# คู่มือการประเมินการควบคุมภายใน (Internal Control Manual)

| | |
|---|---|
| 1. ชื่องาน | คู่มือการประเมินการควบคุมภายใน (Internal Control Manual) |
| 2. วิธีการขั้นตอนการปฏิบัติงาน | กลไกสำคัญในการขับเคลื่อนการควบคุมภายในและการบริหาร ความเสี่ยงระดับปฏิบัติการ *หน้า 18*<br>กรอบและแนวทางการจัดวางระบบการควบคุมภายใน *หน้า 19-21*<br>กระบวนการประเมินความเสี่ยงและการควบคุมภายใน *หน้า 22-26*<br>การรายงานผลการควบคุมภายใน *หน้า 27-29* |
| 3. ระยะเวลาการปฏิบัติงานแต่ละขั้นตอน | Timeline การดำเนินงาน *หน้า 21 และ GRC Assessment Timeline*<br>ขั้นตอนการประเมินความเสี่ยงตาม GRC Assessment *หน้า 66* |
| 4. กฎหมายที่เกี่ยวข้อง | กฎหมาย ระเบียบ ข้อกำหนด แนวปฏิบัติภายนอกและภายใน *หน้า 63* |

หมายเหตุ: สามารถคลิกที่เลขหน้าเพื่อลิงก์ไปหน้าที่เกี่ยวข้องนั้น ๆ

# คู่มือ

# การประเมินการควบคุมภายใน

# (Internal Control Manual)

ฝ่ายควบคุมภายในและจัดการความเสี่ยง (ภสญ.)

# สารบัญ

# สารบัญ

# บทนำ

บริษัท ปตท.จำกัด (มหาชน) (ปตท.) มีสถานะเป็นรัฐวิสาหกิจและบริษัทจดทะเบียนในตลาดหลักทรัพย์ ดำเนินธุรกิจด้านพลังงานและปิโตรเคมีอย่างครบวงจร ในฐานะเป็นบริษัทพลังงานแห่งชาติ โดยมีพันธกิจในการดูแลผู้มีส่วนได้ส่วนเสียอย่างสมดุล สร้างการเติบโตทางเศรษฐกิจ มุ่งยกระดับขีดความสามารถการแข่งขันของประเทศ พัฒนาสังคมและยกระดับคุณภาพชีวิต สร้างนวัตกรรมและนำเทคโนโลยีมาใช้ในทุกภาคส่วน รวมทั้งเป็นพลังขับเคลื่อนวิถีชีวิตผู้คน สังคม ชุมชน สิ่งแวดล้อม ให้ก้าวผ่านการเปลี่ยนแปลงไปข้างหน้า ภายใต้วิสัยทัศน์ “ขับเคลื่อนทุกชีวิต ด้วยพลังแห่งอนาคต” (Powering Life with Future Energy and Beyond)

ปตท. ต้องเผชิญกับกระแสการแข่งขัน และการเปลี่ยนแปลงทางเศรษฐกิจ สังคม และสิ่งแวดล้อมที่รุนแรงและรวดเร็ว การเปลี่ยนแปลงดังกล่าวส่งผลกระทบต่อทิศทางกลยุทธ์ กระบวนการตัดสินใจทางธุรกิจ ตลอดจนการดำเนินงานและความสำเร็จขององค์กร

ปตท. จึงได้กำหนดกรอบและแนวปฏิบัติเรื่องการควบคุมภายในและการบริหารความเสี่ยงซึ่งถือเป็นรากฐานที่สำคัญในการดำเนินธุรกิจ เพื่อใช้เป็นเครื่องมือในการกำกับดูแลกิจการที่ดี สามารถสร้างมูลเพิ่มให้กับองค์กร ตลอดจนสร้างความเชื่อมั่นให้กับผู้มีส่วนได้เสียและผู้เกี่ยวข้องทุกฝ่ายเพื่อสร้างความมั่นใจในระดับสมเหตุสมผลว่าองค์กรจะบรรลุวัตถุประสงค์ และเป้าหมายในการดำเนินธุรกิจทั้งในระยะสั้น และระยาว

# 1

# การควบคุมภายใน

# ความหมายและวัตถุประสงค์ของการควบคุมภายใน

***การควบคุมภายใน*** หมายถึง กระบวนการปฏิบัติงานที่ออกแบบร่วมกันโดยคณะกรรมการ ฝ่ายบริหาร และบุคลากรทุกคนขององค์กร เพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่า การดำเนินงานขององค์กร หน่วยงานสามารถบรรลุวัตถุประสงค์ของการควบคุมภายใน 3 ประการ คือ

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

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

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

# 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 บริหาร จัดการความเสียหายต่างๆ ที่อาจเกิดขึ้นกับบริษัทและผู้มีส่วนได้เสียได้เป็นอย่างดี ทั้งยังก่อให้เกิดความมั่นใจอย่างสมเหตุสมผลว่า องค์กรจะบรรลุวัตถุประสงค์และเป้าหมาย ทั้งด้านการดำเนินงาน การรายงาน และการปฏิบัติตามกฎระเบียบ ดังนั้นเป็นหน้าที่ของคณะกรรมการบริษัท ที่จะต้องดำเนินการให้มั่นใจว่า บริษัทมีระบบการควบคุมภายในที่เหมาะสมและเพียงพอ ในการดูแลการดำเนินงานให้เป็นไปตามเป้าหมาย และวัตถุประสงค์

ฝ่ายบริหารและบุคลากรทุกคนขององค์กร ต้องมีความเข้าใจในระบบและการประเมินการควบคุมภายใน เพื่อที่จะทำการจัดวางและประเมินระบบการควบคุมภายในขององค์กร ให้เป็นไปอย่างเหมาะสมและเพียงพอ

# ขอบเขตและความจำเป็นของการควบคุมภายใน

## ขอบเขตของการควบคุมภายใน

- การควบคุมภายในเป็นกระบวนการที่แทรกอยู่ในกระบวนการดำเนินงานและธุรกรรมของกิจการที่ดำเนินการอยู่เป็นประจำวัน
- การควบคุมภายในจะต้องมีการกำหนดขึ้น ดำรงอยู่ และมีการกำกับติดตามประสิทธิผลของการควบคุมโดยผู้บริหารและบุคลากรทุกระดับ
- การควบคุมภายในเป็นส่วนหนึ่งของกลไกที่ช่วยให้การดำเนินงานสามารถบรรลุผลลัพธ์ตามเป้าหมายและวัตถุประสงค์ที่กำหนดไว้
- การควบคุมภายในจะต้องคำนึงถึงความคุ้มค่า การประหยัดค่าใช้จ่าย และได้ประโยชน์จากการควบคุมมากกว่าค่าใช้จ่ายที่ใช้ในการควบคุม
- ระบบของการควบคุมภายในในกิจการเป็นความรับผิดชอบของบุคลากรทุกคน ตั้งแต่ระดับบริหารถึงระดับพนักงานระดับปฏิบัติการ

## ความจำเป็นที่ทำให้กิจการต้องมีการควบคุมภายใน

- เพื่อให้เกิดความรับผิดรับชอบ (Accountability) โดยความรับผิดชอบขั้นพื้นฐาน คือ การบริหารทรัพยากรที่ได้รับการจัดสรรจากกิจการให้เกิดประสิทธิภาพ ประสิทธิผล และความคุ้มค่า
- เพื่อส่งเสริมให้เกิดการปฏิบัติด้านการบริหารที่ดีในการปกป้องและรักษาสินทรัพย์ของกิจการ และทำให้เกิดมูลค่าเพิ่มแก่กิจการตามลำดับ ซึ่งมาจากการปฏิบัติงานที่ดี รายงานทางการเงินที่ครบถ้วน ถูกต้อง และการกำกับการปฏิบัติตามกฎเกณฑ์อย่างครบถ้วน

# ความเชื่อมโยงของระบบการควบคุมภายในกับระบบอื่น

การควบคุมภายในกระบวนการปฏิบัติงานที่คณะกรรมการ ฝ่ายบริหาร และบุคลากรทุกคนขององค์กร มีบทบาทหน้าที่ร่วมกัน ดังนั้น เพื่อให้องค์กรสามารถบรรลุวัตถุประสงค์ของการควบคุมภายใน จึงต้องมีการบูรณาการ และเชื่อมโยงระบบการควบคุมภายในกับระบบงานอื่น ๆ


## 1. การกำกับดูแลกิจการที่ดี การบริหารจัดการความเสี่ยงในระดับปฏิบัติการและการควบคุมภายใน การปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร (GRC)

การควบคุมภายในเป็นส่วนงานหนึ่งของ 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) จะต้องถูกถ่ายทอดไปยังระดับกลุ่มธุรกิจและสายงานสนับสนุน (Business Group & Support Function Level) และระดับหน่วยปฏิบัติงาน (Functional Level) โดย Risk Owner จะรับผิดชอบในการระบุความเสี่ยงที่ถูกถ่ายทอดจากระดับองค์กรในการประเมินการควบคุมภายในของหน่วยงานด้วย


## 3. การตรวจสอบภายใน

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


## 4. การบริหารคุณภาพองค์กร

การบริหารคุณภาพองค์กร เป็นกระบวนการพัฒนามาตรฐาน แนวปฏิบัติ ระบบการจัดการ เพื่อเพิ่มประสิทธิภาพการนำระบบงาน (PTT Organization System) ไปสู่การปฏิบัติตลอดกระบวนการทำงานแบบ End – to – End Process ควบคู่กับการบูรณาการความเสี่ยง และจุดควบคุมที่สำคัญในขั้นตอนการปฏิบัติงานทั้งกระบวนการหลัก และกระบวนการสนับสนุน ทำให้มั่นใจว่าการดำเนินงานขององค์กรจะสอดคล้องกับกฎหมาย กฎ ระเบียบ ข้อบังคับ และข้อกำหนดที่เกี่ยวข้อง ก้าวสู่องค์กรแห่งความเป็นเลิศอย่างยั่งยืน


## 5. State Enterprise Assessment Model (SE-AM)

ระบบการประเมินผลการดำเนินงานรัฐวิสาหกิจ: SE-AM เป็นเครื่องมือในการกำกับ ติดตาม ประเมินผลการดำเนินงานรัฐวิสาหกิจ โดยสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ซึ่งการบริหารความเสี่ยงและการควบคุมภายใน (Risk Management & Internal Control : RM&IC) เป็นหัวข้อหนึ่งใน 8 หลักเกณฑ์การประเมินกระบวนการปฏิบัติงานและการจัดการ (Core Business Enablers) โดย ปตท. มีหน้าที่รายงานผลการดำเนินงานเพื่อแสดงให้เห็นว่าองค์กรมีการบริหารความเสี่ยงที่เป็นระบบ มีประสิทธิภาพ รวมทั้งมีการบูรณาการระหว่างการบริหารความเสี่ยงและการควบคุมภายในเข้าด้วยกัน เพื่อเสริมสร้างศักยภาพขององค์กรให้สามารถตอบสนองกับความเสี่ยง ภัยคุกคามต่างๆได้เป็นอย่างดี ส่งผลให้องค์กรบรรลุวัตถุประสงค์เชิงยุทธศาสตร์ตามที่ได้กำหนดไว้

# 2

# การจัดวางระบบการควบคุมภายในของ ปตท.

# หน้าที่การจัดวางระบบการควบคุมภายในของ ปตท.

ปตท. ในฐานะรัฐวิสาหกิจ และบริษัทจดทะเบียนในตลาดหลักทรัพย์ มีหน้าที่จัดวางระบบการควบคุมภายใน และประเมินผลการควบคุมภายใน อย่างน้อยปีละ 1 ครั้ง และสรุปผล รวมถึงจัดทำรายงานที่เกี่ยวข้องให้หน่วยงานกำกับดูแลตามกำหนด

## รัฐวิสาหกิจ

- ปตท. มีหน้าที่จัดวางระบบการควบคุมภายใน ประเมินผลการควบคุมภายในอย่างน้อยปีละ 1 ครั้ง และจัดส่งรายงานให้กระทรวงการคลัง ผ่านกระทรวงพลังงาน 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.)

