คู่มือการประเมินการควบคุมภายใน (Internal Control Manual)

1. ชื่องาน	คู่มือการประเมินการควบคุมภายใน (Internal Control Manual)
2. วิธีการขั้นตอนการปฏิบัติงาน	กลไกสำคัญในการขับเคลื่อนการควบคุมภายในและการบริหารความเสี่ยงระดับปฏิบัติการ *หน้า 18* กรอบและแนวทางการจัดวางระบบการควบคุมภายใน *หน้า 19-21* กระบวนการประเมินความเสี่ยงและการควบคุมภายใน *หน้า 22-27* การรายงานผลการควบคุมภายใน *หน้า 28-30*
3. ระยะเวลาการปฏิบัติงานแต่ละขั้นตอน	Timeline การดำเนินงาน *หน้า 21* ขั้นตอนและระยะเวลาในการดำเนินการประเมิน GRC Assessment *หน้า 63*
4. กฎหมายที่เกี่ยวข้อง	กฎหมาย ระเบียบ ข้อกำหนด แนวปฏิบัติภายนอกและภายใน *หน้า 68*

หมายเหตุ: สามารถคลิกที่เลขหน้าเพื่อลิงก์ไปหน้าที่เกี่ยวข้องนั้น ๆ

คู่มือ
การประเมินการควบคุมภายใน
(Internal Control Manual)

ฉบับปรับปรุงปี 2568

ฝ่ายควบคุมภายในและจัดการความเสี่ยง (ภสญ.)

สารบัญ

สารบัญ

บทนำ

บริษัท ปตท.จำกัด (มหาชน) (ปตท.) มีสถานะเป็นรัฐวิสาหกิจและบริษัทจดทะเบียนในตลาดหลักทรัพย์ โดยมีพันธกิจในการดำเนินธุรกิจด้านพลังงานและธุรกิจที่เกี่ยวข้องอย่างครบวงจรในฐานะเป็นบริษัทพลังงานแห่งชาติ โดยดูแลผู้มีส่วนได้ส่วนเสียอย่างสมดุลและยั่งยืน ภายใต้วิสัยทัศน์ ปตท. "แข็งแรงร่วมกับสังคมไทย" และ "เติบโตในระดับโลก" อย่างยั่งยืน (Together For Sustainable Thailand, Sustainable World)

ปตท. ต้องเผชิญกับกระแสการแข่งขัน และการเปลี่ยนแปลงทางเศรษฐกิจ สังคม และสิ่งแวดล้อมที่รุนแรงและรวดเร็ว ซึ่งการเปลี่ยนแปลงดังกล่าวส่งผลกระทบต่อทิศทางกลยุทธ์ กระบวนการตัดสินใจทางธุรกิจ ตลอดจนการดำเนินงานและความสำเร็จขององค์กร

ปตท. มุ่งเน้นการสร้างการเติบโตทางธุรกิจบนพื้นฐานหลักการของความยั่งยืนอย่างสมดุล ทั้งด้านเศรษฐกิจ สังคม สิ่งแวดล้อม และการกำกับดูแลกิจการที่ดี ซึ่งแนวปฏิบัติเรื่องการควบคุมภายในและการบริหารความเสี่ยงถือเป็นรากฐานที่สำคัญ ในการดำเนินธุรกิจ ที่สามารถสร้างมูลค่าเพิ่มให้กับองค์กร ตลอดจนสร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสียและผู้เกี่ยวข้องทุกฝ่าย ในระดับสมเหตุสมผลว่าองค์กรจะบรรลุวัตถุประสงค์ และเป้าหมายในการดำเนินธุรกิจทั้งในระยะสั้น และระยาว

1

การควบคุมภายใน

1.1 ความหมายและวัตถุประสงค์ของการควบคุมภายใน

การควบคุมภายใน หมายถึง กระบวนการปฏิบัติงานที่ออกแบบร่วมกันโดยคณะกรรมการ ฝ่ายบริหาร และบุคลากรทุกคนขององค์กร เพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่า การดำเนินงานขององค์กรหน่วยงาน สามารถบรรลุวัตถุประสงค์ของการควบคุมภายใน 3 ประการ คือ

1. **Operation (O) ประสิทธิภาพและประสิทธิผลของการดำเนินงาน** หมายถึง การดำเนินงานอย่างมีประสิทธิภาพและประสิทธิผล การบรรลุเป้าหมายด้านการดำเนินงาน ด้านการเงิน ตลอดจนการใช้ทรัพยากร การดูแลรักษาทรัพย์สิน การป้องกันหรือลดความผิดพลาด ความเสียหาย การรั่วไหล การสิ้นเปลือง หรือการทุจริต

2. **Reporting (R) ความเชื่อถือได้ของรายงานทางการเงิน และไม่ใช่การเงิน** หมายถึง การจัดทำรายงานทางการเงิน และไม่ใช่การเงินขององค์กรหรือหน่วยงานที่ใช้ทั้งภายในและภายนอก โดยเป็นไปอย่างเชื่อถือได้ ทันเวลา และโปร่งใส

3. **Compliance (C) การปฏิบัติตามกฎหมาย ระเบียบและข้อบังคับ** หมายถึง การปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือ มติคณะรัฐมนตรีที่เกี่ยวข้องกับการดำเนินงานขององค์กรหรือหน่วยงาน รวมทั้งการปฏิบัติตามนโยบาย และวิธีการปฏิบัติงานที่องค์กรหรือหน่วยงานได้กำหนดขึ้น

1.2 แนวคิดของการควบคุมภายใน

ความหมายของการควบคุมภายในสะท้อนให้เห็นแนวคิดเกี่ยวกับการควบคุมภายในว่า**เป็นกระบวนการที่ดำเนินการอย่างต่อเนื่อง (Ongoing Process)** เป็นส่วนหนึ่งที่แทรกอยู่ในการปฏิบัติงานตามปกติ จึงไม่ใช่เหตุการณ์ใดเหตุการณ์หนึ่ง (Event) และไม่ใช่ผลของการกระทำ (Result) แต่เป็นกระบวนการ (Process)

"Internal Control is a PROCESS.
It's a means to an end, not an end in itself."

การมีระบบการควบคุมภายในที่ดี มีความสำคัญอย่างยิ่งต่อการดำเนินงานขององค์กร การควบคุมภายในสามารถช่วยป้องกัน บริหารจัดการความเสียหายต่างๆ ที่อาจเกิดขึ้นกับบริษัทและผู้มีส่วนได้ส่วนเสียได้เป็นอย่างดี อีกทั้งยังก่อให้เกิดความมั่นใจอย่างสมเหตุสมผลว่า องค์กรจะบรรลุวัตถุประสงค์และเป้าหมาย ทั้งด้านการดำเนินงาน การรายงาน และการปฏิบัติตามกฎระเบียบ ดังนั้นเป็นหน้าที่ของคณะกรรมการบริษัท ที่จะต้องดำเนินการให้มั่นใจว่า บริษัทมีระบบการควบคุมภายในที่เหมาะสมและเพียงพอ ในการดูแลการดำเนินงานให้เป็นไปตามเป้าหมาย และวัตถุประสงค์

ฝ่ายบริหารและบุคลากรทุกคนขององค์กร ต้องมีความเข้าใจในระบบและการประเมินการควบคุมภายใน เพื่อที่จะทำการจัดวางและประเมินระบบการควบคุมภายในขององค์กร ให้เป็นไปอย่างเหมาะสมและเพียงพอ

1.3 ขอบเขตและความจำเป็นของการควบคุมภายใน

ขอบเขตของการควบคุมภายใน

- การควบคุมภายในเป็นกระบวนการที่แทรกอยู่ในกระบวนการดำเนินงานและธุรกรรมขององค์กรที่ดำเนินการอยู่เป็นประจำวัน
- การควบคุมภายในจะต้องมีการกำหนดขึ้น ดำรงอยู่ และมีการกำกับติดตามประสิทธิผลของการควบคุมโดยผู้บริหารและบุคลากรทุกระดับ
- การควบคุมภายในเป็นส่วนหนึ่งของกลไกที่ช่วยให้การดำเนินงานสามารถบรรลุผลลัพธ์ตามเป้าหมายและวัตถุประสงค์ที่กำหนดไว้
- การควบคุมภายในจะต้องคำนึงถึงความคุ้มค่า การประหยัดค่าใช้จ่าย และได้ประโยชน์จากการควบคุมมากกว่าค่าใช้จ่ายที่ใช้ในการควบคุม
- ระบบของการควบคุมภายในในกิจการเป็นความรับผิดชอบของบุคลากรทุกคน ตั้งแต่ระดับบริหารถึงพนักงานระดับปฏิบัติการ

ความจำเป็นที่ทำให้องค์กรต้องมีการควบคุมภายใน

- เพื่อให้เกิดความรับผิดรับชอบ (Accountability) โดยความรับผิดชอบขั้นพื้นฐาน คือการบริหารทรัพยากรที่ได้รับการจัดสรรจากองค์กรให้เกิดประสิทธิภาพ ประสิทธิผล และความคุ้มค่า
- เพื่อส่งเสริมให้เกิดการปฏิบัติด้านการบริหารที่ดีในการปกป้องและรักษาสินทรัพย์ขององค์กร และทำให้เกิดมูลค่าเพิ่มแก่องค์กร ซึ่งมาจากการปฏิบัติงานที่ดี รายงานทางการเงินที่ครบถ้วน ถูกต้อง และการกำกับการปฏิบัติตามกฎเกณฑ์อย่างครบถ้วน

1.4 ความเชื่อมโยงของระบบการควบคุมภายในกับระบบอื่น

การควบคุมภายในกระบวนการปฏิบัติงานที่คณะกรรมการ ฝ่ายบริหาร และบุคลากรทุกคนขององค์กร มีบทบาทหน้าที่ร่วมกัน ดังนั้น เพื่อให้องค์กรสามารถบรรลุวัตถุประสงค์ของการควบคุมภายใน จึงต้องมีการบูรณาการ และเชื่อมโยงระบบการควบคุมภายในกับระบบงานอื่น ๆ

1. การกำกับดูแลกิจการที่ดี การบริหารจัดการความเสี่ยงในระดับปฏิบัติการและการควบคุมภายใน การปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร (GRC)

การควบคุมภายในเป็นส่วนหนึ่งของ GRC ซึ่งเป็นการบูรณาการการดำเนินการร่วมกันในการบรรลุวัตถุประสงค์และเป้าหมายทางธุรกิจ ดำรงไว้ซึ่งความถูกต้องสอดคล้องกับกฎหมายและกฎระเบียบ ความมีจริยธรรม ความโปร่งใส ความรับผิดชอบต่อสังคม ชุมชน และสิ่งแวดล้อม รวมถึงการต่อต้านทุจริตและคอร์รัปชันในทุกรูปแบบ

2. การบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management)

การบริหารความเสี่ยงทั่วทั้งองค์กร คือ กระบวนการที่คณะกรรมการ ผู้บริหาร และบุคลากรทั่วทั้งองค์กร ร่วมกันใช้กระบวนการบริหารความเสี่ยง ตั้งแต่การกำหนดกลยุทธ์ การระบุเหตุการณ์ที่อาจส่งผลกระทบต่อองค์กร และบริหารจัดการให้ความเสี่ยงอยู่ในระดับที่องค์กรยอมรับได้ผ่านการกำหนดกิจกรรมการควบคุมที่เพียงพอ เหมาะสม เพื่อให้มั่นใจได้ว่าสามารถบรรลุวัตถุประสงค์ขององค์กร

ทั้งนี้ รายการความเสี่ยงขององค์กร (Corporate Risk Profile) จะต้องถูกถ่ายทอดไปยังระดับกลุ่มธุรกิจ/หน่วยธุรกิจ และสายงานสนับสนุน (Business Group/ Business Unit & Support Function Level) และระดับหน่วยปฏิบัติงาน (Functional Level) โดย Risk Owner จะรับผิดชอบในการระบุความเสี่ยงที่ถูกถ่ายทอดจากระดับองค์กรในการประเมินการควบคุมภายในของหน่วยงานด้วย

1.4 ความเชื่อมโยงของระบบการควบคุมภายในกับระบบอื่น

3. การตรวจสอบภายใน

การตรวจสอบภายใน (Internal Audit : IA) เป็นกระบวนการตรวจสอบประสิทธิภาพและประสิทธิผลของกระบวนการกำกับดูแลที่ดี กระบวนการบริหารความเสี่ยง กระบวนการควบคุมภายในและการปฏิบัติงานต่าง ๆ ของ 1st และ 2nd Line ทั้งนี้ ในการวางแผนการตรวจสอบภายในจะใช้วิธีการวางแผนตามความเสี่ยง (Risk-Based Audit Approach)

4. ระบบบริหารจัดการของ ปตท. (PTT Integrated Management System: PIMS)

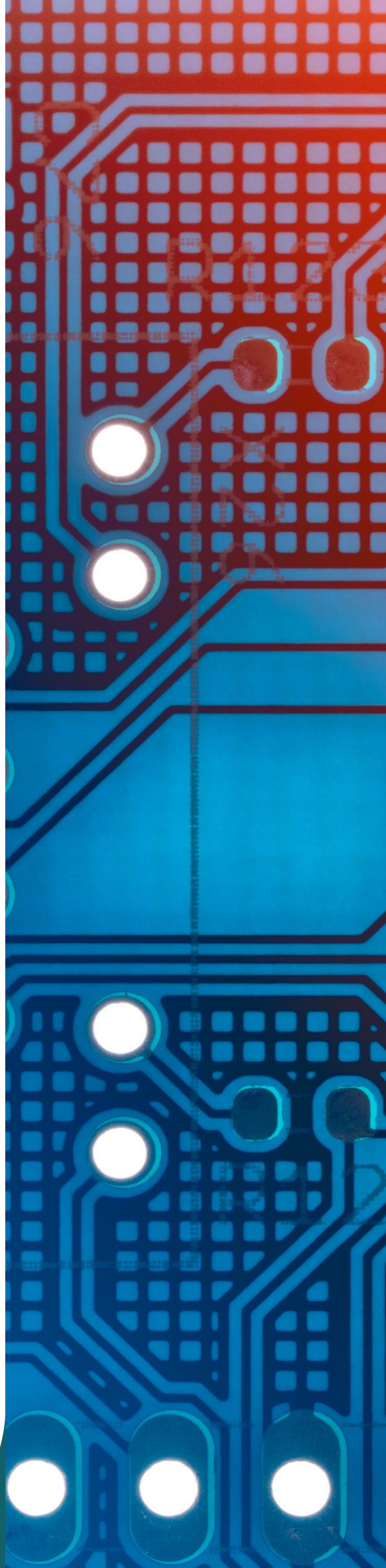
เป็นระบบการจัดการของ ปตท.ที่บูรณาการระบบงานขององค์กร (Organization System)กับมาตรฐานหรือแนวปฏิบัติที่ ปตท. นำมาประยุกต์ใช้ มุ่งเน้นให้หน่วยงานออกแบบ และปรับปรุงกระบวนการทำงานหลัก (Core Process) ให้สอดคล้องตามระบบฯ ผ่านการจัดทำเอกสารการปฏิบัติงานเพื่อใช้ในการกำกับดูแลการทำงานของตนเอง รวมถึงการทำงานที่เชื่อมโยงระหว่างหน่วยงาน และการส่งมอบงาน นับเป็นส่วนหนึ่งของการบริหารความเสี่ยงและควบคุมภายในเชิงป้องกัน ตลอดจนจัดให้มีการทวนสอบประสิทธิผลของการปฏิบัติผ่านการตรวจประเมินภายใน เพื่อให้มั่นใจว่าหน่วยงานมีการปฏิบัติเป็นไปตามระบบฯ รวมถึงมีการพัฒนา และปรับปรุงกระบวนการทำงานอย่างต่อเนื่อง

5. State Enterprise Assessment Model (SE-AM)

SE-AM เป็นระบบที่สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) นำมาใช้ในการประเมินผลการดำเนินงานของรัฐวิสาหกิจในประเทศไทย โดยมีวัตถุประสงค์เพื่อประเมินผลการดำเนินงานด้านความโปร่งใส การมีความรับผิดชอบ และประสิทธิภาพของการดำเนินงาน ซึ่งการประเมินแบ่งเป็น 2 ส่วน คือ 1.ส่วนของผลลัพธ์ ประกอบด้วย การดำเนินงานตามยุทธศาสตร์และผลการดำเนินงานตามตัวชี้วัดของรัฐวิสาหกิจ และ 2.ส่วนของกระบวนการปฏิบัติงานและการจัดการ (Core Business Enablers) ทั้ง 8 ด้าน โดยการบริหารความเสี่ยงและการควบคุมภายใน (Risk Management & Internal Control: RM&IC) มุ่งเน้นประสิทธิภาพของการบริหารความเสี่ยง และการสร้างมูลค่าเพิ่มให้กับองค์กร โดย ปตท. กำหนดนโยบาย และแนวทางการกำกับดูแล รวมถึงการสร้างวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยงเพื่อแสดงให้เห็นว่าองค์กรมีกระบวนการบริหารความเสี่ยงที่เป็นระบบ มีประสิทธิภาพ และมีการบูรณาการร่วมกับการควบคุมภายใน เพื่อเสริมสร้างศักยภาพขององค์กรให้สามารถตอบสนองต่อภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้นได้อย่างมีประสิทธิผล เพื่อให้องค์กรบรรลุวัตถุประสงค์เชิงยุทธศาสตร์ตามที่ได้กำหนดไว้

2

การจัดวางระบบการควบคุมภายในของ ปตท.



2.1 หน้าที่การจัดวางระบบการควบคุมภายในของ ปตท.

ปตท. ในฐานะรัฐวิสาหกิจ และบริษัทจดทะเบียนในตลาดหลักทรัพย์ มีหน้าที่จัดวางระบบการควบคุมภายใน และประเมินผลการควบคุมภายในอย่างน้อยปีละ 1 ครั้ง และสรุปผล รวมถึงจัดทำรายงานที่เกี่ยวข้องให้หน่วยงานกำกับดูแลตามกำหนด

รัฐวิสาหกิจ

- ปตท. มีหน้าที่จัดวางระบบการควบคุมภายใน ประเมินผลการควบคุมภายในอย่างน้อยปีละ 1 ครั้ง และจัดส่งรายงานให้กระทรวงการคลังผ่านกระทรวงพลังงาน ภายใน 90 นับจากวันสิ้นปีปฏิทิน ตาม พ.ร.บ. ประกอบรัฐธรรมนูญวินัยการเงินการคลังของรัฐ พ.ศ. 2561 ม. 79
- ปตท. มีหน้าที่รายงานผลประเมินการบริหารความเสี่ยงและการควบคุมภายใน (Risk Management and Internal Control : RM&IC) และปรับปรุงการดำเนินงานให้เป็นไปตามมาตรฐาน State Enterprise Assessment Model (SE-AM)
- ปตท. ต้องมีมาตรการควบคุมภายในที่เหมาะสมเพื่อป้องกันมิให้มีการกระทำความผิดสำหรับการให้สินบนเจ้าหน้าที่รัฐ เจ้าหน้าที่รัฐต่างประเทศ และเจ้าหน้าที่ขององค์กรระหว่างประเทศ ตาม พ.ร.บ. ว่าด้วยการป้องกันและปราบปรามทุจริต พ.ศ. 2561 ม.176

บริษัทจดทะเบียนในตลาดหลักทรัพย์

ปตท. มีหน้าที่สรุปความเห็นเกี่ยวกับประสิทธิผลของระบบการควบคุมภายในของบริษัทโดยคณะกรรมการบริษัท ในแบบแสดงข้อมูลประจำปี 56-1 (One Report) ของคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

2.2 การพัฒนาการควบคุมภายในของ ปตท.

