COSO 2013 ควบคุมภายในครบวงจร

พร้อม NEW GUIDANCE : INDUSTRY 4.0 & ESG

แนวคิด วิธีดำเนินงาน กระบวนการภาคปฏิบัติ

THE THREE LINES OF DEFENSE
CSA : CONTROL SELF-ASSESSMENT
FRAUD RISK ASSESSMENT
IT GENERAL CONTROL IN DIGITAL AGE
CONTROL SUSTAINABILITY REPORTING

อาจารย์ จิรพร สุเมธีประสิทธิ์

COSO 2013 ควบคุมภายในครบวงจร

พร้อม NEW GUIDANCE : INDUSTRY 4.0 & ESG

อาจารย์ จิรพร สุเมธีประสิทธิ์

ข้อมูลทางบรรณานุกรม

อาจารย์ จิรพร สุเมธีประสิทธิ์

COSO 2013 ควบคุมภายในครบวงจร

พร้อม NEW GUIDANCE : INDUSTRY 4.0 & ESG

493 หน้า

ISBN (E-BOOK) 978-616-616-067-3

พิมพ์ครั้งที่ 1 : พ.ศ. 2567

จำหน่ายในรูปแบบ : E-Book

ราคา : 379 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

ระบบการควบคุมภายในเป็นรากฐานที่สำคัญของการกำกับดูแลกิจการที่ดีในทุกองค์กร เช่นเดียวกับมาตรฐานสากล COSO 2013 ที่ได้รับการยอมรับให้เป็นกรอบแนวทางดำเนินงานด้านการควบคุมภายในจากองค์กรต่างๆ ทั่วโลก ซึ่งการนำเอากรอบแนวทางดำเนินงานดังกล่าวมาใช้จริงในแต่ละองค์กร ที่มักเป็นบทบาทหน้าที่ของหน่วยงานบริหารความเสี่ยงและควบคุมภายในต้องดำเนินการด้วยความเข้าใจ และประยุกต์ใช้มาตรฐานดังกล่าวให้เข้ากับยุคสมัยดิจิทัล และความคาดหวังให้องค์กรมีความรับผิดชอบต่อสังคมและสิ่งแวดล้อม ที่ต้องการรูปแบบและ แนวคิดของการควบคุมภายในที่แตกต่างออกไปจากเดิม

แม้ว่ามาตรฐานนี้จะใช้มากว่า 10 ปีแล้ว แต่ยังคงมีความทันสมัย จากการที่ COSO ได้ประกาศใช้ DUIDANCE ใหม่ออกมารองรับการควบคุมภายในต่อความเสี่ยงเฉพาะด้าน ที่ต้องใช้ความชำนาญ และทักษะในการบริหารจัดการงานควบคุมภายในเพิ่มขึ้น

นอกจากนั้น มาตรฐานด้านการควบคุมภายใน COSO 2013 ยังต้องใช้ควบคู่กับมาตรฐานการบริหารความเสี่ยงทั่วทั้งองค์กร หรือ COSO ERM 2017 และมาตรฐานสากลด้านการตรวจสอบภายในฉบับปี 2024 เพื่อให้เป็นไปในลักษณะที่สอดคล้องและส่งเสริมซึ่งกันและกัน

ด้วยเหตุนี้ ตำรา e-BOOK เล่มนี้จึงเป็นเพียงหนึ่งในชุดของตำรา ที่ผู้เขียนจัดทำไว้ เพื่อรองรับการบริหารจัดการองค์กรภายใต้แนวคิดของ RISK-BASED APPROACH ที่รวมถึงมาตรฐานการบริหารความเสี่ยงทั่วทั้งองค์กร (ERM) การกำกับการปฏิบัติตามกฎเกณฑ์ (COMPLIANCE) และการตรวจสอบภายในตามมาตรฐานสากล (GLOBAL IA STANDARD) เพื่อให้เกิดความเข้าใจที่ครบวงจร

ด้วยรูปแบบการเป็นตำราทางอิเล็กทรอนิกส์ ทำให้ผู้เขียนมีโอกาสที่จะปรับปรุงเพิ่มเติมให้เป็นปัจจุบันได้อยู่เสมอ ซึ่งน่าจะเป็นประโยชน์ สำหรับผู้อ่านที่สนใจจะปรับความรู้และความเข้าใจในเรื่องนี้ให้ทันสมัยอยู่ตลอดเวลา

อาจารย์ จิรพร สุเมธีประสิทธิ์

ผู้เขียน

สารบัญ

บทนำ

กรอบแนวทางดำเนินงานด้านการควบคุมภายใน ยังจำเป็นต้องเรียนรู้เพื่อให้เกิดประสิทธิภาพ

COSO

Committee of Sponsoring Organizations of the Treadway Commission

Internal Control — Integrated Framework

Executive Summary

1. หลักการและเหตุผล

กรอบแนวทางดำเนินงานด้านการควบคุมภายในเป็นเสมือนรากฐานที่สำคัญขององค์กร เนื่องจากเป็นส่วนที่กำหนดอำนาจหน้าที่และความรับผิดชอบให้แก่ผู้ที่เกี่ยวข้องในแต่ละหน่วยงาน แต่ละกลุ่มงาน จึงเป็นเสมือนขั้นตอนการปฏิบัติงาน ข้อกำหนด และเงื่อนไขที่ออกแบบ เครื่องมือ มาตรการ วิธีการ กิจกรรมเพิ่มเติมเพื่อกำกับระหว่างการปฏิบัติงานตามภาระงานที่ได้รับมอบหมายนอกเหนือจากคำอธิบายลักษณะงานที่ปรากฏอยู่ในโครงสร้างองค์กร

ด้วยเหตุนี้ กรอบแนวทางการดำเนินงานด้านการควบคุมภายในที่ดีจึงเปรียบเสมือนข้อกำหนดที่กำกับการปฏิบัติงานอีกส่วนหนึ่งขององค์กร ที่กระจายอำนาจการจัดการความเสี่ยงและการกำกับดูแลออกไปตามสายงานต่างๆ เพื่อทำให้การปฏิบัติงานมีความราบรื่น มีประสิทธิภาพ ควบคุมมิให้ความเสี่ยงอยู่ในระดับที่เกินกว่าเกณฑ์ที่ยอมรับได้ และนำไปสู่ผลสำเร็จของการปฏิบัติงานตามวัตถุประสงค์ที่กำหนดไว้ และกำกับการปฏิบัติให้สอดคล้อง ครบถ้วน และถูกต้องตามกฎเกณฑ์ภาคบังคับ พันธะผูกพัน และข้อตกลงที่เกี่ยวข้อง

กรอบแนวทางดำเนินงานด้านการควบคุมภายในจึงมีความสำคัญที่ทำให้องค์กรต้องเพิ่มขีดความสามารถ และคุณภาพการจัดการความเสี่ยงที่มีผลต่อความสำเร็จขององค์กร เพราะเป็นระบบที่ช่วยในการบริหารจัดการความเสี่ยงผ่านกลไกของการควบคุมที่ดี ดำเนินการอย่างเป็นระบบ มีความสอดคล้องกันทั่วทั้งองค์กร หากปราศจากการควบคุมภายในที่ดี องค์กรมีโอกาสที่จะเผชิญหน้ากับปัญหา อุปสรรค รวมทั้งความล้มเหลวในการดำเนินงาน

อย่างไรก็ตาม การนำกรอบแนวทางการดำเนินงานด้านการควบคุมภายในมาใช้ในองค์กร ควรจะยึดโยงกับมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป และยังใช้กันอยู่ทั่วโลกมาจนถึงปัจจุบัน คือมาตรฐาน COSO 2013 COSO Internal Control – Integrated Framework (ICIF) โดย

- ⇨ *ใช้การดำเนินการด้วยความเข้าใจอย่างเพียงพอ*
- ⇨ *ทำการวางแผนดำเนินงานพัฒนากรอบแนวทางการควบคุมภายในด้วยความระมัดระวัง เพื่อให้เกิดประโยชน์สูงสุดต่อองค์กร*
- ⇨ *ประกาศและสื่อสารให้เกิดการรับทราบอย่างชัดเจนว่ากรอบแนวทางการดำเนินงานด้านการควบคุมภายในเป็นข้อกำหนดที่บุคลากรทุกระดับภายในองค์กรต้องยึดถือเป็นกฎเกณฑ์*
- ⇨ *กรอบแนวทางการดำเนินงานด้านการควบคุมภายในเป็นเรื่องที่ต้องปฏิบัติตามเช่นเดียวกับข้อบังคับการปฏิบัติงานอื่น โดยไม่มีสิทธิ์ที่จะเลือกหรือไม่เลือกปฏิบัติตามใจชอบได้*
- ⇨ *กรอบแนวทางการดำเนินงานด้านการควบคุมภายในมีความจำเป็นต้องทบทวน และปรับปรุงการออกแบบการควบคุมภายในและการนำมาใช้ประกอบการปฏิบัติงานให้เหมาะสมกับสถานการณ์ บริบทการดำเนินงานขององค์กร และประเด็นความเสี่ยงที่มีการ*

เปลี่ยนแปลงไป เช่น ความเสี่ยงที่เกิดขึ้นเนื่องจากความก้าวหน้าของเทคโนโลยี การปฏิบัติงานบนระบบอิเล็กทรอนิกส์ รูปแบบของการดำเนินงานที่เข้าสู่ยุคดิจิทัล เป็นต้น

ด้วยเหตุที่กรอบแนวทางการดำเนินงานด้านการควบคุมภายในจำเป็นต้อง ออกแบบ จัดวางระบบ และนำมาใช้ในองค์กรให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล ผู้ที่เกี่ยวข้องกับการดำเนินการในส่วนนี้ ตั้งแต่คณะกรรมการ ฝ่ายจัดการที่นำโดยผู้บริหารระดับสูง ผู้บริหารสายงานที่ได้รับการมอบหมายให้กำกับดูแลงานในความรับผิดชอบ ไปจนถึงหัวหน้างาน และผู้ปฏิบัติงานต้องใส่ใจและให้ความสำคัญอย่างจริงจังและเพียงพอ ในลักษณะที่เป็นการควบคุมภายในเชิงบูรณาการ (Integrated Framework) ตลอดวงจรของการควบคุมภายใน และทำให้เป็นระบบการบริหารจัดการที่สนับสนุนการกำกับดูแลองค์กรที่ดีอย่างแท้จริง จนสามารถให้คำรับรองที่เชื่อมั่นได้ว่าระดับความเสี่ยงจะอยู่ในเกณฑ์ที่ยอมรับได้และไม่ส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร

2. กรอบแนวทางควบคุมภายในตามมาตรฐาน COSO 2013

มาตรฐานสากลด้านควบคุมภายใน COSO 2013 COSO Internal Control – Integrated Framework (ICIF) ซึ่งเป็นกรอบแนวทางดำเนินงานด้านควบคุมภายในที่รู้จักดีทั่วโลก กำหนดขึ้นเพื่อช่วยเป็นกรอบแนวทางในการดำเนินงานควบคุมภายในเชิงบูรณาการขององค์กรทุกประเภท ทุกรูปแบบ ให้สามารถนำไปออกแบบและบริหารงานควบคุมภายในได้อย่างเหมาะสม

ซึ่งแม้ว่ามาตรฐานของกรอบแนวทางการดำเนินงานด้านควบคุมภายในดังกล่าว ที่ประกอบด้วย 5 องค์ประกอบ และ 17 หลักการจะได้มีการประกาศใช้มาเป็นเวลาเกินกว่า 10 ปีแล้ว แต่ความเปลี่ยนแปลงและพัฒนาการที่สำคัญของมาตรฐานสากลด้านการควบคุมภายใน COSO 2013 คือการเพิ่มเติมกรอบแนวทางการดำเนินงานใหม่ ในลักษณะของ GUIDANCE ที่มีการประกาศใช้เพิ่มเติมมาตามลำดับ เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของบริบทการดำเนินงานขององค์กร และสภาพแวดล้อมของการดำเนินงาน โดยเฉพาะการก้าวเข้าสู่การเปลี่ยนแปลงที่สำคัญ

- **การเปลี่ยนถ่ายภาคอุตสาหกรรมเข้าสู่ INDUSTRY 4.0**

  เป็นยุคที่มีการใช้เทคโนโลยีและระบบดิจิทัลเพื่อการประมวลผลและตัดสินใจ เน้นความรวดเร็วและตรงกับความต้องการตลาดมากที่สุด เกิดความเชื่อมโยงผ่านอินเทอร์เน็ตในทุกสรรพสิ่ง ทำให้เกิดความเชื่อมโยงกันของอุปกรณ์ เครื่องมือที่ใช้ในการผลิตและการดำเนินงานทางธุรกิจ เกิดระบบโครงสร้างพื้นฐานที่สนับสนุนเป็นระบบนิเวศของอุตสาหกรรม 4.0 การสร้างโซลูชั่นให้ผู้ประกอบการด้วยเทคโนโลยีใหม่ๆ

- **การปรับตัวเข้าสู่ระบบเศรษฐกิจหมุนเวียน หรือระบบเศรษฐกิจกระแสใหม่**
  - INDOOR Economy ระบบเศรษฐกิจการใช้จ่ายที่เกิดจากการใช้ชีวิตประจำวันส่วนใหญ่อยู่ในบ้านมากขึ้น

- CARE Economy ระบบเศรษฐกิจที่เกิดจากความต้องการในการดูแลสุขภาพความเป็นอยู่ที่มากขึ้นของผู้สูงอายุ เด็ก คนพิการ ผู้ป่วยรวมถึงกลุ่มวัยทำงาน
- DOMESTIC Economy ระบบเศรษฐกิจสินค้าและบริการที่ตอบสนองความต้องการผู้บริโภคภายในประเทศ และบริการที่สร้างประสบการณ์ใหม่แก่ผู้ใช้
- ONE PLANET Economy ระบบเศรษฐกิจที่ให้ความสำคัญกับการดูแลรักษาโลก ทำให้มีการปรับเปลี่ยนรูปแบบสินค้าและบริการ ตลอดจนการดำเนินธุรกิจที่เป็นมิตรต่อสิ่งแวดล้อม
- VIRTUAL Economy ระบบเศรษฐกิจที่มุ่งสร้างประสบการณ์บนโลกเสมือนจริงให้มีคุณค่าเทียบเท่าประสบการณ์จริงด้วยเทคโนโลยีดิจิทัลรูปแบบใหม่ๆ
- UP-SKILL Economy ระบบเศรษฐกิจรองรับการเรียนรู้ตลอดชีวิต จากการที่ธุรกิจปรับเปลี่ยนรูปแบบการทำงานเพื่อสร้างความอยู่รอด ทำให้เกิดการแสวงหาความรู้และทักษะใหม่ๆ ทั้งรูปแบบออนไลน์และออนไซต์

⇨ การเปลี่ยนแปลงวิธีดำเนินงาน และการปฏิบัติงานทางธุรกิจขององค์กร บนระบบอิเล็กทรอนิกส์ การทำงานบนคลาวด์ คอมพิวติ้ง

⇨ การนำเอาเทคโนโลยีสมัยใหม่มาใช้ในการดำเนิน เช่น BLOCKCHAIN

⇨ กฎเกณฑ์และข้อกำหนดให้องค์กรต้องมีความรับผิดชอบต่อสังคมและสิ่งแวดล้อม รวมทั้งมีเป้าหมายในการพัฒนาอย่างยั่งยืน

