NEW RISK-BASED TOOLs FOR INTERNAL AUDIT

ตามมาตรฐานสากลฉบับใหม่ 2024

GRC FOR INTERNAL AUDIT
RISK THEME FOR AUDIT
RISK UNIVERSE
RISK ASSESSMENT
RISK – CONTROL MATRIX
RISK APPETITE
RISK TOLERANCE

อาจารย์ จิรพร สุเมธีประสิทธิ์

NEW RISK-BASED TOOLs FOR INTERNAL AUDIT

ตามมาตรฐานสากลฉบับใหม่ 2024

อาจารย์ จิรพร สุเมธีประสิทธิ์

ข้อมูลทางบรรณานุกรม

อาจารย์ จิรพร สุเมธีประสิทธิ์

NEW RISK-BASED TOOLs FOR INTERNAL AUDIT

ตามมาตรฐานสากลฉบับใหม่ 2024

313 หน้า

ISBN (E-BOOK) 978-616-612-988-5

พิมพ์ครั้งที่ 1 : พ.ศ. 2567

จำหน่ายในรูปแบบ : E-Book

ราคา : 249 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

มาตรฐานสากลด้านการตรวจสอบภายในฉบับใหม่ หรือ Global Internal Audit Standards 2024 ที่ออกประกาศใช้เมื่อ 9 มกราคม 2024 โดย the Institute of Internal Auditors (IIA) เป็นมาตรฐานที่ยกระดับวิธีการดำเนินงานของงานตรวจสอบภายใน ให้มุ่งเน้นไปสู่การบริหารความเสี่ยงขององค์กรเข้มข้นขึ้นกว่ามาตรฐานเดิมอย่างเห็นได้ชัด

ด้วยเหตุนี้ เครื่องมือที่เกี่ยวข้องกับการบริหารความเสี่ยงจึงกลายเป็นเครื่องมือที่มีความสำคัญที่สุดสำหรับผู้ตรวจสอบภายในและงานตรวจสอบภายใน โดยต้องดำเนินวงจรการบริหารความเสี่ยงในส่วนที่เกี่ยวข้องกับงานตรวจสอบภายในด้วยตนเองแทนที่จะพึ่งพาผลการวิเคราะห์และประเมินความเสี่ยง หรือต้องใช้เกณฑ์ความเสี่ยงที่ยอมรับได้ หรือค่าเบี่ยงเบนความเสี่ยงที่กำหนดมาจากหน่วยงานในกลุ่มงาน 2nd Line หรือแม้แต่กำหนดจะหน่วยงานในกลุ่มงาน 1st Line ผ่านการประเมินตนเอง

ยิ่งกว่านั้น การใช้เครื่องมือที่เกี่ยวข้องกับการบริหารความเสี่ยงของงานตรวจสอบภายในที่ยึดโยงกับเงื่อนไข หลักเกณฑ์ และข้อกำหนด (Criteria) ที่มีความน่าเชื่อถือยังจะเป็นข้อมูลความเสี่ยงที่มีความสำคัญที่สามารถนำไปแบ่งปัน แลกเปลี่ยน เรียนรู้ร่วมกัน รวมทั้งบูรณาการการดำเนินงานกับหน่วยงานอื่นในกลุ่มงาน 2nd Line และ กลุ่มงาน 1st Line ผ่านกลไกการให้บริการด้านการให้ความเชื่อมั่น ด้านคำแนะนำ ด้านการตรวจสอบเชิงลึก และด้านการตรวจสอบเชิงพยากรณ์ได้ด้วย

ตำรา e - BOOK เล่มนี้จึงจะทำขึ้นเพื่อที่จะช่วยให้ CAE และผู้ตรวจสอบภายในได้เครื่องมือที่เกี่ยวข้องกับกระบวนการบริหารความเสี่ยงครบถ้วนตามเงื่อนไขและข้อกำหนดของมาตรฐานสากลด้านการตรวจสอบฉบับใหม่ โดยเฉพาะในส่วนที่เกี่ยวข้องกับกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือที่เรียกว่า GRC – Governance , Risk and Control process คำหลักอื่น ได้แก่ Risk Theme , Risk Universe, Risk Assessment , Risk – Control Matrix , Risk Appetite , Risk Tolerance , Root Cause เพื่อนำไปประกอบการกำหนดวิธีดำเนินงาน (Methodologies) สำหรับหน่วยงานตรวจสอบภายในเพื่อให้สอดคล้องกับมาตรฐานสากลใหม่ และได้ผลดำเนินงานที่มีคุณภาพสูงตามความคาดหวังของผู้ที่เกี่ยวข้อง โดยอาศัยประสบการณ์ ที่ผู้เขียนอยู่ในแวดวงการบริหารจัดการความเสี่ยงมาเป็นเวลาเกือบ 30 ปี ทั้งในบทบาทของการเป็นที่ปรึกษาให้แก่องค์กรต่างๆ ในการพัฒนาระบบกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและควบคุมภายใน และในฐานะที่เคยมีประสบการณ์เป็นอนุกรรมการผู้ทรงคุณวุฒิในคณะกรรมการบริหารความเสี่ยงให้แก่หน่วยงานภาครัฐที่สำคัญ ๆ ติดต่อกันหลายปี

อาจารย์ จิรพร สุเมธีประสิทธิ์

ผู้แต่ง

สารบัญ

บทนำ
เครื่องมือสำคัญสำหรับงานตรวจสอบ
เพื่อรองรับมาตรฐานสากลฉบับปี 2024

งานตรวจสอบภายในเป็นการเข้าถึงข้อมูลเพื่อประเมินกระบวนการ กำกับดูแล บริหารความเสี่ยง และควบคุม หรือ GRC PROCESS ซึ่งส่วนของการบริหารความเสี่ยงตามมาตรฐานข้อ 13.2 RISK ASSESSMENT ขณะที่องค์กรเปลี่ยนผ่านเข้าสู่ยุคดิจิทัลหรือ INDUSTRY 4.0

การดำเนินการนี้ผู้ตรวจสอบภายในต้องใช้เครื่องมือและเทคนิคที่ทันสมัย รวมทั้งการวิเคราะห์ข้อมูลในเชิงลึกได้อย่างรวดเร็ว เพื่อใช้ ประโยชน์จากข้อมูลได้ครอบคลุมมากขึ้น รวดเร็วขึ้น ได้ข้อมูลที่เป็นปัจจุบันอยู่ตลอดเวลา จนสามารถนำไปสู่การระบุสถานะที่เป็นอยู่หรือความน่าจะเป็น ของสถานการณ์ (CONDITION) เทียบกับเงื่อนไขและข้อกำหนดที่ควรจะเป็น (CRITERIA) และเห็นความแตกต่างที่นำไปสู่การให้ความเห็นในงานตรวจสอบได้อย่างมีประสิทธิภาพและประสิทธิผล ภายใต้ข้อจำกัดที่มีอยู่

องค์กรในปัจจุบันมีความจำเป็นต้องปรับตัวให้พร้อมที่จะเผชิญหน้ากับความท้าทายและความเปลี่ยนแปลงที่เกิดขึ้นจากสภาพแวดล้อมและส่งผลต่อการดำเนินงาน จึงส่งผลให้งานตรวจสอบภายในจำเป็นต้องมีการเปลี่ยนแปลงเครื่องมือที่ใช้สำหรับการตรวจสอบภายใน แม้ว่าหน่วยงานตรวจสอบภายในจะไม่ได้เกี่ยวข้องโดยตรงในฐานะผู้กำกับดูแล ผู้บริหารจัดการ หรือผู้ปฏิบัติงานที่สามารถรับมือและตอบโต้ความเสี่ยงเองได้โดยตรง แต่งานบริหารความเสี่ยงต้องทำการตรวจสอบและให้ข้อมูลเชิงลึก หรือข้อมูลเชิงพยากรณ์ด้วยความเที่ยงธรรม ปราศจากการเอนเอียงหรือถูกแทรกแซงให้ต้องดำเนินการออกนอกกรอบ จะช่วยสนับสนุนองค์กร ในฐานะกลุ่มงาน 3rd Line เพื่อแก้ไข ปรับปรุง พัฒนา และยกระดับกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายใน หรือ GRC PROCESS อย่างเต็มที่ และเต็มกำลังเท่าที่จะทำได้

เพื่อให้ผู้ตรวจสอบภายในและหน่วยงานตรวจสอบภายในสามารถพัฒนาและปรับตัวให้เข้ากับสภาพแวดล้อมที่มาจากมาตรฐานสากลเชิงวิชาชีพฉบับใหม่ปี 2024 ที่ยกระดับขึ้นไปจากเดิม จำเป็นต้องมีการพัฒนา เชิงวิชาชีพอย่างต่อเนื่อง เพื่อให้มั่นใจว่าผู้ตรวจสอบภายในได้มาซึ่งทักษะ ในลักษณะของ Upskill/Reskill

