การตรวจสอบภายในแบบบูรณาการ
(Integrated Audit)

วันที่ 14 พฤศจิกายน 2564

อบรมออนไลน์ ผ่านระบบ Microsoft Teams

จัดโดยสภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

จุฑารัตน์ ลอยโคกสูง
กลุ่มตรวจสอบภายใน

การตรวจสอบภายใน

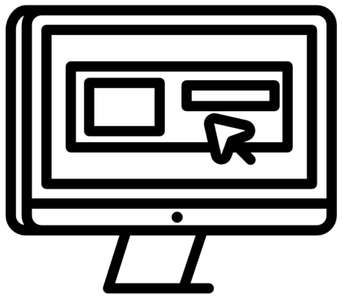
คือ การให้ความเชื่อมั่นและการให้คำปรึกษา อย่างเที่ยงธรรมและเป็นอิสระ เพื่อเพิ่มคุณค่าและปรับปรุงการดำเนินงานขององค์กร การตรวจสอบภายในช่วยให้องค์กรบรรลุเป้าหมายด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแล อย่างเป็นระบบ และเป็นระเบียบ

การตรวจสอบภายในแบบบูรณาการ (Integrated Audit)

ความหมาย

- การผสานรวม/บูรณาการ IT Audit และ Non IT Audit รวมถึงกลยุทธ์/กระบวนการตรวจสอบ ไว้ในโครงการตรวจสอบเดียวกัน
- มุ่งเน้นให้มีกระบวนการตรวจสอบที่น่าเชื่อถือ
- จัดสรรและใช้ทรัพยากรในการตรวจสอบที่เกี่ยวข้องกับความเสี่ยงได้อย่างมีประสิทธิผลและประสิทธิภาพ

ผลกระทบของการใช้เทคโนโลยีสารสนเทศต่องานตรวจสอบภายใน



เทคโนโลยีสารสนเทศ

1. การประมวลผลเชิงกระจาย (Distributed Data Processing) เช่น การแบ่งภาระงานหรือกระจายอำนาจดำเนินการบนระบบสารสนเทศ	- การจำกัดการเข้าถึงระบบตามความจำเป็น - ความครบถ้วนสมบูรณ์ของรายการข้อมูล
2. เครือข่ายคอมพิวเตอร์ (Computer Networking) เช่น ระบบเครือข่ายแบบเชื่อมต่อคอมพิวเตอร์เข้าด้วยกันในระยะจำกัด (Local Area Network : LAN) ระบบเครือข่ายไร้สาย (Wireless LAN)	- ต้องมีมาตรการจำกัดการเข้าใช้งานในเครือข่ายตามความจำเป็นเท่านั้น
3. ระบบการประมวลผลทันที (Real-time systems)	- ไม่รองรับการสอบทานผลรวมรายการทั้งหมด - จำกัด/ควบคุมอำนาจอนุมัติรายการ
4. ผู้ใช้งานพัฒนาระบบงานขึ้นใช้เอง (End-user computing)	- ความถูกต้องครบถ้วนของข้อมูล - การเข้าถึงระบบโดยไม่ได้รับอนุญาตจากช่องทางต่าง ๆ ที่ไม่ได้รับการดูแลควบคุม
5. อินเทอร์เน็ต (Internet/e-commerce) เช่น การทำงานผ่านระบบ Website Web-Application	- การเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต/การบุกรุกเครือข่ายจากบุคคลภายนอก - ความครบถ้วนสมบูรณ์ของรายการข้อมูล

ประโยชน์

ของ

การตรวจสอบแบบบูรณาการ

สำหรับผู้ตรวจสอบภายใน

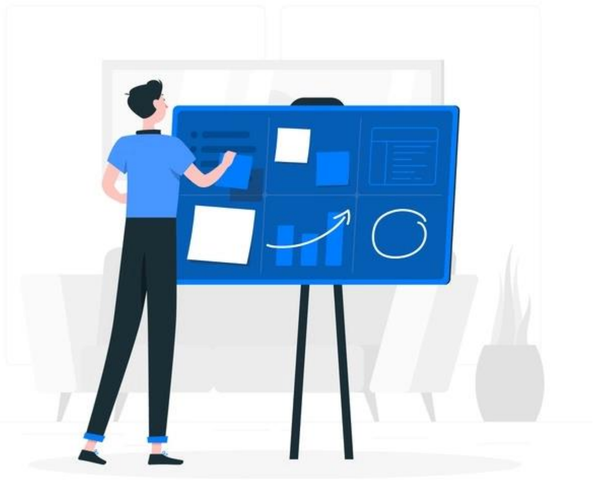
มีความรู้ความเข้าใจเกี่ยวกับความเสี่ยง
และการควบคุมความเสี่ยงได้อย่างครบถ้วน
สมบูรณ์