ทั้งนี้ COSO GUIDANCE ออกประกาศใช้ใหม่และสำคัญๆ ที่เกี่ยวข้องกับ COSO 2013 Internal Control – Integrated Framework (ICIF) ทำให้ทุกองค์กรต้องทำความเข้าใจเพิ่มเติมและนำไปประยุกต์ใช้เพื่อให้สามารถปฏิบัติในระบบการควบคุมภายในเพิ่มเติมได้อย่างเหมาะสม เป็นการเพิ่มเติมกรอบแนวทางดำเนินงานด้านการควบคุมภายในเฉพาะเรื่อง เพื่อนำมาใช้ในแต่ละสถานการณ์เพิ่มเติม หรือดึงเอาประโยชน์จากกรอบแนวทางการดำเนินงานด้านการควบคุมภายในที่เป็นหลักการทั่วไป ใน 5 องค์ประกอบ และ 17 หลักการมาใช้ในกระบวนการควบคุมภายใน COSO 2013 GUIDANCE ใหม่ประกอบด้วย

2.1 Enhancing Board Oversight

2.2 Improving Organizational Performance and Governance

2.3 COSO In the Cyber Age และ Managing Cyber Risk in A Digital Age

2.4 Blockchain and Internal Control

2.5 Internal Control over Sustainability Reporting: ICSR

การเพิ่มเติมในส่วน GUIDANCE ทั้งในระดับคณะกรรมการอำนวยการ และกรอบแนวทางการควบคุมภายในที่รองรับสภาพแวดล้อมทางธุรกิจที่เปลี่ยนแปลงไปจะทำให้มั่นใจว่ากรอบแนวทางดำเนินงาน

ตามมาตรฐาน COSO 2013 COSO Internal Control – Integrated Framework (ICIF) จะยังคงนำไปสู่การบรรลุวัตถุประสงค์ทางธุรกิจขององค์กร ผ่านการกำกับควบคุมความเสี่ยง ป้องกันการทุจริต ลดข้อผิดพลาดคลาดเคลื่อน การบริหารจัดการที่ไม่เหมาะสม เพื่อ

- ⇨ *เป็นเกราะป้องกันที่รักษาดูแลสินทรัพย์ขององค์กร รวมทั้งข้อมูลสำคัญที่ถือเป็นสินทรัพย์รูปแบบใหม่ ซึ่งทำให้ระบบการรักษาความปลอดภัยดีขึ้นทั้งในเชิงบริหาร ทางด้านกายภาพและในทางเทคนิค*
- ⇨ *เพิ่มประสิทธิภาพของการดำเนินงาน กระจายความรับผิดรับชอบต่อการดำเนินงาน ทำให้เกิดการแบ่งแยกหน้าที่ความรับผิดชอบที่อาจเกิดความผิดพลาดคลาดเคลื่อน กำจัดค่าใช้จ่ายหรือต้นทุนที่ไม่เกิดประโยชน์ ลดการสิ้นเปลืองหรือสูญเปล่า*
- ⇨ *ช่วยควบคุมกระบวนการในการเตรียมการเพื่อจะทำรายงาน ซึ่งทำให้รายงานสถานะการเงินและไม่ใช่การเงินมีความถูกต้อง ครบถ้วนและเชื่อถือได้*
- ⇨ *กำกับการปฏิบัติงานได้ครบถ้วนตามกฎหมายและกฎเกณฑ์ต่างๆ และยึดโยงอยู่บนความถูกต้องและชอบด้วยกฎหมาย มีจริยธรรมและจรรยาบรรณทางธุรกิจ*
- ⇨ *ทำให้องค์กรได้รับข้อมูลที่เกี่ยวข้องกับประเด็นความเสี่ยงอย่างเป็นระบบ เพื่อใช้ประกอบการตัดสินใจ และวิธีการปฏิบัติงานที่เหมาะสม*

แม้ว่ากรอบแนวทางการดำเนินงานด้านควบคุมภายใน จะออกแบบไว้เป็นมาตรฐานกลาง แต่การนำไปประยุกต์ใช้ในแต่ละองค์กรยังอาจจะมีความแตกต่างกัน เพื่อให้มีความเหมาะสมกับบริบทขององค์กร โครงสร้างการดำเนินงาน และขนาดของการประกอบการ โดยใช้รูปแบบของการควบคุมภายในที่แตกต่างกันออกไป ตั้งแต่การควบคุมในเชิงป้องกันและป้องปราม การควบคุมในเชิงหลีกเลี่ยง การควบคุมในลักษณะของการสอดส่องติดตามและตรวจจับความผิดปกติระหว่างการปฏิบัติงาน การควบคุมในลักษณะที่วางข้อห้ามและข้อจำกัด การควบคุมด้วยการตั้งสำรองเผื่อความเสียหายล่วงหน้าหรือภาระที่จะเกิดขึ้นในอนาคต และการควบคุมในลักษณะที่เข้าไปเยียวยาหรือลดผลกระทบของความเสียหาย

3. GUIDANCE on Enhancing Board Oversight

คณะกรรมการมีบทบาทสำคัญ และเป็นหลักในการกำหนดกลยุทธ์ จัดวางวัตถุประสงค์ระดับสูงขององค์กร จัดสรรทรัพยากร และยังเป็นผู้ให้แนวทางคำแนะนำและความรับผิดรับชอบที่มอบหมายให้แก่ฝ่ายจัดการหรือผู้บริหาร ทำให้มาตรฐานการควบคุมภายใน และมาตรฐานการบริหารความเสี่ยงจำเป็นต้องระบุบทบาทของการติดตามผลดำเนินงานในองค์รวมของคณะกรรมการ

GUIDANCE ฉบับนี้จึงเป็นหลักการพื้นฐานสำหรับจัดวางสภาพแวดล้อมภายในที่ดีในระดับบนขององค์กร กำหนดความรับผิดชอบของคณะกรรมการอำนวยการในการสร้างกรอบการกำกับดูแลองค์กรที่ดี (Governance) และการติดตามผลดำเนินงานในภาพรวม (Oversight) ขณะเดียวกันมีความคาดหวังว่า

คณะกรรมการจะมีส่วนร่วม และถือเป็นพันธะผูกพันในการดำเนินงานตลอดวงจรของการบริหารกลยุทธ์ในรอบปีงบประมาณ เนื่องจากความซับซ้อนของธุรกรรมทางธุรกิจ ความก้าวหน้าทางเทคโนโลยี ผลกระทบที่เกิดขึ้นจากสถานการณ์ที่มาจากต่างประเทศ อายุของวงจรผลิตภัณฑ์ที่มีแนวโน้มสั้นลง และการเปลี่ยนแปลงในภาพรวมของสภาพแวดล้อมได้เพิ่มขนาดและความซับซ้อนของความเสี่ยงที่องค์กรเผชิญตามไปด้วย

นอกจากนั้น คณะกรรมการอำนวยการยังมีภารกิจในการที่จะต้องทำการวิเคราะ ประเมิน และใช้ดุลพินิจในการตัดสินใจที่มีคุณภาพในระดับสูงเกี่ยวข้องกับการกำกับดูแลองค์กรที่ดี และดำเนินการติดตามผลการดำเนินงานขององค์กร เพื่อหลีกเลี่ยงทั้งสถานการณ์ความสุ่มเสี่ยงต่อการทุจริตและการบริหารความเสี่ยงขององค์กรให้มีประสิทธิผล

เนื้อหาสาระที่สำคัญของ GUIDANCE ฉบับนี้คือ

- ⇨ การนำเสนอโมเดลของการใช้ดุลพินิจที่ดีสำหรับคณะกรรมการ
- ⇨ กระบวนการที่ใช้ในการพิจารณาเพื่อกำหนดการตัดสินใจด้วยดุลพินิจ
- ⇨ กับดักที่สำคัญและมักเกิดขึ้นทั่วไปในการใช้ดุลยพินิจ
- ⇨ แนวทางการเพิ่มพูนความสามารถของคณะกรรมการต่อความท้าทายในการที่ต้องใช้ดุลยพินิจ

ดังนั้น แนวปฏิบัติฉบับนี้จึงมีส่วนที่เติมเต็มคู่มือการปฏิบัติงานในส่วนของคณะกรรมการ โดยเฉพาะในบทบาทที่เกี่ยวข้องกับการกำกับผลการดำเนินงาน ที่มาจากการขับเคลื่อนของฝ่ายจัดการหรือผู้บริหารระดับสูง

4. GUIDANCE on Improving Organizational Performance and Governance

GUIDANCE ฉบับนี้ให้คำอธิบายกรอบแนวทางการดำเนินงานของ COSO ในบริบทของมาตรฐานที่เน้นความเป็นผู้นำที่ต้องทำการกำกับดูแลและบริหารองค์กรสู่ความสำเร็จ โดยกรอบแนวทางการดำเนินงานดังกล่าวมุ่งที่จะบูรณาการกระบวนการกำกับดูแลกิจการและบริหารจัดการองค์กรด้านความรับผิดรับชอบต่อการควบคุมภายในให้บรรลุวัตถุประสงค์และการบริหารความเสี่ยงทั่วทั้งองค์กร เพื่อนำไปสู่ผลลัพธ์ที่ดีขึ้น เพราะองค์กรไม่สามารถประสบความสำเร็จได้ด้วยการดำเนินการเฉพาะการควบคุมภายในโดยไม่เชื่อมต่อสู่การบริหารความเสี่ยง

บริบทขององค์กรที่สอดคล้องตามพันธกิจ กำหนดให้องค์กรต้องดำเนินการออกแบบการดำเนินงานสู่ความสำเร็จของวัตถุประสงค์ ซึ่งนอกเหนือจากการพัฒนากลยุทธ์ แล้วยังต้องระบุความเสี่ยงที่จะมีผลกระทบต่อการบรรลุวัตถุประสงค์ และลดระดับความเสี่ยง เพื่อให้อยู่ภายในเกณฑ์ที่ยอมรับได้ โดยกรอบ

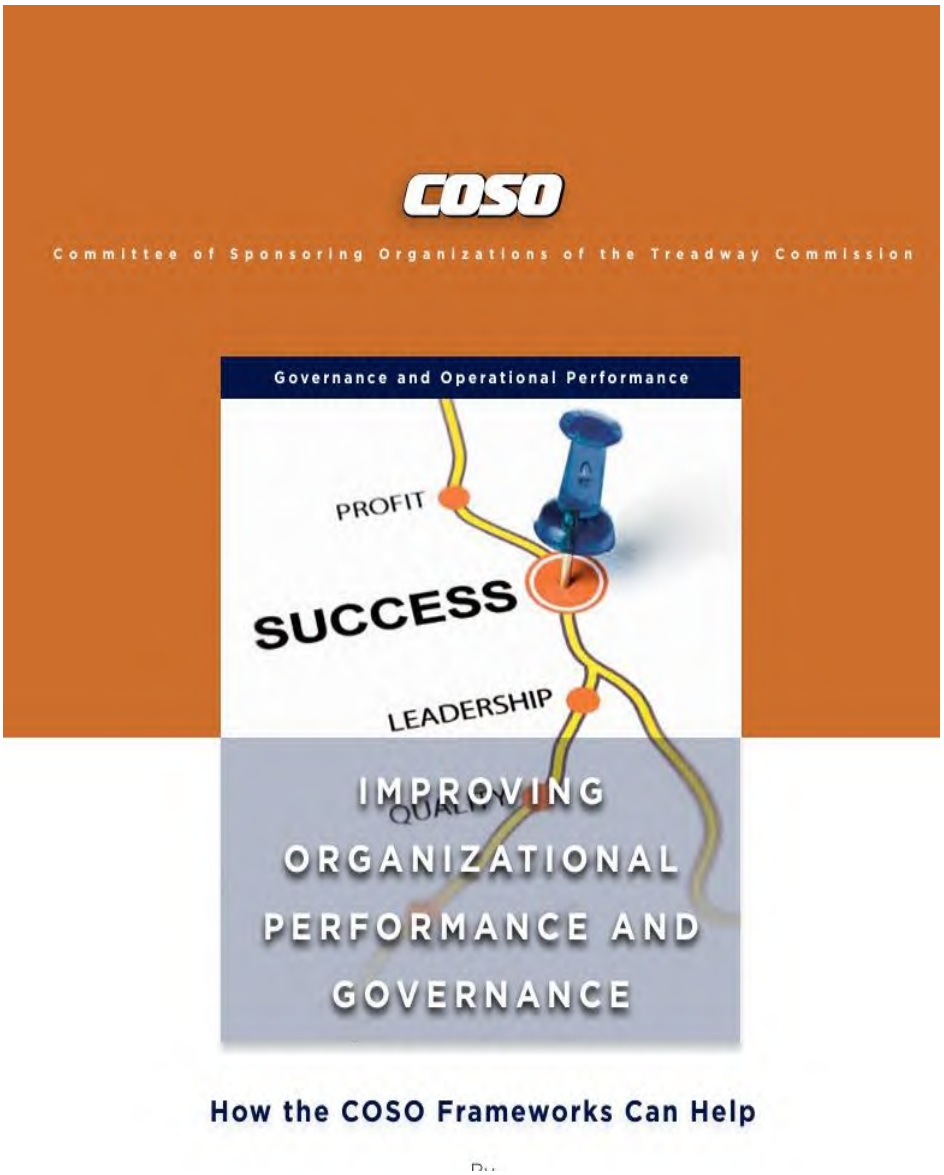
แนวทางดำเนินงานด้านการควบคุมภายในออกแบบมาให้ควบคุมความเสี่ยงเพื่อการบรรลุวัตถุประสงค์ด้วยการลดระดับลงมาอยู่ในเกณฑ์ที่ยอมรับได้ ในขณะที่กรอบการดำเนินงานด้านบริหารความเสี่ยงทั่วทั้งองค์กรขึ้นอยู่กับการกำหนดวัตถุประสงค์ การระบุการรับมือเพื่อลดระดับความเสี่ยง กรอบแนวทางการดำเนินงานทั้งสองส่วนจึงต้องผูกพันและดำเนินการคู่ขนานไปกับการดำเนินงานขององค์กร เพื่อนำไปสู่การบรรลุวัตถุประสงค์องค์กร โดยการบริหารความเสี่ยงทั่วทั้งองค์กร แทรกไว้ในกระบวนการบริหารกลยุทธ์องค์กร ขณะที่การควบคุมภายในเป็นการจัดการต่อความเสี่ยงภายหลังจากการกำหนดกลยุทธ์องค์กรแล้ว ภายใต้วัตถุประสงค์ที่กำหนดให้หน่วยงานในกลุ่มงานต่างๆ รับผิดชอบและรับมอบหมายในการดำเนินการ และมีส่วนในการปรับปรุงผลดำเนินงานขององค์กร

การบริหารความเสี่ยงทั่วทั้งองค์กร ในภาพรวมโดยทั่วไปเป็นการเกี่ยวข้องกับองค์ประกอบของการกำกับดูแลองค์กร และกระบวนการบริหารจัดการองค์กร ช่วยให้ผู้บริหารสามารถตัดสินใจบนฐานความเสี่ยงได้โดยใช้ข้อมูลความเสี่ยง การตอบสนองต่อความเสี่ยงตามข้อมูลที่มีอยู่ ครอบคลุมถึงการควบคุมภายในที่ปรับลดระดับความเสี่ยงที่เกี่ยวข้องกับการบรรลุวัตถุประสงค์ขององค์กรภายในเกณฑ์ความเสี่ยงที่ยอมรับได้ ทั้งสองส่วนนี้จึงมีความสัมพันธ์และเชื่อมโยงกัน

