง โดยนำแผน 4 แผน จากแผนทั้งหมด 14 แผน มาประยุกต์ใช้ในโครงการ พบว่าปัจจัยเสี่ยงที่มีความรุนแรงในระดับ 3 ลดความรุนแรงลงเป็นระดับ 1 หมายความว่า ระดับความเสี่ยงปานกลางจะกลายเป็นระดับความเสี่ยงน้อยมาก ซึ่งสามารถลดระดับความเสี่ยงของโครงการได้เป็นอย่างดี

วราวรรณ ทิพพานิช (2547) ได้ศึกษาแนวทางในการนำกระบวนการบริหารความเสี่ยงมาใช้ในองค์กรของกรณีศึกษา บริษัท ปิโตรเคมีแห่งชาติ จำกัด (มหาชน) หรือ เอ็นพีซี โดยได้อธิบายถึงขั้นตอนและกระบวนการบริหารความเสี่ยงทั่วทั้งองค์กรภายใต้โครงการ Total Risk Management หรือ TRM ซึ่งมีขอบเขตของการประเมินความเสี่ยงในระดับบริษัท (Corporate Risk) ก่อนเป็นอันดับแรก โดยเริ่มตั้งแต่ขั้นตอนการออกแบบระบบ การประเมินและจัดลำดับความเสี่ยง การกำหนดโครงสร้างหน้าที่ความรับผิดชอบ การสื่อสารและระบบสารสนเทศ จนถึงการเตรียมเข้าใช้งาน การประเมินความเสี่ยงของกรณีศึกษาทำโดยการจัดสัมภาษณ์ผู้ที่เกี่ยวข้องในแต่ละสายงาน โดยมีหัวข้อที่สัมภาษณ์ คือ ปัจจัยแห่งความสำเร็จ ทิศทางในอนาคต อุปสรรคที่สำคัญของธุรกิจ ความไม่แน่นอนต่าง ๆ Key Result Area ของหน่วยงานต่าง ๆ และอื่น ๆ พบว่ามีความเสี่ยงจำนวน 74 รายการใน 194 สถานการณ์ของความไม่แน่นอน จากจำนวนวัตถุประสงค์ที่กำหนดไว้ 16

วัตถุประสงค์ โดยแบ่งประเภทของความเสี่ยงได้ 4 ประเภท ได้แก่ Strategy Risk Operation Risk Financial Risk และ Business Risk และมีการจัดระดับของความเสี่ยงหลักที่สำคัญ 10 อันดับแรก จากนั้นได้กำหนดแนวทางจัดการความเสี่ยงหลักโดยกำหนดระดับของการยอมรับความเสี่ยงและแผนดำเนินการเพิ่มเติม (Action Plan) และมีการนำแนวทางและเครื่องมือการบริหารที่บริษัทกรณีศึกษาใช้อยู่แล้วในปัจจุบันมาประยุกต์และเชื่อมโยงให้ใช้กับโปรแกรมการบริหารความเสี่ยง ซึ่งเป็นแนวทางการดำเนินการที่บริษัทกรณีศึกษากำหนดไว้ในเบื้องต้น

ธารชุดา อมรเพชรกุล (2546) พัฒนาระบบบริหารความเสี่ยงในสายงานทะเบียนและตรวจสอบพัสดุ ส่วนการพัสดุ สำนักบริหารแผนและการคลัง จุฬาลงกรณ์มหาวิทยาลัย โดยเริ่มจากการกำหนดวัตถุประสงค์ของสายงาน ระบุความเสี่ยงที่มาจากทุกขั้นตอนการทำงานในสายงาน จัดกลุ่มประเด็นความเสี่ยงด้วยแผนผังกลุ่มความคิด (Affinity Diagram) ดำเนินการประเมินความเสี่ยงผ่านแบบสอบถามโดยใช้เทคนิค FMEA (Failure Mode and Effects Analysis) เพื่อจัดลำดับความเสี่ยง และใช้เทคนิคการวิเคราะห์แบบ FTA (Fault Tree Analysis) เพื่อช่วยค้นหาสาเหตุของความเสี่ยง จากนั้นจึงสร้างแผนจัดการความเสี่ยง โดยได้ระบุระยะเวลาและผู้รับผิดชอบไว้อย่างชัดเจน นอกจากนี้ ผู้เขียนได้ออกแบบใบบันทึก (Check Sheet) เพื่อใช้ติดตามดูผลของการจัดทำระบบบริหารความเสี่ยง ทั้งนี้ การวัดผลระบบบริหารความเสี่ยงที่ได้จัดทำขึ้นจำเป็นต้องใช้ระยะเวลานาน ดังนั้นผู้วิจัยจึงกำหนดให้มีการประเมินความเสี่ยงคาดหมาย เพื่อเปรียบเทียบค่าตัวเลขความเสี่ยงชี้นำ (Risk Priority Number) หรือ RPN ก่อนและหลังการมีแผนจัดการความเสี่ยงในสายงานทะเบียนและตรวจสอบพัสดุ

