NEW GUIDANCE under COSO ERM 2017

การบริหารความเสี่ยงที่บูรณาการกับกลยุทธ์และผลประกอบการ

ERM FOR DIGITAL ENTERPRISE

RISK STRATEGY & PLAN

EFFECTIVE APPETITE vs KRIs

คู่มือสำหรับคณะกรรมการ

คู่มือสำหรับงานบริหารความเสี่ยง

คู่มือสำหรับงานบริหารกลยุทธ์

คู่มือสำหรับประเมินตนเอง

อาจารย์ จิรพร สุเมธีประสิทธิ์

NEW GUIDANCE under COSO ERM 2017

การบริหารความเสี่ยงที่บูรณาการกับกลยุทธ์และผลประกอบการ

อาจารย์ จิรพร สุเมธีประสิทธิ์

ข้อมูลทางบรรณานุกรม

อาจารย์ จิรพร สุเมธีประสิทธิ์

NEW GUIDANCE under COSO ERM 2017

การบริหารความเสี่ยงที่บูรณาการกับกลยุทธ์และผลประกอบการ

659 หน้า

ISBN (E-BOOK) 978-616-616-337-7

พิมพ์ครั้งที่ 1 : พ.ศ. 2567

จำหน่ายในรูปแบบ : E-Book

ราคา : 429 บาท

จัดทำโดย : อาจารย์ จิรพร สุเมธีประสิทธิ์

ออกแบบปก : อาจารย์ จิรพร สุเมธีประสิทธิ์

สั่งซื้อได้ที่ :

ศูนย์หนังสือแห่งจุฬาลงกรณ์มหาวิทยาลัย

ถนนพญาไท เขตปทุมวัน กรุงเทพฯ 10330

http://www.chulabook.com

โทร.086-323-3703-4

customer@cubook.chula.ac.th, info@cubook.chula.ac.th

Apps: CU-eBook Store

คำนำ

ตำรา e-BOOK เล่มนี้ จัดทำขึ้นโดยขยายความมาตรฐานการบริหารความเสี่ยง COSO ERM 2017 พร้อมด้วยแนวปฏิบัติที่ดีหรือ GUIDANCE ที่ทยอยออกมาจนถึงปี 2024 ด้วยหวังว่าจะสามารถตอบโจทย์ และตอบสนองความต้องการพัฒนาระบบบริหารความเสี่ยงซึ่งทุกองค์กรจะเริ่มต้นด้วยมาตรฐานฉบับนี้ และเป็นการเชื่อมโยงกับตำรา e-BOOK ที่ออกไปก่อนหน้านี้ ว่าด้วยมาตรฐานการควบคุมภายใน COSO 2013

การที่กิจการเพิ่มความเข้าใจที่ดีทำให้เส้นทางการพัฒนากรอบการดำเนินงานของระบบบริหารความเสี่ยงที่ครอบคลุมตั้งแต่บทบาทคณะกรรมการในฐานะผู้กำกับดูแลผลดำเนินงานด้านความเสี่ยงในองค์รวม และเป็นผู้กำหนดนโยบายบริหารความเสี่ยงทั่วทั้งองค์การตั้งแต่เริ่มแรก ลงมาถึงบทบาทผู้บริหารระดับสูงในการขับเคลื่อนเพื่อให้เกิดกระบวนการบริหารความเสี่ยงและข้อมูลความเสี่ยงสำคัญที่นำมาใช้ประกอบการตัดสินใจและปรับเปลี่ยนกลยุทธ์ได้ทันท่วงที รวมถึงหน่วยงานรับผิดชอบด้านบริหารความเสี่ยง ที่เป็นฟันเฟืองหลักในกลุ่มงาน ASSURANCE PROVIDER ก่อนที่จะถึงขั้นตอนของหน่วยงานตรวจสอบภายใน เพื่อให้มั่นใจว่าองค์กรจะเข้าถึงเส้นชัยโดยเร็วไปถึงมาตรฐานสากลและไม่ได้ทำเพียงบางส่วน และมีองค์ประกอบครบถ้วน เนื่องจากความเข้าใจว่าส่วนใด “ต้องมี” (Must do) “ส่วนใดควรทำ” (Should do) และส่วนใดที่กิจการ “ต้องการมี” (What to do)

ผู้เขียนพยายามใช้ประสบการณ์จริงในงานที่ปรึกษาด้านบริหารความเสี่ยงเกือบ 2 ทศวรรษ มาช่วยอธิบายการพัฒนาระบบบริหารความเสี่ยงที่ดี ซึ่งน่าจะเป็นประโยชน์แก่ผู้นำไปใช้ และยังได้พยายาม

- ⇨ แทรกแบบประเมินที่สามารถนำไปใช้ในการประเมินตนเองของแต่ละองค์กร
- ⇨ แบบฟอร์มที่จะนำไปใช้ประโยชน์และช่วยลดระยะเวลาในการพัฒนาเอกสารหลักฐาน
- ⇨ แบบคำถามคำตอบที่มักจะได้รับการสอบถามจากลูกศิษย์และผู้เข้าอบรมในหลักสูตรที่จัด
- ⇨ เพิ่มเติมเนื้อหาของ GUIDANCE ที่ COSO เห็นว่าจำเป็นต้องแยกการวิเคราะห์ความเสี่ยงออกมาเป็นการเฉพาะเจาะจง
- ⇨ ขยายความ 5 องค์ประกอบ 20 หลักการ ออกมาเป็น 60 ประเด็นย่อย เพื่อให้นำไปใช้เป็นแนวทางในการพัฒนากิจกรรมขึ้นภายในองค์กรรองรับแต่ละหลักการ
- ⇨ เน้นย้ำให้เห็นว่า ความเสี่ยงเป็นความท้าทายขององค์กรที่ไม่อาจหลีกเลี่ยงได้ หากสามารถจัดการได้อย่างเพียงพอและมีประสิทธิผลย่อมกลายเป็นโอกาสและคุณค่าเพิ่มขององค์กร

หวังว่าข้อมูลที่ได้จากการรวบรวมประสบการณ์การทำงาน ทั้งในฐานะที่ปรึกษาและวิทยากรรวมทั้งอาจารย์พิเศษ จะช่วยเป็นแนวทางที่ชัดเจนแก่ผู้นำไปดำเนินการได้ดีขึ้น

อาจารย์ จิรพร สุเมธีประสิทธิ์

ผู้เขียน

สารบัญ

ส่วนของคำถาม - คำตอบที่น่าสนใจ

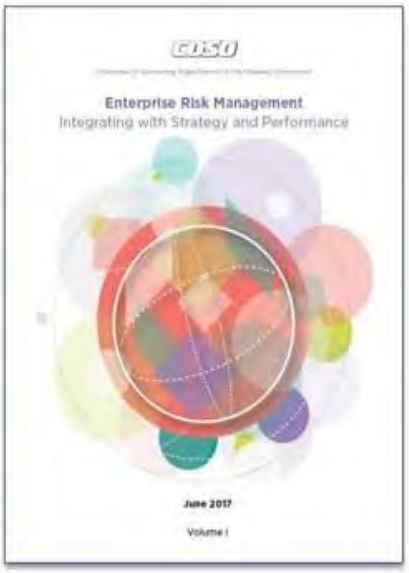
ส่วนของเนื้อหามาตรฐานและ

GUIDANCE

บทนำ

COSO ERM 2017 ถอดบทเรียนมาตรฐาน 2004

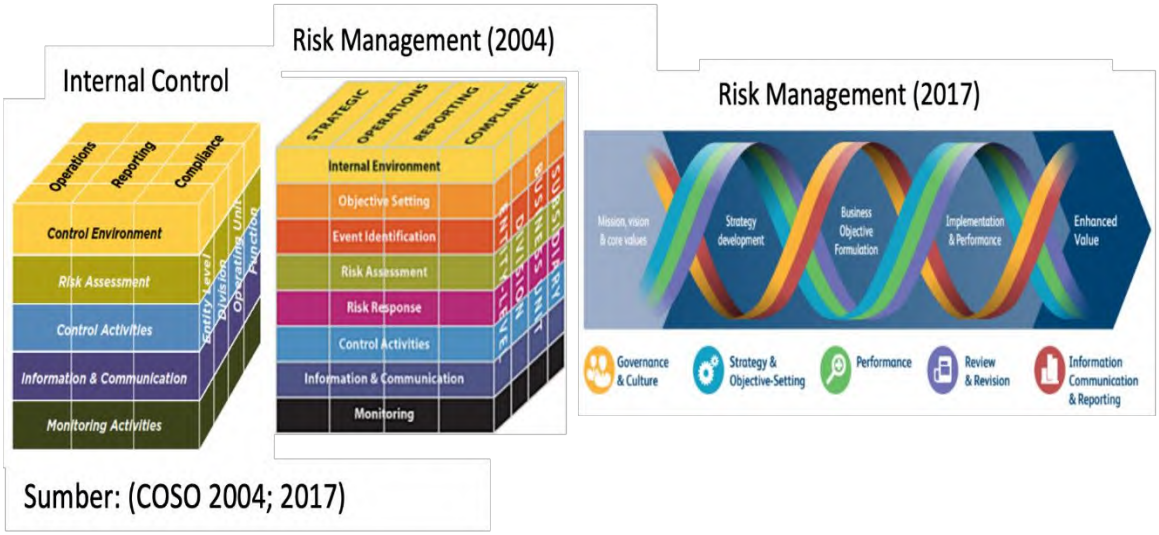
Enterprise Risk Management Framework: Integrating with Strategy and Performance



1. หลักการและเหตุผล

เหตุผลสำคัญส่วนหนึ่งของการที่ COSO มีการเปลี่ยนแปลงมาตรฐานการบริหารความเสี่ยงทั่วทั้งองค์กร จากเวอร์ชั่นของปี 2004 มาเป็นเวอร์ชั่นของปี 2017 มาจากผลการศึกษาทบทวนแนวปฏิบัติและกรอบการดำเนินงานที่เกิดขึ้นจริงกับองค์กรต่างๆ ในการนำมาตรฐานการบริหารความเสี่ยงทั่วทั้งองค์กรไปใช้ ปฏิบัติจริงภายในแต่ละองค์กร

มาตรฐานบริหารความเสี่ยงได้เวอร์ชั่น 2017 จึงพยายามที่จะเปลี่ยนแปลงความเข้าใจผิด การใช้ปฏิบัติที่ผิดพลาดคลาดเคลื่อนของกรอบแนวทางการบริหารความเสี่ยงให้ถูกต้อง จนเกิดเป็นคุณค่าขององค์กรอย่างแท้จริง โดยยกระดับเป้าหมายการบริหารความเสี่ยงขึ้นมาสู่การบูรณาการกับวงจรการบริหารกลยุทธ์และการบริหารผลดำเนินงานระดับองค์กรเพื่อให้เกิดความชัดเจนขึ้นว่าการบริหารความเสี่ยงอยู่ในระดับที่มีความสำคัญเชิงกลยุทธ์ แทนที่จะเป็นมาตรฐานการบริหารความเสี่ยง แบบลอยๆ เช่นเดิม



Sumber: (COSO 2004; 2017)

ประการที่ 1 **งานบริหารความเสี่ยงไม่ใช่งานในลักษณะฟังก์ชั่นประจำ หรืองานปฏิบัติงานระดับฝ่ายงาน**

งานบริหารความเสี่ยงเป็นงาน

- ⇨ การเสริมสร้างวัฒนธรรมการตื่นตัว
- ⇨ การรับมอบหมายในการขับเคลื่อนศักยภาพและสมรรถนะการรับมือความเสี่ยงขององค์กรให้เกิดขึ้นทั่วทั้งองค์กร
- ⇨ การปลูกฝังให้เกิดแนวปฏิบัติทั่วทั้งองค์กรให้กลยุทธ์การบริหารความเสี่ยงบูรณาการและดำเนินการคู่ขนานกับการบริหารกลยุทธ์ผลประกอบการขององค์กร

ประการที่ 2 **งานบริหารความเสี่ยงเป็นงานที่ทำให้เกิดการขับเคลื่อนระบบบริหารความเสี่ยงทั่วทั้งองค์กร จึงเป็นมากกว่าการประสานงาน เพื่อให้หน่วยงานต่างๆ ภายในองค์กรทำการประเมินตนเอง (RCSA : Risk-Control Assessment) และจัดทำทะเบียนความเสี่ยง**

- ⇨ การยกร่างนโยบายการบริหารความเสี่ยงทั่วทั้งองค์กรเพื่อนำเสนอต่อคณะกรรมการให้ความเห็นชอบ
- ⇨ การยกร่างกลยุทธ์บริหารความเสี่ยงระดับองค์กรเพื่อนำเสนอต่อคณะกรรมการให้ความเห็นชอบ
- ⇨ การสื่อสารกลยุทธ์ความเสี่ยงองค์กรกับเกณฑ์ความเสี่ยงที่ยอมรับได้ที่ผ่านความเห็นชอบของคณะกรรมการ

- ⇨ การกำหนดตัวชี้วัดความเสี่ยง เพื่อใช้ในการติดตาม วัดและประเมินผลผลดำเนินงานตามแผนบริหารความเสี่ยงและกลยุทธ์บริหารความเสี่ยง
- ⇨ การประเมินในฐานะกลุ่มงาน 2nd Line เพื่อรับรองและให้ความเชื่อมั่นว่ามีประเด็นความเสี่ยงสำคัญขององค์กรที่อยู่ในเกณฑ์ที่ยอมรับได้ และประเด็นความเสี่ยงสำคัญใด ที่ยังมีการบริหารจัดการไม่เพียงพอ

ประการที่ 3 งานบริหารความเสี่ยงไม่ได้ทับซ้อนกับงานควบคุมภายใน

- ⇨ ระบบควบคุมภายใน เป็นกลไกแรกที่ใช้ในการกำกับความเสี่ยงเพื่อลดลงมาอยู่ในระดับที่ยอมรับได้ โดยเฉพาะในส่วนของปัจจัยความเสี่ยงที่อยู่ในวิสัยที่สามารถควบคุมได้ ภายใต้วัตถุประสงค์การควบคุมที่กำหนดให้ 3 ด้าน ประกอบด้วย
  - (ก) ประสิทธิภาพของการดำเนินงาน
  - (ข) การควบคุมให้ได้มาซึ่งรายงานที่ถูกต้องครบถ้วน และ
  - (ค) การกำกับการปฏิบัติตามกฎเกณฑ์ที่เพียงพอ
- ⇨ การบริหารความเสี่ยงจึงจัดการกับประเด็นความเสี่ยงที่หลงเหลือ โดยเฉพาะปัจจัยความเสี่ยงภายนอกที่อยู่นอกเหนือความสามารถในการควบคุม และความเสี่ยงระดับกลยุทธ์ และผลประกอบการในภาพรวมขององค์กร

ประการที่ 4 งานบริหารความเสี่ยงไม่ใช่การจัดทำแบบตรวจสอบรายการหรือ CHECKLIST ตามประเด็นที่กำหนดให้เท่านั้น แต่ต้องพัฒนาแผนที่ความเสี่ยง และแผนการรับมือและตอบโต้ความเสี่ยงในทุกกลยุทธ์ขององค์กร

- ⇨ แผนบริหารความเสี่ยงจึงเป็นส่วนหนึ่งของข้อเสนอในการขออนุมัติดำเนินแผนงานหรือโครงการขององค์กรตามกลยุทธ์ที่กำหนดให้
- ⇨ ข้อมูลที่ได้จากผลการวิเคราะห์และประเมินความเสี่ยงถือเป็นข้อมูลสำคัญ
  - (ก) ใช้ในการจัดทำแผนบริหารความเสี่ยงใช้รองรับความเสี่ยงระดับองค์กรส่วนที่เกินกว่ายอมรับได้และมีผลกระทบต่อผลดำเนินงานองค์กร และ

(ข) ใช้ประกอบการตัดสินใจระดับนโยบายขององค์กร

⇨ แผนบริหารความเสี่ยงที่ผ่านการพิสูจน์ว่าสามารถใช้ได้ จะพัฒนาไปสู่การเป็น RISK RESPONSE MODEL หรือภูมิปัญญาการจัดการความเสี่ยงที่ถ่ายทอดและส่งต่อกัน

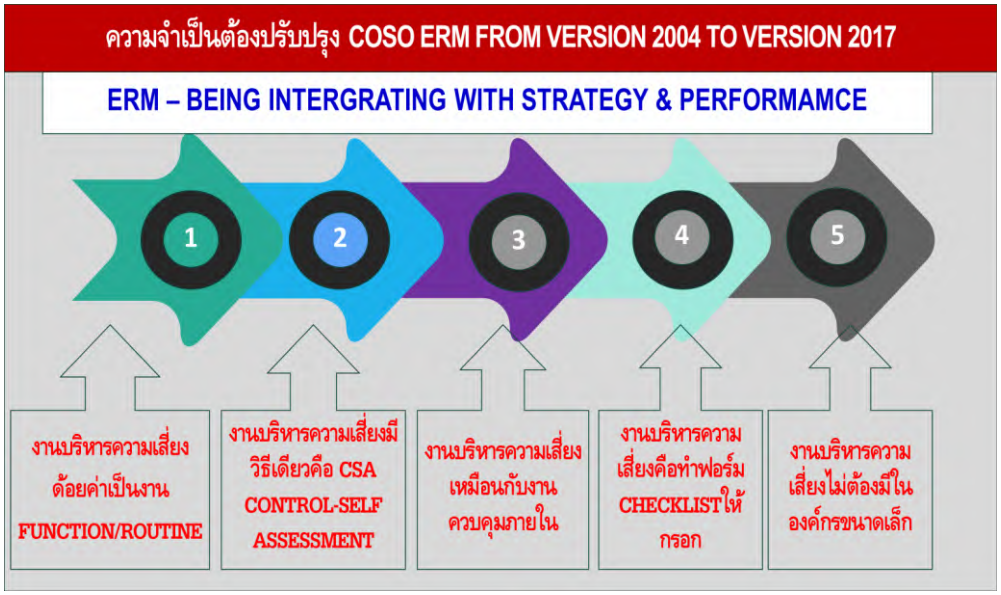
ประการที่ 5 งานบริหารความเสี่ยงไม่เกี่ยวข้องกับขนาดขององค์กร

⇨ แต่ละองค์กรสามารถนำกรอบแนวทางตามมาตรฐานไปประยุกต์ให้เหมาะสมกับบริบท วัฒนธรรม แนวกำกับดูแลองค์กรที่ดีองค์กร

⇨ ผู้บริหารองค์กรทุกระดับจำเป็นต้องทำความเข้าใจความเสี่ยงสำคัญที่มีผลกระทบต่อการดำเนินธุรกิจของตน และใช้เป็นส่วนหนึ่ง ข้อมูลที่ประกอบการบริหารจัดการและตัดสินใจองค์กร