เนื้อหาสาระของ GUIDANCE ฉบับนี้ ประกอบด้วย

- ⇨ ***งานพิจารณาโมเดลธุรกิจในเชิงบริบทการดำเนินงาน***
- ⇨ ***กรอบแนวทางการดำเนินงานที่สำคัญต่อการกำกับดูแลองค์กร***
- ⇨ ***กรอบแนวทางการดำเนินงานเพื่อกำหนดกลยุทธ์และแผนธุรกิจ***
- ⇨ ***กรอบแนวทางการดำเนินงานเพื่อการบริหารจัดการขับเคลื่อนผลดำเนินงานองค์กร***
- ⇨ ***กรอบแนวทางการดำเนินงานเพื่อบริหารการติดตามผลดำเนินงาน***
- ⇨ ***กรอบแนวทางการดำเนินงานเพื่อการปรับตัวขององค์กร***
- ⇨ ***ตรอกแนวทางการดำเนินงานในส่วนของการบูรณาการงานควบคุมภายใน***

แนวปฏิบัติฉบับนี้มุ่งที่จะทำให้เห็นว่า คุณค่าของกรอบแนวทางการดำเนินงานด้านการควบคุมภายใน ควรจะมีส่วนที่ทำให้เกิดผลในเชิงประจักษ์ต่อการยกระดับผลการดำเนินงาน ในภาพรวมขององค์กร รวมทั้งการกำกับดูแลองค์กรที่ดีซึ่งส่วนหนึ่งเป็นเรื่องของการควบคุมภายใน



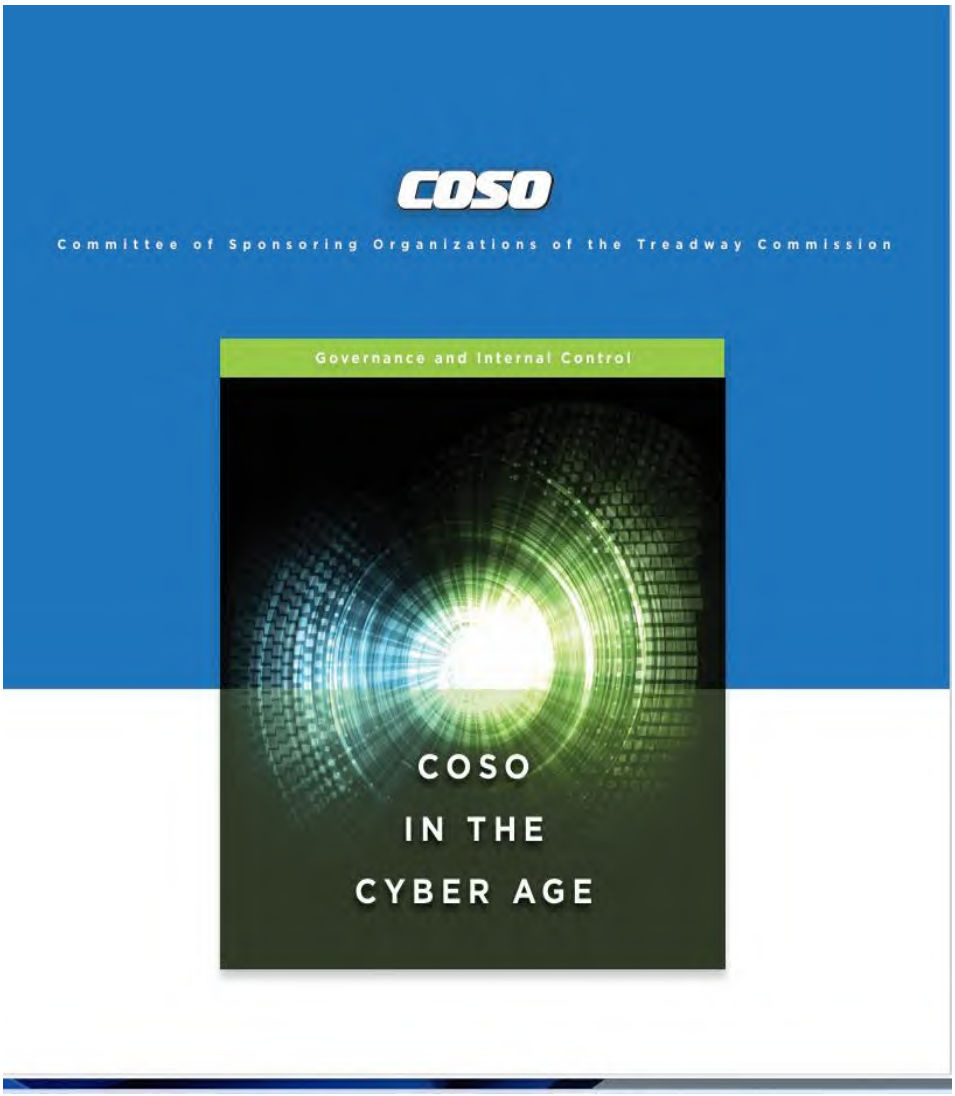
5. COSO in the Cyber Age และ Managing Cyber Risk in a Digital Age

วัตถุประสงค์ของ GUIDANCE ฉบับนี้ เพื่อเสริมกรอบแนวทางการบูรณาการด้านการควบคุมภายในและการบริหารความเสี่ยงทั่วทั้งองค์กรเมื่อองค์กรต่างๆ จำเป็นต้อง พิจารณาประเด็นที่เกี่ยวข้องกับความเสี่ยงด้านการรักษาความปลอดภัยทางไซเบอร์ เพื่อช่วยให้แนวคิด ในเชิงประสิทธิภาพและประสิทธิผลสำหรับการวิเคราะ ประเมินและบริหารความเสี่ยงดังกล่าว โดยกรอบแนวทางการดำเนินงาน จะให้โครงสร้าง ที่จะนำองค์กรสู่การระบุประเด็นความเสี่ยงทางไซเบอร์ผ่านมุมมองของ COSO

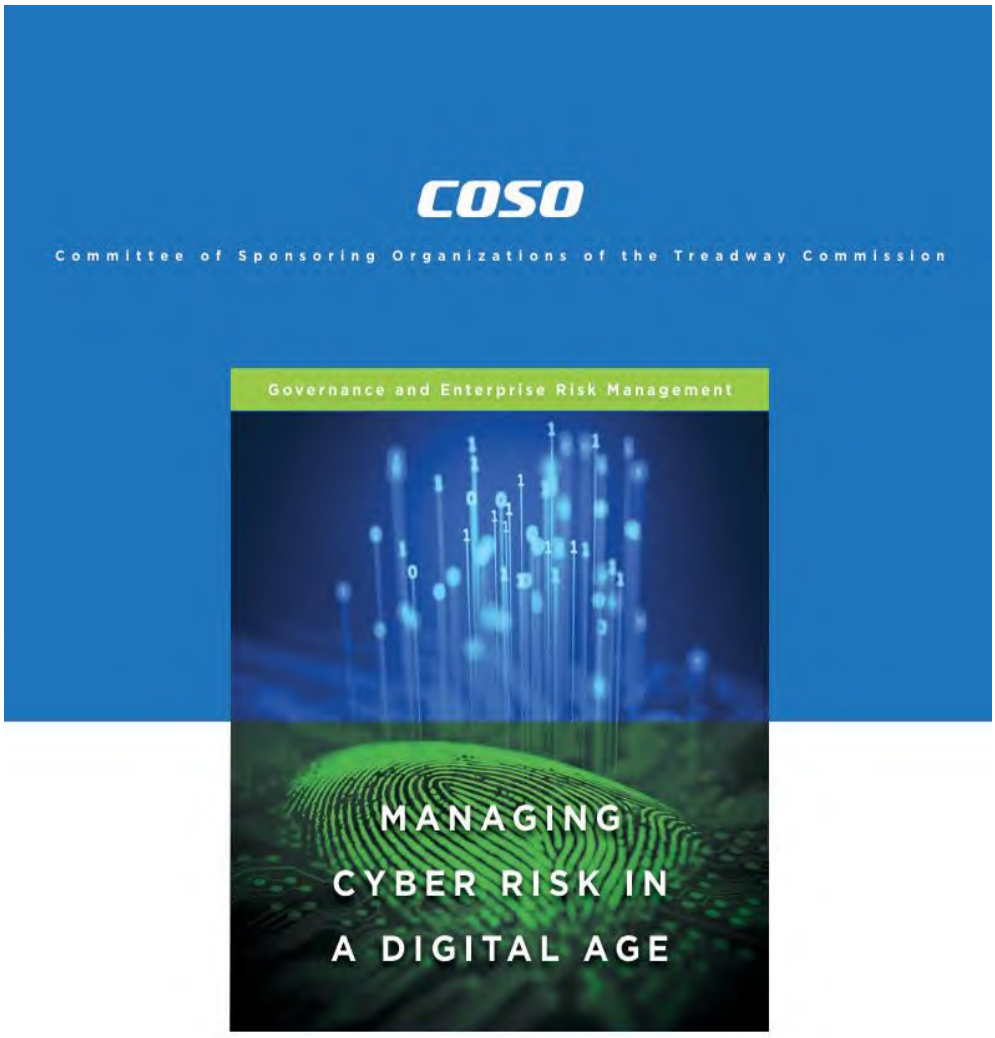
นอกจากนั้น COSO ยังเห็นความจำเป็นที่องค์กรต่างๆ จำเป็นต้องใช้และพึ่งพาเทคโนโลยีในวัตถุประสงค์การควบคุมภายในเพิ่มมากขึ้น การวิเคราะห์และประเมินเพื่อสร้างการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ และการบริหารนวัตกรรมด้านไอทีที่เกิดใหม่ขึ้นตามลำดับ ควบคู่กับความซับซ้อนของกระบวนการดำเนินงานทางธุรกิจที่พึ่งพาทางด้านเทคโนโลยีเพิ่มขึ้น ข้อมูลที่กลายเป็นสินทรัพย์สำหรับการ

ดำเนินงานที่สำคัญของทุกองค์กร ตลอดจนความจำเป็นในการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับการปฏิบัติงานทางอิเล็กทรอนิกส์ หรือกฎหมายที่เกี่ยวข้องกับไอที ทั้งนี้เพื่อให้องค์กรสามารถจัดการวางมาตรการควบคุมภายในที่จะช่วยลดอุบัติการณ์ไม่พึงประสงค์ทางไซเบอร์ที่จะมีผลกระทบทางลบ ต่อสถานะการเงิน การหยุดชะงักของการดำเนินงาน ตลอดจนชื่อเสียงภาพลักษณ์ขององค์กร

GUIDANCE ได้นำเสนอกรอบแนวทางการวิเคราะห์และประเมินความเสี่ยงไซเบอร์ นำไปสู่กิจกรรมการควบคุมและการสื่อสารข้อมูล สถานะความเสี่ยงทางไซเบอร์ภายในองค์กร และภายนอกองค์กร ตามความจำเป็นซึ่งเป็นส่วนที่เกี่ยวข้องกับองค์ประกอบที่ 2 – 4 จาก 5 องค์ประกอบของมาตรฐานการควบคุมภายใน ยกเว้นส่วนที่เกี่ยวข้องกับสภาพแวดล้อมการควบคุมในองค์ประกอบที่ 1 และการติดตามผลดำเนินงานเพื่อปรับปรุงแก้ไขในองค์ประกอบที่ 5



การใช้งานควบคู่กับ Managing Cyber Risk in a Digital Age



ในส่วนของมาตรฐานด้านการบริหารความเสี่ยง COSO ERM 2017 – Integrating with Strategy & Performance ได้มีการออก GUIDANCE ในลักษณะที่ใกล้เคียงกัน โดยวัตถุประสงค์ของ GUIDANCE ฉบับนี้ คือการนำเสนอภาพรวมของการบริหารธุรกิจและบทบาทของคณะกรรมการอำนวยการต่อการบริหารจัดการความเสี่ยงทางไซเบอร์ ด้วยการใช้หลักเกณฑ์ กรอบการดำเนินงานตามมาตรฐาน COSO เพื่อให้บริบทที่เกี่ยวข้องกับแนวคิดพื้นฐานเทคนิคการบริหารความเสี่ยงทางไซเบอร์ แต่ไม่รวมถึงการพัฒนากลยุทธ์ในเชิงเทคนิค

GUIDANCE ฉบับนี้จึงช่วยให้คณะกรรมการสามารถทำความเข้าใจ ต่อประเด็นที่จะนำไปใช้ในการติดตามผลดำเนินงานการบริหารกระบวนการทางไซเบอร์ที่ต้องมีแผนดำเนินงานจัดการความเสี่ยงด้านไซเบอร์ที่เหมาะสม ขณะเดียวกันก็ช่วยให้คณะกรรมการตรวจสอบสามารถเข้าใจประเด็นหลัก และตัวอย่างของ

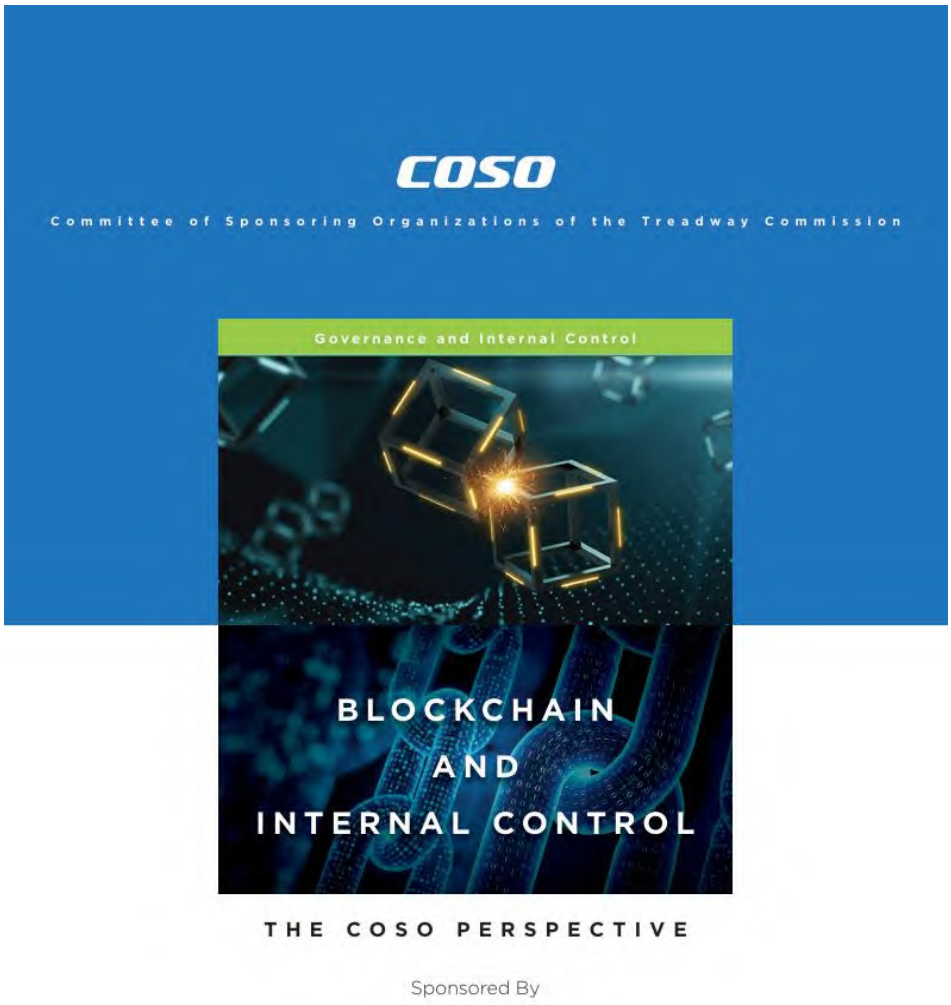
การบริหารกลยุทธ์ความเสี่ยงด้านไซเบอร์ ขณะที่ผู้บริหารองค์การในระดับสูงก็จำเป็นต้องมีความเข้าใจต่อประเด็นทิศทางของการบริหารความเสี่ยงด้านไซเบอร์ด้วย