หนึ่งในการพัฒนาที่จำเป็นสำหรับผู้ตรวจสอบภายในและหน่วยงานตรวจสอบภายในตามมาตรฐานสากลเชิงวิชาชีพ คือการศึกษาและเรียนรู้เกี่ยวกับเครื่องมือที่จำเป็นต้องนำมาใช้เพิ่มเติม และทำให้เกิดประโยชน์สูงสุดในงานตรวจสอบภายใน โดยเฉพาะ

- ⇨ เครื่องมือที่เกี่ยวข้องกับการวิเคราะห์ข้อมูล เพื่อนำไปสู่การกำหนดสถานะของบริบทองค์กร จนสามารถตั้งข้อสงสัยเยี่ยงผู้ประกอบวิชาชีพที่นำไปสู่การหารือเพื่อสร้างพันธะผูกพันกับผู้บริหารสายงานที่เป็นเจ้าของภาระงาน และจัดทำแผนการตรวจสอบ ตามพันธะผูกพันนั้นๆ ได้
- ⇨ เครื่องมือที่สนับสนุนรูปแบบและวิธีการใหม่ ๆ ของการตรวจสอบภายใน อย่างเช่น AGILE AUDITING , COMBINED AUDITING , REMOTE AUDITING เป็นต้น

1. การผลักดันจากมาตรฐานสากลฉบับใหม่

ตามมาตรฐานสากลด้านการตรวจสอบภายในฉบับใหม่ ที่ออกประกาศใช้ เมื่อวันที่ 9 มกราคม 2024 กำหนดชัดเจนให้งานตรวจสอบภายในไม่สามารถดำเนินงานได้ตามลำพัง หรือแปลกแยกออกมาจากองค์กรและไม่สามารถอยู่อย่างอิสระนอกกรอบกระบวนการกำกับดูแล บริหารความเสี่ยง แนะควบคุมภายใน หรือ GRC PROCESS ได้ ด้วยการกำหนดบทบาทของงานตรวจสอบภายใน

- ⇨ **ให้เกี่ยวข้องอย่างใกล้ชิดกับกระบวนการกำกับดูแล บริหารความเสี่ยง แนะควบคุมภายใน หรือ GRC PROCESS ทั้งก่อนและหลังวงจรการตรวจสอบภายใน**
- ⇨ **ให้ดำเนินกระบวนการที่เกี่ยวข้องกับประเด็นความเสี่ยง ด้วยการใช้กระบวนการบริหารความเสี่ยงเช่นเดียวกับหน่วยงานในกลุ่ม 2nd Line และ หน่วยงานในกลุ่ม 1st Line**
  - ➢ ต้องจัดทำ AUDIT RISK THEME
  - ➢ ต้องพิจารณาและกำหนด AUDIT RISK UNIVERSE
  - ➢ ต้องดำเนินกระบวนการวิเคราะห์และประเมินความเสี่ยงหรือ RISK ASSESSMENT
  - ➢ ต้องกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้ และค่าเบี่ยงเบนความเสี่ยงที่ยอมรับได้สำหรับงานตรวจสอบภายใน

- ต้องวิเคราะห์ความเพียงพอ และประสิทธิผลของ GRC PROCESS ด้วย วิธีการ RISK – CONTROL MATRIX
- ต้องเข้าไปเกี่ยวข้องกับกระบวนการบริหารความเสี่ยงของหน่วยงานในกลุ่มงานอื่น ผ่านกิจกรรมการให้บริการด้าน ADVISORY SERVICE ไม่ว่าจะเป็น บทบาทการเป็นผู้อำนวยความสะดวก (Facilitator) บทบาทการเป็นพี่เลี้ยง (Trainer) บทบาทการเป็นผู้ให้การเรียนรู้ (Educator)
- ต้องพิจารณาดำเนินการตรวจสอบแบบ AGILE AUDITING
- ต้องพิจารณาดำเนินการตรวจสอบร่วมกับหน่วยงานในกลุ่ม 2nd LINE ด้วยการใช้รูปแบบ COMBINED AUDITING เพื่ออาศัยการดำเนินกิจกรรมร่วมกันไปสู่พลังในการขับเคลื่อนให้เกิดการเปลี่ยนแปลง การแก้ไขหรือปรับปรุงองค์กรได้ครบวงจร ลดความซ้ำซ้อนและปิดช่องว่างของการดำเนินการที่ไม่มีผู้รับผิดชอบ
- ต้องพิจารณาดำเนินการตรวจสอบที่รองรับ บริบทธุรกิจและความรับผิดชอบที่เกี่ยวข้องกับสังคมและสิ่งแวดล้อม ด้วยการใช้รูปแบบ ESG AUDITING
- ต้องสื่อสาร แลกเปลี่ยน สร้างการเรียนรู้ รวมถึงการเปิด ศูนย์ เรียนรู้ที่เกี่ยวข้องกับประเด็นความเสี่ยงที่มาจากการสะสมผลงานตรวจสอบภายใน

2. ความคาดหวังต่อบทบาทงานตรวจสอบภายในในอนาคต

บทบาทที่เกี่ยวข้องกับประเด็นความเสี่ยง และการใช้กระบวนการบริหารความเสี่ยงสำหรับงานตรวจสอบภายใน ในฐานะของผู้ประกอบวิชาชีพ ถูกคาดหวังว่า

- **จะดำเนินการ ในลักษณะของผู้ที่เปี่ยมไปด้วยองค์ความรู้ มีความแม่นยำต่อเงื่อนไขที่เป็นหลักเกณฑ์หรือข้อกำหนด หรือแนวปฏิบัติ หรือบรรทัดฐาน หรือมาตรฐานที่ควรจะเป็น เพื่อสามารถให้คำแนะนำได้ว่าช่องว่างการดำเนินงานและจุดอ่อนองค์กรควรมีการดำเนินการอย่างไร**
- **จะใช้ความรู้และความสามารถที่มีอยู่ตลอดจนมุมมองที่มีความแม่นยำต่อเงื่อนไขที่เป็นหลักเกณฑ์หรือข้อกำหนด หรือแนวปฏิบัติ หรือบรรทัดฐาน หรือมาตรฐานที่ควรจะเป็น**
  - ทำการวิเคราะห์ข้อมูล จนมีความเข้าใจเกี่ยวกับสถานะของ กระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กร
  - ตั้งข้อสงสัยเยี่ยงผู้ประกอบวิชาชีพเพื่อนำไปสู่การกำหนดขอบเขตการตรวจสอบภายในที่เป็นประโยชน์และสร้างมูลค่าเพิ่มให้แก่องค์กร

- ⇨ **จะทำการสื่อสาร แจ้งเตือนเพิ่มเติม สร้างการตื่นตัวที่จำเป็น ผ่านการให้ข้อมูลต่อองค์กรต่อผู้มีส่วนได้ส่วนเสียและต่อสาธารณะในลักษณะที่เป็นข้อมูลเชิงลึก และ/หรือข้อมูลเชิงพยากรณ์ ที่ทำให้คณะกรรมการ ผู้บริหาร มีข้อมูลอันทรงคุณค่าประกอบการการตัดสินใจและปรับแผนกลยุทธ์ในอนาคตตามความจำเป็น**
- ⇨ **จะให้ความร่วมมือและร่วมดำเนินงานในลักษณะที่ประสานความสัมพันธ์กับหน่วยงานในกลุ่มงานที่เกี่ยวข้องกับวงจรการบริหารความเสี่ยงมากขึ้น โดยยึดโยงกับประเด็นความเสี่ยงสำคัญที่มีโอกาสส่งผลกระทบเกินยอมรับได้ต่อองค์กร ด้วยข้อมูลชุดเดียวกันหรือข้อมูลใกล้เคียงกัน**
- ⇨ **จะใช้ข้อมูลที่ได้จากการวิเคราะห์ความเสี่ยงควบคู่กับการวิเคราะห์บริบทขององค์กรในด้าน GRC PROCESS ทำการหารือและตกลงร่วมกับผู้บริหารสายงานที่เป็นเจ้าของภาระงานเพื่อทำให้เกิดพันธะผูกพัน (ENGAGEMENT) และทำการตรวจสอบตามพันธะผูกพันนั้น**

3. เครื่องมือที่ช่วยทำความเข้าใจและระบุสถานะของ GRC PROCESS

งานตรวจสอบภายในเป็นงานที่ให้บริการต่อองค์กรในการสร้างมูลค่าเพิ่มแก่องค์กร จึงต้องเริ่มจากการทำความเข้าใจต่อบริบทองค์กร โดยเฉพาะในส่วนของกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กรหรือ GRC PROCESS ไปสู่ระบุประเด็นที่สำคัญทั้งเป็นปัจจัยภายในองค์กร และปัจจัยภายนอกองค์กร ซึ่งมีความเชื่อมโยงกับวัตถุประสงค์ กลยุทธ์ และผลดำเนินงานโดยภาพรวมขององค์กร