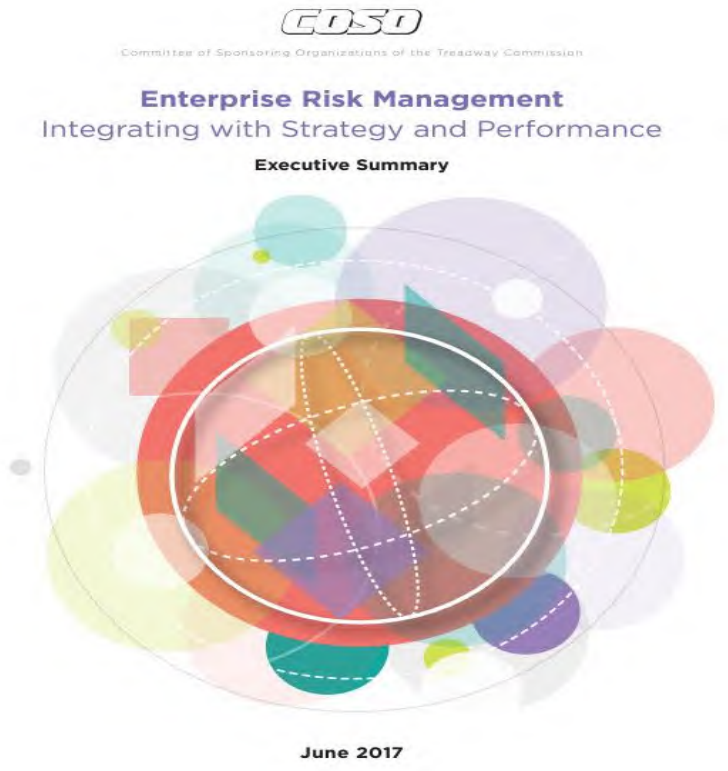
⇨ ความความสามารถในการบริหารจัดการและรับมือต่อความเสี่ยงเป็นเรื่องที่องค์กรทุกระดับต้องมีระบบบริหารจัดการนี้ และพัฒนาให้ดีขึ้นตามลำดับ ทำให้องค์กรมีความยืดหยุ่นในการปรับเปลี่ยนการดำเนินงานและกลยุทธ์จนเปลี่ยนวิกฤติให้เป็นโอกาสในการยกระดับขีดความสามารถในการแข่งขัน

⇨ การจัดการความเสี่ยงที่ดีเป็นส่วนหนึ่งที่จะลดความผันผวน ของผลดำเนินงานองค์กร และเพิ่มเสถียรภาพของการดำเนินงาน



2. แนวคิดการพัฒนามาตรฐาน COSO ERM

มาตรฐานการบริหารความเสี่ยง ทั่วทั้งองค์กร หรือ COSO ERM 2017 จะมิได้เปลี่ยนแปลงตัวเนื้อหาของมาตรฐาน ที่มี 5 องค์ประกอบ และ 20 หลักการ แต่ความเปลี่ยนแปลงที่สำคัญหลังจากปี 2017 เป็นต้นมาคือ การประกาศใช้ GUIDANCE ฉบับใหม่ไหม เพื่อเป็นกรอบแนวทางดำเนินงานในการบริหารจัดการความเสี่ยงองค์กร จนมั่นใจว่ากลไกการบริหารความเสี่ยงเป็นส่วนที่มีความเชื่อมโยงกับกลยุทธ์และผลดำเนินงานระดับองค์กร โดยกรอบแนวทางการดำเนินงานที่เพิ่มเติมเป็นรายเรื่องดังกล่าว



มาตรฐาน COSO ERM 2017 ออกมาใช้เพื่อทดแทนมาตรฐานฉบับเดิมที่ประกาศใช้เมื่อปี 2004 เพื่อให้มั่นใจว่าวงจรการบริหารจัดการความเสี่ยงได้รับความสำคัญในระดับเดียวกับกระบวนการและวงจรการบริหารกลยุทธ์และผลดำเนินงานขององค์กร

- ⇨ *แสดงให้เห็นว่าการบริหารจัดการความเสี่ยงมีคุณค่าต่อองค์กร หากแทรกไว้ในวงจรการบริหารกลยุทธ์ขององค์กร*
- ⇨ *ส่งเสริมให้มีการดำเนินงานที่ยืดหยุ่นและสอดคล้องกันและระหว่างผลดำเนินงานบริหารความเสี่ยงที่ต้องมีส่วนในการปรับปรุงและยกระดับผลดำเนินงานที่เป็นเป้าหมายองค์กร จากการทำความเข้าใจต่อผลกระทบของความเสี่ยงที่มีต่อความสำเร็จของผลดำเนินงานองค์กรและวางมาตรการในการรับมือและตอบโต้ความเสี่ยงอย่างได้ผล*

- *ให้ความสำคัญกับการกำกับดูแลในภาพรวม (Governance & Oversight) และการติดตามผลดำเนินงานที่เกิดจริงไว้ในกระบวนการบริหารจัดการของคณะกรรมการและผู้บริหารระดับสูง*
- *แต่ละองค์กรต้องทำความเข้าใจต่อปัจจัยความเสี่ยงในระดับสภาพแวดล้อมและบริบทการดำเนินงานขององค์กรเพื่อให้ระบบบริหารความเสี่ยงที่ออกแบบกรอบแนวทางการดำเนินงานและนำมาใช้ในการรับมือและตอบโต้ต่อความเสี่ยงสำคัญของแต่ละองค์กรสามารถประยุกต์ให้เหมาะสมกับการดำเนินงานของแต่ละองค์กรได้*
- *ความเสี่ยงที่ควรจะอยู่ในวงจรของการบริหารความเสี่ยงควรมีการปรับเปลี่ยนให้เหมาะสมกับความซับซ้อนของธุรกิจ ซึ่งอาจมีความหลากหลายของรูปแบบการดำเนินงาน โมเดลธุรกิจทั้งในเชิงพาณิชย์หรือเชิงธุรกิจ และในเชิงความรับผิดชอบต่อสังคมและสิ่งแวดล้อม ที่แต่ละองค์กรต้องใช้วงจรการบริหารความเสี่ยงที่เหมาะสมแตกต่างกัน*
- *เพิ่มความสำคัญของการรายงานผลดำเนินงานด้านการบริหารความเสี่ยง นอกเหนือจากการนำเสนอเพื่อประกอบการตัดสินใจเชิงบริหารของผู้บริหาร รับรู้รับทราบและกำกับดูแลในภาพรวมของคณะกรรมการแล้ว ยังมีความสำคัญที่ต้องดำเนินการให้สอดคล้องกับความคาดหมายของผู้มีส่วนได้ส่วนเสียภายนอก โดยยึดหลักความโปร่งใสของการจัดทำรายงาน*
- *ให้ความสำคัญกับการบริหารความเสี่ยง ผ่านการวิเคราะห์ข้อมูลที่ทันท่วงทีและสอดคล้องกับความจำเป็นในการบริหารจัดการและการตัดสินใจเชิงกลยุทธ์ขององค์กร*

3. การเปลี่ยนแปลงสำคัญของภูมิทัศน์ความเสี่ยง

ลักษณะโดยธรรมชาติของความเสี่ยงและรูปแบบของความเสี่ยงขึ้นอยู่กับรูปแบบของเศรษฐกิจ โดยทุกธุรกรรมและกิจกรรมทางเศรษฐกิจ ล้วนแต่มีโอกาสที่จะเกิดความเสี่ยง ตั้งแต่การตัดสินใจในกระบวนงานประจำวัน ไปจนถึงการตัดสินใจเชิงนโยบายในคณะกรรมการบริหาร จนถึงการอนุมัติหรือเห็นชอบเชิงนโยบายของคณะกรรมการอำนวยการ หากสามารถยกระดับการบริหารจัดการความเสี่ยงขึ้นไปอยู่ในระดับเดียวกับการจัดวางกลยุทธ์องค์กร และวัตถุประสงค์ขององค์กรในเชิงธุรกิจได้ การบริหารความเสี่ยง น่าจะมีส่วนช่วยในการทำให้ผลลัพธ์ที่เกิดจากการดำเนินงานอยู่ในตำแหน่งที่เหมาะสมและเกิดประโยชน์สูงสุดต่อองค์กรมากขึ้น

3.1 พัฒนางานบริหารความเสี่ยงที่ไม่ทันอัตราความเปลี่ยนแปลงของโลก

แต่ละกลุ่มก้อนที่ยังคงดำเนินธุรกิจมาอย่างต่อเนื่องจนถึงปัจจุบันได้พัฒนาการรับรู้ ความเข้าใจที่เกี่ยวข้องกับความเสี่ยง และแนวปฏิบัติในการบริหารความเสี่ยงดีขึ้นตามลำดับ เพียงแต่ยังไม่ทันต่อความผันผวน ความไม่แน่นอน และความรุนแรงของความเสี่ยงที่เนื่องมาจากความซับซ้อน การพัฒนาในระดับลักษณะ

ของภาวะสุดขั้วที่ไม่เคยเกิดขึ้นมาก่อน ความเปลี่ยนแปลงในลักษณะที่ยากต่อการคาดเดาล่วงหน้า และสถานการณ์ที่เปลี่ยนแปลงอย่างรวดเร็วเฉียบพลันของสภาพแวดล้อมในตลาดโลก

ด้วยเหตุนี้ องค์กรจึงจำเป็นต้องมีการปรับตัวเรื่องการบริหารจัดการความเสี่ยงให้สอดคล้องกับการเปลี่ยนแปลงที่มีอัตราความที่เพิ่มขึ้น ระดับความรุนแรงและซับซ้อนมากขึ้น โดยงานบริหารความเสี่ยงต้องคิดในมุมมองที่เป็นเชิงกลยุทธ์ (Strategic-Based Thinking) ขณะที่งานบริหารกลยุทธ์ต้องมีแนวคิดด้วยมุมมองที่เป็นฐานความเสี่ยง (Risk-Based Thinking) ซึ่งบุคคลากรที่ทำงานในกระบวนการบริหารความเสี่ยงต้องผ่านการฝึกอบรมให้เรียนรู้ถึงมุมมองเชิงกลยุทธ์และมุมมองที่เป็นฐานความเสี่ยงอย่างเพียงพอ

ด้วยเหตุนี้ มาตรฐาน COSO ERM 2017 จึงพัฒนาขึ้นบนธีม ที่ชัดเจนของ ***Enterprise Risk Management—Integrating with Strategy and Performance*** โดย

- ⇨ การกำหนดกรอบแนวทางดำเนินงานของคณะกรรมการและผู้บริหารระดับสูงไว้ในทุกองค์ประกอบของ 5 องค์ประกอบ พร้อมทั้งจัดทำ GUIDANCE รองรับบทบาทของคณะกรรมการและผู้บริหารระดับสูงแยกต่างหากไว้อย่างชัดเจน ทำให้คณะกรรมการและผู้บริหารต้องอยู่ในวงจรของการบริหารความเสี่ยงด้วย
- ⇨ เชื่อมโยงกลยุทธ์และผลดำเนินงานระดับองค์กรลงไปสู่ผู้รับผิดชอบแผนงานหรือโครงการ ที่รองรับกลยุทธ์ทั่วทั้งองค์กร ให้ต้องคำนึงถึง ค้นหา ระบุ วิเคราะห์ และประเมินความเสี่ยง พร้อมทั้งจัดทำแผนรับมือและตอบโต้ความเสี่ยงในระดับของแผนงานหรือโครงการที่คู่ขนานกับการขออนุมัติโครงการ
- ⇨ ตัวชี้วัดความเสี่ยง (KRIs) ในระดับของแผนงานหรือโครงการเชิงกลยุทธ์ และเกณฑ์ความเสี่ยงที่ยอมรับได้จึงมีโอกาสสูงที่จะมีความเชื่อมโยงกับผลดำเนินงาน (KPIs) ที่เป็นความสำเร็จของแผนงานหรือโครงการเชิงกลยุทธ์ จากการที่แผนบริหารความเสี่ยงเป็นส่วน หนึ่งของแผนบริหารแผนงานหรือโครงการเชิงกลยุทธ์

3.2 ผู้มีส่วนได้ส่วนเสียในวงจรบริหารความเสี่ยง

การบริหารความเสี่ยงไม่ใช่เรื่องของการจัดการในเชิงกลยุทธ์และผลดำเนินงานภายในองค์กรเองหากแต่องค์กรยังมีผู้มีส่วนได้ส่วนเสียที่ร่วมอยู่ในวงจรการบริหารความเสี่ยงเพิ่มเติม โดยเฉพาะ คู่ค้าคู่สัญญา พันธมิตร ผู้ความร่วมมือ ผู้ให้บริการภายนอกในลักษณะเอาท์ซอร์ส ซึ่งถือว่าอยู่ในวงจรของห่วงโซ่อุปทาน ซึ่งต้องเข้ามามีส่วนร่วมพันธะผูกพันในวงจรการบริหารความเสี่ยงขององค์กรด้วย เพื่อให้มั่นใจว่าองค์กรจะสามารถขับเคลื่อนการบริหารความเสี่ยงไปยังผลลัพธ์และกลยุทธ์ที่พึงประสงค์ ตอบรับต่อโอกาสทางธุรกิจที่เปิดกว้างอยู่ได้จริง และเป็นไปอย่างยั่งยืน

ขณะที่ผู้มีส่วนได้ส่วนเสียอีกกลุ่มหนึ่ง ซึ่งได้รับผลกระทบจากผลดำเนินงานและกลยุทธ์ขององค์กรก็ต้องการข้อมูลที่เปิดเผยอย่างโปร่งใสเกี่ยวกับผลดำเนินงานด้านบริหารความเสี่ยงควบคู่กับผลดำเนินงานขององค์กร รายงานทางการเงินและสถานะทางบัญชีขององค์กรด้วย

สถานการณ์ดังกล่าวข้างต้น ทำให้การบริหารความเสี่ยงเป็นเรื่องที่ต้องบริหารความสัมพันธ์กับกลุ่มผู้มีส่วนได้ส่วนเสียภายนอกทุกภาคส่วนที่เกี่ยวข้องอย่างเพียงพอและเป็นระบบ เพื่อให้สามารถสร้างความไว้วางใจและความเชื่อมั่นที่มีต่อการบริหารความเสี่ยงขององค์กรว่าช่วยสนับสนุนความสำเร็จต่อการดำเนินงานตามวัตถุประสงค์ขององค์กร และสะท้อนถึงศักยภาพ ขีดความสามารถ และสมรรถนะขององค์กรในการทนทานและรับมือต่อความเสี่ยงที่มีแนวโน้มรุนแรงขึ้นในอนาคต

3.3 คู่มือบริหารความเสี่ยงทั่วทั้งองค์กรสำหรับผู้บริหารระดับสูง

ผู้บริหารระดับสูงเป็นผู้รับมอบนโยบายและความเห็นชอบกลยุทธ์และผลประกอบการองค์กร ที่ผ่านจากคณะกรรมการอำนวยการ เพื่อลงมาทำการขับเคลื่อนให้เกิดผลดำเนินงานที่เป็นผลสำเร็จจริง

- ⇨ ฝ่ายจัดการหรือผู้บริหารระดับสูงจึงเป็นผู้รับผิดรับชอบต่อผลดำเนินงานในภาคองค์รวมของการบริหารจัดการความเสี่ยงที่เชื่อมโยงกับความสำเร็จของกลยุทธ์และผลดำเนินงานองค์กร
- ⇨ ได้จัดการหรือผู้บริหารระดับสูงต้องหารือ ทำความเข้าใจ ทำความตกลงร่วมกับคณะกรรมการ และทำให้ยอมรับในพันธะผูกพันที่เกี่ยวข้องกับผู้มีส่วนได้ส่วนเสีย ในการนำเอาแนวทางการบริหารจัดการความเสี่ยงทั่วทั้งองค์กร มาออกแบบ จัดวาง และนำไปสู่การใช้งานจริงที่เกิดประสิทธิภาพและประสิทธิผล
- ⇨ มีอำนาจในฐานะที่เป็นผู้บริหารสูงสุดที่มีอำนาจบริหารจัดการบุคลากรทั้งหมดภายในองค์กร และลงนามในข้อตกลงหรือพันธะสัญญาความร่วมมือกับผู้มีส่วนได้ส่วนเสียภายนอกในนามขององค์กร จึงต้อง
  1) รับผิดชอบในการมอบหมายสั่งการบุคลากรภายใน ที่เป็นผู้ใต้บังคับบัญชา และเป็นผู้มีส่วนได้ส่วนเสียภายในองค์กร เพื่อกระจายความรับผิดชอบต่อการบริหารจัดการความเสี่ยงที่ส่งผลต่อความสำเร็จของผลดำเนินงานเชิงกลยุทธ์ โดยเฉพาะผู้รับผิดชอบแผนงานหรือโครงการ และผู้รับผิดชอบกระบวนการหลักที่เกี่ยวข้องกับการสนับสนุนความสำเร็จของกลยุทธ์องค์กร
  2) รับผิดชอบทำความตกลงร่วมกับผู้มีส่วนได้ส่วนเสียภายนอกที่เกี่ยวข้องกับวงจรการบริหารจัดการความเสี่ยง ให้เกิดการยกระดับศักยภาพและสมรรถนะในการจัดการความเสี่ยงที่สัมพันธ์กับความสำเร็จเชิงกลยุทธ์องค์กร

- ผู้บริหารจำเป็นต้องมีความเข้าใจและรับรู้เกี่ยวกับประเด็นความเสี่ยงสำคัญที่มีผลกระทบต่อองค์กรและลักษณะของผลกระทบที่จะเกิดขึ้นในภาพองค์รวม (Portfolio Views of Risk) ต่อความสำเร็จเชิงกลยุทธ์ เพื่อใช้ในการจัดวางกลไกกำกับดูแล การขับเคลื่อนผ่านการชี้นำ สื่อสาร จัดสรรทรัพยากรและงบประมาณที่จำเป็น เห็นชอบในแผนการบริหารความเสี่ยงของแผนงานหรือโครงการ และการมอบหมายสั่งการผู้รับผิดชอบบริหารจัดการความเสี่ยงในระหว่างการดำเนินแผนงานโครงการได้อย่างถูกต้องเหมาะสม
- ผู้บริหารจำเป็นต้องได้รับทราบรายงานความคืบหน้าและผลดำเนินงานด้านบริหารความเสี่ยง ตลอดจนข้อมูลสถานะความเสี่ยง การเปลี่ยนแปลงไปของแผนที่ความเสี่ยงที่สำคัญ
  1) เพื่อใช้ข้อมูลดังกล่าวประกอบการบริหารจัดการ การตัดสินใจ หรือการเปลี่ยนแปลงใดๆในเชิงกลยุทธ์ตามความจำเป็น
  2) เพื่อให้ผู้ที่ได้รับมอบหมายในการบริหารจัดการความเสี่ยง ให้การรับรองและยืนยันถึงความเพียงพอและประสิทธิผลของการกำกับและรับมือต่อความเสี่ยงจนมั่นใจได้ว่าอยู่ในเกณฑ์ที่ยอมรับได้ และไม่เกิดผลกระทบต่อความสำเร็จเชิงกลยุทธ์
  3) เพื่อกำหนดความเชื่อมโยงของผลดำเนินงานด้านบริหารความเสี่ยงกับระบบการประเมินผลการปฏิบัติงานและระบบแรงจูงใจแก่บุคลากร

3.4 คู่มือบริหารความเสี่ยงทั่วทั้งองค์กรสำหรับคณะกรรมการ

- ***คณะกรรมการอำนวยการหรือคณะกรรมการย่อยที่แต่งตั้งโดยคณะกรรมการให้เป็นองค์คณะตามโครงสร้างมีบทบาทหน้าที่ความรับผิดชอบในการกำกับผลดำเนินงานในภาพรวม*** เพื่อช่วยให้การดำเนินงานขององค์กรสามารถสร้างมูลค่าเพิ่ม ควบคู่กับการธำรงรักษาคุณค่าที่ควรจะมีหรือที่มีอยู่แล้วขององค์กร ที่เป็นการรักษาผลประโยชน์ของผู้มีส่วนได้ส่วนเสีย โดยเฉพาะผู้ถือหุ้น และรักษาการดำรงอยู่และความยั่งยืนขององค์กรในระยะยาว
- ***ผลดำเนินงานด้านการบริหารความเสี่ยงจึงต้องแสดงให้เห็นในเชิงประจักษ์*** ว่ามีส่วนในการเสริมสร้าง ยกระดับ และสร้างผลดำเนินงานที่ดีขึ้นและมูลค่าเพิ่มให้แก่องค์กรอย่างไร
- ***คณะกรรมการยังมีบทบาทในการให้การสนับสนุนอย่างต่อเนื่องและสม่ำเสมอ*** เพื่อให้ฝ่ายจัดการหรือผู้บริหารระดับสูงสามารถดำเนินงานขับเคลื่อนการบริหารจัดการความเสี่ยงสู่การบรรลุผลสำเร็จเชิงกลยุทธ์ได้จริง