การจัดทำ GUIDANCE ทั้งสองฉบับนี้ ทำให้เห็นได้ชัดเจนว่า COSO ให้ความสำคัญกับการจัดวางกรอบแนวทางดำเนินงานด้านการควบคุมภายในเพื่อกำกับกระบวนการปฏิบัติงานภายในองค์กร และกรอบแนวคิดในเชิงกลยุทธ์เพื่อจัดการความเสี่ยงไซเบอร์ที่มาจากการเปลี่ยนแปลงวิธีการบริหารจัดการ กลยุทธ์ในยุคดิจิทัล จนทำให้องค์กรมีความเสี่ยงไซเบอร์ที่ต้องเผชิญหน้าจากสภาพแวดล้อมภายนอก และมีผลกระทบต่อการบรรลุความสำเร็จเชิงกลยุทธ์

6. Blockchain and Internal Control

จากการที่ Blockchain ได้กลายเป็นองค์ประกอบส่วนหนึ่งของการดำเนินงานและการบริหารความสัมพันธ์ขององค์กรเพิ่มขึ้น จึงเห็นสมควรที่จะมุ่งเน้นการนำเอาเทคโนโลยีนี้มาใช้ภายในองค์กรภายใต้การควบคุมภายในที่ดี ด้วยการเสนอให้แต่ละองค์กร ประยุกต์ใช้และบูรณาการ Blockchain ภายในองค์กรด้วยความระมัดระวังบนความเข้าใจต่อศักยภาพและความเสี่ยงของ Blockchain เพื่อนำมาสร้างการควบคุมภายในที่เหมาะสม อีกทั้งแนวโน้มในอนาคต ที่จะมีเครื่องมือซึ่งส่งเสริมให้ต้องนำ Blockchain มาใช้มีแนวโน้มเพิ่มขึ้น เนื่องจากมีโอกาสที่จะช่วยเพิ่มประสิทธิภาพและประสิทธิผลของการดำเนินงาน ปรับปรุงและทำให้การตอบสนองต่อการจัดทำรายงานทางการเงินและรายงานอื่นๆมีความคล่องตัวมากขึ้น และยังช่วยในการกำกับการปฏิบัติตามกฎเกณฑ์ของกฎหมายที่จะเกิดใหม่ในอนาคตเกี่ยวกับ Blockchain อีกด้วย

GUIDANCE ฉบับนี้จึงเป็นความพยายามที่จะนำเสนอแนวคิดเชิงประสิทธิภาพและประสิทธิผลที่จะช่วยให้องค์กรสามารถออกแบบการควบคุม และประยุกต์ใช้การควบคุม ในส่วนที่เกี่ยวข้องกับความเสี่ยงจาก Blockchain ได้ดีขึ้น โดยครอบคลุมถึง การกำกับดูแลผลดำเนินงานในองค์รวม ประเด็นความเสี่ยงและการควบคุมเพื่อให้ได้มาซึ่งรายงานทางการเงินที่เหมาะสมในอนาคต จากการที่องค์กรจำเป็นต้องใช้ ฐานข้อมูล (Database) ที่มีลักษณะกระจายออกจากส่วนกลาง มีการแบ่งปันข้อมูล และการบันทึกข้อมูลซึ่งต้องการการกำกับดูแลที่เข้มงวดและชัดเจนมากขึ้น



7. Achieving Effective Internal Control over Sustainability Reporting

จากการที่ผู้มีส่วนได้ส่วนเสียและภาคสาธารณะมีความคาดหวังให้องค์กรต่างๆ ต้องทำการเปิดเผยข้อมูลที่เกี่ยวข้องกับการกำกับดูแลส่วนที่เป็นความรับผิดชอบต่อสังคมและสิ่งแวดล้อมเพิ่มขึ้น ทำให้องค์กรมีความจำเป็นต้องจัดทำข้อมูลทางธุรกิจที่อยู่บนเป้าหมายด้านความยั่งยืน ไม่ว่าจะเป็นข้อมูลที่ไม่ใช่การเงิน ข้อมูลที่เกี่ยวข้องกับ Balanced Scorecard หรือ ESG เพื่อช่วยแสดงถึงผลดำเนินงานขององค์กร ที่เป็นความรับผิดชอบต่อสังคมและสิ่งแวดล้อม รวมทั้งอยู่บนเป้าหมายในการพัฒนาอย่างยั่งยืนทางเศรษฐกิจและสังคม และเปิดเผยข้อมูลที่เป็นไปตามความคาดหวังของผู้มีส่วนได้ส่วนเสียเพื่อช่วยองค์กรในการบริหารความสัมพันธ์กับผู้มีส่วนได้ส่วนเสียด้วย

ด้วยความจำเป็นในการบูรณาการ ระหว่างประเด็นของเป้าหมายการพัฒนาอย่างยั่งยืน กับข้อกำหนดและเงื่อนไขทางการเงิน ทำให้องค์กรมีความจำเป็นต้องปรับปรุงการควบคุมภายใน เพื่อนำไปสู่การจัดทำรายงานสำหรับบริหารองค์กรภายในและเปิดเผยต่อภายนอกในส่วนที่เกี่ยวข้องกับการพัฒนาอย่างยั่งยืน โดยต้องปรับปรุงคุณภาพของข้อมูล และบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับการบริหารข้อมูลดังกล่าว จนถึงกระบวนการที่นำข้อมูลเข้าสู่ระบบบัญชีและการรายงานทางการเงิน โดยข้อมูลที่รวบรวมได้จากการ

ดำเนินงานด้านความยั่งยืนมีแหล่งที่มาทั้งภายในองค์กรเอง และแหล่งที่มาจากองค์กรในห่วงโซ่อุปทาน ตลอดจนผู้ที่ได้รับผลกระทบทางสังคมและสิ่งแวดล้อมจากผลดำเนินงานขององค์การหรือ องค์กรในห่วงโซ่อุปทาน ทำให้ความเสี่ยงที่เกี่ยวข้องในส่วนนี้จำเป็นต้องมีการควบคุมภายในที่มีความทันสมัย น่าเชื่อถือ ได้รับการยอมรับเมื่อมีการจัดทำเป็นรายงาน และนำเสนอข้อมูล รวมทั้งเปิดเผยต่อหน่วยงาน

COSO ได้เข้ามานำเสนอกรอบแนวทางการดำเนินการเพื่อบูรณาการมาตรฐานการควบคุมภายใน กับกิจกรรมและข้อมูลทางธุรกิจบนเป้าหมายของความยั่งยืน ด้วยการใช้องค์ประกอบทั้ง 5 ประการ และหลักการ 17 หลักการตามกรอบแนวทางการบูรณาการการควบคุมภายใน เพื่อให้แต่ละองค์กรจะวางระบบการควบคุมที่มีประสิทธิภาพ และบูรณาการสำหรับข้อมูลการดำเนินงานบนเป้าหมายเพื่อความยั่งยืนได้ดียิ่งขึ้น โดยการพัฒนาระบบการควบคุมภายในดังกล่าวมีความคล้ายคลึงกับการควบคุมภายในที่เกี่ยวข้องกับรายงานทางการเงิน เพียงแต่อยู่บนวัตถุประสงค์ของการดำเนินงานที่มีความรับผิดชอบด้านความยั่งยืนเฉพาะตัวของแต่ละองค์กร และสอดคล้องกับความคาดหวังของผู้มีส่วนได้ส่วนเสียของแต่ละองค์กร

8. การนำมาตรฐาน COSO 2013 และ GUIDANCE สู่การใช้ประโยชน์

การที่องค์กรจะนำเอามาตรฐาน COSO 2013 พร้อมทั้ง GUIDANCE ที่มีการพัฒนาเพิ่มเติมภายหลังจากปี 2013 มาใช้ประโยชน์ จำเป็นต้องดำเนินการตามขั้นตอนดังนี้

⇨ ***ทำความเข้าใจต่อกรอบแนวทางการดำเนินงานตามมาตรฐาน COSO 2013 ให้ชัดเจนเป็นลำดับแรก ในส่วนของรายละเอียด***

ความล้มเหลวของการพัฒนาระบบการควบคุมภายในตามมาตรฐาน COSO 2013 ส่วนหนึ่งเกิดจากการไม่พยายามทำความเข้าใจถึงองค์ประกอบและหลักการของมาตรฐานว่า

(ก) มีการกำหนดรายละเอียดและเนื้อหาที่มุ่งหวังจะปรับปรุงประสิทธิภาพในการควบคุมภายในขององค์กรอย่างไร ในแต่ละองค์ประกอบต้องนำไปดำเนินการอย่างไร

(ข) ผู้ที่ต้องมีส่วนเกี่ยวข้องในการดำเนินการควรเป็นบุคลากรในส่วนใด มีคุณสมบัติและสมรรถนะที่เกี่ยวข้องอย่างไร เพื่อให้มั่นใจว่าจะทำให้ระบบการควบคุมภายในขององค์กรมีความเข้มแข็ง โปร่งใส อยู่บนหลักการของความรับผิดรับชอบที่ดี

⇨ ***ทำความเข้าใจต่อข้อเสนอของ COSO ที่เกี่ยวกับการจัดโครงสร้างความรับผิดชอบเพื่อรองรับการพัฒนาระบบการควบคุมภายในบนกรอบแนวทาง THE THREE LINES OF DEFENSE MODEL ที่จะแบ่งหน่วยงานออกเป็น 3 กลุ่ม ประกอบด้วย 1st Line กลุ่มงาน 2nd Line และกลุ่มงาน 3rd Line***

องค์กรที่ประสบความล้มเหลวในการพัฒนาระบบการควบคุมภายในตามมาตรฐาน COSO 2013 คือองค์กรที่ใช้โครงสร้างองค์กรที่มีการจัดวางและกำหนดขึ้นโดยผู้บริหารและคณะกรรมการ และใช้ขอบเขตภาระงานที่มีการมอบหมายให้แก่ผู้ปฏิบัติงานแต่ละหน่วยงานไปใช้ในการพัฒนาระบบการควบคุมภายใน ขณะที่ COSO เสนอว่า

(ก) องค์กรจำเป็นต้องมีการจัดทำโครงสร้างความรับผิดรับชอบที่จะนำไปสู่การมอบหมายให้เกิดการควบคุมภายในแยกต่างหากบนหลักการของ THE THREE LINES OF DEFENSE MODEL

(ข) ความเชื่อมโยงระหว่างหน่วยงานในแต่ละกลุ่มงาน ภายใต้ THE THREE LINES OF DEFENSE MODEL จำเป็นต้องกำหนดให้ชัดเจน เพื่อให้มั่นใจว่าการควบคุมภายในจะมีลักษณะบูรณาการ

(ค) บทบาทและความรับผิดชอบของคณะกรรมการในการกำกับผลดำเนินงานในภาพรวม

(ง) บทบาทและความรับผิดชอบของผู้บริหารระดับสูงในฐานะฝ่ายจัดการที่ต้องขับเคลื่อนให้เกิดผลดำเนินงาน และระบบการควบคุมภายในที่ดี

⇨ ***นำผลที่ได้จากการทำความเข้าใจต่อกรอบแนวทางการดำเนินงานตามมาตรฐาน COSO 2013 และ THE THREE LINES MODEL มากำหนดถึงความจำเป็นขององค์กรที่จะนำมาใช้ ภายใต้เงื่อนไขและหลักเกณฑ์ที่ไม่ต่ำกว่าข้อกำหนดของมาตรฐาน***

เมื่อนำเอาหลักการ เงื่อนไข ข้อกำหนด ตามมาตรฐาน COSO 2013 ตลอดจน THE THREE LINES OF DEFENSE MODEL มาพิจารณาในฐานะที่เป็นแนวปฏิบัติที่ดี จะทำให้องค์กร

(ก) สามารถระบุช่องว่างของการดำเนินการที่ยังไม่เป็นไปตามมาตรฐาน

(ข) สามารถระบุช่องว่างของโครงสร้างองค์กร ที่ยังจำเป็นต้องแยกหน่วยงานออกเป็น 3 กลุ่มงานตาม THE THREE LINES OF DEFENSE MODEL

(ค) สามารถเปิดให้มีการรับฟังความคิดเห็น ข้อเสนอแนะเกี่ยวกับการปิดช่องว่างทั้งส่วนของการดำเนินการและช่องว่างในส่วนของโครงสร้างองค์กร

(ง) สามารถกำหนดผู้ที่มีส่วนร่วมสำคัญในการดำเนินการที่สามารถช่วยให้ปิดช่องว่างแต่ละประเด็นได้อย่างมีประสิทธิภาพและประสิทธิผล

⇨ ***จัดทำการออกแบบแผนการดำเนินงานเพื่อการพัฒนาระบบการควบคุมภายในให้เป็นไปตามมาตรฐาน***

การนำเอากิจกรรมที่เกี่ยวข้องกับการปิดช่องว่างมาพัฒนาเป็นแผนดำเนินงาน

(ก) กำหนดวัตถุประสงค์ของแผนดำเนินงานแต่ละแผน

(ข) กำหนดกรอบเวลา

(ค) กำหนดทรัพยากรที่จำเป็น

(ง) กำหนดผู้รับผิดชอบหลัก

(จ) กำหนดผู้ที่ต้องร่วมมือในฐานะผู้มีส่วนได้ส่วนเสีย ผู้กำกับดูแล

(ฉ) กำหนดการสนับสนุนและความช่วยเหลือจากผู้เชี่ยวชาญ ที่ปรึกษา ในส่วนที่เป็นรายละเอียด เนื้อหาของนโยบาย วิธีดำเนินการ เอกสารแบบฟอร์ม คู่มือการปฏิบัติ การกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้และค่าเบี่ยงเบนความเสี่ยงที่ยอมรับได้ เครื่องมือในการติดตามและประเมินผล ตลอดจนรูปแบบของรายงานที่เกี่ยวข้อง

(ช) ออกแบบระบบงาน เพื่อใช้รองรับกระบวนการควบคุมภายในทั้งวงจร

(ซ) ออกแบบระบบรายงาน ที่ต้องนำเสนอหรือรับรองเพื่อให้ความเชื่อมั่นต่อผู้บริหารและคณะกรรมการ

(ฌ) ออกแบบวิธีการสื่อสาร การเปิดเผยข้อมูล การนำข้อมูลสารสนเทศมาใช้ประโยชน์ภายในองค์กรในเชิงบริหาร และเปิดเผยต่อบุคคลภายนอก