# การพัฒนา การควบคุมภายในของ ปตท.

**2535**

**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**

- แบบประเมินตนเองเกี่ยวกับมาตรการต่อต้านการคอร์รัปชัน
- 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 onward**

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

# นโยบาย
# การควบคุมภายในของ ปตท.

**ประกาศบริษัท ปตท. จำกัด (มหาชน)**
**เรื่อง นโยบายการควบคุมภายใน**

---

เพื่อสร้างความเชื่อมั่นต่อผู้มีส่วนได้เสียทุกภาคส่วนว่า 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 ตลอดจนประเมินความเสี่ยงในระดับปฏิบัติการและกำหนดกิจกรรมควบคุมที่เพียงพอ เหมาะสม และถ่ายทอดให้พนักงานในหน่วยงานนำการควบคุมภายในไปปฏิบัติและปรับปรุง รวมทั้งติดตามผลการดำเนินงานของหน่วยงานที่รับผิดชอบ

ข้อ 4 กำหนดให้มีหน่วยงานตรวจสอบ เป็นผู้สอบทานหรือประเมินผลการควบคุมภายในขององค์กรอย่างเป็นอิสระ เพื่อให้ความมั่นใจว่าหน่วยรับตรวจมีการควบคุมภายในที่มีประสิทธิภาพและประสิทธิผล มีการบริหารความเสี่ยงอยู่ในระดับที่ยอมรับได้

ข้อ 5 บุคลากรของ ปตท. มีหน้าที่ปฏิบัติงานตามระบบการควบคุมภายใน รวมถึงรายงานปัญหาจากการปฏิบัติงานให้ผู้บังคับบัญชารับทราบ เพื่อให้เกิดการปรับปรุงแก้ไขและลดผลกระทบที่อาจเกิดขึ้นได้อย่างทันท่วงที

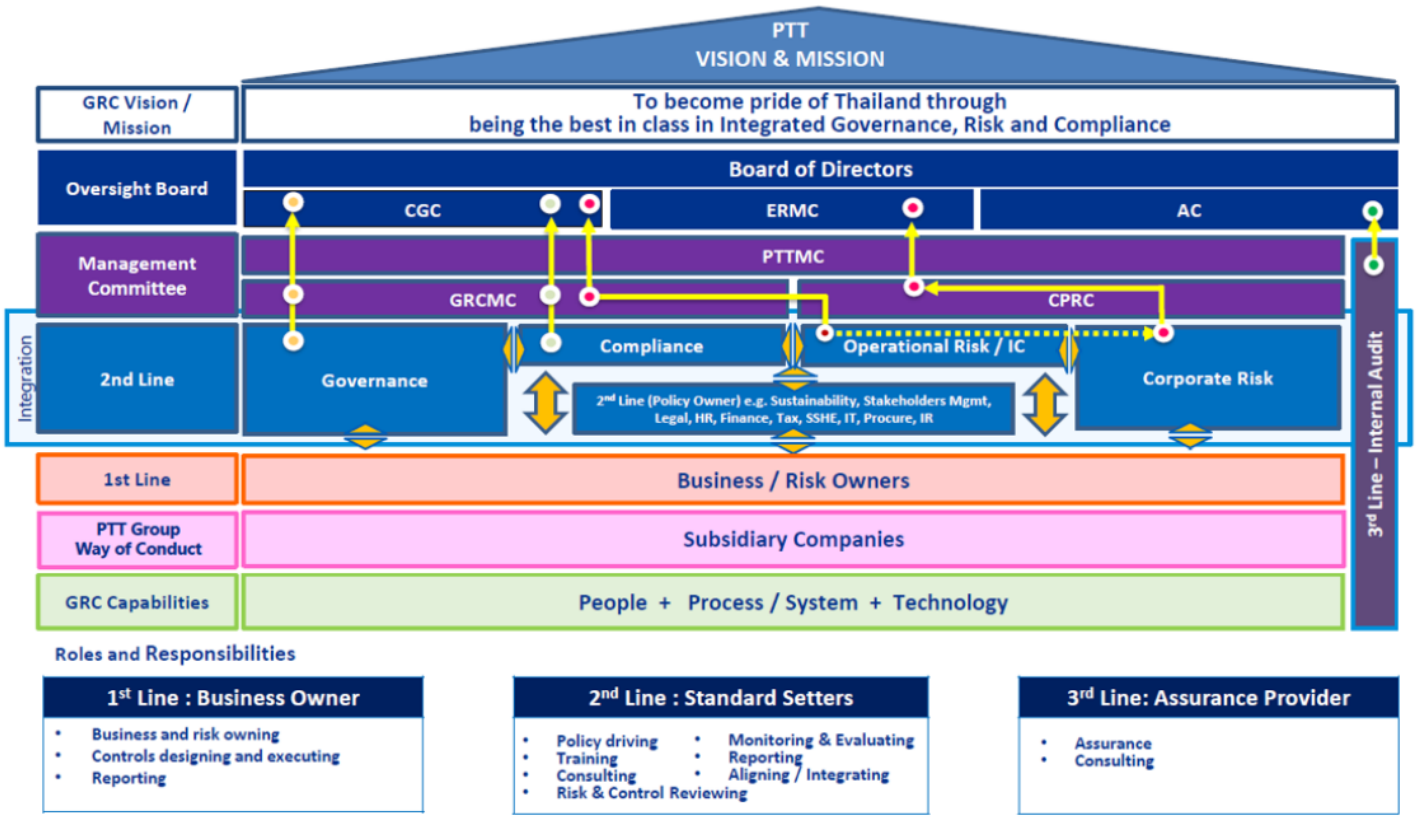
ประกาศ ณ วันที่ 26 กุมภาพันธ์ พ.ศ. 2562

(นายชาญศิลป์ ตรีนุชกร)

ประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่

# โครงสร้างและบทบาทหน้าที่

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




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

- กำหนดแนวทางการบริหารจัดการความเสี่ยงและการควบคุมในระดับองค์กร และกำกับดูแลกระบวนการบริหารจัดการความเสี่ยงและการควบคุมให้มีประสิทธิภาพ ประสิทธิผล

## คณะกรรมการตรวจสอบ (Audit Committee)

- สอบทานประสิทธิภาพและประสิทธิผลของกระบวนการกำกับดูแลที่ดี กระบวนการบริหารความเสี่ยง และกระบวนการควบคุมภายใน

## คณะกรรมการกำกับดูแลกิจการที่ดีของบริษัท ปตท. จำกัด (มหาชน) (CGC)

- กำกับดูแลและติดตามการดำเนินงานด้าน การกำกับดูแลกิจการที่ดี 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)

## คณะกรรมการการกำกับดูแล การบริหารความเสี่ยง และการกำกับการปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร (GRCMC)

- กำกับการดำเนินงานด้าน GRC การต่อต้านทุจริตและคอร์รัปชัน การบริหารจัดการความยั่งยืน และการดูแลสังคม ชุมชน และสิ่งแวดล้อม ให้มีการจัดทำแผนงานระยะสั้นและระยะยาวซึ่งสอดคล้องกับกรอบนโยบายของคณะกรรมการ CGC
- กำกับดูแลและติดตามความคืบหน้าผลการดำเนินงานตามแผนงาน ให้ข้อคิดเห็น คำแนะนำ และให้คำปรึกษา เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพ และประสิทธิผล
- ผลักดัน ส่งเสริม และให้คำปรึกษา เพื่อให้หน่วยธุรกิจและสายงานสนับสนุนนำหลักการและนโยบายไปปฏิบัติ รวมถึงปรับปรุงกระบวนการทำงานให้สอดคล้องกับวัตถุประสงค์ของ ปตท. และเป็นไปตามกรอบการดำเนินงานที่กำหนด
- ส่งเสริมให้ขยายผลการดำเนินงานไปสู่บริษัทในกลุ่ม ปตท. รวมทั้ง กลุ่มผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง อาทิ คู่ค้า ลูกค้า เพื่อร่วมยกระดับสู่มาตรฐานสากล

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

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

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

- กำหนดมาตรฐาน แนวปฏิบัติ นโยบาย ระเบียบ ข้อกำหนด เช่น นโยบาย CG/ IC/ Digital
- 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 Lines ตาม Risk-Based Audit Approach
- ประสานงาน แลกเปลี่ยนข้อมูล และกำหนดแนวทางการดำเนินงานร่วมกันกับ 2nd Line

# กลไกสำคัญในการขับเคลื่อนการควบคุมภายในและการบริหารความเสี่ยงระดับปฏิบัติการ

ปตท. กำหนดบทบาทหน้าที่ในการผลักดันการประเมินการควบคุมภายใน ในแต่ละระดับ ดังนี้

**ผู้บริหารทุกระดับ**

- สื่อสาร ถ่ายทอดนโยบายการบริการความเสี่ยงและการควบคุมภายใน
- สนับสนุน ผลักดัน ให้หน่วยงานในสังกัดมีระบบการควบคุมภายในที่มีประสิทธิผล
- ให้ข้อเสนอแนะเกี่ยวกับความเสี่ยงและการกำหนดกิจกรรมควบคุมที่เพียงพอ เหมาะสม
- ถ่ายทอดให้พนักงานในหน่วยงานนำกิจกรรมการควบคุมไปปฏิบัติและปรับปรุง
- ติดตามผลการดำเนินงานของหน่วยงานในสังกัด

## GRCMC

- กำกับดูแลให้มีการจัดทำแผนงานด้านการบริหารความเสี่ยงในระดับปฏิบัติการและการควบคุมภายใน
- กำกับดูแล ติดตามความคืบหน้า ให้ข้อคิดเห็นและคำปรึกษา
- ส่งเสริมให้มีการขยายผลการดำเนินงานไปสู่บริษัทในกลุ่ม รวมทั้งผู้มีส่วนได้ส่วนเสีย เพื่อร่วมยกระดับมาตรฐาน

## IC Team

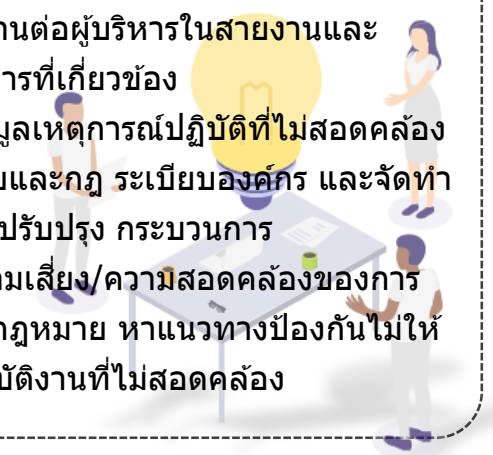
- จัดทำนโยบาย กรอบการควบคุมภายใน แนวทางการประเมินการควบคุมภายใน
- จัดให้มีการประเมินการควบคุมภายใน
- สรุปรายงานผลการประเมินฯ นำเสอคณะกรรมการที่เกี่ยวข้อง และหน่วยงานกำกับดูแล

## Risk Owner

- เป็นศูนย์กลางของหน่วยงานในการรวบรวมข้อมูลเพื่อใช้ประกอบในการประเมินความเสี่ยงและการควบคุมภายใน (GRC Assessment)
- ทบทวน ประเมินความเสี่ยงและการควบคุมภายใน รวมถึงจัดทำแผนปรับปรุงการดำเนินงานร่วมกับพนักงานในหน่วยงาน และผู้จัดการฝ่าย
- บันทึกข้อมูลในระบบ RCP
- ติดตามผลการดำเนินงานตามแผนปรับปรุงที่กำหนด

## GRC Agent

- เป็นตัวแทนสายงานในการสนับสนุน ผลักดันการดำเนินงานด้าน GRC
- ศึกษา ทำความเข้าใจ และเข้าร่วมกิจกรรมด้าน GRC
- ร่วมกำหนดเกณฑ์การประเมินความเสี่ยงระดับสายงาน
- สื่อความแผน เกณฑ์ วิธีการประเมินความเสี่ยง
- และการควบคุมภายใน และกฎหมาย กฎระเบียบที่เกี่ยวข้องในการปฏิบัติงาน
- ถ่ายทอดความรู้ สร้างความตระหนักด้านความสำคัญของการบริหารความเสี่ยง การควบคุมภายใน การปฏิบัติตามกฎหมายและกฎระเบียบ
- ให้คำแนะนำแก่หน่วยงานภายใต้สายงาน ในการระบุและประเมินความเสี่ยง การควบคุม รวมถึงแผนการปรับปรุงกระบวนการ
- รวบรวมผลการประเมิน และแผนการปรับปรุง พร้อมรายงานต่อผู้บริหารในสายงานและคณะกรรมการที่เกี่ยวข้อง
- รวบรวมข้อมูลเหตุการณ์ปฏิบัติที่ไม่สอดคล้องกับกฎหมายและกฎ ระเบียบองค์กร และจัดทำแผนแก้ไข ปรับปรุง กระบวนการ
- ประเมินความเสี่ยง/ความสอดคล้องของการปฏิบัติตามกฎหมาย หาแนวทางป้องกันไม่ให้เกิดการปฏิบัติงานที่ไม่สอดคล้อง



# กรอบและแนวทางการจัดวางระบบการควบคุมภายใน

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


- **ภายนอก**
  - กระทรวงการคลัง
  - ตลาดหลักทรัพย์
- **ภายใน**
  - ผู้บริหารสายงาน
  - GRCMC
  - PTTMC
  - CGC
  - PTT AC
  - PTT BOD

- **กำหนดวัตถุประสงค์**
- **วิเคราะห์/รวบรวมข้อมูลประสิทธิภาพ ประสิทธิผลของกระบวนการ ความเสี่ยง**
- **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

- **การประเมินภายในด้วยตนเอง**
  - E-CSA
  - GRC Assessment

  โดยพิจารณาประสิทธิภาพ ประสิทธิผลของกระบวนการ / ข้อบกพร่อง
- **การประเมินผลอย่างเป็นอิสระ**
  - Internal Audit
  - External Party

- **รวบรวมข้อมูลประสิทธิภาพประสิทธิผลของ Control**
- **Control Testing**

  เช่น การทดสอบความถูกต้อง การเปรียบเทียบข้อมูล
- **ทดสอบ Present และFunction ของ Control**
- **รายงานข้อบกพร่อง**