Heller (2006) พัฒนาระบบบริหารความเสี่ยงโดยใช้เทคนิค Multi – Criteria Decision Making (MCDM) ซึ่งเป็นระบบคอมพิวเตอร์ที่ช่วยในการตัดสินใจในขั้นตอนของการประเมินและวิเคราะห์ความเสี่ยง ที่มีความแม่นยำและสามารถแก้ไขเปลี่ยนแปลงข้อมูลได้ตลอดเวลา ทำให้สามารถขจัดความซับซ้อนของปัญหาลงได้ โดยเสนอเป็นแบบจำลอง (Model) ซึ่งนำวิธีการทางคณิตศาสตร์มาใช้ร่วมกับการจัดการความเสี่ยง สำหรับเทคนิค MCDM ที่นำมาใช้ เช่น กระบวนการลำดับชั้นเชิงวิเคราะห์ (Analytic Hierarchy Process; AHP) เทคนิค Risk Scoring และ Indexing Technique เป็นต้น การวิจัยจะวิเคราะห์หาปัจจัยเสี่ยงไปเรื่อย ๆ ตามลำดับชั้น โดยเริ่มจากจำแนกประเภทความเสี่ยง และค้นหาปัจจัยความเสี่ยงในแต่ละประเภท จนสุดท้ายจะทำให้ทราบแหล่งที่มาของความเสี่ยง โดยการประเมินคะแนนความเสี่ยง ซึ่งพิจารณาจากความถี่ โอกาส และผลกระทบที่เกิดขึ้น ทำให้จัดลำดับความสำคัญของปัจจัยเสี่ยงได้ จากนั้นนำมาจัดทำเป็น Risk Matrix เพื่อ

เปรียบเทียบระดับของความเสี่ยงในแต่ละแหล่งที่มาของแต่ละกลุ่มประเภทความเสี่ยง แล้วนำความเสี่ยงหลักที่สำคัญมาวางแผนจัดการต่อไป

Mills et al. (2006) ศึกษาวิเคราะห์ความเสี่ยงทางการเงินในโครงการประหยัดพลังงาน โดยอธิบายเทคนิคและวิธีการบริหารความเสี่ยง ซึ่งแบ่งเป็นความเสี่ยงที่ควบคุมได้และความเสี่ยงที่ควบคุมไม่ได้ โดยการสัมภาษณ์จากกลุ่มบุคคล 4 กลุ่ม คือ The Financial Service Sector, In-house Operations Management, Owners of Energy-using Facilities, และ Energy Policy Makers ในการระบุความเสี่ยง ได้แบ่งประเภทความเสี่ยงเป็น 5 ประเภท ได้แก่ ความเสี่ยงด้านเศรษฐกิจ สิ่งแวดล้อม เทคโนโลยี การปฏิบัติงาน และการวัดและการตรวจสอบ ซึ่งแต่ละด้านอาจมีทั้งความเสี่ยงที่ควบคุมได้และควบคุมไม่ได้ จากนั้นเป็นการวิเคราะห์ความเสี่ยงโดยใช้สัมประสิทธิ์ความเปลี่ยนแปลง (Coefficient of Variation; CV) ในการวิเคราะห์ด้วยโปรแกรมอารีนา (Arena) โดยเปรียบเทียบให้เห็นถึงความเสี่ยงในการลงทุนแต่ละแบบ ถ้า CV น้อยแสดงว่ามีความเสี่ยงน้อย และการวิเคราะห์ด้วยเทคนิค Monte Carlo Simulation จะใช้ตัวแปรต่าง ๆ ในการประเมิน และได้เสนอแนวทางในการจัดการความเสี่ยงสำหรับความเสี่ยงทั้ง 5 ประเภท ทั้งความเสี่ยงที่ควบคุมได้และควบคุมไม่ได้