2535
Internal Control Integrated Framework Issued by COSO

2544
- ปตท. จดทะเบียนในตลาดหลักทรัพย์
- ระเบียบ คตง.ว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน
- คณะกรรมการบริหารความเสี่ยง

2550
- COSO Framework
- คณะกรรมการบริหารระบบควบคุมภายใน

2553
- PTT Internal Control Framework
- Entity-wide Questionnaire Improvement
- CSA Facilitated Workshop

2554
- คณะกรรมการบริหารความเสี่ยงและควบคุมภายใน

2555
- แบบประเมินตนเองเกี่ยวกับมาตรการต่อต้านการคอร์รัปชั่น
- Specific Questionnaire

2556
- COSO Framework 2013
- นโยบายการควบคุมภายใน ปตท.
- Internal Control Database

2557
- E- Questionnaire
- PTT Group Policy (WoC)
- PTT Group Management System

2558
- พรบ. ป.ป.ช. 123/5
- Process Focused
  1. Anti- Corruption
  2. Procurement

2559
- Workshop 2nd Line
  1. Procurement
  2. Risk Management
  3. Budget
- คณะกรรมการแผนวิสาหกิจและบริหารความเสี่ยง (CPRC)

2560
- IC Health-Check
- IC E-Learning

2561
- IC Health-Check (Integrated GRC)
- พ.ร.บ. วินัยการเงินการคลังของรัฐ พ.ศ. 2561 มาตรา 79
- พรบ. ป.ป.ช. 176
- คณะกรรมการ GRCMC

2562
- GRC Assessment
- Specific Area in PTT & PTT Group

2563
- Risk & Control Platform (RCP)
- Integrated Process
- Management of Change
- คณะกรรมการกำกับดูแลกิจการที่ดี (CGC)

2564
- Supporting Assessment guideline by 2nd Line
- Promote GRC Agent
- Process and Sub-process alignment with PIMS

2565
- คณะกรรมการกำกับดูแลกิจการที่ดีและความยั่งยืน (CGSC)
- E learning ฉบับปรับปรุง
- IC Tools

2566
- Risk Owner ดีเด่น
- GRC Assessment Workshop in PTT (IT/OT และ Engineering & maintenance) and PTT Group by consultant
- Knowledge Awareness workshop
- Company Playbook

2567
- Risk Owner ดีเด่น
- Train the risk owner
- PTT Risk Management Integration

2568 Onward
- Risk Owner Role Model
- ESG Risk Assessment

นโยบายการควบคุมภายในของ ปตท. 2.3

ประกาศบริษัท ปตท. จำกัด (มหาชน)

เรื่อง นโยบายการควบคุมภายใน

เพื่อสร้างความเชื่อมั่นต่อผู้มีส่วนได้ส่วนเสียทุกภาคส่วนว่า ปตท. มีการปฏิบัติงานที่มีประสิทธิภาพและประสิทธิผล รายงานการเงินและรายงานการดำเนินงานมีความเชื่อถือได้ ดำเนินงานตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายขององค์กร ควบคู่กับการเป็นองค์กรที่มีการกำกับดูแลกิจการที่ดี ประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่ จึงกำหนดนโยบายการควบคุมภายใน ดังนี้

ข้อ 1 ปตท. ต้องพัฒนาระบบการควบคุมภายในตามมาตรฐานสากล และปลูกฝังเป็นวัฒนธรรมองค์กรควบคู่กับการสื่อสารให้พนักงานทุกคนตระหนักถึงความสำคัญของการควบคุมภายใน

ข้อ 2 กำหนดให้มีคณะกรรมการทำหน้าที่อำนวยการ กำหนดแนวทางการประเมินผลการควบคุมภายใน รวบรวม พิจารณากลั่นกรอง และสรุปผลการประเมินการควบคุมภายในในภาพรวมของ ปตท.

ข้อ 3 ผู้บริหารทุกระดับของ ปตท. มีหน้าที่รับผิดชอบในการกำหนด และจัดให้มีระบบการควบคุมภายในที่มีประสิทธิผล ริเริ่ม สร้างบรรยากาศเพื่อให้เกิดสภาพแวดล้อมของการควบคุม ปฏิบัติตนเป็นผู้นำและตัวอย่างที่ดีในเรื่องความซื่อสัตย์ ความมีคุณธรรม จริยธรรม ตลอดจนประเมินความเสี่ยงในระดับปฏิบัติการ และกำหนดกิจกรรมควบคุมที่เพียงพอ เหมาะสม และถ่ายทอดให้พนักงานในหน่วยงานนำการควบคุมภายในไปปฏิบัติและปรับปรุง รวมทั้งติดตามผลการดำเนินงานของหน่วยงานที่รับผิดชอบ

ข้อ 4 กำหนดให้มีหน่วยงานตรวจสอบ เป็นผู้สอบทานหรือประเมินผลการควบคุมภายในขององค์กรอย่างเป็นอิสระ เพื่อให้ความมั่นใจว่าหน่วยรับตรวจมีการควบคุมภายในที่มีประสิทธิภาพและประสิทธิผล มีการบริหารความเสี่ยงอยู่ในระดับที่ยอมรับได้

ข้อ 5 บุคลากรของ ปตท. มีหน้าที่ปฏิบัติงานตามระบบการควบคุมภายใน รวมถึงรายงานปัญหาจากการปฏิบัติงานให้ผู้บังคับบัญชารับทราบ เพื่อให้เกิดการปรับปรุงแก้ไขและลดผลกระทบที่อาจเกิดขึ้นได้อย่างทันท่วงที

ประกาศ ณ วันที่ 26 กุมภาพันธ์ พ.ศ. 2562

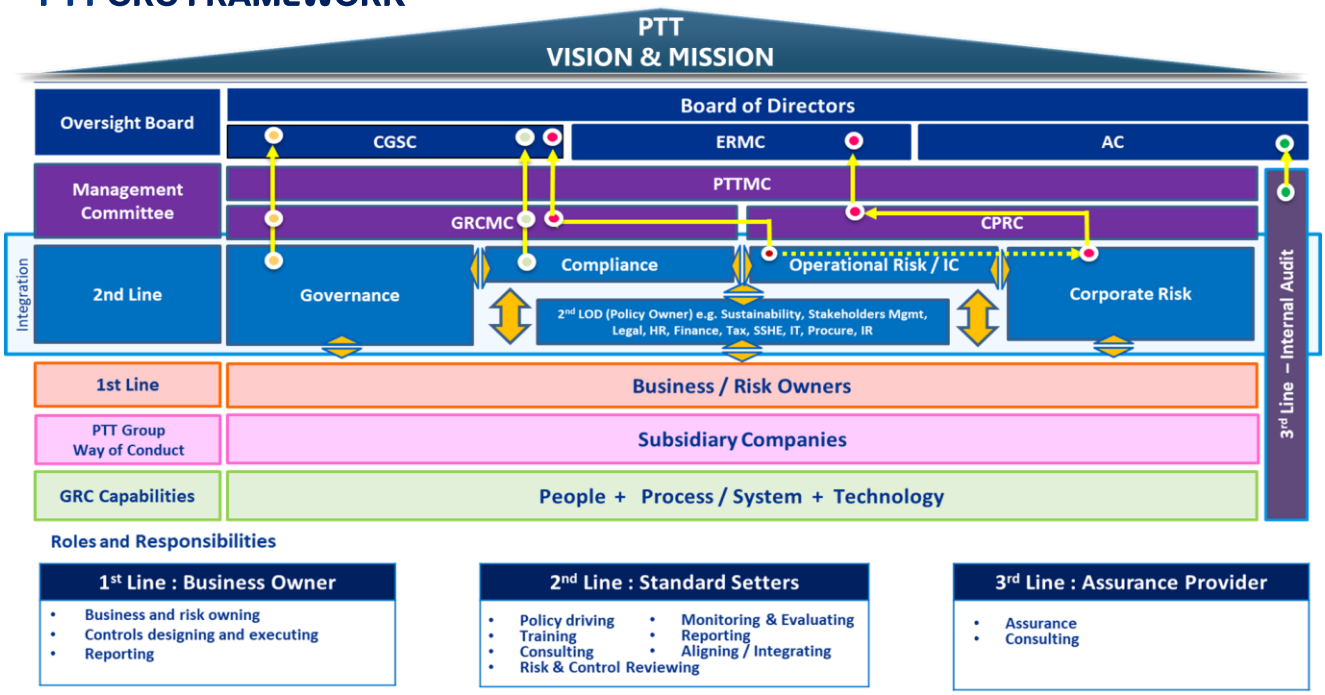
นายชาญศิลป์ ตรีนุชกร

ประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่

โครงสร้างและบทบาทหน้าที่ 2.4

ปตท. มีการกำหนดโครงสร้างการกำกับดูแลเฉพาะเรื่อง และได้นำหลักการ Three Lines Model จาก “The IIA's Three Lines Model 2020 ; The Update of Three Lines of Defense” ของสมาคมผู้ตรวจสอบภายในประเทศสหรัฐอเมริกา (IIA) มาปรับใช้ เพื่อแบ่งแยกบทบาทหน้าที่ของหน่วยงาน ไม่ให้เกิดการทับซ้อน และส่งเสริมการกำกับดูแลและการบริหารความเสี่ยงให้มีประสิทธิภาพ

PTT GRC FRAMEWORK



คณะกรรมการบริษัท ปตท. จำกัด (มหาชน) (Board of Director)

- กำหนดแนวทางการบริหารจัดการความเสี่ยงและการควบคุมในระดับองค์กร และกำกับดูแลกระบวนการบริหารจัดการความเสี่ยงและการควบคุมให้มีประสิทธิภาพ ประสิทธิผล

คณะกรรมการตรวจสอบ (Audit Committee)

- สอบทานประสิทธิภาพและประสิทธิผลของกระบวนการบริหารความเสี่ยง กระบวนการควบคุมภายใน และกระบวนการกำกับดูแลที่ดี รวมถึงระบบบริหารจัดการความเสี่ยงด้านการทุจริต และระบบการร้องเรียนและแจ้งเบาะแสการทุจริต (Whistleblowing) ของ ปตท.

โครงสร้างและบทบาทหน้าที่ 2.4

คณะกรรมการกำกับดูแลกิจการที่ดีและความยั่งยืนของบริษัท ปตท. จำกัด (มหาชน) (CGSC)

- กำกับดูแลและติดตามการดำเนินงานด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงในระดับปฏิบัติการและการควบคุมภายใน การปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร (GRC) การต่อต้านทุจริตและคอร์รัปชัน การบริหารจัดการความยั่งยืน และการดูแลสังคม ชุมชนและสิ่งแวดล้อม
- ให้ความเห็นชอบ วัตถุประสงค์ เป้าหมาย กลยุทธ์ กรอบการบริหารจัดการ รวมถึงแผนการดำเนินงานประจำปีด้านการควบคุมภายใน พร้อมทั้งมอบนโยบายและแนวทางการดำเนินงาน
- ให้คำแนะนำและคำปรึกษา แก่คณะกรรมการการกำกับดูแล การบริหารความเสี่ยง และการกำกับการปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร (GRCMC)

คณะกรรมการจัดการของ ปตท. (PTTMC)

- กำหนดทิศทางการกำกับดูแลธรรมาภิบาล และการบูรณาการงานด้านการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงในระดับปฏิบัติการและการควบคุมภายใน การปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร (GRC)

คณะกรรมการจัดการการกำกับดูแล การบริหารความเสี่ยง การกำกับการปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร และความยั่งยืน (GRCMC)

- กำกับการดำเนินงานด้าน GRC การต่อต้านทุจริตและคอร์รัปชัน การบริหารจัดการความยั่งยืน และการดูแลสังคม ชุมชน และสิ่งแวดล้อมให้มีการจัดทำแผนงานระยะสั้นและระยะยาวซึ่งสอดคล้องกับกรอบนโยบายของคณะกรรมการ CGSC
- กำกับดูแลและติดตามความคืบหน้าผลการดำเนินงานตามแผนงาน ให้ข้อคิดเห็น คำแนะนำ และให้คำปรึกษา เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพ และประสิทธิผล
- ผลักดัน ส่งเสริม และให้คำปรึกษา เพื่อให้หน่วยธุรกิจและสายงานสนับสนุน นำหลักการและนโยบายไปปฏิบัติ รวมถึงปรับปรุงกระบวนการทำงานให้สอดคล้องกับวัตถุประสงค์ของ ปตท. และเป็นไปตามกรอบการดำเนินงานที่กำหนด
- ส่งเสริมให้ขยายผลการดำเนินงานไปสู่บริษัทในกลุ่ม ปตท. รวมทั้ง กลุ่มผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง อาทิ คู่ค้า ลูกค้า เพื่อร่วมยกระดับสู่มาตรฐานสากล

โครงสร้างและบทบาทหน้าที่ 2.4

หน่วยงาน 1st Line (Business Owner/Risk Owner) : ทุกหน่วยงานใน ปตท.

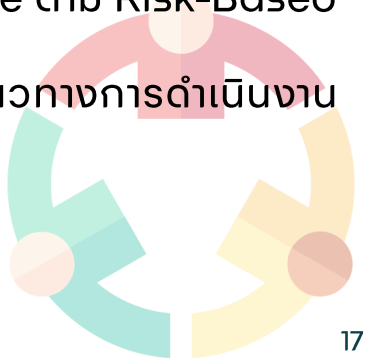
- ทบทวนกระบวนการทำงาน และกำกับดูแลงานของตนเองให้เป็นไปตามกฎหมาย กฎระเบียบ วัตถุประสงค์ขององค์กร
- บริหารความเสี่ยงพร้อมทั้งกำหนดการควบคุมภายในของหน่วยงาน และปรับปรุงการควบคุมดังกล่าวให้มีประสิทธิภาพ ประสิทธิผล
- หารือกับหน่วยงาน 2nd และ 3rd Line เพื่อพัฒนากระบวนการปฏิบัติงาน

หน่วยงาน 2nd Line (Standard Setter) : หน่วยงานซึ่งมีหน้าที่กำหนดมาตรฐาน นโยบาย ระเบียบ ข้อกำหนด ในภาพรวมขององค์กรอีกหน้าที่หนึ่ง

- กำหนดมาตรฐาน แนวปฏิบัติ นโยบาย ระเบียบ ข้อกำหนด
- บริหารจัดการความเสี่ยงและกำหนดการควบคุมภายในในภาพรวมองค์กร
- สื่อสาร ให้ความรู้ คำแนะนำ และสนับสนุนการปฏิบัติงานแก่ 1st Line
- ประสานงาน แลกเปลี่ยนข้อมูล และกำหนดแนวทางการดำเนินงานร่วมกันกับ 3rd Line

หน่วยงาน 3rd Line (Assurance Provider) : สำนักตรวจสอบภายใน

- ตรวจสอบประสิทธิภาพและประสิทธิผลของกระบวนการควบคุมภายใน กระบวนการกำกับดูแลที่ดี กระบวนการบริหารความเสี่ยง และการปฏิบัติงานต่าง ๆ ของ 1st และ 2nd Line ตาม Risk-Based Audit Approach
- ประสานงาน แลกเปลี่ยนข้อมูล และกำหนดแนวทางการดำเนินงานร่วมกันกับ 2nd Line



2.5 กลไกสำคัญในการขับเคลื่อนการควบคุมภายในและการบริหารความเสี่ยงระดับปฏิบัติการ

ปตท. กำหนดบทบาทหน้าที่ในการผลักดันการประเมินการควบคุมภายในในแต่ละระดับ ดังนี้

ผู้บริหารทุกระดับ

- กำหนด และจัดให้มีระบบการควบคุมภายในที่มีประสิทธิผล
- ประเมินความเสี่ยงในระดับปฏิบัติการและกำหนดกิจกรรมควบคุมที่เพียงพอ เหมาะสม
- ถ่ายทอดให้พนักงานในหน่วยงานนำการควบคุมภายในไปปฏิบัติและปรับปรุง
- ติดตามผลการดำเนินงานของหน่วยงานที่รับผิดชอบ

GRCMC

- กำกับดูแลให้มีการจัดทำแผนงานด้านการบริหารความเสี่ยงในระดับปฏิบัติการและการควบคุมภายใน
- กำกับดูแล ติดตามความคืบหน้า ให้ข้อคิดเห็นและคำปรึกษา
- ส่งเสริมให้มีการขยายผลการดำเนินงานไปสู่บริษัทในกลุ่ม รวมทั้งผู้มีส่วนได้ส่วนเสีย เพื่อร่วมยกระดับมาตรฐาน

IC Team

- จัดทำนโยบาย กรอบการควบคุมภายใน แนวทางการประเมินการควบคุมภายใน
- จัดให้มีการประเมินการควบคุมภายใน
- สรุปรายงานผลการประเมินฯ นำเสนอคณะกรรมการที่เกี่ยวข้อง และหน่วยงานกำกับดูแล

Risk Owner หน่วยงาน

- เป็นตัวแทนฝ่ายในการประเมินความเสี่ยงและการควบคุมภายใน (GRC Assessment) ประจำปีในระบบ RCP
- จัดเตรียมข้อมูลของหน่วยงาน เพื่อทำการประเมินความเสี่ยงและการควบคุมภายในประจำปี
- ทบทวนความเสี่ยงและควบคุมภายในตามสภาพแวดล้อมในการปฏิบัติงานที่เปลี่ยนแปลงไป
- สื่อความความเสี่ยงและจุดควบคุมที่สำคัญ แก่พนักงานในหน่วยงาน เพื่อจัดเก็บเป็นองค์ความรู้ขององค์กร
- จัดทำแผนปรับปรุงและดำเนินงานตามแผน

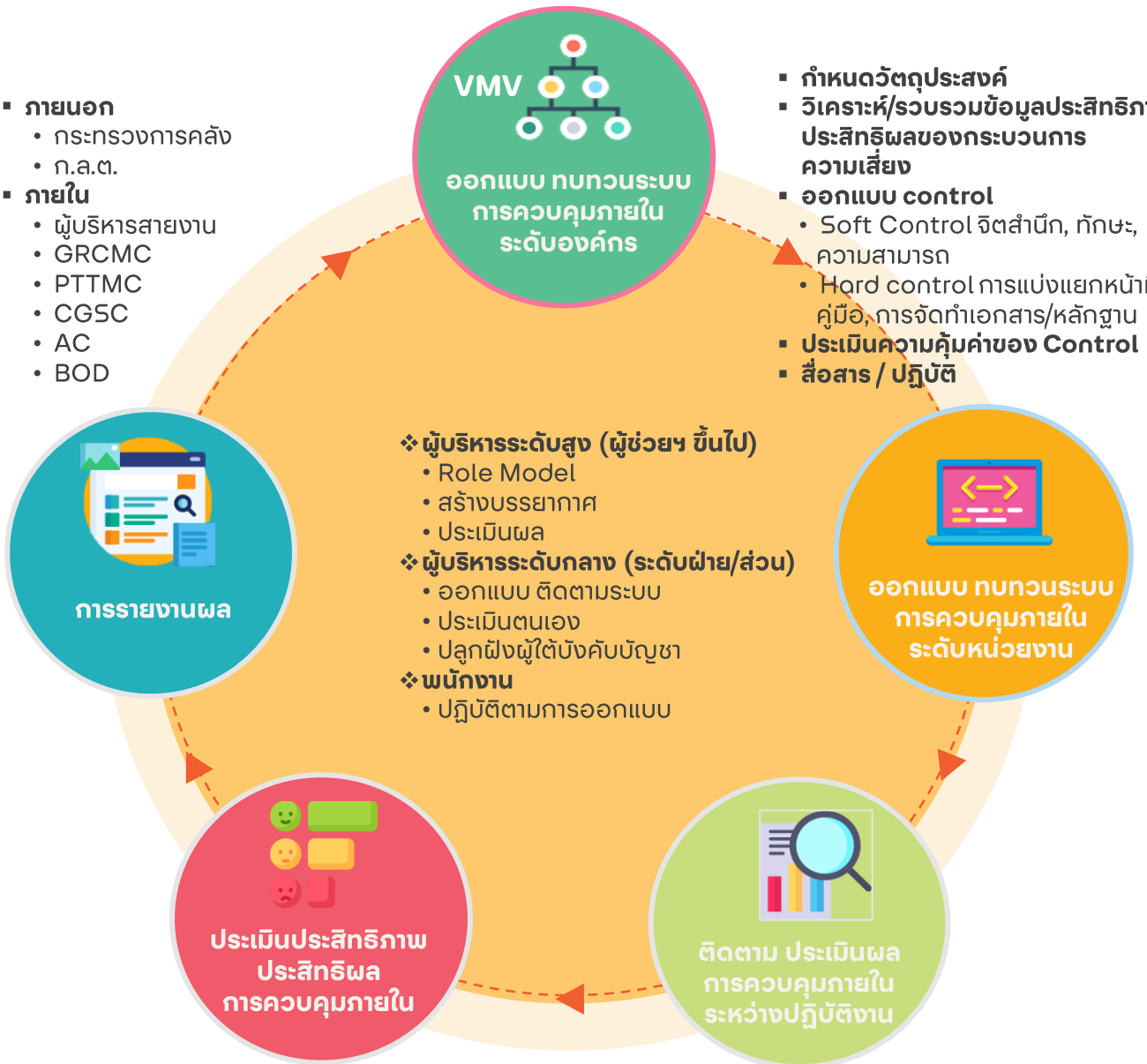
GRC Agent

- ศึกษาทำความเข้าใจงาน GRC
- เข้าร่วมอบรมเพื่อเสริมสร้างความรู้ความเข้าใจและพัฒนาศักยภาพในการปฏิบัติหน้าที่เป็น GRC Agent และเข้าร่วมกิจกรรมเกี่ยวกับ GRC
- ร่วมกำหนดเกณฑ์การประเมินความเสี่ยงระดับสายงาน (BU Risk Criteria)
- สื่อความแผน เกณฑ์ และวิธีการประเมินความเสี่ยงและการควบคุมภายใน รวมทั้งกฎหมาย กฎระเบียบที่เกี่ยวข้องในการปฏิบัติงานของหน่วยธุรกิจ/สายงาน
- ถ่ายทอดความรู้ สร้างความตระหนักด้านความสำคัญของการบริหารความเสี่ยง การควบคุมภายใน การปฏิบัติตามกฎหมายและกฎระเบียบภายใน ปตท.
- ให้คำแนะนำแก่หน่วยงานภายใต้สายงาน ในการระบุ และประเมินความเสี่ยง การควบคุม รวมถึงแผนการปรับปรุงกระบวนการ
- ส่งเสริมให้หน่วยงานในสายงานมีการ KM sharing ความเสี่ยงและจุดควบคุมที่สำคัญ
- รวบรวมผลการประเมิน และแผนการปรับปรุงความเสี่ยงและการควบคุมภายในของทุกหน่วยงานในสายงานและรายงานต่อผู้บริหารสายงาน
- รวบรวมข้อมูลเหตุการณ์ปฏิบัติที่ไม่สอดคล้องกับกฎหมายและกฎ ระเบียบองค์กร จัดทำแผนแก้ไข ปรับปรุงกระบวนการ และหาแนวทางป้องกันไม่ให้เกิดการปฏิบัติงานไม่สอดคล้องกับกฎหมายและกฎระเบียบ รวมถึงติดตามการรายงานข้อมูลการมีใบอนุญาตและสถานะการต่ออายุใบอนุญาตเพื่อป้องกันโอกาสเกิดเหตุ Non-Compliance จากการขาดต่ออายุใบอนุญาต