# กรอบและแนวทางการจัดวางระบบการควบคุมภายใน

การกำหนดหรือการออกแบบระบบการควบคุมภายในที่มีประสิทธิผลมีขั้นตอนดังนี้

1. กำหนดวัตถุประสงค์ของหน่วยงาน และกระบวนการหลักที่ชัดเจนเพื่อช่วยให้ผู้บริหารสามารถบริหารและติดตามการปฏิบัติงาน พนักงานสามารถดำเนินงานให้บรรลุวัตถุประสงค์นั้นๆ ซึ่งการกำหนดวัตถุประสงค์ของหน่วยงานควรมีลำดับ ดังนี้
   - กำหนดภารกิจหลักของหน่วยงาน
   - กำหนดวัตถุประสงค์ของกระบวนการปฏิบัติงาน
2. กำหนดกระบวนการปฏิบัติงานและออกแบบการควบคุมให้มีครบทั้ง 5 องค์ประกอบของการควบคุมภายในที่จะทำให้การดำเนินงานสามารถบรรลุตามวัตถุประสงค์ที่กำหนดไว้ และสอดคล้องกับวัตถุประสงค์ของการควบคุมภายในทั้ง 3 ประการ คือ
   - ประสิทธิภาพประสิทธิผลของการดำเนินงาน (Operation: O)
   - ความเชื่อถือได้ของรายงานทางการเงิน และไม่ใช่การเงิน (Reporting: R) และ
   - การปฏิบัติตามกฎหมาย ระเบียบและข้อบังคับ (Compliance: C)
3. ประเมินความเสี่ยงทั้งจากปัจจัยภายในและภายนอกที่อาจทำให้การดำเนินงานไม่สามารถบรรลุวัตถุประสงค์ของกระบวนการปฏิบัติงาน รวมถึงการประเมินความเสี่ยงด้านทุจริต
4. พิจารณาว่ากระบวนปฏิบัติงานและการควบคุมที่ออกแบบไว้ว่าสามารถที่จะป้องกันหรือลดความเสี่ยงได้
5. ออกแบบหรือกำหนดกิจกรรมควบคุมเพิ่มเติมเพื่อป้องกันความเสี่ยง หรือลดความเสี่ยงที่เหลือให้อยู่ในระดับที่ยอมรับได้
6. ประมาณการต้นทุนที่จะต้องใช้ในการดำเนินการให้มีกิจกรรมควบคุมนั้นๆ และพิจารณาว่าต้นทุนหรือค่าใช้จ่ายต้องไม่สูงกว่าประโยชน์ที่จะได้รับจากการมีกิจกรรมควบคุม
7. กำหนดแผนในการนำกิจกรรมควบคุมนั้นมาปฏิบัติใช้ในการดำเนินงาน
8. ดำเนินการตามแผนและปฏิบัติตามการควบคุมที่ได้ออกแบบไว้ รวมทั้งติดตามและประเมินผล
9. ประเมินประสิทธิภาพของการปฏิบัติงานและประสิทธิผลของการควบคุมภายใน (ตามเกณฑ์การประเมินการประเมินระดับองค์กร (Appendix 4))

เนื่องจากองค์กรมีการดำเนินงานเรื่องการควบคุมภายในอยู่แล้ว และการจัดวางระบบการควบคุมภายใน จะแฝงอยู่ในกระบวนการปฏิบัติงาน ดังนั้นการกำหนดหรือการออกแบบการควบคุมจะเป็นการประเมินเพื่อปรับปรุงการควบคุมภายในที่มีการออกแบบไว้แล้ว

# Timeline การดำเนินงาน

| | GRC Agent & Risk owner | IC Team (ภสญ.) |
|---|---|---|
| Q1 |  <br>▪ **Risk owner**<br>• รวบรวมแนวโน้ม กระแสการเปลี่ยนแปลงที่กระทบกับการปฏิบัติงาน<br>• รวบรวมข้อมูลประสิทธิภาพ ประสิทธิผลของกิจกรรมการควบคุม ข้อบกพร่อง Non-compliance เพื่อใช้ประกอบการทบทวน ประเมินการควบคุมภายใน<br>• ทบทวนกระบวนการปฏิบัติงาน | ▪ ทบทวนระเบียบ คำสั่ง และกฎหมายที่เกี่ยวข้อง เพื่อปรับปรุงนโยบาย กรอบการควบคุมภายใน แนวทางการประเมินการควบคุมภายใน<br>▪ ทบทวนฐานข้อมูลความเสี่ยง จุดควบคุมที่สำคัญ ให้สอดคล้องกับกระบวนการที่เปลี่ยนแปลงไป<br>▪ ทบทวนข้อมูลโครงสร้างองค์กร และเนื้อหา FD ของหน่วยงาน เพื่อจัดทำ Process List and Process Mapping สำหรับการประเมินฯ<br>▪ ทบทวนข้อมูลคำถามในการประเมิน E-CSA |
| Q2 | ▪ **GRC Agent และ Risk owner** รับฟังสื่อความแผนและแนวทางการประเมิน GRC Assessment และ E-CSA | ▪ อบรม ให้ความรู้ ด้านความเสี่ยงระดับปฏิบัติการและการควบคุมภายใน<br>▪ สื่อความแผนและแนวทางการประเมิน GRC Assessment & E-CSA ให้แก่ GRC Agent และ Risk owner |
| Q3 | ▪ **Risk owner** ประเมินฯ และจัดทำแผนปรับปรุงการดำเนินงาน ร่วมกับพนักงานในหน่วยงาน ผู้จัดการฝ่าย พร้อมขออนุมัติผ่านระบบ RCP<br>▪ **GRC Agent** ติดตามและสอบทานความถูกต้องผลประเมินฯ ของหน่วยงานในสายงาน<br>▪ ผู้บริหารระดับ EVP SEVP และ C Level ตอบ E-CSA และอนุมัติการประเมิน GRC Assessment | ▪ Launch GRC Assessment & E-CSA เพื่อให้หน่วยงานและผู้บริหารทำการประเมิน<br>▪ ให้คำปรึกษาและสอบทานความถูกต้องของผลการประเมินฯ<br>▪ จัดทำรายงานสรุปผลการประเมินฯ ของแต่ละสายงานให้ GRC Agent |
| Q4 | ▪ **GRC Agent** รายงานสรุปผลการประเมินของสายงานต่อที่ประชุมสายงาน และ GRCMC | ▪ สรุปและรายงานผลการควบคุมภายในของ ปตท. ต่อคณะกรรมการต่างๆ GRCMC > PTTMC > CGC > AC >BOD<br>▪ จัดทำรายงานผลการประเมินการควบคุมภายใน รายงานต่อหน่วยงานกำกับดูแล กระทรวงการคลัง/ ก.ล.ต./ SE-AM |

# GRC Assessment Timeline

GRC Agent | Risk Owner | 2nd Line

## Preparation

- **ทบทวน** BU Risk Criteria
- สรุปรายการจุดมุ่งเน้น (FCY)
- **เชื่อมโยง**ความเสี่ยง CRP กับความเสี่ยงและกิจกรรมควบคุมระดับกระบวนการ
- **ทบทวน**รายชื่อตัวแทน

- ทบทวนคำถามของแบบประเมิน E-CSA
- นำข้อมูล BU Risk Criteria/ FCY/ CRP/ อื่นๆ เข้าระบบ RCP

## Assessment

- ประเมิน GRC Assessment สำหรับหน่วยงานระดับฝ่าย/ส่วนขึ้นตรง โดยผลการประเมินผ่านการอนุมัติจาก ผจ.ฝ่าย
- Risk Owner มีการสื่อความและร่วมกับพนักงานในหน่วยงานระบุความเสี่ยงและจุดควบคุมที่สำคัญ พร้อมนำเสนอในที่ประชุมฝ่าย ก่อนอนุมัติการประเมินในระบบ
- Risk Owner ผลักดันให้หน่วยงานมีการ *KM sharing ความเสี่ยงและจุดควบคุมที่สำคัญ*
- GRC Agent **สอบทาน**ความถูกต้องและความสอดคล้องของผลการประเมินฯ

- ประเมิน E-CSA สำหรับผู้บริหารระดับผู้ช่วยขึ้นไป
- **นำเสนอ**ผลการประเมินฯ แก่ผู้บริหารของสายงาน

## Report

- **ติดตามสถานะ**ของแผนปรับปรุง ให้เป็นไปตามแผนงานที่กำหนด
- สรุปผลการประเมินฯ สำหรับจุดมุ่งเน้น นำส่งหน่วยงาน 2nd Line
- 2nd Line พิจารณาแผนการปรับปรุง
- รายงานผลการประเมินภาพรวมของ ปตท. แก่คณะกรรมการต่างๆ

**FEB-MAR**

PR สื่อความบทบาทหน้าที่และแผนการดำเนินงานประจำปีด้าน GRC แก่ GRC Agent (20 มี.ค.)

**APR-MAY**

**JUN-JUL**

PR สื่อความเกณฑ์และแนวทางการประเมินฯ (5 มิ.ย.)

**(Onsite) Train the Risk Owner** NEW
สอนขั้นตอนการประเมินฯ และการใช้งานระบบ RCP ให้แก่ Risk Owner และผู้สนใจแยกตามแต่ละสายงาน

**AUG-SEP**

**OCT-DEC**

# 3

# กระบวนการการประเมินความเสี่ยงและการควบคุมภายใน

# การประเมินความเสี่ยงและการควบคุมภายใน

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

**Present** – การควบคุมภายในมีอยู่จริงทั้งในด้านของการออกแบบและการนำไปปฏิบัติ

**Functioning** – การควบคุมภายในที่ออกแบบไว้สามารถทำหน้าที่ควบคุม จัดการ ป้องกัน หรือช่วยให้ค้นพบความเสี่ยงได้อย่างทันเวลา หรือสามารถทำหน้าที่ได้ตามที่ได้ออกแบบไว้

การประเมินการควบคุมภายใน จะดำเนินการควบคู่ไปกับการประเมินความเสี่ยงในระดับปฏิบัติการ โดยใช้แนวทางการประเมินความเสี่ยงตามคู่มือ Enterprise Risk Management (ERM) และคู่มือการบริหารความเสี่ยงด้านการทุจริตและคอร์รัปชัน

## แนวทางการประเมินความเสี่ยงและการควบคุมภายใน

ปตท. กำหนดแนวทางประเมินความเสี่ยงระดับปฏิบัติการและการควบคุมภายในออกเป็น 2 รูปแบบ ได้แก่

### I. การประเมินแบบทั่วทั้งองค์กร (All Area)

- ระดับผู้บริหาร (E-CSA)
- ระดับกระบวนการ (GRC Assessment)

### II. การประเมินแบบเฉพาะเจาะจง (Specific Area)

- ภายใน ปตท. (PTT Specific area)
- ภายในกลุ่ม ปตท. (PTT Group Specific area)

# I. การประเมินแบบทั่วทั้งองค์กร (All Area)

การประเมินแบบ All Area เป็นการประเมินการควบคุมด้วยตนเอง (Control Self-Assessment : CSA) โดย ปตท. จัดให้มีการประเมินปีละ 1 ครั้ง โดยกำหนดแนวทางการประเมินออกเป็น 2 ระดับ ดังนี้

## 1. ระดับผู้บริหาร (E-CSA)

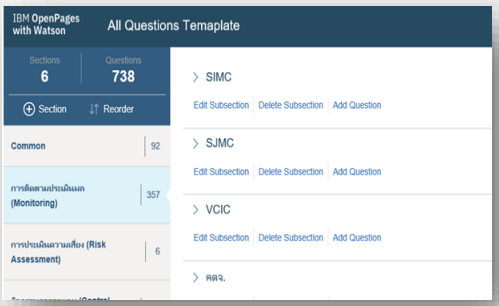
EVP /SEVP / C-Level/ Secondment

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)



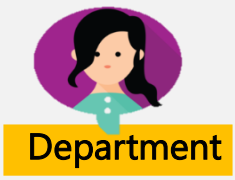

โดยคำถามครอบคลุมองค์ประกอบทั้ง 5 ของการควบคุม แบ่งออกเป็นคำถามทั่วไป (Common) เกี่ยวกับการปฏิบัติตามแนวปฏิบัติ ระเบียบ และนโยบายขององค์กร และคำถามเฉพาะเจาะจง (Specific) เกี่ยวกับบทบาทหน้าที่ตามที่ได้รับมอบหมาย

**2** **ให้ความเห็นและกำหนดแนวทางเพื่อการพัฒนาการควบคุมภายใน**

กรณีมีกระบวนการที่ไม่ได้ปฏิบัติตามการควบคุมไว้ ผู้บริหารต้องให้ความเห็นและกำหนดแนวทางเพื่อการพัฒนาและบริหารจัดการต่อไป

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

## 2. ระดับกระบวนการ (GRC Assessment)




คือ การประเมินความเสี่ยงและการควบคุมภายในระดับกระบวนการตามจุดมุ่งเน้นด้านการบริหารความเสี่ยง 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
- **กระบวนการสนับสนุน (Support)** : กระบวนการที่หน่วยงานต้องปฏิบัติตามแนวปฏิบัติ ระเบียบ และนโยบายตามที่หน่วยงาน 2nd Line กำหนด

**2 ประเมินความเสี่ยงและการควบคุม**

- **ประเมินความเสี่ยงที่สำคัญ*** : ประเมินความรุนแรงและโอกาสเกิดความเสี่ยง โดยเลือกใช้เกณฑ์ ดังนี้
  - **ความเสี่ยงที่ไม่ใช่ด้านการทุจริต (Non-Fraud)**
    - เกณฑ์ความเสี่ยงระดับ BU : สำหรับกระบวนการหลัก
    - เกณฑ์ความเสี่ยงระดับองค์กร : สำหรับกระบวนการสนับสนุน และกระบวนการหลักที่ความเสี่ยงเชื่อมโยงกับความเสี่ยงระดับองค์กร
  - **ความเสี่ยงด้านการทุจริต (Fraud)**
    - เกณฑ์ความเสี่ยงด้านการทุจริตและคอร์รัปชัน
- **ประเมินการควบคุม :** ประเมินความเพียงพอของการออกแบบการควบคุมภายในและการปฏิบัติตามภายควบคุม (Control Design & Compliance)

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

**3 กำหนดและปฏิบัติตามแผนการปรับปรุง (Action Plan)**

ระบุแผนการปรับปรุง กรณีที่คะแนนความเสี่ยงหลังการควบคุมอยู่ในระดับ E (Extreme) และ/หรือ คะแนนการควบคุม ≤ 3

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

# II. การประเมินแบบเฉพาะเจาะจง (Specific area)

การประเมินแบบเฉพาะเจาะจง เป็นการประเมินการควบคุมภายในและการบริหารความเสี่ยงในระดับปฏิบัติการของหน่วยงานใน ปตท. และบริษัทในกลุ่ม โดยมีการกำหนดกระบวนการดำเนินธุรกิจระดับปฏิบัติการ เพื่อให้กระบวนการดำเนินงานเป็นไปอย่างมีประสิทธิภาพ มีการจัดวางระบบการควบคุมภายในที่เพียงพอเหมาะสม สอดคล้องกับกรอบการควบคุมภายในหลักการบริหารความเสี่ยงและควบคุมภายในตามมาตรฐานสากล และเป็นไปตามหลักการ GRC (Governance Risk & Compliance)