⇨ การนำเอาสิ่งที่ออกแบบไว้สู่การขับเคลื่อนและบังคับใช้ในภาคปฏิบัติ โดยเน้นการบูรณาการของการควบคุมภายใน

(ก) ออกประกาศใช้นโยบายกรอบแนวทางดำเนินงานด้านการควบคุมภายใน ที่ผ่านความเห็นชอบจากคณะกรรมการ

(ข) ออกประกาศนโยบายการขับเคลื่อนการควบคุมภายในที่ลงนามโดยผู้บริหารระดับสูงสุดให้เป็นไปตามนโยบายที่คณะกรรมการให้ความเห็นชอบ

(ค) ออกคำสั่งมอบหมายผู้ที่รับผิดชอบดำเนินงานตามนโยบายการขับเคลื่อนการควบคุมภายใน พร้อมตรวจชี้วัดผลดำเนินงาน วิธีการรายงานผลดำเนินงาน

(ง) ออกคำสั่งกำหนดโครงสร้างการควบคุมภายใน ตามกรอบ THE THREE LINES OF DEFENSE ที่ยึดโยงกับโครงสร้างองค์กร (Organization Chart) ที่กำหนดไว้

(จ) ออกคำสั่งกำหนดอำนาจกระทำการ หน้าที่ ความรับผิดชอบ กรณีที่มีการจัดตั้งคณะทำงาน หรือผู้กำกับดูแลผลดำเนินงานด้านการควบคุมภายในในองค์รวม ภายใต้ความรับผิดชอบของผู้บริหารระดับสูงสุดขององค์กร

(ฉ) ออกประกาศใช้คู่มือการดำเนินงานด้านการควบคุมภายใน ที่ครอบคลุมผู้รับผิดชอบดำเนินงานตามนโยบายการขับเคลื่อนการควบคุมภายใน

(ช) ออกประกาศกำหนดปฏิทินกิจกรรมการดำเนินงานด้านการควบคุมภายในประจำปี

(ซ) กำหนดและออกแบบกระบวนการหลักขององค์กร ภายใต้ THE THREE LINES

(ฌ) จัดให้มีการฝึกอบรม เพื่อให้ความรู้ ตั้งแต่ระดับนโยบาย คู่มือการดำเนินงานด้านการควบคุมภายใน การใช้งานระบบงานรองรับการควบคุมภายใน รูปแบบของเอกสาร แบบฟอร์ม สเปรดชีต แพตฟอร์ม แอพพลิเคชั่นที่เกี่ยวข้อง

(ญ) ขึ้นทะเบียนผู้รับผิดชอบดำเนินงานด้านการควบคุมภายในแต่ละหน่วยงานย่อย เพื่อทำหน้าที่ประสานงานและเป็นจุดที่ติดต่อและรับเรื่อง รวมทั้งอำนวยการตามปฏิทินกิจกรรมการดำเนินงานด้านการควบคุมภายในประจำปี

(ฎ) ออกประกาศกำหนด วิธีการ ขั้นตอนการดำเนินการในการนำเสนอผลการควบคุมภายในต่อคณะกรรมการ หรือคณะอนุกรรมการเฉพาะ มีองค์คณะตามโครงสร้างที่ดูแลด้านการควบคุมภายใน

⇨ ***การเชื่อมโยงระหว่างกรอบแนวทางการดำเนินงานด้านการควบคุมภายใน กับการส่งต่อสู่ระบบการบริหารจัดการความเสี่ยงที่รองรับความจำเป็นในระดับกลยุทธ์***

(ก) ออกประกาศกำหนดวิธีการ กระบวนการและขั้นตอนการดำเนินงานในการเชื่อมโยงและบูรณาการควบคุมภายในสู่งานบริหารความเสี่ยง

(ข) การเชื่อมโยงระบบงานการควบคุมภายใน การบริหารความเสี่ยง และการตรวจสอบภายในภายใต้ THE THREE LINES

(ค) การพัฒนาเครื่องมือเพื่อเชื่อมโยง ประเด็นความเสี่ยงในระดับ การควบคุมภายใน ความเสี่ยงในระดับบริหารความเสี่ยง และความเสี่ยงในขอบเขตของงานตรวจสอบภายใน เช่น ธีมความเสี่ยง แผนที่ความเสี่ยง เกณฑ์ความเสี่ยงที่ยอมรับได้ ค่าเบี่ยงเบนความเสี่ยงที่ยอมรับได้ ตัวชี้วัดติดตามผลการควบคุมภายใน ตัวชี้วัดนำด้านความเสี่ยง เกณฑ์การจัดระดับความเสี่ยง เกณฑ์การประเมินความเพียงพอและประสิทธิผลของการควบคุมภายใน เป็นต้น

(ง) การพัฒนาวิธีการและช่องทางในการสื่อสาร ข้อมูลความเสี่ยงที่เชื่อมโยงระบบงานการควบคุมภายใน การบริหารความเสี่ยง และการตรวจสอบภายในภายใต้ THE THREE LINES

บทที่ 1
จรรยาบรรณวิบัติด้านการควบคุมภายใน
- จุดพลุ COSO Internal Control

1. เริ่มเรื่องเมื่อเกิดวิกฤติ ENRON

วิกฤติการณ์ในตลาดหลักทรัพย์ของสหรัฐในปี 2001 – 2002 สร้างความเปลี่ยนแปลงไม่แต่เฉพาะกับบริษัทจดทะเบียนในตลาดหลักทรัพย์ของสหรัฐ แต่สร้างความเปลี่ยนแปลงกับผู้ประกอบการในองค์กรประเภทต่าง ๆ ทั่วโลกด้วย เนื่องจากสภาคองเกสของสหรัฐได้ผ่านกฎหมายชื่อ Sarbanes-Oxley Act of 2002 (SOX)

ซึ่งกำหนดหลักเกณฑ์และเงื่อนไขใหม่เป็นครั้งแรกในประวัติศาสตร์โลกว่าให้องค์กรที่เป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์ในสหรัฐต้องจัดทำรายการทางการเงินที่เชื่อถือได้และเปิดเผยอย่างโปร่งใส

การเกิดขึ้นของระบบการควบคุมภายใน เป็นมาตรการแบบวัวหายล้อมคอก ภายหลังจากการทุจริตระดับนโยบายขึ้นในบริษัท ENRON

เงื่อนไขของกฎหมาย SOX มาตรา 404 กำหนดให้ผู้บริหารของบริษัทและผู้ตรวจสอบบัญชีภายนอกต้อง

(1) จัดทำรายงานผลดำเนินงานด้านการควบคุมภายในต่อรายงานทางเงินขององค์กร

(2) เพิ่มเติมความเห็นเกี่ยวกับผลดำเนินงานด้านการควบคุมภายในประกอบการเปิดเผยผลประกอบการทางการเงินรายไตรมาสและรายปีขององค์กร

(3) นำส่งข้อมูลตาม (1) และ (2) ให้แก่คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (SEC) ของสหรัฐ

นอกจากนั้น SEC หรือตลาดหลักทรัพย์ของสหรัฐได้ออกประกาศเพิ่มเติมที่อาศัยเงื่อนไขตามมาตรา 404 ของกฎหมาย SOX ที่กำหนดให้บริษัทมหาชนที่จดทะเบียนในตลาดหลักทรัพย์ต้อง

1) รายงานผลการประเมินจุดอ่อนของการควบคุมภายในและเปิดเผยไว้ในรายงานของคณะกรรมการตรวจสอบ
2) รายงานผลการตรวจสอบบัญชีเกี่ยวกับจุดอ่อนของการควบคุมภายในและเปิดเผยไว้ในรายงานผู้สอบบัญชี

โดยเปิดเผยข้อมูลรายงานดังกล่าวต่อสาธารณชนผ่านการนำส่งรายงานจากองค์กรที่เปิดเผยต่อ SEC ของสหรัฐและต่อสาธารณชนอย่างสม่ำเสมอ

หลักเกณฑ์และเงื่อนไขดังกล่าวได้สร้างภาระเพิ่มเติมแก่ทั้งผู้บริหารองค์กรและผู้สอบบัญชี

- ⇨ *จนทำให้ทั้งสองกลุ่มต้องแสวงหากรอบแนวคิดด้านการควบคุมภายในที่ดีเพื่อนำมาใช้เป็นกระบวนการดำเนินการให้มีระบบการควบคุมภายในที่ดีและรายงานผลดำเนินงานการควบคุมภายในอย่างต่อเนื่อง*
- ⇨ *กรอบแนวคิดของ COSO 1992 Internal Control – Integrated Framework ได้รับการยอมรับว่าน่าเชื่อถือและเหมาะสมในการนำไปใช้ประเมินความเพียงพอของการควบคุมภายในขององค์กรได้*
- ⇨ *เริ่มมีการจัดทำรายงานผลดำเนินงานด้านการควบคุมภายในและเปิดเผยข้อมูลตั้งแต่ปีงบประมาณสิ้นสุด หรือหลังจากวันที่ 15 พฤศจิกายน 2004*

ผู้สอบบัญชีเพิ่มการตรวจสอบและออกรายงานตรวจสอบระบบควบคุมภายใน

ผลการเปลี่ยนแปลงเงื่อนไขทางกฎหมายดังกล่าวทำให้ผู้สอบบัญชีภายนอกต้องมีการปรับตัวตามไปด้วย มาอ้างอิงตามมาตรฐาน Auditing Standard No.2 (AS2) ของ Public Company Accounting Oversight Board (PCAOB) เพื่อ

- ⇨ ***ให้มั่นใจว่ามาตรฐานการตรวจสอบจะมีแนวทางการตรวจประเมินผลดำเนินงานด้านการควบคุมภายในที่สอดคล้องกับ COSO 1992 ซึ่งมุ่งเน้นการประเมินการควบคุมภายใน***
- ⇨ ***จากที่เคยให้ความสำคัญกับการควบคุมระดับหน่วยงานย่อย (Bottom-up) และจำกัดเฉพาะการควบคุมตามขอบเขตหน้าที่ความรับผิดชอบระดับสายงาน (Control-centric Approach) สู่การให้ความสำคัญกับการกำกับการควบคุมโดยผู้บริหาร (Top-down)***
- ⇨ ***เน้นการควบคุมตามฐานความเสี่ยง (Risk – based Approach) เพื่อให้การควบคุมภายในครอบคลุมการดำเนินงานโดยรวมและเน้นธุรกรรมหลักขององค์กร***

2. วิกฤติแฮมเบอร์เปลี่ยน COSO 1992 สู่ COSO 2013

- มาตรฐานการควบคุมภายในตามกรอบแนวคิด COSO 1992 ใช้เป็นกรอบแนวทางในการจัดวางระบบควบคุมภายในขององค์กรต่าง ๆ ทั้งในสหรัฐและองค์กรต่าง ๆ ทั่วโลกมานานหลายสิบปี
- จนกระทั่งมีการทบทวนโดย COSO และออกมาตรฐานใหม่มาทดแทนเรียกว่า COSO 2013 – Internal Control – Integrated Framework และใช้กันมาจนถึงปัจจุบัน
- ซึ่งก็ยังคงเป็นมาตรฐานที่ได้รับการยอมรับว่าน่าเชื่อถือและสามารถรองรับการดำเนินงานได้เพียงพอตามกฎหมาย SOX Act

การเกิดวิกฤติแฮมเบอร์เกอร์พิสูจน์ว่ามาตรฐานควบคุมภายในเดิมเอาไม่อยู่ เมื่อแต่ละกิจการทำผิดตามอย่างกันจนเป็นจรรยาบรรณวิบัติทั้งระบบ จนเกิด COSO 2013

ผลการสำรวจหลังเกิดวิกฤตแฮมเบอร์เกอร์

อย่างไรก็ตาม ประเด็นที่พบในการสำรวจและวิจัยตลาดของสถาบันและองค์กรต่าง ๆ เกี่ยวกับการนำกรอบแนวคิด COSO Internal Control มาใช้ในองค์กรไม่ว่าจะเป็น COSO 1992 หรือแม้แต่ COSO 2013 ซึ่งใช้มาถึง 5 ปีแล้วจนถึงปัจจุบัน มีจุดน่าสนใจบางประการได้แก่

ประการที่ 1 **มองว่าเป็นเพียงการทำรายงานกระดาษนำส่งหน่วยงานกำกับ**

องค์กรส่วนใหญ่นำเอากรอบแนวคิด COSO Internal Control มาใช้เพราะมีความวิตกกังวลว่า ผู้บริหารต้องจัดทำรายงานผลดำเนินงานด้านการควบคุมภายในและนำส่ง SEC เพื่อเปิดเผยข้อมูลต่อสาธารณชนตามมาตรา 404 ของกฎหมาย SOX เป็นสำคัญ

ผลการสำรวจดังกล่าวสะท้อนว่า ผู้บริหารขององค์กรกังวลต่อการจัดทำรายงานให้เป็นไปตามเงื่อนไขของกฎหมาย มากกว่าจะมองเห็นและมีความเข้าใจในเจตนารมย์ที่แท้จริงของ SEC ที่ต้องการให้ผู้บริหารองค์กรมีการนำเอาระบบการควบคุมภายในที่ดีไปเป็นส่วนหนึ่งของการบริหารจัดการองค์กรและทำให้องค์กรมีการกำกับดูแลที่ดี

ประการที่ 2 **ทีมงานคือคนเขียนรายงานเองในระดับองค์กรไม่ใช่รวบรวมจากการกำกับดูแลองค์กรด้านควบคุมภายในจริง**

ในภาคปฏิบัติ ผู้บริหารองค์กรทั้งหมดได้มีการแต่งตั้งบุคลากรภายในองค์กรขึ้นมาเพื่อทำการจัดทำรายงานผลดำเนินงานด้านการควบคุมภายใน โดยอิงตามกรอบแนวคิดของมาตรฐาน COSO 2013 Internal Control เป็นการมอบหมายหน้าที่และความรับผิดชอบจากระดับบนลงล่างก็จริง

แต่ข้อมูลที่ได้จากการประเมินความเพียงพอของการควบคุม

- ⇨ *ได้กลายเป็นข้อมูลจากล่างขึ้นบน (Bottom-Up)*
- ⇨ *กิจกรรมการควบคุมเป็นการควบคุมตนเอง แยกกันในแต่ละฝ่ายงานแต่ละสายงาน ไม่มีลักษณะบูรณาการ*
- ⇨ *มีความจำกัดเพียงการประเมินความเสี่ยงในระดับกระบวนงาน หรือ Functional – based รายคน บางกระบวนการ*
- ⇨ *องค์กรไม่ได้มีระบบการควบคุมภายใน ที่เป็น เงื่อนไขการกำกับการปฏิบัติงานในทุกภาระงานจริง*

ประการที่ 3 **การประเมินจากบางคน และขาดเกณฑ์**

การประเมินความเพียงพอด้านการควบคุมภายในขององค์กรส่วนใหญ่ พบว่า

- ⇨ *ไม่ได้เป็นกิจกรรมเชิงบูรณาการ*
- ⇨ *บุคลากรทุกคนทุกตำแหน่งไม่ได้มีส่วนร่วมอย่างทั่วถึงกัน*
- ⇨ *ข้อมูลที่นำไปจัดทำรายงานด้านการควบคุมภายในจึงมาจากบุคลากรบางส่วนเท่านั้น*