สำหรับกิจการ

มีการตรวจสอบการควบคุมความเสี่ยงทางธุรกิจ
และความเสี่ยงสืบเนื่องด้าน IT ซึ่งเกี่ยวข้อง
สัมพันธ์กับความเสี่ยงโดยรวมของกิจการ
เพื่อสนับสนุนความสามารถในการบรรลุ
เป้าหมายของกิจการได้อย่างมั่นใจ

สำหรับหน่วยรับตรวจ

มีความเข้าใจและได้รับข้อเสนอแนะ
ที่ตรงประเด็น และเพียงพอ ครอบคลุม
ความเสี่ยงทั้งในส่วนของความเสี่ยงทางธุรกิจ
และความเสี่ยงในการใช้เทคโนโลยีสารสนเทศ



ขอบเขตงานตรวจสอบแบบบูรณาการ

การวางแผน

01

มีการวางแผนโครงการการตรวจสอบ
ที่ครอบคลุมความเสี่ยงด้าน IT ที่มีผลกระทบ
สืบเนื่องต่อความเสี่ยงทางธุรกิจของกิจการ
โดยรวม

การลดงาน

02

ลดงานตรวจสอบที่ซ้ำซ้อนกันระหว่างการตรวจสอบ
การควบคุมในระบบมือ และการควบคุมอัตโนมัติ
ในระบบงานที่มีวัตถุประสงค์การควบคุมเดียวกัน