## *รูปแบบประเมิน >>*

- **GRC Assessment Specific Area in PTT**
  การประเมินการควบคุมภายในแบบเฉพาะเจาะจง
- **GRC Assessment in PTT Group**
  การประเมินการดำเนินงานด้าน Governance, Risk และ Compliance ของบริษัทในกลุ่ม

## *แนวทางการประเมิน >>*

- วิเคราะห์และคัดเลือกกระบวนการ/บริษัท จากประเด็นความเสี่ยง ผลการตรวจสอบ และข้อคิดเห็นคณะกรรมการตรวจสอบ รวมถึงความเสี่ยงระดับองค์กร และทิศทางกลยุทธ์ ปตท. เป็นต้น
- รวบรวมข้อมูลเบื้องต้นเกี่ยวกับกระบวนการ /บริษัท ที่จะเข้าประเมินฯ เช่น ระเบียบ ข้อกำหนด คู่มือปฏิบัติงานที่เกี่ยวข้อง ข้อมูลการประเมินความเสี่ยงและการควบคุมภายในของกระบวนการในระบบ RCP Management Concerns ข้อมูลประเด็นตรวจสอบ และข้อคิดเห็นของคณะกรรมการตรวจสอบ เป็นต้น
- ประเมินความเสี่ยงและการควบคุมภายในของกระบวนการ ให้คำแนะนำและจัดทำแผนการปรับปรุงการควบคุมภายในร่วมกับเจ้าของกระบวนการ
- สรุปผลการประเมิน รวมทั้งแผนการปรับปรุงการควบคุมภายใน พร้อมรายงานให้คณะกรรมการที่เกี่ยวข้องทราบ
- ติดตามการดำเนินงานตามแผนการปรับปรุงการควบคุมภายใน

# 4

# การรายงานผล การควบคุมภายใน

# การรายงานผล การควบคุมภายใน

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

## I การรายงานผลภายใน ปตท.

***ภสญ.*** รายงานผลการควบคุมภายในต่อคณะกรรมการที่มีหน้าที่ในการบริหารความเสี่ยงและการควบคุมภายในต่อไปนี้

- รายงานความก้าวหน้าการดำเนินงาน เป็นประจำทุกไตรมาส
  - คณะกรรมการจัดการการกำกับดูแล การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร (GRCMC)
  - คณะกรรมการกำกับดูแลกิจการที่ดี (CGC)

- สรุปผลการดำเนินงานประจำปี และนำเสนอแผนการดำเนินงานปีถัดไป
  - คณะกรรมการจัดการการกำกับดูแล การบริหารความเสี่ยงและการควบคุมภายใน และการปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร (GRCMC)
  - คณะกรรมการจัดการของบริษัท ปตท. จำกัด (มหาชน) (PTTMC)
  - คณะกรรมการกำกับดูแลกิจการที่ดี (CGC)
  - คณะกรรมการตรวจสอบ (PTT AC)
  - คณะกรรมการ ปตท. (PTT BOD)

โดยนำข้อคิดเห็นและข้อเสนอแนะของคณะกรรมการที่ได้รับ มาพิจารณาทบทวน และปรับปรุงกระบวนการทำงานในปีถัดไป

***GRC Agent:*** *นอกจากต้องรายงานผลการประเมินการควบคุมภายในของสายงานต่อผู้บริหารสูงสุดของสายงาน ยังต้องรายงานผลต่อ คณะกรรมการ GRCMC ด้วย*

# II การรายงานผลภายนอก ปตท.

ปตท. ในฐานะรัฐวิสาหกิจสังกัดกระทรวงพลังงานและเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์ 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.

**คำถาม: แบ่งออกเป็น 5 องค์ประกอบ 17 หลักการ ตามมาตรฐาน COSO Control 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

เนื่องจากการควบคุมภายในไม่สามารถป้องกันการตัดสินใจที่ไม่ดี หรือไม่สามารถป้องกันเหตุการณ์ภายนอกที่ส่งผลกระทบทำให้องค์กรล้มเหลว ไม่สามารถบรรลุวัตถุประสงค์ เป้าหมายของการดำเนินงาน การควบคุมภายในจึงยังคงมีข้อจำกัด โดยข้อจำกัดอาจเกิดจาก

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

ข้อจำกัดเหล่านี้เป็นอุปสรรคต่อคณะกรรมการบริษัท และผู้บริหารในการได้มาซึ่งความเชื่อมั่นอย่างสมบูรณ์ในการบรรลุวัตุประสงค์ของกิจการ นั่นคือการควบคุมภายในให้ความเชื่อมั่นอย่างสมเหตุสมผล แต่ไม่ได้ให้ความเชื่อมั่นอย่างสมบูรณ์ เนื่องจากมีข้อจำกัดดังกล่าวข้างต้น

ดังนั้น ผู้บริหารควรตระหนักถึงข้อจำกัดเมื่อจะมีการเลือก การพัฒนาและการนำการควบคุมไปใช้ เพื่อลดข้อจำกัดให้อยู่ในขอบเขตที่สามารถปฏิบัติได้

# บทสรุป

การควบคุมภายในนั้นถือเป็นกระบวนการทำงานที่กำหนดขึ้นมาเพื่อให้ฝ่ายบริหารเกิดความมั่นใจอย่างสมเหตุสมผลว่าการดำเนินงานจะบรรลุวัตถุประสงค์อย่างมีประสิทธิผลและประสิทธิภาพ เพื่อให้เกิดความน่าเชื่อถือได้ของรายงานทางการเงิน และเพื่อให้เกิดความมั่นใจว่าจะปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

การบูรณาการระหว่างการบริหารความเสี่ยงกับการควบคุมภายในอย่างเป็นระบบที่ดี มีประสิทธิภาพ สามารถสร้างมูลค่าเพิ่ม (Value Enhancement) ให้กับองค์กร ช่วยให้หน่วยงานบรรลุวัตถุประสงค์ของการดำเนินงาน ตลอดจนสนับสนุนและปรับปรุงการดำเนินงานให้ดีขึ้น โดยเริ่มจากการระบุความเสี่ยงที่สำคัญให้ครอบคลุมกิจกรรมต่างๆของหน่วยงาน การกำหนดความเพียงพอของกิจกรรมการควบคุมภายใน การประเมินความเสี่ยงและประสิทธิภาพของการควบคุมภายใน รวมถึงการจัดทำแผนปรับปรุงการควบคุมภายในสำหรับรายการความเสี่ยงที่อยู่ในระดับ Extreme หรือกิจกรรมการควบคุมใดที่ยังมีจุดที่สามารถพัฒนาเพิ่มเติมได้ และการเชื่อมโยงข้อมูลระดับ Operation และ Corporate

นอกจากนี้ประเด็นสำคัญที่ต้องดำเนินการควบคู่กันไปคือการมุ่งเน้นเรื่องการสร้างความรู้ความเข้าใจ สร้างวัฒนธรรมองค์กรให้เห็นถึงความสำคัญของการบริหารความเสี่ยงและการควบคุมภายใน ว่าความเสี่ยงไม่ใช่จุดด้อย /จุดอ่อนขององค์กรแต่เป็นการสร้างความมั่นใจการดำเนินงานของหน่วยงานจะบรรลุตามเป้าหมายที่กำหนดไว้

# 6

# ภาคผนวก

# องค์ประกอบทั้ง 5 ของการควบคุมภายในตามหลักการ COSO Framework 2013

COSO คือ กรอบมาตรฐานเรื่องการควบคุมภายใน เพื่อช่วยให้ผู้ปฏิบัติงานบรรลุเป้าหมายและวัตถุประสงค์ ทั้งเรื่องของการปฏิบัติงานอย่างมีประสิทธิภาพและประสิทธิผล ความถูกต้องครบถ้วนของรายงาน และการปฏิบัติตามกฎหมาย กฎระเบียบ และข้อบังคับที่เกี่ยวข้อง

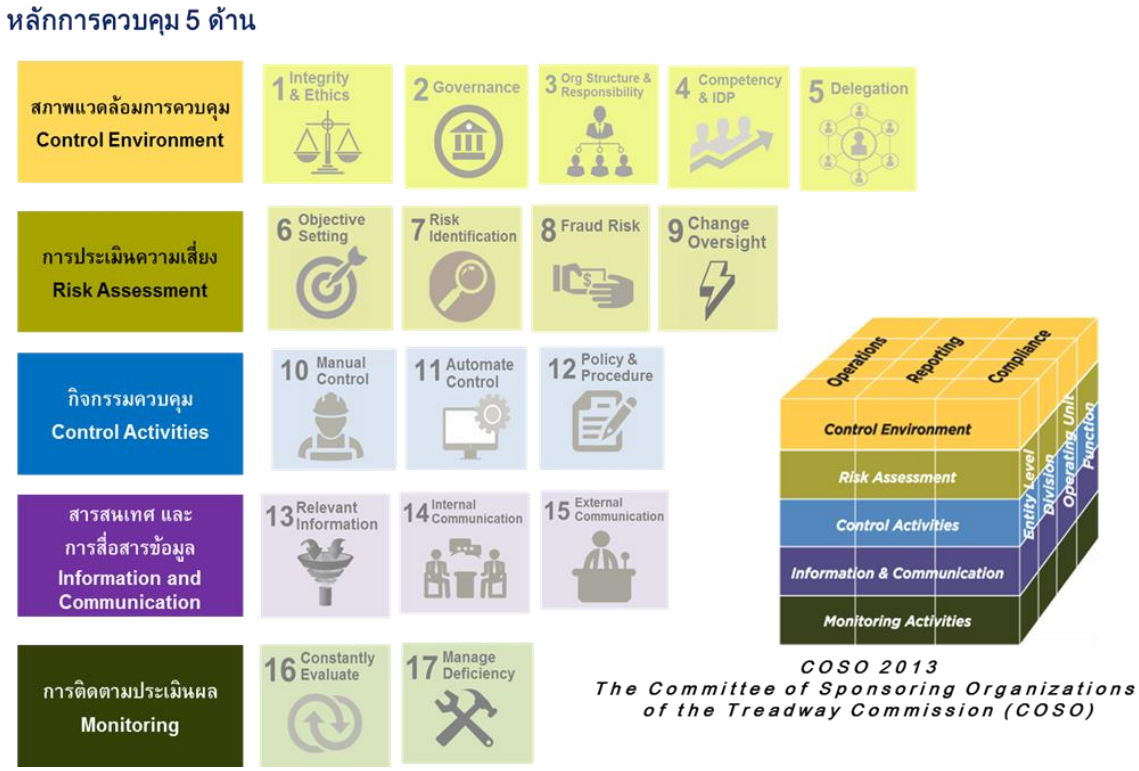
COSO ย่อมาจาก Committee of Sponsoring of the Treadway Commission เป็นคณะทำงานที่ก่อตั้งขึ้น โดยคณะกรรมาธิการของประเทศสหรัฐอเมริกา ที่ชื่อว่า Treadway Commission ซึ่งตั้งขึ้นในปี 1985 โดยจัดตั้งขึ้นเพื่อศึกษาและพัฒนาแนวทางการบริหารความเสี่ยง รูปแบบการควบคุมภายในที่มีประสิทธิผล และป้องกันการทุจริตของรายงานทางการเงิน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

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 องค์ประกอบหลักเดิม แต่เพิ่มเติม 17 หลักการย่อย เพื่อทำให้ระบบการควบคุมภายในมีความเข้มแข็งและชัดเจนยิ่งขึ้น



# องค์ประกอบของการควบคุมภายใน

## 1. สภาพแวดล้อมการควบคุม (CONTROL ENVIRONMENT)

หมายถึง ปัจจัยต่าง ๆ ที่ส่งผลต่อทัศนคติและความตระหนักถึงความจำเป็นและความสำคัญของการควบคุมภายในของบุคลากรทุกคนในองค์กร โดยบุคลากรทุกคนเข้าใจถึงความรับผิดชอบและขอบเขตอำนาจหน้าที่ของตนเอง มีความรู้ความสามารถ และทักษะที่จำเป็นต่อการปฏิบัติงาน รวมถึงการยอมรับและปฏิบัติตามกฎเกณฑ์และวิธีการทำงานต่าง ๆ ที่องค์กรกำหนดไว้ ซึ่งถือได้ว่าสภาพแวดล้อมของการควบคุมมีผลกระทบอย่างมากกับกระบวนการปฏิบัติงานทั้งหมดที่เกิดขึ้นในองค์กร จึงเป็นรากฐานที่สำคัญขององค์ประกอบอื่น ๆ ของการควบคุมภายใน เพื่อสร้างระเบียบวินัยด้านการควบคุมภายในให้แก่ทุกคนในองค์กร

ปัจจัยที่ช่วยเสริมสร้างให้มีสภาพแวดล้อมของการควบคุมที่ดี ได้แก่

- ความซื่อสัตย์และจริยธรรม ซึ่งอาจพิจารณาได้จากการกำหนดแนวทางปฏิบัติในเรื่องต่างๆ ให้ชัดเจน แล้วแจ้งให้ทุกคนที่เกี่ยวข้องทราบ รวมไปถึงการกระทำตนเป็นแบบอย่างให้กับผู้ใต้บังคับบัญชา ทั้งคำพูดและการกระทำ
- รูปแบบและปรัชญาการทำงานของฝ่ายบริหาร โดยพิจารณาจากความรู้ความสามารถ และประสบการณ์ของฝ่ายบริหารที่เป็นประโยชน์ต่อหน้าที่ที่รับผิดชอบ และความสนใจในองค์กรที่ตนเป็นผู้บริหาร
- การจัดโครงสร้างองค์กรและสายการบังคับบัญชาให้เหมาะสมกับขนาดและลักษณะการดำเนินงาน
- การกำหนดลักษณะงานและคุณสมบัติเฉพาะตำแหน่ง (Job Description & Job Specification) สำหรับทุกตำแหน่งงาน อย่างชัดเจน