Aven and Kristensen (2005) อธิบายกรอบการบริหารความเสี่ยง ซึ่งประกอบด้วย 2 ทิศทาง คือ ความเสี่ยงที่เป็นผลกระทบจากเหตุการณ์ต่าง ๆ ที่อาจจะเกิดขึ้น และความเสี่ยงที่เกิดขึ้นจากความไม่แน่นอนของเหตุการณ์ ในมุมมองต่าง ๆ เช่น ความเสี่ยงด้านเศรษฐกิจ ด้านสังคม และด้านวัฒนธรรม เป็นต้น โดยโครงสร้างของการบริหารความเสี่ยงเริ่มจากการระบุปัญหาหรือความเสี่ยง แล้วกำหนดวัตถุประสงค์หรือเกณฑ์การพิจารณาความเสี่ยง จากนั้นวิเคราะห์และประเมินความเสี่ยง แล้วจึงตัดสินใจพิจารณาแผนการจัดการความเสี่ยงหรือนำไปปฏิบัติ งานวิจัยนี้ได้นำรูปแบบการวิเคราะห์ความเสี่ยงนี้ไปใช้ในบริษัทกรณีศึกษา 3 แห่ง ที่ดำเนินการเกี่ยวกับอุตสาหกรรมก๊าซและน้ำมัน ซึ่งส่วนมากเป็นความเสี่ยงด้านความปลอดภัยในการทำงานเป็นหลัก พบว่า ต้องมีการกำหนดระดับความปลอดภัยหรือความเสี่ยงให้แน่นอน ว่าความเสี่ยงระดับใดที่ยอมรับได้ ระดับใดยอมรับไม่ได้ แล้วจึงนำมาพิจารณาร่วมกับกระบวนการตัดสินใจต่อไป

Eskesen et al. (2004) ได้จัดทำแนวทางการบริหารความเสี่ยงโดยการพัฒนาจากแนวทางการบริหารความเสี่ยงเดิมที่มีอยู่ ด้วยเทคนิคการบริหารความเสี่ยงที่เป็นระบบ (Systematic Risk Management Techniques) เพื่อเป็นคู่มือแนวปฏิบัติที่ดีเลิศ (Best-Practice) ของการบริหารความเสี่ยงสำหรับเจ้าของกิจการ และเพื่อเป็นแนวทางการบริหารความเสี่ยงในการขุดเจาะ

อุโมงค์หรือทางลอดใต้ดินแก่ผู้ที่สนใจ โดยกระบวนการบริหารความเสี่ยงจะวิเคราะห์ความเสี่ยงตั้งแต่ขั้นตอนการออกแบบ การประมูลและทำสัญญา จนถึงการก่อสร้าง ซึ่งจะทำให้โครงการสามารถแล้วเสร็จได้ทันเวลาและเสียค่าใช้จ่ายน้อยที่สุด ในการระบุความเสี่ยงต้องคำนึงถึงขอบเขต วัตถุประสงค์ และกลยุทธ์ในการบริหารความเสี่ยงเป็นหลัก ในการบริหารความเสี่ยงนี้คณะผู้วิจัยได้ใช้หลัก ALARP (*as low as reasonably practicable*) คือ การลดความเสี่ยงทั้งหมดให้เหลือน้อยที่สุด การระบุปัจจัยเสี่ยงทำโดยการศึกษาจากงานวิจัยของโครงการที่คล้ายคลึงกันและการสัมภาษณ์จากผู้ปฏิบัติงาน ทีมงาน หรือองค์กรต่างๆ ทั่วโลก แล้วนำปัจจัยเสี่ยงที่ได้มาจัดเป็น 10 กลุ่มประเด็นความเสี่ยง จากนั้นทำการประเมินความเสี่ยงด้วยการออกแบบสอบถามโดยประเมินจากโอกาสและความรุนแรงที่จะเกิดขึ้น นำค่าเฉลี่ยที่ได้มาจัดระดับของความเสี่ยงและเปรียบเทียบกับเกณฑ์ในการยอมรับความเสี่ยง ซึ่งแบ่งเป็น 4 ระดับ คือ Unacceptable, Unwanted, Acceptable และ Negligible เพื่อจัดลำดับความสำคัญของปัจจัยเสี่ยงที่จะทำการลดความเสี่ยงตามหลัก ALARP ต่อไป ในการวิเคราะห์หาสาเหตุของความเสี่ยงจะใช้เครื่องมือต่าง ๆ เช่น Fault Tree Analysis, Event Tree Analysis และ Decision Tree Analysis เป็นต้น สำหรับวิธี Multirisk เป็นวิธีการคำนวณเกี่ยวกับค่าใช้จ่ายและเวลาโดยใช้ฐานคอมพิวเตอร์ เหมาะในการใช้เมื่อยังมีความไม่แน่นอนหลงเหลืออยู่ในระดับสูง ส่วนวิธี Monte Carlo Simulation ใช้ในกรณีที่มีตัวแปรมากและเป็นปัญหาที่ซับซ้อน