⇨ ***คณะกรรมการตั้งกำหนดกิจกรรมในการกำกับดูแลผลดำเนินงานในภาพรวมด้านการบริหารความเสี่ยง*** รวมทั้ง

1) การวางกรอบแนวทางการกำกับดูแลด้านการบริหารความเสี่ยง เป็นส่วนหนึ่งของการกำกับดูแลองค์กรที่ดี
2) การปลูกฝังและส่งเสริมวัฒนธรรมสร้างการตื่นตัวต่อความเสี่ยงสำคัญขององค์กร และประเมินผลสำเร็จในเชิงวัฒนธรรมดังกล่าวเพื่อทบทวนและปรับปรุงให้เหมาะสมกับ ประเด็นความเสี่ยงอย่างต่อเนื่องและสม่ำเสมอ
3) การให้ความเห็นชอบนโยบายการบริหารความเสี่ยงทั่วทั้งองค์กร ที่สอดคล้องและบูรณาการกับกลยุทธ์และผลดำเนินงานองค์กรที่กำหนดไว้
4) ทำให้ได้รับข้อมูล รายงาน การสื่อสารที่จำเป็น ด้วยความที่ที่เหมาะสม เพื่อให้รับรู้ รับทราบ และนำข้อมูลดังกล่าวมาประกอบการกำกับดูแลผลดำเนินงานด้านการบริหารความเสี่ยง รวมทั้งทบทวนในเชิงนโยบาย การกำกับดูแล หรือวัฒนธรรมการตื่นตัวต่อความเสี่ยง ที่จำเป็นต้องเปลี่ยนแปลงเพื่อให้เหมาะสมกับกลยุทธ์และผลดำเนินงานองค์การได้อย่างต่อเนื่อง และทันท่วงที

⇨ ***ขอบเขตการดำเนินงานของคณะกรรมการตามวงจรบริหารความเสี่ยง***

1) กำหนดนโยบาย เพื่อให้เกิดกรอบแนวทางการดำเนินงานด้านบริหารความเสี่ยง
   (1) การนำเสนอกลยุทธ์การบริหารความเสี่ยง (Risk Strategy) และเกณฑ์ความเสี่ยงที่ยอมรับได้ ที่สอดคล้องต่อความสำเร็จของกลยุทธ์ ตามพันธกิจและวิสัยทัศน์ ตลอดจนค่านิยมหลักขององค์กร
   (2) การนำเอาเงื่อนไขและข้อกำหนดในนโยบายไปสู่แผนการดำเนินงานและแผนปฏิบัติการเพื่อให้เกิดการขับเคลื่อนจริง ผ่านการให้ความเห็นชอบแผนพัฒนาระบบบริหารความเสี่ยง และแผนบริหารจัดการความเสี่ยง
   (3) ให้ความเห็นชอบผลการทบทวนและปรับปรุงแผนพัฒนาระบบบริหารความเสี่ยงและแผนบริหารจัดการความเสี่ยงที่สอดคล้องกับการเปลี่ยนแปลงในบริบทเชิงกลยุทธ์ขององค์กรหรือสภาพแวดล้อมความเสี่ยง
2) ทบทวนผลดำเนินงานของผู้บริหาร ให้ข้อคิดเห็นและข้อสังเกตที่สร้างความท้าทายและผลักดันให้ผู้บริหารนำเสนอข้อมูลที่เกี่ยวข้อง

4. บทบาทงานบริหารความเสี่ยงช่วงกำหนด-จัดวางกลยุทธ์องค์กร

ที่มา COSO

หลังจากองค์กรสามารถกำหนดพันธกิจ วิสัยทัศน์ และค่านิยมหลักขององค์กรในระยะยาวได้แล้ว สิ่งที่คณะกรรมการและผู้บริหารองค์กรต้องดำเนินการหลังจากนั้น คือการเลือกสรรและจัดวางกลยุทธ์ที่เหมาะสม และสอดคล้องกับการบรรลุตามพันธกิจ วิสัยทัศน์และค่านิยมหลักนั้นๆ

การกำหนดกลยุทธ์ขององค์กรเป็นการเลือกวิธีการที่จะดำเนินงานในเชิงกลยุทธ์ ส่วนที่อยู่นอกเหนือจากกระบวนการดำเนินงานประจำ ซึ่งเป็นที่รับรู้ของผู้ปฏิบัติงานไม่จำเป็นต้องมีวิธีดำเนินงานเพิ่มเติม ในการกำหนดกลยุทธ์องค์กร คณะกรรมการและผู้บริหารต้องใช้ข้อมูลรอบด้านมาประกอบการพิจารณา รวมทั้งข้อมูลประเด็นความเสี่ยงสำคัญที่คาดว่าจะเกิดขึ้น และมีผลกระทบในระดับที่รุนแรงต่อองค์กร

ข้อมูลความเสี่ยงที่ผ่านการค้นหา ระบุ วิเคราะห์ และประเมินความเสี่ยง จนสามารถเรียงลำดับความสำคัญของความเสี่ยง และอธิบายถึงลักษณะและรูปแบบของผลกระทบที่จะเกิดต่อองค์กรได้ จึงเป็นสิ่งที่มีความสำคัญสำหรับนำมาใช้ประกอบการตัดสินใจ การทบทวน เปลี่ยนแปลงหรือปรับปรุงกลยุทธ์ให้เหมาะสมกับสถานการณ์ ข้อมูลความเสี่ยงที่ดี (Informed Risk) สำหรับใช้ประกอบการกำหนดกลยุทธ์องค์กรอาจจัดวางในรูปแบบของ

⇨ **RISK THEME**

ธีมความเสี่ยงที่มาจากสภาพแวดล้อมภายนอกเป็นการจำแนกประเภทของความเสี่ยงสำคัญที่องค์กรควรให้ความใส่ใจ ติดตามและเฝ้าระวัง

ธีมความเสี่ยงขององค์กร ควรแยกออกเป็น 3 ส่วน คือส่วนที่เป็นความเสี่ยงของแนวโน้มในระดับโลก ความเสี่ยงของแนวโน้มปัจจัยในทางลบภายในองค์กรห่วงโซ่อุปทานหรือห่วงโซ่คุณค่าของแต่ละองค์กรเอง และความเสี่ยงต่อความรับผิดชอบใหม่ขององค์กรที่เป็นความรับผิดชอบต่อสังคมและสิ่งแวดล้อม

(ก) GLOBAL RISK THEME

ประเด็นที่นักวิชาการและผู้เชี่ยวชาญมีความเห็นร่วมกันว่าควรอยู่ในระดับที่ต้องระมัดระวัง ซึ่งส่วนใหญ่เป็นเรื่องของภาวะที่เป็นอุบัติการณ์สุดสุดขั้ว ประเด็นความเสี่ยงเกิดใหม่ ที่มีโอกาสเกิดผลกระทบกับหลายพื้นที่หลายภูมิภาคของโลก

(ข) SUPPLY CHAIN / VALUE CHAIN RISK THEME

ประเด็นความเสี่ยงที่เกี่ยวข้องกับองค์กรในห่วงโซ่อุปทานหรือห่วงโซ่คุณค่าของแต่ละองค์กรเอง รวมทั้งผู้ให้บริการเอาท์ซอสที่องค์กรมีระดับการพึ่งพาสูง หากมีความเสี่ยงเกิดขึ้นอาจจะทำให้ยุติการดำเนินงาน หรือการดำเนินงานเกิดการหยุดชะงักเป็นเวลานาน ซึ่งเป็นปัจจัยที่องค์กรไม่สามารถจัดการหรือแก้ไขหรือควบคุมเองได้โดยตรง

(ค) POLICY / POLITICAL RISK THEME

ประเด็นความเสี่ยงที่เกี่ยวข้องกับแนวโน้มเชิงนโยบาย หรือประเด็นการเมือง ทั้งส่วนที่มีการเปลี่ยนแปลงไป มีความไม่แน่นอน คาดเดาล่วงหน้าได้ยาก ที่มีผลกระทบต่อการดำเนินงานขององค์กรในอนาคต

(ง) ESG RESPONSIBILITY RISK THEME

⇨ **ENTERPRISE RISK MAPPING**

ประเด็นความเสี่ยงย่อยในแต่ละกลุ่มที่มีการแยกจำแนกประเภทของความเสี่ยงไว้ หรือประเด็นความเสี่ยงย่อยรายกลยุทธ์หรือร้ายยุทธศาสตร์ พร้อมกับการกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้

⇨ **RISK – CONTROL MATRIX**

ผลที่ได้จากการวิเคราะห์แนวโน้มของความเสี่ยงสำคัญ เปรียบเทียบกับการประเมินคุณภาพการจัดการและรับมือความเสี่ยงในปัจจุบัน และแบ่งแยกประเด็นความเสี่ยงที่อยู่ในระดับคุณภาพการจัดการ (ก) อ่อนหรือ (ข) พอใช้ ในขณะที่ระดับความเสี่ยงมีความรุนแรงของผลกระทบสูง และหรือมีความรุนแรงของผลกระทบและโอกาสเกิดสูงที่เกินกว่ายอมรับได้ ที่เรียกว่า **“RED ZONE”**

RED ZONE จะทำให้เห็นภาพว่าองค์กรจำเป็นต้องมีการรับมือและตอบโต้ความเสี่ยง ที่ใช้ในการประกอบการกำหนดกลยุทธ์องค์กร และกระทบต่อความสำเร็จของผลดำเนินงานระดับองค์กร ในลักษณะที่

(ก) เป็นการลดโอกาสเกิดที่ยอมรับไม่ได้ หรือ

(ข) ลดระดับความรุนแรงของผลกระทบที่ยอมรับไม่ได้ หรือ

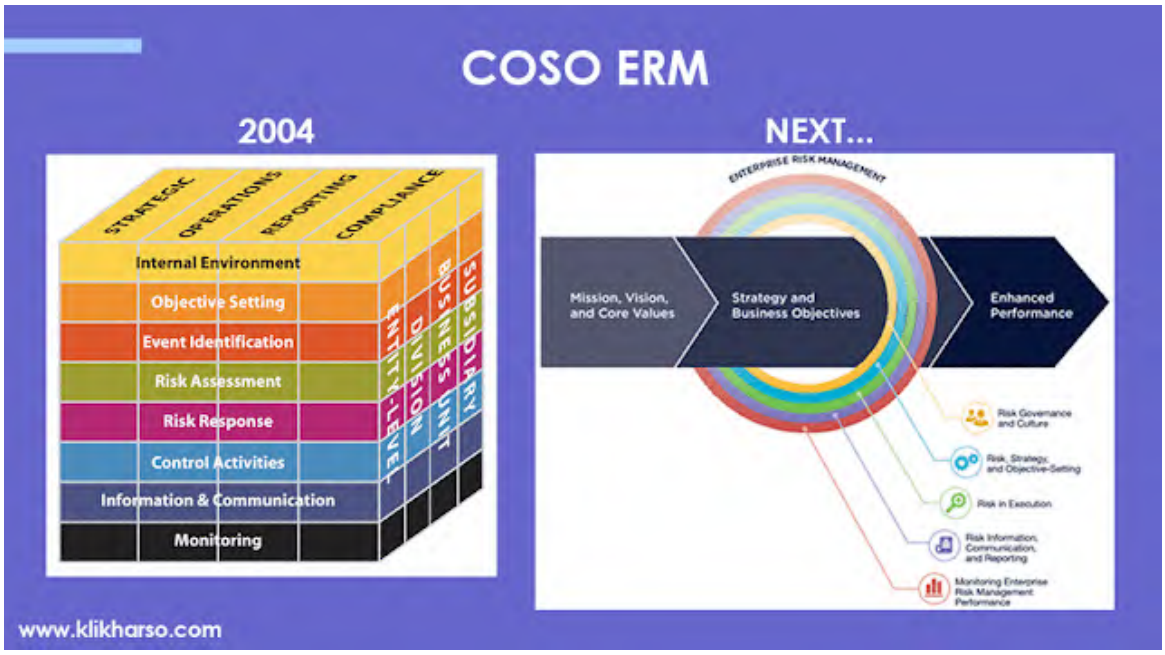
(ค) ลดทั้งสองอย่าง หรือ

(ง) เพิ่มขีดความสามารถและศักยภาพในการทนทานต่อความเสี่ยง หรือความสามารถในการแบกรับความเสี่ยงเพื่อ เป็นโอกาสในการแลกกับผลตอบแทนในอนาคต

เงื่อนไขของการทบทวนและการปรับเปลี่ยนข้อมูลความเสี่ยง

1) เมื่อใดที่คณะกรรมการหรือผู้บริหารมีแนวโน้มของการเปลี่ยนแปลงหรือทบทวนกลยุทธ์ เครื่องมือของข้อมูลความเสี่ยงดังกล่าวข้างต้นทั้ง 4 ส่วน จำเป็นต้องมีการทบทวนเพื่อให้สอดคล้องกับการเปลี่ยนแปลงของกลยุทธ์ด้วย เนื่องจาก ทั้งประเด็นความเสี่ยงที่เกี่ยวข้องและกระบวนการวิเคราะห์ ประเมิน และเรียงลำดับความเสี่ยง ตลอดจนผลกระทบที่จะเกิดขึ้นกับองค์กรย่อมมีการเปลี่ยนแปลงตามไปด้วย
2) เมื่อใดที่สถานการณ์ แหล่งข้อมูลที่นำมาสู่การจัดทำข้อมูลความเสี่ยงระดับ RISK THEME มีการเปลี่ยนแปลง ข้อมูลที่นำส่งเพื่อประกอบการพิจารณาในระดับกลยุทธ์ดังกล่าวต้องเปลี่ยนแปลงไปด้วย

5. แนวทางการจัดการความเสี่ยงสมัยใหม่



การดำเนินงานของแต่ละองค์กรในแนวทางสมัยใหม่

⇨ มีโอกาสที่จะเผชิญหน้ากับความผันผวน ความยุ่งยากซับซ้อน ความไม่แน่นอนอีกมากมาย ทั้งความเสี่ยงที่รับรู้อยู่แล้ว ความเสี่ยงเกิดใหม่ ตลอดจนภาวะการณ์สุดขั้วที่ยังไม่เคยเผชิญหน้ามาก่อน

⇨ สถานการณ์เหล่านี้จะผลักดันให้ระบบบริหารความเสี่ยงขององค์กรมีความสำคัญขึ้น และต้องเข้าไปสนับสนุนในระดับกลยุทธ์และผลดำเนินงานองค์กรอย่างหลีกเลี่ยงไม่ได้

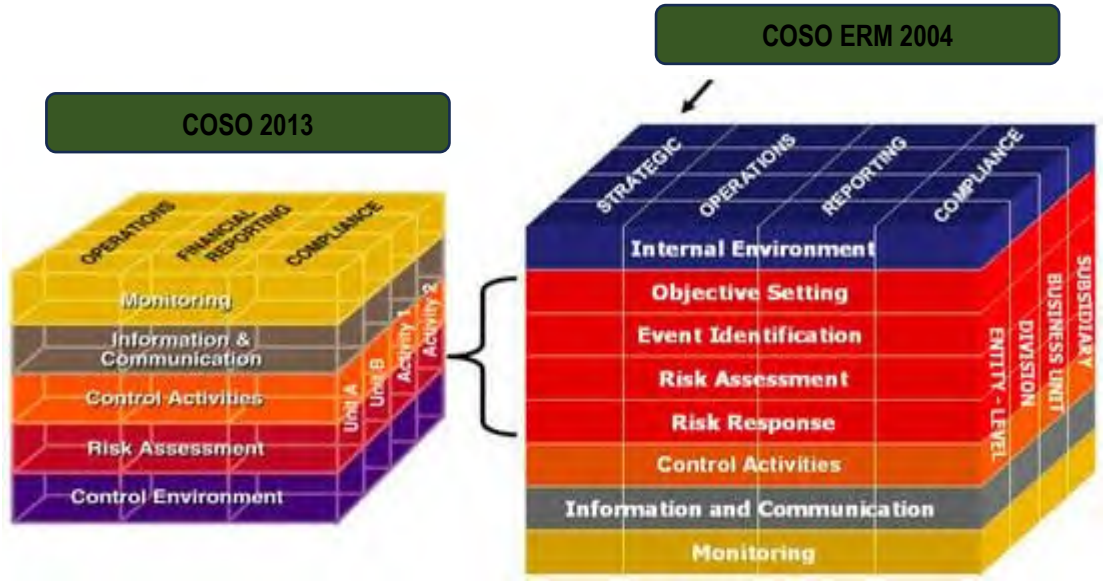
⇨ ไม่ว่าจะเป็นองค์กรขนาดเล็กหรือใหญ่ก็ตาม การบริหารจัดการกลยุทธ์เป็นส่วนที่จะทำให้องค์กรสามารถ ดำรงอยู่ เติบโต และขยายตัวต่อไปได้ในอนาคต และการบริหารความเสี่ยงในระดับกลยุทธ์เป็นสิ่งที่จำเป็นเพื่อให้ผลดำเนินงานบรรลุตามผลสำเร็จที่วางไว้

สรุปการทบทวนและปรับปรุง เพิ่มเติม GUIDANCE ของ COSO

1) COSO in the Cyber Age
2) Practical Approaches to Creating and Protecting Organizational Value
3) Understanding and Communicating Risk Appetite
4) Monitoring Guidance
5) ERM for Cloud Computing
6) Using COSO ERM to Manage Compliance Risks
7) Blockchain and its Impact on Internal Controls
8) ERM in an Agile Environment
9) Assessment Tools for Risk
10) Psychology and Sociology of Fraud
11) Robotic Process Automation and Artificial Intelligence
12) Applying Enterprise Risk Management to Environmental Social and Governance -related Risks

บทที่ 1

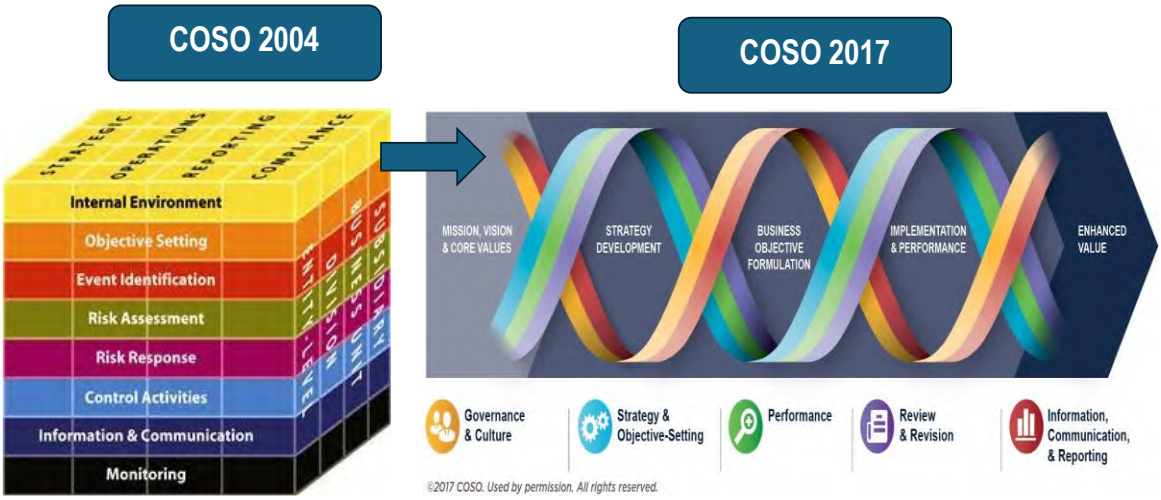
มาตรฐานใหม่ COSO ERM 2017 ทดแทน COSO 2004



1. กลุ่มมาตรฐานของ COSO

องค์กรไม่แสวงหากำไรอย่าง COSO ออกมาตรฐานระหว่างประเทศมาใช้ในองค์กรประเภทต่าง ๆ อย่างน้อย 4 กลุ่ม มาตรฐานหลักได้แก่