กรอบและแนวทางการจัดวางระบบการควบคุมภายใน 2.6

- **วางระบบการควบคุมภายใน**
  - กำหนดวิสัยทัศน์ ภารกิจ วัตถุประสงค์ ค่านิยม จรรยาบรรณ
  - กำหนดเป้าหมายระยะสั้น ระยะยาว
  - กำหนดโครงสร้างองค์กร หน้าที่ ความรับผิดชอบ
  - พัฒนาบุคลากร

- **ภายนอก**
  - กระทรวงการคลัง
  - ก.ล.ต.
- **ภายใน**
  - ผู้บริหารสายงาน
  - GRCMC
  - PTTMC
  - CGSC
  - AC
  - BOD



- **กำหนดวัตถุประสงค์**
- **วิเคราะห์/รวบรวมข้อมูลประสิทธิภาพประสิทธิผลของกระบวนการความเสี่ยง**
- **ออกแบบ control**
  - Soft Control จิตสำนึก, ทักษะ, ความสามารถ
  - Hard control การแบ่งแยกหน้าที่ คู่มือ, การจัดทำเอกสาร/หลักฐาน
- **ประเมินความคุ้มค่าของ Control**
- **สื่อสาร / ปฏิบัติ**

❖ **ผู้บริหารระดับสูง (ผู้ช่วยฯ ขึ้นไป)**
- Role Model
- สร้างบรรยากาศ
- ประเมินผล

❖ **ผู้บริหารระดับกลาง (ระดับฝ่าย/ส่วน)**
- ออกแบบ ติดตามระบบ
- ประเมินตนเอง
- ปลูกฝังผู้ใต้บังคับบัญชา

❖ **พนักงาน**
- ปฏิบัติตามการออกแบบ

- **การประเมินการควบคุมภายใน**
  - GRC Assessment
  - E-CSA
  - GRC Assessment in Key Process โดยพิจารณาประสิทธิภาพ ประสิทธิผลของกระบวนการ / ข้อบกพร่อง
- **การประเมินผลอย่างเป็นอิสระ**
  - Internal Audit
  - External Party

- **รวบรวมข้อมูลประสิทธิภาพ ประสิทธิผลของ Control**
- **Control Testing** เช่น การทดสอบความถูกต้อง การเปรียบเทียบข้อมูล
- **ทดสอบ Present และ Function ของ Control**
- **รายงานข้อบกพร่อง**

2.6 กรอบและแนวทางการจัดวางระบบการควบคุมภายใน

การกำหนดหรือการออกแบบระบบการควบคุมภายในที่มีประสิทธิผลมีขั้นตอนดังนี้

1. กำหนดวัตถุประสงค์ของหน่วยงาน และกระบวนการหลักที่ชัดเจนเพื่อช่วยให้ผู้บริหารสามารถบริหารและติดตามการปฏิบัติงาน พนักงานสามารถดำเนินงานให้บรรลุวัตถุประสงค์นั้นๆ ซึ่งการกำหนดวัตถุประสงค์ของหน่วยงานควรมีลำดับดังนี้
   - กำหนดภารกิจหลักของหน่วยงาน
   - กำหนดวัตถุประสงค์ของกระบวนการปฏิบัติงาน
2. กำหนดกระบวนการปฏิบัติงานและออกแบบการควบคุมให้มีครบทั้ง 5 องค์ประกอบของการควบคุมภายในที่จะทำให้การดำเนินงานสามารถบรรลุตามวัตถุประสงค์ที่กำหนดไว้ และสอดคล้องกับวัตถุประสงค์ของการควบคุมภายในทั้ง 3 ประการ คือ
   - ประสิทธิภาพประสิทธิผลของการดำเนินงาน (Operation: O)
   - ความเชื่อถือได้ของรายงานทางการเงิน และไม่ใช่การเงิน (Reporting: R)
   - การปฏิบัติตามกฎหมาย ระเบียบและข้อบังคับ (Compliance: C)
3. ประเมินความเสี่ยงทั้งจากปัจจัยภายในและภายนอกที่อาจทำให้การดำเนินงานไม่สามารถบรรลุวัตถุประสงค์ของกระบวนการปฏิบัติงาน รวมถึงการประเมินความเสี่ยงด้านทุจริต
4. พิจารณาว่ากระบวนการปฏิบัติงานและการควบคุมที่ออกแบบไว้สามารถที่จะป้องกันหรือลดความเสี่ยงได้
5. กำหนดหรือออกแบบกิจกรรมควบคุมเพิ่มเติมเพื่อป้องกันความเสี่ยง หรือลดความเสี่ยงที่เหลือให้อยู่ในระดับที่ยอมรับได้
6. ประมาณการต้นทุนที่จะต้องใช้ในการดำเนินการให้มีกิจกรรมควบคุมนั้นๆ และพิจารณาว่าต้นทุนหรือค่าใช้จ่ายต้องไม่สูงกว่าประโยชน์ที่จะได้รับจากการมีกิจกรรมควบคุม
7. กำหนดแผนในการนำกิจกรรมควบคุมนั้นมาปฏิบัติใช้ในการดำเนินงาน
8. ดำเนินการตามแผนและปฏิบัติตามการควบคุมที่ได้ออกแบบไว้ รวมทั้งติดตามและประเมินผล
9. ประเมินประสิทธิภาพของการปฏิบัติงานและประสิทธิผลของการควบคุมภายใน (ตามเกณฑ์การประเมินการควบคุมภายใน (ภาคผนวก 4))

Timeline การดำเนินงาน 2.7

Q1

GRC Agent & Risk owner

- **GRC Agent และ Risk owner** รับฟังสื่อความบทบาทหน้าที่และแผนการดำเนินงานด้าน GRC ประจำปี

IC Team (ภสญ.)

- ทบทวนระเบียบ คำสั่ง และกฎหมายที่เกี่ยวข้อง เพื่อปรับปรุงนโยบาย กรอบการควบคุมภายใน แนวทางการประเมินการควบคุมภายใน
- ทบทวนฐานข้อมูลความเสี่ยง จุดควบคุมที่สำคัญ ให้สอดคล้องกับกระบวนการที่เปลี่ยนแปลงไป
- ทบทวนข้อมูลโครงสร้างองค์กร และเนื้อหา FD ของหน่วยงาน เพื่อจัดทำ Process List and Process Mapping สำหรับการประเมินฯ
- ทบทวนข้อมูลคำถามในการประเมิน E-CSA
- สื่อความบทบาทหน้าที่และแผนการดำเนินงานด้าน GRC ประจำปี ให้แก่ GRC Agent

Q2

- **Risk owner** รวบรวมผลการดำเนินงานของหน่วยงาน เช่นKPI, Non-Compliance ข้อคิดเห็นของผู้บริหาร ข้อมูลสถานการณ์ปัจจุบัน กฎหมายที่เปลี่ยนแปลง เป็นต้น เพื่อเป็นข้อมูลในการทบทวนการประเมินฯ
- **GRC Agent และ Risk owner** รับฟังสื่อความแผนและแนวทางการประเมิน GRC Assessment
- **Risk owner** ประเมินฯ และจัดทำแผนปรับปรุงการดำเนินงาน ร่วมกับพนักงานในหน่วยงาน และผู้จัดการฝ่าย พร้อมขออนุมัติผ่านระบบ RCP

- สื่อความแผนและแนวทางการประเมิน GRC Assessment ให้แก่ GRC Agent และ Risk owner
- Launch GRC Assessment เพื่อให้หน่วยงานทำการประเมิน

Q3

- ผู้บริหารระดับ EVP SEVP และ C Level ตอบ E-CSA และรับทราบการประเมิน GRC Assessment ของสายงาน
- **GRC Agent**
  - ติดตามและสอบทานความถูกต้องผลประเมินฯ ของหน่วยงานในสายงาน
  - รายงานสรุปผลการประเมินของสายงานต่อผู้บริหารสายงาน

- Launch E-CSA เพื่อให้ผู้บริหารทำการประเมิน
- ให้คำปรึกษาและสอบทานความถูกต้องของผลการประเมินฯ
- จัดทำรายงานสรุปผลการประเมินฯ ของแต่ละสายงานให้ GRC Agent

Q4

- สรุปและรายงานผลการควบคุมภายในของ ปตท. ต่อคณะกรรมการต่างๆ

GRCMC > PTTMC > CGSC > AC >BOD

- จัดทำรายงานผลการประเมินการควบคุมภายใน รายงานต่อหน่วยงานกำกับดูแล กระทรวงการคลัง/ก.ล.ต./ SE-AM

3

กระบวนการการประเมินความเสี่ยงและการควบคุมภายใน

3.1 การประเมินความเสี่ยงและการควบคุมภายใน

การประเมินการควบคุมภายใน คือ การประเมินประสิทธิภาพของการปฏิบัติงานและการประเมินประสิทธิผลของการควบคุมภายในว่าองค์ประกอบทั้ง 5 ของการควบคุม มีอยู่อย่างครบถ้วน สามารถทำงานอย่างสอดคล้องและสัมพันธ์กัน กล่าวคือการควบคุมภายในนั้นมีอยู่จริง (Present) และทำหน้าที่ได้จริง (Functioning)

Present – การควบคุมภายในมีอยู่จริงทั้งในด้านของการออกแบบและการนำไปปฏิบัติ

Functioning – การควบคุมภายในที่ออกแบบไว้สามารถทำหน้าที่ควบคุม จัดการ ป้องกัน หรือช่วยให้ค้นพบความเสี่ยงได้อย่างทันเวลาหรือสามารถทำหน้าที่ได้ตามที่ได้ออกแบบไว้

การประเมินการควบคุมภายใน จะดำเนินการควบคู่ไปกับการประเมินความเสี่ยงในระดับปฏิบัติการ โดยใช้แนวทางการประเมินความเสี่ยงตามคู่มือ Enterprise Risk Management (ERM) และคู่มือการบริหารความเสี่ยงด้านการทุจริตและคอร์รัปชัน

แนวทางการประเมินความเสี่ยงและการควบคุมภายใน

ปตท. กำหนดแนวทางประเมินความเสี่ยงระดับปฏิบัติการและการควบคุมภายในออกเป็น 3 รูปแบบ ได้แก่

I. การประเมินความเสี่ยงและการควบคุมภายในด้วยตนเองระดับกระบวนการ (GRC Assessment)

II. การประเมินการควบคุมภายในด้วยตนเองของผู้บริหาร (E-CSA)

III. การประเมินการควบคุมภายใน กระบวนการที่สำคัญ (GRC Assessment in Key Process)

การประเมินความเสี่ยงและการควบคุมภายใน 3.1

I. การประเมินความเสี่ยงและการควบคุมภายในด้วยตนเอง ระดับกระบวนการ (GRC Assessment)

Department

คือ การประเมินความเสี่ยงและการควบคุมภายในระดับกระบวนการตามบทบาทหน้าที่และจุดมุ่งเน้นด้านการบริหารความเสี่ยง การกำกับดูแลกิจการที่ดี นโยบายต่อต้านการทุจริตและคอร์รัปชัน และการปฏิบัติตามกฎหมาย กฎ ระเบียบ (GRC) โดยหน่วยงานระดับฝ่ายและส่วนขึ้นตรง ผ่านระบบ Risk and Control Platform (RCP) โดยผู้บริหารทำการพิจารณา และอนุมัติผลการประเมิน

แนวทางการประเมิน >>

1 กำหนด ทบทวนกระบวนการ

- **กระบวนการหลัก (Core)** : กระบวนการตามบทบาทหน้าที่ ที่สอดคล้องกับคำบรรยายคุณลักษณะงาน (FD) ของหน่วยงาน รวมถึงความเสี่ยงระดับองค์กร (CRP) ที่หน่วยงานรับผิดชอบ
- **กระบวนการสนับสนุน (Support) หรือ FoCus Process of the Year (FCY)** : กระบวนการที่หน่วยงานต้องปฏิบัติตามแนวปฏิบัติ ระเบียบ และนโยบายตามที่หน่วยงาน 2nd Line กำหนด โดยหน่วยงาน 2nd Line เจ้าของกระบวนการเป็นผู้กำหนดความเสี่ยง และการควบคุมให้หน่วยงาน 1st Line ที่เกี่ยวข้องกับความเสี่ยงดังกล่าว ทำการประเมินเพิ่มเติม

2 ประเมินความเสี่ยง

- **ระบุความเสี่ยง :** ระบุความเสี่ยงที่เกี่ยวข้องในทุกกระบวนการ รวมถึงสาเหตุของความเสี่ยง(Root cause)
- **ประเมินความเสี่ยงที่สำคัญ*** : ประเมินความรุนแรง(Impact)และโอกาสเกิดความเสี่ยง(Likelihood) ทั้งก่อนการควบคุม(Inherent Risk) และหลังการควบคุม(Residual Risk) โดยเลือกใช้เกณฑ์ ดังนี้
  - **ความเสี่ยงที่ไม่ใช่ด้านการทุจริต (Non-Fraud)**
    - เกณฑ์ความเสี่ยงระดับ BU : สำหรับกระบวนการหลัก(Core)
    - เกณฑ์ความเสี่ยงระดับองค์กร : สำหรับกระบวนการสนับสนุน (FCY) และกระบวนการหลักที่ความเสี่ยงเชื่อมโยงกับความเสี่ยงระดับองค์กร(CRP)
  - **ความเสี่ยงด้านการทุจริต (Fraud)**
    - เกณฑ์ความเสี่ยงด้านการทุจริตและคอร์รัปชัน

ทั้งนี้ หน่วยงานที่มีหน้าที่รับผิดชอบในการบริหารความเสี่ยงระดับ Functional ที่ถูกถ่ายทอดมาจากระดับ Corporate นั้นจะต้องระบุแผนบริหารความเสี่ยงที่ถูกถ่ายทอดจากระดับ Corporate ในการประเมินการควบคุมภายในของหน่วยงาน เพื่อให้มั่นใจว่ามีการบริหารความเสี่ยงสอดคล้องกับกระบวนการและกิจกรรมควบคุมภายในอย่างเพียงพอเหมาะสม

** อ้างอิงคู่มือ Enterprise Risk Management (ERM) และ คู่มือการบริหารความเสี่ยงด้านการทุจริตและคอร์รัปชัน*

การประเมินความเสี่ยงและการควบคุมภายใน 3.1

I. การประเมินความเสี่ยงและการควบคุมภายในด้วยตนเอง ระดับกระบวนการ (GRC Assessment)

3 ประเมินการควบคุม

- **ระบุการควบคุมภายใน**: พิจารณาจากสาเหตุของความเสี่ยง(Root Cause)
- **ประเมินความเพียงพอของการออกแบบการควบคุมภายใน** (Control Design)
- **ประเมินการปฏิบัติตามการควบคุม** (Control Compliance)

ทั้งนี้ ในการประเมินการควบคุม จะต้องพิจารณาถึงผลการดำเนินงานของหน่วยงาน เช่น KPI, Non-Compliance, Incident & Non-Conformance Report(INCR), ผลการดำเนินงานของแผนปรับปรุง(Action plan), ข้อคิดเห็นของผู้บริหาร ข้อมูลสถานการณ์ในปัจจุบัน หรือทิศทางในอนาคต, กฎหมายที่เปลี่ยนแปลง เป็นต้น (ภาคผนวก 4)

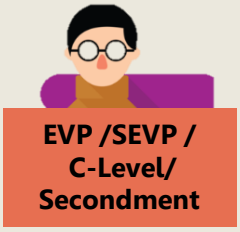
ระดับคะแนนการประเมิน IC	การออกแบบการควบคุม (Control Design)	การปฏิบัติตามการควบคุม (Control Compliance)
ระดับ 4	• การควบคุมเหมาะสม เพียงพอ สามารถทำให้มั่นใจว่าการดำเนินงานสามารถบรรลุวัตถุประสงค์ขององค์กร และไม่เกิดความเสียหายจากความเสี่ยง	• มีการปฏิบัติตามการควบคุมที่ออกแบบไว้อย่างสม่ำเสมอ ≥ 90%
ระดับ 3	• การควบคุมเหมาะสม เพียงพอ แต่ยังมีจุดที่ควรปรับปรุงเพื่อเพิ่มประสิทธิภาพ ลดความซ้ำซ้อน หรือทำให้การทำงานรวดเร็วขึ้น	• มีการปฏิบัติตามการควบคุมที่ออกแบบไว้ แต่ไม่ได้ปฏิบัติอย่างสม่ำเสมอ < 90%
ระดับ 2	• การควบคุมยังไม่เหมาะสม เพียงพอ ไม่สามารถทำให้มั่นใจว่าการดำเนินงานสามารถบรรลุวัตถุประสงค์ขององค์กร หรือยังอาจก่อให้เกิดความเสียหายจากความเสี่ยง	• มีการปฏิบัติตามการควบคุมที่ออกแบบไว้ < 50%
ระดับ 1	• ไม่มีการออกแบบการควบคุม / ไม่ได้กำหนดแนวทางปฏิบัติที่ชัดเจน	• ไม่ปฏิบัติตามการควบคุมที่ออกแบบไว้

4 กำหนดและปฏิบัติตามแผนการปรับปรุง (Action Plan)

- ระบุแผนการปรับปรุง กรณีดังต่อไปนี้
  - คะแนนความเสี่ยงหลังการควบคุมอยู่ในระดับ E (Extreme) หรือ H (High) และ คะแนนการควบคุมน้อยกว่าระดับ 4
  - คะแนนการควบคุมน้อยกว่าระดับ 4
  - มีประเด็น Non-Compliance ที่สำนักตรวจสอบตรวจพบ และยังแก้ไขไม่แล้วเสร็จ
- รายงานสถานะและรายละเอียดแผนปรับปรุงในปีถัดไปเป็นรายไตรมาสในระบบ RCP

การประเมินความเสี่ยงและการควบคุมภายใน 3.1

II. การประเมินการควบคุมภายในด้วยตนเองของผู้บริหาร (E-CSA)

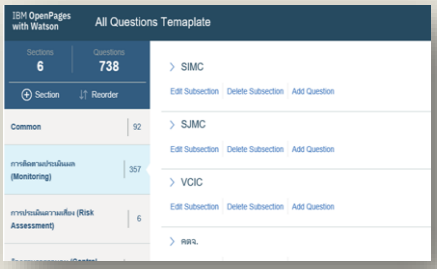


คือ การประเมินการควบคุมด้วยตนเองโดยการใช้แบบประเมิน CSA Questionnaire โดยผู้บริหารตั้งแต่ระดับผู้ช่วยกรรมการผู้จัดการใหญ่ขึ้นไป รวมถึงผู้บริหารที่ปฏิบัติงานในบริษัทในกลุ่ม ปตท. (Secondment) ผ่านระบบ Risk and Control Platform* (RCP)

แนวทางการประเมิน >>

1 ตอบแบบประเมิน ตามบทบาทหน้าที่ที่ได้รับมอบหมาย ดังนี้

- **ผู้บริหารตามโครงสร้าง** (FD)
- **คณะกรรมการจัดการภายใน ปตท. และ กลุ่ม ปตท.** (Committee)
- **คณะกรรมการบริษัทในกลุ่ม ปตท.** (BOD)
- **ผู้บริหารที่ดำรงตำแหน่งสูงสุดในบริษัทในกลุ่ม ปตท.** (Secondment)



โดยคำถามครอบคลุมองค์ประกอบทั้ง 5 ของการควบคุม แบ่งออกเป็นคำถามทั่วไป (Common) เกี่ยวกับการปฏิบัติตามหลักการ COSO Framework 2013 และคำถามเฉพาะเจาะจง (Specific) เกี่ยวกับบทบาทหน้าที่ตามที่ได้รับมอบหมาย