Yu (2002) อธิบายถึงกรอบการบริหารความเสี่ยง ที่เรียกว่า Integrated Risk Management หรือ IRM โดยกล่าวถึงวิธีการจัดการและกลยุทธ์ในการตัดสินใจเกี่ยวกับความเสี่ยงสำหรับอุตสาหกรรมพลังงานภายใต้สภาวะที่มีความไม่แน่นอน การศึกษาแบ่งเป็น 4 ส่วน โดยส่วนแรกเป็นการระบุและรวบรวมความเสี่ยงทั้งหมดที่อาจจะเกิดขึ้น ส่วนที่ 2 กล่าวถึงการจัดประเภทของความเสี่ยงทั้งหมดนั้นออกเป็น 5 ประเภท คือ ความเสี่ยงที่เกี่ยวกับ คน ธุรกิจ การเงิน ผลกระทบจากเหตุการณ์ และข้อมูล ส่วนที่ 3 อธิบายกระบวนการ IRM โดยมองถึงโครงสร้างการทำงานของแต่ละคนในองค์กร (Work Breakdown Structure; WBS) และมีการตรวจสอบย้อนกลับ (Feedback) ด้วยกระบวนการตัดสินใจ (Decision Making) เป็นวงจรต่อเนื่องกันไป ซึ่งขั้นตอนจะประกอบด้วย การระบุความเสี่ยง มีการใช้เครื่องมือและเทคนิคต่าง ๆ เช่น Scenario Analysis, การระดมสมอง (Brainstorming) และการใช้แบบใบบันทึก (Check Sheet) จากนั้นประเมินโอกาสและผลกระทบ โดยใช้ Monte Carlo, Extreme Value Approach, Distribution Analysis และ Stress Testing ซึ่งประกอบด้วย Scenario Analysis, Stress Modeling และ Risk Control Plan เป็นต้น แล้ววางแผนจัดการความเสี่ยง โดยใช้ If-Then-Else ซึ่งพิจารณาจากสถานการณ์ปัจจุบันและในอนาคต IRM เป็นวงจรแห่งการเรียนรู้และปฏิบัติการ จึงต้องมีการตรวจสอบและประเมินประสิทธิภาพ รวมถึง

พัฒนาปรับปรุงอยู่ตลอดเวลา และสามารถนำไปประยุกต์ใช้ได้ในธุรกิจทุกระดับ สุดท้ายกล่าวถึงประโยชน์ของ IRM ว่าสามารถใช้เป็นเครื่องมือในการช่วยให้องค์กรบรรลุวิสัยทัศน์และวัตถุประสงค์ในการจัดการความเสี่ยงและช่วยจัดสรรทรัพยากรต่าง ๆ อย่างเหมาะสมด้วย

Freimut et al. (2001) เสนอวิธีการบริหารความเสี่ยงที่มีชื่อว่า Riskit Method โดยมีวัตถุประสงค์เพื่อวิเคราะห์ประโยชน์และความพอเพียงของ Riskit Method เพื่อเป็นการพัฒนาและยืนยันว่าสามารถใช้ Riskit Method นี้ได้ในโครงการบริหารความเสี่ยงทั่ว ๆ ไป และเพื่อวิเคราะห์ค่าใช้จ่ายและผลกำไรในการใช้ Riskit Method โดยมีขั้นตอนดังนี้ การระบุความเสี่ยง จะใช้เทคนิคการระดมสมองและแบบใบบันทึก (Check Sheet) การวิเคราะห์ความเสี่ยงใช้เทคนิค Riskit Analysis Graph หรือ Risk Scenario ซึ่งจะช่วยให้ทำความเข้าใจได้ง่ายขึ้น การจัดลำดับความเสี่ยงของ Risk Scenario จะประเมินจากโอกาสร่วมกับความสูญเสียที่จะเกิดขึ้น เรียกเทคนิคนี้ว่า Riskit Pareto Ranking จากนั้นได้นำ Riskit Method นี้ไปใช้ในกรณีศึกษา บริษัทโทรคมนาคมในประเทศเยอรมัน พบว่า สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ได้คือ สามารถใช้ Riskit Method ได้ในกิจการทั่ว ๆ ไป เหมาะสำหรับโครงการบริหารความเสี่ยงที่มีข้อจำกัดด้านเวลา และค่าใช้จ่ายในการบริหารความเสี่ยงก็เป็นที่ยอมรับได้ ซึ่งจะได้มีการพัฒนาวิธีการให้เป็นสากลมากขึ้น