กลุ่มที่ 1	*มาตรฐานการควบคุมภายใน (Internal Control)*
กลุ่มที่ 2	*มาตรฐานบริหารความเสี่ยงด้านการทุจริต (Fraud Risk Management Guide)*
กลุ่มที่ 3	*มาตรฐานด้าน COSO's The Three Lines of Defense*
กลุ่มที่ 4	*มาตรฐานบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management: ERM)*
	>> ปี 2004 ออกมาตรฐานสากลชื่อ Enterprise Risk Management-Integrated Framework
	>> 2006 ออกมาตรฐานการบริหารความเสี่ยงสำหรับองค์กรระดับ SMEs
	>> 2017 ประกาศใช้มาตรฐานในชื่อ ERM-Integrating with Strategy and Performance ทดแทนฉบับ 2004



ที่มา COSO

ในส่วนของมาตรฐานการบริหารความเสี่ยงของ COSO การสำรวจชี้ว่ามีความจำเป็นในการปรับปรุงหลักเกณฑ์และเงื่อนไขของการบริหารความเสี่ยง ให้เหมาะสมปับความซับซ้อน ความหลากหลายของความเสี่ยง การเกิดใหม่ของความเสี่ยงตามยุคตามสมัย ทำให้ต้องยกระดับความเข้มข้นและความครอบคลุมในกระบวนการบริหารความเสี่ยงให้เท่าทัน โดยเฉพาะในส่วนของ

1) *Risk Oversight มองภาพความเสี่ยงให้ทั่วและครบถ้วน*
2) *Integrating with strategy บูรณาการการบริหารความเสี่ยงกับการจัดทำกลยุทธ์องค์กร*
3) *Reflect Performance สะท้อนสถานะความเสี่ยงบนความสำเร็จระดับผลประกอบการองค์กร*

2. องค์ประกอบเชิงโครงสร้างของ COSO ERM 2107

COSO ERM 2017 มี 5 องค์ประกอบสำคัญของมาตรฐานที่แยกออกเป็น 2 ส่วน

ส่วนที่ 1 ***การแทรกงานประเมินความเสี่ยง และบริหารความเสี่ยงในระหว่างการกำหนดกลยุทธ์ระดับนโยบายขององค์กรให้เพียงพอ***

ส่วนที่ 2 ***การดำเนินกิจกรรมการบริหารความเสี่ยงที่มีการจัดทำจริง และนำมาใช้ได้จริงในระหว่างการขับเคลื่อนผลการดำเนินงานสู่ผลประกอบการตามเป้าหมาย***

ซึ่งการกำหนดประเด็นในเนื้อหาของ COSO ERM 2017 ประกอบด้วย

ประเด็นที่ 1 ***การกำหนดกรอบแนวคิดหลัก***

ประเด็นที่ 2 ***การจัดวางแอบพิเคชั่นที่จะใช้ในการบริหารความเสี่ยงที่เหมาะสม***

ประเด็นที่ 3 ***กรอบแนวทางปฏิบัติแยกออกเป็น 5 ส่วนเพื่อให้เกิดความเข้าใจง่าย***

สิ่งที่มีการปรับปรุงให้เป็นปัจจุบันและทันสมัยใน COSO 2017 ประกอบด้วย

ประเด็นที่ 1 **ทำให้เกิดความชัดเจนว่าคุณค่าของการบริหารความเสี่ยงว่ามีความสำคัญยิ่งต่อองค์กร** และควรจะเริ่มใช้อย่างเป็นระบบและจริงจัง ตั้งแต่ขั้นตอนในการกำหนดกลยุทธ์ระดับนโยบายขององค์กร ที่เตรียมจัดการความเสี่ยงควบคู่กันไปเลย ให้เป็นการบริหารแบบ Top-Down ไม่ใช่ Bottom-Up

ประเด็นที่ 2 **ส่งเสริมให้มีการวิเคราะห์และประเมินความเสี่ยงแนวใหม่ให้เห็นความสำคัญและสัมพันธ์เชื่อมโยงกันระหว่างผลประกอบที่เกิดจริง** กับความเสี่ยงที่มีผลกระทบต่อการบรรลุผลสำเร็จของค่าเป้าหมายของผลประกอบการ

เมื่อประเมินความเสี่ยงได้แล้ว ก็ควรจะปรับปรุงวิธีกำหนดค่าเป้าหมายด้านความเสี่ยงที่เชื่อมโยงกับผลประกอบการและรับรู้ถึงผลกระทบของความเสี่ยงต่อผลประกอบการด้วย

ประเด็นที่ 3 **การผูกพันการบริหารความเสี่ยงกับความคาดหวังจากภายนอกที่มีต่อองค์กรในด้านของการกำกับดูแลองค์กรที่ดี** ซึ่งเป็นส่วนที่อยู่นอกเหนือผลประกอบการหรือค่าเป้าหมายที่องค์กรได้กำหนดขึ้นเอง

หากองค์กรยังไม่สามารถบรรลุผลความคาดหวังที่มีต่อการกำกับดูแลองค์กรที่ดี ก็ต้องถือว่าองค์กรยังมีสถานะความเสี่ยงเกินกว่ายอมรับได้ แม้ว่าองค์กรจะได้บรรลุค่าเป้าหมายด้านผลประกอบการไปแล้วก็ตาม

ในการพิจารณาความเสี่ยงจึงต้องพิจารณาให้ครอบคลุมและครบถ้วน ทั้งความเสี่ยงที่มีผลกระทบต่อผลประกอบการและที่มีผลกระทบต่อการกำกับดูแลที่ดี ในส่วนของ “Risk Oversight” ความเสี่ยงในภาพองค์รวม

ประเด็นที่ 4 **มองภาพปัจจัยความเสี่ยงในมุมของโลกาภิวัฒน์ ครอบคลุมทุกพื้นที่ ทุกภูมิภาค ความไม่แน่นอนจากสภาพแวดล้อมในระดับโลก ไม่ใช่เพียงปัจจัยเสี่ยงในระดับภายในองค์กรอย่างเดียว**

ประเด็นที่ 5 **พิจารณาแนวทางการจัดการความเสี่ยงในมิติใหม่** ที่นำเอาข้อมูลความเสี่ยงและผลการประเมินความเสี่ยงเป็นข้อมูลที่นำไปใช้ประกอบการตัดสินใจตั้งแต่การวางแผนงานจนถึงการกำหนดเป้าหมายการประกอบการโดยให้สอดคล้องกับความซับซ้อนของการดำเนินงานในปัจจุบันและในอนาคต

ประเด็นที่ 6 **ขยายบทบาทของรายงานการบริหารความเสี่ยงให้รองรับผู้ใช้งานที่เป็นผู้มีส่วนได้ส่วนเสียในภาคส่วนสำคัญหลากหลายกลุ่มมากขึ้น** เพิ่มบทบาทของรายงานการบริหารความเสี่ยงต่อบุคคลภายนอก ที่ต้องเปิดเผยอย่างโปร่งใสน่าเชื่อถือและตรวจสอบได้

ประเด็นที่ 7 **ส่งเสริมและสนับสนุนให้ใช้เทคโนโลยีสมัยใหม่ และเทคนิคการวิเคราะห์และการบริหารข้อมูลความเสี่ยงสำคัญที่มีประสิทธิภาพ** รวดเร็ว ทันท่วงที เพื่อประกอบการตัดสินใจสำคัญได้จริง

ประเด็นที่ 8 **กำหนดนิยาม องค์ประกอบ และหลักการที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงในทุกระดับในองค์กรในประเด็นของ**

(ก) การออกแบบระบบบริหารความเสี่ยง

(ข) การจัดวางระบบบริหารความเสี่ยง ประกาศใช้ และนำมาใช้จริง

(ค) การมีกิจกรรมบริหารความเสี่ยงที่คู่ขนานกับการบริหารจัดการผลดำเนินงานหลัก ที่นำสู่การบรรลุเป้าประสงค์ของผลประกอบการ

ประเด็นที่ 9 **สร้างความเชื่อมโยงและส่งต่อกันระหว่างการบริหารความเสี่ยงและการควบคุมภายใน** ให้เกิดการบริหารจัดการร่วมกันในการจัดการความเสี่ยงสำคัญร่วมกัน โดยไม่เกิดช่องว่างของการบริหารจัดการ

ความเชื่อมโยงดังกล่าวทำให้การจัดการความเสี่ยงเกิดขึ้น ทั้งระดับการปฏิบัติงานในภาระงานประจำวัน จนถึงการตัดสินใจในการจัดการความเสี่ยงในระดับโครงการของผู้บริหารและคณะกรรมการ

ประเด็นที่ 10 **ขยายเป้าหมายการบริหารความเสี่ยง ไม่ให้จำกัดเฉพาะความเสี่ยงในแต่ละปีปฏิทิน หรือแต่ละปีงบประมาณเท่านั้น แต่มองเป้าหมายความยั่งยืนในระยะยาว** ครอบคลุมถึงผลลัพธ์และการรับรู้ผลประโยชน์ที่เกิดจริงกับกลุ่มเป้าหมายสุดท้ายขององค์กร กับระดับความพึงพอใจของผู้ใช้ แทนที่จะเป็นผลประกอบระดับผลผลิตที่ส่งมอบจากองค์กรเท่านั้น แต่ครอบคลุม

ความรับผิดชอบต่อสังคมและสิ่งแวดล้อม ไม่ใช่เพียงผลประกอบการขององค์กรเองเพียงลำพัง

ประเด็นที่ 11 **มาตรฐาน COSO 2017 มีเป้าหมายที่จะให้เกิดการรับรู้และตระหนักในระดับของคณะกรรมการและผู้บริหารระดับสูงขององค์กร** และให้คณะกรรมการและผู้บริหารระดับสูงเป็นเจ้าภาพความเสี่ยงระดับกลยุทธ์เชิงนโยบายและระดับผลประกอบการโดยรวมขององค์กร ตลอดจนความคาดหวังจากผู้มีส่วนได้ส่วนเสียทุกภาคส่วนที่สำคัญ

ซึ่งเป็นการแบ่งระดับการบริหารจัดการที่แตกต่างจาก COSO 2013 ที่เป็นระบบการควบคุมภายใน ที่ผู้บริหารทำหน้าที่กำกับดูแลให้ทุกสายงาน ฝ่ายงาน กระบวนงานทำการวิเคราะห์และประเมินความเสี่ยง เพื่อออกแบบ จัดวาง และเพิ่มเติมกิจกรรมการควบคุมภายในเพื่อแทรกไว้ในระหว่างการปฏิบัติงานในการดำเนินธุรกิจตามปกติ

ประเด็นที่ 12 **การบริหารความเสี่ยงตามกรอบใหม่ของ COSO 2017 มีเป้าหมายที่ใหญ่กว่าการจัดการกับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์การดำเนินงานในระดับกระบวนการหลัก**

COSO 2017 มีเป้าหมายถึงการยกระดับและปรับเพิ่มขีดความสามารถในการแข่งขันทางธุรกิจ (Business Enabler) ในระดับธุรกิจและระดับตลาดโลก ตั้งแต่กระบวนการจัดทำแผนกลยุทธ์เชิงนโยบายและกำหนดค่าเป้าหมายผลประกอบการที่สอดคล้องเหมาะสมกับความเสี่ยงสำคัญ

3 มิติตามองค์ประกอบและหลักการ COSO ERM 2017

ในการบริหารจัดการองค์กรให้ผลดำเนินงานบรรลุผลประกอบการที่กำหนดมีส่วนหนึ่งที่ต้องยึดโยงกับการบริหารจัดการความเสี่ยง ในมิติต่าง ๆ ที่ประกอบด้วย

มิติที่ 1 ***การกำหนดหลักการและกรอบการบริหารความเสี่ยงตามระยะการจัดการกลยุทธ์องค์กรที่แบ่งระยะในการจัดการองค์กรออกเป็น 5 ระยะได้แก่***

ระยะที่ 1 การกำหนดพันธกิจ วิสัยทัศน์และคุณค่าหลักขององค์กร (Mission, Vision, Core, Value)

ระยะที่ 2 การพัฒนากลยุทธ์เชิงนโยบาย

(Strategy Development)

ระยะที่ 3 การจัดวางวัตถุประสงค์เชิงธุรกิจ

(Business Objective Formulation)

ระยะที่ 4 การนำเอากลยุทธ์มาดำเนินงานและขับเคลื่อนไปผลประกอบการ (Implementation & Performance)

ระยะที่ 5 การส่งเสริมสู่มูลค่าและคุณค่าเพิ่ม

(Enhanced Value)

มิติที่ 2 องค์ประกอบการบริหารความเสี่ยงแบ่งเป็น 5 องค์ประกอบได้แก่

องค์ประกอบที่ 1 การสร้างกรอบการกำกับดูแลองค์กรที่ดีและวัฒนธรรมความเสี่ยง (Governance & Culture)

องค์ประกอบที่ 2 การกำหนดกลยุทธ์และกำหนดวัตถุประสงค์ทางธุรกิจที่ใช้ข้อมูลความเสี่ยง (Strategy & Objective Setting)

องค์ประกอบที่ 3 การวิเคราะห์ ประเมินความเสี่ยงและจัดการความเสี่ยงเพื่อบรรลุผลประกอบการ (Performance)

องค์ประกอบที่ 4 การทบทวนและพิจารณาปรับปรุงพัฒนา (Review & Revision)

องค์ประกอบที่ 5 สารสนเทศ การสื่อสาร และการรายงานผล

(Information, Communication & Reporting)

องค์ประกอบ	ประเด็น	คำอธิบาย
1	**สร้างกรอบการกำกับดูแลองค์กรที่ดีและวัฒนธรรมด้านความเสี่ยงให้ชัดเจน** **(Risk) Governance and Culture**	การกำกับดูแลองค์กรที่ดี เป็นการกำหนดกรอบเป้าหมายของการกำกับการบริหารจัดการด้านความเสี่ยงในภาพองค์รวม (Oversight Responsibilities) ว่าต้องเป็นการมอบหมายหน้าที่และความรับผิด

องค์ประกอบ	ประเด็น	คำอธิบาย
		ชอบด้านการบริหารความเสี่ยงแก่คณะกรรมการและผู้บริหารอย่างไร ที่จะทำให้กลไกการบริหารจัดการความเสี่ยงเป็นกลไกสำคัญในระดับองค์กร (High Level) แทนที่จะเป็นระดับบุคลากรผู้ปฏิบัติงาน วัฒนธรรมความเสี่ยงที่พึงประสงค์ ซึ่งเป็นวิธีปฏิบัติ วิถีการคิดที่ต้องค่อย ๆ ปลูกฝัง ทำให้เกิดพฤติกรรมตื่นตัวต่อความเสี่ยงจริงอย่างต่อเนื่อง สม่ำเสมอ จนกลายเป็นความเคยชินของบุคลากรในองค์กร วัฒนธรรมสำคัญได้แก่ 1) คุณค่าของจริยธรรมและจรรยาบรรณที่ดี 2) พฤติกรรมพึงประสงค์ขององค์กร 3) วิธีคิดด้านความเสี่ยง และทำความเข้าใจกับความเสี่ยงอย่างเพียงพอ (Risk – based Thinking)
2	**กำหนดกลยุทธ์และกำหนดวัตถุประสงค์ทางธุรกิจที่ใช้ข้อมูลความเสี่ยงประกอบการพิจารณา** **(Risk-based) Strategy and Objective Setting**	ระหว่างกระบวนการกำหนดกลยุทธ์และระบุวัตถุประสงค์เชิงกลยุทธ์ขององค์กร จะต้องกำหนดแผนบริหารความเสี่ยงที่มีความสำคัญในระดับที่เป็นกลยุทธ์หนึ่งขององค์กรด้วย องค์กรจะต้องกำหนดให้กระบวนการวางแผนเชิงกลยุทธ์มีการกำหนดที่ครอบคลุม 1) แผนกลยุทธ์ที่รองรับโอกาสทางธุรกิจ 2) แผนบริหารความเสี่ยงที่ตอบโต้ภัยคุกคามต่อการบรรลุ

องค์ประกอบ	ประเด็น	คำอธิบาย
		2.1) เป้าหมายผลประกอบการในระดับภาพรวมประจำปี 2.2) การสนองตอบต่อความคาดหวังของกลุ่มผู้มีส่วนได้ส่วนเสีย 2.3) ความยั่งยืนระยะยาว การวางแผนกลยุทธ์จะต้องกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้ (Risk Appetite) ในแต่ละแผนกลยุทธ์ ควบคู่กับวัตถุประสงค์เชิงธุรกิจ เพื่อใช้เป็นกติกาในการค้นหา ระบุ วิเคราะห์และประเมินความเสี่ยง และกำหนดแนวทางการจัดการความเสี่ยงที่เหมาะสม
3	**วิเคราะห์ ประเมินความเสี่ยงและกำหนดแนวทางจัดการความเสี่ยงเพื่อให้มั่นใจว่าจะทำให้ผลประกอบการบรรลุผล (Performance)**	เป็นการวิเคราะห์ ประเมินความเสี่ยงที่มีผลกระทบสำคัญต่อการบรรลุผลสำเร็จของแผนกลยุทธ์และวัตถุประสงค์ทางธุรกิจ โดยผลการเรียงลำดับความเสี่ยงพิจารณาจาก 1) ระดับความรุนแรงของผลกระทบ 2) สถานะความเสี่ยงที่เกินกว่าเกณฑ์ความเสี่ยงที่ยอมรับได้ หลังจากนั้น ก็พิจารณาและเลือกแนวทางการจัดการความเสี่ยงที่เหมาะสม และนำแนวทางการจัดการความเสี่ยงแต่ละประเด็นมาติดตามและประเมินผลดำเนินงานที่เกิดจริงในภาพรวม หรือ Portfolio View of Risk ผลจากการเร่งรัด ติดตาม และประเมินผลดำเนินงานที่เกิดจริงให้จัดทำเป็นรายงานนำเสนอผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

องค์ประกอบ	ประเด็น	คำอธิบาย
4	**ทบทวนและปรับปรุง พัฒนาให้ดีขึ้นและสอดคล้องกับสถานการณ์ความเสี่ยงและความเปลี่ยนแปลง (Review and Revision)**	เป็นการทบทวนผลประกอบการที่เกิดจริงในแต่ละช่วงเวลาของทั้งองค์กร โดยส่วนหนึ่งเป็นการสะท้อนถึงประสิทธิผลที่เกิดจริงของการดำเนินงานตามแนวทางของการจัดการความเสี่ยงที่กำหนดไว้ว่าได้ผลจริงหรือไม่ (functioning) ในแต่ละช่วงเวลา เป็นการระบุความเปลี่ยนแปลง/ความก้าวหน้าที่เกิดขึ้นในแต่ละช่วงเวลาจากการดำเนินกิจกรรมตามแนวทางการจัดการความเสี่ยง (Before and After หรือ Ex-Ante and Ex-Post) นำผลการทบทวนมาพิจารณาว่า ควรจะปรับปรุง แก้ไข เพิ่มเติม แนวทางการจัดการความเสี่ยงใหม่ให้มั่นใจว่าจะเกิดประสิทธิผลที่ดีขึ้นจากแนวทางการจัดการความเสี่ยงเดิมอย่างไร
5	**บริหารสารสนเทศ การสื่อสารและการรายงานผล (Information, Communication and Reporting)**	กระบวนการจัดการความเสี่ยงจำเป็นต้องใช้ข้อมูลสารสนเทศสำคัญที่เป็นปัจจุบันให้รู้เท่าทันสภาพของความเสี่ยง ข้อมูลสานเทศด้านความเสี่ยงและผลประกอบการเป็นข้อมูลที่เกี่ยวข้องกับการดำเนินงานของหน่วยงานและโครงการ ซึ่งต้องรวบรวมให้เป็นฐานข้อมูลกลาง เพื่อแบ่งปัน แลกเปลี่ยน พัฒนาเป็นบทเรียนสู่การตระหนักรู้ เพื่อมิให้เกิดความเสี่ยงซ้ำ ข้อมูลสารสนเทศสนับสนุนการตัดสินใจด้านการจัดการความเสี่ยง ประกอบด้วย

