การนำกรอบการบริหารความเสี่ยงไปใช้ในองค์กร

อัญชลี พิพัฒนเสริญ

รองศาสตราจารย์ประจำภาควิชาการบัญชี

คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

บทคัดย่อ

บทความนี้นำเสนอการนำกรอบการบริหารความเสี่ยงไปใช้ในองค์กร โดยได้อธิบายเรื่องต่าง ๆ เกี่ยวกับกรอบการบริหารความเสี่ยงและการนำไปใช้ในองค์กร เช่น คำจำกัดความ ประเด็นสำคัญสำหรับกรอบการบริหารความเสี่ยง ขั้นตอนการบริหารความเสี่ยง บทบาทหน้าที่และความรับผิดชอบของหน่วยงานด้านการบริหารความเสี่ยงขององค์กร ขอบเขตของกิจกรรมในการบริหารความเสี่ยงและการวางแผนการตรวจสอบ กลยุทธ์ในการบริหารความเสี่ยง การตัดสินใจของคณะกรรมการ ผู้บริหารและการบริหารความเสี่ยง บทบาทของผู้ตรวจสอบภายในในการบริหารความเสี่ยงขององค์กร มาตรฐานการตรวจสอบภายในสำหรับการประเมินความเสี่ยง เทคโนโลยีสารสนเทศและการบริหารความเสี่ยงองค์กร

คำสำคัญ: การบริหารความเสี่ยง กรอบการบริหารความเสี่ยง ความเสี่ยง

The Adoption of Enterprise Risk Management Framework in Organizations

Anchalee Pipatanasern

Associate Professor of Department of Accounting,
Thammasat Business School, Thammasat University

ABSTRACT

This article demonstrates adoption of a Enterprise Risk Management Framework (ERM) in organizations. It narrates various matters relating risk management framework and adoption in organizations. Those matters include significant matters for ERM Framework, processes of risk management, roles and responsibilities of risk management department, scopes of activities in risk management and audit planning, risk management strategies, decisions of board and management and risk management, roles of internal auditors in risk management of an organizations, internal audit standards for risk assessment, information system and organizational risk management.

Keywords: Risk Management, Framework of Risk Management, Risk

บทนำ

องค์กรต่าง ๆ ไม่ว่าจะเป็นองค์กรเพื่อแสวงหากำไรหรือองค์กรเพื่อการกุศลต่างมีจุดมุ่งหมายเพื่อสร้างมูลค่าให้กับผู้ที่มีส่วนได้เสียขององค์กร แต่ปัจจัยที่จะทำให้องค์กรไม่สามารถทำตามวัตถุประสงค์ดังกล่าวได้ก็คือ ความเสี่ยง ทั้งความเสี่ยงต่อการดำเนินงานทั่วไปขององค์กร หรือความเสี่ยงต่อการปฏิบัติตามกลยุทธ์ขององค์กร

ในอดีตที่ผ่านมาองค์กรหลายแห่งไม่ได้มีการระบุคำนิยามของคำว่าความเสี่ยงอย่างชัดเจน และส่วนมากมักจะมองความเสี่ยงเป็นแค่หน่วยย่อย ๆ ไม่ได้มองความเสี่ยงในภาพรวมขององค์กรดังเช่นที่ John Flaherty ประธานกรรมการโคโซ่ คนแรกได้เคยกล่าวไว้ว่า “ถึงแม้จะผู้คนมากมายที่พูดถึงเรื่องความเสี่ยง แต่ก็ไม่มีคำนิยามของคำว่าการบริหารความเสี่ยงที่เป็นที่ยอมรับโดยทั่วไป และไม่มีกรอบกระบวนการในการบริหารความเสี่ยงที่ชัดเจน จึงทำให้การสื่อสารด้านความเสี่ยงระหว่างคณะกรรมการและผู้บริหารมีความสับสน” ซึ่งเป็นสถานการณ์ที่คล้ายคลึงกับกรณีของการควบคุมภายใน จึงทำให้เกิดแนวความคิดในการจัดทำกรอบการบริหารความเสี่ยงหรือ COSO Enterprise Risk Management หรือ ERM Framework ที่จะช่วยให้องค์กรมีนิยามของการบริหารความเสี่ยงที่ครอบคลุมความเสี่ยงระดับองค์กร โดย COSO ERM Framework นี้เป็นการร่วมมือกันระหว่าง COSO และ PricewaterhouseCoopers (PwC) ซึ่งเผยแพร่ในเดือนกันยายนของปี ค.ศ. 2004

ERM Framework หมายถึง การบริหารปัจจัย การควบคุมกิจกรรม รวมทั้งการกำหนดกระบวนการดำเนินงานด้านต่าง ๆ ขององค์กรเพื่อจัดมาตรเหตุ หรือโอกาสที่จะก่อให้เกิดความเสียหายแก่องค์กร โดยพยายามให้ระดับความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่องค์กรยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ ทั้งนี้ต้องคำนึงถึงการบรรลุเป้าหมายทั้งในด้านกลยุทธ์ การปฏิบัติตามระเบียบ ข้อบังคับ และชื่อเสียงขององค์กรเป็นสำคัญ ซึ่งควรจะได้รับการสนับสนุน และการมีส่วนร่วมในการบริหารความเสี่ยงจากคณะกรรมการบริษัท ผู้บริหาร และบุคคลากรในทุกระดับทั่วทั้งองค์กร