**<u>หลักการย่อยขององค์ประกอบที่ 1 สภาพแวดล้อมการควบคุม</u>** ได้แก่

**หลักการที่ 1** องค์กรแสดงให้เห็นถึงความยึดมั่นในคุณค่าของความซื่อตรงและจริยธรรม

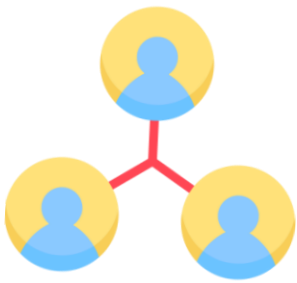
**หลักการที่ 2** คณะกรรมการบริษัทแสดงให้เห็นถึงความเป็นอิสระจากผู้บริหารและทำหน้าที่สอดส่องดูแลการพัฒนาและการดำเนินงานด้านการควบคุมภายใน

**หลักการที่ 3** ผู้บริหารจัดให้มีโครงสร้าง สายการรายงาน รวมทั้งการกำหนดอำนาจหน้าที่และความรับผิดชอบที่เหมาะสมเพื่อให้องค์กรบรรลุวัตถุประสงค์ ภายใต้การสอดส่องดูแลของคณะกรรมการบริษัท

**หลักการที่ 4** องค์กรจะแสดงให้เห็นถึงความมุ่งมั่นในการจูงใจ พัฒนาและรักษาบุคคลากรที่มีความรู้ความสามารถที่สอดคล้องกับวัตถุประสงค์ขององค์กร

**หลักการที่ 5** องค์กรกำหนดให้บุคลากรที่มีหน้าที่ความรับผิดชอบต่อผลการปฏิบัติงานตามหน้าที่การควบคุมภายในเพื่อให้องค์กรบรรลุวัตถุประสงค์

*ในการดำเนินการเกี่ยวกับสภาพแวดล้อมการควบคุม ผู้กำกับคณะกรรมการบริษัท จะต้องมีความอิสระในการสอดส่องดูแลการพัฒนาและการดำเนินงานด้านการควบคุมภายในและ ฝ่ายบริหารและบุคคลากรของหน่วยงานต้องสร้างบรรยากาศในการดำเนินงานที่ส่งเสริมและให้ความสำคัญกับการควบคุมภายใน เพื่อให้ทุกคนในองค์กรมีความเข้าใจและทัศนคติที่ดีต่อการควบคุมภายใน*



## 2. การประเมินความเสี่ยง (RISK ASSESSMENT)

หมายถึง กระบวนการที่ใช้ในการระบุและการวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยงาน รวมทั้งการกำหนดการควบคุมที่เหมาะสมที่ใช้ในการควบคุมความเสี่ยง

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 ฝ่ายบริหารต้องประเมินความเสี่ยงทั้งจากปัจจัยภายในและปัจจัยภายนอกที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยงาน*

## 3. กิจกรรมการควบคุม (CONTROL ACTIVITIES)

กิจกรรมการควบคุมเป็นองค์ประกอบที่จะช่วยให้มั่นใจได้ว่า นโยบายและกระบวนการเกี่ยวกับการควบคุมภายในที่กำหนดขึ้นนั้น ได้มีการนำไปปฏิบัติภายในองค์กรอย่างทั่วถึง นอกจากนี้ กิจกรรมการควบคุมยังช่วยสร้างความมั่นใจว่าหน่วยงาน/องค์กรมีกิจกรรมที่เหมาะสมในการป้องกันหรือลดความเสี่ยงที่อาจเกิดขึ้น ดังนั้น กิจกรรมการควบคุมควรกำหนดให้สอดคล้องกับความเสี่ยงที่ประเมินได้ โดยมีข้อควรพิจารณาในการกำหนดกิจกรรมการควบคุม ดังต่อไปนี้

- กิจกรรมการควบคุมควรเป็นส่วนหนึ่งของกระบวนการปฏิบัติงานตามปกติ
- กิจกรรมการควบคุมต้องสามารถป้องกันหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- ค่าใช้จ่ายในการกำหนดให้กิจกรรมการควบคุมต้องไม่สูงกว่าผลเสียหายที่คาดว่าจะเกิดขึ้น

หากไม่กำหนดให้มีกิจกรรมการควบคุมปัญหาที่เกิดขึ้นกับองค์กรส่วนใหญ่ คือ การกำหนดกิจกรรมการควบคุมตามที่มีการปฏิบัติอยู่เดิม โดยมิได้พิจารณาความมีประสิทธิภาพ และความสอดคล้องกับวัตถุประสงค์ ของการดำเนินงาน และความเสี่ยงที่เปลี่ยนไปขององค์กร

**หลักการย่อยขององค์ประกอบที่ 3 กิจกรรมการควบคุม** ได้แก่

**หลักการที่ 10** องค์กรเลือกและพัฒนากิจกรรมการควบคุมที่ลดความเสี่ยงในการบรรลุวัตถุประสงค์ให้อยู่ในระดับที่ยอดรับได้

**หลักการที่ 11** องค์กรเลือกและพัฒนากิจกรรมควบคุมทั่วไปด้านเทคโนโลยีเพื่อสนับสนุนการบรรลุวัตถุประสงค์

**หลักการที่ 12** องค์กรจัดให้มีกิจกรรมควบคุมผ่านทางนโยบายซึ่งได้กำหนดสิ่งที่คาดหวังและวิธีการปฏิบัติเพื่อนำนโยบายไปสู่การปฏิบัติ

*ในการดำเนินการเกี่ยวกับกิจกรรมควบคุมนั้น ฝ่ายบริหารรวมทั้งพนักงานทุกคนต้องจัดให้มีกิจกรรมควบคุมที่ประสิทธิภาพและประสิทธิผล เพื่อป้องกันหรือลดความเสียหาย ความผิดพลาดที่อาจเกิดขึ้น และให้สามารถบรรลุผลตามวัตถุประสงค์ของการควบคุมภายใน ตัวอย่างของกิจกรรมควบคุม เช่น*

- *การกำหนดวิสัยทัศน์ กลยุทธ์ และทิศทางในภาพรวมขององค์กร*
- *การกำหนดแผนงาน เป้าหมายและงบประมาณของหน่วยงาน*
- *การกำหนดนโยบาย*
- *การกำหนดขั้นตอนและวิธีการปฏิบัติงาน*
- *การอนุมัติ*
- *การแบ่งแยกหน้าที่*
- *การสอบทาน*
- *การวิเคราะห์*
- *การสื่อสาร*
- *การประชุม*
- *การกระทบยอด*
- *การควบคุมโดยระบบ IT*
- *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

**หลักการย่อยขององค์ประกอบที่ 4 สารสนเทศและการสื่อสาร** ได้แก่

**หลักการที่ 13** องค์กรได้รับหรือสร้างและใช้สารสนเทศที่เกี่ยวข้องและมีคุณภาพ เพื่อสนับสนุนให้การควบคุมภายในทำหน้าที่ได้

**หลักการที่ 14** องค์กรมีการสื่อสารภายในเกี่ยวกับสารสนเทศ รวมถึงวัตถุประสงค์และความรับผิดชอบต่อการควบคุมภายในที่จำเป็นเพื่อให้การควบคุมภายในทำหน้าที่ได้

**หลักการที่ 15** องค์กรมีการสื่อสารกับบุคคลภายนอกเกี่ยวกับประเด็นที่มีผลกระทบต่อการทำหน้าที่ของการควบคุมภายใน

*ในการดำเนินการเกี่ยวกับสารสนเทศและการสื่อสาร ฝ่ายบริหารต้องจัดให้มีสารสนเทศอย่างเพียงพอ และมีการสื่อสารให้ฝ่ายบริหารและบุคลากรอื่นๆ อย่างเหมาะสมทั้งภายในและภายนอกองค์กร รวมทั้งต้องพิจารณาถึงความถูกต้อง ครบถ้วน เหมาะสมและทันเวลาของข้อมูล*

## 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

การประเมินการควบคุมภายใน สามารถทำได้โดยการสร้างความรับผิดชอบในการควบคุมภายในให้แก่ทุกคนที่เป็นเจ้าของงานนั้น ซึ่งจะช่วยให้ผู้บริหารสามารถบริหารงานได้อย่างมีประสิทธิภาพและพนักงานสามารถปฏิบัติและปรับปรุงการควบคุมภายในได้อย่างมีประสิทธิผล เพราะทุกคนในหน่วยงานเป็นเจ้าของกระบวนการและมีความเข้าใจดีที่สุด สามารถประเมินการดำเนินงานรวมถึงการปฏิบัติตามระบบการควบคุมภายในที่ออกแบบไว้สม่ำเสมอในงานที่ตนต้องรับผิดชอบให้สามารถบรรลุวัตถุประสงค์ได้ ซึ่งการปฏิบัติแบบนี้เรียกว่า การประเมินการควบคุมด้วยตนเอง (Control Self-Assessment)

**หลักการย่อยขององค์ประกอบที่ 5 การติดตามประเมินผล** ได้แก่

**หลักการที่ 16** องค์กรเลือก พัฒนา และดำเนินการประเมินผลอย่างต่อเนื่องและ/หรือ ประเมินผลแยกต่างหาก เพื่อให้มั่นใจว่าองค์ประกอบของการควบคุมภายในมีปรากฏและทำหน้าที่อยู่

**หลักการที่ 17** องค์กรประเมินผลและสื่อสารข้อบกพร่องของการควบคุมภายในอย่างทันเวลาต่อบุคคลที่รับผิดชอบในการดำเนินการแก้ไข รวมถึงผู้บริหารระดับสูงและคณะกรรมการบริษัทตามความเหมาะสม

*ในการดำเนินการเกี่ยวกับการติดตามประเมินผล ฝ่ายบริหารต้องจัดให้มีการติดตามประเมินผล โดยการติดตามผลในระหว่างการปฏิบัติงาน และการประเมินผลเป็นรายครั้งอย่างต่อเนื่องและสม่ำเสมอ เพื่อให้มั่นใจว่า*

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

# การควบคุมภายในตามหลักเกณฑ์กระทรวงการคลัง



รัฐวิสาหกิจ มีหน้าที่จัดวางระบบการควบคุมภายใน และประเมินผลการควบคุมภายในตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ.2561 ดังนี้

- กำกับดูแลให้มีการวางและประเมินผลการควบคุมภายในตามมาตรฐานการควบคุมภายใน (COSO Control Framework)
- จัดวางระบบการควบคุมภายในให้แล้วเสร็จภายใน 1 ปี กรณีรัฐวิสาหกิจตั้งใหม่/ปรับปรุงโครงสร้างองค์กร
- จัดให้มีคณะกรรมการ ทำหน้าที่ดูแลการประเมินผลการควบคุมภายใน
- จัดให้มีการประเมินผลการควบคุมภายใน อย่างน้อยปีละ 1 ครั้ง
- จัดทำรายงานการจัดวางระบบการควบคุมภายใน และส่งให้ผู้กำกับดูแลภายใน 60 วัน นับแต่วันที่จัดวางฯ แล้วเสร็จ
- จัดทำรายงานการประเมินผลการควบคุมภายใน และส่งให้ผู้กำกับดูแลภายใน 90 วัน นับแต่วันสิ้นปีปฏิทิน

# 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 ด้านการรายงานที่เกี่ยวกับการเงินและไม่ใช่การเงินที่เชื่อถือได้ ทันเวลา และโปร่งใส รวมทั้งด้านการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้องกับการดำเนินงาน

จากผลการประเมินดังกล่าว .....ชื่อรัฐวิสาหกิจ....เห็นว่า การควบคุมภายในของหน่วยงานมีความเพียงพอ ปฏิบัติตามอย่างต่อเนื่อง 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.....

# แนวทางการกรอกข้อมูล

## รายงานการประเมินองค์ประกอบของการควบคุมภายใน (ปค.4)

**แบบ ปค. ๔**

..... ชื่อรัฐวิสาหกิจ.....

**รายงานการประเมินองค์ประกอบของการควบคุมภายใน**

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

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

ผลการประเมินโดยรวม

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

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

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

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

# แนวทางการกรอกข้อมูล

## รายงานการประเมินผลการควบคุมภายใน (ปค.5)

**แบบ ปค. ๕**

..... ชื่อรัฐวิสาหกิจ.....

**รายงานการประเมินผลควบคุมภายใน**

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

| ภารกิจตามกฎหมายที่จัดตั้งหน่วยงานของรัฐ หรือภารกิจตามแผนการดำเนินการหรือภารกิจอื่นๆ ที่สำคัญของหน่วยงานของรัฐ/วัตถุประสงค์ | ความเสี่ยง | การควบคุมภายในที่มีอยู่ | การประเมินผลการควบคุมภายใน | ความเสี่ยงที่ยังมีอยู่ | การปรับปรุงการควบคุมภายใน | หน่วยงานที่รับผิดชอบ/กำหนดเสร็จ |
|---|---|---|---|---|---|---|
| • ภารกิจตามกฎหมายที่จัดตั้งหน่วยงานของรัฐ หรือภารกิจตามแผนการดำเนินงานหรือภารกิจอื่นๆ ที่สำคัญของหน่วยงานของรัฐ<br>• วัตถุประสงค์ของภารกิจดังกล่าว | ความเสี่ยงสำคัญของแต่ละภารกิจ | การควบคุมภายในของแต่ละภารกิจเพื่อลด หรือควบคุมความเสี่ยง | ผลการประเมินผลการควบคุมภายในว่าเพียงพอและปฏิบัติตามอย่างต่อเนื่องหรือไม่ | ความเสี่ยงที่ยังมีอยู่ของแต่ละภารกิจ | การปรับปรุงการควบคุมภายในในปีปฏิทินถัดไป | • หน่วยงานที่รับผิดชอบ<br>• กำหนดเสร็จ (ว/ด/ป) |

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

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

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

# แนวทางการกรอกข้อมูล

## รายงานการสอบทานการประเมินผลการควบคุมภายในของผู้ตรวจสอบภายใน (ปค.6)

**แบบ ปค. ๖**

**รายงานการสอบทานการประเมินผลการควบคุมภายในของผู้ตรวจสอบภายใน**

เรียน ..... หัวหน้ารัฐวิสาหกิจ.....