ประการที่ 4 **ยึดองค์ประกอบ ทำในระดับย่อย แต่ไม่ยึดโครงสร้าง THE THREE LINES และไม่ใช่ความเสี่ยงระดับองค์กร**

แม้ว่ากระบวนการประเมินความเสี่ยงจะยึดกรอบ 5 องค์ประกอบของ COSO Internal Control แต่การประเมินความเสี่ยงและการจัดการด้วยมาตรการด้านควบคุมภายในกลับยึดติดกับ 5 องค์ประกอบที่เป็นประเด็นการประเมินในระดับองค์กร ซึ่งให้ความเห็นจากระดับผู้ปฏิบัติงานในระดับภาระงานเท่านั้น

ประการที่ 5 **ยึดการประเมินตนเอง กำหนดระดับความเสี่ยงต่ำไป ประเมินระดับการควบคุมดีเกินจริง**

วิธีการที่องค์กรจะนำมาใช้ในการประเมินความเสี่ยงและประเมินความเพียงพอของการควบคุมภายใน

- ⇨ *เน้นวิธีการประเมินด้วยตนเอง (Self - Assessment)*
- ⇨ *ผู้ประเมินในระดับปฏิบัติการจะทำการประเมินระดับความเสี่ยงและความเพียงพอของการควบคุมเท่าที่มีประสบการณ์ ทักษะ ความเข้าใจ ภายใต้ขอบเขตของหน้าที่และความรับผิดชอบระดับภาระงานเท่านั้น*
- ⇨ *ทำให้ขาดการระบุจุดอ่อนการควบคุมภายในระดับองค์กรโดยรวม*

ประการที่ 6 **ไม่มีแผนปรับปรุงแก้ไขในระดับภาพรวมและสภาพแวดล้อมการควบคุมมีแต่ระดับปฏิบัติการ**

แม้ว่า COSO 2013 จะมีการระบุระดับของการควบคุมภายในเป็น 4 ระดับ คือ

1) Entity Level ระดับองค์กรโดยรวม
2) Division ระดับสายงาน
3) Operating Unit ระดับหน่วยงานย่อย
4) Function ระดับภาระงานรายบุคคล

แต่ในทางปฏิบัติ ผู้ปฏิบัติงานที่ทำหน้าที่ประเมินตนเองจะเสนอแผนการควบคุมภายในระดับภาระงานของตนเอง ไม่ได้เสนอแผนการควบคุมภายในครบถ้วนทั้ง 4 ระดับ

3. กว่า 30 ปี (1992 – 2024) มั่นใจการควบคุมได้หรือยัง

จากประเด็นที่กล่าวมาข้างต้น ทำให้เห็นชัดว่า

- ⇨ องค์กรต่าง ๆ ทั่วโลกได้ให้การยอมรับมาตรฐานสากลตามกรอบแนวคิด COSO Internal Control มาตั้งแต่ 1992
- ⇨ เริ่มนำมาสู่การดำเนินกระบวนการประเมินความเพียงพอของการควบคุมภายในเป็นรายไตรมาส และสามารถออกรายงานด้านการควบคุมภายในเพิ่มเติมจากตัวเลขผลประกอบการมาตั้งแต่ปี 2004
- ⇨ จนถึงปัจจุบันที่มีการปรับปรุงมาตรฐานการควบคุมภายใน จาก COSO 1992 สู่ COSO 2013 แล้วอีกกว่า 10 ปี แต่สิ่งที่ยังไม่อาจจะให้หลักประกันและสร้างความมั่นใจได้มีหลายประเด็นด้วยกันที่ไม่นำไปสู่ความมั่นคงอย่างเหมาะสมอย่างยั่งยืน (Criteria of Suitability)

ผ่านมา 27 ปี พบว่ากิจการส่วนใหญ่ยังทำการควบคุมภายในเพียงให้มีรายงานนำส่งหน่วยงานกำกับ แต่ไม่ได้เกิดกิจกรรมควบคุมแทรกในระหว่างดำเนินงานจริง

ประเด็นที่ 1 **จะมั่นใจได้อย่างไรว่าการประเมินความเสี่ยงและการประเมินตนเองด้านความเพียงพอของการควบคุมภายในจะเที่ยงตรง**

- ⇨ ไม่ได้มาจากดุลยพินิจส่วนบุคคล
- ⇨ ไม่เกิดความเอนเอียงไม่ว่าจะมีลักษณะที่มั่นใจเกินจริง (Over-confidence) หรือมองโลกในแง่ร้ายเกินไป

หากไม่สามารถรับรองอย่างมั่นใจได้จริง

- ⇨ ***การดำเนินกระบวนการควบคุมภายในย่อมขาดคุณสมบัติของ “Being free from bias”***

ประเด็นที่ 2 **จะมั่นใจได้อย่างไรว่าการกระบวนการติดตาม และวัดผล เพื่อประเมินประสิทธิภาพของการควบคุมภายใน**

- ⇨ ได้ครอบคลุมทั้งมาตรการวัดผลในเชิงปริมาณและเชิงคุณภาพ
- ⇨ ไม่ได้เป็นเพียงการให้ความเห็นในระดับส่วนบุคคล

⇨ มีความพร้อมทั้งมีตัวชี้วัดด้านการควบคุม (Key Control Indicators: KCIs) ที่ครอบคลุมทุกกระบวนการดำเนินงานที่สำคัญ

⇨ เป็นการประเมินผลที่มีความสมเหตุสมผล เชื่อถือได้และสอดคล้องกับผลประกอบการขององค์กร

หากองค์กรยังไม่สามารถมีความมั่นใจได้อย่างเพียงพอ

⇨ ***การดำเนินกระบวนการควบคุมภายในย่อมยังขาดคุณสมบัติในเรื่อง "Permit reasonably consistent qualitative and quantitative measurements of entity's internal control "***

ประเด็นที่ 3 **จะมั่นใจได้อย่างไรว่า การดำเนินกระบวนการควบคุมภายใน**

⇨ จะครอบคลุมและครบถ้วนเพียงพอต่อประเด็นความเสี่ยงสำคัญ

⇨ นำสู่ประสิทธิผลของการควบคุมภายในระดับองค์กร

หากไม่สามารถมั่นใจได้จริง

⇨ ***การดำเนินกระบวนการควบคุมภายในย่อมขาดคุณสมบัติของ "Being sufficiently complete so that those relevant factors that would alter a conclusion about the effectiveness of entity's internal control"***

ประเด็นที่ 4 **จะมั่นใจได้อย่างไรว่า แผนการควบคุมภายในที่มีการดำเนินงานจะมีความเหมาะสม และสอดคล้องกับจุดอ่อนด้านการควบคุมภายใน**

หากไม่สามารถมั่นใจได้

⇨ ***การบริหารแผนการควบคุมภายในนั้นย่อมขาดคุณสมบัติของ "Being relevant to an evaluation of Internal Control"***

4. COSO 2013 ใช้กับหน่วยงานรัฐและเอกชน

องค์กรต่างๆ และหน่วยงานกำกับการดำเนินงานขององค์กรต่างเห็นควรว่า

- ⇨ ผู้บริหารระดับสูงและคณะกรรมการจะต้องให้ความสำคัญ และเพิ่มการระมัดระวังในการออกหลักเกณฑ์การควบคุมภายใน โดยอิงกับกรอบแนวคิด COSO 2013 ที่เกี่ยวข้องกับองค์กรทั้งภาครัฐและเอกชน
- ⇨ ประเด็นที่พบมาข้างต้น ในกรณีของประเทศไทย ได้มีการวางเงื่อนไขการควบคุมภายในเป็นส่วนหนึ่งของการบริหารจัดการใน 2 กรณี

วันนี้ COSO 2013 เป็นมาตรฐานภาคบังคับทั้งหน่วยงานรัฐและกิจการเอกชนทุกกิจการจะส่งข้อมูลอันเป็นเท็จอีกไม่ได้แล้ว

กรณีของบริษัทเอกชน

บริษัทมหาชนที่เป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์ ทั้งตลาด SET และตลาด mai

- ⇨ *ถูกกำหนดเงื่อนไขให้กรอกแบบฟอร์ม 69-1 ซึ่งเป็นแบบฟอร์มที่ยกเอาเนื้อหาและ 17 หลักการของ COSO 2013 มาใช้ทั้งหมด ตั้งแต่การจัดทำหนังสือชี้ชวน*
- ⇨ *ต้องมีรายงานผลดำเนินงานใน 56-1 ก็มีส่วนของการบริหารความเสี่ยงและการควบคุมภายใน*
- ⇨ *กำหนดให้คณะกรรมการตรวจสอบให้ความเห็นผลการตรวจสอบความเพียงพอของการควบคุมภายใน*

บริษัทจำกัด

- ⇨ *ต้องมีกลไกการตรวจสอบภายใน มาตรฐานการตรวจสอบภายในเชิงวิชาชีพ กำหนดให้ทำการตรวจสอบภายในกรอบของ การกำกับดูแล บริหารความเสี่ยง และควบคุมภายใน*

⇨ *การควบคุมภายในเป็นส่วนหนึ่งขององค์ประกอบที่ดีด้านการกำกับดูแลองค์กร โดยเฉพาะในส่วนการควบคุมการนำเข้าข้อมูลสู่ระบบบัญชี เพื่อจัดทำสถานะทางการเงินและรายทางการเงิน ซึ่งผู้สอบบัญชีจะใช้ในการประเมินการควบคุมว่ามีความเพียงพอที่จะให้การรับรองความถูกต้องแท้จริงของรายงานทางการเงินดังนั้นหรือไม่*

⇨ *กรณีของบริษัทญี่ปุ่น ได้พัฒนาจากมาตรฐาน COSO 2013 ไปเป็นมาตรฐาน J-SOX โดย*

(ก) เพิ่มองค์ประกอบจาก 5 องค์ประกอบเป็น 6 องค์ประกอบ แยกส่วนของกิจกรรมการควบคุม ด้านเทคโนโลยีสารสนเทศออกมาต่างหาก

(ข) เพิ่มวัตถุประสงค์ของการควบคุม เป็น 4 วัตถุประสงค์ ในด้านของการคุ้มครองและปกป้องสินทรัพย์

กรณีของหน่วยงานภาครัฐ

พระราชบัญญัติวินัยการเงินการคลัง พ.ศ. 2561 มาตรา 79 กำหนดให้หน่วยงานรัฐต้องทำการตรวจสอบภายใน บริหารความเสี่ยง และควบคุมภายใน ตามหลักเกณฑ์และเงื่อนไขที่กำหนดโดยกระทรวงการคลัง

⇨ กระทรวงการคลังได้ออกหลักเกณฑ์การควบคุมภายใน เมื่อปลายปี 2561 ที่เป็นไปตามหลักเกณฑ์และเงื่อนไขของ พรบ. วินัยการเงินการคลัง พ.ศ.. 2561 โดยอิงตามกรอบแนวคิด COSO 2013 และให้หน่วยงานรัฐนำส่งเป็นรายงานภาคบังคับ

⇨ สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจกำหนดให้การควบคุมภายในเป็นเงื่อนไข หนึ่งของการประเมินผลดำเนินงาน

⇨ สำนักงาน กพร. กำหนดให้การควบคุมภายในเป็นเงื่อนไขหนึ่งของการประเมินผลดำเนินงานสำหรับหน่วยงานรัฐอื่นที่มิใช่รัฐวิสาหกิจ

5. เข้าใจความท้าทายเพื่อเตรียมจัดการให้ครบถ้วน

สิ่งที่ควรจะใส่ใจในการนำกรอบแนวคิด COSO 2013 Internal Control มาใช้งานการควบคุมภายใน เพื่อให้องค์กรต่าง ๆ มีการกำกับการปฏิบัติตามกฎเกณฑ์ด้านการควบคุมภายใน (Internal Control Compliance) ที่เพียงพอ เหมาะสมและทำให้องค์กรมีความมั่นคงและการกำกับดูแลองค์กรที่ดีอย่างยั่งยืน ประกอบด้วยการจัดการกับความท้าทายสำคัญ ได้แก่

ความท้าทายที่ 1

องค์กรอาจจะแจ้งว่าได้นำเอากรอบแนวคิด COSO 2013 Internal Control มาใช้ในการดำเนินการ โดยสามารถแสดงเอกสารหลักฐานที่เป็นรายงานผลการประเมินความเพียงพอของการควบคุมภายในได้ แต่ไม่ได้นำเอากลไกการควบคุมภายในที่ดีตามกรอบแนวคิดของ COSO มาใช้เป็นส่วนหนึ่งของระบบบริหารจัดการ (Management System) ในภาคปฏิบัติ และใช้กิจกรรมและแผนการควบคุมภายในในระหว่างดำเนินธุรกิจและดำเนินการตามพันธกิจหลักขององค์กรอย่างต่อเนื่องและสม่ำเสมอ

ทั้งนี้ ต้องไม่ใช่กรณีที่องค์กรจัดทำรายงานผลการประเมินความเพียงพอของการควบคุมภายในเพียงเพราะหน่วยงานกำกับ และผู้สอบบัญชีภายนอกต้องการให้มีรายงานดังกล่าวหรือมองเป็นการกำกับการปฏิบัติตามกฎเกณฑ์ ที่ต้องทำให้ครบถ้วนตามแบบแผนเท่านั้น

ความท้าทายที่ 2

องค์กรมีความจำเป็นต้องค้นหา ระบุ วิเคราะห์ และประเมินความเสี่ยงสำคัญ ที่เป็นอุปสรรคต่อการดำเนินงานอยู่แล้ว และต้องกระทำอย่างเข้มข้น เข้มงวด และเอาจริงเอาจัง เพื่อมิให้มีจุดอ่อนที่มีผลต่อความสำเร็จของการประกอบการและการดำเนินงาน

ทั้งนี้ ต้องไม่ใช่กรณีที่ยึดโยงกับ COSO 2013 เท่านั้น เพราะ COSO 2013 เป็นเพียงเครื่องมือที่ให้กรอบแนวคิดและขั้นตอน

ของการดำเนินการ ซึ่งเป็นเพียงหลักเกณฑ์ขั้นต่ำ (Minimum Requirement) หากมีความจำเป็น องค์กรจะต้องจัดทำโดยต่อยอด ขยายผล และประยุกต์ใช้ให้เพียงพอ ครอบคลุมครบถ้วนจริง ไม่ใช่ข้อมูลที่มาจากตัวแทนบางคนบางส่วนงาน แต่ต้องมาจากผู้รับผิดชอบทุกภาระงาน

องค์กรทุกองค์กร ที่มีความเข้าใจในความท้าทายข้างต้นแล้ว และพิจารณาอย่างมีเหตุมีผล เพื่อให้สามารถออกแบบ จัดวาง และพัฒนาระบบการควบคุมภายในมาใช้ในองค์กรอย่างเป็นระบบต่อไป

บทที่ 2
COSO เป็นใครและมีความสำคัญอย่างไร

1. สมาชิกจาก 5 องค์กรที่สนับสนุน

COSO (อ่านว่า โคโซ) เป็นชื่อย่อของคณะกรรมการที่เป็นชื่อย่อของคณะกรรมการที่มีชื่อเต็มว่า The Committee of Sponsoring Organizations of The Treadway Commission ซึ่งมีรูปแบบมีสมาชิกระดับองค์กรที่สนับสนุนเป็นคณะกรรมการร่วมของสถาบันวิชาชีพ 5 แห่ง ได้แก่