- ⇨ การทำความเข้าใจต่อบริบทองค์กรและต่อกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กรหรือ GRC PROCESS จะทำให้งานตรวจสอบภายในสามารถระบุรายละเอียด ขององค์ประกอบ โครงสร้าง ผู้รับผิดชอบ ผลการดำเนินงานที่ผ่านมา สถานะในปัจจุบัน และแนวโน้มที่คาดว่าจะเกิดขึ้นในอนาคตได้
- ⇨ การดำเนินงานขององค์กรยังมีความเกี่ยวข้องกับภาคส่วนอื่นเป็นผู้มีส่วนได้ส่วนเสีย ตั้งแต่กิจการในห่วงโซ่อุปทาน คู่ค้าคู่สัญญา คู่ความร่วมมือ พันธมิตรธุรกิจ หน่วยงานกำกับดูแลตามกฎหมาย ไปจนถึงลูกค้าหรือผู้ใช้บริการ และสาธารณะหรือภาคประชาสังคม
  ซึ่งผู้มีส่วนได้ส่วนเสียดังกล่าวข้างต้นแต่ละภาคส่วน มีความคาดหวัง ร้องขอการดำเนินการจากองค์กร และมีความกังวลต่อผลดำเนินงานขององค์กรที่แตกต่างกัน รวมทั้งผู้มีส่วนได้ส่วนเสียแต่ละภาคส่วนยังมีบทบาท อิทธิพล ที่ทำให้องค์กรต้องให้ความสำคัญและนำมาเป็นข้อมูลประกอบการพิจารณา กำหนดกลยุทธ์ เป้าหมายผลดำเนินงานองค์กร รวมทั้งปรับเปลี่ยนบริบทขององค์กร ซึ่งกระทบต่อกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กรหรือ GRC PROCESS ด้วย

- ⇨ บริบทองค์กรและกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กร หรือ GRC PROCESS ประกอบด้วย ส่วนที่เป็นสภาพแวดล้อมที่ทำให้เกิดรูปแบบของการดำเนินงานขององค์กรที่เชื่อมโยง สัมพันธ์ และบูรณาการกับปัจจัยทั้งภายในและภายนอก ที่เกี่ยวข้องกับกิจกรรมและกระบวนการหลักขององค์กร

หน่วยงานตรวจสอบภายในจำเป็นต้องทำความเข้าใจต่อบริบทองค์กรและกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กรหรือ GRC PROCESS เพื่อให้สามารถระบุรายละเอียด และสถานะในเชิงคุณภาพ โดยเฉพาะความเพียงพอและประสิทธิผลของการดำเนินงาน รวมทั้งผู้รับผิดชอบที่เกี่ยวข้อง ตลอดจนผู้มีส่วนได้ส่วนเสียภายนอกที่มีความสัมพันธ์กัน

เครื่องมือที่นำมาใช้ในส่วนของกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กรหรือ GRC PROCESS เพื่อนำไปประกอบการดำเนินงานตามวงจรการตรวจสอบภายใน จึงเป็นเครื่องมือที่ต้องช่วยให้หน่วยงานตรวจสอบภายใน

- ⇨ สามารถระบุรายละเอียดและสถานะของกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กรหรือ GRC PROCESS ที่ทำให้เกิดรูปแบบการดำเนินงานขององค์กรตามที่ปรากฏอยู่
- ⇨ สามารถเชื่อมโยงประเด็นที่เป็นความเสี่ยงสำคัญจากปัจจัยแวดล้อมภายนอกองค์กร ที่มีผลกระทบให้องค์กรต้องมีการทบทวน และพิจารณาปรับเปลี่ยนกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กรหรือ GRC PROCESS เพื่อให้เหมาะสมตามสถานการณ์ และรองรับการเปลี่ยนแปลงที่จำเป็น
- ⇨ เครื่องมือที่เป็นหลักการสนับสนุนความสามารถของงานตรวจสอบภายใน ให้มีหลักเกณฑ์เงื่อนไข ข้อกำหนดที่มีความสมเหตุสมผลและยอมรับได้ในการระบุถึงสถานะความก้าวหน้าที่ควรจะเป็น ในระดับ Maturity Stage ของกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กรหรือ GRC PROCESS
- ⇨ เครื่องมือที่ช่วยงานตรวจสอบภายในในการประเมินถึงระดับความเพียงพอและประสิทธิผลของกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กรหรือ GRC PROCESS
- ⇨ เครื่องมือที่ช่วยในการระบุถึงขอบเขตและความจำเป็นของงานตรวจสอบภายในที่ต้องเข้าไปเกี่ยวข้องกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กรหรือ GRC PROCESS

4. เครื่องมือที่ช่วยระบุประเด็นเสี่ยงและวิเคราะห์และประเมินความเสี่ยง

เครื่องมือที่จะช่วยผู้ตรวจสอบภายในและหน่วยงานตรวจสอบภายใน ในการระบุความเสี่ยง และวิเคราะห์ ประเมิน และเรียงลำดับความเสี่ยง จะช่วยให้กระบวนการในการดำเนินการดังกล่าวของงานตรวจสอบภายใน เป็นไปอย่างมีระบบ มีหลักเกณฑ์ที่ใช้ในการดำเนินการ จนทำให้สามารถรวบรวมประเด็นความเสี่ยงสำคัญ ทั้งในระดับขององค์กร ความเสี่ยงที่อยู่ในความรับผิดชอบของผู้บริหาร อยู่ในความรับผิดชอบของผู้บริหารแต่ละสายงานที่เป็นเจ้าของภาระงาน อยู่ในความรับผิดชอบของหน่วยงานในกลุ่ม 2nd Line และความเสี่ยงที่ควรอยู่ในความรับผิดชอบของงานตรวจสอบภายในเอง

เครื่องมือที่จะช่วยระบุความเสี่ยงและวิเคราะห์ และประเมินความเสี่ยง สำหรับงานตรวจสอบภายในควรมีความครอบคลุมถึงเนื้อหาของมาตรฐานสากลด้านการตรวจสอบภายในฉบับใหม่ ปี 2024 ได้แก่

เครื่องมือที่ 1 เครื่องมือที่ช่วยในการกำหนด RISK THEME สำหรับงานตรวจสอบภายใน

เครื่องมือที่ 2 เครื่องมือที่ช่วยในการกำหนด AUDIT RISK UNIVERSE

เครื่องมือที่ 3 เครื่องมือ RISK MAPPING

ที่ช่วยในการระบุรูปแบบและหมวดหมู่ของประเด็นความเสี่ยง รวมทั้ง

- ⇨ ประเด็นความเสี่ยงโดยธรรมชาติ (INHERENT RISK)
- ⇨ ประเด็นความเสี่ยงที่หลงเหลือ (RESIDUAL RISK)
- ⇨ ประเด็นความเสี่ยงเกิดใหม่ (EMERGING RISK)
- ⇨ ประเด็นความเสี่ยงจากสถานการณ์สุดขั้ว (EXTREME RISK)

เครื่องมือที่ 4 เครื่องมือ RISK MATRIX

ที่ช่วยในการวิเคราะห์ประเด็นความเสี่ยง ในมิติต่างๆ

- ⇨ มิติของโอกาสเกิดหรือความน่าจะเป็นที่จะเกิด
- ⇨ มิติของระดับความรุนแรงจากผลกระทบที่ได้รับเมื่อเกิดเหตุการณ์ความเสี่ยง
- ⇨ มิติของความเฉียบพลันของผลกระทบที่เกิด

และนำผลการวิเคราะห์ประเด็นความเสี่ยงจัดทำ RISK MATRIX

เครื่องมือที่ 5 เครื่องมือ RISK – CONTROL MATRIX

ที่ช่วยในการวิเคราะห์เปรียบเทียบคุณภาพการควบคุม การรับมือและตอบโต้ต่อประเด็นความเสี่ยงที่มีความสำคัญ กับด้านบริหารจัดการจัดอยู่ในลำดับต้นๆ ของความเสี่ยง ให้อยู่ในเกณฑ์ที่ยอมรับได้ และส่วนที่ยังเกินกว่าเกณฑ์ที่ยอมรับได้ที่งานตรวจสอบภายในต้องให้ความสำคัญ

เครื่องมือที่ 6 เครื่องมือที่ใช้ในการกำหนดที่มาของเงื่อนไข (CRITERIA) การกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้ และค่าเบี่ยงเบนความเสี่ยงที่ยอมรับได้ในมุมมองของงานตรวจสอบภายใน

เครื่องมือที่ 7 เครื่องมือในการวิเคราะห์ RISK ROOT CAUSE ที่ช่วยให้งานตรวจสอบภายในสามารถระบุ ข้อเสนอแนะ สำหรับแผนการแก้ไขและปรับปรุงแก่ผู้บริหารสายงานที่รับผิดชอบภาระงาน