ประเด็นสำคัญสำหรับกรอบการบริหารความเสี่ยงประกอบไปด้วยประเด็นเหล่านี้

- **การบริหารความเสี่ยงเป็นกระบวนการในการทำงาน** ไม่ใช่แค่กฎที่ต้องปฏิบัติตาม ตัวอย่างเช่น กระบวนการอนุมัติสินเชื่อ ก็จะมีการกำหนดกฎเกณฑ์ในการให้สินเชื่อที่สามารถเปลี่ยนแปลงได้ตามเงื่อนไขหรือปัจจัยอื่น ๆ กระบวนการบริหารความเสี่ยงก็เป็นกระบวนการที่มีขั้นตอนของการตรวจทานและประเมินความเสี่ยงเพื่อให้สามารถตอบสนองต่อปัจจัยต่าง ๆ ของทั้งองค์กรได้
- **กระบวนการบริหารความเสี่ยงจะนำไปใช้โดยคนในองค์กร** กระบวนการบริหารความเสี่ยงจะต้องถูกจัดการโดยบุคคลที่มีความเข้าใจความเสี่ยงนั้น ๆ เป็นอย่างดี เพื่อให้สามารถระบุความเสี่ยงและปัจจัยอื่น ๆ ที่เกี่ยวข้อง และสามารถนำกระบวนการบริหารความเสี่ยงไปใช้ได้อย่างเหมาะสม
- **กระบวนการบริหารความเสี่ยงจะนำไปใช้ผ่านทางการวางกลยุทธ์ของทั้งองค์กร** ในบางครั้งองค์กรอาจต้องตัดสินใจด้านกลยุทธ์ เช่น การตัดสินใจระหว่างการซื้อหน่วยงานย่อยขององค์กรอื่น หรือว่าการสร้างขึ้นเองภายในองค์กร ซึ่งองค์กรก็สามารถนำกระบวนการบริหารความเสี่ยงไปใช้ประกอบในการตัดสินใจด้านกลยุทธ์และประเมินความเสี่ยงของแต่ละกิจกรรมภายในองค์กร
- **จะต้องมีการนำหลักการยอมรับความเสี่ยงมาใช้** การยอมรับความเสี่ยง คือ ระดับของความเสี่ยงที่องค์กรและผู้จัดการแต่ละคนยอมรับ โดยอาจกำหนดเป็นระดับ สูง ปานกลาง และต่ำ หรืออาจกำหนดเป็นจำนวนเงินก็ได้
- **กระบวนการบริหารความเสี่ยงเป็นแค่การให้ความเชื่อมั่นอย่างสมเหตุสมผล** แต่ไม่ใช่เครื่องรับประกันว่าจะทำให้บรรลุวัตถุประสงค์ขององค์กรถึงแม้ว่ากระบวนการบริหารความเสี่ยงจะถูกวางแผนไว้อย่างดีแค่ไหน แต่ก็ไม่สามารถยืนยันได้ว่าผลที่เกิดขึ้นจะสามารถบรรลุวัตถุประสงค์ได้ องค์กรที่มีการควบคุมที่ดีมากก็อาจ

ดำเนินงานได้อย่างราบรื่นในช่วงเวลาหนึ่ง ๆ แต่ก็มีความเป็นไปได้ที่จะเกิดเหตุการณ์ที่กระทบต่อองค์กรจากความผิดพลาดของบุคลากร หรือจากบุคคลอื่น ๆ

• **กระบวนการบริหารความเสี่ยงสร้างขึ้นเพื่อช่วยให้องค์กรสามารถบรรลุวัตถุประสงค์** องค์กรต้องมีการจัดทำวัตถุประสงค์โดยรวมของทั้งองค์กร และสื่อสารไปยังผู้มีส่วนได้เสียขององค์กร โดยวัตถุประสงค์ดังกล่าวก็คือการสร้างและรักษาชื่อเสียงขององค์กรโดยการจัดทำรายงานทางการเงินที่เชื่อถือได้ และปฏิบัติตามกฎระเบียบข้อกฎหมายอย่างถูกต้อง และกระบวนการบริหารความเสี่ยงก็จะช่วยทำให้บรรลุวัตถุประสงค์ได้

เป้าหมายและวัตถุประสงค์ขององค์กรจะไม่สามารถสร้างคุณค่าให้แก่องค์กรได้หากว่าไม่มีการจัดการวิธีในการบริหารงานที่ครอบคลุมหลาย ๆ มุมมอง และจะต้องเข้าใจความสัมพันธ์ระหว่างกระบวนการต่าง ๆ ในการดำเนินงาน ซึ่งนับว่าเป็นจุดเด่นของ ERM Framework ที่สามารถใช้ระบุผลกระทบของการปฏิบัติตามกฎระเบียบข้อกฎหมายที่มีต่อการควบคุมภายในแต่ละระดับ และความสำคัญของการปฏิบัติตามข้อกฎหมายต่อองค์กรทั้งองค์กร

ขั้นตอนในการบริหารความเสี่ยง

การบริหารความเสี่ยงประกอบไปด้วยกระบวนการ 4 ขั้นตอน คือ (1) การระบุความเสี่ยง (2) การประเมินความเสี่ยงในเชิงปริมาณและเชิงคุณภาพ (3) การจัดลำดับความสำคัญของความเสี่ยงและการวางแผนการตอบสนองความเสี่ยง และ (4) การติดตามและประเมินผล

พนักงานทุกระดับและทุกแผนกงานจะมีส่วนเกี่ยวข้องในกระบวนการบริหารความเสี่ยงขององค์กรด้วย ไม่ว่าจะเป็นองค์กรขนาดใหญ่ที่มีแผนกบริหารความเสี่ยงแยกต่างหาก หรือจะเป็นองค์กรขนาดเล็กที่มีเพียงทีมบริหารความเสี่ยงจำนวนไม่กี่คนก็ตาม เนื่องจากพนักงานจากแต่ละสายงานก็จะมีมุมมองเรื่องความเสี่ยงที่แตกต่างกัน

กระบวนการระบุความเสี่ยงนั้นเป็นกระบวนการที่ต้องมีการพิจารณาอย่างละเอียดรอบคอบเพื่อให้สามารถระบุได้ว่าในแต่ละการดำเนินงานขององค์กรจะมีความเสี่ยงใดที่สามารถเกิดขึ้นได้บ้าง และจะต้องจำแนกให้ได้ว่าความเสี่ยงใดที่มีความสำคัญที่จะส่งผลต่อการดำเนินงานในช่วงเวลาที่สมเหตุสมผลของการระบุความเสี่ยง

นอกจากนี้ กระบวนการระบุความเสี่ยงยังต้องเกิดขึ้นในทุกระดับขององค์กร เนื่องจากความเสี่ยงที่ส่งผลต่อหน่วยงานย่อย ๆ อาจไม่ได้ส่งผลกระทบต่อองค์กรโดยภาพรวมมากนัก ในขณะที่ความเสี่ยงบางอย่างอาจส่งผลกระทบต่อทั้งองค์กร วิธีการระบุความเสี่ยงของทั้งองค์กรอาจเริ่มจากการสร้างภาพรวมว่าองค์กรมีการดำเนินงานระดับใหญ่ ๆ อย่างไรบ้าง ในแต่ละแผนกการดำเนินงานอาจจะประกอบไปด้วยโรงงานในหลาย ๆ ประเทศ ซึ่งมีการดำเนินงานที่แตกต่างกันออกไป และมีแผนกหรือหน่วยงานย่อยที่แตกต่างกันด้วย