- ⇨ สถาบันผู้สอบบัญชีรับอนุญาตแห่งสหรัฐอเมริการ หรือ AICPA (The American Institute of Certified Public Accountants) เป็นองคืกรที่มีสมาชิกมากที่สุดในโลก ประกอบด้วยผู้ที่อยู่ในวิชาชีพการบัญชี บทบาทที่สำคัญจึงเป็นการกำหนดมาตรฐานจริยธรรม พัฒนาและยกระดับ การออกข้อสอบสำหรับผู้สอบวิชาชีพ กำหนดมาตรฐานการ

ตรวจสอบภายในสำหรับบริษัทเอกชน องค์กรที่ไม่แสวงหากำไร หน่วยงานภาครัฐ และรัฐบาลท้องถิ่นในสหรัฐอเมริกา

- ⇨ สถาบันผู้ตรวจสอบภายใน หรือ Institute of Internal Auditors: IIA เป็นผู้กำหนดมาตรฐาน และจุดรับฟังความคิดเห็นจากผู้ตรวจสอบภายในเชิงวิชาชีพ ทำหน้าที่เป็นแหล่งข้อมูลสำหรับผู้ตรวจสอบภายใน ผ่านการพัฒนากรอบแนวทางการปฏิบัติเชิงวิชาชีพของการตรวจสอบภายใน และการให้ใบรับรองแก่ผู้ตรวจสอบภายใน
- ⇨ สถาบันผู้บริหารการเงิน หรือ Financial Executives Institute หรือ FEI เป็นสมาคมในเชิงวิชาชีพสำหรับผู้บริหารงานทางการเงินระดับอาวุโสจากภาคอุตสาหกรรมต่างๆ เปิดโอกาสให้มีการพัฒนาเครือข่าย ทำการวิจัย และร่วมหารือกันในประเด็นของวิกฤติทางด้านการเงิน รวมทั้งช่วยสมาชิก ในการให้ได้รับข้อมูลและเชื่อมต่อกับความเปลี่ยนแปลงของโลกการเงิน
- ⇨ สถาบันนักบัญชีแห่งสหรัฐอเมริการ หรือ American Accounting Association: AAA เป็นองค์กรที่ส่งเสริมความเป็นเลิศในการศึกษาทางบัญชี การวิจัย และพัฒนาแนวปฏิบัติที่เป็นเลิศทางการบัญชี ด้วยการผ่านความร่วมมือกับสถาบันการศึกษาที่มีการเปิดสอนในคณะบัญชี ผู้ปฏิบัติงานทางด้านบัญชีและกลุ่มผู้มีส่วนได้ส่วนเสียอื่น เพื่อเพิ่มความรู้ที่ทันสมัยและก้าวหน้า สำหรับการปฏิบัติงานทางบัญชี
- ⇨ สถาบันนักบัญชีเพื่อการบริหาร หรือ Institute of Management Accountants: IMA เป็นองค์กรระดับโลกทางด้านวิชาชีพการเงินและบัญชี มุ่งเน้นที่ระบบบัญชีบริหาร และวิชาชีพการบัญชีเชิงบริหารที่มีความก้าวหน้า เป็นผู้ออกใบรับรองนักบัญชีบริหาร อีกทั้งยังเป็นผู้ให้ข้อมูลในเชิงวิชาการ ผลการสำรวจวิจัย และให้โอกาสสำหรับสมาชิกในการสร้างเครือข่ายระหว่างกัน

Sponsoring Organizations

The Institute of Internal Auditors Elevating Impact

AICPA

fei

American Accounting Association | Thought Leaders in Accounting

ima | The Association of Accountants and Financial Professionals in Business

องค์กรที่สนับสนุนทั้ง 5 องค์กรนี้ มีส่วนอย่างมากในการพัฒนา และออกประกาศใช้กรอบแนวทางการบริหารจัดการ ทั้งด้านการควบคุมภายใน การบริหารความเสี่ยง การบริหารทุจริต เพื่อให้มั่นใจว่า จะมี

เครื่องมือที่เชื่อถือได้และมีประสิทธิผลสำหรับองค์กรต่างๆ ในการเพิ่มความเข้มแข็งของกระบวนการควบคุมภายในและบริหารความเสี่ยง

พันธกิจและวิสัยทัศน์ของ COSO

Mission

The Committee of Sponsoring Organizations' (COSO) mission is to help organizations improve performance by developing thought leadership that enhances internal control, risk management, governance and fraud deterrence.

Vision

COSO's vision is to be globally recognized as an authority on internal control and a thought leader on risk management, governance and fraud deterrence.

พันธกิจ คือ การช่วยให้องค์กรต่าง ๆ ด้านปรับปรุงผลการดำเนินงานด้วยการปรับปรุงการเป็นผู้นำทางความคิดสำหรับองค์กรที่สามารถส่งเสริมกรอบดำเนินงานด้านการกำกับดูแลกิจการ การบริหารความเสี่ยง การควบคุมภายใน และการป้องกันและต่อต้านการทุจริต

วิสัยทัศน์ คือการเป็นที่รับรู้ในระดับโลกในฐานะที่เป็นผู้มีอำนาจในการจัดวางการควบคุมภายในและการเป็นผู้นำทางความคิดแก่องค์กรด้านการกำกับดูแล การบริหารความเสี่ยง และการป้องกันและต่อต้านการทุจริต

COSO กำหนดเป้าหมายการดำเนินงาน

COSO's goal is to provide thought leadership dealing with three interrelated subjects: Enterprise Risk Management (ERM), Internal Control, Fraud Deterrence and Governance.

มีเป้าหมายที่จะนำเสนอผ่านการเป็นผู้นำทางความคิดแก่องค์กรเพื่อให้มีแนวทางการจัดการใน 3 ประเด็นหลัก

- ⇨ การบริหารความเสี่ยงทั่วทั้งองค์กร
- ⇨ การควบคุมภายใน
- ⇨ การกำกับดูแลและ ป้องปรามการทุจริต

2. COSO บทบาทชัดเจนจาก SOX ACT

2.1 ตีพิมพ์กรอบแนวคิดชี้นำปี 1992

เผยแพร่ผลงานการเป็นผู้นำทางความคิดแก่องค์กร มาจากการเผยแพร่มาตรฐานการควบคุมภายใน เมื่อปี 1992 ภายใต้ชื่อ Internal Control — Integrated Framework

กระนั้นก็ตาม บทบาทของ COSO ไม่ได้มีความโดดเด่นมากนัก ในช่วงที่ประกาศมาตรฐานแนวคิด COSO 1992 Internal Control เพราะในช่วงนั้น กระบวนการดำเนินงานที่กำกับการจัดทำการประเมินการควบคุมภายในและรายงานผลการประเมินความเพียงพอของการควบคุมภายในยังไม่ใช่หลักเกณฑ์ภาคบังคับแต่อย่างใด จนกระทั่งสหรัฐโดยประธานาธิบดีบุชได้ลงนามใช้กฎหมายที่เรียกว่า Sarbanes –

Oxley Act (SOX) เมื่อวันที่ 30 กรกฎาคม 2002 ทำให้กระบวนการควบคุมภายในเป็นภาคบังคับและต้องเปิดเผยต่อสาธารณชน

ทั้งนี้ จากแรงกระตุ้นที่เกิดการทุจริตและการตกแต่งบัญชีและรายงานทางการเงินขึ้นกับบริษัท Enron และ WorldCom ที่เป็นบริษัทจดทะเบียนขนาดใหญ่และเป็นกลุ่มหุ้นบลูชิปทำให้เกิดความเสียหายในวงกว้างต่อนักลงทุนในตลาด โดยหวังว่าการออกกฎหมาย SOX Act จะช่วยพลิกฟื้นความเชื่อมั่นของตลาดหลักทรัพย์และนักลงทุนในตลาด รวมทั้งความเชื่อมั่นในบทบาทและผลการตรวจสอบและรับรองงบการเงินของผู้สอบบัญชีที่รับรองงบการเงินของบริษัทจดทะเบียนในตลาดหลักทรัพย์โดยไม่ได้ให้ความสำคัญกับการควบคุมภายในก่อนที่จะจัดทำรายงานทางการเงินด้วย

2.2 อานิสงค์จาก SOX ACT

ผลของการมี SOX Act ทำให้ COSO มีโอกาสการนำเอากรอบแนวคิดของ COSO 1992 มาเป็นแนวทางในการประเมินความเพียงพอของการควบคุมภายใน ที่ช่วยให้บริษัทจดทะเบียนทั้งหลายสามารถออกรายงานผลการประเมินการควบคุมภายใน เพื่อเปิดเผยต่อสาธารณะชน และช่วยให้ผู้สอบบัญชีมีแนวทางการตรวจสอบระบบการควบคุมภายในของบริษัทก่อนที่จะรับรองงานการเงินด้วย

การนำเอามาตรฐานการควบคุมภายใน COSO Internal Control — Integrated Framework 1992 มาใช้ไม่ได้จำกัดอยู่แต่เฉพาะบริษัทจดทะเบียนในตลาดหลักทรัพย์สหรัฐเท่านั้น

หากแต่ได้เกิดการยอมรับกรอบแนวความคิดตามแนวทางดำเนินงานนี้ในหน่วยงาน SEC ที่กำกับตลาดหลักทรัพย์และตลาดหลักทรัพย์ทั่วโลก รวมทั้งในกลุ่มผู้ตรวจสอบบัญชี จนทำให้มาตรฐานการควบคุมภายใน COSO Internal Control — Integrated Framework 1992

- ⇨ *กลายเป็นคำตอบหนึ่งของการกำกับดูแลที่ดีทั่วโลก*
- ⇨ *เป็นกรอบแนวทางดำเนินงานควบคุมความเสี่ยงที่ให้ความสำคัญของการประเมินความเพียงพอของการควบคุมภายในในระดับองค์กร*

บริษัทมหาชนในตลาดและตลาดหลักทรัพย์ มีส่วนช่วยกดดันและขับเคลื่อนให้กิจการเอกชนนำเอามาตรฐาน COSO INTERNAL CONTROL – INTEGRATED FRAMEWORK มาใช้เป็นกรอบแนวทางดำเนินงานเพื่อประกอบการออกรายงานผลดำเนินงานด้านการควบคุมภายในเป็นประจำทุกปี

⇨ *ผู้บริหารและคณะกรรมการขององค์กรต้องจัดให้มีการประเมินนี้ และจัดทำรายงานเพื่อเสนอหน่วยงานกำกับดูแลภายนอกและนักลงทุนในตลาดเป็นประจำทุกปี*

การออกมาตรฐานกรอบแนวทางด้านการควบคุมภายในของ COSO Internal Control — Integrated Framework ถูกทบทวนและปรับปรุงใหม่จนเป็น Version ของ COSO 2013 หลังจากการเกิดวิกฤติการณ์ทางการเงินครั้งใหญ่ของโลก ที่เรียกว่า "วิกฤติการณ์แฮมเบอร์เกอร์" ในปี 2008 เพื่อให้เหมาะสมและสอดคล้องกับสถานการณ์การจัดการธุรกิจสมัยใหม่

2.3 มาตรฐานอื่นของ COSO ที่ออกตามมา

มาตรฐานการบริหารความเสี่ยงทั่วทั้งองคกร

ในส่วนของมาตรฐานการบริหารความเสี่ยงทั่วทั้งองค์กร COSO ได้ออกเผยแพร่กรอบแนวคิด Enterprise Risk Management — Integrated Framework เมื่อปี 2004 และแก้ไขปรับปรุง จนเป็น COSO Enterprise Risk Management — Integrating with Strategy and Performance เวอร์ชั่นใหม่ในปี 2017 ให้เหมาะสมกับความซับซ้อนของประเด็นความเสี่ยงที่เปลี่ยนแปลงไปรวมทั้งความเสี่ยงในรูปแบบใหม่ที่เพิ่มขึ้น แต่ยกระดับการบริหารความเสี่ยงขึ้นไปอยู่ในการบูรณาการกับกลยุทธ์และผลดำเนินงานระดับองค์กร ทั้งให้ข้อมูลในลักษณะ GUIDANCE ที่เพิ่มเติมอีกจำนวนมาก เพื่อให้องค์กรมีรายละเอียดของแนวทางการปฏิบัติในแต่ละเรื่องที่มุ่งเน้นเฉพาะประเด็น

มาตรฐานการบริหารความเสี่ยงด้านทุจริต

สำหรับบทบาทในส่วนของการจะทำกรอบแนวคิดเพื่อชี้นำการป้องกันการทุจริต COSO เริ่มมีบทบาทในส่วนนี้ด้วยการเผยแพร่ผลงานการศึกษาวิจัยจำนวน 2 ฉบับ

⇨ ปี 1999 ผลงานวิจัยชื่อ Fraudulent Financial Reporting: 1987-1997ที่เกิดจากการถอดบทเรียนการทุจริตที่เกิดขึ้นในอดีต

⇨ ปี 2010 ภายหลังจากการเกิด วิกฤตการณ์แฮมเบอร์เกอร์ ในปี 2009 COSO ได้ออกเผยแพร่ผลงานชื่อ Fraudulent Financial Reporting: 1998-2007

จนกระทั่งในปี 2016 องค์กร COSO ได้เริ่มเผยแพร่มาตรฐานเพื่อเป็นกรอบแนวคิดสำหรับการจัดการความเสี่ยงที่เกิดขึ้นจากการทุจริตเป็นฉบับแรก และมีการปรับปรุงเป็นเวอร์ชั่นที่ 2 ในปี 2023 ปรับปรุงแนวคิดให้ทันสมัย.ในชื่อ Fraud Risk Management Guide (Second Edition)

มาตรฐานการกำกับดูแลกิจการที่ดี

หลังจากนั้น COSO ได้เริ่มทำการพัฒนากรอบแนวทางการกำกับดูแลกิจการ ซึ่งเป็นบทบาทที่เน้นการดำเนินงานจากระดับคณะกรรมการอำนวยการ และผู้บริหารระดับสูงขององค์กรเป็นสำคัญ เพื่อให้คณะกรรมการมีบทบาทเป็นองค์คณะในการกำกับดูแล และมอบหมายการดำเนินงานให้แก่ฝ่ายจัดการเพื่อนำไปสู่การขับเคลื่อน โดยทำหน้าที่ในการติดตามผลดำเนินงานจริงที่เกิดขึ้น และสถานะความเสี่ยงและประสิทธิผลของการควบคุมภายในในภาพรวมระดับองค์กร

2.4 FRAMEWORK ไม่ใช่คู่มือปฏิบัติสำเร็จรูป

บทบาทของการเป็น Framework

การพัฒนามาตรฐานของ COSO มาจากผลการศึกษาวิจัย การถอดบทเรียนที่เรียนรู้ จากการเกิดวิกฤติ จรรยาบรรณวิบัติที่เกิดขึ้นในองค์กรต้นแบบ ในแต่ละช่วงเวลา เพื่อนำมาใช้ในการพัฒนา และทำการทดสอบโดยผ่านการหารือร่วมกันและกระบวนการออกแบบที่มีลักษณะเปิดกว้าง โดยมีองค์กรย่อยที่ให้การสนับสนุน COSO ร่วม 5 องค์กร และอาจจะรวมถึงองค์กรภาคเอกชนที่ทำหน้าที่ในการสอบบัญชี ซึ่งมีประสบการณ์จริงในการตรวจสอบบัญชีมาก่อน เพื่อพัฒนาขึ้นมาเป็นองค์ประกอบหลักและหลักการที่สำคัญสำหรับกรอบแนวทางการดำเนินงานด้านการควบคุมภายใน เพื่อแทรกไว้ในระหว่างกระบวนการดำเนินงานทางธุรกิจหรือเชิงพาณิชย์ตามวัตถุประสงค์การจัดตั้งและดำรงอยู่ขององค์กร