ในการดำเนินงานตามวงจรตรวจสอบภายใน ผู้ตรวจสอบภายในและหน่วยงานตรวจสอบภายในสามารถนำเครื่องมือดังกล่าวมาใช้ประกอบการจัดวางกลยุทธ์การตรวจสอบ การสื่อสารเพื่อแลกเปลี่ยน และแบ่งปันแนวคิดเกี่ยวกับการระบุ การวิเคราะห์ และประเมินความเสี่ยงแก่หน่วยงานในกลุ่มงานอื่น เพื่อทำข้อตกลงที่เป็นพันธะผูกพัน หรือความร่วมมือในการดำเนินงานให้บริการด้านการรับรองหรือให้ความเชื่อมั่นต่อประเด็นที่มีความเสี่ยง หรือกับผู้มีส่วนได้ส่วนเสียภายนอกองค์กรที่เป็นภาคส่วนสำคัญ เพื่อผนวกประเด็นเสี่ยงจากความคาดหวังของผู้มีส่วนได้ส่วนเสียภายนอกไว้ในแผนที่ความเสี่ยงของหน่วยงานตรวจสอบภายใน

5. เครื่องมือช่วยพัฒนารูปแบบใหม่ของวิธีการตรวจสอบ

มาตรฐานสากลด้านการตรวจสอบภายในฉบับใหม่ ปี 2024 ได้ระบุถึงรูปแบบใหม่และวิธีการตรวจสอบภายในสมัยใหม่ ที่อาจมีการใช้กันแล้วในประเทศอื่นๆ รวมทั้งมีความเชื่อมโยงกับมาตรฐานสากลด้านการควบคุมภายในหรือด้านการบริหารความเสี่ยงทั่วทั้งองค์กรในกลุ่มของ COSO แต่รูปแบบหรือวิธีการตรวจสอบดังกล่าวยังถือเป็นเรื่องใหม่ในประเทศไทย และในองค์กรขนาดใหญ่ในประเทศไทย

ด้วยเหตุนี้ การมีคู่มือที่ช่วยในการพัฒนารูปแบบใหม่หรือวิธีการตรวจสอบสมัยใหม่ ที่สอดคล้องกับแนวโน้มที่ปฏิบัติกันในประเทศที่ก้าวหน้าหรือพัฒนาแล้ว รวมทั้งมีการพิสูจน์ทราบมาแล้วด้วยการปฏิบัติงานจริง ว่าช่วยให้เกิดการประหยัด ลดการทำงานที่ทับซ้อนกัน หรือสอดคล้องกับรูปแบบของการดำเนินงานขององค์กรในลักษณะที่ข้ามสายงาน หรือมีลักษณะบูรณาการ ไม่ใช่การแบ่งแยกหรือปฏิบัติงานประจำตามปกติ

รวมทั้งสอดคล้องกับข้อจำกัดของทรัพยากร งบประมาณขององค์กร ตลอดจนข้อจำกัดด้านสมรรถนะและขีดความสามารถของบุคลากร ที่ไม่สามารถรวบรวมและสั่งสมความชำนาญที่ครอบคลุมได้ทุกด้าน

เครื่องมือสำคัญที่นำมาช่วยในการพัฒนารูปแบบใหม่ของวิธีการตรวจสอบภายในได้แก่

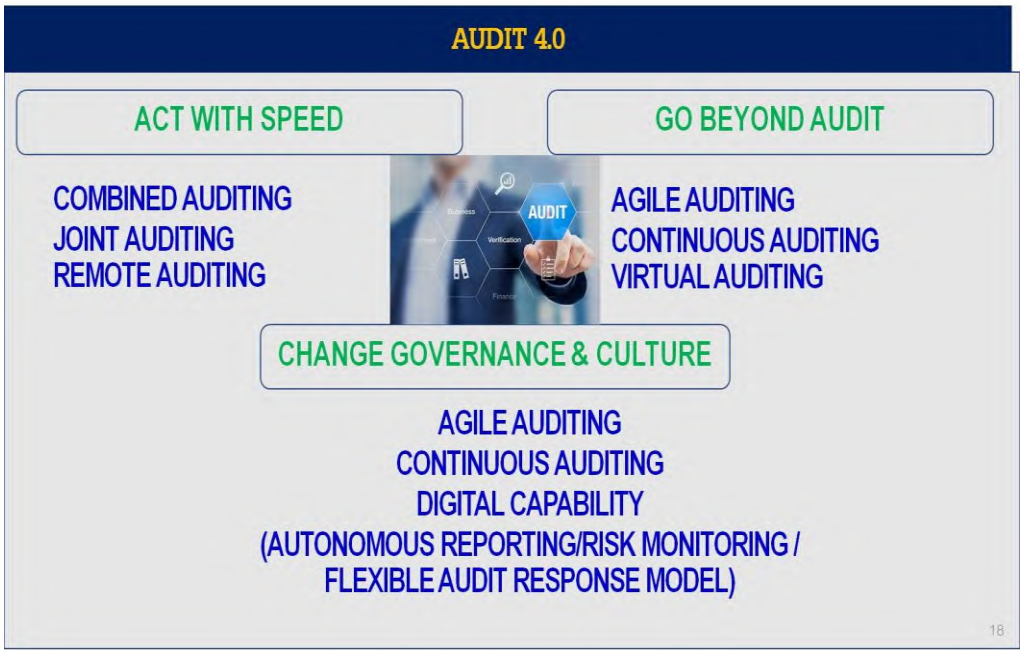
เครื่องมือที่ 1 เครื่องมือที่ช่วยพัฒนารูปแบบและวิธีการตรวจสอบแบบ AGILE AUDITING

เครื่องมือที่ 2 เครื่องมือที่ช่วยพัฒนารูปแบบและวิธีการตรวจสอบแบบ COMBINED AUDITING

เครื่องมือที่ 3 เครื่องมือที่ช่วยพัฒนารูปแบบและวิธีการตรวจสอบแบบ REMOTE AUDITING

บทที่ 1

กระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายในขององค์กร หรือ GRC กับงานตรวจสอบภายใน



มาตรฐานสากลด้านการตรวจสอบภายในฉบับใหม่ หรือ Global Internal Audit Standards 2024 ที่ออกประกาศใช้เมื่อ 9 มกราคม 2024 โดย The Institute of Internal Auditors (IIA) มุ่งที่จะปฏิรูปและยกระดับความเป็นวิชาชีพของงานตรวจสอบภายใน และทำให้งานตรวจสอบภายในมีส่วนสำคัญในการช่วยองค์กรให้สามารถรับมือ และตอบโต้ต่อความเสี่ยงท่ามกลางการเปลี่ยนแปลงรวดเร็วและความไม่แน่นอนสูง

1. GRC PROCESS ตามมาตรฐานสากลตรวจสอบภายใน 2024

ในบรรดาประเด็นที่มีการเปลี่ยนแปลงตามมาตรฐานสากลด้านการตรวจสอบฉบับใหม่ที่มีผลต่อบทบาทของ CAE (Chief Audit Executive) คณะกรรมการตรวจสอบ และผู้ตรวจสอบภายใน คือการที่งาน

ตรวจสอบภายในต้องมีความเข้าใจเชิงลึกและเพียงพอต่อกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือที่เรียกว่า GRC PROCESS – Governance , Risk and Control process ภายใต้เศรษฐกิจกระแสใหม่ ที่มีผลให้แต่ละองค์กรจำเป็นต้องมีการปรับเปลี่ยนกลยุทธ์องค์กรให้ทันต่อการเปลี่ยนแปลง ซึ่งส่งผลต่อกรอบการกำกับดูแลผลดำเนินงาน การรับมือและตอบโต้ต่อประเด็นความเสี่ยงสำคัญ และกลไกการควบคุมภายใน ที่มีประสิทธิผลในการจัดการต่อความท้าทายในอนาคตได้อย่างเพียงพอ

- **งานตรวจสอบภายในต้องทำความเข้าใจเกี่ยวกับกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายใน** เพื่อใช้เป็นเงื่อนไขบรรทัดฐานในการประเมิน ความเพียงพอและประสิทธิผลของการบริหารจัดการและผลดำเนินงานที่ควรจะเป็นขององค์กร

  Domain I วัตถุประสงค์การตรวจสอบภายใน (Purpose of Internal Auditing) นิยาม ระบุว่า

  งานตรวจสอบภายใน คือให้การรับรองด้วยความเชื่อมั่น และให้บริการคำแนะนำบนฐานของความเสี่ยงอย่างอิสระ internal audit's role in providing independent, risk-based assurance and advice to strengthen organizations

- **Domain I วัตถุประสงค์การตรวจสอบภายใน (Purpose of Internal Auditing)** การตรวจสอบภายในที่ดีต้องช่วยส่งเสริมและสนับสนุนองค์กร ให้บรรลุเป้าหมายดังต่อไปนี้
  - ประสบความสำเร็จในการบรรลุเป้าหมายตามวัตถุประสงค์
  - มีความเพียงพอและประสิทธิผลการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและกระบวนการควบคุมภายใน
- **Standard 4.2: Exercising Due Care** ระบุว่าในการพิจารณาระมัดระวังเยี่ยงผู้ประกอบวิชาชีพประกอบด้วยสถานการณ์และมุมมองความเสี่ยงที่ CAE ต้องพิจารณาเมื่อดำเนินการวิเคราะห์และประเมินความเสี่ยงซึ่งเป็นที่มาการทำแผนตรวจสอบภายใน สถานการณ์ที่เกี่ยวข้องอาจรวมถึง
  - วัตถุประสงค์และกลยุทธ์การดำเนินงานองค์กร และ
  - ความเพียงพอและประสิทธิผลของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยงและการควบคุมภายใน
- **Standard 8.1: Enabling Board Interaction** ความสามารถในการมีปฏิสัมพันธ์กับคณะกรรมการ ระบุว่า