ผู้ตรวจสอบภายในของ .....ชื่อรัฐวิสาหกิจ.... ได้สอบทานการประเมินผลการควบคุมภายในของหน่วยงาน สำหรับปีสิ้นสุดวันที่ ...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 โดยความเห็นของคณะกรรมฯ ประกอบด้วย

- ความเพียงพอและความเหมาะสมของระบบการควบคุมภายในของบริษัท และการจัดให้มีบุคลากรอย่างเพียงพอที่จะดำเนินการดังกล่าวได้อย่างมีประสิทธิภาพ รวมทั้งการติดตามควบคุมดูแลการดำเนินงานของบริษัทย่อยว่า สามารถป้องกันทรัพย์สินของบริษัทและบริษัทย่อยจากการที่กรรมการหรือผู้บริหารนำไปใช้โดยมิชอบหรือโดยไม่มีอำนาจหรือไม่

- ข้อบกพร่องเกี่ยวกับระบบการควบคุมภายในที่ผ่านมาของบริษัทมีเรื่องใดบ้าง ถ้ามีบริษัทได้แก้ไขข้อบกพร่องดังกล่าวเสร็จสิ้นแล้วหรือไม่ เพราะเหตุใด

# แนวทางการกรอกข้อมูล

## 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<br>1.1.1 การปฏิบัติหน้าที่ประจำวัน และการตัดสินใจในเรื่องต่าง ๆ<br>1.1.2 การปฏิบัติต่อคู่ค้า ลูกค้า และบุคคลภายนอก | ✓ | | |
| 1.2 มีข้อกำหนดที่เป็นลายลักษณ์อักษรให้ผู้บริหารและพนักงานปฏิบัติหน้าที่ด้วยความซื่อตรงและรักษาจรรยาบรรณ ที่ครอบคลุมถึง<br>1.2.1 มีข้อกำหนดเกี่ยวกับจริยธรรม (code of conduct) สำหรับผู้บริหารและพนักงาน ที่เหมาะสม<br>1.2.2 มีข้อกำหนดห้ามผู้บริหารและพนักงานปฏิบัติตนในลักษณะที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์กับกิจการ ซึ่งรวมถึงการห้ามคอร์รัปชันอันทำให้เกิดความเสียหายต่อองค์กร<br>1.2.3 มีบทลงโทษที่เหมาะสมหากมีการฝ่าฝืนข้อกำหนดข้างต้น<br>1.2.4 มีการสื่อสารข้อกำหนดและบทลงโทษข้างต้นให้ผู้บริหารและพนักงาน<br>ทุกคนรับทราบ เช่น รวมอยู่ในการปฐมนิเทศพนักงานใหม่ ให้พนักงานลงนามรับทราบข้อกำหนดและบทลงโทษเป็นประจำทุกปี รวมทั้งมีการเผยแพร่ code of conduct ให้แก่พนักงานและบุคคลภายนอกได้รับทราบ | ✓ | | |
| 1.3 มีกระบวนการติดตามและประเมินผลการปฏิบัติตาม Code of Conduct<br>1.3.1 การติดตามและประเมินผลโดยหน่วยงานตรวจสอบภายในหรือหน่วยงานกำกับดูแลการปฏิบัติ (compliance unit)<br>1.3.2 การประเมินตนเองโดยผู้บริหารและพนักงาน<br>1.3.3 การประเมินโดยผู้เชี่ยวชาญที่เป็นอิสระจากภายนอกองค์กร | ✓ | | |

# เกณฑ์การประเมิน GRC Assessment



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 แต่ยังยังมีจุดที่ควรปรับปรุงเพื่อเพิ่มประสิทธิภาพ ลดความซ้ำซ้อน หรือทำให้การทำงานรวดเร็วขึ้น | · มีการปฏิบัติตามการควบคุมที่ออกแบบไว้แต่ไม่ได้ปฏิบัติอย่างสม่ำเสมอ < 90% |
| ระดับ 2 | · การควบคุมยังไม่เหมาะสม เพียงพอ ไม่สามารถทำให้มั่นใจว่าการดำเนินงานสามารถบรรลุวัตถุประสงค์ขององค์กร หรือยังอาจก่อให้เกิดความเสียหายจากความเสี่ยง | · มีการปฏิบัติตามการควบคุมที่ออกแบบไว้ < 50% |
| ระดับ 1 | · ไม่มีการออกแบบการควบคุม / ไม่ได้กำหนดแนวทางปฏิบัติที่ชัดเจน | · ไม่ปฏิบัติตามการควบคุมที่ออกแบบไว้ |

## กรณี Auditor พบประเด็น Non-Compliance ในช่วง 1 ปีที่ผ่านมา

ภาคผนวก 5

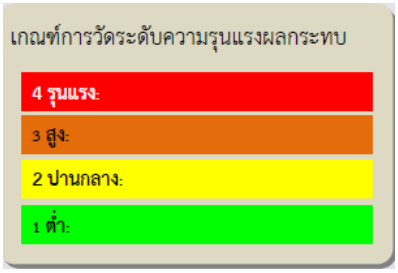
# เกณฑ์การประเมินความเสี่ยงระดับปฏิบัติการ

การประเมินความเสี่ยง คือ การวัดระดับความรุนแรงของความเสี่ยงว่ามีระดับความรุนแรงมากน้อยเพียงใด เพื่อพิจารณาจัดลำดับความสำคัญ และจัดการความเสี่ยงให้มีระดับความรุนแรงอยู่ในระดับที่ยอมรับได้ (Risk Appetite)

โดยการประเมินความเสี่ยง นอกเหนือจากการประเมินความเสี่ยงตามหลักเกณฑ์การวัดระดับความรุนแรงขององค์กรแล้ว กลุ่มธุรกิจ/สายงานสนับสนุน และหน่วยปฏิบัติงาน สามารถกำหนดเกณฑ์การวัดระดับความรุนแรงของความเสี่ยงที่แตกต่างกันของแต่ละหน่วยปฏิบัติงานได้ ตามวัตถุประสงค์ในการปฏิบัติงาน

## หลักเกณฑ์กำหนดเกณฑ์การวัดระดับความรุนแรง

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



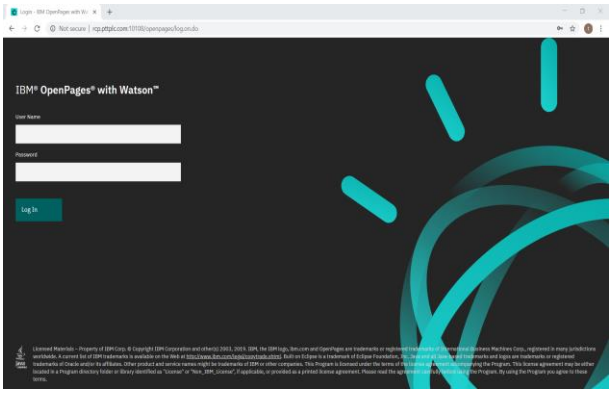

- **เกณฑ์การวัดระดับความรุนแรงของโอกาสเกิดความเสี่ยง (Likelihood)** สามารถวัดได้ตามรูปแบบ ดังนี้
  - เชิงปริมาณ สำหรับความเสี่ยงที่มีข้อมูลตัวเลขมาใช้ในการวิเคราะห์
  - เชิงคุณภาพ สำหรับความเสี่ยงที่ไม่สามารถระบุเป็นตัวเลขที่ชัดเจนได้

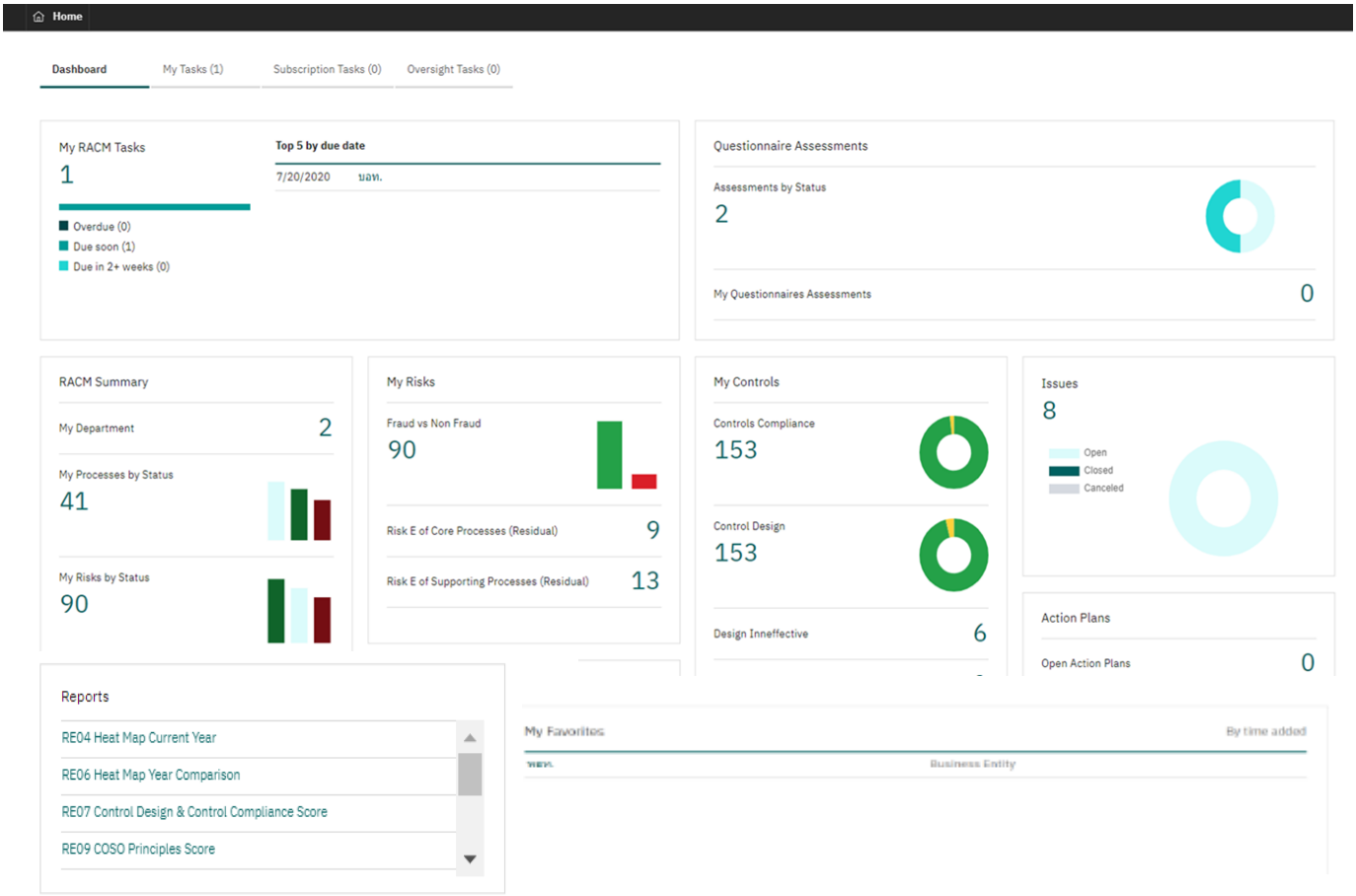
ทั้งนี้ หลักเกณฑ์กำหนดเกณฑ์การวัดระดับความรุนแรง ของกลุ่มธุรกิจ/สายงานสนับสนุน และหน่วยปฏิบัติงาน ได้ถูกระบุไว้ในคู่มือการบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management Manual) และมีการทบทวนอย่างสม่ำเสมอ

# ภาพรวมระบบ Risk and Control Platform (RCP)



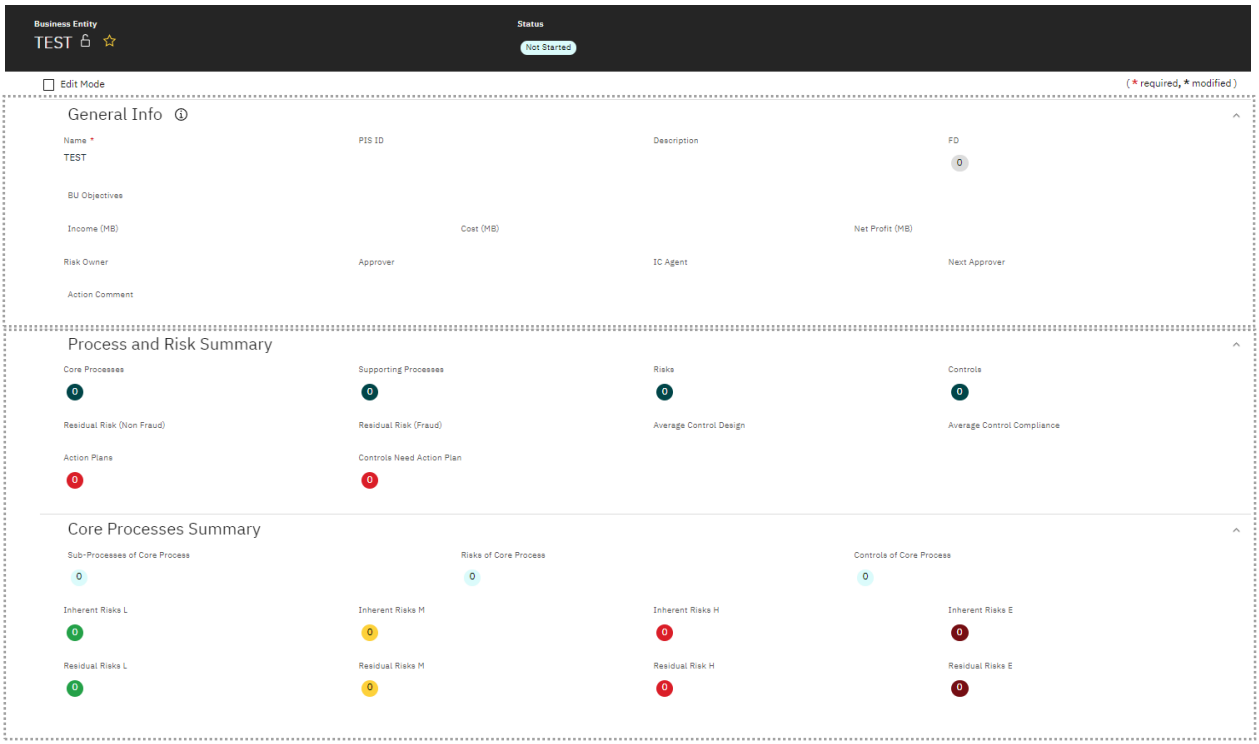
การประเมินความเสี่ยงและการควบคุมภายใน (GRC Assessment) ของ ปตท. ดำเนินการผ่านระบบ Risk and Control Platform (RCP) ตั้งแต่การระบุและกำหนดวัตถุประสงค์ของกระบวนการ การระบุ วิเคราะห์และวัดระดับความเสี่ยง การทบทวนและกำหนดกิจกรรมการควบคุม รวมถึงการกำหนดแผนการปรับปรุงการควบคุม (Action Plan) อีกด้วย