วิธีการระบุความเสี่ยงอาจทำได้โดยการกำหนดผู้ประเมินความเสี่ยงจากแต่ละแผนกภายในองค์กร เช่น แผนกผลิต การเงิน การบัญชี และไอที และให้ผู้ประเมินความเสี่ยงทำการประเมินความเสี่ยงที่เกี่ยวข้องกับหน่วยงานที่ตนเองรับผิดชอบอยู่ การที่จะรวบรวมความเสี่ยงในแต่ละด้านให้ครอบคลุม จะต้องมีการรวบรวมบุคลากรที่สำคัญจากแต่ละฝ่ายมาประชุมร่วมกัน และทำการระดมสมอง (Brainstorming) เพื่อระบุความเสี่ยงในแต่ละด้าน

เมื่อมีการระดมสมองกันระหว่างบุคลากรจากแต่ละฝ่ายก็จะมีการทำความเข้าใจถึงความเสี่ยงในแต่ละด้าน โดยการถามคำถาม เช่น

- ความเสี่ยงต่าง ๆ จะส่งผลต่อองค์กรทั้งองค์กร หรือว่าส่งผลกระทบเพียงแค่หน่วยงานเดียว
- ความเสี่ยงนั้นจะเกิดจากปัจจัยภายในองค์กร หรือเกิดจากปัจจัยภายนอก
- ความเสี่ยงต่าง ๆ มีความเกี่ยวข้องกับความเสี่ยงอื่น ๆ หรือไม่

การถามคำถามเหล่านี้จะทำให้เกิดความเข้าใจลักษณะของแต่ละความเสี่ยงมากขึ้น และสามารถระบุได้ว่าความเสี่ยงใดที่มีความสำคัญและจะต้องถูกจัดประเภทเป็นความ

เสี่ยงหลัก เช่น ความเสี่ยงด้านความพึงพอใจของลูกค้า หรือความเสี่ยงจากการมีคู่แข่งรายใหญ่เข้ามาในอุตสาหกรรม ซึ่งความเสี่ยงหลักเหล่านี้อาจส่งผลกระทบต่อองค์กร ทำให้นักลงทุนขาดความเชื่อมั่น และองค์กรก็จะขาดแคลนเงินทุน ซึ่งก็จะส่งเสียต่อองค์กรโดยรวม

เมื่อผู้ประเมินความเสี่ยงสามารถระบุความเสี่ยงหลักขององค์กรออกจากความเสี่ยงทั่วไปได้แล้ว ความเสี่ยงเหล่านี้ก็จะต้องเผยแพร่และสื่อสารให้กับบุคคลที่มีส่วนเกี่ยวข้อง ทั้งผู้จัดการฝ่ายการเงิน ผู้จัดการฝ่ายผลิต บุคลากรที่เข้าร่วมในการประชุม รวมไปถึงบุคลากรจากแผนกอื่น ๆ ที่ไม่ได้เข้าร่วมประชุมด้วย

บทบาทหน้าที่และความรับผิดชอบของหน่วยงานด้านการบริหารความเสี่ยงขององค์กร

องค์กรขนาดใหญ่ในปัจจุบันต่างมีแผนกหรือหน่วยงานที่รับผิดชอบด้านการบริหารความเสี่ยง เช่น ประธานฝ่ายสารสนเทศ (Chief Information Officer: CIO) ประธานผู้บริหารงานตรวจสอบภายใน (Chief Audit Executive: CAE) ซึ่งประธานอาจรายงานโดยตรงไปที่กรรมการบริหารโดยตรง หรือประธานฝ่ายอื่น ๆ ที่เกี่ยวข้องก็ได้ แต่สำหรับองค์กรที่มีการบริหารความเสี่ยงที่มีประสิทธิภาพ หน่วยงานบริหารความเสี่ยงจะควบคุมโดยประธานฝ่ายบริหารความเสี่ยง (Chief Risk Officer: CRO) ซึ่งมีหน้าที่รับผิดชอบว่าความเสี่ยงขององค์กรได้ถูกประเมินและสื่อสารไปยังหน่วยงานภายในองค์กรที่รับผิดชอบเรียบร้อยแล้ว หน่วยงานบริหารความเสี่ยงจะเป็นผู้กำหนดนโยบายในการตอบสนองต่อความเสี่ยงแต่ละความเสี่ยง และผลักดันให้กระบวนการตอบสนองความเสี่ยงนั้นมีการนำไปใช้จริง รวมถึงบทลงโทษในกรณีที่ไม่มีการปฏิบัติตามอย่างถูกต้อง เนื่องจากการควบคุมที่ไม่มีประสิทธิภาพของหน่วยงานเพียงหน่วยเดียวก็อาจส่งผลเสียต่อทั้งองค์กรได้

ความรับผิดชอบของหน่วยงานด้านความเสี่ยงภายในองค์กรในปัจจุบันได้ขยายไปถึงเรื่องการปฏิบัติตามกฎระเบียบ ข้อคำนึงที่เกี่ยวกับตลาดทุน การรายงานทางการเงิน สินทรัพย์ทางปัญญา และกิจกรรมที่เกี่ยวข้องกับระบบเทคโนโลยี ผู้ที่ทำหน้าที่ในหน่วยงานบริหารความเสี่ยงและประธานฝ่ายบริหารความเสี่ยงจึงต้องมีความรู้ที่กว้างขวางเพื่อให้ตระหนักถึงความเสี่ยงจากหลาย ๆ ด้าน และบริหารงานครอบคลุมการบริหารความเสี่ยงของทั้งองค์กร

คณะกรรมการบริหารความเสี่ยง

แนวความคิดเรื่องประธานฝ่ายบริหารความเสี่ยงและหน่วยงานบริหารความเสี่ยงอาจเป็นสิ่งที่ค่อนข้างใหม่สำหรับบางองค์กรในปัจจุบัน แต่ก็เป็นกระบวนการที่จะช่วยปรับปรุงสภาพแวดล้อมในการควบคุม และปรับปรุงกระบวนการต่าง ๆ ภายในองค์กรให้มีประสิทธิภาพมากขึ้น ทั้งประธานฝ่ายบริหารความเสี่ยงและหน่วยงานบริหารความเสี่ยงมีหน้าที่รับผิดชอบการบริหารความเสี่ยงของทั้งองค์กรตาม COSO ERM Framework ซึ่งประกอบไปด้วย สามมิติคือ องค์ประกอบในการบริหารความเสี่ยงแปดระดับที่จะถูกนำไปใช้กับทุกระดับในองค์กรตามมิติที่สอง และมิติที่สามก็คือการบริหารความเสี่ยงภายใต้วัตถุประสงค์ทางด้านการปฏิบัติตามกฎระเบียบ การรายงาน การปฏิบัติงาน และกลยุทธ์