  ให้คณะกรรมการต้องเพิ่มพูนความเข้าใจเกี่ยวกับประสิทธิผลของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กรอันเป็นผลมาจากผลการตรวจสอบและการหารือร่วมกับผู้บริหารระดับสูง

ให้ผู้บริหารระดับสูงต้องช่วยเหลือคณะกรรมการสร้างความเข้าใจเกี่ยวกับประสิทธิผลของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์

⇨ **Standard 9.1: Understanding Governance, Risk and Controls)** ความเข้าใจต่อการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายใน ระบุว่า

ด้วยความรู้ความเข้าใจในกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กรจะช่วยให้ CAE สามารถระบุและเรียงลำดับโอกาสที่จะให้บริการด้านการควบคุมภายในแก่องค์กร และยังช่วยส่งเสริมความสำเร็จขององค์กรได้ รวมทั้งระบุโอกาสวางกลยุทธ์และแผนตรวจสอบภายใน

⇨ **Standard 9.4: Creating a Risk-based Audit Plan** การตรวจสอบบนฐานความเสี่ยง ระบุว่า

การประเมินกลยุทธ์องค์กร วัตถุประสงค์ และประเด็นความเสี่ยงขององค์กรดังกล่าวต้องได้รับข้อมูลและรายละเอียดจากคณะกรรมการและผู้บริหารระดับสูงควบคู่กับการที่ CAE มีความเข้าใจเกี่ยวกับกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร

⇨ **Domain V ส่วนของบทนำ** ระบุว่า

บริการด้านการให้ความเชื่อมั่นมีจุดประสงค์ที่จะให้ความมั่นใจเกี่ยวกับกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายใน แก่ผู้มีส่วนได้ส่วนเสียองค์กร โดยเฉพาะอย่างยิ่งคณะกรรมการ ผู้บริหารระดับสูง และผู้บริหารสายงานที่เป็นเจ้าของภาระงานที่ทำการตรวจสอบ

⇨ **มาตรฐานย่อย 14.1 การรวบรวมข้อมูลเพื่อวิเคราะห์และประเมินผล (Gathering Information for Analyses and Evaluation)** ระบุว่า

ในการดำเนินงานวิเคราะห์และประเมินการตรวจสอบ ผู้ตรวจสอบภายในต้องรวบรวมข้อมูลที่มีคุณสมบัติสำคัญประกอบด้วย การรวบรวมมาจากที่ระบุซึ่งมีประสิทธิผลของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายใน

⇨ **มาตรฐานย่อย 14.2 การวิเคราะห์และระบุสิ่งที่ค้นพบที่อาจเกิดขึ้นจากผลตรวจสอบตามพันธะผูกพัน (Analyses and Potential Engagement Findings)** ระบุว่า

กรณีที่ผู้ตรวจสอบภายในตัดสินใจว่าไม่จำเป็นต้องมีการวิเคราะห์เพิ่มเติม และไม่มีความแตกต่างระหว่างเงื่อนไขที่เป็นบรรทัดฐานที่ใช้ประเมินกับสถานะที่พบจากการตรวจสอบในปัจจุบัน ผู้ตรวจสอบภายในต้องให้ความเชื่อมั่นไว้ในผลสรุปการตรวจสอบ ที่เกี่ยวข้องถึงประสิทธิผลของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายใน

2. ตีความข้อกำหนดตามมาตรฐานสากลฉบับใหม่ 2024

ในฐานะที่ผู้ตรวจสอบภายในเป็นผู้ประกอบวิชาชีพ (Audit Professional) การทำความเข้าใจต่อบริบทการดำเนินงานขององค์กรกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS

- ⇨ **กระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS เป็นองค์ประกอบและโครงสร้างที่แต่ละองค์กรทำการออกแบบ จัดวาง เปลี่ยนแปลงและแก้ไขได้เอง** หากเห็นว่ามีความจำเป็นหรือมีความเหมาะสมเพื่อนำไปสู่สถานะที่ดีขึ้น โดยเฉพาะในการบริหารจัดการเชิงกลยุทธ์และผลดำเนินงานโดยรวมขององค์กร
- ⇨ **แต่ละองค์กรย่อมมีบริบทการดำเนินงานที่แตกต่างกัน**ทำให้กระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS มีความแตกต่างกันตามไปด้วย
- ⇨ **แต่ละองค์กรเผชิญหน้ากับสภาพแวดล้อมจากปัจจัยภายนอกที่มีผลต่อการดำเนินงานแตกต่างกัน** ตามบริบทการดำเนินงานขององค์กร กระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS จึงต้องมีการปรับตัวให้ยืดหยุ่นและสอดคล้องกับสภาพแวดล้อมจากปัจจัยภายนอกด้วย
- ⇨ **ระบบงานตรวจสอบภายในถือเป็นส่วนหนึ่งของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ตามกรอบแนวคิดของ LINES OF DEFENSE** จึงมีความรับผิดชอบที่จะต้องมีส่วนในการส่งเสริม สนับสนุน ผลักดันไปสู่ ระดับที่มีประสิทธิภาพและประสิทธิผล
- ⇨ **บทบาทหน่วยงานตรวจสอบภายในเป็นการระบุถึงประเด็นที่เกี่ยวข้องทั้งจากภายในและภายนอกองค์กรที่มีผลต่อความสำเร็จขององค์กร ซึ่งองค์กรต้องมีการแก้ไข ปรับปรุง หรือพัฒนากระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS** ทั้งในระดับมหภาคและในระดับที่แยกส่วนรายสายธุรกิจ หรือหลายพื้นที่ส่วนที่เป็นจุดอ่อนอย่างมีนัยสำคัญเพื่อให้สามารถต้านทานต่อประเด็นที่มีโอกาสเกิดผลในทางลบต่อองค์กร ทำให้สถานะของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS มีโอกาสเปลี่ยนแปลงไปตามสถานการณ์แวดล้อม

- ข้อกำหนดดังกล่าวสะท้อนให้เห็นว่ามาตรฐานสากลด้านการตรวจสอบภายใน**ให้ความสำคัญกับการที่งานตรวจสอบภายในต้องมีความเข้าใจอย่างดีต่อโครงสร้างของมาตรฐานการบริหารจัดการองค์กรสมัยใหม่ที่พูดถึงบริบทขององค์กร**
- **มีความตระหนักว่าในการดำเนินงานประจำวันแต่ละองค์กร**ทั้ง

  (ก) ที่เกี่ยวข้องกับการดำเนินงานภายในองค์กรเองและ

  (ข) ที่เกี่ยวข้องกับบุคคลอื่นภายนอกองค์กร

  ย่อมอาศัยกิจกรรมที่มีประสิทธิภาพและประสิทธิผลของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ซึ่งเชื่อมโยงกับกลยุทธ์ และผลประกอบการในภาพรวมขององค์กร
- **กรณีที่กระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS มีความเกี่ยวข้องกับบุคคลอื่นภายนอกองค์กร** หมายถึงความเกี่ยวข้องกับผู้มีส่วนได้ส่วนเสีย คู่ค้าคู่สัญญา คู่ความร่วมมือ พันธมิตรธุรกิจ ไปจนถึงภาคประชาสังคม ซึ่งตามขอบเขตการดำเนินงานของการตรวจสอบภายในตามมาตรฐานสากลฉบับใหม่ ระบุให้งานตรวจสอบภายในเป็นไปเพื่อผู้รับบริการ และเพื่อประโยชน์แห่งสาธารณะด้วย ความเข้าใจที่เกี่ยวข้องกับบุคคลอื่นภายนอกองค์กรดังกล่าว จึงอาจมีผลต่อการพิจารณานำไปสู่ การวางกรอบการดำเนินงานตรวจสอบภายในด้วย
- **วงจรการบริหารงานตรวจสอบภายในรวมทั้งการดำเนินงานด้วยความระมัดระวังให้ความสำคัญกับผลที่ได้จากการทำความเข้าใจและวิเคราะห์ต่อกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS** ขององค์กร ด้านความเพียงพอและประสิทธิผลในการรับมือกับความเปลี่ยนแปลงและความไม่แน่นอน ซึ่งในปัจจุบันที่มีการเปลี่ยนแปลงไป และแนวโน้มในอนาคตที่อาจจะต้องมีการเปลี่ยนแปลงตามการเปลี่ยนแปลงของสถานการณ์และสภาพแวดล้อมองค์กร