# ส่วนประกอบของระบบ RCP

- **General Info and Summary**



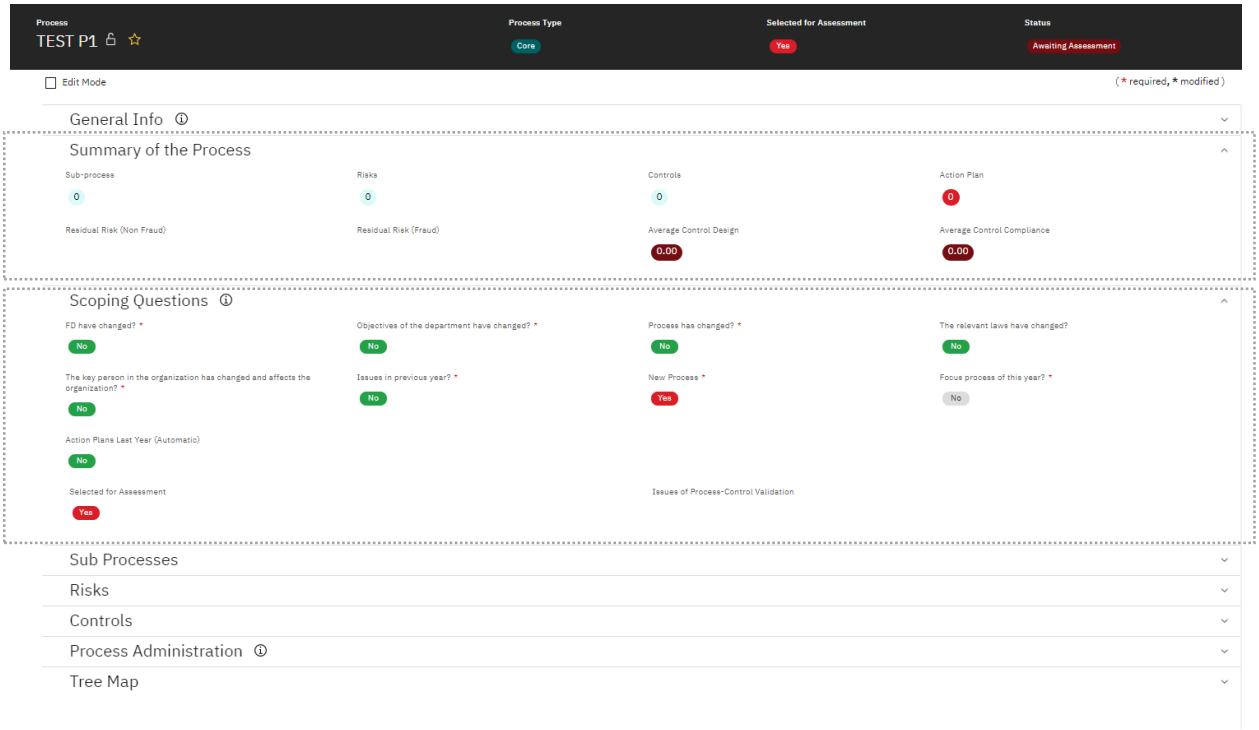

***General Info :***

หน้าจอแสดงข้อมูลทั่วไปของกระบวนการทำงานหลัก (Process) สำหรับระบุชื่อกระบวนการทำงานหลัก และรายละเอียดของกระบวนการทำงานที่นำมาใช้ในการประเมินความเสี่ยงในระดับปฏิบัติการ

***Process and Risk Summary :***

หน้าจอสรุปข้อมูลกระบวนการและความเสี่ยงที่บันทึกข้อมูลไว้ สำหรับใช้ตรวจสอบความถูกต้องในภาพรวม

- **Summary of the Process**




***Summary of the Process :***

การสรุปรายละเอียดของกระบวนการที่บันทึกไว้ในระบบ RCP ได้แก่

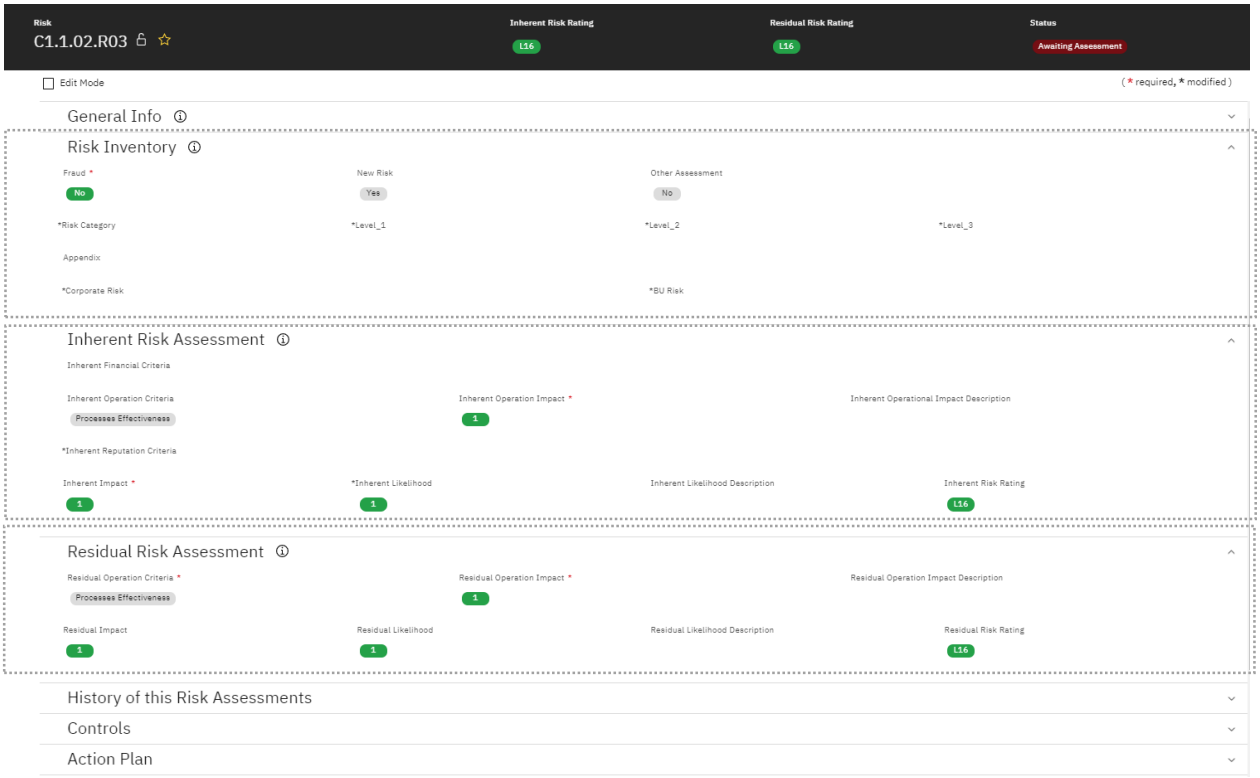
- จำนวนกระบวนการทำงานย่อย (Sub-process)
- จำนวนความเสี่ยง (Risk)
- จำนวนการควบคุม (Control)
- จำนวนแผนการปรับปรุงการควบคุม (Action plan)
- คะแนนเฉลี่ยการออกแบบการควบคุม (Average Control Design) และคะแนนเฉลี่ยการปฏิบัติตามการควบคุมที่ได้ออกแบบไว้ (Average Control Compliance)

***Scoping Questions :***

การระบุการเปลี่ยนแปลงต่าง ๆ ในกระบวนการเปรียบเทียบกับปีก่อนหน้า โดยการตอบคำถามต่าง ๆ เช่น

- มีการเปลี่ยนแปลงวัตถุประสงค์ของหน่วยงานหรือไม่
- มีการเปลี่ยนแปลงกระบวนการทำงานหรือไม่
- มีกระบวนการทำงานใหม่เกิดขึ้นหรือไม่