2 ให้ความเห็นและกำหนดแนวทางเพื่อการพัฒนาการควบคุมภายใน

กรณีมีกระบวนการที่ไม่ได้ปฏิบัติตามการควบคุมไว้ ผู้บริหารต้องให้ความเห็นและกำหนดแนวทางเพื่อการพัฒนาและบริหารจัดการต่อไป

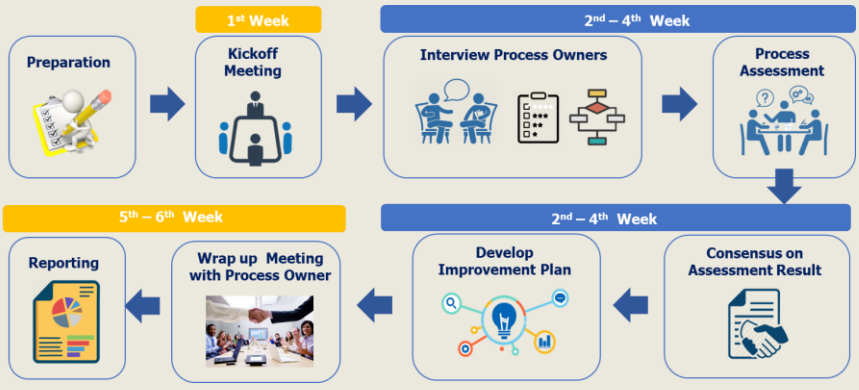
** ภาคผนวก 6 ภาพรวมระบบ Risk and Control Platform (RCP)*

III. การประเมินการควบคุมภายใน กระบวนการที่สำคัญ (GRC Assessment in Key Process)

การประเมินการควบคุมภายใน กระบวนการที่สำคัญ เป็นการประเมินการควบคุมภายในและการบริหารความเสี่ยงในระดับปฏิบัติการของหน่วยงานใน ปตท. และบริษัทในกลุ่ม ปตท. เพื่อให้มั่นใจว่ากระบวนการดำเนินงานเป็นไปอย่างมีประสิทธิภาพ มีการจัดวางระบบการควบคุมภายในที่เพียงพอเหมาะสม สอดคล้องกับกรอบการควบคุมภายใน หลักการบริหารความเสี่ยงและควบคุมภายในตามมาตรฐานสากล และเป็นไปตามหลักการ GRC (Governance Risk & Compliance) โดยฝ่ายควบคุมภายในและจัดการความเสี่ยง (ภสญ.) ดำเนินการร่วมกับหน่วยงานเจ้าของกระบวนการที่ได้รับคัดเลือกในการประเมินฯ

แนวทางการประเมิน >>

- วิเคราะห์และคัดเลือกกระบวนการ/บริษัทจากประเด็นความเสี่ยงต่างๆ ที่เกี่ยวข้อง รวมถึงความเสี่ยงระดับองค์กร ทิศทางกลยุทธ์ ปตท. และข้อคิดเห็นจากคณะกรรมการต่างๆ
- รวบรวมข้อมูลเบื้องต้นเกี่ยวกับกระบวนการ /บริษัท ที่จะเข้าประเมินฯ เช่น ระเบียบ ข้อกำหนด คู่มือปฏิบัติงานที่เกี่ยวข้อง ข้อมูลการประเมินความเสี่ยงและการควบคุมภายในของกระบวนการในระบบ RCP ข้อคิดเห็นของฝ่ายบริหาร (Management Concerns) และข้อคิดเห็นจากคณะกรรมการต่างๆ
- ประเมินความเสี่ยงและการควบคุมภายในของกระบวนการ ให้คำแนะนำและจัดทำแผนการปรับปรุงการควบคุมภายในร่วมกับเจ้าของกระบวนการ
- สรุปผลการประเมิน รวมทั้งแผนการปรับปรุงการควบคุมภายใน พร้อมรายงานให้คณะกรรมการที่เกี่ยวข้องทราบ
- ติดตามการดำเนินงานตามแผนการปรับปรุงการควบคุมภายใน



4

การรายงานผล
การควบคุมภายใน

4.1 การรายงานผลการควบคุมภายใน

ฝ่ายควบคุมภายในและจัดการความเสี่ยง (ภสญ.) มีหน้าที่รวบรวม สรุป และรายงานผลการประเมิน และการดำเนินงานด้านการควบคุมภายในของ ปตท. ต่อผู้กำกับดูแลภายใน และภายนอกองค์กร

I การรายงานผลภายใน ปตท.

ภสญ. รายงานผลการควบคุมภายในต่อคณะกรรมการที่มีหน้าที่ในการบริหารความเสี่ยงและการควบคุมภายในต่อไปนี้

- รายงานความก้าวหน้าการดำเนินงาน เป็นประจำทุกไตรมาส
  - คณะกรรมการจัดการการกำกับดูแล การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎหมาย กฎระเบียบองค์กร (GRCMC)
  - คณะกรรมการกำกับดูแลกิจการที่ดีและความยั่งยืน (CGSC)

- สรุปผลการดำเนินงานประจำปี และนำเสนอแผนการดำเนินงานปีถัดไป
  - คณะกรรมการจัดการการกำกับดูแล การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎหมาย กฎระเบียบองค์กร (GRCMC)
  - คณะกรรมการจัดการของบริษัท ปตท. จำกัด (มหาชน) (PTTMC)
  - คณะกรรมการกำกับดูแลกิจการที่ดีและความยั่งยืน (CGSC)
  - คณะกรรมการตรวจสอบ (AC)
  - คณะกรรมการ ปตท. (BOD)

โดยนำข้อคิดเห็นและข้อเสนอแนะที่ได้รับจากคณะกรรมการมาพิจารณาทบทวน และปรับปรุงกระบวนการทำงานในปีถัดไป

GRC Agent: *ต้องรายงานผลการประเมินการควบคุมภายในของสายงานต่อผู้บริหารสูงสุดของสายงาน*

II การรายงานผลภายนอก ปตท.

ปตท. ในฐานะรัฐวิสาหกิจสังกัดกระทรวงพลังงานและเป็นบริษัท จดทะเบียนในตลาดหลักทรัพย์ จึงมีหน้าที่ที่ต้องปฏิบัติตาม พ.ร.บ. ประกอบรัฐธรรมนูญวินัยการเงินการคลังของรัฐ พ.ศ. 2561 ม. 79 และตามข้อกำหนดของตลาดหลักทรัพย์

กระทรวงการคลัง

จัดทำรายงานการประเมินผลการควบคุมภายใน

1. หนังสือรับรองการประเมินผลการควบคุมภายใน (ปค.1)
2. รายงานการประเมินองค์ประกอบของการควบคุมภายใน (ปค.4)
3. รายงานการประเมินผลการควบคุมภายใน (ปค.5)
4. รายงานการสอบทานการประเมินผลการควบคุมภายในของผู้ตรวจสอบภายใน (ปค. 6)

คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

- **สอบทานแบบแสดงข้อมูลรายการประจำปี 56-1** รายงานต่อตลาดหลักทรัพย์ หัวข้อเรื่องการควบคุมภายใน
- **จัดทำแบบประเมินความเพียงพอของระบบการควบคุมภายใน** ตามแบบรายงานของ ก.ล.ต.

รูปแบบคำถามโดยแบ่งออกเป็น 5 องค์ประกอบ 17 หลักการ ตามมาตรฐาน COSO Internal Control Integrated Framework ดังนี้

1. **การควบคุมภายในองค์กร** (Control Environment)
2. **การประเมินความเสี่ยง** (Risk Assessment)
3. **การควบคุมการปฏิบัติงาน** (Control Activities)
4. **ระบบสารสนเทศและการสื่อสารข้อมูล** (Information and Communication)
5. **ระบบการติดตาม** (Monitoring Activities)

5

ข้อจำกัด และบทสรุป

ข้อจำกัด 5.1

เนื่องจากการควบคุมภายในไม่สามารถป้องกันการตัดสินใจที่ไม่ดีหรือไม่สามารถป้องกันเหตุการณ์ภายนอกที่ส่งผลกระทบทำให้องค์กรล้มเหลว ไม่สามารถบรรลุวัตถุประสงค์ เป้าหมายของการดำเนินงาน การควบคุมภายในจึงยังคงมีข้อจำกัด โดยข้อจำกัดอาจเกิดจาก

- ความเหมาะสมของวัตถุประสงค์ที่กำหนดขึ้น ซึ่งเป็นเงื่อนไขเบื้องต้นสำหรับการควบคุมภายใน
- การใช้ดุลยพินิจในการตัดสินใจอาจจะมีข้อผิดพลาด หรือมีอคติ
- ความเสียหายที่อาจเกิดขึ้นจากความล้มเหลวของบุคคล เช่น การกระทำที่ผิดพลาด
- ความสามารถของผู้บริหารในการฝ่าฝืนการควบคุมภายใน
- ความสามารถของผู้บริหาร บุคลากร และ/หรือบุคคลที่สามที่จะหลีกเลี่ยงการควบคุมโดยการสมรู้ร่วมคิด
- เหตุการณ์ภายนอกที่นอกเหนือการควบคุมขององค์กร
- การมองข้ามความเสี่ยง
- การประเมินผลกระทบต่ำเกินไป

ข้อจำกัดเหล่านี้เป็นอุปสรรคต่อคณะกรรมการบริษัท และผู้บริหารในการได้มาซึ่งความเชื่อมั่นอย่างสมบูรณ์ในการบรรลุวัตถุประสงค์ของกิจการ นั่นคือการควบคุมภายในให้ความเชื่อมั่นอย่างสมเหตุสมผล แต่ไม่ได้ให้ความเชื่อมั่นอย่างสมบูรณ์ เนื่องจากมีข้อจำกัดดังกล่าวข้างต้น

ดังนั้น ผู้บริหารควรตระหนักถึงข้อจำกัดเมื่อจะมีการเลือกการพัฒนา และการนำการควบคุมไปใช้ เพื่อลดข้อจำกัดให้อยู่ในขอบเขตที่สามารถปฏิบัติได้

บทสรุป 5.2

การควบคุมภายในนั้นถือเป็นกระบวนการทำงานที่กำหนดขึ้นมาเพื่อให้ฝ่ายบริหารเกิดความมั่นใจอย่างสมเหตุสมผลว่าการดำเนินงานจะบรรลุวัตถุประสงค์อย่างมีประสิทธิภาพและประสิทธิผล เพื่อให้เกิดความน่าเชื่อถือได้ของรายงานทางการเงิน และไม่ใช่การเงิน รวมถึงเพื่อให้เกิดความมั่นใจว่าจะปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

การบูรณาการระหว่างการบริหารความเสี่ยงกับการควบคุมภายในอย่างเป็นระบบและมีประสิทธิภาพ สามารถสร้างมูลค่าเพิ่ม (Value Enhancement) ให้กับองค์กร ช่วยให้หน่วยงานบรรลุวัตถุประสงค์ของการดำเนินงาน ตลอดจนสนับสนุนและปรับปรุงการดำเนินงานให้ดียิ่งขึ้น โดยเริ่มจากการระบุและประเมินความเสี่ยงที่สำคัญให้ครอบคลุมกิจกรรมต่างๆของหน่วยงาน รวมถึงความเสี่ยงที่ถูกถ่ายทอดจากระดับองค์กร (Corporate Level) โดยกำหนดกิจกรรมการควบคุมภายในอย่างเพียงพอเหมาะสม การประเมินประสิทธิภาพและประสิทธิผลของการควบคุมภายใน รวมถึงการจัดทำแผนปรับปรุงการควบคุมภายในสำหรับรายการความเสี่ยงที่อยู่ในระดับ Extreme หรือ High หรือกิจกรรมการควบคุมที่ยังมีจุดที่สามารถพัฒนาเพิ่มเติมได้

นอกจากนี้ประเด็นสำคัญที่ต้องดำเนินการควบคู่กันไปคือการมุ่งเน้นเรื่องการสร้างความรู้ความเข้าใจ สร้างวัฒนธรรมองค์กรให้เห็นถึงความสำคัญของการบริหารความเสี่ยงและการควบคุมภายใน ว่าความเสี่ยงไม่ใช่จุดด้อย /จุดอ่อนขององค์กรแต่เป็นการสร้างความมั่นใจการดำเนินงานของหน่วยงานจะบรรลุตามเป้าหมายที่กำหนดไว้

6

ภาคผนวก

องค์ประกอบทั้ง 5 ของการควบคุมภายใน ตามหลักการ COSO Framework 2013

COSO คือ กรอบมาตรฐานเรื่องการควบคุมภายใน เพื่อช่วยให้ผู้ปฏิบัติงานบรรลุเป้าหมายและวัตถุประสงค์ ทั้งเรื่องของการปฏิบัติงานอย่างมีประสิทธิภาพและประสิทธิผล ความถูกต้องครบถ้วนของรายงาน และการปฏิบัติตามกฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้อง

COSO ย่อมาจาก Committee of Sponsoring of the Treadway Commission เป็นคณะทำงานที่ก่อตั้งขึ้น โดยคณะกรรมาธิการของประเทศสหรัฐอเมริกา ที่ชื่อว่า Treadway Commission ซึ่งตั้งขึ้นในปี 1985 โดยจัดตั้งขึ้นเพื่อศึกษาและพัฒนาแนวทางการบริหารความเสี่ยง รูปแบบการควบคุมภายในที่มีประสิทธิผล และป้องกันการทุจริตของรายงานทางการเงิน และในปี ค.ศ. 1987 Treadway Commission ได้เสนอให้ตั้งคณะทำงานในนามว่า Committee of Sponsoring of the Treadway Commission หรือ COSO เพื่อศึกษาและพัฒนารูปแบบการควบคุมภายในที่มีประสิทธิผล ดังนั้น COSO จึงเป็นการรวมตัวของคณะกรรมการของสถาบันวิชาชีพ 5 สถาบัน ในสหรัฐอเมริกาซึ่งได้ศึกษาวิจัยและพัฒนาแนวคิดของการควบคุมภายใน และได้ให้ความหมายของการควบคุมภายในซึ่งประกอบไปด้วย 5 สถาบันวิชาชีพ อันได้แก่

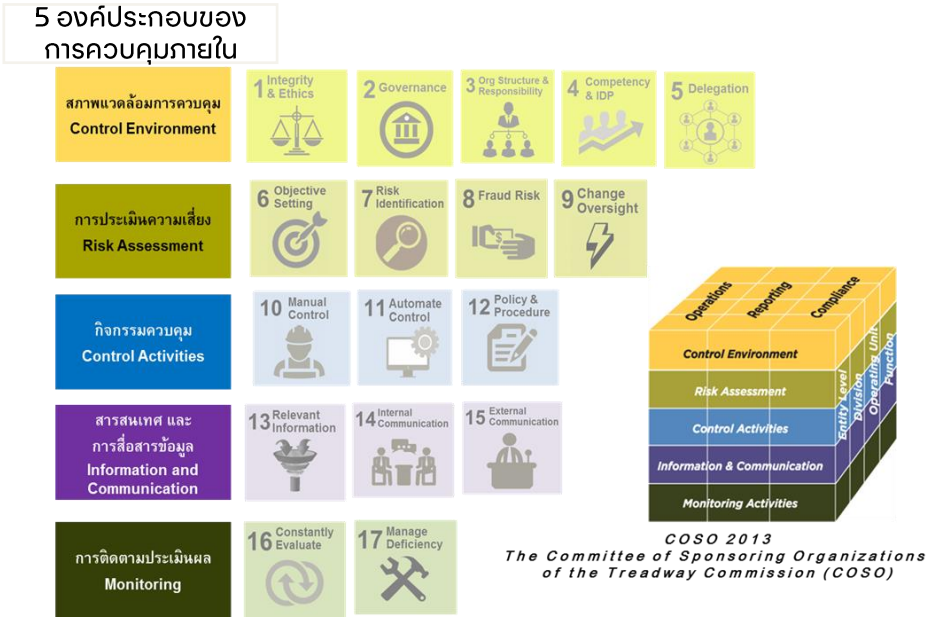
- สมาคมผู้สอบบัญชีรับอนุญาตแห่งสหรัฐอเมริกา (The American Institute of Certified Public Accountants หรือ AICPA)
- สมาคมผู้ตรวจสอบภายใน (The Institute of Internal Auditor หรือ IIA)
- สมาคมผู้บริหารการเงิน (The Financial Executives Institute หรือ FEI)
- สมาคมนักบัญชีแห่งสหรัฐอเมริกา (The American Accounting Association หรือ AAA) และ
- สมาคมนักบัญชีเพื่อการบริหาร (Institute of Management Accountants หรือ IMA)

องค์ประกอบทั้ง 5 ของการควบคุมภายใน ตามหลักการ COSO Framework 2013

กรอบการควบคุมภายใน หรือ COSO Internal Control Integrated Framework เป็นมาตรฐานสากลเพื่อใช้เป็นกรอบในการจัดวางระบบการควบคุมภายในและการประเมินการควบคุมภายใน ซึ่งประกอบไปด้วย 5 องค์ประกอบดังนี้

1. สภาพแวดล้อมการควบคุม Control Environment
2. การประเมินความเสี่ยง Risk Assessment
3. กิจกรรมควบคุม Control Activities
4. สารสนเทศและการสื่อสาร Information and Communication
5. การติดตามประเมินผล Monitoring

นับตั้งแต่การเสนอกรอบการควบคุมภายใน COSO ในปี ค.ศ. 1992 กรอบแนวทางการควบคุมภายในตาม COSO ได้กลายเป็นแนวทางปฏิบัติที่เกี่ยวข้องกับระบบการควบคุมภายในที่ได้รับการยอมรับอย่างกว้างขวางมาเป็นเวลากว่า 20 ปี จนกระทั่งมีการปรับปรุงครั้งใหญ่ เมื่อเดือน พฤษภาคม 2013 ซึ่ง COSO 2013 ได้ถูกปรับปรุงใหม่ให้สอดคล้องกับสภาพแวดล้อมทางธุรกิจที่พัฒนาและเปลี่ยนแปลงไปอย่างรวดเร็ว ซึ่งยังตั้งอยู่บน 5 องค์ประกอบตามเดิม แต่เพิ่มเติม 17 หลักการย่อย เพื่อทำให้ระบบการควบคุมภายในมีความเข้มแข็งและชัดเจนยิ่งขึ้น อย่างไรก็ตามในเดือนมีนาคม 2023 มีการอ้างอิงแนวทางการปฏิบัติสำหรับการควบคุมภายใน โดยประยุกต์แนวคิดสำคัญของการพัฒนาองค์กรอย่างยั่งยืน (ESG) เพื่อสร้างความน่าเชื่อถือและความมั่นใจด้านข้อมูลธุรกิจยั่งยืน



องค์ประกอบทั้ง 5 ของการควบคุมภายใน ตามหลักการ COSO Framework 2013

1. สภาพแวดล้อมการควบคุม (CONTROL ENVIRONMENT)

หมายถึง ปัจจัยต่าง ๆ ที่ส่งผลต่อทัศนคติและความตระหนักของบุคลากรทุกคนในองค์กรถึงความจำเป็นและความสำคัญของการควบคุมภายใน โดยเข้าใจถึงความรับผิดชอบและขอบเขตอำนาจหน้าที่ของตนเอง มีความรู้ความสามารถ และทักษะที่จำเป็นต่อการปฏิบัติงาน รวมถึงการยอมรับและปฏิบัติตามกฎเกณฑ์และวิธีการทำงานต่าง ๆ ที่องค์กรกำหนดไว้ ซึ่งถือได้ว่าสภาพแวดล้อมของการควบคุมมีผลกระทบอย่างมากกับกระบวนการปฏิบัติงานทั้งหมดที่เกิดขึ้นในองค์กร จึงเป็นพื้นฐานที่สำคัญขององค์ประกอบอื่น ๆ ของการควบคุมภายใน เพื่อสร้างระเบียบวินัยด้านการควบคุมภายในให้แก่ทุกคนในองค์กรอย่างยั่งยืน โดยปัจจัยที่ช่วยเสริมสร้างให้มีสภาพแวดล้อมของการควบคุมที่ดี เช่น

- ความซื่อสัตย์และจริยธรรม ซึ่งอาจพิจารณาได้จากการกำหนดแนวทางปฏิบัติในเรื่องต่างๆ ให้ชัดเจน และสื่อสารให้ทุกคนที่เกี่ยวข้องทราบ รวมถึงการกระทำตนเป็นแบบอย่างให้กับผู้ใต้บังคับบัญชา ทั้งคำพูดและการกระทำ

- รูปแบบและปรัชญาการทำงานของฝ่ายบริหาร โดยพิจารณาจากความรู้ความสามารถ และประสบการณ์ของฝ่ายบริหารที่เป็นประโยชน์ต่อหน้าที่ที่รับผิดชอบ และความสนใจในองค์กรที่ตนเป็นผู้บริหาร