การตรวจสอบ

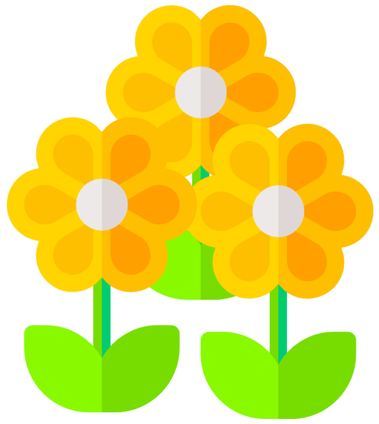
03

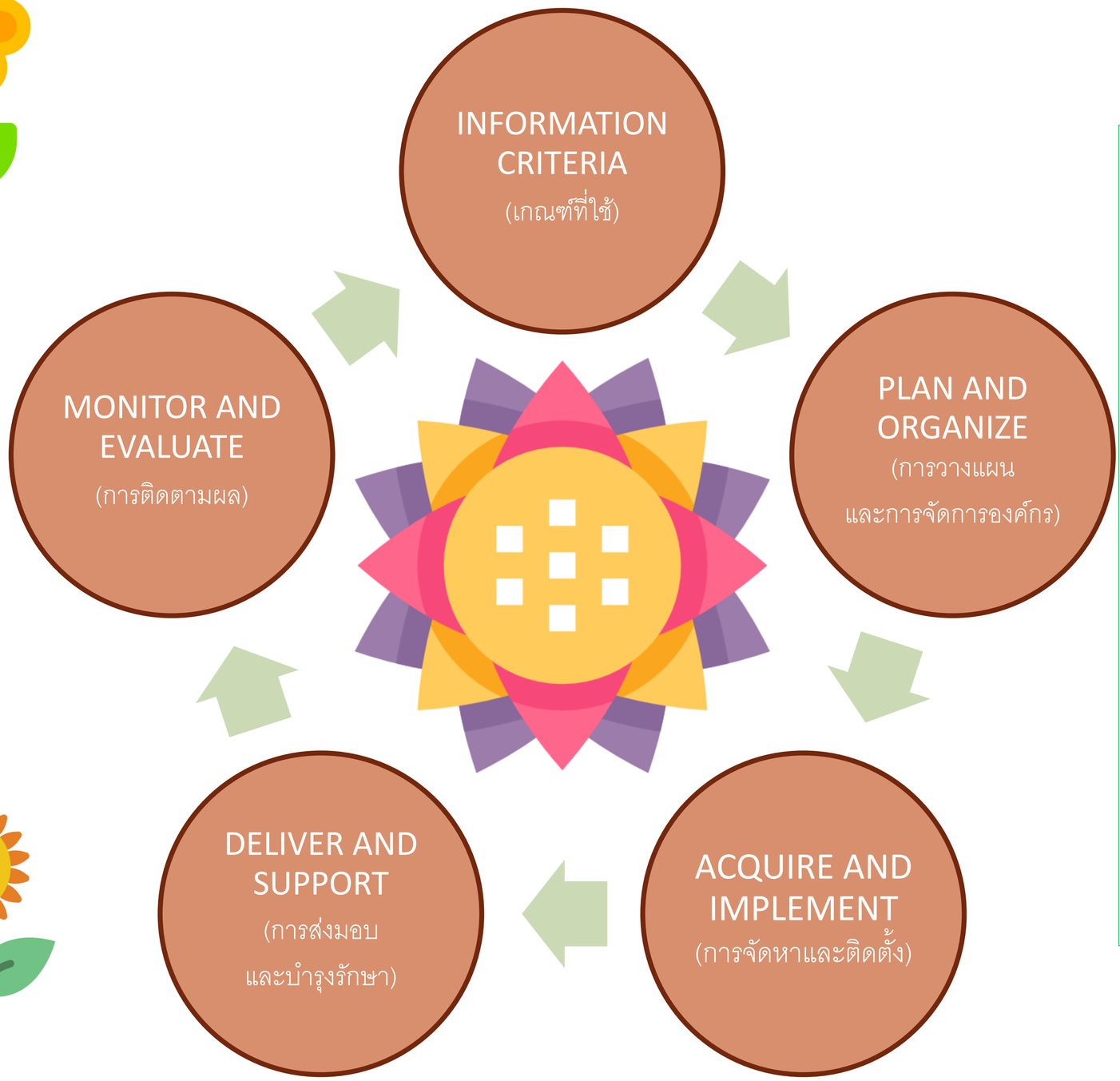
การตรวจสอบความถูกต้องครบถ้วน
ของการส่งผ่านข้อมูลระหว่างวงจรธุรกิจ
(Data Interface)

ขอบเขตการตรวจสอบแบบบูรณาการ (ต่อ)

การตรวจสอบการควบคุมทั่วไปเทคโนโลยีสารสนเทศ

- Effectiveness
- Availability
- Efficiency
- Compliance
- Confidentiality
- Reliability





- การให้บริการด้านเทคโนโลยีสารสนเทศสามารถสนับสนุนการปฏิบัติงานได้อย่างสอดคล้องกับเป้าหมายและพันธกิจขององค์กรหรือไม่

- ทำให้ผู้บริหารขององค์กรได้ทราบว่ากลยุทธ์ทางด้านเทคโนโลยีสารสนเทศและกลยุทธ์ทางด้านธุรกิจเป็นไปในทิศทางเดียวกันหรือไม่
- เพื่อให้ทราบว่าผู้ปฏิบัติงานมความรู้ ความเข้าใจเกี่ยวกับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศหรือไม่ และจะมีวิธีการบริหารจัดการความเสี่ยงดังกล่าวได้อย่างไร

- ระบบสารสนเทศใหม่ที่จะนำมาใช้งานนั้นสามารถทำงานได้อย่างมีประสิทธิภาพ ตรงตามความต้องการขององค์กรหรือไม่
- การเปลี่ยนแปลงที่เกิดขึ้นทำให้เกิดผลเสียต่อการปฏิบัติงานขององค์กรในปัจจุบันหรือไม่

- โครงการด้านเทคโนโลยีสารสนเทศ ที่กำลังจะพัฒนาหรือดำเนินการจัดหานั้นสามารถนำมาใช้แก้ไขปัญหาหรือสนับสนุนการปฏิบัติงานขององค์กรได้หรือไม่
- โครงการด้านเทคโนโลยีสารสนเทศ ที่กำลังจะพัฒนาหรือดำเนินการจัดหานั้นสามารถนำมาใช้งานได้ทันตามระยะเวลา และงบประมาณที่กำหนดไว้หรือไม่