ประธานฝ่ายบริหารความเสี่ยง หรือ Chief Risk Officer: CRO จะเป็นผู้ที่บริหารจัดการและตรวจตราการบริหารความเสี่ยงของทั้งองค์กร จึงต้องมีอำนาจและความรับผิดชอบในการจัดการโปรแกรมความเสี่ยงให้แก่องค์กร และสามารถสื่อสารกิจกรรมในการตอบสนองต่อความเสี่ยงไปยังผู้บริหารระดับรองลงไปได้

ความรับผิดชอบหลักของประธานฝ่ายบริหารความเสี่ยง คือ การบริหารจัดการกระบวนการประเมินความเสี่ยงของทั้งองค์กร จัดทำกระบวนการแก้ไขความเสี่ยงอย่างเหมาะสม รวมถึงการบริหารหน่วยงานฝ่ายสนับสนุนการบริหารความเสี่ยงด้วย ดังเช่นที่หน่วยงานการควบคุมภายในจะมีผู้เชี่ยวชาญพิเศษในการประเมินการควบคุมภายในและให้คำแนะนำในการแก้ไข หน่วยงานฝ่ายสนับสนุนการบริหาร

ความเสี่ยงก็จะทำหน้าที่ติดตามและให้คำแนะนำสำหรับการบริหารความเสี่ยง

หน้าที่ของหน่วยงานบริหารความเสี่ยงนั้นนอกจากจะตรวจสอบความเสี่ยงขององค์กรแล้ว ยังต้องทำหน้าที่สำคัญในการผลักดันให้กระบวนการตอบสนองต่อความเสี่ยงและการแก้ไขความเสี่ยงนั้นได้นำไปใช้จริงภายในองค์กร

ตัวอย่างของการบริหารความเสี่ยงที่มีประสิทธิภาพ เช่น

- นักวิเคราะห์ของหน่วยงานบริหารความเสี่ยงพิจารณาความเสี่ยงด้านหนี้สินที่อาจเกิดจากการการพัฒนาผลิตภัณฑ์ใหม่ แล้วก็ต้องวางแผนเพื่อที่จะตอบสนองต่อความเสี่ยง ไม่ใช่แค่ยื่นเรื่องให้กับหน่วยงานดังกล่าวให้หาวิธีแก้ไขเอง
- วิเคราะห์สถานการณ์ทางการเมืองหรือทางด้านกฎหมายว่าจะส่งผลกระทบต่อการดำเนินงานในประเทศต่าง ๆ อย่างไร โดยปรึกษากับที่ปรึกษาด้านกฎหมาย, ผู้จัดการของหน่วยงานในต่างประเทศหรือที่ปรึกษาจากภายนอก เพื่อลดผลกระทบจากกฎหมาย
- ร่วมมือกับฝ่ายเทคนิคของแผนกไอทีเพื่อนำระบบเทคโนโลยีที่มีประสิทธิภาพมาใช้ภายในองค์กร

บทบาทของคณะกรรมการบริหารความเสี่ยงนี้ยังไม่ได้ถูกกำหนดว่าแต่ละองค์กรจะต้องจัดตั้งคณะกรรมการบริหารความเสี่ยงขึ้นมา จึงทำให้ยังไม่มีข้อกำหนดถึงลักษณะของผู้ที่จะมาดำรงตำแหน่งในคณะกรรมการ แต่อย่างไรก็ตามเนื่องจากเป็นส่วนหนึ่งของคณะกรรมการบริหาร ดังนั้นคณะกรรมการบริหารความเสี่ยงจึงควรเป็นบุคคลภายนอกที่มีความเป็นอิสระ และเช่นเดียวกับการที่คณะกรรมการตรวจสอบจะต้องมีคณะกรรมการอย่างน้อยหนึ่งคนที่มีความรู้ความสามารถในด้านการบัญชีและการเงิน คณะกรรมการบริหารความเสี่ยงก็ควรจะเป็นผู้ที่มีความรู้ความเชี่ยวชาญในการบริหารความเสี่ยงด้วย

ขอบเขตของกิจกรรมในการบริหารความเสี่ยงและการวางแผนการตรวจสอบ

การบริหารความเสี่ยงเป็นกิจกรรมที่ถูกขับเคลื่อนโดยเหตุการณ์ความเสี่ยงที่เกิดขึ้นอย่างฉุกเฉิน ซึ่งต้องมีการปรับปรุงและพัฒนาอยู่เสมอ เพื่อให้ตอบสนองต่อความเสี่ยงใหม่ ๆ ได้ทันเวลา จึงทำให้ต้องมีการวางมาตรฐานที่มีความชัดเจนเพื่อใช้เป็นแนวทางในการตอบสนองต่อความเสี่ยง โดยเริ่มจากการทำความเข้าใจและจัดทำเอกสารที่เกี่ยวข้องกับความเสี่ยงต่าง ๆ ความเสี่ยงบางอย่างอาจจะใหญ่หรือเล็กน้อยมากกว่าขอบเขตที่ตั้งไว้ ขอบเขตความเสี่ยงขององค์กรนั้นต้องได้รับการตรวจทานและอนุมัติโดยผู้บริหารระดับคณะกรรมการบริหาร เพื่อให้ตระหนักถึงขอบเขตการบริหารความเสี่ยงที่ตั้งไว้ และสื่อสารขอบเขตนี้ไปยังบุคลากรในองค์กรที่มีความเกี่ยวข้องเป็นการภายใน

สำหรับความเสี่ยงที่มีความสำคัญต่อองค์กรและมีการวางแผนการบริหารความเสี่ยงไว้ก็จะต้องวางแผนสำหรับการติดตามและตรวจสอบขั้นตอนการบริหารความเสี่ยงอย่างสม่ำเสมอ โดยอาจใช้วิธีการเหล่านี้

- การตอบสนองต่อความเสี่ยงในทันที ในบางกรณีอาจมีความเสี่ยงที่เกิดขึ้นในทันทีหรือกำลังจะเกิดขึ้นซึ่งสามารถแก้ไขได้ในทันที เช่น เครื่องจักรเสียหาย
- การสอบทานความเสี่ยงและเสนอวิธีการแก้ไข เพื่อลดโอกาสในการเกิดความเสี่ยงนั้น วิธีนี้จะคล้ายกับการทำงานของผู้ตรวจสอบภายในคือผู้บริหารความเสี่ยงจะประเมินและตรวจทานความเสี่ยงที่สำคัญและนำเสนอวิธีการแก้ไข
- ร่วมกับผู้ตรวจสอบภายในเพื่อประเมินความเสี่ยงในแต่ละหน่วยงาน ในบางเหตุการณ์ความเสี่ยงขององค์กรอาจเกิดจากการควบคุมภายในที่ไม่มีประสิทธิภาพ ดังนั้น จึงอาจให้ฝ่ายตรวจสอบภายในตรวจสอบว่าการควบคุมภายในในหน่วยงานหรือกระบวนการที่มีความเสี่ยงสูงมีประสิทธิภาพเพียงพอหรือไม่