องค์ประกอบ	ประเด็น	คำอธิบาย
		1) แหล่งที่มาของข้อมูลจากภายในองค์กร 2) แหล่งที่มาของข้อมูลจากภายนอกองค์กร 3) การไหลของข้อมูลจากระดับล่างขึ้นระดับบน และไหลจากระดับบนลงล่างหรือการไหลไปมาในการปฏิบัติงานในระดับเดียวกัน

มิติที่ 3

หลักการสำคัญ 20 หลักการใน 5 องค์ประกอบบริหารความเสี่ยง

COSO ERM 2017 ได้แยกแนวพึงปฏิบัติที่ดีทั้ง 5 องค์ประกอบในมิติที่ 2 ข้างต้นออกเป็นหลักการสำคัญเรียงลำดับขั้นตอนการดำเนินการตามลำดับสอดคล้องกับวงจรการบริหารกลยุทธ์ในรอบปีงบประมาณแต่ละปี เพื่อแทรกและบูรณาการให้เป็นเนื้อเดียวกัน เหมือนการมององค์กรแบบเหรียญ 2 ด้านพร้อมกัน ทำให้งานบริหารความเสี่ยงมีความยืดหยุ่น คล่องตัวตามผลดำเนินงานปัจจุบัน ปรับลดระดับความเสี่ยงที่เกินยอมรับได้และเตรียมจัดการความเสี่ยงที่ประเมินว่าจะมีผลกระทบในระยะต่อไปของวงจรบริหารกลยุทธ์ที่จะทำให้องค์กรบรรลุรวม 20 หลักการและกระจายในแต่ละองค์ประกอบ ดังนี้

องค์ประกอบที่ 1	***การกำกับดูแลองค์กรที่ดีและวัฒนธรรมความเสี่ยง***	***5 หลักการ (หลักการที่ 1- 5)***
องค์ประกอบที่ 2	***การกำหนดกลยุทธ์และระบุวัตถุประสงค์ที่มีแผนบริหารความเสี่ยง***	***4 หลักการ (หลักการที่ 6 - 9)***
องค์ประกอบที่ 3	***ผลประกอบการองค์กรที่เกิดจริงกับความเสี่ยงที่มีผลกระทบ***	***5 หลักการ (หลักการที่ 10 - 14)***

องค์ประกอบที่ 4	***การทบทวนและปรับปรุงพัฒนา***	***3 หลักการ (หลักการที่ 15 - 17)***
องค์ประกอบที่ 5	***สารสนเทศ การสื่อสาร และการรายงานผล***	***3 หลักการ (หลักการที่ 18 - 20)***

ทั้งนี้ รายละเอียดในแต่ละหลักการรายองค์ประกอบหลักจะได้กล่าวถึงในบทต่อ ๆ ไป

ในขั้นนี้ องค์กรได้รับรู้แล้วว่าการมีระบบบริหารความเสี่ยงที่ดรตามกรอบ COSO ERM 2017 ต้องการองค์ประกอบ 5 ด้าน 20 หลักการที่เกี่ยวข้องในระดับกลยุทธ์ การกำหนดวัตถุประสงค์ทางธุรกิจ และค่าเป้าหมายผลประกอบการเป็นสำคัญ และการดำเนินการใช้การจัดทำกรอบแนวทาง (Framework) เรียงตามลำดับ

บทที่ 2
หลักการ ความเป็นมา การบริหารความเสี่ยงทั่วทั้งองค์กร (ERM)

การบริหารความเสี่ยงทั่วทั้งองค์กร หรือ Enterprise Risk Management: ERM เป็นคำที่นักบริหารความเสี่ยงเคยได้ยินมาหลายปี อย่างน้อยก็ตั้งแต่ COSO ออกมาตรฐานการบริหารความเสี่ยงครั้งแรกของโลกในปี 2004 แต่นักบริหารส่วนใหญ่หรือนักบริหารความเสี่ยงหน้าใหม่อาจจะยังไม่ได้ใช้ความพยายามในการทำความเข้าใจกับความหมายของคำนี้อย่างจริงจังและอย่างลึกซึ้ง หรือดำเนินกระบวนการไปไม่ถึงก็ได้ ทำให้กรอบแนวทางการบริหารความเสี่ยงยังไม่เกิดประโยชน์สูงสุดต่อองค์กร รวมทั้งยังมีโอกาสที่จะพัฒนาขยายต่อยอดของขอบเขตการบริหารความเสี่ยง ให้เข้าตามนิยามของความเสี่ยงทั่วทั้งองค์กรอย่างแท้จริง

1. ความหมายการบริหารความเสี่ยงทั่วทั้งองค์กรหรือ ERM

การบริหารความเสี่ยงทั่วทั้งองค์กรหรือ ERM หมายถึง กรอบการดำเนินงานที่ครอบคลุมตั้งแต่การกำกับดูแลที่ดีด้านประเด็นความเสี่ยงสำคัญส่วนที่เกินกว่าองค์กรยอมรับได้ การปลูกฝังและส่งเสริมวัฒนธรรม การตื่นตัวต่อความเสี่ยง การยกระดับขีดความสามารถ สมรรถนะ และศักยภาพในการรับมือและตอบโต้ความเสี่ยง รวมถึงเพิ่มความทนทานและการแบกรับความเสี่ยงเพิ่มเติมเพื่อแลกกับผลตอบแทนที่คุ้มค่า และการทบทวนและปรับปรุงแนวปฏิบัติที่องค์กรได้นำมาใช้เพื่อบริหารจัดการกับความเสี่ยง จนนำไปสู่การสร้างมูลค่าเพิ่ม และการธำรงรักษาไว้ซึ่งคุณค่าหรือทำให้เกิดการรับรู้ในคุณค่าซึ่งเป็นผลประกอบการขององค์กร รวมทั้งการสั่งสมเป็นภูมิปัญญาจัดการ ความเสี่ยงขององค์กร

COSO ERM 2017 ได้นิยามเพิ่มเติมว่า การบริหารความเสี่ยงทั่วทั้งองค์กรหรือ ERM จะต้อง

ประการที่ 1 **บูรณาการให้เข้าไปเป็นส่วนหนึ่งของกระบวนการกำหนดกลยุทธ์และเชื่อมโยงถึงผลประกอบการขององค์กร เพื่อนำสู่การบริหารจัดการเชิงกลยุทธ์ร่วมกัน ผ่านกลยุทธ์ความเสี่ยงและกลยุทธ์ทางธุรกิจ**

ประการที่ 2 **ความเสี่ยง (Risk) คือ เหตุการณ์ไม่แน่นอน (Uncertain event) ซึ่งจะมีผลกระทบต่อการที่องค์กรจะบรรลุเป้าหมายกลยุทธ์ทางธุรกิจ หรือมีความเป็นไปได้ที่จะทำให้ผลประกอบการแตกต่างจากค่าเป้าหมาย หรือเป็นโอกาสทางธุรกิจที่องค์กรจะสามารถเพิ่มเติมได้ หากสามารถทนทานและแบกรับความเสี่ยงที่เพิ่มขึ้นได้**

ประการที่ 3 **เป็นการจัดการกับความเสี่ยงที่เกิดขึ้นกับองค์กรเนื่องจาก**

ประการที่ 4 **ความแตกต่างในผลประกอบการจากค่าเป้าหมายที่กำหนดมีความเป็นไปได้ว่าจะเกิดจาก 2 กรณี**

กรณีที่ 1 *Negative Risk ความเสี่ยงทางลบที่ไม่พึงประสงค์*

กรณีที่ 2 *Positive Risk ความเสี่ยงทางบวกที่พึงประสงค์หรือเป็นโอกาสทางธุรกิจที่เปิดให้กับองค์กรที่ทนทานและแบกรับความเสี่ยงเพิ่มเติมได้*

ประการที่ 5 **การบริหารความเสี่ยงมุ่งเน้นองค์ประกอบ (elements) ต่อไปนี้**

องค์ประกอบที่ 1	เป็นส่วนหนึ่งของวัฒนธรรมองค์กร ที่บุคลากรเชื่อและยึดถือปฏิบัติเป็นประจำ
องค์ประกอบที่ 2	เป็นส่วนหนึ่งของการพัฒนาขีดความสามารถขององค์กร ในการพัฒนาและยกระดับทักษะและสมรรถนะหลัก ศักยภาพในการยืดหยุ่นและปรับตัวต่อความเปลี่ยนแปลงต่าง ๆ ได้อย่างเหมาะสม
องค์ประกอบที่ 3	ความสามารถในการแทรกและบูรณาการแนวปฏิบัติด้านบริหารความเสี่ยงกับการดำเนินธุรกิจตามปกติ โดยมีลักษณะเป็นพลวัตรและบูรณาการในภาระงานทุกระดับขององค์กร
องค์ประกอบที่ 4	การบริหารความเสี่ยงสำคัญที่เกี่ยวข้องกับการกำหนดกลยุทธ์และวัตถุประสงค์ขององค์กร
องค์ประกอบที่ 5	การเชื่อมโยงกับคุณค่าหลักผ่านเกณฑ์ความเสี่ยงที่ยอมรับได้ ที่สะท้อนถึงพันธกิจคุณค่าและกลยุทธ์องค์กร เพื่อเปลี่ยนวิกฤติเป็นโอกาส (คุณค่า)

ประการที่ 5 **การกำหนดตำแหน่งใหม่ของการบริหารความเสี่ยง ที่แตกต่างจากมาตรฐาน COSO ERM 2004 ที่เป็นฉบับเดิม อย่างน้อยในประเด็นต่อไปนี้**

ประเด็นที่ 1	ERM ไม่ได้เป็นเพียงการจัดทำทะเบียนความเสี่ยงหรือทำคลังข้อมูลความเสี่ยง แต่ครอบคลุมถึงแนวปฏิบัติที่ดีด้วย
ประเด็นที่ 2	ERM ไม่ได้เหมาะกับองค์กรขนาดใหญ่เท่านั้น แต่จำเป็นในทุกขนาด ทุกประเภทขององค์กร ซึ่งต้องการระบบการบริหารจัดการความเสี่ยงเช่นเดียวกัน

ประเด็นที่ 3 ERM ไม่ใช่การควบคุมภายใน มีบทบาทที่กว้างขวางกว่า อิงกับเกณฑ์ความเสี่ยงที่ยอมรับได้ และยึดโยงกับกลยุทธ์เป็นศูนย์กลาง จึงต้องทำให้สำเร็จจนไม่กระทบต่อเป้าหมายและผลประกอบการ ไม่ใช่เพียง “Bottom-up” แต่เป็นการดำเนินงานแบบ “Top-down”

ประเด็นที่ 4 ERM ไม่ใช่เป็นกิจกรรมเสริมหรือการดำเนินกระบวนการที่แยกออกต่างหากจากการดำเนินงานตามปกติ หากแต่ต้องแทรกเข้าไปเป็นส่วนหนึ่งของกระบวนการดำเนินงานตามปกติ และปรับเปลี่ยนการจัดการความเสี่ยงตามการเปลี่ยนแปลงของกลยุทธ์และวัตถุประสงค์ทางธุรกิจ

ประเด็นที่ 5 ERM ไม่ได้เป็นเพียงการจัดทำรายงานภาคบังคับเพื่อนำส่งแก่หน่วยงานกำกับดูแล แม้ว่า ERM จะเป็นกฎเกณฑ์หนึ่งของหน่วยงานกำกับดูแล แต่ ERM เป็นระบบบริหารจัดการย่อยที่เป็นส่วนหนึ่งของการกำกับดูแลองค์กรที่ดีในทุกองค์กรเอง

ประการที่ 6 การบริหารความเสี่ยงทั่วทั้งองค์กรหรือ ERM ที่เป็นส่วนหนึ่งของคุณค่าหลักขององค์กร เนื่องจาก

ประเด็นที่ 1 มีส่วนในการขยายโอกาสทางธุรกิจ ทำให้องค์กรสามารถฉวยโอกาสทางธุรกิจที่มีอยู่ในปัจจุบันและสามารถท้าทายต่อโอกาสทางธุรกิจใหม่ ๆ

ประเด็นที่ 2 มีบทบาทในการระบุ ค้นหา วิเคราะห์ประเมินความเสี่ยง และกำหนดแนวทางจัดการความเสี่ยงสำคัญในวงกว้างอย่างครอบคลุมและเพียงพอ อย่างเป็นระบบแทนการจัดการแบบ

ต่างคนต่างทำและไม่เพียงพอ ไม่ครอบคลุมและไม่ทั่วถึงทั้งองค์กร

ประเด็นที่ 3 เพิ่มโอกาสที่องค์กรจะบรรลุผลประกอบการที่พึงประสงค์ และลดโอกาสที่จะเกิดผลประกอบการที่ไม่พึงประสงค์ได้ ทำให้องค์กรก้าวสู่องค์กรที่เป็นเลิศ (High Performance) และการกำกับที่เป็นเลิศ(Good Governance)

ประเด็นที่ 4 มีส่วนในการลดความแปรปรวนและเบี่ยงเบนที่จะเกิดกับผลประกอบการ และการจัดการกับค่าความแปรปรวนไม่พึงประสงค์ด้วยการบริหารความเสี่ยงที่มีประสิทธิภาพ

ประเด็นที่ 5 มีผลให้เกิดการจัดสรร ใช้ประโยชน์ในสินทรัพย์และการมอบหมายหน้าที่ความรับผิดชอบของบุคคล เพราะความเสี่ยงต้องการทรัพยากรในการจัดการ

ประการที่ 7 การบริหารความเสี่ยงให้ความสำคัญกับคณะกรรมการในการกำกับดูแลและควบคุมผลดำเนินงานจริงตลอดวงจรการดำเนินงาน

บทบาทและหน้าที่ของคณะกรรมการประกอบด้วย

บทบาทที่ 1 พิจารณา ทำความเข้าใจและเห็นชอบกับกลยุทธ์องค์กรและเกณฑ์ความเสี่ยงที่ยอมรับได้ ในระหว่างที่มีการกำหนดกลยุทธ์และวัตถุประสงค์ทางธุรกิจ

บทบาทที่ 2 พิจารณา และเห็นชอบการเปลี่ยนแปลงกลยุทธ์และวัตถุประสงค์ทางธุรกิจให้สอดคล้องกับพันธกิจ วิสัยทัศน์ และคุณค่าหลักขององค์กร และการจัดสรรทรัพยากรเพื่อจัดทำแผนบริหารความเสี่ยง

บทบาทที่ 3	รับทราบข้อมูลความเสี่ยง สถานะความเสี่ยงในภาพองค์รวม เพื่อประเมินประเด็นที่ยังคงมีผลการบริหารความเสี่ยงที่บกพร่องและยังไม่สามารถสร้างคุณค่าหลักขององค์กร

2. ERM กับการกำหนด SUPPLY-CHAIN RISK STRATEGY

เมื่อทุกองค์กรจำเป็นต้องยอมรับความเสี่ยงในระดับหนึ่ง เพื่อแลกกับผลตอบแทนที่คุ้มค่า หรือการเติบโตและขยายตัวขององค์กร กรอบแนวทางการดำเนินงานด้านบริหารความเสี่ยงทั่วทั้งองค์กร ที่จะพัฒนาในอนาคต ไม่ได้หมายถึงองค์กรหรือนิติบุคคลใดบุคคลหนึ่งในความหมายที่จำกัดหรือวงแคบอีกต่อไป หากแต่มีแนวโน้มที่ความหมายของการบริหารความเสี่ยงทั่วทั้งองค์กรต้องพิจารณาด้วยความหมายอย่างกว้าง

- **กระบวนการดำเนินงานด้านความเสี่ยงต้องครอบคลุมพันธมิตรธุรกิจ** ที่ต้องทำความเข้าใจในบริบทของความร่วมมือระหว่างสองฝ่ายตั้งแต่แรก และเตรียมแผนรับมือต่อความเสี่ยงร่วมกันในส่วนที่มีเป้าหมายและผลดำเนินงานร่วมกัน
- **กระบวนการดำเนินงานด้านความเสี่ยงต้อง ครอบคลุมผู้ให้บริการภายนอก หรือกลุ่มเอาท์ซอร์สที่เป็นผู้ดำเนินกิจกรรมวิกฤต**

ผู้ให้บริการภายนอกทำหน้าที่ ดำเนินการ รับผิดชอบ และส่งมอบผลผลิตแทนการจัดวางโครงสร้างภายในองค์กรเอง จึงถือเป็นเสมือนหน่วยงานที่อยู่ภายนอกสำนักงานปกติ การทำความตกลงเพื่อจัดจ้างเป็นผู้ให้บริการ จึงต้องรวมถึงการบริหารจัดการความเสี่ยงที่เหมาะสมและเพียงพอด้วย

⇨ **กระบวนการดำเนินงานด้านความเสี่ยงต้องแยกกลุ่มกิจการในห่วงโซ่อุปทาน**

กลุ่มกิจการที่ถือเป็น First Tier เป็นซับพลายเออร์หลักที่องค์กรขาดไม่ได้ มีความสัมพันธ์ระหว่างกันในฐานะการจัดจ้างและการรับจ้างในระยะยาว จำเป็นต้องพัฒนาศักยภาพสมรรถนะในการดำเนินงานคู่ขนานกันและทัดเทียมกัน ส่วนหนึ่งของการเสนอโครงการเพื่อรับงาน ไปจนถึงกลไกการร่วมทำแผนบริหารจัดการความเสี่ยง และการตรวจสอบข้ามองค์กรณสถานที่ประกอบการจริง จึงจัดทำอย่างต่อเนื่องอย่างน้อยปีละ 1 ครั้ง

กลุ่มกิจการที่ถือเป็น Second Tier เป็นซับพลายเออร์หลักของซับพลายเออร์ในกลุ่ม First Tier ซึ่งองค์การปล่อยให้ล้มเหลว มีปัญหา หรือหยุดดำเนินงานกะทันหันไม่ได้ กลุ่มซับพลายเออร์หลักของซับพลายเออร์เหล่านี้จึงควรอยู่ในทะเบียนรายชื่อที่องค์กรผู้จัดจ้างต้องรับรู้รับทราบและให้ความเห็นชอบในแผนบริหารความเสี่ยงด้วยตามความจำเป็น

⇨ **กระบวนการดำเนินงานด้านความเสี่ยงต้องทำให้มั่นใจการพัฒนาและเพิ่มพูนสมรรถนะ ศักยภาพ ทักษะ ความเข้าใจและการตื่นตัวต่อความเสี่ยงของบุคลากร**

ทั้งภายในองค์กรเอง รวมทั้งบุคลากรของพันธมิตรทางธุรกิจ และบุคลากรของกลุ่มกิจการในห่วงโซ่อุปทาน เพื่อให้มั่นใจว่าอยู่ในระดับที่เท่าเทียมกัน รวมทั้ง มาตรฐานการบริหารความเสี่ยงที่นำมาใช้ เครื่องมือที่ใช้ในวงจรการบริหารความเสี่ยง หรือรูปแบบการรายงานผลดำเนินงาน สถานะความเสี่ยง แนวโน้มและทิศทางความเสี่ยงในอนาคต

⇨ **กระบวนการดำเนินงานด้านความเสี่ยงต้องคำนึงถึงการแบ่งปัน ถ่ายทอด แจ้งเตือนข้อมูลความเสี่ยงให้ทั่วทั้งองค์กร**

รวมถึง กิจการภายนอกที่อยู่ในห่วงโซ่คุณค่าของการดำเนินงาน เพื่อให้เกิดการตื่นตัว รับรู้รับทราบ ทบทวนและปรับปรุงแผนการบริหารความเสี่ยง ให้สอดคล้องกับการเปลี่ยนแปลงของสถานการณ์ และไปในทิศทางเดียวกัน