- การสร้างวัฒนธรรมองค์กรด้านความรับผิดชอบ และทัศนคติของฝ่ายบริหารและพนักงานทุกคนให้ตระหนักถึงความสำคัญของการดำเนินธุรกิจอย่างยั่งยืน

- การจัดโครงสร้างองค์กรและสายการบังคับบัญชาให้เหมาะสมกับขนาดและลักษณะที่สอดคล้องกับการดำเนินงานของธุรกิจ

- การกำหนดลักษณะงานและคุณสมบัติเฉพาะตำแหน่ง (Job Description & Job Specification) สำหรับทุกตำแหน่งงาน อย่างชัดเจน

- การกำหนดนโยบาย และแนวทางในการจูงใจ พัฒนา และรักษาบุคลากรที่มีความรู้ความสามารถ

องค์ประกอบทั้ง 5 ของการควบคุมภายใน ตามหลักการ COSO Framework 2013

1. สภาพแวดล้อมการควบคุม (CONTROL ENVIRONMENT)

หลักการย่อยขององค์ประกอบที่ 1 สภาพแวดล้อมการควบคุม ได้แก่

หลักการที่ 1 องค์กรแสดงให้เห็นถึงความยึดมั่นในคุณค่าของความซื่อตรงและจริยธรรม

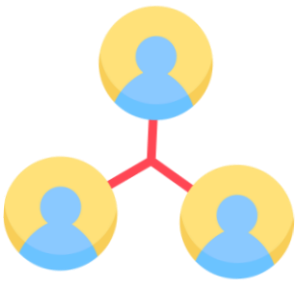
หลักการที่ 2 คณะกรรมการบริษัทแสดงให้เห็นถึงความเป็นอิสระจากผู้บริหารและทำหน้าที่สอดส่องดูแลการพัฒนาและการดำเนินงานด้านการควบคุมภายใน

หลักการที่ 3 ผู้บริหารจัดให้มีโครงสร้าง สายการรายงาน รวมทั้งการกำหนดอำนาจหน้าที่และความรับผิดชอบที่เหมาะสมเพื่อให้องค์กรบรรลุวัตถุประสงค์ ภายใต้การสอดส่องดูแลของคณะกรรมการบริษัท

หลักการที่ 4 องค์กรจะแสดงให้เห็นถึงความมุ่งมั่นในการจูงใจ พัฒนาและรักษาบุคลากรที่มีความรู้ความสามารถที่สอดคล้องกับวัตถุประสงค์ขององค์กร

หลักการที่ 5 องค์กรกำหนดให้บุคลากรที่มีหน้าที่ความรับผิดชอบต่อผลการปฏิบัติงานตามหน้าที่การควบคุมภายในเพื่อให้องค์กรบรรลุวัตถุประสงค์

ในการดำเนินการเกี่ยวกับสภาพแวดล้อมการควบคุม ผู้กำกับคณะกรรมการบริษัท จะต้องมีความอิสระในการสอดส่องดูแลการพัฒนาและการดำเนินงานด้านการควบคุมภายใน และฝ่ายบริหารและบุคลากรของหน่วยงานต้องสร้างบรรยากาศในการดำเนินงานที่ส่งเสริมและให้ความสำคัญกับการควบคุมภายในเพื่อให้ทุกคนในองค์กรมีความเข้าใจและทัศนคติที่ดีต่อการควบคุมภายในอย่างยั่งยืน



2. การประเมินความเสี่ยง (RISK ASSESSMENT)

หมายถึง กระบวนการที่ใช้ในการระบุและการวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยงาน รวมทั้งการกำหนดการควบคุมที่เหมาะสมที่ใช้ในการควบคุมความเสี่ยงที่เกี่ยวข้องกับความยั่งยืนทางธุรกิจ

การประเมินความเสี่ยงที่มีประสิทธิผลนั้น ผู้ประเมินต้องเข้าใจวัตถุประสงค์ของการดำเนินงานอย่างชัดเจน จึงจะสามารถประเมินความเสี่ยงในกระบวนการปฏิบัติงานได้ แล้วจึงพิจารณาว่าความเสี่ยงเหล่านั้นเกิดขึ้นบ่อยครั้งหรือไม่ และเมื่อเกิดความเสี่ยงนั้นแล้วจะส่งผลกระทบต่อการดำเนินงานมากน้อยเพียงใด หากผู้ประเมินพิจารณาแล้ว เห็นว่ายังคงมีความเสี่ยงสูงเกินกว่าที่จะยอมรับได้ จะต้องพิจารณาปรับเปลี่ยนการควบคุมภายในให้เพียงพอและเหมาะสมต่อไป

หลักการย่อยขององค์ประกอบที่ 2 การประเมินความเสี่ยง ได้แก่

หลักการที่ 6 องค์กรระบุวัตถุประสงค์ไว้อย่างชัดเจนเพียงพอ เพื่อให้สามารถระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับวัตถุประสงค์

หลักการที่ 7 องค์กรระบุความเสี่ยงในการบรรลุวัตถุประสงค์อย่างครอบคลุมทั่วทั้งกิจการ และวิเคราะห์ความเสี่ยงเพื่อเป็นเกณฑ์ในการพิจารณาวิธีการจัดการความเสี่ยง

หลักการที่ 8 องค์กรพิจารณาถึงโอกาสที่จะเกิดการทุจริตในการประเมินความเสี่ยงในการบรรลุวัตถุประสงค์

หลักการที่ 9 องค์กรระบุและประเมินการเปลี่ยนแปลงที่อาจมีผลกระทบอย่างมีนัยสำคัญต่อระบบการควบคุมภายใน

ในการดำเนินการเกี่ยวกับการประเมินความเสี่ยง ฝ่ายบริหารต้องประเมินความเสี่ยงทั้งจากปัจจัยภายในและปัจจัยภายนอกที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยงานที่สอดคล้องกับการดำเนินงานของธุรกิจเพื่อความยั่งยืน

3. กิจกรรมการควบคุม (CONTROL ACTIVITIES)

กิจกรรมการควบคุมเป็นองค์ประกอบที่จะช่วยให้มั่นใจได้ว่านโยบายและกระบวนการเกี่ยวกับการควบคุมภายในที่กำหนดขึ้นนั้น ได้มีการนำไปปฏิบัติภายในองค์กรอย่างทั่วถึง นอกจากนี้ กิจกรรมการควบคุมยังช่วยสร้างความมั่นใจว่าหน่วยงาน/องค์กรมีกิจกรรมที่เหมาะสมในการป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้น ดังนั้น กิจกรรมการควบคุมควรกำหนดให้สอดคล้องกับความเสี่ยงที่ประเมินได้ โดยมีข้อควรพิจารณาในการกำหนดกิจกรรมการควบคุม ดังต่อไปนี้

- กิจกรรมการควบคุมควรเป็นส่วนหนึ่งของกระบวนการปฏิบัติงานตามปกติ
- กิจกรรมการควบคุมต้องสามารถป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- ค่าใช้จ่ายในการกำหนดให้กิจกรรมการควบคุมต้องไม่สูงกว่าผลเสียหายที่คาดว่าจะเกิดขึ้น หรือประโยชน์ที่จะได้รับ

กิจกรรมการควบคุม ควรมีการประเมินประสิทธิภาพและประสิทธิผล รวมถึงความสอดคล้องกับวัตถุประสงค์ของการดำเนินงาน และความเสี่ยงที่เปลี่ยนไปขององค์กรอย่างสม่ำเสมอ

หลักการย่อยขององค์ประกอบที่ 3 กิจกรรมการควบคุม ได้แก่

หลักการที่ 10 องค์กรเลือกและพัฒนากิจกรรมการควบคุมที่ลดความเสี่ยงในการบรรลุวัตถุประสงค์ให้อยู่ในระดับที่ยอมรับได้

หลักการที่ 11 องค์กรเลือกและพัฒนากิจกรรมควบคุมทั่วไปด้านเทคโนโลยีเพื่อสนับสนุนการบรรลุวัตถุประสงค์

หลักการที่ 12 องค์กรจัดให้มีกิจกรรมควบคุมผ่านทางนโยบายซึ่งได้กำหนดสิ่งที่คาดหวังและวิธีการปฏิบัติเพื่อนำนโยบายไปสู่การปฏิบัติ

องค์ประกอบทั้ง 5 ของการควบคุมภายใน ตามหลักการ COSO Framework 2013

ในการดำเนินการเกี่ยวกับกิจกรรมควบคุมนั้น ฝ่ายบริหารรวมทั้งพนักงานทุกคนต้องจัดให้มีกิจกรรมควบคุมที่มีประสิทธิภาพและประสิทธิผล เพื่อป้องกันหรือลดความเสียหาย ความผิดพลาดที่อาจเกิดขึ้น และให้สามารถบรรลุผลตามวัตถุประสงค์ของการควบคุมภายในอย่างยั่งยืน ตัวอย่างของกิจกรรมควบคุม เช่น

- *การกำหนดวิสัยทัศน์ กลยุทธ์ และทิศทางในภาพรวมขององค์กรโดยคำนึงถึงการดำเนินธุรกิจอย่างยั่งยืน*
- *การกำหนดนโยบายความยั่งยืน*
- *การกำหนดแผนงาน เป้าหมายและงบประมาณของหน่วยงานที่สอดคล้องกับการดำเนินธุรกิจอย่างยั่งยืน*
- *การกำหนดโครงสร้างคณะกรรมการกำกับดูแลด้านความยั่งยืน*
- *การกำหนดขั้นตอนและวิธีการปฏิบัติงาน*
- *การอนุมัติ*
- *การแบ่งแยกหน้าที่*
- *การสอบทาน*
- *การวิเคราะห์*
- *การสื่อสาร*
- *การประชุม*
- *การกระทบยอด*
- *การควบคุมโดยระบบ IT และการใช้เทคโนโลยีในการจัดเก็บ รวบรวม ติดตาม และรายงานผลเกี่ยวกับการดำเนินงานด้านความยั่งยืน*
- *การดูแลป้องกันทรัพย์สิน*
- *การตรวจสอบ*
- *การควบคุมและสอบทานการปฏิบัติงาน*
- *การติดตามประสิทธิผลเกี่ยวกับการควบคุมภายใน*
- *การติดตามผลการปฏิบัติงานและการใช้งบประมาณ*

4. สารสนเทศและการสื่อสาร (INFORMATION AND COMMUNICATION)

การควบคุมภายในที่ดีจะเกิดขึ้นได้ เมื่อข้อมูลที่เกี่ยวข้องกับการดำเนินงานนั้นได้มีการบ่งชี้ รวบรวมและชี้แจงให้แก่บุคคลที่ควรทราบ โดยผ่านทางรูปแบบและการสื่อสารที่เหมาะสม ข้อมูลที่มีประโยชน์ต่อการตัดสินใจ การบริหารจัดการ และการปฏิบัติงานนั้น อาจเป็นได้ทั้งข้อมูลที่เกี่ยวกับการดำเนินงาน การเงิน และการปฏิบัติตามกฎระเบียบต่าง ๆ โดยแหล่งข้อมูลอาจมาจากภายในหรือภายนอกองค์กร

องค์ประกอบในเรื่องสารสนเทศและการสื่อสาร อาจพิจารณาประเด็นที่สำคัญได้ดังนี้

- ข้อมูลเพียงพอ ถูกต้อง ภายใต้รูปแบบที่เหมาะสม และทันเวลา เพื่อช่วยสนับสนุนการตัดสินใจ การบริหารจัดการ และการปฏิบัติงานในเรื่องต่าง ๆ
- การสื่อสารข้อมูลเกิดขึ้นอย่างทั่วถึงทั้งองค์กร จากผู้บริหารถึงพนักงาน และในทางกลับกัน ระหว่างหน่วยงานหรือแผนก ระหว่างองค์กรกับบุคคลภายนอกเช่น สื่อมวลชน ผู้ออกกฎและระเบียบต่าง ๆ
- การสื่อสารอย่างชัดเจนให้บุคลากรทราบถึงความสำคัญและความรับผิดชอบต่อการควบคุมภายใน
- การสื่อสารแผนการบริหารจัดการและการวิเคราะห์ผลกระทบต่อผู้มีส่วนได้ส่วนเสียในห่วงโซ่คุณค่าของธุรกิจ

องค์ประกอบทั้ง 5 ของการควบคุมภายใน ตามหลักการ COSO Framework 2013

หลักการย่อยขององค์ประกอบที่ 4 สารสนเทศและการสื่อสาร ได้แก่

หลักการที่ 13 องค์กรได้รับหรือสร้างและใช้สารสนเทศที่เกี่ยวข้องและมีคุณภาพ เพื่อสนับสนุนให้การควบคุมภายในทำหน้าที่ได้

หลักการที่ 14 องค์กรมีการสื่อสารภายในเกี่ยวกับสารสนเทศ รวมถึงวัตถุประสงค์และความรับผิดชอบต่อการควบคุมภายในที่จำเป็น เพื่อให้การควบคุมภายในทำหน้าที่ได้

หลักการที่ 15 องค์กรมีการสื่อสารกับบุคคลภายนอกเกี่ยวกับประเด็นที่มีผลกระทบต่อการทำหน้าที่ของการควบคุมภายใน

ในการดำเนินการเกี่ยวกับสารสนเทศและการสื่อสาร ฝ่ายบริหารต้องจัดให้มีสารสนเทศอย่างเพียงพอ และมีการสื่อสารให้ฝ่ายบริหารและบุคลากรอื่นๆ อย่างเหมาะสม ทั้งภายในและภายนอกองค์กร รวมถึงมีการรายงานผลการดำเนินการด้านความยั่งยืน (ESG) แก่ผู้มีส่วนได้ส่วนเสีย โดยต้องพิจารณาถึงความถูกต้อง ครบถ้วน เหมาะสม และทันเวลาของข้อมูล เพื่อให้ผู้ที่เกี่ยวข้องเข้าใจถึงความรับผิดชอบของตนในการบรรลุวัตถุประสงค์ทางธุรกิจที่ยั่งยืนขององค์กร

5. การติดตามประเมินผล (MONITORING)

การติดตามประเมินผล หมายถึง กระบวนการประเมินประสิทธิภาพการปฏิบัติงานและประเมินประสิทธิผลของการควบคุมภายในที่ได้ออกแบบไว้ การควบคุมภายในทั้งหลายที่จัดให้มีขึ้นนั้น จำเป็นอย่างยิ่งที่ต้องมีกลไกในการติดตามประเมินผล เพื่อให้มั่นใจว่าได้มีการปฏิบัติการควบคุมภายในนั้นอย่างสม่ำเสมอ และการปฏิบัตินั้นยังมีความเหมาะสมกับลักษณะการดำเนินงานและการเปลี่ยนแปลงที่เกิดขึ้น เพราะการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นอาจมีผลกระทบต่อความเสี่ยงในการดำเนินงาน และความเสี่ยงที่เปลี่ยนแปลงไป อาจจำเป็นต้องปรับปรุงการควบคุมภายในให้เหมาะสมด้วย

การติดตามผล นั้นสามารถทำได้โดยรวมอยู่ในกระบวนการปฏิบัติงานนั้นๆ เช่น การที่ผู้บังคับบัญชาคอยติดตามปัญหาในการทำงาน ก็ถือว่าเป็นการติดตามผลอย่างหนึ่ง

การประเมินผล คือ การประเมินผลการดำเนินงานเป็นระยะหรือเป็นครั้งคราว เช่น การตรวจสอบโดยหน่วยตรวจสอบภายใน ซึ่งอาจจะเป็นบุคคลในองค์กรเอง หรือการมอบหมายให้บุคคลภายนอกมาทำหน้าที่เป็นผู้ตรวจสอบภายใน

การประเมินการควบคุมภายในอย่างยั่งยืน สามารถทำได้โดยการสร้างความรับผิดชอบในการควบคุมภายในให้แก่ทุกคนที่เป็นเจ้าของงานนั้น ซึ่งจะช่วยให้ผู้บริหารสามารถบริหารงานได้อย่างมีประสิทธิภาพและพนักงานสามารถปฏิบัติและปรับปรุงการควบคุมภายในได้อย่างมีประสิทธิผล เพราะทุกคนในหน่วยงานเป็นเจ้าของกระบวนการและมีความเข้าใจดีที่สุด สามารถประเมินการดำเนินงานรวมถึงการปฏิบัติตามระบบการควบคุมภายในที่ออกแบบไว้สม่ำเสมอในงานที่ตนต้องรับผิดชอบให้สามารถบรรลุวัตถุประสงค์ได้ ซึ่งการปฏิบัติแบบนี้เรียกว่าการประเมินการควบคุมด้วยตนเอง (Control Self-Assessment)

องค์ประกอบทั้ง 5 ของการควบคุมภายใน ตามหลักการ COSO Framework 2013

หลักการย่อยขององค์ประกอบที่ 5 การติดตามประเมินผล ได้แก่

หลักการที่ 16 องค์กรเลือก พัฒนา และดำเนินการประเมินผลอย่างต่อเนื่องและ/หรือ ประเมินผลแยกต่างหาก เพื่อให้มั่นใจว่าองค์ประกอบของการควบคุมภายในมีปรากฏและทำหน้าที่อยู่

หลักการที่ 17 องค์กรประเมินผลและสื่อสารข้อบกพร่องของการควบคุมภายในอย่างทันเวลาต่อบุคคลที่รับผิดชอบในการดำเนินการแก้ไข รวมถึงผู้บริหารระดับสูงและคณะกรรมการบริษัทตามความเหมาะสม

ในการดำเนินการเกี่ยวกับการติดตามประเมินผล ฝ่ายบริหารต้องจัดให้มีการติดตามในระหว่างการปฏิบัติงาน และการประเมินผลอย่างต่อเนื่องและสม่ำเสมอ เพื่อให้มั่นใจว่า

- *ระบบการควบคุมภายในที่วางไว้เพียงพอ เหมาะสม มีประสิทธิภาพ และมีการปฏิบัติจริง*
- *การควบคุมภายในดำเนินไปอย่างมีประสิทธิผล*
- *ข้อตรวจพบจากการตรวจสอบภายในรวมทั้งการประเมินการควบคุมภายในของหน่วยงาน ได้รับการปรับปรุงแก้ไขอย่างเหมาะสมและทันเวลา สอดคล้องกับการดำเนินงานและสถานการณ์ที่เปลี่ยนแปลงไป*

การควบคุมภายในตามหลักเกณฑ์กระทรวงการคลัง

รัฐวิสาหกิจ มีหน้าที่จัดวางระบบการควบคุมภายใน และประเมินผลการควบคุมภายในตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ.2561 ดังนี้

- จัดให้มีคณะกรรมการ ทำหน้าที่กำหนดแนวทางการประเมินผลการควบคุมภายใน รวบรวมพิจารณากลั่นกรอง และสรุปผลการประเมินการควบคุมภายในในภาพรวมของรัฐวิสาหกิจ

- จัดวางระบบการควบคุมภายในให้แล้วเสร็จภายใน 1 ปี กรณีรัฐวิสาหกิจตั้งใหม่/ปรับปรุงโครงสร้างองค์กร และจัดทำรายงานการจัดวางระบบการควบคุมภายใน และส่งให้ผู้กำกับดูแลภายใน 60 วัน นับแต่วันที่จัดวางฯ แล้วเสร็จ

- จัดให้มีการประเมินผลการควบคุมภายใน อย่างน้อยปีละ 1 ครั้ง และจัดทำรายงานการประเมินผลการควบคุมภายใน เสนอต่อประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่ เพื่อพิจารณาลงนาม และจัดส่งให้ผู้กำกับดูแล และกระทรวงเจ้าสังกัด ภายใน 90 วัน นับแต่วันสิ้นปีปฏิทิน

การควบคุมภายในตามหลักเกณฑ์กระทรวงการคลัง

แนวทางการกรอกข้อมูล

หนังสือรับรองการประเมินผลการควบคุมภายใน (ปค.1)

แบบ ปค. ๑

หนังสือรับรองการประเมินผลการควบคุมภายใน
(ระดับหน่วยงานของรัฐ)

เรียน ..... ผู้กำกับดูแลรัฐวิสาหกิจ .....

.....ชื่อรัฐวิสาหกิจ....ได้ประเมินผลการควบคุมภายในของหน่วยงาน สำหรับปีสิ้นสุดวันที่...วัน/เดือน/ปี สิ้นรอบระยะเวลาประเมินฯ...เดือน.....พ.ศ. .....ด้วยวิธีการที่หน่วยงานกำหนดซึ่งเป็นไปตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติ การควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ โดยมีวัตถุประสงค์เพื่อให้ความมั่นใจอย่างสมเหตุสมผลว่า ภารกิจของหน่วยงานจะบรรลุวัตถุประสงค์ของการควบคุมภายในด้านการดำเนินงานที่มีประสิทธิผล ประสิทธิภาพ ด้านการรายงานที่เกี่ยวกับการเงิน และไม่ใช่การเงินที่เชื่อถือได้ ทันเวลา และโปร่งใส รวมทั้งด้านการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้องกับการดำเนินงาน

จากผลการประเมินดังกล่าว .....ชื่อรัฐวิสาหกิจ....เห็นว่า การควบคุมภายในของหน่วยงานมีความเพียงพอปฏิบัติตามอย่างต่อเนื่อง และเป็นไปตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ ภายใต้ การกำกับดูแลของ.....ตำแหน่งผู้กำกับดูแล..... .