- ติดตามความเสี่ยงอย่างสม่ำเสมอ โดยเฉพาะความเสี่ยงที่เกิดจากปัจจัยภายนอก เช่น ความผันแปรในอัตราแลกเปลี่ยนเงินตราต่างประเทศ
- จัดทำแผนการรับมือสำหรับความเสี่ยงที่อาจเกิดขึ้นได้

ไม่ว่าจะเป็นความเสี่ยงที่ต้องได้รับการแก้ไขทันทีหรือความเสี่ยงที่อยู่ในประเภทความเสี่ยงที่ต้องติดตามอย่างสม่ำเสมอ ประธานฝ่ายบริหารความเสี่ยงจะต้องทำแผนการประเมินความเสี่ยงเป็นรายปี ซึ่งมีรายละเอียดหน้าที่ความรับผิดชอบของแต่ละความเสี่ยง การประมาณการเวลาในการแก้ไขและปรับปรุงความเสี่ยง รวมถึงระยะเวลาและงบประมาณที่จำเป็น โดยรายงานนี้จะต้องได้รับอนุมัติจากผู้บริหารระดับสูงเพื่อพิจารณาความเหมาะสม

ในการประเมินขอบเขตและแผนการประเมินความเสี่ยงเหล่านี้ ประธานฝ่ายบริหารความเสี่ยงและทีมผู้ประเมินความเสี่ยงต้องคำนึงถึงวัตถุประสงค์โดยรวมของ COSO ERM Framework นั่นคือ การประเมินความเสี่ยงของทั้งภาพรวมขององค์กร แล้วจึงนำแผนการตอบสนองนั้นมาใช้กับแต่ละแผนกและแต่ละหน่วยงาน ซึ่งต้องใช้ทั้งการสื่อสาร การร่วมมือและการวางแผนร่วมกันระหว่างแต่ละหน่วยงานอย่างมีประสิทธิภาพ

กลยุทธ์ในการบริหารความเสี่ยง

COSO ERM ได้ทำให้กระบวนการบริหารความเสี่ยงแบบเดิมที่รับมือกับความเสี่ยงแบบรายละความเสี่ยงมาเป็นกระบวนการติดตามความเสี่ยงแบบต่อเนื่องของทั้งองค์กร ซึ่งการบริหารความเสี่ยงจะถูกจัดการและสื่อสารไปยังบุคคลที่มีหน้าที่รับผิดชอบภายในองค์กร ภายใต้การกำกับดูแลของประธานฝ่ายบริหารความเสี่ยง (CRO) ซึ่งจะเป็นผู้ที่กำหนดนโยบายและมาตรฐานในการบริหารความเสี่ยง ส่วนการนำกิจกรรมที่เกี่ยวข้องกับการบริหารความเสี่ยงไปใช้ในกระบวนการของธุรกิจจะเป็นหน้าที่ของหน่วยงานแต่ละหน่วยงาน ผู้มีส่วนได้ส่วนเสียขององค์กรจะต้องตระหนักถึงความเสี่ยง ผลกระทบ และวิธีการรับมือกับความเสี่ยง ซึ่งกระบวนการในการสร้างวัฒนธรรมขององค์กรให้สามารถบริหารความเสี่ยงได้อย่างมีประสิทธิภาพ ดังนี้

- สร้างวัฒนธรรมองค์กรที่ตระหนักถึงความเสี่ยง (Tone At The Top) จากผู้บริหาร ซึ่งจะสร้างความตระหนักเรื่องความเสี่ยงให้แก่บุคคลในองค์กรได้ รวมถึงการจัดทำเอกสารแนวทางเรื่องการตระหนักถึงความเสี่ยงและการสื่อสารสำหรับบุคคลากรในองค์กร เช่น ความเสี่ยงในกระบวนการดำเนินงาน หรือความเสี่ยงจากปัจจัยคุกคามภายนอก สำหรับความเสี่ยงที่เกิดจากปัจจัยภายใน เช่น การนำข้อมูลของลูกค้าไปเปิดเผย องค์กรอาจสร้างความตระหนักโดยการสื่อสารผ่านทางข้อความบนเว็บไซต์ภายในองค์กร จดหมายถึงพนักงาน หรือในการประชุมต่าง ๆ เป็นต้น
- มีหน่วยงานที่ดูแลความเสี่ยงของทั้งองค์กรในภาพรวม นอกเหนือจากประธานฝ่ายบริหารความเสี่ยงที่มีความสามารถแล้ว ยังต้องมีบุคลากรที่จะช่วยทำงานสนับสนุนภายในหน่วยงานบริหารความเสี่ยงอีกด้วย ซึ่งอาจจะเป็นผู้เชี่ยวชาญที่มีความเข้าใจเรื่องความเสี่ยงทางการเงินและบัญชี ความเสี่ยงด้านเทคโนโลยี และความเสี่ยงต่อกระบวนการดำเนินงานขององค์กร นอกจากนี้หน่วยงานบริหารความเสี่ยงจะต้องบริหารงานให้ครอบคลุมการดำเนินงานขององค์กรที่อยู่ในต่างประเทศด้วย สำหรับองค์กรที่มีการทำธุรกิจในต่างประเทศอาจจัดตั้งหน่วยงานบริหารความเสี่ยงย่อยขึ้นมา และทำงานภายใต้การนำของหน่วยงานบริหารความเสี่ยงที่อยู่ที่สำนักงานใหญ่

กระบวนการทางธุรกิจ เทคโนโลยี และการถ่ายโอนความเสี่ยง

ในการสร้างโปรแกรมการบริหารความเสี่ยงที่มีประสิทธิภาพ ผู้บริหารจะต้องมีความเข้าใจความเสี่ยงที่มีผลกระทบโดยตรงต่อองค์กร และสร้างกระบวนการในการ