3. กระบวนการทำความเข้าใจ GRC PROCESS สำหรับงานตรวจสอบ

กระบวนการดำเนินการของงานตรวจสอบภายในที่เกี่ยวข้องกับการทำความเข้าใจต่อกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ซึ่งเป็นการทำความเข้าใจต่อบริบทขององค์กร ทั้งในส่วนที่เกี่ยวข้องกับปัจจัยภายในองค์กรเอง และปัจจัยภายนอกที่เกี่ยวข้องกับการดำเนินงานขององค์กร เพื่อให้ได้ข้อมูลที่นำมาใช้ประโยชน์ในการดำเนินงานสำหรับงานตรวจสอบภายใน จึงครอบคลุมตั้งแต่

กระบวนการที่ 1 การแสวงหาข้อมูลเพื่อระบุสถานะ

(1) การระบุผู้มีส่วนได้ส่วนเสียภายนอกที่เกี่ยวข้องกับบริบทองค์กร

(2) การทำความเข้าใจต่อปัจจัยภายนอกองค์กรที่มีผลกระทบต่อการดำเนินงานขององค์กร ตามบริบทองค์กร

(3) การประเมินถึงสภาพแวดล้อมการควบคุมภายในขององค์กร ทั้งในด้านของโครงสร้าง วัฒนธรรม ทรัพยากร ศักยภาพและสมรรถนะ จุดแข็งและจุดอ่อน ตลอดจนผลการดำเนินงานโดยรวมขององค์กร เพื่อรองรับ การขับเคลื่อนองค์กรตามบริบทที่กำหนดไว้

(4) การกำหนดขอบเขตและรูปแบบการดำเนินงานขององค์กร ภายใต้วัตถุประสงค์ที่กำหนดไว้ รวมทั้งการระบุถึงผลิตภัณฑ์ บริการ และกระบวนการภายในการดำเนินงานขององค์กร

(5) การระบุถึงเงื่อนไข ข้อกำหนด ความคาดหวัง สิ่งที่ต้องการและเรียกร้องจากองค์กร ที่มาจากผู้มีส่วนได้ส่วนเสียแต่ละภาคส่วน

(6) การนำสิ่งที่มีความเข้าใจดังกล่าวข้างต้นมาทำการจัดวางเป็นสถานะและองค์ประกอบของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ภายใต้บริบทองค์กร

ผลที่ได้จากกระบวนการข้างต้น ➔ แผนภาพของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS

GRC PROCESS MAPPING

กระบวนการที่ 2 เฝ้าระวัง ติดตาม ทบทวนและปรับปรุงสถานะ

(7) การมอบหมายให้มีบุคลากรของงานตรวจสอบภายในเองที่ทำการเฝ้าระวังและติดตามการเปลี่ยนแปลงและเคลื่อนไหวของประเด็นที่เป็นปัจจัยต่างๆ ที่กล่าวมาแล้วข้างต้น เพื่อนำมาสู่การพิจารณาทบทวน และปรับปรุงสถานะและองค์ประกอบของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ให้เป็นปัจจุบันอยู่เสมอ ตามการเปลี่ยนแปลงและการปรับตัวตามสถานการณ์

ผลที่ได้จากกระบวนการข้างต้น ➔ แผนภาพของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ที่ผ่านการทบทวนและปรับปรุงให้เป็นปัจจุบัน

กระบวนการที่ 3 การนำ GRC PROCESS MAPPING ไปใช้ประโยชน์

(8) การบูรณาการสถานะและองค์ประกอบของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS เข้ากับกระบวนการวิเคราะห์

และประเมินความเสี่ยงเพื่อนำมาสู่การกำหนดขอบเขตความรับผิดชอบของงานตรวจสอบภายใน

(9) การสื่อสารทำความเข้าใจ GRC PROCESS MAPPING กับวงจรการบริหารงานตรวจสอบภายใน

(10) การติดตามสถานะการปรับปรุงและพัฒนาที่ดีขึ้นของ GRC PROCESS MAPPING ที่มาจากผลงานให้บริการตรวจสอบภายใน

ผลที่ได้จากกระบวนการข้างต้น ➔ หลักฐานที่แสดงถึง คุณภาพงานตรวจสอบภายใน และผลดำเนินงาน ด้าน GRC PROCESS

4. การบริหารจัดการข้อมูลที่เป็นความเข้าใจ GRC PROCESS

4.1 ข้อมูลที่ได้จากความเข้าใจต่อ GRC PROCESS

➔ **เป็นข้อมูลสำคัญที่นำไปสู่กระบวนการวิเคราะห์และประเมินประเด็นความเสี่ยงสำคัญ (Risk Assessment)** ซึ่งหากเกิดขึ้นจริงจะมีผลกระทบต่อองค์กรเกินกว่ายอมรับได้ ในมุมมอง ตรวจสอบภายใน

➔ **เป็นข้อมูลสำคัญที่นำไปสู่การจับคู่กับแผนที่ความเสี่ยง (Global Risk Mapping)** ที่เป็นสภาพแวดล้อมการเปลี่ยนแปลงและความไม่แน่นอนภายนอกองค์กร เพื่อหาว่าประเด็นความเสี่ยงได้จากภายนอกที่น่าจะมีผลกระทบต่อความสำเร็จขององค์กรผ่านกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร (GRC Process) และเปรียบเทียบกับผลการวิเคราะห์และประเมินความเสี่ยงตลอดจนเกณฑ์ความเสี่ยงที่ยอมรับได้และค่าเบี่ยงเบนความเสี่ยงที่จัดทำโดยฝ่ายจัดการ ผ่านการประเมินตนเองของหน่วยงานในกลุ่มงาน 1st Line และการรวบรวมประเด็นความเสี่ยงสำคัญในระดับองค์กรของหน่วยงานในกลุ่มงาน 2nd Line ที่ทำให้เห็นส่วนที่มีความแตกต่างและส่วนที่มีความเห็นไปในทิศทางเดียวกัน

➔ **จัดทำแผนที่เชื่อมโยงแสดงแนวโน้มเชิงกลยุทธ์องค์กรและแนวทางบริหารจัดการผ่านกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร (GRC Process)** ที่มีความเป็นไปได้จะได้รับผลกระทบทางลบจากประเด็นความเสี่ยงสำคัญภายนอก (Risk – Strategy Mapping) กำหนด Audit Risk Theme ที่ควรจะเกี่ยวข้องกับบทบาทของงานตรวจสอบภายใน

- **พัฒนากลยุทธ์การตรวจสอบภายใน (Internal Audit Strategy) สำหรับหน่วยงานตรวจสอบภายใน**ที่มีความจำเป็นต้องสนับสนุนและปรับเปลี่ยนไปตามการเปลี่ยนแปลงของวัตถุประสงค์เชิงกลยุทธ์และความสำเร็จขององค์กร เพื่อเป็นแนวทางสำหรับงานตรวจสอบภายใน ในการใช้กลยุทธ์การตรวจสอบภายในบรรลุตามวัตถุประสงค์ของงานบริการตรวจสอบภายใน ในระยะ 3 ถึง 5 ปีข้างหน้า
- **ใช้ข้อมูลกิจกรรมการตรวจสอบภายในตามพันธะผูกพันเป็นแนวทางที่ใช้ในการกำหนดทรัพยากรที่จำเป็น** งบประมาณสนับสนุนสำหรับการดำเนินงาน ตลอดจนคุณสมบัติของบุคลากรที่เกี่ยวข้องกับวงจรงานตรวจสอบภายใน
- **ใช้ข้อมูลที่มีการจัดทำขึ้นไปกำหนดกิจกรรมตามฐานความเสี่ยงที่อยู่ภายใต้ขอบเขตการตรวจสอบภายใน (Risk-based Activity under audit review**) และใช้ประโยชน์ในการสื่อสารกับผู้รับผิดชอบสายงานที่เป็นเจ้าของภาระงานตามกิจกรรมที่อยู่ในขอบเขตการตรวจสอบภายใน เพื่อทำความเข้าใจและกำหนดกรอบการตรวจสอบรายพันธะผูกพัน (Engagement Audit)
- **ทำการสื่อสารผลการตรวจสอบภายในและนำเสนอรายงานผลการตรวจสอบภายใน**ที่แสดงให้เห็นถึงประเด็นที่ต้องมีการปรับปรุงแก้ไขในด้านกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS

4.2 วงจรงานตรวจสอบภายในที่เริ่มต้นจาก GRC PROCESS

จากวงจรการตรวจสอบภายในที่กล่าวมาข้างต้น ทำให้เห็นได้ว่ากระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS– Governance , Risk and Control process เป็นจุดเริ่มต้นและจุดสิ้นสุดบทบาทของวงจรการดำเนินงาน

1) ความเข้าใจที่เพียงพอต่อกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS มีความสำคัญในการเตรียมการงานตรวจสอบภายใน
   - ⇨ *ให้ความมั่นใจว่างานตรวจสอบภายในเป็นส่วนหนึ่งของวงจรการบริหารบริบทองค์กรภายใต้กระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS*
   - ⇨ *เกิดการใช้ประโยชน์จากกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ตามข้อกำหนดของมาตรฐานสากลด้านตรวจสอบภายใน*