ลายมือชื่อ.....ลายมือชื่อหัวหน้ารัฐวิสาหกิจ.....

ตำแหน่ง..... ตำแหน่งหัวหน้ารัฐวิสาหกิจ.....

วันที่..วัน/เดือน/ปี ที่รายงาน.. เดือน.....พ.ศ. .....

กรณีมีความเสี่ยงสำคัญ และกำหนดจะดำเนินการปรับปรุงการควบคุมภายในสำหรับความเสี่ยงดังกล่าวในปีงบประมาณ/ปีปฏิทินถัดไป ให้อธิบายเพิ่มเติมในวรรคสาม ดังนี้

อย่างไรก็ดี มีความเสี่ยงและได้กำหนดปรับปรุงการควบคุมภายใน ในปีงบประมาณหรือปีปฏิทินถัดไป สรุปได้ดังนี้

๑. ความเสี่ยงที่มีอยู่ที่ต้องกำหนดปรับปรุงการควบคุมภายใน
(สอดคล้องกับความเสี่ยงที่ระบุใน ปค. ๕)

๑.๑.....

๑.๒.....

๒. การปรับปรุงการควบคุมภายใน (เพื่อป้องกันหรือลดความเสี่ยงตาม ๑)

๒.๑.....

๒.๒.....

การควบคุมภายในตามหลักเกณฑ์กระทรวงการคลัง

แนวทางการกรอกข้อมูล

รายงานการประเมินองค์ประกอบของการควบคุมภายใน (ปค.4)

แบบ ปค. ๔

..... ชื่อรัฐวิสาหกิจ.....

รายงานการประเมินองค์ประกอบของการควบคุมภายใน

สำหรับระยะเวลาดำเนินงานสิ้นสุด ...วัน/เดือน/ปี สิ้นรอบระยะเวลาประเมินฯ.....

องค์ประกอบของการควบคุมภายใน	ผลการประเมิน/ข้อสรุป
๑. สภาพแวดล้อมการควบคุม ระบุ.....	.....ระบุผลการประเมิน/ข้อสรุปของแต่ละองค์ประกอบ พร้อมความเสี่ยงที่ยังมีอยู่/จุดอ่อน.....
๒. การประเมินความเสี่ยง ระบุ.....	
๓. กิจกรรมการควบคุม ระบุ.....	.....
๔. สารสนเทศและการสื่อสาร ระบุ.....	.....
๕. กิจกรรมการติดตามผล ระบุ.....	.....

ผลการประเมินโดยรวม

.....สรุปผลการประเมินโดยรวมขององค์ประกอบของการควบคุมภายในทั้ง 5 องค์ประกอบ.....

ลายมือชื่อ.....ลายมือชื่อหัวหน้ารัฐวิสาหกิจ.....

ตำแหน่ง..... ตำแหน่งหัวหน้ารัฐวิสาหกิจ.....

วันที่..วัน/เดือน/ปี ที่รายงาน.. เดือน.....พ.ศ. .....

การควบคุมภายในตามหลักเกณฑ์กระทรวงการคลัง

แนวทางการกรอกข้อมูล

รายงานการประเมินผลการควบคุมภายใน (ปค.5)

แบบ ปค. ๕

..... ชื่อรัฐวิสาหกิจ.....

รายงานการประเมินผลควบคุมภายใน

สำหรับระยะเวลาดำเนินงานสิ้นสุด ...วัน/เดือน/ปี สิ้นรอบระยะเวลาประเมินฯ.....

ภารกิจตามกฎหมายที่จัดตั้งหน่วยงานของรัฐหรือภารกิจตามแผนการดำเนินการหรือภารกิจอื่นๆ ที่สำคัญของหน่วยงานของรัฐ/วัตถุประสงค์	ความเสี่ยง	การควบคุมภายในที่มีอยู่	การประเมินผลการควบคุมภายใน	ความเสี่ยงที่ยังมีอยู่	การปรับปรุงการควบคุมภายใน	หน่วยงานที่รับผิดชอบ/กำหนดเสร็จ
• ภารกิจตามกฎหมายที่จัดตั้งหน่วยงานของรัฐหรือภารกิจตามแผนการดำเนินงานหรือภารกิจอื่นๆ ที่สำคัญของหน่วยงานของรัฐ • วัตถุประสงค์ของภารกิจดังกล่าว	ความเสี่ยงสำคัญของแต่ละภารกิจ	การควบคุมภายในของแต่ละภารกิจเพื่อลด หรือควบคุมความเสี่ยง	ผลการประเมินผลการควบคุมภายในว่าเพียงพอและปฏิบัติตามอย่างต่อเนื่องหรือไม่	ความเสี่ยงที่ยังมีอยู่ของแต่ละภารกิจ	การปรับปรุงการควบคุมภายในในปีปฏิทินถัดไป	• หน่วยงานที่รับผิดชอบ • กำหนดเสร็จ (ว/ด/ป)

ลายมือชื่อ.....ลายมือชื่อหัวหน้ารัฐวิสาหกิจ.....

ตำแหน่ง..... ตำแหน่งหัวหน้ารัฐวิสาหกิจ.....

วันที่..วัน/เดือน/ปี ที่รายงาน.. เดือน.....พ.ศ. .....

การควบคุมภายในตามหลักเกณฑ์กระทรวงการคลัง

แนวทางการกรอกข้อมูล

รายงานการสอบทานการประเมินผลการควบคุมภายในของผู้ตรวจสอบภายใน (ปค.6)

แบบ ปค. ๖

รายงานการสอบทานการประเมินผลการควบคุมภายในของผู้ตรวจสอบภายใน

เรียน ..... หัวหน้ารัฐวิสาหกิจ.....

ผู้ตรวจสอบภายในของ .....ชื่อรัฐวิสาหกิจ.... ได้สอบทานการประเมินผลการควบคุมภายในของหน่วยงานสำหรับปีสิ้นสุดวันที่ ...วัน/เดือน/ปี สิ้นรอบระยะเวลาประเมินฯ... เดือน .....พ.ศ. .....ด้วยวิธีการสอบทานตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ โดยมีวัตถุประสงค์เพื่อให้ความมั่นใจอย่างสมเหตุสมผลว่า ภารกิจของหน่วยงานจะบรรลุวัตถุประสงค์ของการควบคุมภายในด้านการดำเนินงานที่มีประสิทธิผล ประสิทธิภาพ ด้านการรายงานที่เกี่ยวกับการเงิน และไม่ใช่การเงินที่เชื่อถือได้ ทันเวลา และโปร่งใส รวมทั้งด้านการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้องกับการดำเนินงาน

จากผลการสอบทานดังกล่าว ผู้ตรวจสอบภายในเห็นว่า การควบคุมภายในของ.....ชื่อรัฐวิสาหกิจ.....มีความเพียงพอ ปฏิบัติตามอย่างต่อเนื่อง และเป็นไปตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑

ลายมือชื่อ.....ลายมือชื่อหัวหน้าหน่วยงานตรวจสอบภายใน.....

ตำแหน่ง.....ตำแหน่งหัวหน้าหัวหน้าหน่วยงานตรวจสอบภายใน.....

วันที่..วัน/เดือน/ปี ที่รายงาน.. เดือน.....พ.ศ. .....

กรณีได้สอบทานการประเมินผลการควบคุมภายในแล้ว มีข้อตรวจพบหรือข้อสังเกตเกี่ยวกับความเสี่ยง และการควบคุมภายในหรือการปรับปรุงการควบคุมภายในสำหรับความเสี่ยงดังกล่าว ให้รายงานข้อตรวจพบหรือข้อสังเกตดังกล่าวในวรรคสาม ดังนี้

อย่างไรก็ดี มีความเสี่ยงและได้กำหนดปรับปรุงการควบคุมภายใน ในปีงบประมาณหรือปีปฏิทินถัดไป สรุปได้ดังนี้

๑. ความเสี่ยงที่มีอยู่ที่ต้องกำหนดปรับปรุงการควบคุมภายใน

๑.๑.....

๑.๒.....

๒. การปรับปรุงการควบคุมภายใน (เพื่อป้องกันหรือลดความเสี่ยงตาม ๑)

๒.๑.....

๒.๒.....

การควบคุมภายในตามหลักเกณฑ์ ก.ล.ต.

บริษัทจดทะเบียน มีหน้าที่สรุปความเห็นของคณะกรรมการบริษัทเกี่ยวกับระบบการควบคุมภายในของบริษัท เพื่อแสดงในแบบแสดงรายการข้อมูลประจำปี(แบบ 56-1) โดยใช้แบบประเมินความเพียงพอของระบบการควบคุมภายในของคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) เพื่อประกอบการประเมินด้วย โดยความเห็นของคณะกรรมการฯ ประกอบด้วย

- ความเพียงพอและความเหมาะสมของระบบการควบคุมภายในของบริษัท และการจัดให้มีบุคลากรอย่างเพียงพอที่จะดำเนินการดังกล่าวได้อย่างมีประสิทธิภาพ รวมทั้งการติดตามควบคุมดูแลการดำเนินงานของบริษัทย่อยว่า สามารถป้องกันทรัพย์สินของบริษัทและบริษัทย่อยจากการที่กรรมการหรือผู้บริหารนำไปใช้โดยมิชอบหรือโดยไม่มีอำนาจหรือไม่

- ข้อบกพร่องเกี่ยวกับระบบการควบคุมภายในที่ผ่านมาของบริษัทมีเรื่องใดบ้าง ถ้ามีบริษัทได้แก้ไขข้อบกพร่องดังกล่าวเสร็จสิ้นแล้วหรือไม่ เพราะเหตุใด

การควบคุมภายในตามหลักเกณฑ์ ก.ล.ต.

แบบประเมินความเพียงพอของระบบการควบคุมภายใน (แบบ ก.ล.ต.)

เป็นการตอบคำถาม “ใช่” หรือ “ไม่ใช่” หากประเมินแล้วพบว่า บริษัทยังขาดการควบคุมภายในที่เพียงพอในข้อใด บริษัทควรอธิบายเหตุผลและแนวทางแก้ไขประกอบไว้ด้วย

การควบคุมภายในองค์กร (Control Environment)

1. องค์กรแสดงถึงความยึดมั่นในคุณค่าของความซื่อตรง (integrity) และจริยธรรม

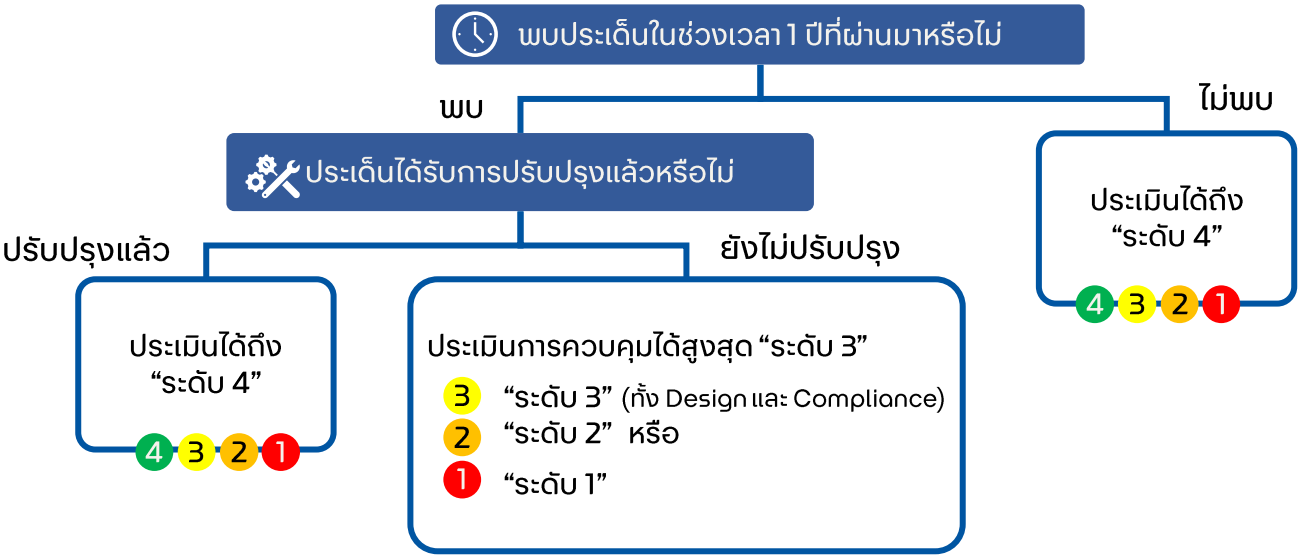
คำถาม	ใช่	ไม่ใช่	คำอธิบายเพิ่มเติม
1.1 คณะกรรมการและผู้บริหารกำหนดแนวทาง และมีการปฏิบัติที่อยู่บนหลักความซื่อตรงและการรักษาจรรยาบรรณในการดำเนินงาน ที่ครอบคลุมถึง 1.1.1 การปฏิบัติหน้าที่ประจำวัน และการตัดสินใจในเรื่องต่าง ๆ 1.1.2 การปฏิบัติต่อคู่ค้า ลูกค้า และบุคคลภายนอก	✓		
1.2 มีข้อกำหนดที่เป็นลายลักษณ์อักษรให้ผู้บริหารและพนักงานปฏิบัติหน้าที่ด้วยความซื่อตรงและรักษาจรรยาบรรณ ที่ครอบคลุมถึง 1.2.1 มีข้อกำหนดเกี่ยวกับจริยธรรม (code of conduct) สำหรับผู้บริหารและพนักงาน ที่เหมาะสม 1.2.2 มีข้อกำหนดห้ามผู้บริหารและพนักงานปฏิบัติตนในลักษณะที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์กับกิจการ ซึ่งรวมถึงการห้ามคอร์รัปชันอันทำให้เกิดความเสียหายต่อองค์กร[2] 1.2.3 มีบทลงโทษที่เหมาะสมหากมีการฝ่าฝืนข้อกำหนดข้างต้น 1.2.4 มีการสื่อสารข้อกำหนดและบทลงโทษข้างต้นให้ผู้บริหารและพนักงาน ทุกคนรับทราบ เช่น รวมอยู่ในการปฐมนิเทศพนักงานใหม่ ให้พนักงานลงนามรับทราบข้อกำหนดและบทลงโทษเป็นประจำทุกปี รวมทั้งมีการเผยแพร่ code of conduct ให้แก่พนักงานและบุคคลภายนอกได้รับทราบ	✓		
1.3 มีกระบวนการติดตามและประเมินผลการปฏิบัติตาม Code of Conduct 1.3.1 การติดตามและประเมินผลโดยหน่วยงานตรวจสอบภายในหรือหน่วยงานกำกับดูแลการปฏิบัติ (compliance unit) 1.3.2 การประเมินตนเองโดยผู้บริหารและพนักงาน 1.3.3 การประเมินโดยผู้เชี่ยวชาญที่เป็นอิสระจากภายนอกองค์กร	✓		

เกณฑ์การประเมินการควบคุมภายใน

ปตท. กำหนดเกณฑ์การประเมินการควบคุมภายใน สำหรับใช้ในการประเมิน GRC Assessment ดังนี้

ระดับคะแนนการประเมิน IC	การออกแบบการควบคุม (Control Design)	การปฏิบัติตามการควบคุม (Control Compliance)
ระดับ 4	• การควบคุมเหมาะสม เพียงพอ สามารถทำให้มั่นใจว่าการดำเนินงานสามารถบรรลุวัตถุประสงค์ขององค์กร และไม่เกิดความเสียหายจากความเสี่ยง	• มีการปฏิบัติตามการควบคุมที่ออกแบบไว้อย่างสม่ำเสมอ ≥ 90%
ระดับ 3	• การควบคุมเหมาะสม เพียงพอ แต่ยังมีจุดที่ควรปรับปรุงเพื่อเพิ่มประสิทธิภาพ ลดความซ้ำซ้อน หรือทำให้การทำงานรวดเร็วขึ้น	• มีการปฏิบัติตามการควบคุมที่ออกแบบไว้ แต่ไม่ได้ปฏิบัติอย่างสม่ำเสมอ < 90%
ระดับ 2	• การควบคุมยังไม่เหมาะสม เพียงพอ ไม่สามารถทำให้มั่นใจว่าการดำเนินงานสามารถบรรลุวัตถุประสงค์ขององค์กร หรือยังอาจก่อให้เกิดความเสียหายจากความเสี่ยง	• มีการปฏิบัติตามการควบคุมที่ออกแบบไว้ < 50%
ระดับ 1	• ไม่มีการออกแบบการควบคุม / ไม่ได้กำหนดแนวทางปฏิบัติที่ชัดเจน	• ไม่ปฏิบัติตามการควบคุมที่ออกแบบไว้

กรณี Auditor/Compliance พบประเด็น Non-Compliance ในช่วง 1 ปีที่ผ่านมา



เกณฑ์การประเมินความเสี่ยงระดับปฏิบัติการ

การประเมินความเสี่ยง คือ การวัดระดับความรุนแรงของความเสี่ยงว่ามีระดับความรุนแรงมากน้อยเพียงใด เพื่อพิจารณาจัดลำดับความสำคัญ และจัดการความเสี่ยงให้มีระดับความรุนแรงอยู่ในระดับที่ยอมรับได้ (Risk Appetite)

โดยการประเมินความเสี่ยง นอกเหนือจากการประเมินความเสี่ยงตามหลักเกณฑ์การวัดระดับความรุนแรงขององค์กรแล้ว กลุ่มธุรกิจ/สายงานสนับสนุน และหน่วยปฏิบัติงาน สามารถกำหนดเกณฑ์การวัดระดับความรุนแรงของความเสี่ยงที่แตกต่างกันของแต่ละหน่วยปฏิบัติงานได้ ตามวัตถุประสงค์ในการปฏิบัติงาน

หลักเกณฑ์การวัดระดับความรุนแรง

- **เกณฑ์การวัดระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact)** สามารถวัดได้จากผลกระทบ ดังต่อไปนี้
  - ผลกระทบด้านการเงิน (Financial Impact)
  - ผลกระทบด้านกระบวนการธุรกิจและการปฏิบัติการ (Business Process and Operation Impact)
  - ผลกระทบด้านชื่อเสียงองค์กร (Image and Reputation Impact)

เกณฑ์การวัดระดับความรุนแรงผลกระทบ

4 รุนแรง
3 สูง
2 ปานกลาง
1 ต่ำ

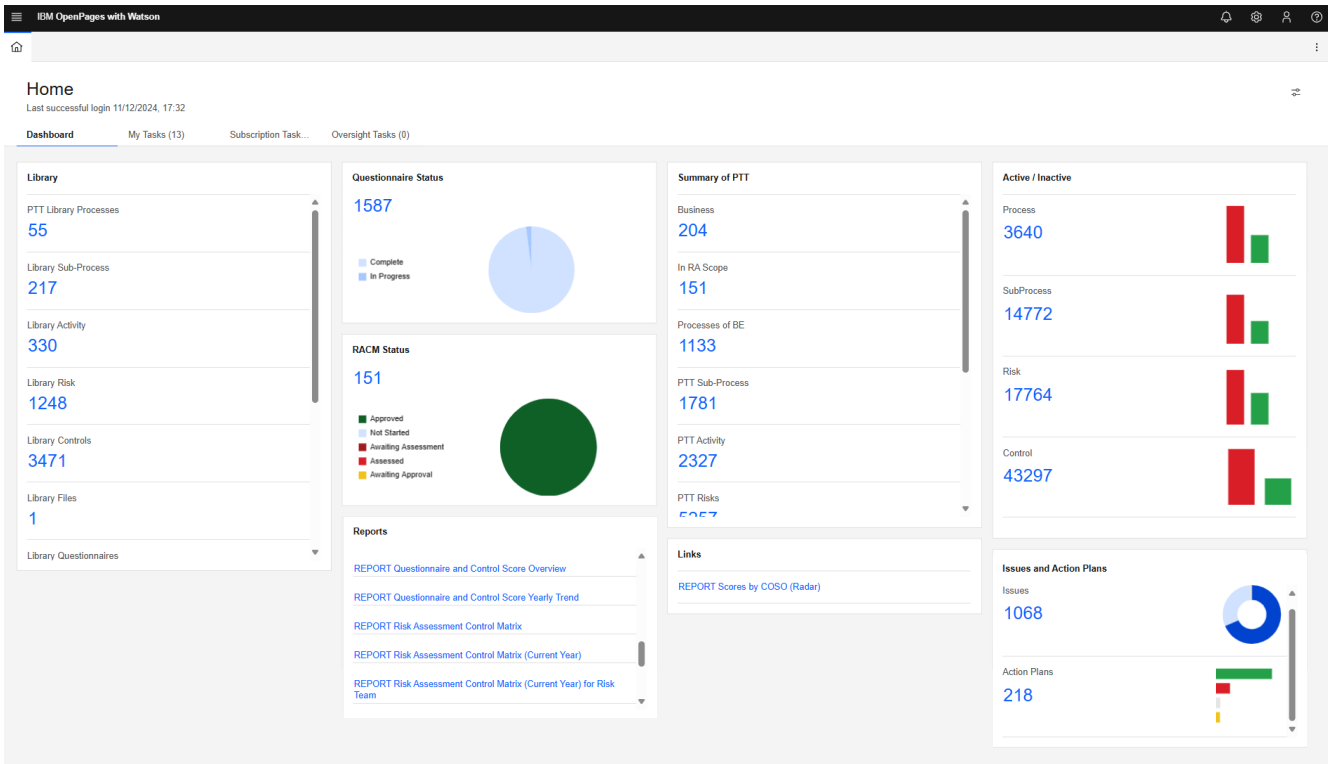
- **เกณฑ์การวัดระดับความรุนแรงของโอกาสเกิดความเสี่ยง (Likelihood)** สามารถวัดได้ตามรูปแบบ ดังนี้
  - เชิงปริมาณ สำหรับความเสี่ยงที่มีข้อมูลตัวเลขมาใช้ในการวิเคราะห์
  - เชิงคุณภาพ สำหรับความเสี่ยงที่ไม่สามารถระบุเป็นตัวเลขที่ชัดเจนได้