- **Risk Assessment**




***Risk inventory :***

การระบุประเภทความเสี่ยง ได้แก่

- ความเสี่ยงด้านการทุจริต
- ประเภทของความเสี่ยง (Risk category) และ level ย่อย

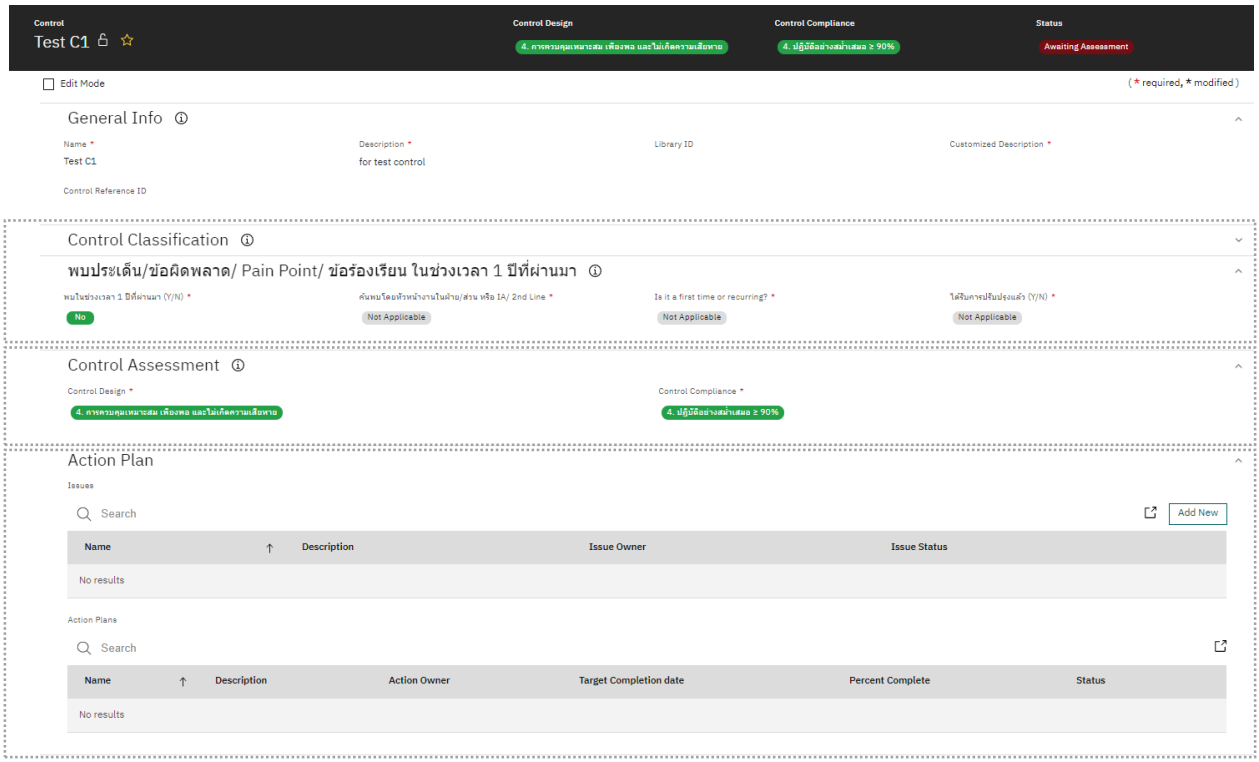
***Inherent Risk Assessment:***

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

***Residual Risk Assessment:***

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

- **Control assessment**




***Control Classification :***

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

***Control Assessment :***

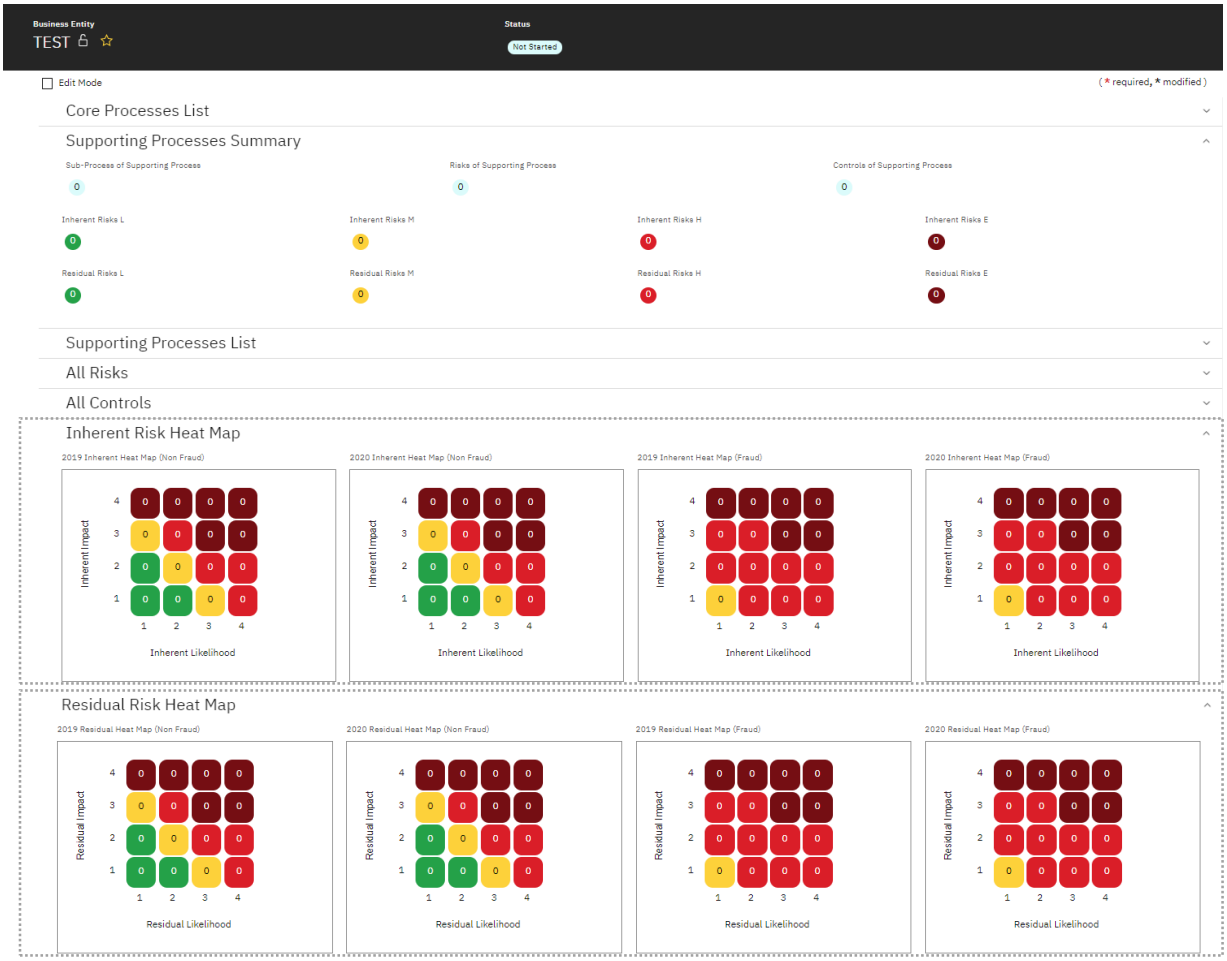
การประเมินความเพียงพอของการออกแบบการควบคุมภายในและการปฏิบัติตามภายควบคุม (Control Design & Compliance)

***Action Plan :***

การระบุแผนการปรับปรุงการควบคุม (Action plan) เพิ่มเติมในกรณีที่การควบคุมภายในยังไม่มีประสิทธิภาพ ประสิทธิผลเพียงพอ

ข้อมูลที่ต้องระบุ เช่น รายละเอียดของแผนการปรับปรุงการควบคุม ผู้รับผิดชอบ วันที่คาดว่าจะแล้วเสร็จ สถานะความคืบหน้าของแผน เป็นต้น

- **Functional Heat Map**



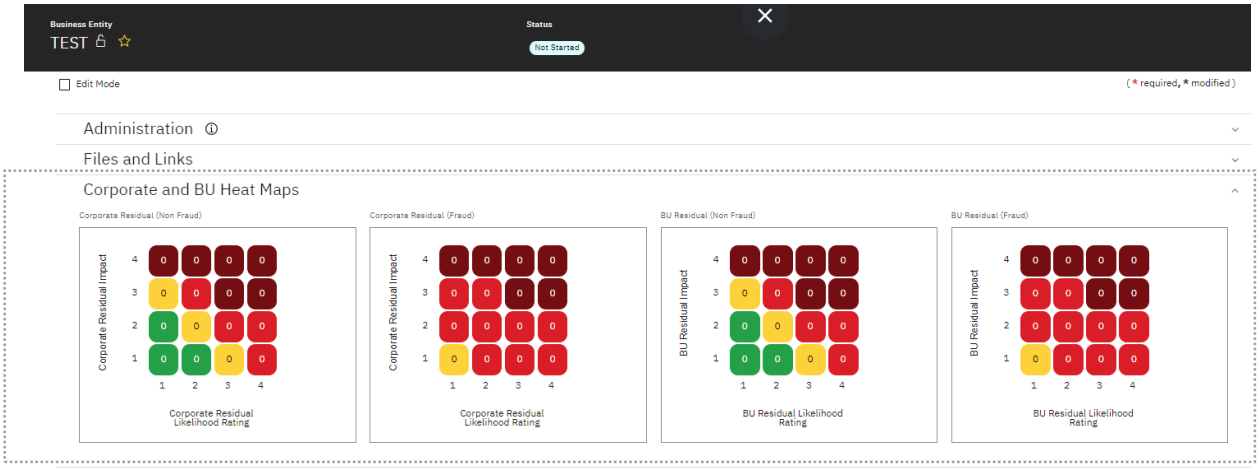

***Inherent Risk Heat Map :***

สรุปค่าระดับความรุนแรงของความเสี่ยงสืบเนื่อง หรือความเสี่ยงก่อนการดำเนินกิจกรรมการควบคุม (Inherent Risk) ที่ได้จากการประเมินผลกระทบและโอกาสเกิดของปัจจัยเสี่ยง โดยแสดงความเสี่ยงด้านการทุจริตและคอร์รัปชัน (Fraud) และไม่ใช่ด้านการทุจริตและคอร์รัปชัน (Non Fraud) ออกจากกันตามเกณฑ์การจัดกลุ่มความเสี่ยง

***Residual Risk Heat Map : :***

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

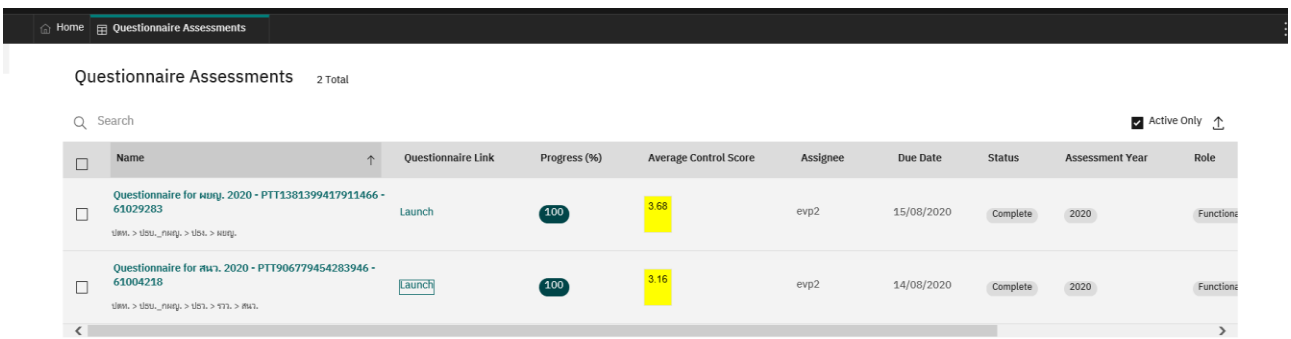
- ## Corporate and BU Heat Maps




***Corporate and BU Heat Map :***

สรุปค่าระดับความรุนแรงของความเสี่ยงคงเหลือ หรือความเสี่ยงที่เหลือภายหลังการดำเนินกิจกรรมการควบคุม (Residual Risk) ที่ได้จากการประเมินผลกระทบและโอกาสเกิดของปัจจัยเสี่ยง ตามเกณฑ์การวัดระดับความรุนแรงของความเสี่ยงระดับสายงาน (BU) และเกณฑ์การวัดระดับความรุนแรงของความเสี่ยงระดับองค์กร (Corporate) โดยแสดงความเสี่ยงด้านการทุจริตและคอร์รัป-ชัน (Fraud) และไม่ใช่ด้านการทุจริตและคอร์รัปชัน (Non Fraud) ออกจากกันตามเกณฑ์การจัดกลุ่มความเสี่ยง

- ## Questionnaire Assessment



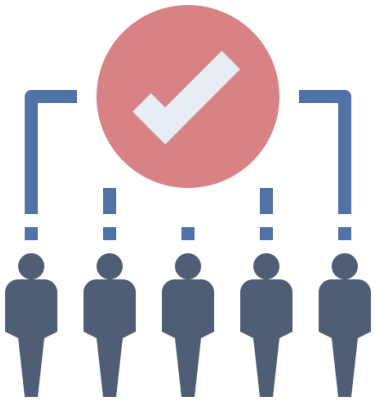

หน้าจอแสดงจำนวนแบบสอบถามทั้งหมดที่ต้องดำเนินการประเมิน โดยแต่ละแบบสอบถามมีการแสดงข้อมูลสรุปจากการประเมิน ดังนี้

- เปอร์เซ็นต์การตอบคำถามจากจำนวนข้อทั้งหมด
- คะแนนเฉลี่ยการควบคุม
- ผู้รับผิดชอบในการตอบแบบสอบถาม
- วันที่ครบกำหนดดำเนินการ
- สถานะ: In Progress หรือ Complete
- ปีที่กำหนดสำหรับแบบสอบถาม
- ประเภทของแบบสอบถาม : Functional, Board, Committee หรือ Secondment

# นิยาม คำจำกัดความ

**บริษัทและคณะกรรมการ :**

| | |
|---|---|
| **ปตท.** | บริษัท ปตท. จำกัด (มหาชน) |
| **บริษัทในกลุ่ม ปตท.** | บริษัทหรือนิติบุคคลใด ๆ ที่ ปตท. ถือหุ้นไม่ว่าจะโดยตรงหรือโดยอ้อม และไม่ว่าจำนวนเท่าใดของทุนจดทะเบียน |
| **BOD** | คณะกรรมการบริษัท ปตท. จำกัด (มหาชน) |
| **Audit Committee** | คณะกรรมการตรวจสอบ |
| **CGC** | คณะกรรมการกำกับดูแลกิจการที่ดีของบริษัท ปตท. จำกัด (มหาชน) |
| **PTTMC** | คณะกรรมการจัดการของ ปตท. |
| **GRCMC** | คณะกรรมการการกำกับดูแล การบริหารความเสี่ยง และการกำกับการปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร |



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

# 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)
- 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

- คำสั่งแต่งตั้งคณะกรรมการบริษัท ปตท. จำกัด (มหาชน)
- คำสั่งแต่งตั้งคณะกรรมการตรวจสอบ
- คำสั่งแต่งตั้งคณะกรรมการกำกับดูแลกิจการที่ดีของ บริษัท ปตท. จำกัด (มหาชน)
- คำสั่งแต่งตั้งคณะกรรมการการกำกับดูแล การบริหารความเสี่ยง และการกำกับการปฏิบัติตามกฎหมาย กฎ ระเบียบองค์กร

ฝ่ายควบคุมภายในและจัดการความเสี่ยง

บริษัท ปตท. จำกัด (มหาชน)

โทร 02-537-2000 ต่อ 12948

# ขั้นตอนการประเมินความเสี่ยงตาม GRC Assessment

**ขั้นตอนที่ 1: เตรียมความพร้อม (Preparation)**
- ทบทวน BU Risk Criteria
- สรุปรายการจุดมุ่งเน้น (FCY)
- เชื่อมโยงความเสี่ยง CRP และกิจกรรมควบคุมระดับกระบวนการ

ระยะเวลา 60 วัน

**ขั้นตอนที่ 2: สื่อความบทบาทหน้าที่และแผนการดำเนินงานประจำปีด้าน GRC แก่ GRC Agent**

ระยะเวลา 1 วัน

**ขั้นตอนที่ 3: เตรียมความพร้อมและนำข้อมูลเข้าสู่ระบบ**
- ทบทวนคำถามของแบบประเมิน E-CSA
- นำข้อมูล BU Risk Criteria/ FCY/ CRP/ อื่น ๆ เข้าระบบ

ระยะเวลา 60 วัน

**ขั้นตอนที่ 4: สื่อความเกณฑ์และแนวทางการประเมินฯ**

ระยะเวลา 1 วัน

**ขั้นตอนที่ 5: ประเมิน GRC Assessment**
- ประเมิน GRC Assessment สำหรับหน่วยงานระดับฝ่าย/ส่วนขึ้นตรง
- Risk Owner สื่อความและร่วมกับพนักงานในหน่วยงานระบุความเสี่ยงและจุดควบคุมที่สำคัญ พร้อมนำเสนอในที่ประชุมฝ่าย ก่อนอนุมัติในระบบ
- GRC Agent สอบทานความถูกต้องและความสอดคล้องของผลประเมินฯ

ระยะเวลา 60 วัน

**ขั้นตอนที่ 6: ผู้บริหารประเมิน E-CSA**
- ผู้บริหารระดับผู้ช่วยขึ้นไป ประเมิน E-CSA
- นำเสนอผลการประเมินฯ แก่ผู้บริหารของสายงาน

ระยะเวลา 60 วัน

**ขั้นตอนที่ 7: การติดตามและรายงาน**
- สรุปผลประเมิน GRC Assessment และรายงานผลการประเมินภาพรวมของ ปตท. แก่คณะกรรมการต่าง ๆ
- ติดตามสถานะของแผนปรับปรุงให้เป็นไปตามแผนงานที่กำหนด
- สรุปผลการประเมินฯ สำหรับจุดมุ่งเน้น นำส่งหน่วยงาน 2nd Line เพื่อจัดทำแผนการปรับปรุง

ระยะเวลา 60 วัน