รับมือกับความเสี่ยงนั้น ซึ่งอาจแบ่งกลุ่มความเสี่ยงได้ตามผลกระทบที่มีต่อองค์กร คือ ความเสี่ยงในการปฏิบัติงานทั่วไปขององค์กร ความเสี่ยงในกระบวนการด้านเทคโนโลยี และความเสี่ยงในกระบวนการถ่ายโอนความเสี่ยง สิ่งที่ต้องคำนึงในการจัดประเภทความเสี่ยงเป็นกลุ่มก็คือระยะเวลาความเสี่ยงบางอย่าง เช่น ความเสี่ยงด้านเทคโนโลยี อาจจะเกิดขึ้นหลังจากมีสัญญาณเตือนแค่ไม่นาน แต่จะต้องมีการตอบสนองอย่างรวดเร็วและทันท่วงที ในขณะที่ความเสี่ยงที่เกี่ยวข้องกับการรายงานทางการเงินอาจจะไม่ต้องตอบสนองในทันที เนื่องจากมีช่วงเวลาสำหรับการแก้ไขก่อนจะถึงเวลาออกงบการเงิน

ประเภทของความเสี่ยงที่สำคัญต่อองค์กรจะมีดังต่อไปนี้ ซึ่งองค์กรอาจนำแนวทางไปปรับเปลี่ยนให้เหมาะกับประเภทของความเสี่ยงที่องค์กรมีอยู่

- ความเสี่ยงด้านการดำเนินงานในธุรกิจทั่วไป อาจมีความเสี่ยงได้หลากหลายด้าน เช่น ความเสี่ยงด้านการเงิน ความเสี่ยงด้านคู่แข่ง และความเสี่ยงในกระบวนการผลิต ซึ่งความเสี่ยงเหล่านี้เป็นสิ่งที่องค์กรมักจะต้องให้ความสำคัญเสมอเนื่องจากมีสำคัญต่อการดำเนินธุรกิจ
- ความเสี่ยงด้านเทคโนโลยี เป็นความเสี่ยงที่ต้องมีการติดตามอยู่ตลอดเวลา และต้องใช้ทักษะทางเทคนิคและเครื่องมือที่เหมาะสมในการตอบสนองความเสี่ยงอย่างหนึ่งที่ต้องให้ความสำคัญคือระบบการติดต่อสื่อสาร เช่น อินเทอร์เน็ต ซึ่งได้กลายมาเป็นเครื่องมือที่ใช้ส่งต่อข้อมูลระหว่างกันภายในองค์กร
- การถ่ายโอนความเสี่ยง เช่น การทำประกันภัยกรณีเกิดอุบัติเหตุ หรือไฟไหม้ ซึ่งเป็นสิ่งที่อาจเกิดขึ้นไม่บ่อย แต่เมื่อเกิดขึ้นจริงจะมีผลเสียหายอย่างมาก องค์กรจึงอาจพิจารณาให้มีการประกันภัยเพื่อป้องกัน หรือในทางการเงินอาจมีการประกันการเสี่ยง (Hedging) ในราคาหลักทรัพย์เพื่อป้องกันการผันผวนของราคา หรือการลงทุนในเครื่องมือทางการเงินอื่น ๆ ที่จะช่วยลดความเสี่ยงจากการผันผวนของราคาหลักทรัพย์ ซึ่งการลงทุนในเครื่องมือทางการเงินจะต้องอยู่ภายใต้การดูแลโดยผู้เชี่ยวชาญ เนื่องจากการตัดสินใจที่ผิดพลาดอาจส่งผลเสียต่อองค์กรในแง่ของค่าใช้จ่ายที่เพิ่มขึ้น
- ความเสี่ยงด้านกฎหมายและข้อบังคับ ประธานฝ่ายบริหารความเสี่ยงและผู้ที่มีหน้าที่ในการบริหารความเสี่ยงจะต้องติดตามการเปลี่ยนแปลงในทางกฎหมายอย่างสม่ำเสมอ ผ่านทางการปรึกษากับผู้เชี่ยวชาญทางกฎหมายหรือแหล่งข้อมูลอื่น ๆ

การตัดสินใจของคณะกรรมการ ผู้บริหารและการบริหารความเสี่ยง

คณะกรรมการผู้บริหารจะมีการประชุมกันเป็นระยะ ซึ่งอาจเกิดขึ้นทุกเดือน เพื่อประเมินและตรวจสอบข้อมูลการดำเนินงานขององค์กร และตัดสินใจเรื่องที่สำคัญ ๆ ทางธุรกิจ ซึ่งจะส่งผลต่อองค์กรทั้งองค์กร เช่น การประกาศจ่ายเงินปันผลแก่ผู้ถือหุ้น ซึ่งในการตัดสินใจแต่ละครั้งก็จะต้องมาจากเสียงส่วนมากของคณะกรรมการผู้บริหาร เนื่องจากคณะกรรมการทำหน้าที่เป็นเสมือนตัวแทนของผู้ถือหุ้นจึงต้องตัดสินใจอย่างระมัดระวังโดยคำนึงถึงประโยชน์ของผู้ถือหุ้นเป็นหลัก

การตัดสินใจของคณะกรรมการผู้บริหารแต่ละครั้ง จะต้องคำนึงถึงการทำความเข้าใจ การประเมินและการยอมรับความเสี่ยงในแต่ละด้านด้วย เนื่องจากคณะกรรมการผู้บริหารเป็นผู้บริหารระดับสูงสุดขององค์กร จึงเป็นที่คาดหวังจากทั้งนักลงทุนและผู้ออกกฎระเบียบ ว่าคณะกรรมการผู้บริหารจะมีความรู้ความเข้าใจในธุรกิจที่ตนเองบริหารงานอยู่ รวมถึงความเสี่ยงที่เกี่ยวข้องกับธุรกิจด้วย หลักการบริหารงานซึ่งประกอบด้วยการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ จึงเข้ามามีบทบาทในการบริหารงานโดยคณะกรรมการผู้บริหารในการเป็นหลักการที่ช่วยให้ผู้บริหารสามารถนำไปใช้ในการบริหารงานได้อย่างมีประสิทธิภาพมากขึ้น

บทบาทของผู้ตรวจสอบภายในในการบริหารความเสี่ยงขององค์กร

ด้วยหน้าที่ในการตรวจสอบการทำงานของหน่วยงานต่าง ๆ ภายในองค์กรและรายงานผลการตรวจสอบไปยังคณะกรรมการตรวจสอบ ผู้ตรวจสอบภายในจึงทำหน้าที่เสมือนหูและตาให้กับผู้บริหาร ซึ่งการทำงานของผู้ตรวจสอบภายในก็เป็นงานที่เกี่ยวข้องกับความเสี่ยง ตั้งแต่ขั้นตอนการวางแผนการตรวจสอบ ผู้ตรวจสอบภายในจะประเมินความเสี่ยงของแต่ละการควบคุมภายใน COSO ERM Framework ทำให้ผู้ตรวจสอบภายในจะต้องคำนึงถึงความเสี่ยงมากขึ้นในการวางแผนการตรวจสอบ เพื่อให้ครอบคลุมความเสี่ยงในการควบคุมภายในของทั้งองค์กร