3. หลักการสำคัญที่ใช้ในวงจร ERM

เนื่องจากองค์กรสมัยใหม่ยอมรับว่าการบริหารความเสี่ยงทั่วทั้งองค์กรหรือ ERM เป็นส่วนสำคัญต่อความสำเร็จเชิงกลยุทธ์และผลดำเนินงานขององค์การ ที่ต้องเข้ามาพิจารณาตั้งแต่การกำหนดพันธกิจ วิสัยทัศน์ และค่านิยมหลักขององค์กร รวมทั้งเปลี่ยนแปลงและปรับตัวให้ทันต่อการเปลี่ยนแปลงเชิงกลยุทธ์หรือการเปลี่ยนแปลงของสถานการณ์ที่เป็นสภาพแวดล้อมความเสี่ยง องค์กรจึงต้องมีหลักการยึดโยงที่สำคัญเพื่อใช้ในวงจรการบริหารความเสี่ยงทั่วทั้งองค์กร และให้ความเข้มงวด เอาจริงเอาจังต่อการดำเนินการดังกล่าว

เพื่อให้มั่นใจว่าการบริหารความเสี่ยงจะมีผลต่อการสร้างมูลค่าเพิ่มให้แก่องค์กร และทำให้ข้อมูลความเสี่ยงเป็นส่วนหนึ่งของการตัดสินใจ และการเปลี่ยนแปลงใดๆที่จำเป็นไหนเชิงกลยุทธ์องค์กร

1) ผู้ที่เกี่ยวข้องกับวงจรบริหารความเสี่ยงทั่วทั้งองค์กร

- ⇨ ภายในองค์กรเอง ครอบคลุมตั้งแต่คณะกรรมการ ฝ่ายจัดการที่นำโดยผู้บริหารระดับสูงสุด ผู้รับผิดชอบสายงาน หัวหน้างาน ผู้ปฏิบัติงาน ไม่ว่าจะเป็นหน่วยงานในกลุ่มงานได้ภายใต้ THE THREE LINES OF DEFENSE
- ⇨ ภายนอกองค์กร ครอบคลุมกิจการในห่วงโซ่คุณค่า คู่ค้าคู่สัญญา คู่ความร่วมมือพันธมิตรธุรกิจ
- ⇨ ผู้มีส่วนได้ส่วนเสีย ที่มีผลต่อการดำเนินงานและการตัดสินใจขององค์กร

2) หลักการของการยึดโยงกับมาตรฐานสากล (Comply or Explain)

มาตรฐานการบริหารความเสี่ยงทั่วทั้งองค์กรที่ออกประกาศใช้ในระดับสากล ได้กำหนดกรอบแนวทางดำเนินงานสำหรับวงจรการบริหารความเสี่ยงไว้เพื่อให้มั่นใจว่าการบริหารจัดการด้านความเสี่ยงจะเกิดประสิทธิผล

- ⇨ จึงควรกำกับการดำเนินงานที่สอดคล้อง กับข้อกำหนดและเงื่อนไขของมาตรฐานสากล
- ⇨ ยกเว้นองค์กรที่เป็นหน่วยงานภาครัฐ ซึ่งมีข้อกำหนด เงื่อนไขที่เป็นคำสั่งทางปกครองกำหนดให้ต้องดำเนินการเป็นอย่างอื่น เฉพาะประเด็นที่มีความแตกต่างกัน เช่น การบริหารจัดการความเสี่ยงให้เป็นไปตามมาตรา 79 แห่งพระราชบัญญัติวินัยการเงินการคลัง พ.ศ. 2561 เนื่องจากองค์กรรัฐได้ใช้เงินแผ่นดินในการบริหารจัดการ จึงต้องให้ความสำคัญกับการดำเนินงานอย่างมีวินัย
- ⇨ กรณีที่ไม่มีข้อกำหนดหรือเงื่อนไขที่เป็นคำสั่งทางปกครองอื่นใด ที่มีความแตกต่างกัน องค์กรควรดำเนินงานด้านการบริหารความเสี่ยงที่สอดคล้องกับมาตรฐานสากล ยกเว้นในกรณีที่สามารถอธิบายได้ว่าการดำเนินงานที่ทำอยู่มีความซับซ้อน ลึกซึ้ง นำไปสู่ความเพียงพอและประสิทธิผลที่มากกว่าการดำเนินงานที่เป็นเพียงหลักเกณฑ์ขั้นต่ำของมาตรฐานสากล หรือมีเหตุผลความจำเป็นอื่นใดที่ต้องมีความยืดหยุ่น หรือแตกต่างมากกว่า

การยืนยันถึงความสอดคล้องของการดำเนินงานบนหลักการยึดโยงกับมาตรฐานสากลทำได้ด้วยการนำเอา หลักการ และองค์ประกอบของมาตรฐานสากลมาพัฒนาเป็น Checklist สำหรับตรวจสอบรายการ ว่ามีการดำเนินการครบถ้วน เพียงพอ โดยมีเอกสารหลักฐานประกอบอย่างชัดเจน

ประเด็นใดที่มีความแตกต่างกันบนหลักการและเหตุผลที่สมควร ควรจะมีกลไกการเปิดเผย ถึงความแตกต่างดังกล่าวเพื่อให้เกิดการรับรู้รับทราบโดยทั่วกัน

3) การจัดวางโครงสร้าง ที่สนับสนุน อำนวยความสะดวกต่อการบริหารความเสี่ยง (Risk-based Structure)

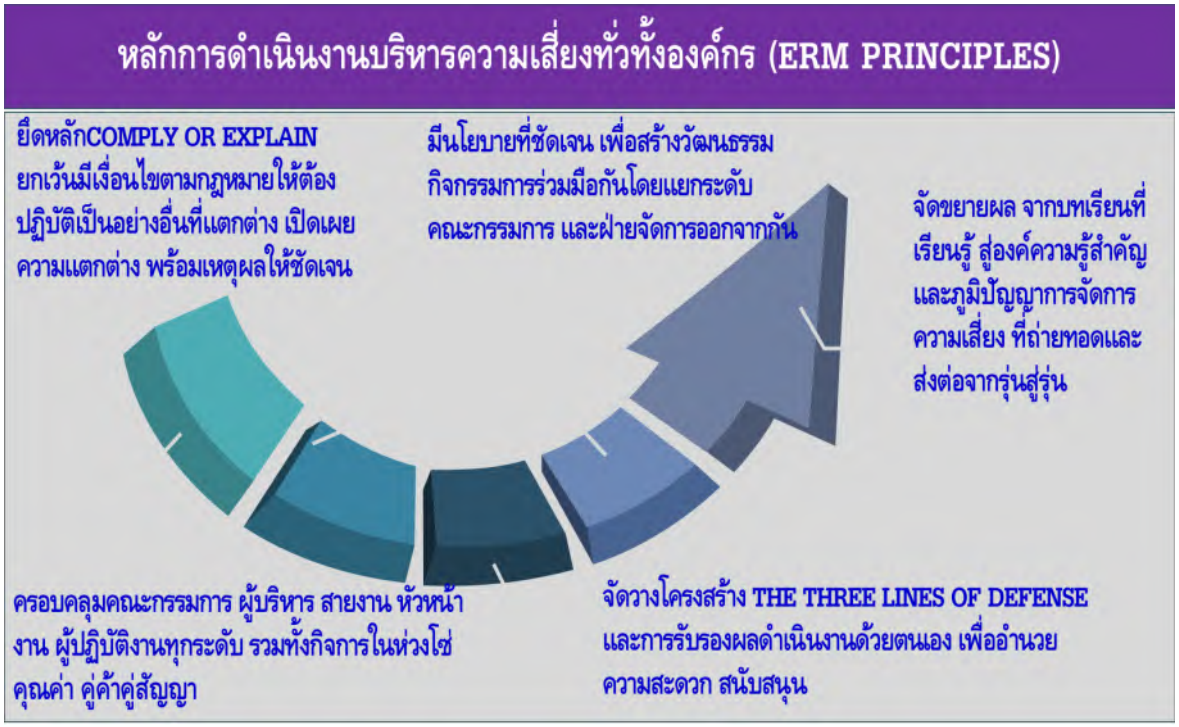
- ⇨ ความชัดเจนของบทบาทหน้าที่ อำนาจกระทำการ ความรับผิดรับชอบต่อผลดำเนินงานด้านบริหารความเสี่ยง มีความสำคัญต่อการสนับสนุน และอำนวยความสะดวกในการบริหารความเสี่ยงทั่วทั้งองค์กร
- ⇨ ทำให้เกิดความเชื่อมโยงระหว่างความรับผิดชอบต่อการบริหารจัดการความเสี่ยงทั้งในส่วนของกลไกการควบคุมภายใน และกลไกการบริหารความเสี่ยงทั่วทั้งองค์กร
- ⇨ เป็นช่องทางที่จะกำจัดวิธีการบริหารจัดการความเสี่ยงแบบ Silo ที่ต่างคนต่างทำ และไม่เชื่อมโยงต่อความเสี่ยงในระดับองค์กร
- ⇨ กำหนดทะเบียนของกระบวนการในการบริหารจัดการความเสี่ยงที่มีลักษณะข้ามสายงาน อยู่บนหลักการของการเชื่อมโยงตั้งแต่กิจกรรมต้นน้ำจนถึงปลายน้ำ หรือรูปแบบของ End-to-End Process เพื่อให้เกิดการบริหารจัดการความเสี่ยงที่มีความสัมพันธ์เกี่ยวข้องกัน หรือจำเป็นต้องบริหารจัดการพร้อมกัน จึงจะทำให้ลดลงมาอยู่ในเกณฑ์ความเสี่ยงที่ยอมรับได้
- ⇨ เชื่อมโยงตัวชี้วัดผลดำเนินงานด้านการบริหารความเสี่ยง กับตัวชี้วัดผลดำเนินงาน ตามกลยุทธ์และผลประกอบการองค์กรให้ชัดเจน
- ⇨ กำหนดระบบการประเมินผลดำเนินงานและระบบแรงจูงใจที่เกี่ยวข้องกับการบริหารความเสี่ยงในลักษณะที่แยกออกจากผลดำเนินงานตามภาระงานประจำ

4) กลไกการกำกับการดำเนินงานด้านบริหารความเสี่ยงผ่านการชี้นำ นโยบาย การสร้างวัฒนธรรม และมอบหมายกิจกรรมที่ร่วมมือกัน

- ⇨ กรอบการดำเนินงานและการขับเคลื่อนต้องอาศัยการชี้นำ การมอบหมายสั่งการ และการติดตามผลในสิ่งที่ได้มอบหมายไปโดยคณะกรรมการและผู้บริหารระดับสูง เพื่อให้มั่นใจว่ามีการดำเนินการไปในทิศทางเดียวกันทั้งองค์กร
- ⇨ วัฒนธรรมที่มีการตื่นตัวต่อความเสี่ยงและบูรณาการกับกิจกรรมการดำเนินงานตามปกติ ไปจนถึงการตัดสินใจเชิงนโยบายต้องดำเนินการอย่างต่อเนื่องสม่ำเสมอ
- ⇨ ผู้ที่เกี่ยวข้องภายในองค์กรทุกระดับที่ต้องเป็นหูเป็นตา ต้องเป็นผู้ที่มีความรู้ความเข้าใจในเรื่องการบริหารความเสี่ยงและบริบทการดำเนินงานที่เกี่ยวข้อง จนสามารถนำส่งข้อมูลความเสี่ยงสำคัญได้อย่างเหมาะสม

5) กลไกทบทวน สอบทาน ทดสอบ ถอดบทเรียน เพื่อนำไปสู่เส้นทางแห่งการเรียนรู้ และองค์กรแห่งการเรียนรู้

- ⇨ องค์กรมีความสามารถในการรับมือและตอบโต้ต่อความเสี่ยงได้ดีขึ้น โดยผ่านกระบวนการทบทวน สอบทาน ทดสอบ ถอดบทเรียน เพื่อนำไปสู่เส้นทางแห่งการเรียนรู้
- ⇨ การเรียนรู้ที่สั่งสมและผ่านการทดสอบแล้วว่าได้ผล ควรพัฒนาต่อยอดไปสู่การเป็นองค์ความรู้ที่สำคัญ เพื่อส่งต่อ ถ่ายทอด และสร้างการเรียนรู้จากรุ่นสู่รุ่น
- ⇨ แผนการรับมือตอบโต้ความเสี่ยงที่ใช้ได้ผลดี ถือเป็นภูมิปัญญาการจัดการความเสี่ยงขององค์กร ที่ต้องธำรงรักษาไว้และพัฒนาปรับปรุงให้ดีขึ้นตามลำดับ



4. ข้อจำกัดการบริหารความเสี่ยง Silo ที่ไม่เกิดประสิทธิผลสูงสุด

แม้ว่าการมอบหมายให้ผู้รับผิดชอบแต่ละสายงานกำกับดูแลการบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับภาระงานของตนแบบ Silo จะมีความสมเหตุสมผลแต่ก่อให้เกิดข้อจำกัด เพราะทำให้การบริหารจัดการความเสี่ยงไม่เชื่อมโยงในแ/นวนอน (Horizon) แต่เป็นการบริหารจัดการความเสี่ยงภายในสายงานเองหรือในแนวดิ่ง (Vertical) ซึ่งส่งผลเสียต่อองค์กรคือ

- ⇨ อาจทำให้ประเด็นความเสี่ยงสำคัญบางเรื่องตกหล่นไป เนื่องจากไม่อยู่ในความรับผิดชอบของผู้บริหารสายงานทุกสาย จึงไม่ได้ให้ความสำคัญ หรือเฝ้าระวัง หรือยกขึ้นมาเป็นแฟ้มข้อมูลความเสี่ยงที่ต้องบริหารจัดการซึ่งเป็นเรื่องที่มีโอกาสเกิดขึ้นในทุกสายงาน

- ⇨ ทำให้ประเด็นความเสี่ยงสำคัญมากซึ่งมีผลกระทบต่อความสำเร็จการดำเนินงานของสายงานรับผิดชอบหลายสายงานแต่อาจจะในลักษณะที่แตกต่างกัน ระดับความเสี่ยงที่แต่ละสายงานมองเห็นที่จำกัดอยู่แต่เฉพาะขอบเขตภาระงานของตนจึงน้อยกว่าหรือต่ำกว่าระดับความรุนแรงจริงโดยรวมของความเสี่ยงนั้น เมื่อรวมเอาทุกสายงานมาพิจารณาพร้อมกัน
- ⇨ การที่แต่ละสายงานกำหนดแผนการรับมือและตอบโต้ความเสี่ยงเฉพาะในส่วนของตนขึ้นโดยมิได้พิจารณาว่าการดำเนินการดังกล่าวมีผลอย่างไรต่อสายงาน อาจจะทำให้ วิธีการในการรับมือและตอบโต้ความเสี่ยงมีลักษณะที่ย้อนแย้งกัน สวนทางกัน แตกต่างกัน และขาดการบูรณาการเพื่อผนึกพลังในการจัดการความเสี่ยง และอาจทำให้การดำเนินงานเพียงส่วนใดส่วน หนึ่ง ที่แยกจากกันไม่ได้ผลต่อการจัดการความเสี่ยงในองค์รวม
- ⇨ มุมมองต่อความเสี่ยงของแต่ละสายงานอาจเน้นเฉพาะ ปัจจัยเสี่ยงจากภายใน ตอบโต้ความเสี่ยงด้วยการควบคุมภายใน เน้นการลดระดับความเสี่ยงลงมาอยู่ในเกณฑ์ที่ยอมรับได้สถานะที่คุ้นเคยของแต่ละสายงาน แต่ไม่ครอบคลุมความเสี่ยงที่เกิดจากปัจจัยภายนอก และอยู่นอกเหนือการควบคุมขององค์กร ซึ่งต้องใช้กลไกการบริหารความเสี่ยงหรือโมเดลการรับมือและโตความเสี่ยงในเชิงรุก รวมทั้งไม่ได้ใช้การพยายามเพิ่มศักยภาพและสมรรถนะ ในการทนทานต่อความเสี่ยงหรือแบกรับความเสี่ยงเพิ่มขึ้น
- ⇨ แม้ว่าผู้บริหารแต่ละสายงานอาจมีความรู้และความเข้าใจพื้นฐาน ระหว่างความเสี่ยงและผลตอบแทนที่จะเกิดขึ้นหลังจากการบริหารจัดการเสียงที่เพียงพอและมีประสิทธิผล แต่ไม่ได้ใช้ความพยายามในการที่จะ บริหารความเสี่ยงในเชิงที่ท้าทายหรือเชิงรุก แต่เน้นการบริหารความเสี่ยงที่อยู่ในขอบเขตของการมอบหมายตัวชี้วัดผลดำเนินงาน หรือ ภายใต้แผนงานหรือโครงการตามกลยุทธ์ที่เกี่ยวข้องเท่านั้น

บทสรุป

จากหลักการของการบริหารความเสี่ยงทั่วทั้งองค์กร หรือ ERM ดังกล่าวข้างต้น เมื่อเปรียบเทียบกับการบริหารจัดการความเสี่ยงตามมาตรฐานสากลฉบับเดิม COSO 2004 จะเห็นว่ามีการเพิ่มบทบาทของคณะกรรมการและผู้บริหารระดับสูงต่อความรับผิดชอบด้านผลดำเนินงานด้านการบริหารความเสี่ยงที่ชัดเจนขึ้น ขณะที่มาตรฐานเดิมทำให้มองเหมือนว่าการบริหารจัดการความเสี่ยงเป็นหน้าที่ของผู้บริหารแต่ละสายงานและแต่ละด้านที่จะรับผิดชอบความเสี่ยงในส่วนที่เกี่ยวข้องกับความรับผิดชอบหลักของตน และอาจจะไม่ได้ดำเนินงานทั่วทั้งองค์กรจริง ทำให้การบริหารความเสี่ยงมีแนวโน้มที่จะเป็นแบบ Silo

ดังนั้น COSO ERM 2017 จึงเป็นความพยายามในการปรับเปลี่ยนการบริหารความเสี่ยง ที่เน้นประสิทธิผล เพื่อเป็นเครื่องมือกลยุทธ์ที่มีคุณค่าขององค์กร และทำให้มีการกำกับดูแลผลดำเนินงานองค์รวมขององค์กรด้านบริหารความเสี่ยงอย่างต่อเนื่อง จริงจัง และสม่ำเสมอจากระดับคณะกรรมการลงมา ต้องทำให้การบริหารความเสี่ยงมีลักษณะในเชิงรุก และเตรียมพร้อมล่วงหน้าที่จะไม่ให้เกิดผลกระทบต่อความสำเร็จของ

กลยุทธ์และผลดำเนินงานองค์กรไม่ว่ากรณีใดๆ ก็ตาม ให้ความสำคัญกับภาพพอร์ตฟอริโอของความเสี่ยงในองค์รวม (Holistic Portfolio)

คำว่า E ที่เป็นตัวแทนคำว่า Enterprise

- ⇨ เป็นการแสดงให้เห็นถึงมุมมองการบริหารความเสี่ยงแบบบนลงล่าง ไม่ใช่การกระจายการบริหารความเสี่ยงในระดับสายงานเท่านั้น ทำให้มีมุมมองของการเฝ้าระวังความเสี่ยงจากปัจจัยภายนอกองค์กรมากขึ้น
- ⇨ เป็นการแสดงถึงเครื่องมือตามหลักเกณฑ์การวิเคราะห์ความเสี่ยงว่าเป็นเครื่องมือที่อยู่ในระดับของความสำเร็จเชิงกลยุทธ์และผลประกอบการโดยรวมขององค์กร
- ⇨ เป็นมุมมองความเสี่ยงที่ ต้องเห็นทั้งความเป็นภัยคุกคามหรือวิกฤตต่อองค์กร และความเป็นช่องทางในการแสวงหาโอกาสเพิ่มเติมผ่านการแบกรับความเสี่ยงหรือทนทานต่อความเสี่ยงเพิ่มขึ้น
- ⇨ เมื่อคณะกรรมการและผู้บริหารระดับสูง มีความรู้ เข้าใจ และตื่นตัวต่อความเสี่ยงในระดับองค์กรอย่างเพียงพอ ก็จะนำเอาข้อมูลความเสี่ยงดังกล่าวมาใช้ในการออกแบบ ปรับเปลี่ยนกลยุทธ์การบริหารความเสี่ยงควบคู่กับกลยุทธ์ธุรกิจเพื่อรับมือต่อความเสี่ยงที่อาจจะเกิดขึ้นทั้งกรณีที่เป็นอุปสรรคต่อความสำเร็จและกรณีที่เป็นโอกาสในการเพิ่มขีดความสามารถในการแข่งขัน

