มีอะไรใหม่ใน COSO-ERM 2017

สิงหาคม 2020 (เผยแพร่ใน TRIS Academy Club ฉบับ กุมภาพันธ์ 2018) ● Risk Management ●

ดร.สุรเดช จองวรรณศิริ ผู้อำนวยการอาวุโส ทริส คอร์ปอเรชั่น

มีอะไรใหม่ใน COSO-ERM 2017

จากที่ได้นำเสนอถึงกรอบการบริหารความเสี่ยงองค์กร COSO-ERM 2017 ไปในฉบับที่แล้ว ซึ่งถือว่าเป็นการเปลี่ยนแปลงครั้งสำคัญหลังจากเวอร์ชั่นแรกในปี 2004 ใช้มาแล้วกว่า 13 ปี

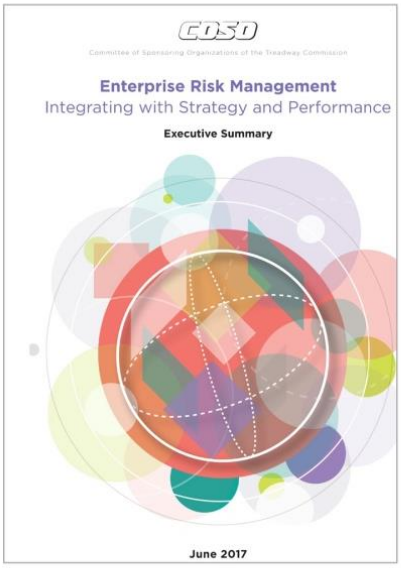
โดยในช่วงระหว่างที่ COSO-ERM 2004 แพร่หลายนั้น ก็ได้มีกรอบแนวทางการบริหารความเสี่ยงอื่นๆ พัฒนาขึ้นมาเป็นทางเลือก หนึ่งในกรอบแนวทางที่ได้รับความนิยมรองจาก COSO-ERM ก็คือ ISO 31000 ที่พัฒนาและเผยแพร่ในปี 2009 โดย ISO หรือ International Organization for Standardization องค์กรที่ทำหน้าที่ในการพัฒนามาตรฐานสากลในด้านต่างๆ ดังเช่นที่เรารู้จักกันดีใน ISO 9000 หรือมาตรฐานด้านการบริหารงานคุณภาพ

สำหรับ ISO 31000 นั้น ไม่ได้เป็นมาตรฐานที่มีการตรวจรับรอง แต่เป็นเพียงแนวทางการพัฒนาระบบการบริหารความเสี่ยงองค์กรที่ดี ซึ่งถือได้ว่าเป็นการสร้างความชัดเจนให้กับผู้บริหาร และผู้รับผิดชอบในการวางกรอบนโยบาย กลไก กระบวนการ รวมทั้งการจัดการสารสนเทศและวัฒนธรรมความเสี่ยงมากขึ้นกว่า COSO-ERM ทั้งนี้อาจเนื่องด้วยการพัฒนาขึ้นมาในภายหลัง

กลับมาว่ากันต่อที่ COSO-ERM ซึ่งเมื่อครั้งที่จะต้องมีการปรับปรุงในปี 2017 นั้น ได้ขยายขอบเขตแนวทางให้ครอบคลุมในลักษณะเดียวกับ ISO 31000 ดังกล่าวข้างต้นนั้นด้วยส่วนหนึ่ง นอกจากนั้น COSO-ERM 2017 ยังมีการเปลี่ยนแปลงอื่นๆ โดยมี 2 ประเด็นที่น่าสนใจ

ประเด็นแรก ในเวอร์ชั่นใหม่นี้ มุ่งชี้ให้เห็นถึงการเชื่อมโยงการทำงานของกลไกการบริหารความเสี่ยงองค์กรเข้ากับกลยุทธ์ และการดำเนินงานขององค์กร ดังสิ่งที่ต่อท้ายชื่อว่า "COSO Enterprise Risk Management-Integrating with Strategy and Performance" รวมทั้งใช้กราฟฟิกแสดงลักษณะของการทำงานคู่ขนานกันระหว่าง "การจัดการเชิงกลยุทธ์" และ "การบริหารความเสี่ยง" ในแต่ละขั้นตอน

ซึ่งทั้งหมดนี้ เป็นการแสดงถึงความสำคัญของการบริหารความเสี่ยงองค์กรกับ "การดำรงอยู่และเติบโต" ขององค์กรตามเป้าหมายกลยุทธ์ ดังนิยามของ ERM ที่กำหนดขึ้นใหม่ว่า "The culture, capabilities and practices integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving and realizing value."