ทั้งนี้ หลักเกณฑ์การวัดระดับความรุนแรง ของกลุ่มธุรกิจ/ สายงานสนับสนุน และหน่วยปฏิบัติงาน ได้ถูกระบุไว้ในคู่มือการบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management Manual) ซึ่งมีการทบทวนอย่างสม่ำเสมอทุกปี

ภาพรวมระบบ Risk and Control Platform (RCP)

การประเมินความเสี่ยงและการควบคุมภายใน (GRC Assessment) ของ ปตท. ดำเนินการผ่านระบบ Risk and Control Platform (RCP) ตั้งแต่การระบุและกำหนดวัตถุประสงค์ของกระบวนการ การระบุ วิเคราะห์และวัดระดับความเสี่ยง การทบทวนและกำหนดกิจกรรมการควบคุม รวมถึงการกำหนดแผนการปรับปรุงการควบคุม (Action Plan) อีกด้วย

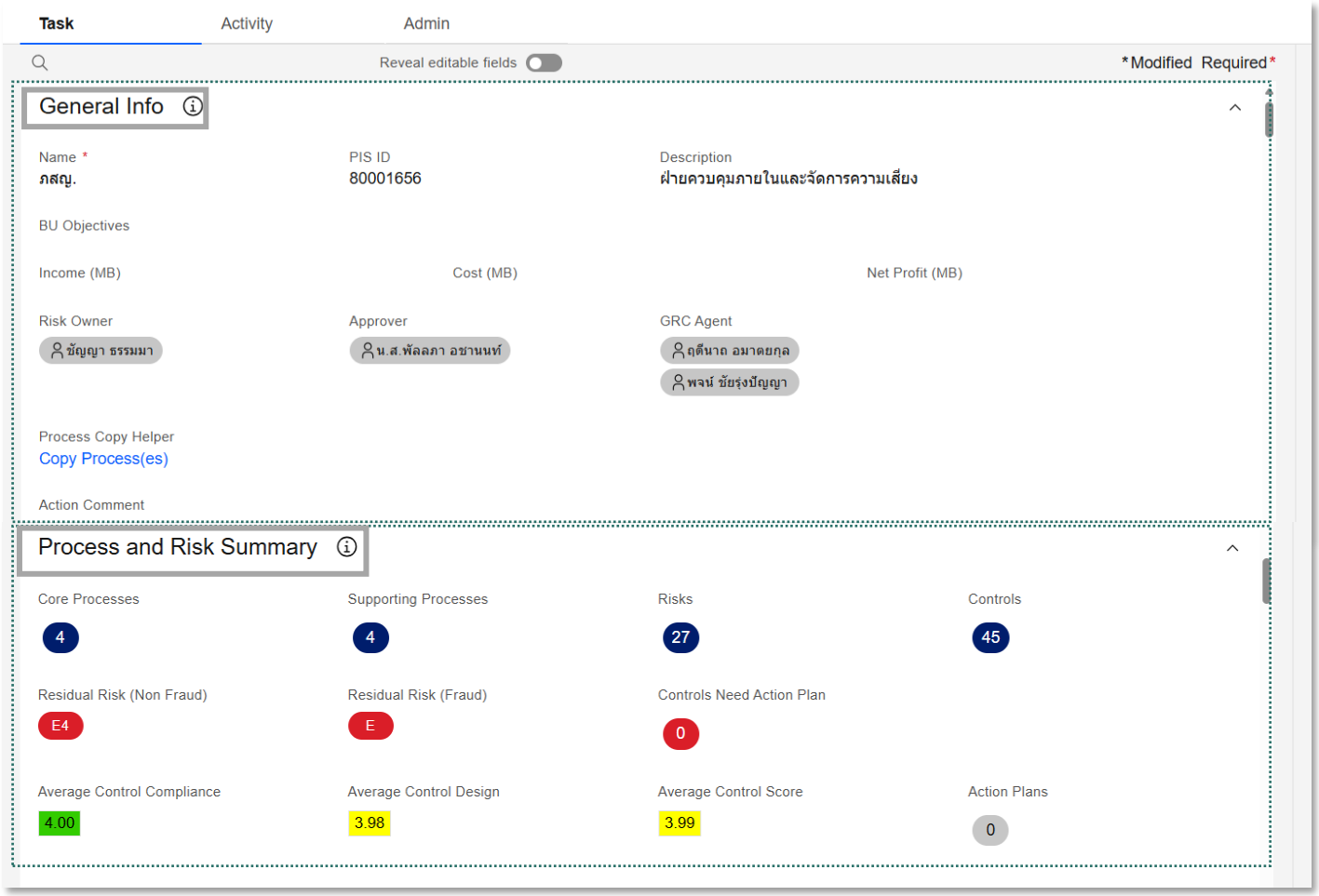
RCP



ภาพรวมระบบ Risk and Control Platform (RCP)

ส่วนประกอบของระบบ RCP

General Info and Summary



General Info :

หน้าจอแสดงข้อมูลทั่วไปของกระบวนการทำงาน (Process) สำหรับระบุชื่อกระบวนการทำงาน และรายละเอียดของกระบวนการทำงานที่นำมาใช้ในการประเมินความเสี่ยงในระดับปฏิบัติการ

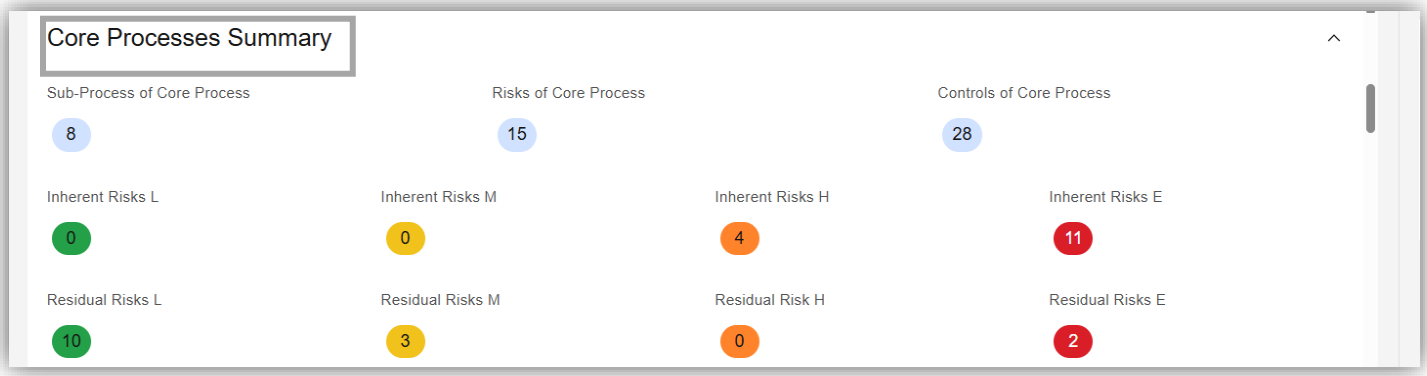
Process and Risk Summary :

หน้าจอสรุปข้อมูลกระบวนการและความเสี่ยง สำหรับใช้ตรวจสอบความถูกต้องในภาพรวม

ภาพรวมระบบ Risk and Control Platform (RCP)

ส่วนประกอบของระบบ RCP

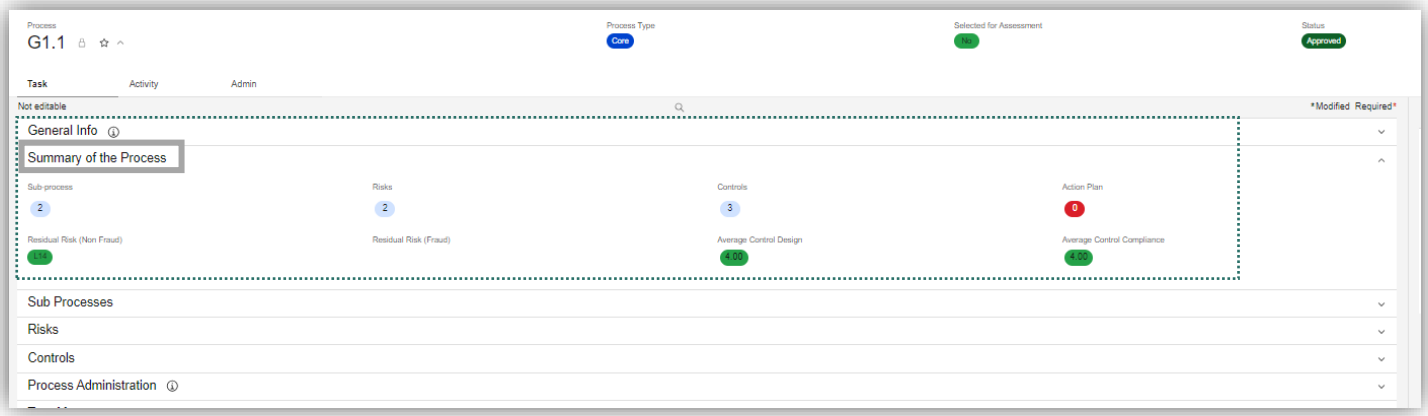
Summary of the Process



Core Processes Summary :

หน้าจอสรุปรายละเอียดของกระบวนการทำงานหลัก(Core Process) ได้แก่

- จำนวนกระบวนการทำงานย่อย (Sub Process of Core Process)
- จำนวนความเสี่ยง (Risk of Core Process)
- จำนวนการควบคุม (Control of Core Process)
- จำนวนความเสี่ยงในระดับต่างๆ ของความเสี่ยงก่อนการดำเนินกิจกรรมการควบคุม (Inherent Risk) และความเสี่ยงที่เหลือภายหลังการดำเนินกิจกรรมการควบคุม (Residual Risk)



Summary of the Process :

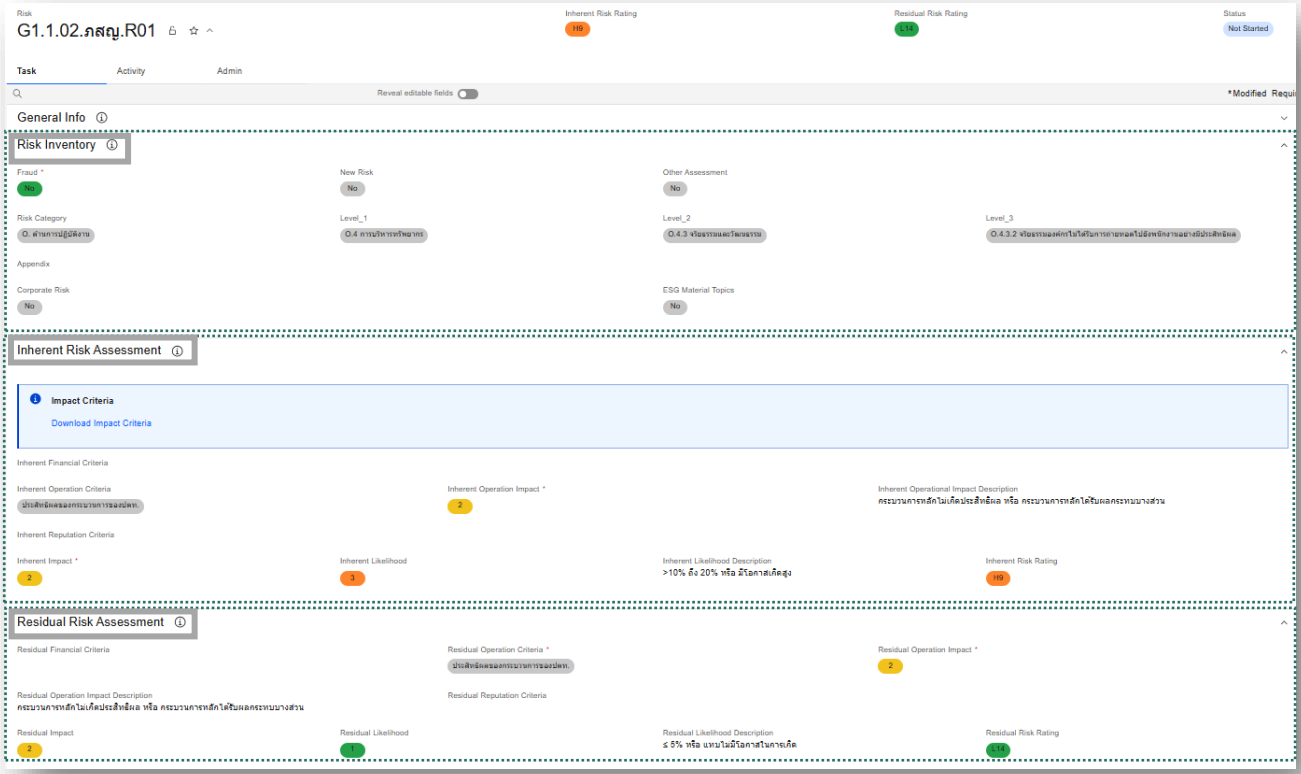
หน้าจอสรุปรายละเอียดของกระบวนการ ได้แก่

- จำนวนกระบวนการทำงานย่อย (Sub Process)
- จำนวนความเสี่ยง (Risk)
- จำนวนการควบคุม (Control)
- จำนวนแผนการปรับปรุงการควบคุม (Action plan)
- คะแนนเฉลี่ยการออกแบบการควบคุม (Average Control Design) และคะแนนเฉลี่ยการปฏิบัติตามการควบคุมที่ได้ออกแบบไว้ (Average Control Compliance)

ภาพรวมระบบ Risk and Control Platform (RCP)

ส่วนประกอบของระบบ RCP

Risk Assessment



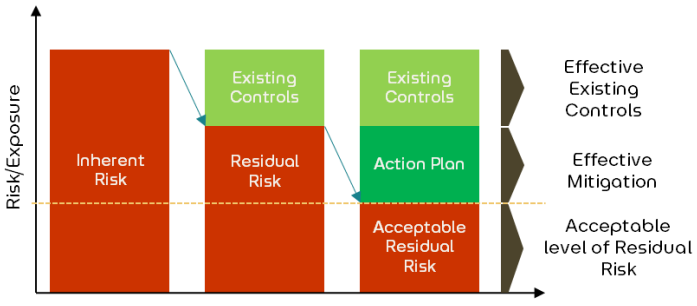
Risk inventory :

การระบุประเภทความเสี่ยง ได้แก่

- ความเสี่ยงด้านการทุจริต
- ประเภทของความเสี่ยง (Risk category) และ level ย่อย
- ประเภทความเสี่ยงด้าน ESG (ESG Material Topic)

Inherent Risk Assessment:

การประเมินผลกระทบ (Impact) และโอกาสเกิด (Likelihood) ของความเสี่ยงสืบเนื่อง หรือความเสี่ยงก่อนการดำเนินกิจกรรมการควบคุม (Inherent Risk) ตามหลักเกณฑ์การประเมินความเสี่ยง



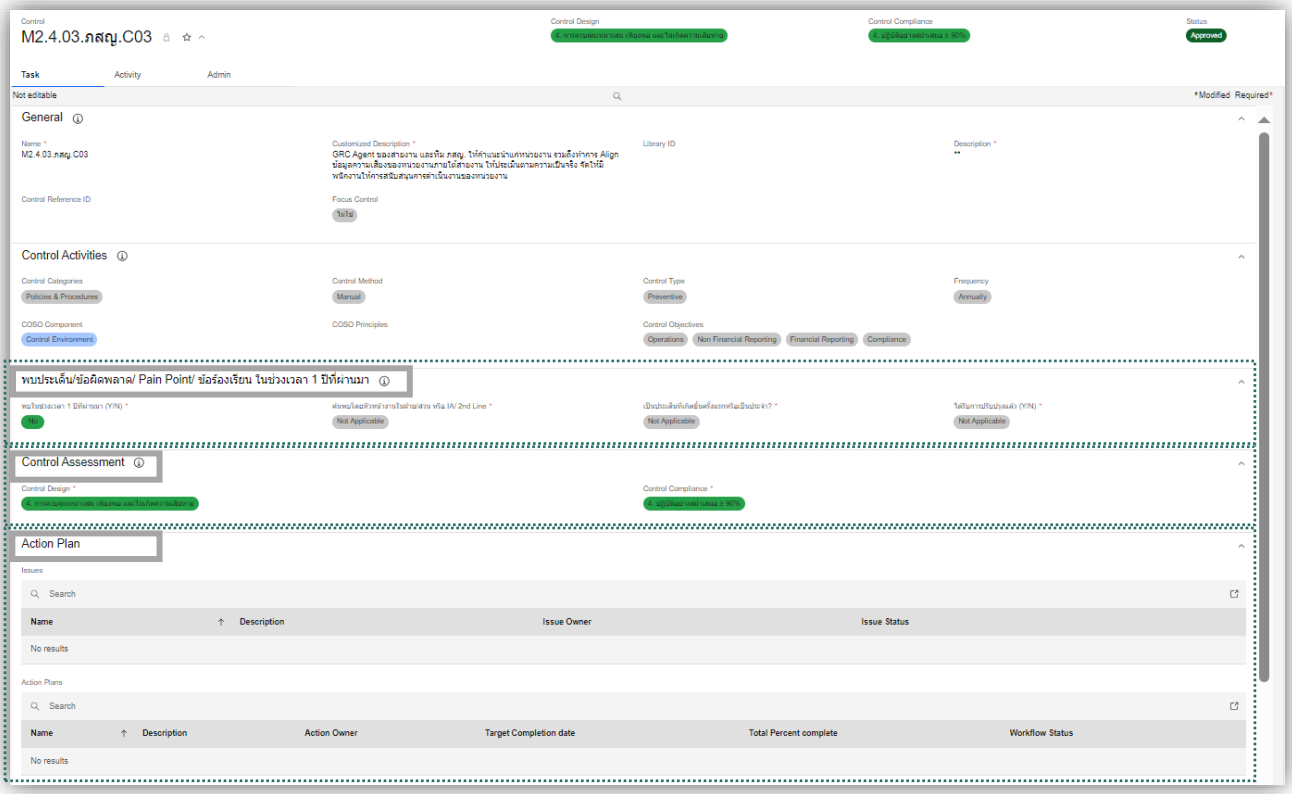
Residual Risk Assessment:

การประเมินผลกระทบ (Impact) และโอกาสเกิด (Likelihood) ของความเสี่ยงคงเหลือ หรือความเสี่ยงที่เหลือภายหลังการดำเนินกิจกรรมการควบคุม (Residual Risk) ตามหลักเกณฑ์การประเมินความเสี่ยง

ภาพรวมระบบ Risk and Control Platform (RCP)

ส่วนประกอบของระบบ RCP

Control assessment



พบประเด็น/ข้อผิดพลาด/ Pain point/ข้อร้องเรียนในช่วง 1 ปีที่ผ่านมา :

การระบุประเด็น/ ข้อผิดพลาด/ Pain point และข้อร้องเรียนในช่วง 1 ปีที่ผ่านมาและตอบคำถามต่าง ๆ เช่น ประเด็นได้รับการค้นพบโดยใคร เป็นประเด็นใหม่หรือเกิดขึ้นซ้ำ และได้รับการปรับปรุงแล้วหรือไม่ เป็นต้น

Control Assessment :

การประเมินความเพียงพอของการออกแบบการควบคุมภายในและการปฏิบัติตามการควบคุม (Control Design & Compliance)

Action Plan :