บทที่ 3

BIG BANG ของ COSO 2004 สู่ COSO ERM 2017

1. มุมมองความเสี่ยงเปลี่ยนไปจนปฏิวัติกรอบดำเนินงานองค์กร

มาตรฐานการบริหารความเสี่ยงของ COSO ERM 2004 ใช้ลูกเต๋าเป็นตัวอธิบายองค์ประกอบของความเสี่ยง โดยขยายความและแยกย่อยแนวคิดออกมาจาก COSO 1992 Internal Control ที่อธิบายองค์ประกอบของมาตรฐานด้วยลูกเต๋า 3 ด้านเช่นกัน เพียงแต่ COSO 1992 มี 5 องค์ประกอบสำหรับงานควบคุมภายใน แต่เป็น 8 องค์ประกอบสำหรับงานบริหารความเสี่ยง

เมื่อเปลี่ยนจากกรอบการควบคุมภายใน COSO 1992 เป็น COSO 2013 การอธิบายองค์ประกอบของการควบคุมภายในยังคงยึด 3 ด้านของลูกเต๋าเหมือนเดิม แต่เปลี่ยนแปลงด้วยการแทรก 17 หลักการและ 77 ประเด็นมุ่งเน้นไว้ใน 5 องค์ประกอบหลักของการควบคุมภายใน

ด้วยความแตกต่างจากกรอบแนวคิดการบริหารความเสี่ยง COSO ERM 2017 ที่เปลี่ยนแปลงกระบวนการบริหารความเสี่ยงใหม่ทั้งหมด จนต้องทำให้องค์กรที่จะนำเอากรอบแนวคิดนี้ไปใช้ต้องทำการศึกษาและต้องทำความเข้าใจกันใหม่อย่างละเอียดและด้วยความเข้าใจอย่างเพียงพอ จากสัญลักษณ์ของสายรุ้ง (Rainbow) แทนลูกเต๋า (Cubic)

แนวความคิดสำคัญคือ คณะกรรมการบีหน้าที่กำกับผลดำเนินงานทางองค์กร ขณะที่ฝ่ายจัดการโดยผู้บริหารระดับสูงมีหน้าที่ขับเคลื่อน และรับผิดชอบผลดำเนินงานทั้งหมดที่เกิดขึ้นจริงขององค์กร รวมทั้งการบริหารจัดการความเสี่ยง เพื่อให้มั่นใจว่าผลดำเนินงานจะสอดคล้องตามวัตถุประสงค์และบรรลุผลสำเร็จของผลประกอบการตามที่ได้ตั้งไว้

ดังนั้น วงจรการบริหารกลยุทธ์ซึ่งเป็นการบริหารการดำเนินงานตามปกติขององค์กร จึงต้องแทรกด้วยวงจรการบริหารความเสี่ยงเป็นส่วนหนึ่งของการดำเนินงานเพื่อสร้างมูลค่าแก่กิจการตามปกติ

โครงสร้างของมาตรฐาน COSO ERM 2017 ไม่ใช่เพียง 5 องค์ประกอบ 20 หลักการซึ่งเป็นเพียงกรอบการดำเนินงานในภาพรวมของแต่ละองค์กร หากแต่ภายใต้มาตรฐานเดียวกันนี้ ยังมีการประกาศใช้ GUIDANCE ซึ่งเป็นแนวปฏิบัติที่ดีเฉพาะเจาะจง เพื่ออำนวยความสะดวกและทำให้การบริหารความเสี่ยงซึ่งต้องใช้ผู้มีความรู้ ผู้เชี่ยวชาญในแต่ละเรื่องแตกต่างกันออกไป แทนที่จะเป็นเจ้าหน้าที่บริหารความเสี่ยงหรือ Risk Officer เพียงกลุ่มเดียวในการขับเคลื่อนวงจรของการบริหารความเสี่ยง

หากเปรียบเทียบกรณีนี้จะเห็นว่ามีความใกล้เคียงกับการจัดทำมาตรฐานเชิงคุณภาพของกลุ่ม ISO ที่มีการประกาศใช้มาตรฐานหลักด้านระบบการบริหารความเสี่ยงคือ ISO 31000 และมาตรฐานด้านระบบการบริหารคุณภาพ คือ ISO 9001 ที่นำไปประยุกต์ใช้เป็นส่วนหนึ่งของมาตรฐานอื่น ภายใต้มาตรฐาน ISO 31000 ยังมีการออกมาตรฐานในชุดเดียวกันเพื่อขยายความในลักษณะที่เป็นเครื่องมือของการดำเนินงานของระบบบริหารความเสี่ยง ตัวอย่างเช่น

>> ISO 31010 :2019 Risk management — Risk assessment techniques

>> ISO 31022:2020 Risk management — Guidelines for the management of legal risk

>> ISO 31050: Introducing the risk intelligence cycle for emerging risks

>> ISO 27001 risk assessment methodology ในส่วนของ IT

ในส่วนของมาตรฐาน COSO ERM 2017 ได้มีการออกแนวทางการปฏิบัติที่ดีเพื่อรองรับบริบทและแนวดำเนินงานขององค์กรสมัยใหม่เพิ่มเติมอีกหลายเรื่อง และมีแนวโน้มที่จะเพิ่มเติมในประเด็นอื่นต่อไปในแต่ละปีต่อจากนี้

>> แนวปฏิบัติที่ดีในการบริหารความเสี่ยง AGILE ERM ให้ทันต่อการเปลี่ยนแปลงอย่างเฉียบพลัน

>> แนวปฏิบัติที่ดีในการบริหารความเสี่ยงไซเบอร์ เพื่อสอดคล้องกับยุคดิจิทัล

>> แนวปฏิบัติที่ดีในการบริหารความเสี่ยงการปฏิบัติงานบนคลาวด์ คอมพิวติ้ง

>> แนวปฏิบัติที่ดีในการบริหารความเสี่ยงด้านกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance Risk Management) ก่อนที่จะนำกลับไปบูรณาการในความเสี่ยงทั่วทั้งองค์กร

>> แนวปฏิบัติที่ดีในการบริหารความเสี่ยงที่มุ่งฟื้นฟูและพลิกฟื้นองค์กรหลังวิกฤต

เป็นต้น

2. การยกเครื่องใหม่ทั้งหมดของ ERM ภายใต้ COSO 2017

ประเด็นที่ต้องทำความเข้าใจเกี่ยวกับ การเปลี่ยนแปลงที่สำคัญของการบริหารความเสี่ยงทั่วทั้งองค์กร แทนการบริหารความเสี่ยงที่แยกตามสายงานในลักษณะ Silo ก่อนที่จะนำไปประยุกต์ใช้งานภายในองค์กรให้เหมาะสมกับบริบทของธุรกิจ ได้แก่

ประเด็นที่ 1 ***เปลี่ยนกระบวนการบริหารความเสี่ยงจากการเป็นจุดเริ่มต้นที่เป็นเพียงแหล่งข้อมูลที่ส่งให้ผู้บริหารนำไปพิจารณาใช้เชิงกลยุทธ์เป็นระดับกลยุทธ์เสียเอง***

การนำเอาพันธกิจ วิสัยทัศน์ คุณค่าหลักขององค์กร มากำหนดกลยุทธ์ และกำหนดวัตถุประสงค์ทางธุรกิจเป็นข้อมูลตั้งต้น (Input) เพื่อป้อนเข้าสู่กระบวนการออกแบบ จัดวางกระบวนการบริหารความเสี่ยง โดยมีผลลัพธ์เดียวกับองค์กรคือ ผลประกอบการขององค์กรที่บรรลุผลสำเร็จ บนเกณฑ์ความเสี่ยงที่ยอมรับได้

ประเด็นที่ 2 ***การบริหารความเสี่ยงตาม COSO ERM 2017 ไม่ใช่การรู้เฉพาะหน้าที่ตามภาระของแต่ละหน่วยงาน***

หากแต่ต้องทำการศึกษา รวบรวมองค์ความรู้ในระดับองค์กรทั้งหมด จนสามารถตีความกลับมาเป็นเกณฑ์ความเสี่ยงที่ยอมรับได้ เป็นทะเบียนข้อมูลความเสี่ยง วิเคราะห์และประเมินความเสี่ยงจากคลังข้อมูลได้ ซึ่งในทางปฏิบัติหากไม่ดำเนินการโดยผู้บริหารระดับสูงย่อมเป็นไปไม่ได้ หรือไม่อาจจะครบถ้วนและเพียงพอ

นอกจากนั้น หากองค์กรไม่ได้มีการจัดสรรทรัพยากร งบประมาณ เวลา บุคลากร ที่มีสมรรถนะมาดำเนินกระบวนการ ERM คงไม่สามารถนำเอากรอบแนวคิดไปใช้ได้ครบถ้วนตามมาตรฐานที่กำหนดไว้ และไม่สามารถช่วยส่งเสริมผลประกอบการขององค์กรได้จริง

ประเด็นที่ 3 ***กรอบการบริหารความเสี่ยงไม่ใช่กิจกรรมที่ทำลอย ๆ และดำเนินการปีละ 1 ครั้ง เป็นการทบทวนตามความเหมาะสมของสถานการณ์***

กรอบเวลาการบริหารความเสี่ยงต้องครอบคลุมในทุกระยะของการบริหารจัดการทางธุรกิจโดยรวม 5 ระยะของการดำเนินงานปกติ

ระยะที่ 1 ERM Governance and Culture

การสร้างกลไกการบริหารความเสี่ยงเป็นส่วนหนึ่งของคุณค่าหลักขององค์กร

ระยะที่ 2 ERM Strategy and Objective Setting

การแทรกเป้าหมายความเสี่ยงไว้ในระดับคู่ขนานกับการกำหนดกลยุทธ์และวัตถุประสงค์ทางธุรกิจ

ระยะที่ 3 ERM Performance and Risk in Execution

การดำเนินกิจกรรมการบริหารความเสี่ยงที่กำกับความเสี่ยงที่จะมีผลกระทบต่อผลประกอบการขององค์กรและความเสี่ยงส่วนที่ยังเกินเกณฑ์ที่ยอมรับได้

ระยะที่ 4 ERM Information, Communication and Reporting

เป็นการสื่อสารเพื่อสนับสนุนข้อมูลสารสนเทศที่จำเป็นในการบริหารความเสี่ยง และแก้ไขปรับปรุงตามการเปลี่ยนแปลงระหว่างปี

ระยะที่ 5 Monitoring ERM Performance

เป็นการติดตาม ประเมิน สรุปผลและบทเรียนเพื่ออธิบายผลประกอบการขององค์กร

ประเด็นที่ 4 เครื่องมือและเทคนิคการได้มาซึ่งทะเบียนข้อมูลความเสี่ยง เพื่อจัดเก็บเป็นคลังข้อมูลและเทคนิคในการวิเคราะห์ ประเมินความเสี่ยงไม่ได้ง่ายดายเหมือน COSO ERM 2004

COSO ERM 2017 เน้นการรวบรวมความเสี่ยงให้ครบถ้วนและเพียงพอ ทั้ง

1) ความเสี่ยงยังหลงเหลือจากการใช้ระบบควบคุมภายในแล้ว
2) ความเสี่ยงเกิดใหม่ที่ควรจะเพิ่มเติมไว้ในคลังข้อมูลความเสี่ยงให้เป็นปัจจุบัน
3) ความเสี่ยงที่เกิดจากความเปลี่ยนแปลงสำคัญระหว่างปี ที่อยู่นอกเหนือความคาดหมายและไม่ได้ใส่ใจในคลังข้อมูลความเสี่ยงแต่แรก

โดยในการวิเคราะห์และประเมินความเสี่ยงจะต้องมีรายละเอียดที่ครบถ้วนด้วยมิติหลายมิติ

ประเด็นที่ 5 **COSO ERM 2017 ที่เกี่ยวกับการจัดเรียงลำดับความจำเป็น ความเร่งด่วน และความสำคัญของความเสี่ยงที่จะใช้ในการตัดสินใจจัดทำแผนและแนวทางการตอบโต้ความเสี่ยงในรอบปีธุรกิจใด ๆ ไว้ชัดเจน โดยใช้มิติพิจารณาที่หลายมิติ**

ตามมาตรฐานใหม่นี้ องค์กรต้องพิจารณาระดับความรุนแรงของผลกระทบของความเสี่ยงที่มีผลต่อผลดำเนินงาน และเปรียบเทียบค่าความเสี่ยงที่ประเมินได้กับเกณฑ์ความเสี่ยงที่ยอมรับได้

การออกแบบแนวทางปฏิบัติใหม่นี้ เท่ากับยกเลิกวิธีปฏิบัติเดิมในการเรียงลำดับความเสี่ยงด้วยการใช้ค่าคณิตศาสตร์ที่ได้จากผลคูณของโอกาสเกิด x ระดับความรุนแรงของผลกระทบ เช่น 2 X 4 เท่ากับ 8 หรือ 1 X 5 เท่ากับ 5 ทั้งหมด

การเรียงลำดับความจำเป็นความเร่งด่วนของความเสี่ยงต้องพิจารณาตามมิติที่ COSO ERM 2017 ได้กำหนดไว้อย่างครบถ้วนทุกมิติ

ประเด็นที่ 6 **COSO ERM 2017 ได้อิงตามกรอบ COSO 2013 ในส่วนของการแยกการบริหารความเปลี่ยนแปลงที่เกิดระหว่างปีออกจากข้อมูลความเสี่ยงที่ผ่านกระบวนการประเมินและจัดเรียงลำดับความจำเป็นและความเร่งด่วนไว้ตั้งแต่แรก**

เมื่อใดที่เกิดการเปลี่ยนแปลงสำคัญจนทำให้ผลการประเมินและจัดเรียงลำดับความเสี่ยงหรือการจัดวางกลยุทธ์และวัตถุประสงค์ความเสี่ยงตั้งแต่แรกไม่เหมาะสม หรือไม่สอดคล้องกับสถานการณ์ที่เปลี่ยนไป จะต้องเกิดการทบทวน ปรับปรุงและแก้ไข กระบวนการบริหารความเสี่ยงทุกประเด็นใหม่ให้มั่นใจว่า การบริหารความเสี่ยงสามารถปรับตัวอย่างเป็นพลวัตร ไม่ใช่ยึดติดกับแผนดำเนินการที่จัดทำไว้เดิมตลอดปีธุรกิจ

ประเด็นที่ 7 **แนวคิดเกี่ยวกับความเสี่ยง ซึ่งในเวอร์ชั่น 2004 ทำให้องค์กรมีความเข้าใจและทัศนคติในทางลบต่อความเสี่ยง มองความเสี่ยงเป็นมุม**

Negative Risk ได้เกิดการปรับเปลี่ยนให้แนวคิดคำว่า “ความเสี่ยง” มีความใกล้เคียงกับมาตรฐาน ISO 31000: 2018 มากขึ้น

ความเสี่ยงตามมาตรฐานใหม่ในเวอร์ชั่น 2017

1) ความเสี่ยงไม่ได้เลวร้ายอย่างเดียว แต่เป็นภาวะที่มีความเปลี่ยนแปลง ความไม่แน่นอน ความไม่เสถียร
2) ความเสี่ยงก็คือ โอกาสทางธุรกิจ และเป็นส่วนที่จะสร้างมูลค่าเพิ่มแก่องค์กรได้ ถ้าองค์กรกล้ารับความเสี่ยงนั้น แทนที่จะหนีความเสี่ยง
3) ความเสี่ยงยังคงเป็นลบและภัยคุกคามต่อผลประกอบการขององค์กร หากองค์กรไม่ได้ใช้ความพยายาม และพัฒนาในการยกระดับขีดความสามารถในการจัดการกับความเสี่ยงอย่างเพียงพอ จนสถานะความเสี่ยงไม่เกินกว่าเกณฑ์ที่ยอมรับได้

ประเด็นที่ 8 **แนวคิดเดิมของ COSO อิงมาจากมาตรฐานการควบคุมภายใน และพัฒนาต่อยอดมาเป็นการบริหารความเสี่ยงขององค์กร**

จึงเน้นสภาพแวดล้อมการควบคุมภายในองค์กรเป็นสำคัญ และไม่ได้คำนึงถึงสังคม สิ่งแวดล้อม ผู้มีส่วนได้ส่วนเสียภายนอกอย่างชัดเจน

แต่ใน COSO ERM 2017 มองความเสี่ยงจากสภาพแวดล้อมทางธุรกิจทำให้เครื่องมือในการวิเคราะห์และประเมินความเสี่ยงครอบคลุมถึง SWOT Analysis หรือ PESTLE หรือ PPPs ที่มี Planet เป็น P ตัวสุดท้ายด้วย ซึ่งเป็นความพยายามปิดจุดอ่อนของมาตรฐาน COSO ERM เดิม

ประเด็นที่ 9 **COSO ERM 2017 กำหนดให้องค์ประกอบที่ 1 การกำกับดูแลและการปลูกฝังวัฒนธรรมการตื่นตัวต่อความเสี่ยงทั่วทั้งองค์กร (Risk Governance and Culture) เป็นเสมือนร่มหลักที่วางรากฐานและโครงสร้างพื้นฐานให้กับกระบวนการบริหารความเสี่ยงในองค์ประกอบการอื่น ๆ**

เนื่องจากเป็นการรับรู้คุณค่าหลักขององค์กรที่นำมาเชื่อมโยงกับความเสี่ยงที่ต้องเฝ้าระวัง ซึ่งเป็นองค์ประกอบสำคัญที่สุด ที่ต้องมาจากผู้บริหารระดับสูงขององค์กร ก่อนที่จะส่งต่อไปยังหน่วยงานอื่น ๆ

ตารางที่ 1 การเชื่อมโยงองค์ประกอบ COSO ERM 2017 กับโครงสร้างองค์กร

องค์ประกอบของ COSO ERM 2017	หน่วยงานภายในที่เชื่อมโยง
1. ERM Governance and Culture 2. ERM Strategy and Objective Setting 3. ERM Performance and Risk in Execution 4. ERM Information, Communication and Reporting 5. Monitoring ERM Performance	ผู้บริหารระดับสูง ฝ่ายงานวางแผน กลยุทธ์ Strategic Business Unit สายงาน และฝ่ายงาน ผู้รับผิดชอบโครงการ ฝ่ายงาน IT บริหารข้อมูล MIS สื่อสารองค์กร สายงาน และฝ่ายงาน ผู้รับผิดชอบโครงการ

การที่ COSO ERM เวอร์ชั่น 2017 เปลี่ยนแปลงอย่างมากมายจากเวอร์ชั่น 2004 จึงเป็นการยากที่จะเปรียบเทียบกรอบแนวคิดของแต่ละเวอร์ชั่นอย่างชัดเจน เพราะความแตกต่างจนไม่อาจเปรียบเทียบกันได้