⇨ *มีเอกสารหลักฐานที่ใช้ประกอบการยืนยันการดำเนินงานตรวจสอบภายในที่สอดคล้องกับมาตรฐานสากลด้านตรวจสอบภายใน*

2) ความเข้าใจที่เพียงพอต่อกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ทำให้สามารถประเมินถึงความเพียงพอและประสิทธิผลในเบื้องต้นของการรับมือและตอบโต้ต่อความเสี่ยงสำคัญ ที่คาดว่าจะมีผลกระทบต่อความสำเร็จตามวัตถุประสงค์ กลยุทธ์ และผลประกอบการขององค์กรในภาพรวม

⇨ ประเด็นย่อยส่วนที่ตั้งข้อสงสัยเยี่ยงผู้ประกอบวิชาชีพว่า GRC PROCESS ยังไม่เพียงพอในการรับมือและตอบโต้ต่อความเสี่ยง คือกิจกรรมที่อยู่ภายใต้การตรวจสอบตามพันธะผูกพัน

⇨ ผลการวิเคราะห์และประเมินสถานะของ GRC PROCESS นำสู่การหารือแลกเปลี่ยนความคิดเห็นกับหน่วยงานอื่น และกับผู้บริหารสายงานที่รับผิดชอบภาระงานนั้น ๆ

⇨ ผลการวิเคราะห์และประเมินความเสี่ยงนำสู่การร่วมมือ บูรณาการ ประสานงานและแบ่งขอบเขตหน้าที่ความรับผิดชอบในการรับรองเพื่อให้ความเชื่อมั่นด้านความเพียงพอและประสิทธิผลของ GRC PROCESS ร่วมกัน

3) ความเข้าใจที่เพียงพอต่อกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ทำให้งานตรวจสอบภายในสามารถเริ่มต้นเข้าสู่วงจรของการวิเคราะห์และประเมินความเสี่ยงในมุมมองของงานตรวจสอบภายในได้ เพราะกิจกรรมที่อยู่ในขอบเขตของการตรวจสอบภายในอาศัยการวิเคราะห์และประเมินด้วยฐานความเสี่ยง

⇨ เชื่อมโยงไปสู่การพัฒนา AUDIT RISK THEME

⇨ คัดเลือกและเรียงลำดับความสำคัญของ AUDIT RISK UNIVERSE จาก AUDIT RISK THEME

⇨ วิเคราะห์และประเมิน RISK – CONTROL MATRIX

⇨ กำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้และค่าเบี่ยงเบนความเสี่ยงที่ยอมรับได้ในมุมมองของงานตรวจสอบภายใน

4) ความเข้าใจที่เพียงพอต่อกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ตั้งแต่แรก ทำให้งานตรวจสอบภายในสามารถให้บริการงานในขอบเขตของการตรวจสอบภายในได้

- ⇨ ให้บริการด้านความเชื่อมั่น (Assurance service) สรุปสถานการณ์ที่เป็นอยู่ในปัจจุบัน เทียบกับสถานการณ์ที่ควรเป็นภายใต้หลักเกณฑ์และเงื่อนไขที่เหมาะสม และมีประสิทธิผลขององค์กร
- ⇨ ให้บริการด้านคำแนะนำ (Advisory Service) โดยการวิเคราะห์ความแตกต่างของสถานการณ์ที่เป็นอยู่จริงในปัจจุบันกับสถานการณ์ที่ควรจะเป็นภายใต้หลักเกณฑ์และเงื่อนไขที่เหมาะสม และมีประสิทธิผล เพื่อนำไปสู่การปรับปรุงและส่งเสริม เพื่อยกระดับกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือที่เรียกว่า GRC – Governance , Risk and Control process ในอนาคต
- ⇨ ให้บริการงานตรวจสอบเชิงลึกเฉพาะเจาะจง (Special & Insight Auditing)
- ⇨ ให้บริการงานตรวจสอบภายในเชิงพยากรณ์ (foresight Auditing)

5. การกำหนดนิยามและความหมายของ GRC PROCESS

การให้คำอธิบายหรือนิยามของคำว่า **"กระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS"** ในส่วนที่เชื่อมโยงกับงานตรวจสอบภายในมีแนวโน้มที่จะยึดโยงกับความหมายที่ขยายขอบเขตออกไปอย่างกว้างขวาง เนื่องจากบริบทการดำเนินงานขององค์กรแต่ละองค์กรมีความแตกต่างกัน มีขอบเขตในเชิงของพื้นที่ มีความมุ่งมั่นและยึดมั่นต่อเป้าหมายการดำเนินงาน พื้นที่กว้างใหญ่แตกต่างกัน รวมทั้งบริบทของการดำเนินงานมีแนวโน้มที่จะเปลี่ยนแปลงไปในอนาคต

ด้วยสาเหตุและที่มาของประเด็นเหล่านี้ส่งผลให้ภาระงานของตรวจสอบภายในที่เกี่ยวข้องกับการทำความเข้าใจต่อกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ไม่ใช่เรื่องง่ายอีกต่อไป

มิติที่ใช้ในการให้ความหมายของกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS อาจจะต้องครอบคลุมอย่างน้อย 4 มิติ เพื่อให้หน่วยงานตรวจสอบภายในของแต่ละองค์กรมีทางเลือกที่หลากหลายและสอดคล้องกับแนวโน้มในอนาคตในการที่จะพิจารณากำหนดนิยามดังกล่าวได้อย่างเหมาะสมกับบริบทขององค์กร

มิติที่ 1	**ความรับผิดชอบที่มีต่อโลก หรือ ONE PLANET MODEL**
มิติที่ 2	**ความรับผิดชอบเชิงพาณิชย์และเชิงสังคม หรือ COMMERCIAL vs SOCIAL ACCOUNTING**
มิติที่ 3	**ความรับผิดชอบที่มีต่อผู้มีส่วนได้ส่วนเสียภาคส่วนสำคัญหรือ OCEG'S INTEGRATED GRC**

มิติที่ 4 ความรับผิดชอบตามกลุ่มงานภายในองค์กร หรือ SEVEN LINES OF DEFENSE

มิติที่ 1 ONE PLANET

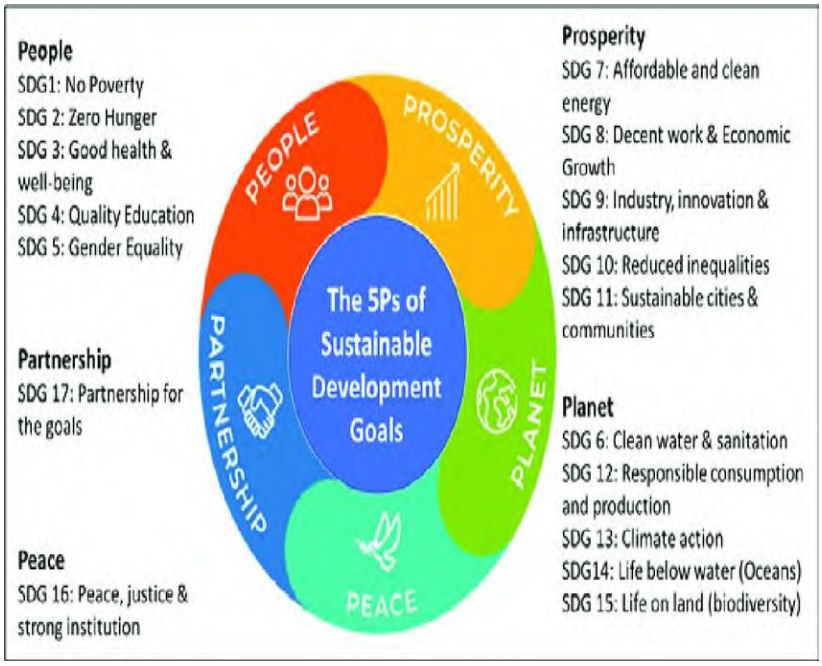
เป็นการนิยามที่พิจารณาตามบทบาทและความรับผิดชอบขององค์กร ในปัจจุบันความรับผิดชอบขององค์กรต่างๆ ไม่ใช่เพียงผลดำเนินงานภายในขององค์กรเองเท่านั้น หากกลายเป็นความรับผิดชอบขององค์กรที่มีต่อสังคมและสิ่งแวดล้อม หรือพิจารณาด้านความยั่งยืน ขององค์กร ระบบเศรษฐกิจ และสังคมด้วยด้วย การทำความเข้าใจต่อกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS สำหรับงานตรวจสอบภายในต้องแยกออกเป็นประเด็นดังนี้