ด้วยเหตุที่มาตรฐานการควบคุมภายใน COSO 2013 มีลักษณะเป็นกรอบแนวทางดำเนินงาน (Framework) ด้านการควบคุมภายในที่จัดวางไว้ในลักษณะที่เป็นโครงสร้าง (Structures) สำหรับดำเนินการเป็นการทั่วไป ซึ่งวัตถุประสงค์สำคัญของการชี้นำในลักษณะกรอบแนวทางดำเนินงาน จึงประกอบด้วย

1) ให้แนวทางและสนับสนุนองค์กรให้พัฒนาการมีส่วนร่วมแบบบูรณาการของผู้ที่เกี่ยวข้องให้เกิดระบบการควบคุมภายในที่ลดระดับความเสี่ยงจนลงมาอยู่ในเกณฑ์ที่ยอมรับได้เพื่อสนับสนุนผลดำเนินงานที่ดีขึ้น

2) ให้กรอบแนวทางที่จะนำไปสู่การสื่อสารจนเกิดกิจกรรมการออกแบบและการนำไปใช้จริงของมาตรการควบคุมภายในที่มีความเพียงพอและมีประสิทธิผล

3) ให้แนวทางที่จะสร้างพันธะผูกพันธ์และความมุ่งมั่นของผู้เกี่ยวข้องภายในองค์กร ที่นำไปสู่ความรับผิดชอบต่อการจัดการความเสี่ยงผ่านการควบคุมภายในระหว่างการปฏิบัติงานตามพันธกิจและภาระงานขององค์กร

กระนั้นก็ตาม มาตรฐานการควบคุมภายใน COSO 2013 ก็ยังคงเป็นเพียงกรอบแนวทางดำเนินงานทั่วไปที่ให้แบบจำลองหรือโมเดลที่อิงบน 17 หลักการ เพื่อให้องค์กรมีความเข้าใจที่เป็นหลักเกณฑ์เดียวกัน และนำไปใช้ประเมินความเพียงพอของการควบคุมภายในในแต่ละองค์กรเอง

ดังนั้น การนำมาใช้ปฏิบัติจริงจึง

- ⇨ *พิจารณาควบคู่กับ GUIDANCE ที่ COSO เผยแพร่และประกาศใช้เพิ่มเติมในระยะหลังจากการออกมาตรฐานฉบับหลักแล้ว เพื่อให้มีกรอบการดำเนินงานด้านการควบคุมเฉพาะเจาะจงตามความจำเป็น*
- ⇨ *สามารถใช้ประกอบกับกรอบแนวทางการดำเนินการที่มีลักษณะเฉพาะเจาะจงตามมาตรฐานอื่น เช่น CoBiT ซึ่งเป็นกรอบแนวทางการดำเนินงานเพื่อควบคุมทางด้านเทคโนโลยีสารสนเทศ*

จุดอ่อนพึงระวังของ Framework

ทั้งนี้ มาตรฐาน COSO 2013 ไม่ได้บอกลึกลงไปถึงวิธีการดำเนินการในการประเมินความเพียงพอของการควบคุมภายในที่แต่ละองค์กรต้องทำการประเมินตนเอง และเป็นวิธีดำเนินงานทั่วไป เพื่อให้ความมั่นใจว่าการดำเนินงานขององค์กรจะบรรลุตามวัตถุประสงค์ 3 ด้าน ประกอบด้วย

(ก) การเพิ่มประสิทธิภาพของการปฏิบัติงาน

(ข) การนำไปสู่การจัดทำรายงานทางการเงินและไม่ใช่การเงินที่ถูกต้อง ครบถ้วน

(ค) การกำกับการปฏิบัติตามกฎเกณฑ์ที่สอดคล้องและเหมาะสมเพียงพอ

ซึ่งอาจจะทำให้ขาดหลักประกันว่าการประเมินความเพียงพอของการควบคุมภายในในแต่ละองค์กรจะเป็นไปได้อย่างมีประสิทธิภาพและเกิดประสิทธิผลในการลดจุดอ่อนของการควบคุมภายในที่ยังคงมีอยู่ หากการกำหนดวัตถุประสงค์ของการควบคุมภายในแต่ละองค์กรนั้นๆ ไม่ชัดเจน จนไม่ได้มีการมอบหมายความรับผิดรับชอบของการควบคุมภายในให้แก่ผู้ที่เกี่ยวข้องอย่างเหมาะสม

ดังนั้น แม้ว่ากิจกรรมการประเมินความเพียงพอของการควบคุมภายในนี้จะเกิดขึ้นทุกปีก็ตาม และไม่ได้ให้หลักประกันว่าการทำกิจกรรมการประเมินความเพียงพอของการควบคุมภายในจะเป็นรูปแบบของ Top-down และเป็นการประเมินบน Risk-based Assessment

- ⇨ องค์กรอาจจะมอบหมายให้การประเมินความเพียงพอของการควบคุมภายในเป็นงานระดับภาระงานหรือ Function – based ที่มีบุคลากรเฉพาะกลุ่มจัดทำภาระงานนี้
- ⇨ เป็นเพียงกระบวนการหนึ่งขององค์กร (Process Level) ที่ไม่ได้ครอบคลุม
- ⇨ การดำเนินการไม่ครบถ้วนและไม่ได้สะท้อนจุดอ่อนการควบคุมสำคัญที่เชื่อมโยงถึงการบรรลุผลสำเร็จของการประกอบการอย่าเพียงพอ

ยิ่งกว่านั้น องค์กรจำนวนไม่น้อยอาจจะดึงเอากรอบแนวคิดการควบคุมภายใน COSO 2013 ไปใช้เพียงบางส่วน เพื่อลดภาระค่าใช้จ่าย ภาระด้านการเสียเวลา หรือขาดการศึกษาและทำความเข้าใจอย่างเพียงพอและชัดเจนเกี่ยวกับกรอบแนวทางการประเมินความเพียงพอของการควบคุมภายใน หรือเข้าใจว่าไม่จำเป็นต้องจัดให้มีการควบคุมภายในที่ครบทุกข้อ และไม่เห็นว่าบางประเด็นในหลักการของ COSO 2013 มีความสำคัญกับองค์กร

ซึ่งประเด็นเหล่านี้ทำให้การประเมินความเพียงพอของการควบคุมภายในสามารถออกเป็นรายงานและแม้แต่แผนการควบคุมภายในได้ แต่ไม่ได้เป็นไปตามหลักการ “Comply or Explained” หรือต้องมีความเพียงพอของการควบคุมภายในที่ครบถ้วนทุกประเด็นย่อย (Points of Focus) และทุกหลักการทั้ง 17 หลักการ มิฉะนั้นองค์กรต้องอธิบายให้ได้ว่าแนวทางการควบคุมภายในดีกว่าหลักการที่กำหนดไว้อย่างไร

การออกแบบเพื่อเติมเต็ม Framework

กรอบแนวทางการดำเนินงานด้านการควบคุมภายในจึงจำเป็นต้องมีการนำไปออกแบบและจัดวางให้เหมาะสม เพื่อให้เกิดการดำเนินงานจริงที่เป็นรูปธรรมภายในองค์กร โดยครอบคลุมถึง

1) การทำความเข้าใจต่อหลักการในแต่ละองค์ประกอบ ที่มีจุดมุ่งเน้น (Points of Focus) ที่ชัดเจนเพื่อนำไปสู่การออกแบบและขับเคลื่อนไปสู่การปฏิบัติจริง
2) การกำหนดวิธีการ วิธีดำเนินงาน ที่จะทำให้เกิดการขับเคลื่อน และเกิดการควบคุมภายในจริงในระดับปฏิบัติ
3) การกำหนดความคาดหวังที่องค์กรมีต่อการควบคุมภายใน และกำหนดมาตรฐานของขั้นตอนการปฏิบัติงาน เพื่อสื่อสารและทำความเข้าใจเป็นกระบวนการที่ผู้เกี่ยวข้องทุกภาคส่วนและทุกฝ่ายต้องดำเนินการให้สอดคล้องกัน
4) การจัดหาเครื่องมือเพื่อมาสนับสนุนการดำเนินงาน อำนวยความสะดวก เป็นโครงสร้างพื้นฐานเพื่อให้ระบบการควบคุมภายในสามารถดำรงอยู่ และพัฒนาให้ดีขึ้นตามลำดับ
5) การนำข้อมูลที่เกี่ยวข้องกับความเสี่ยง ที่ได้จากกระบวนการค้นหา ระบุ วิเคราะห์ ประเมิน และจัดลำดับความเสี่ยงที่มีรายละเอียดของผลกระทบต่อองค์กร และโอกาสในการเกิดประเด็นความเสี่ยงดังกล่าว ไปใช้ประกอบการตัดสินใจ และการสื่อสารจุดอ่อนเพื่อนำไปสู่การแก้ไขปรับปรุงที่ทันท่วงที

3. การควบคุมภายใน – ภาคบังคับสำหรับหน่วยงานรัฐ

เมื่อวันที่ 19 เมษายน 2561 ราชกิจจานุเบกษาได้ลงประกาศ พระราชบัญญัติวินัยการเงินการคลัง พ.ศ. 2561 บังคับใช้กับหน่วยงานรัฐทั้งหมด ให้ต้องดำเนินนโยบายการคลัง การจัดทำงบประมาณ การจัดหารายได้ การใช้จ่าย การบริหารการเงินการคลังและการก่อหนี้อย่างมีประสิทธิภาพ โปร่งใสและตรวจสอบได้

ทั้งนี้ตามหลักการรักษาเสถียรภาพและการพัฒนาเศษฐกิจอย่างยั่งยืน และหลักความเป็นธรรมในสังคม และต้องรักษาวินัยการเงินการคลังอย่างเคร่งครัด

พรบ.วินัยการเงินการคลังเป็นอัศวินม้าขาวที่ออกมากำหนดเงื่อนไขให้หน่วยงานรัฐต้องบูรณาการ เชื่อมโยง การควบคุมภายใน การบริหารความเสี่ยง และการตรวจสอบ ส่งให้กระทรวงที่กำกับดูแลมีส่วนรับรู้

3.1 มาตราของกฎหมายที่เกี่ยวข้อง

⇨ ในมาตรา 9 ระบุว่าในการพิจารณาเรื่องที่เกี่ยวกับนโยบายการคลัง การจัดทำงบประมาณ การจัดหารายได้ การใช้จ่าย การบริหารการเงินการคลังและการก่อหนี้ คณะรัฐมนตรีต้องพิจารณาประโยชน์ที่รัฐหรือประชาชนจะได้รับ ความคุ้มค่า และภาระการเงินการคลังที่เกิดขึ้นแก่รัฐ รวมถึงความเสี่ยงและความเสียหายที่อาจเกิดขึ้นแก่การเงินการคลังอย่างรอบคอบ

⇨ มาตรา 78 ภายในเดือนมีนาคมของทุกปี ให้กระทรวงการคลังจัดทำรายงานความเสี่ยงทางการคลังประจำปี ซึ่งอย่างน้อยต้องแสดงผลการประเมินความเสี่ยงที่คาดว่าจะเกิดขึ้นจากผลกระทบของเศรษฐกิจมหภาค ระบบการเงิน นโยบายของรัฐบาล และผลการดำเนินงานของหน่วยงานของรัฐ ที่อาจก่อให้เกิดภาระทางการคลังของรัฐบาล และแนวทางการบริหารจัดการความเสี่ยงนั้น

เมื่อกระทรวงการคลัง ได้จัดทำรายงานความเสี่ยงทางการคลังประจำปีแล้ว ให้นำเสนอต่อคณะกรรมการเพื่อประกอบการพิจารณาจัดทำแผนการคลังระยะปานกลาง และเสนอรัฐมนตรีเพื่อทราบ

⇨ มาตรา 79 ให้หน่วยงานของรัฐให้มีการตรวจสอบภายใน การควบคุมภายใน และการบริหารความเสี่ยงโดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด

3.2 มาตรฐานและหลักเกณฑ์การปฏิบัติ

ต่อมาในวันที่ 5 ตุลาคม 2561 กระทรวงการคลังได้มีหนังสือที่ กค 0409.3/จ.105 เรื่อง หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 โดยให้มีผลบังคับใช้ ตั้งแต่วันถัดจากวันที่กระทรวงการคลังประกาศเป็นต้นไป ซึ่งวันที่ประกาศใช้หลักเกณฑ์คือวันที่ 3 ตุลาคม 2561 จึงเริ่มบังคับใช้มาตั้งแต่วันที่ 4 ตุลาคม 2561

ในบทนำของหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐฯ ระบุว่าจัดทำขึ้นตามมาตรฐานสากลของ COSO 2013 โดยปรับให้เหมาะสมกับบริบทของระบบการบริหารราชการแผ่นดิน เพื่อใช้เป็นกรอบแนวทางในการกำหนด ประเมิน และปรับปรุงระบบการควบคุมภายในของรัฐ อันจะทำให้การดำเนินงาน และการบริหารงานของหน่วยงานรัฐบรรลุผลสำเร็จตามวัตถุประสงค์ เป้าหมาย และมีการกำกับดูแลที่ดี

เนื้อหาสาระของหลักเกณฑ์และมาตรฐานของกระทรวงการคลังกำหนดให้

ข้อ 2 ให้หน่วยงานของรัฐจัดวางระบบการควบคุมภายใน โดยใช้มาตรฐานการควบคุมภายในสำหรับหน่วยงานรัฐที่ กระทรวงการคลังกำหนดเป็นแนวทางในการจัดวางระบบการควบคุมภายในให้บรรลุตามวัตถุประสงค์ของการควบคุมภายใน

ข้อ 3 ให้หน่วยงานของรัฐจัดให้มีการประเมินผลการควบคุมภายในตามที่ให้หน่วยงานของรัฐกำหนดไว้อย่างน้อยปีละ 1 ครั้ง ตามข้อ 8 และข้อ 9

ข้อ 4 ให้ฝ่ายบริหาร หมายถึง ผู้บริหารทุกระดับของหน่วยงานรัฐ เป็นผู้รับผิดชอบในการกำกับดูแล โดยทำให้มีการนำมาตรฐานการควบคุมภายในสำหรับให้หน่วยงานของรัฐที่ กระทรวงการคลังกำหนด ใช้เป็นแนวทางในการจัดวางระบบการควบคุมภายใน และประเมินผลการควบคุมภายในสำหรับให้หน่วยงานของรัฐ

ส่วนที่ 1 วางระบบการควบคุมและการประเมินผลการควบคุมภายในสำหรับกระบวนงานหลัก

ส่วนที่ 2 วางระบบการควบคุมและการประเมินผลการควบคุมภายในสำหรับงานโครงการ

ข้อ 5 ให้หน่วยงานของรัฐจัดให้มีคณะกรรมการคณะหนึ่ง เป็น คณะกรรมการกำกับการควบคุมภายใน ตามคุณสมบัติที่หน่วยงานของรัฐกำหนดเอง