โดยสรุปแล้ว COSO ERM 2017 ออกแบบมาเพื่อนำมาใช้เป็นเครื่องมือช่วยงานการบริหารจัดการธุรกิจของผู้บริหารและคณะกรรมการเท่านั้น ผู้ใช้งานจึงเป็นผู้บริหารและคณะกรรมการขององค์กรเองที่ไม่อาจจะปฏิเสธได้เพราะอธิบายผลสำเร็จของผลประกอบการจากปัจจัยด้านความเสี่ยงด้วย โดยผู้บริหารและคณะกรรมการต้องแยกบริหารจัดการระบบควบคุมภายในตาม COSO 2013 และแยกบริหารความเสี่ยงออกจากกันต่างหาก ไม่ใช่ส่วนต่อขยายอีกต่อไป

3. ทางเลือกระหว่าง COSO ERM 2017 กับ ISO 31000: 2018

มาตรฐานสากลด้านบริหารความเสี่ยงไม่ได้มีเพียงมาตรฐานเดียว COSO ERM 2017 เป็นเพียงมาตรฐานทางเลือกหนึ่งที่องค์กรอาจจะไม่นำมาใช้ก็ได้ เปรียบเทียบกับมาตรฐานสากลอื่น ๆ ที่สำคัญโดยเฉพาะ ได้แก่

- ⇨ มาตรฐาน ISO 31000: 2018 และกลุ่มมาตรฐาน ISO 31XXX ที่เกี่ยวข้อง
- ⇨ มาตรฐาน GRC ของ OECD ที่ให้ความสำคัญกับคณะกรรมการลงมากำกับองค์กรใน 3 ด้านพร้อมกันคือ Governance, Risk Management และ Compliance Management โดยตรง ไม่ใช่เรื่องที่ผู้บริหารระดับสูงที่จะดำเนินได้ตามลำพังในเรื่องสำคัญ
- ⇨ มาตรฐาน ES-G-RC ที่ครอบคลุมประเด็นความเสี่ยงต่อความรับผิดชอบขององค์กรในทางสังคมและสิ่งแวดล้อมด้วย

กรณีของมาตรฐาน ISO 31000: 2018 ซึ่งเป็นเวอร์ชั่นที่ปรับปรุงใหม่จากเวอร์ชั่น 2018 มีข้อได้เปรียบและจุดเด่นหลายประการที่ทำให้หลายประการ ได้แก่

ประการที่ 1 **ISO 31000 ให้หลักการในการบริหารความเสี่ยงที่มีความยุ่งยากน้อยกว่า มีทั้งมาตรฐานและ Series ที่เป็นแนวปฏิบัติที่จะต้องใช้ (Guidelines) ขณะที่ COSO ERM 2017 มีแต่หลักการจึงง่ายต่อการนำไปใช้ได้มากกว่า**

ISO 31000 ยังเปิดโอกาสให้แต่ละองค์กรสามารถปรับเปลี่ยน จัดน้ำหนักของกระบวนการบริหารความเสี่ยงโดยคำนึงถึง

1) รูปแบบของวัฒนธรรมองค์กรแต่ละแห่งที่แตกต่างกัน
2) ข้อจำกัดของทรัพยากรและความพร้อมภายใน

ประการที่ 2 **แนวคิดหลักๆ ของ ISO 31000 และ COSO ERM ในปัจจุบันนี้ไม่ได้แตกต่างกัน ในแง่ของ**

1) การมองความเสี่ยงว่าเป็นทั้งโอกาสและวิกฤติ
2) ความเสี่ยงที่ต้องจัดการคือ ความเสี่ยงที่เกี่ยวข้องและเชื่อมโยงกับคุณค่าหลักขององค์กร

แต่มาตรฐาน ISO เป็นมาตรฐานที่มาจากการประเมินและออกหนังสือรับรองขององค์กรกลางภายนอก ภายใต้หลักเกณฑ์ เงื่อนไข ข้อกำหนด และเอกสารหลักฐานประกอบการดำเนินงานเดียวกัน ขณะที่ มาตรฐาน COSO ERM 2017 ขึ้นอยู่กับความตระหนัก แรงบันดาลใจ และมุมมองต่อความเสี่ยงของผู้บริหารและคณะกรรมการแต่ละองค์กรเอง โดยไม่ได้ พิจารณาว่าต้องจัดทำองค์ประกอบการบริหารความเสี่ยง เพื่อให้หน่วยงานที่เป็นองค์กรกลางภายนอกมาทำการตรวจประเมินและให้ใบรับรอง

ประการที่ 3 **แต่เดิมองค์กรอาจจะมองว่าเมื่อใช้มาตรฐานการควบคุมภายในของ COSO 2013 แล้วก็ต้องใช้การบริหารความเสี่ยงของ COSO ERM ด้วยเพื่อให้การจัดการความเสี่ยงเป็นไปในทางเดียวกัน**

แต่เมื่อเนื้อหาและกรอบแนวทางการปฏิบัติที่ดีของ COSO ERM ไม่ได้เกี่ยวข้องสัมพันธ์กับการควบคุมภายในเป็นส่วนใหญ่ จึงไม่ได้มีความจำเป็นต้องใช้ระบบการควบคุมภายในและระบบบริหารความเสี่ยงที่ออกมาจากองค์กรเดียวกันอย่าง COSO อาจจะใช้มาตรฐาน

การบริหารความเสี่ยงตามกรอบ ISO ก็ได้ แต่ถ้าองค์กรนำมาใช้ร่วมกันจะพบความเชื่อมโยงของ แนวปฏิบัติที่ดีหรือ GUIDANCE ที่มีความสัมพันธ์และส่งต่อถึงกัน การนำมาใช้งานจึงง่ายกว่า เช่น

- ⇨ แนวปฏิบัติของการควบคุมภายในที่เกี่ยวข้องกับยกดิจิทัลส่งต่อมาถึงการบริหารความเสี่ยงทั่วทั้งองค์กรด้วย
- ⇨ แนวปฏิบัติของการบริหารความเสี่ยงเชิงสังคมและสิ่งแวดล้อม ที่มีทั้งส่วนของการควบคุมการจัดทำรายงานความยั่งยืน และเชื่อมโยงและ ประสานกับแนวปฏิบัติที่ดีของการบริหารความเสี่ยงด้านความยั่งยืนขององค์กร
- ⇨ แนวปฏิบัติที่ดีในการบริหารความเสี่ยงงานกำกับการปฏิบัติตามกฎเกณฑ์ ได้เชื่อมโยงเครื่องมือในการจัดการความเสี่ยง ทั้งในส่วนของการควบคุมภายใน และการรับมือตอบโต้ความเสี่ยงตามมิติของการบริหารความเสี่ยงทั่วทั้งองค์กร
- ⇨ ได้แยกบทบาทในส่วนของคณะกรรมการที่เป็นองค์คณะกำกับออกมาต่างหากจากฝ่ายจัดการที่มีหน้าที่ขับเคลื่อนการบริหารจัดการความเสี่ยง
- ⇨ ภาษาที่ใช้ กรอบแนวทางการปฏิบัติมีความสอดคล้องและเป็นไปในทิศทางเดียวกัน

ประการที่ 4 **มาตรฐาน ISO จะมีองค์กรภายนอกมาช่วยในการวางกรอบแนวทางปฏิบัติที่เป็นบรรทัดฐานเดียวกันไม่ว่าจะเป็น ISO ฉบับใด**

ดังนั้น องค์กรที่ได้รับใบรับรอง ISO ในเรื่องอื่น ๆ อย่างเช่น ISO 9001 Quality Management และ ISO 14001 การบริหารสิ่งแวดล้อมแล้ว จะมีความเข้าใจแนวทางการจัดการ และเพิ่มเติมการจัดการด้วยมาตรฐานการบริหารความเสี่ยง ISO 31000 จึงเป็นเรื่องไม่ยุ่งยาก

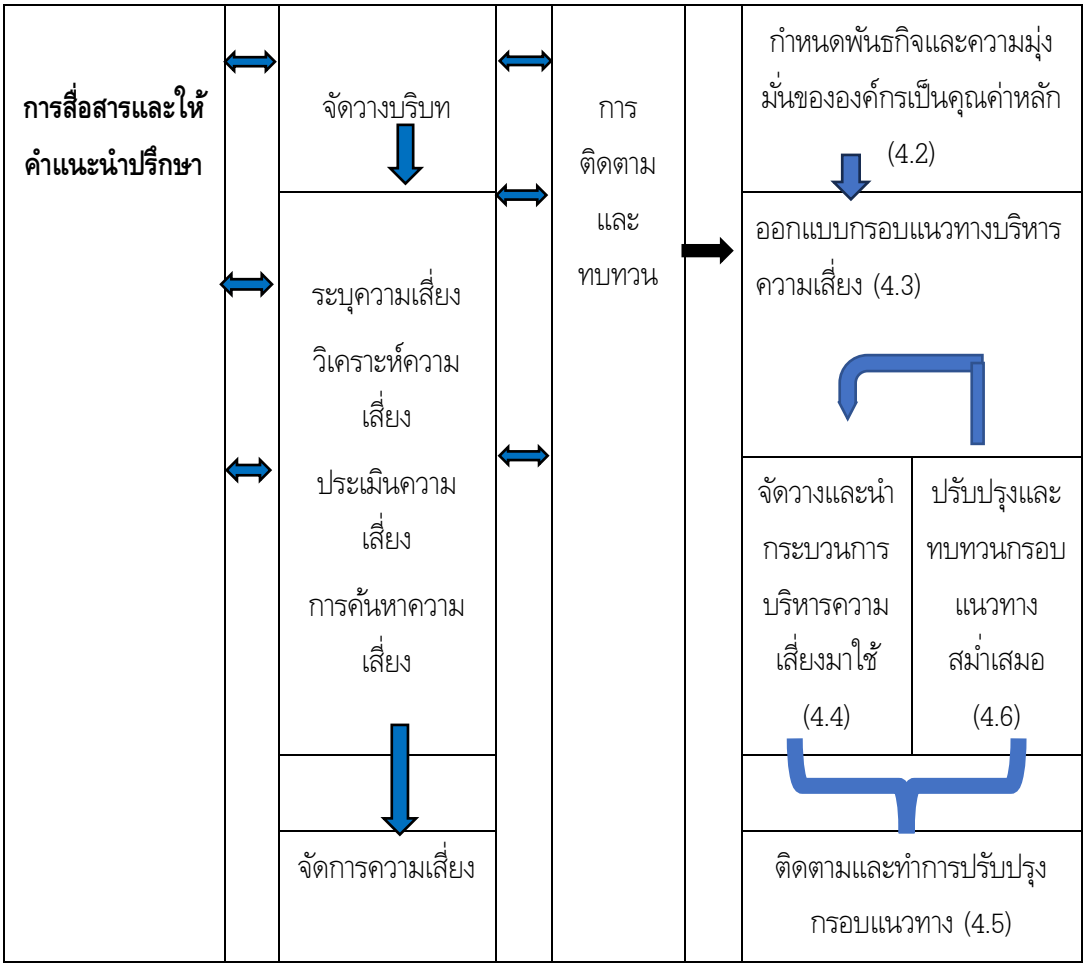
นอกจากนั้น กรณีที่ใช้มาตรฐาน ISO จะมีทีมงานออกใบรับรองมาตรฐาน หรือแจกเกียรติบัตรจาก ISO มาช่วยทำการประเมินองค์ประกอบ ความพร้อม มีข้อเสนอแนะจุดอ่อน ประเด็นที่ต้องแก้ไข ซึ่งจะอำนวยความสะดวกแก่องค์กรมากกว่าประเมินเองภายในองค์กรทั้งหมด

ประการที่ 5 **เมื่อเปรียบเทียบเนื้อหาของ ISO 31000 กับ COSO 2013 Internal Control แล้วจะพบว่ามีความสัมพันธ์และเชื่อมต่อกันได้ดีและง่ายกว่าการนำ COSO 2013 มาเชื่อมต่อกับ COSO ERM 2017**

องค์กรใดองค์กร หนึ่ง จึงสามารถผสมผสานการใช้มาตรฐานสากลได้ทั้งมาตรฐานของ COSO ERM 2017 รวมทั้งแนวปฏิบัติที่มีอยู่ขณะเดียวกันก็สามารถเติมเต็มส่วนของแนวปฏิบัติบางเรื่องที่ไม่ปรากฏอยู่ในมาตรฐานในกลุ่มของ COSO ERM 2017 ได้ เช่น

- ⇨ แนวปฏิบัติเรื่องการบริหารความเสี่ยงเกิดใหม่ และความเสี่ยงที่มีสภาวะสุดขั้วของวิกฤตการณ์ที่ปรากฏอยู่แต่เฉพาะในมาตรฐาน ISO
- ⇨ แนวปฏิบัติเรื่องการบริหารเทคโนโลยีสารสนเทศ ที่ปรากฏอยู่ในชุดของมาตรฐาน ISO 27001
- ⇨ แนวปฏิบัติเรื่องการบริหารความต่อเนื่องทางธุรกิจ ซึ่ง ISO 22301 และชุดของมาตรฐานที่เกี่ยวข้องได้ให้แนวทางการรับมือไหวในหลากหลายมิติ
- ⇨ แนวปฏิบัติเรื่องการบริหารระบบการกำกับการปฏิบัติตามกฎเกณฑ์ ซึ่ง ISO ยกระดับขึ้นไปเป็นระบบบริหารจัดการที่แยกต่างหากจากการบริหารความเสี่ยง

แผนภาพรวม ISO 31000: 2018



ประการที่ 6 **มาตรฐาน ISO 31000 เวอร์ชั่นใหม่ออกมาภายหลังจาก COSO ประกาศ ERM 2017 ได้ไม่นาน คือประกาศตาม ๆ กันออกมา**

จึงทำให้องค์กรต้องปรับตัวทุกองค์กร ไม่ว่าจะเลือกใช้ COSO ERM หรือเปลี่ยนมาใช้ ISO 31000 หรือใช้ผสมผสานกันแบบไพ่บริดจ์ก็ตาม สามารถดำเนินการได้ในช่วงเวลาที่เหมาะสม

จังหวะการปรับเปลี่ยนที่อยู่ในช่วงเวลาที่ใกล้เคียงกัน มีผลอย่างมากต่อการจะเปลี่ยนใจจากการใช้มาตรฐานเดิมมาใช้มาตรฐานใหม่ได้โดยไม่ต้องคิดมาก เพราะองค์กรต้องทำความเข้าใจกับขอบเขตใหม่และความเปลี่ยนแปลงที่เกิดขึ้นกับมาตรฐานการบริหารความเสี่ยงต่อแต่ละค่ายในประเด็นต่อไปนี้

ประเด็นย่อย 1 **องค์กรใส่ใจให้ความสำคัญกับคุณค่าหลัก**

จะพบว่า ISO 31000 ให้แนวทางปฏิบัติที่ง่ายและไม่ซับซ้อนเท่าCOSO ERM และให้แนวทางปฏิบัติที่ชัดเจนกว่าเวอร์ชั่น 2009 แต่มีเป้าหมายเดียวกัน

ประเด็นย่อย 2 **กรณีที่องค์กรได้ดำเนินกระบวนการบริหารความเสี่ยงอยู่แล้ว** จะพบว่าการใช้ ISO 31000 ไม่ทำให้ต้องปรับเปลี่ยนกระบวนการที่มีอยู่แล้วมากนัก

ขณะที่ COSO ERM จะต้องพบแรงกดดันในการปรับเปลี่ยนตั้งแต่ขั้นตอนการกำหนดกลยุทธ์ วัตถุประสงค์ทางธุรกิจ เกณฑ์ความเสี่ยงที่ยอมรับได้ กรอบแนวทางปฏิบัติและกระบวนการใหม่ รวมทั้งมีศัพท์เทคนิคมากกว่า ISO 31000

ประเด็นย่อย 3 **กำหนดความเสี่ยงก่อนหรือหลังกำหนดกลยุทธ์**

ISO 31000 จะทำการวิเคราะห์ความเสี่ยงก่อน และส่งข้อมูลความเสี่ยงประกอบการกำหนดกลยุทธ์ เป็นข้อมูลช่วยสนับสนุนการกำหนดกลยุทธ์

COSO ERM ให้องค์กรทำการกำหนดกลยุทธ์และวัตถุประสงค์ทางธุรกิจก่อนแล้วจึงนำมากำหนดกลยุทธ์ความเสี่ยงภายหลัง

ทั้งมาตรฐานเชื่อมโยงการบริหารความเสี่ยงกับกิจกรรมการตัดสินใจระดับองค์กรและการกำกับดูแลองค์กรเหมือนกัน จึงทำให้กระบวนการบริหารความเสี่ยงไม่ได้มีลักษณะ Stand – alone โดยปราศจากการยึดมั่นเป็นพันธะผูกพันระดับกลยุทธ์

ประเด็นย่อย 4 **กระบวนการบริหารความเสี่ยงใช้ในระดับอื่นด้วยหรือไม่**

ISO 31000 ให้กรอบแนวทางการบริหารความเสี่ยงทั้งระดับกลยุทธ์ ระดับกระบวนการ ระดับแผนงาน/โครงการ ยังมีมาตรฐาน ISO ฉบับอื่นที่เกี่ยวข้องมา

ช่วยสนับสนุนอีกหลายฉบับ โดยใช้กรอบแนวทางการจัดการบท Risk – based Thinking เหมือนกัน ซึ่ง COSO ERM ไม่มีส่วนนี้

ประเด็นย่อย 5 **การพิจารณาครอบคลุมสภาพแวดล้อมภายในและภายนอกหรือไม่**

ทั้งสองมาตรฐานได้แสดงให้เห็นว่าให้ความสำคัญกับปัจจัยเสี่ยงที่มาจากภายในและภายนอกองค์กรเหมือนกัน

ประเด็นย่อย 6 **การใช้ดุลยพินิจในการระบุ และประเมินความเสี่ยง**

ISO 31000 เวอร์ชั่นใหม่ให้ความสำคัญกับความเบี่ยงเบน ความลำเอียงอันเนื่องมาจากการใช้บุคคลนำเอาดุลยพินิจมาใช้ในการวิเคราะห์และประเมินความเสี่ยง ซึ่งองค์กรจะต้องให้ความสำคัญเรื่องนี้

COSO ERM เองก็เริ่มกำหนดเป็นเงื่อนไขให้ใช้บุคลากรที่มีความเข้าใจในกลยุทธ์ และมีสมรรถนะในการดำเนินกระบวนการบริหารความเสี่ยงด้วย

ประเด็นย่อย 7 **การแสดงผลดำเนินงานความเสี่ยงกับผลประกอบการขององค์กร**

ISO 31000 ให้กรอบแนวทางในเรื่องนี้ไม่ชัดเจนเท่ากับ COSO ERM ที่ต้องแสดงผลประกอบการที่เกิดจริงในมุมของปัจจัยเสี่ยงด้วยเสมอ

4. บริหารความเสี่ยงที่มีประสิทธิผลตาม COSO ERM 2017

การออกมาตรฐานใหม่ด้านการควบคุมภายใน ภายใต้กรอบแนวคิด COSO ERM 2017 โดยเน้นการขยายความว่า **“บูรณาการกับกลยุทธ์และผลประกอบการขององค์กร (Integrating With Strategy and Performance)”** มีสิ่งที่เปลี่ยนแปลงจาก COSO ERM 2004 อย่างชัดเจนในการอธิบายกรอบแนวทาง (Framework) ที่แสดงถึงการเชื่อมโยงเชิงลึกระหว่างการกำหนดกลยุทธ์ ความเสี่ยง และผลประกอบการ ขณะเดียวกันก็ไม่ได้ละทิ้ง การบริหารความเสี่ยงตามบริบทหรือรูปแบบการดำเนินงานเฉพาะของแต่ละองค์กร ที่ทำให้ประเด็นความเสี่ยงแตกต่างกันออกไป เช่น ในกรณีที่องค์กรจำเป็นต้องปรับเปลี่ยนอย่างทันท่วงที และรวดเร็วตามสถานการณ์ของตลาด การพลิกฟื้นและฟื้นฟูหลังจากการเกิดวิกฤต การเปลี่ยนถ่ายสู่ยุคดิจิทัล ที่