มาตรฐานการตรวจสอบภายในสำหรับการประเมินความเสี่ยง

มาตรฐานการตรวจสอบภายในเป็นมาตรฐานที่ออกโดยสมาคมผู้ตรวจสอบภายในสากล (The Institute of Internal Auditors: IIA) ซึ่งจะเป็นมาตรฐานการตรวจสอบที่มีปรับปรุงอย่างสม่ำเสมอ เรียกว่า มาตรฐานสากลการปฏิบัติงานวิชาชีพการตรวจสอบภายใน (International Standards for the Professional Practice of Internal Auditing) และผู้ตรวจสอบภายในทุกคนจะปฏิบัติตามมาตรฐานนี้ ซึ่งนอกเหนือจากกระบวนการในการตรวจสอบแล้ว มาตรฐานฯ ยังได้อ้างอิงถึงความรับผิดชอบของผู้ตรวจสอบภายในที่จะต้องนำปัจจัยเรื่องความเสี่ยงไปพิจารณาในการวางแผนและการตรวจสอบภายในด้วย

2010 – การวางแผน
หัวหน้าผู้บริหารงานตรวจสอบต้องจัดทำแผนงานตรวจสอบตามความเสี่ยงเพื่อกำหนดลำดับความสำคัญของกิจกรรมการตรวจสอบภายในให้สอดคล้องกับเป้าหมายขององค์กร

2010.A1 – แผนภารกิจของกิจกรรมการตรวจสอบภายในต้องจัดทำอย่างน้อยปีละครั้งโดยใช้ข้อมูลที่รวบรวมได้จากการประเมินความเสี่ยง และต้องนำข้อมูลข่าวสารจากผู้บริหารระดับสูงและคณะกรรมการมาใช้ประกอบการพิจารณาในการทำแผนด้วย
2010.C1 – ในการพิจารณาให้คำปรึกษา หัวหน้าผู้บริหารงานตรวจสอบต้องพิจารณาถึงโอกาสที่จะก่อให้เกิดการปรับปรุงเกี่ยวกับการบริหารความเสี่ยง การเพิ่มคุณค่า และการปรับปรุงการดำเนินงานขององค์กรและต้องรวมภารกิจที่รับไว้ลงในแผนงานตรวจสอบด้วย

มาตรฐานฯ ได้กำหนดให้ผู้ตรวจสอบภายในจะต้องจัดทำแผนงานตรวจสอบตามความเสี่ยงเพื่อกำหนดลำดับความสำคัญของกิจกรรม และต้องจัดทำอย่างน้อยปีละครั้งโดยใช้ข้อมูลที่รวบรวมได้จากการประเมินความเสี่ยง นอกจากนี้ยังมีส่วนที่เกี่ยวข้องกับความเสี่ยง ซึ่งอยู่ในส่วนของลักษณะของงาน

2100 – ลักษณะของงาน: กิจกรรมการตรวจสอบภายในต้องสามารถประเมินและช่วยสนับสนุนให้มีการปรับปรุงกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุม โดยใช้วิธีการที่เป็นระบบและเป็นระเบียบ
2120 – การบริหารความเสี่ยง: กิจกรรมการตรวจสอบภายในต้องประเมินความมีประสิทธิผลและมีส่วนช่วยในการปรับปรุงกระบวนการบริหารความเสี่ยง
2120.A1 – กิจกรรมการตรวจสอบภายในต้องประเมินความเสี่ยงขององค์กรที่เกี่ยวกับการกำกับดูแล การดำเนินงาน และระบบสารสนเทศขององค์กรในเรื่องต่อไปนี้

- การบรรลุวัตถุประสงค์เชิงกลยุทธ์ขององค์กร
- ความถูกต้อง ครบถ้วน และเชื่อถือได้ของสารสนเทศทางการเงินและ
- สารสนเทศการดำเนินงาน
- ความมีประสิทธิผลและประสิทธิภาพของการดำเนินงานและแผนงาน (Programs)
- การดูแลรักษาทรัพย์สิน และการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ นโยบาย วิธีการปฏิบัติงาน (Procedures) และสัญญา

2120.A2 – กิจกรรมการตรวจสอบภายในต้องประเมินโอกาสของการเกิดทุจริตและวิธีการในการบริหารความเสี่ยงจากการทุจริตในองค์กร

2120.C1 – ระหว่างปฏิบัติภารกิจให้คำปรึกษา ผู้ตรวจสอบภายในต้องระบุความเสี่ยงที่เกี่ยวข้องกับวัตถุประสงค์ของภารกิจและต้องตระหนักถึงการมีอยู่ของความเสี่ยงอื่น ๆ ที่มีนัยสำคัญ

2120.C2 – ผู้ตรวจสอบภายใน ต้องผสมผสานและนำความรู้ในเรื่องของความเสี่ยงที่ได้มาจากการให้บริการให้คำปรึกษาไปใช้ในการประเมินผลของกระบวนการบริหารจัดการความเสี่ยงขององค์กร

จะเห็นว่าจากมาตรฐานการตรวจสอบภายใน ผู้ตรวจสอบภายในจะต้องประเมินความเสี่ยงขององค์กรในด้านต่าง ๆ ซึ่งหลักการบริหารความเสี่ยงก็เป็นเครื่องมือที่มีประสิทธิภาพที่จะช่วยผู้ตรวจสอบภายในวางแผนและทำความเข้าใจความเสี่ยงที่มีผลต่อระบบการควบคุมภายในได้ดียิ่งขึ้น

การนำ COSO ERM มาจัดทำแผนการตรวจสอบรายปี

เช่นเดียวกับที่หน่วยงานในองค์กรจะต้องมีการจัดทำแผนการงบประมาณของแต่ละหน่วยงาน ผู้ตรวจสอบภายในก็ต้องจัดทำแผนการตรวจสอบประจำปี เพื่อรายงานให้แก่คณะกรรมการตรวจและผู้บริหารระดับสูงรับทราบถึงงบประมาณและกิจกรรมที่ผู้ตรวจสอบภายในจะทำในแต่ละปี ในแผนการตรวจสอบผู้ตรวจสอบภายในจะวางแผนการตรวจสอบโดยคำนึงถึงความเสี่ยงในแต่ละกิจกรรม แล้วจึงเลือกตรวจสอบในกิจกรรมที่มีความเสี่ยงสูง อย่างไรก็ตามการประเมินความเสี่ยงของผู้ตรวจสอบภายในยังค่อนข้างเป็นการประเมินที่ไม่มีรูปแบบเป็นทางการ มักประเมินความเสี่ยงตามกลยุทธ์ของผู้บริหารฝ่ายตรวจสอบภายในหรือผู้บริหารระดับสูง