ความเสี่ยง

ความหมาย

ปัจจัยต่าง ๆ ที่ส่งผลกระทบต่อความสามารถในการบรรลุเป้าหมายของกิจการ ซึ่งมีโอกาสเกิดขึ้นและส่งผลกระทบให้เกิดความเสียหายในระดับที่แตกต่างกันไปตามสภาพแวดล้อมและวิธีการดำเนินธุรกิจและบริหารงานของกิจการ

การประเมินความเสี่ยง

ในการประเมินความเสี่ยงเราจะดำเนินการประเมินใน 2 ด้าน คือ

ผลกระทบ (Impact)

ระดับความรุนแรงของความเสียหายที่เกิดขึ้น ซึ่งอาจพิจารณาจากผลกระทบรุนแรงที่สุดที่เกิดขึ้นต่อความสามารถอยู่รอดของกิจการ ความสามารถในการแข่งขัน สภาพความคลองทางการเงิน ตลอดจนสภาพทั่วไปทางสังคม ชื่อเสียง และกำลังบุคลากร

โอกาสที่จะเกิดขึ้น (Likelihood)

ระดับของโอกาสที่จะเกิดเหตุการณ์ความเสียหาย โดยอาจพิจารณาถึงค่าความน่าจะเป็น หรือค่าความถี่ของการเกิดเหตุการณ์

กระบวนการจัดการความเสี่ยงด้านเทคโนโลยี

1.

IT Risk Assessment
(ประเมินระดับความเสี่ยง
เทคโนโลยีสารสนเทศ)

- ❑ Objective : กำหนดวัตถุประสงค์
- ❑ Risk Identification : ระบุความเสี่ยง
- ❑ Assessment : ประเมิน วิเคราะห์
  ผลกระทบทางธุรกิจ และโอกาส
  ที่จะเกิดขึ้น

2.

IT Control Evaluation
(ประเมินระดับการควบคุม)

- ❑ Legends for Ranking used : การวัดคุณภาพการควบคุม

0 Non-exist-Mgt. = ไม่ใช้กระบวนการเลย

1 Initial = กระบวนการเป็นแบบเฉพาะกิจและไม่เป็นระเบียบ

2 Repeatable = กระบวนการเป็นไปตามรูปแบบปกติ

3 Defined & Managed = กระบวนการได้รับการจัดทำเป็นเอกสาร
และมีการสื่อสาร

4 Optimised = มีการปฏิบัติตามแนวทางที่ดีที่สุดและเป็นไป
โดยอัตโนมัติ

3.

Gap Analysis for Residual Risk
(วิเคราะห์ระดับความเสี่ยงในส่วนที่เหลือ)

- ❑ Planning and organization
  การวางแผนและการจัดองค์กร
- ❑ Acquisition and implementation
  การได้มาและการดำเนินการ

กลยุทธ์การตรวจสอบแบบบูรณาการ

Non-IT Audit Work ***Integrated Audit Work*** ***IT Audit Work***

การวางแผนการตรวจสอบ

รวบรวม/ศึกษาเป้าหมายธุรกิจ
ผลการประเมินความเสี่ยง และการควบคุมธุรกิจ

ขอบเขตและแผนการตรวจสอบการควบคุม
วงจรธุรกิจต่าง ๆ

พิจารณาขอบเขตและแผนการตรวจสอบ
วงจรธุรกิจต่าง ๆ ที่ดำเนินงาน
ภายใต้สภาพแวดล้อมของระบบสารสนเทศ
ที่ใช้คอมพิวเตอร์

ศึกษาสภาพแวดล้อมระบบสารสนเทศ ประเมิน
ความเสี่ยง และการควบคุม
ด้านเทคโนโลยีสารสนเทศ