ประเด็นที่สอง การจัดกลุ่มองค์ประกอบของกระบวนการบริหารความเสี่ยงองค์กร ให้มีน้อยลงจากเดิม 8 องค์ประกอบ เหลือเพียง 5 องค์ประกอบ แต่เพิ่มประเด็นหลักการในแต่ละองค์ประกอบให้ชัดเจนมากขึ้นรวม 20 หลักการ ดังนี้

1) Governance and Culture (การกำกับดูแลกิจการและวัฒนธรรมองค์กร) ประกอบด้วย บทบาทของคณะกรรมการ โครงสร้างการดำเนินงานตามเป้าหมายกลยุทธ์ การกำหนดวัฒนธรรมที่พึงประสงค์ การยึดมั่นต่อค่านิยมองค์กร และการสร้างความเข้มแข็งด้านทุนมนุษย์

2) Strategy & Objective Setting (กลยุทธ์และวัตถุประสงค์องค์กร) ประกอบด้วย การวิเคราะห์บริบทของธุรกิจ การกำหนดระดับความสามารถในการรับความเสี่ยง การประเมินทางเลือกของกลยุทธ์จัดการความเสี่ยงองค์กร และการวางเป้าประสงค์ทางธุรกิจภายใต้ความเสี่ยง

3) Performance (เป้าหมายผลการดำเนินงาน) ประกอบด้วย การระบุความเสี่ยง การประเมินระดับความรุนแรง การจัดลำดับความเสี่ยง การตอบสนองความเสี่ยง และการพิจารณาภาพรวมของความเสี่ยงองค์กรทั้งหมด

4) Review & Revision (การทบทวนและปรับปรุง) ประกอบด้วย การประเมินความเปลี่ยนแปลงที่เกิดขึ้นจากการบริหารความเสี่ยง การทบทวนความสามารถในการจัดการและระดับความเสี่ยง และการปรับปรุงพัฒนาระบบการบริหารความเสี่ยงองค์กร

5) Information, Communication & Reporting (สารสนเทศ การสื่อสาร และการรายงาน) ประกอบด้วย การใช้สารสนเทศสนับสนุนการบริหารความเสี่ยง การใช้ช่องทางการสื่อสารต่างๆ สนับสนุนการบริหารความเสี่ยง และการรายงานความสำเร็จ-การดำเนินการ รวมทั้งวัฒนธรรมความเสี่ยงที่เกิดขึ้น

สำหรับเวอร์ชั่นเดิมใน COSO-ERM 2004 ที่มี 8 องค์ประกอบ ได้แก่

1) Internal Environment-สภาพแวดล้อมภายใน **2) Objective Setting**-การกำหนดวัตถุประสงค์ **3) Event Identification**-การระบุเหตุการณ์ที่สร้างกระทบ **4) Risk Assessment**-การประเมินความเสี่ยง **5) Risk Response**-การตอบสนองต่อความเสี่ยง **6) Control Activities**-กิจกรรมควบคุม **7) Information and Communication**-สารสนเทศและการสื่อสาร และ **8) Monitoring**-การติดตามและปรับปรุง

ทั้งนี้เมื่อนำมาเปรียบเทียบกัน จะเห็นถึงประเด็นที่มีการปรับปรุงเพิ่มเติมชัดเจนที่สุดคือเรื่องของ การกำกับดูแลกิจการและวัฒนธรรมองค์กร ซึ่งเป็นองค์ประกอบในเชิงของค่านิยมและพฤติกรรม และเป็นองค์ประกอบพื้นฐานให้กับองค์ประกอบอื่นๆ ที่เหลือ ที่ COSO ได้พิจารณาแล้วว่าเป็นปัจจัยที่มีบทบาทสำคัญต่อการบริหารความเสี่ยงองค์กรในยุคปัจจุบัน โดยเฉพาะในหลักการที่เกี่ยวข้องกับบทบาทของคณะกรรมการที่ว่า "คณะกรรมการจะมีภาระรับผิดชอบและต้องแสดงความรับผิดชอบต่อการกำกับดูแลต่อความเสี่ยงขององค์กร โดยจะต้องมีทักษะ ประสบการณ์ และความรู้ที่เกี่ยวข้องกับธุรกิจ สนับสนุนภาระรับผิดชอบด้านความเสี่ยงดังกล่าว"

นอกจากทั้ง 2 ประเด็นหลักที่นำเสนอมาแล้วนั้น การเปลี่ยนแปลงในเวอร์ชั่น 2017 นี้ ยังมุ่งการนำเสนอกรอบการบริหารความเสี่ยงนี้ว่าเป็น "The Principles-based Approach" ที่ให้ตระหนักว่ากรอบนี้เป็นเพียงแนวทางให้องค์กรต่างๆ สามารถปรับใช้ได้ตามความเหมาะสม ตามความแตกต่างของลักษณะของอุตสาหกรรม กลยุทธ์ โครงสร้างบริหาร วัฒนธรรม ตัวแบบธุรกิจ และสถานะทางการเงินขององค์กร

ทั้งหมดนี้ เราต้องตระหนักเสมอว่า การบริหารความเสี่ยงองค์กร หรือ ERM เป็นการสนับสนุนการสร้าง "คุณค่า" ให้กับองค์กร ผ่านการจัดการภายใต้ความเสี่ยงอย่างเหมาะสม ให้เกิดประสิทธิผลต่อการบรรลุเป้าประสงค์ได้ดีขึ้น และสร้าง "ความตระหนักและค่านิยม" ของบุคลากร ต่อความไม่แน่นอนต่างๆ ที่จะเป็นความเสี่ยงต่อองค์กร รวมทั้งอาจสามารถพลิกเป็น "โอกาส" ให้กับองค์กร เมื่อสภาพแวดล้อมและสภาวะการแข่งขันเอื้ออำนวยได้อีกด้วย

> **"I have learned that nothing is certain except for the need to have strong risk management, a lot of cash, the willingness to invest even when the future is unclear, and great people."**
>
> – Jeffrey R. Immelt, former GE CEO