ในการตรวจสอบภายใน ผู้ตรวจสอบภายในจะจัดทำแผนในการตรวจสอบโดยรวบรวมกิจกรรมทั้งหมดในองค์กรที่สามารถทำการตรวจสอบได้ออกมาแล้วจึงมาวิเคราะห์ว่ากิจกรรมใดที่จะต้องทำการตรวจสอบ ซึ่งในแต่ละหน่วยงานก็จะสามารถแบ่งออกเป็นหน่วยงานย่อย ๆ ได้ เช่น แผนกผลิต แผนกบัญชี และแผนกไอที ซึ่งแผนกไอทีก็อาจจะแบ่งออกได้เป็น การจัดการฐานข้อมูล การรักษาความปลอดภัยของระบบ และกิจกรรมทั่วไปของแผนกไอที จากนั้นจึงประเมินความเสี่ยงของแต่ละกิจกรรม โดยพิจารณาปัจจัย เช่น โอกาสในการเกิดความเสี่ยง, ผลกระทบของความเสี่ยง และความจำเป็นในการตรวจสอบ

เทคโนโลยีสารสนเทศและการบริหารความเสี่ยงองค์กร

เนื่องจากความซับซ้อนในโครงสร้างและการดูแลรักษาระบบเทคโนโลยีสารสนเทศในปัจจุบัน ทำให้กระบวนการทางเทคโนโลยีกลายมาเป็นหนึ่งในหัวข้อที่สำคัญในหลักการบริหารความเสี่ยง ซึ่ง COSO ERM Framework ได้กล่าวถึงการบริหารความเสี่ยงที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศในองค์ประกอบเรื่อง “ข้อมูลและการสื่อสาร” แต่ก็เป็นเพียงการพูดถึงอย่างกว้าง ๆ ซึ่งอาจไม่ครอบคลุมถึงประเด็นความเสี่ยงและข้อควรพิจารณาของระบบเทคโนโลยีสารสนเทศที่มีการเปลี่ยนไปอยู่เสมอ ประเด็นเรื่องความเสี่ยงที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ แบ่งออกได้เป็น (1) ความเสี่ยงในการนำระบบเทคโนโลยีสารสนเทศมาใช้ในองค์กร (2) แผนการดำเนินธุรกิจต่อเนื่อง เพื่อป้องกันการล้มเหลวหรือความผิดพลาดของระบบที่ไม่ได้คาดคิด และ (3) ความเสี่ยงจากการเข้าถึงระบบขององค์กร

ระบบเทคโนโลยีสารสนเทศและ COSO ERM Framework

องค์ประกอบด้านข้อมูลและสารสนเทศของ COSO ERM Framework นั้นพูดถึงความเสี่ยงจากระบบเทคโนโลยีสารสนเทศโดยภาพรวม ซึ่งการควบคุมที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศนั้นสามารถแบ่งออกได้เป็น 2 ประเภท คือ การควบคุมภายในทั่วไป (General Controls) และการควบคุมภายในเฉพาะงาน (Application Controls) ซึ่งการควบคุมภายในทั่วไปจะเป็นการควบคุมที่เกี่ยวข้องกับการจัดการระบบสารสนเทศ, โครงสร้างของระบบเทคโนโลยี, การรักษาความปลอดภัย และการได้มา, การบำรุงรักษา และการพัฒนาซอฟต์แวร์ต่าง ๆ ในขณะที่การควบคุมภายในเฉพาะงานจะเป็นการควบคุมที่เกี่ยวข้องกับกระบวนการที่มีความเฉพาะเจาะจง เช่น นโยบายทางด้านเทคโนโลยีที่กำหนดให้การนำระบบเทคโนโลยีใหม่มาใช้จะต้องมีระดับความปลอดภัยและการควบคุมในระดับที่เหมาะสม

บทสรุป

การนำกรอบการบริหารความเสี่ยง ไปใช้ในองค์กรทั้งหมดนั้น เป็นไปตามหลักการของ COSO ซึ่งเป็นแนวทางสำคัญ เพื่อนำไปใช้ในการบริหารความเสี่ยงด้านต่าง ๆ ที่จะมีขึ้นในองค์กร ดังนั้นผู้บริหารและบุคลากรทุกระดับในองค์กรจะต้องมีความเข้าใจและต้องมีการคำนึงถึงเรื่องต่าง ๆ ไม่ว่าจะเป็นความหมายของกรอบการบริหารความเสี่ยง ขั้นตอนการบริหารความเสี่ยง ตลอดจนบทบาทหน้าที่และความรับผิดชอบของหน่วยงานด้านการบริหารความเสี่ยงขององค์กร รวมถึงเรื่องของระบบเทคโนโลยีสารสนเทศ เพื่อที่จะสามารถนำกรอบการบริหารความเสี่ยงไปใช้ในองค์กรของตนได้อย่างมีประสิทธิภาพ และเพื่อที่จะทำให้องค์กรสามารถบรรลุวัตถุประสงค์ได้อย่างเหมาะสม ทั้งนี้ควรมีการทบทวน ERM อย่างสม่ำเสมอ อย่างน้อย 2 ปีต่อ 1 ครั้ง เพื่อให้เกิดประโยชน์ต่อการบริหารความเสี่ยง และให้สอดคล้องกับสภาวะปัจจุบันขององค์กรมากที่สุด

เอกสารอ้างอิง

English

Committee of Sponsoring Organizations of the Treadway Commission. (2013a). *Internal Control - Integrated Framework: Executive Summary*. The United States of America: Committee of Sponsoring Organizations of the Treadway Commission.

Committee of Sponsoring Organizations of the Treadway Commission. (2013b). *Internal Control - Integrated Framework: Framework and Appndices*. The United States of America: Committee of Sponsoring Organizations of the Treadway Commission.

Moeller, Robert R. (2011). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance (GRC) Processes. Second edition*. NJ: Wiley.

Rittenberg, L. E. (2013). *COSO Internal Control - Integrated Framework: Turning Principles into Positive Action*. Altamonte Springs, Florida: The Institute of Internal Auditors Research Foundation.

JAP