1) กรณีที่ยึดโยงกับเป้าหมายการพัฒนาสู่ความยั่งยืนขององค์การสหประชาชาติ (The “5 Ps” of the UN Sustainable Development Goals) ซึ่งมีเป้าหมายที่จะสร้างผลกระทบในเชิงบวกต่อสังคมและสิ่งแวดล้อม ควบคู่กับการสร้างผลประโยชน์ต่อผู้ถือหุ้น และผู้มีส่วนได้ส่วนเสียโดยตรง องค์กรมีความรับผิดชอบที่ต้องบรรลุผลใน 5 ด้านด้วยกัน ประกอบด้วย
   (1) People หมายถึงความรับผิดชอบต่อคุณภาพชีวิตของคนในสังคม
   (2) Planet หมายถึงความรับผิดชอบต่อสิ่งแวดล้อม และภาพรวมที่เป็นปัญหาในระดับโลก

(3) Prosperity หมายถึงความรับผิดชอบต่อความเจริญรุ่งเรือง

(4) Peace หมายถึงความรับผิดชอบต่อการสร้างความสงบและสันติสุขให้เกิดขึ้นในสังคม

(5) Partnerships หมายถึงความรับผิดชอบต่อพันธมิตรทางธุรกิจ คู่ความร่วมมือ



ที่มา UN

ซึ่งเมื่อรวมกับ Profit ที่เป็นความรับผิดชอบต่อผู้ถือหุ้นและผู้มีส่วนได้ส่วนเสียโดยตรงขององค์กรแล้ว องค์กรจึงมีความรับผิดชอบทุกด้านรวมทั้งหมด 6 ด้าน ประกอบด้วย

- ความรับผิดชอบต่อผลดำเนินงานขององค์กรโดยตรง 1 ด้าน และ
- ความรับผิดชอบต่อกลยุทธ์ธุรกิจที่เน้นความยั่งยืนอีก 5 ด้าน

ทั้งนี้ แต่ละองค์กรต้องกำหนดให้ชัดเจนถึงเป้าหมาย ระดับความเกี่ยวข้องและความเชื่อมโยง การมุ่งเน้นขององค์กรเองภายใต้กรอบที่เป็นไปตาม 5P's องค์การสหประชาชาติ ซึ่งแยกเป้าหมายใหญ่ออกเป็น 17 เป้าหมาย

ซึ่งเป้าหมายใดก็ตามที่เกี่ยวข้องกัน องค์การต้องมีกระบวนการกำกับดูแล บริหารความเสี่ยง และควบคุมภายใน หรือ GRC PROCESS ที่สอดคล้องกัน และเป็นเงื่อนไขหลักเกณฑ์ที่จะนำมาใช้ในการดำเนินงานตรวจสอบภายในต่อไป

มิติที่ 2 การแบ่งแยกธุรกรรมและการบันทึกบัญชีองค์กร

เป็นแนวคิดที่ใกล้เคียงกับมิติที่ 1 โดยงานตรวจสอบภายในจะพิจารณาและทำความเข้าใจกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS ผ่านการแบ่งแยกธุรกรรมและการบันทึกบัญชีขององค์กร

องค์กรที่ใช้บริบทนี้จะพิจารณาดำเนินงานที่สอดคล้องกับความรับผิดชอบทางธุรกิจบนหลักการ 3 P's (Profit, People , Planet)

องค์กรที่ดำเนินงานตามกรอบแนวคิดและเป้าหมายการดำเนินงานแบบ 3 P's นี้ จะมีหรือการดำเนินงานที่โปร่งใส เปิดเผยข้อมูลต่อหน่วยงานกำกับดูแล สังคมและสาธารณชน ที่แยกให้เห็นถึงสิ่งที่เป็นธุรกรรมแต่ละด้านขององค์กรและผลการดำเนินงาน ผ่านการแสดงสถานะทางบัญชีและความมั่นคงทางการเงิน โดยแยกบัญชีออกเป็น 3 ส่วน

- **บัญชีที่มีการบันทึกธุรกรรมเชิงพาณิชย์ (Financial Accounting)**
  โดยใช้มาตรฐานการบัญชีที่เป็นที่ยอมรับทั่วไป ในลักษณะที่มีการดำเนินงานมาตั้งแต่เดิม
- **บัญชีที่มีการบันทึกธุรกรรมเชิงสังคม (Social Accounting)**
  โดยใช้มาตรฐานการบัญชีที่ออกแบบมาสำหรับการบันทึกบัญชีเชิงสังคมโดยเฉพาะ และรองรับผลตอบแทนทางสังคมที่เกิดขึ้นจากการใช้จ่ายทรัพยากร งบประมาณ และเงินทุนดำเนินงานขององค์กร รวมทั้งบัญชีทุนมนุษย์ และทุนสังคม
- **บัญชีที่มีการบันทึกธุรกรรมรองรับสิ่งแวดล้อม (Environmental Accounting)**
  โดยใช้มาตรฐานการบัญชีที่ออกแบบมาสำหรับการบันทึกบัญชีสำหรับสิ่งแวดล้อมโดยตรง ตัวอย่างเช่น บัญชีการปลูกป่า บัญชีการแก้ไข เยียวยา หรืออนุรักษ์สิ่งแวดล้อม

กรณีนี้ การดำเนินงานตรวจสอบภายในส่วนที่เกี่ยวข้องกับกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC PROCESS จะยึดโยงกับกระบวนการดำเนินงาน (Business Process) และการบันทึกธุรกรรมที่แยกจากกันในแต่ละประเภทของบัญชีเป็นแนวทางในการนำมาพิจารณาเพื่อกำหนดขอบเขต ของงานตรวจสอบภายในต่อไป

มิติที่ 3 OCEG's INTEGRATED GRC บริษัทมหาชน หน่วยงานภาครัฐ

กระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กร หรือ GRC ตามกรอบแนวคิดสำหรับกรณีบริษัทมหาชน หรือหน่วยงานภาครัฐ ด้วยการยึดโยงผลดำเนินงานองค์กรที่นำเอาความคาดหวัง เงื่อนไขและข้อกำหนดจากผู้มีส่วนได้ส่วนเสียหลัก 2 กลุ่มเข้ามาเกี่ยวข้องกับการกำกับดูแลองค์กร จึงยึดโยงอยู่บนมาตรฐานสากลที่เรียกว่า INTERGRATED GRC และขยายผลออกไปเป็น ES-G-RC ในอนาคต

ภายใต้กรอบมาตรฐานสากล INTERGRATED GRC

1) **GOVERNANCE** เป็นบทบาทของคณะกรรมการอำนวยการและฝ่ายจัดการหรือผู้บริหารระดับสูงมีความรับผิดชอบในการดำเนินงานองค์กร ที่ตื่นตัวต่อความเสี่ยงทางธุรกิจ (Business Risk) ที่จะกระทบต่อผลดำเนินงานที่เป็นเป้าหมายหรือวัตถุประสงค์หลักขององค์กร
2) **(Business) RISK** ก่อนที่จะตัดสินใจเชิงธุรกิจ หรือทำแผนธุรกิจใดๆ ที่มีเป้าหมายอยู่บนผลตอบแทนทางการเงิน ผลกำไร การเติบโตและขยายตัวขององค์กร ฝ่ายจัดการหรือผู้บริหารระดับสูงจะให้ความสำคัญกับการกำกับดูแลที่ดีบนหลักธรรมาภิบาลที่สอดคล้องกับความคาดหวังของผู้มีส่วนได้ส่วนเสียเพื่อแสดงว่าองค์กรยึดโยงกับการดำเนินธุรกิจอย่างมีจรรยาบรรณ และให้ความสำคัญกับการดำเนินงานตามกรอบจริยธรรม หรือยืนหยัดอยู่บนความถูกต้องเสมอ ไม่ใช่คำนึงถึงถึงผลกำไรขององค์กรเพียงอย่างเดียว
3) **COMPLIANCE** ก่อนที่จะตัดสินใจเชิงธุรกิจ หรือทำแผนธุรกิจใดๆ เพื่อเพิ่มพูนผลกำไร หรือผลประโยชน์ขององค์กร องค์กรจะให้ความสำคัญ กับการปฏิบัติที่สอดคล้องและครบถ้วนตามเงื่อนไขและข้อกำหนดทางกฎหมาย กฎระเบียบ ข้อบังคับ ประกาศ คำสั่งที่เป็นภาคบังคับของหน่วยงานกำกับดูแลที่มีอำนาจทางปกครอง ไม่กระทำการใดๆที่มีลักษณะผิดกฎหมาย ฝ่าฝืนหรือละเมิดกฎหมาย

องค์กรที่มีลักษณะเข้าข่ายมิติที่ให้ความสำคัญเพิ่มขึ้นจากเป้าหมายภายในองค์กรด้วยการยึดโยงกับความคาดหวังและข้อกำหนดจากผู้มีส่วนได้ส่วนเสียอย่างน้อย 2 ภาคส่วนสำคัญ (Stakeholder for Governance & Regulator for Compliance) ดังกล่าวข้างต้น จะทำให้การทำความเข้าใจกับกระบวนการกำกับดูแลที่ดี การบริหารความเสี่ยง และการควบคุมภายในขององค์กรหรือ GRC