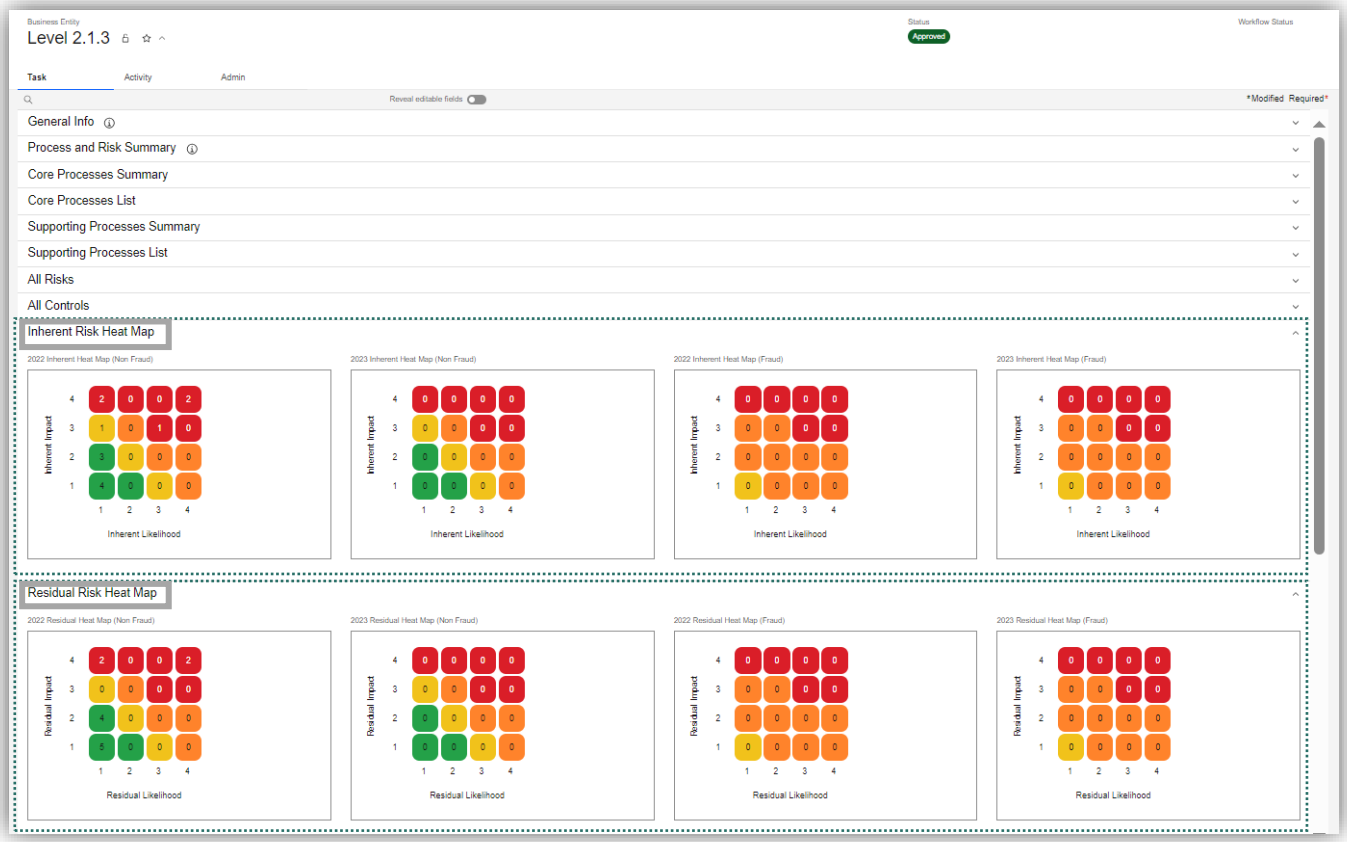
การระบุแผนการปรับปรุงการควบคุม (Action plan) เพิ่มเติมในกรณีที่การควบคุมภายในยังไม่มีประสิทธิภาพ ประสิทธิผลเพียงพอ

ข้อมูลที่ต้องระบุ เช่น รายละเอียดของแผนการปรับปรุงการควบคุม ผู้รับผิดชอบ วันที่คาดว่าจะแล้วเสร็จ สถานะความคืบหน้าของแผน เป็นต้น

ภาพรวมระบบ Risk and Control Platform (RCP)

ส่วนประกอบของระบบ RCP

Functional Heat Map



Inherent Risk Heat Map :

สรุปค่าระดับความรุนแรงของความเสี่ยงสืบเนื่อง หรือความเสี่ยงก่อนการดำเนินกิจกรรมการควบคุม (Inherent Risk) ที่ได้จากการประเมินผลกระทบและโอกาสเกิดของปัจจัยเสี่ยง โดยแสดงความเสี่ยงด้านการทุจริตและคอร์รัปชัน (Fraud) และไม่ใช่ด้านการทุจริตและคอร์รัปชัน (Non Fraud) ออกจากกัน ตามเกณฑ์การจัดกลุ่มความเสี่ยง

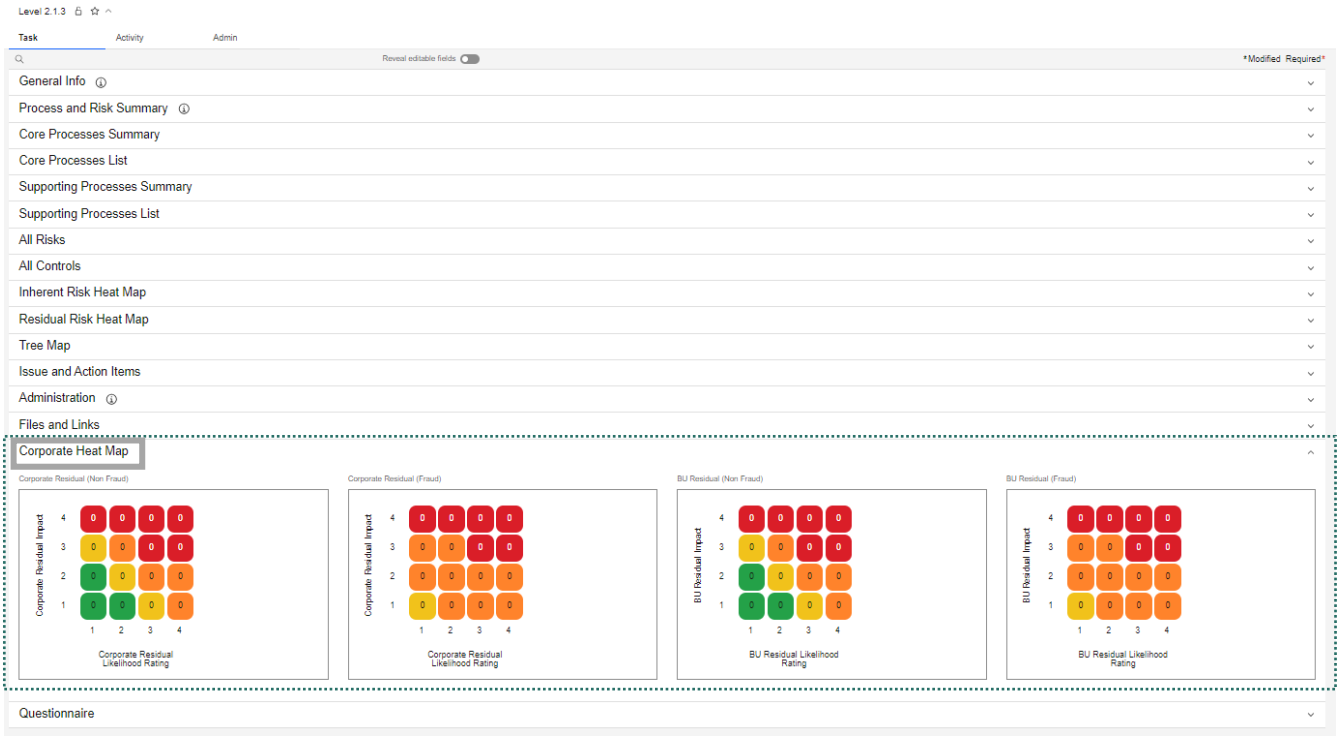
Residual Risk Heat Map :

สรุปค่าระดับความรุนแรงของความเสี่ยงคงเหลือ หรือความเสี่ยงที่เหลือภายหลังการดำเนินกิจกรรมการควบคุม (Residual Risk) ที่ได้จากการประเมินผลกระทบและโอกาสเกิดของปัจจัยเสี่ยง โดยแสดงความเสี่ยงด้านการทุจริตและคอร์รัปชัน (Fraud) และไม่ใช่ด้านการทุจริตและคอร์รัปชัน (Non Fraud) ออกจากกัน ตามเกณฑ์การจัดกลุ่มความเสี่ยง

ภาพรวมระบบ Risk and Control Platform (RCP)

ส่วนประกอบของระบบ RCP

Corporate Heat Map



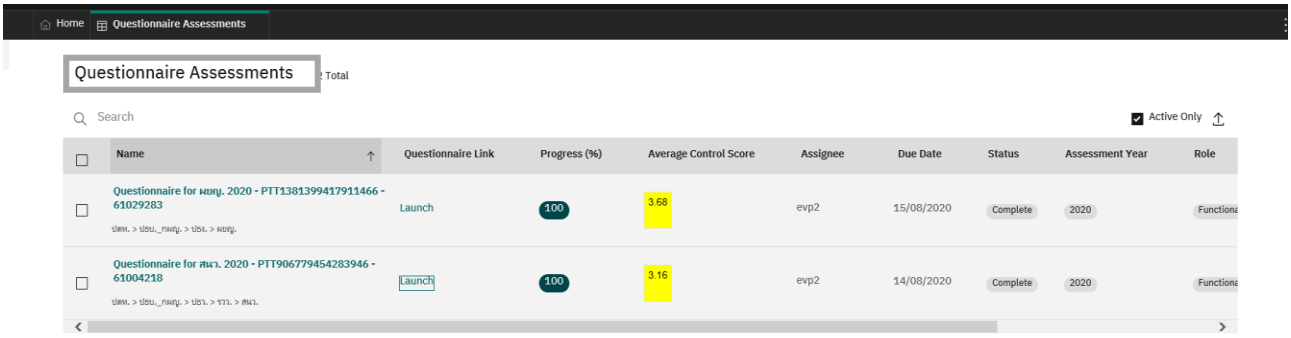
Corporate Heat Map :

สรุปค่าระดับความรุนแรงของความเสี่ยงคงเหลือ หรือความเสี่ยงที่เหลือภายหลังการดำเนินกิจกรรมการควบคุม (Residual Risk) ที่ได้จากการประเมินผลกระทบและโอกาสเกิดของปัจจัยเสี่ยง ตามเกณฑ์การวัดระดับความรุนแรงของความเสี่ยงระดับสายงาน(BU) และเกณฑ์การวัดระดับความรุนแรงของความเสี่ยงระดับองค์กร (Corporate) โดยแสดงความเสี่ยงด้านการทุจริตและคอร์รัปชัน (Fraud) และไม่ใช่ด้านการทุจริตและคอร์รัปชัน (Non Fraud) ออกจากกันตามเกณฑ์การจัดกลุ่มความเสี่ยง

ภาพรวมระบบ Risk and Control Platform (RCP)

ส่วนประกอบของระบบ RCP

Questionnaire Assessment



หน้าจอแสดงจำนวนแบบสอบถามทั้งหมดที่ต้องดำเนินการประเมิน โดยแต่ละแบบสอบถามมีการแสดงข้อมูลสรุปจากการประเมิน ดังนี้

- เปอร์เซ็นต์การตอบคำถามจากจำนวนข้อทั้งหมด (Progress)
- คะแนนเฉลี่ยการควบคุม (Average Control Score)
- ผู้รับผิดชอบในการตอบแบบสอบถาม (Assignee)
- วันที่ครบกำหนดดำเนินการ (Due Date)
- สถานะ : In Progress หรือ Complete (Status)
- ปีที่กำหนดสำหรับแบบสอบถาม (Assessment Year)
- ประเภทของแบบสอบถาม : Functional, Board, Committee หรือ Secondment (Role)

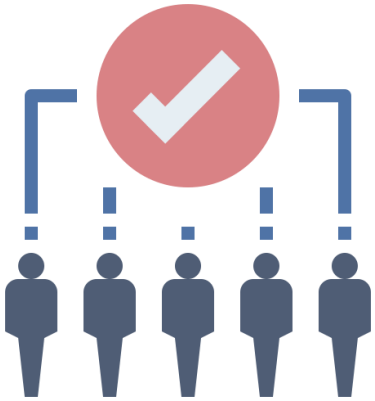
ขั้นตอนและระยะเวลาในการดำเนินการประเมิน GRC Assessment ภายใน ปตท.

	ผู้รับผิดชอบ	ระยะเวลา
ขั้นตอนที่ 1: เตรียมความพร้อม (Preparation) • ทบทวน BU Risk Criteria • สรุปรายการจุดมุ่งเน้น (FCY) • เชื่อมโยงความเสี่ยง CRP และกิจกรรมควบคุมระดับกระบวนการ	IC Team	60 วัน
ขั้นตอนที่ 2: สื่อความบทบาทหน้าที่และแผนการดำเนินงานด้าน GRC ประจำปี ให้แก่ GRC Agent	IC Team	1 วัน
ขั้นตอนที่ 3: เตรียมความพร้อมและนำข้อมูลเข้าสู่ระบบ • ทบทวนคำถามของแบบประเมิน E-CSA • นำข้อมูล BU Risk Criteria/ FCY/ CRP/ อื่น ๆ เข้าระบบ	IC Team	60 วัน
ขั้นตอนที่ 4: สื่อความเกณฑ์และแนวทางการประเมินฯ	IC Team	1 วัน
ขั้นตอนที่ 5: ประเมิน GRC Assessment • ประเมิน GRC Assessment สำหรับหน่วยงานระดับฝ่าย/ส่วนขึ้นตรง • Risk Owner สื่อความและร่วมกับพนักงานในหน่วยงานระบุความเสี่ยงและจุดควบคุมที่สำคัญ พร้อมนำเสนอในที่ประชุมฝ่าย ก่อนอนุมัติในระบบ • GRC Agent สอบทานความถูกต้องและความสอดคล้องของผลประเมินฯ	Risk Owner GRC Agent ผู้บริหาร และ พนักงาน	60 วัน
ขั้นตอนที่ 6: ผู้บริหารประเมิน E-CSA • ผู้บริหารระดับผู้ช่วยขึ้นไป ประเมิน E-CSA • GRC Agent นำเสนอผลการประเมินฯ แก่ผู้บริหารของสายงาน	ผู้บริหาร	60 วัน
ขั้นตอนที่ 7: การติดตามและรายงาน • สรุปผลประเมิน GRC Assessment และรายงานผลการประเมินภาพรวมของ ปตท. แก่คณะกรรมการต่าง ๆ • ติดตามสถานะของแผนปรับปรุงให้เป็นไปตามแผนงานที่กำหนด • สรุปผลการประเมินฯ สำหรับจุดมุ่งเน้น นำส่งหน่วยงาน 2nd Line เพื่อจัดทำแผนการปรับปรุง	IC Team	60 วัน

นิยาม คำจำกัดความ

บริษัทและคณะกรรมการ :

ปตท.	บริษัท ปตท. จำกัด (มหาชน)
บริษัทในกลุ่ม ปตท.	บริษัทหรือนิติบุคคลใด ๆ ที่ ปตท. ถือหุ้นไม่ว่าจะโดยตรงหรือโดยอ้อม และไม่ว่าจำนวนเท่าใดของทุนจดทะเบียน
BOD	คณะกรรมการบริษัท ปตท. จำกัด (มหาชน)
AC	คณะกรรมการตรวจสอบ
CGSC	คณะกรรมการกำกับดูแลกิจการที่ดีและความยั่งยืนของบริษัท ปตท. จำกัด (มหาชน)
PTTMC	คณะกรรมการจัดการของ ปตท.
GRCMC	คณะกรรมการจัดการการกำกับดูแล การบริหารความเสี่ยง การกำกับการปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กรและความยั่งยืน



นิยาม คำจำกัดความ

บุคลากร :

ผู้บริหาร	พนักงานของ ปตท. ตั้งแต่ระดับผู้จัดการส่วนหรือเทียบเท่าขึ้นไป รวมถึงประธานเจ้าหน้าที่บริหาร และกรรมการผู้จัดการใหญ่ของ ปตท. ด้วย
พนักงาน	พนักงานของ ปตท. และพนักงาน ปตท. ที่ได้รับมอบหมายให้ไปปฏิบัติงานในบริษัทในกลุ่ม ปตท. และพนักงานของบริษัทในกลุ่ม ปตท. ที่ได้รับมอบหมายให้มาปฏิบัติงานใน ปตท. รวมถึงลูกจ้างทดลองงานของ ปตท. ด้วย
IC Team	หน่วยงาน (ฝ่ายควบคุมภายในและจัดการความเสี่ยง : ภสญ.) ที่รับผิดชอบในการกำหนดนโยบายและแนวทางการดำเนินงานเกี่ยวกับการควบคุมภายใน และกำกับให้ทุกหน่วยงานในองค์กรมีการจัดวางระบบและ ทำการประเมินความเสี่ยงและการควบคุมภายใน (GRC Assessment) อย่างเป็นระบบเป็นประจำทุกปี รวมถึงมีหน้าที่รายงานผลการประเมินการควบคุมภายในขององค์กรต่อคณะกรรมการต่าง ๆ ที่เกี่ยวข้อง พร้อมทั้งจัดทำรายงานส่งหน่วยงานภายนอก
Risk owner	ตัวแทนหน่วยงาน รับผิดชอบในการประเมินความเสี่ยงและการควบคุมภายใน (GRC Assessment) รวมถึงบริหารจัดการความเสี่ยงภายในหน่วยงาน
GRC Agent	ตัวแทนหน่วยงานแผนของสายงาน รับผิดชอบส่งเสริมและผลักดันให้เกิดการบูรณาการงานที่ครอบคลุมทั้งด้านการกำกับดูแล การควบคุมภายในและจัดการความเสี่ยงในระดับปฏิบัติการ และการปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร ตามแนวทาง GRC

นิยาม คำจำกัดความ

การประเมินและระบบสารสนเทศ :

GRC Assessment การประเมินความเสี่ยงและการควบคุมภายในระดับกระบวนการ

E-CSA การประเมินการควบคุมด้วยตนเอง โดยผู้บริหารระดับผู้ช่วยกรรมการผู้จัดการใหญ่ขึ้นไป ผ่าน Electronic Questionnaire

GRC Assessment in Key Process การประเมินการควบคุมภายใน กระบวนการที่สำคัญ

RCP ระบบปฏิบัติการและจัดการฐานข้อมูล สำหรับใช้ในการประเมินฯ GRC Assessment และ E-CSA และใช้จัดเก็บรายการกระบวนการ ความเสี่ยง และการควบคุม

KPI Key Performance Indicator ตัวชี้วัดผลการดำเนินงานที่สำคัญ

Non-Compliance เหตุการณ์ปฏิบัติที่ไม่สอดคล้องกับกฎหมาย และกฎระเบียบ ของ ปตท.

INCR Incident & Non-Conformance Report ระบบรายงานอุบัติการณ์ของ ปตท.

7

เอกสารอ้างอิง

กฎหมาย ระเบียบ ข้อกำหนด แนวปฏิบัติภายนอก

- พ.ร.บ. ประกอบรัฐธรรมนูญวินัยการเงินการคลังของรัฐ พ.ศ. 2561 มาตรา 79
- หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561
- การประเมินความเพียงพอของระบบการควบคุมภายในของคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)
- คู่มือการประเมินผลการดำเนินงานรัฐวิสาหกิจ ตามมาตรฐาน State Enterprise Assessment Model (SE-AM)
- Achieving Effective Internal Control Over Sustainability Reporting (ICSR): Building Trust and Confidence through the COSO Internal Control –Integrated Framework (2023)
- COSO Internal Control Integrated Framework 2013
- The IIA's Three Lines Model 2020 ; The Update of Three Lines of Defense

กฎหมาย ระเบียบ ข้อกำหนด แนวปฏิบัติภายใน

- นโยบายการควบคุมภายใน
- คู่มือ Enterprise Risk Management (ERM)
- คู่มือการบริหารความเสี่ยงด้านการทุจริตและคอร์รัปชัน
- PTT Integrated Management System (PIMS) Framework

คณะกรรมการกำกับดูแล

- คำสั่งแต่งตั้งคณะกรรมการ บริษัท ปตท. จำกัด (มหาชน)
- คำสั่งแต่งตั้งคณะกรรมการตรวจสอบบริษัท ปตท. จำกัด (มหาชน)
- คำสั่งแต่งตั้งคณะกรรมการกำกับดูแลกิจการที่ดีและความยั่งยืนของบริษัท ปตท. จำกัด (มหาชน)
- คำสั่งแต่งตั้งคณะกรรมการจัดการการกำกับดูแล การบริหารความเสี่ยง การกำกับการปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร และความยั่งยืน

ฝ่ายควบคุมภายในและจัดการความเสี่ยง

บริษัท ปตท. จำกัด (มหาชน)