ขอบเขตและแผนการตรวจสอบ
การควบคุมทั่วไปเทคโนโลยีสารสนเทศ
และการควบคุมเฉพาะระบบ

การปฏิบัติงานตรวจสอบ

ประเมินการออกแบบและทดสอบการควบคุม
วงจรธุรกิจต่าง ๆ / รายงานผล

ส่งจดหมายเข้าตรวจสอบและประชุม
เปิดการตรวจสอบ

ประเมินการออกแบบ และทดสอบการควบคุมทั่วไป
เทคโนโลยีสารสนเทศ/รายงานผล

เชื่อถือได้

ประเมินการออกแบบ และทดสอบการควบคุมเฉพาะ
ระบบ/รายงานผล

พิจารณาผลการตรวจสอบการควบคุม
และกำหนดขอบเขตการตรวจสอบเนื้อหาสาระสำหรับ
ประเด็นข้อตรวจพบ

ตรวจสอบเนื้อหาสาระ/รายงานผล

ตรวจสอบเนื้อหาสาระ/รายงานผล

การรายงานผลการตรวจสอบ

พิจารณาผลการตรวจสอบเนื้อหาสาระ/
ออกรายงานผลการตรวจสอบ

ข้อดีของการตรวจสอบแบบบูรณาการ

Multiple audit techniques

แลกเปลี่ยน/เรียนรู้ซึ่งกันและกัน

Increased use of external resources or knowledge of staff and additional skill sets

เชิญบุคลากรภายนอกที่มีความเชี่ยวชาญ มาช่วยในการตรวจสอบ

Enhanced project management skills to ensure coordination and effectiveness

การทำงานร่วมกัน

A balanced approach to risk identification and rating

ผู้ตรวจทั่วไปเข้าใจมุมมองธุรกิจ ผู้ตรวจ IT เข้าใจ IT ซึ่งจะทำให้มองเห็นชัดเจน ไม่ตกหล่น

Increased oversight and creativity to think outside the box, and communication among all parties involved in the engagement.

จะเห็นเรื่องใหม่ ๆ เรียนรู้ด้วยกัน เกิดการสื่อสารในการจัดการดูแล

Changes in the current staffing model and career development

เรียนรู้ชิ้นงานใหม่ ขอบเขตงานใหม่ที่ท้าทาย เป็นการพัฒนาบุคลากร

Time saving/effective use of resources

เป็นการเปิดตรวจครั้งเดียว งานก็จะไม่ซ้ำซ้อน

จรรยาบรรณของผู้ประกอบวิชาชีพตรวจสอบภายใน

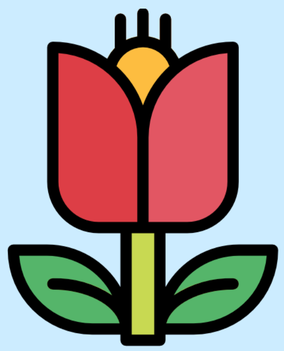
ความซื่อสัตย์ (Integrity)

- ✓ ปฏิบัติหน้าที่ของตนด้วยความซื่อสัตย์ ขยันหมั่นเพียร และมีความรับผิดชอบ
- ✓ ปฏิบัติตามกฎหมายและเปิดเผยข้อมูลตามที่กฎหมายหรือการกระทำที่อาจเสื่อเสียต่อวิชาชีพการตรวจสอบภายในหรือองค์กร
- ✓ เคารพและสนับสนุนวัตถุประสงค์ที่ถูกต้องตามกฎหมายและหลักจริยธรรมขององค์กร

ความเที่ยงธรรม (Objectivity)

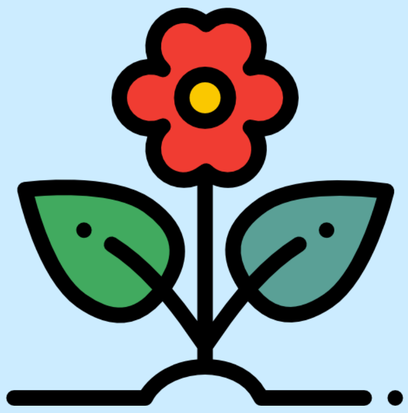
- ✓ ไม่มีส่วนร่วมในกิจกรรมหรือความสัมพันธ์ที่บั่นทอนการประเมินอย่างไม่เป็นกลาง ไม่ลำเอียง ทั้งนี้ รวมไปถึงการกระทำหรือความสัมพันธ์ที่ขัดต่อผลประโยชน์ขององค์กรด้วย
- ✓ ไม่รับสิ่งตอบแทนใด ๆ ที่บั่นทอนหรืออาจบั่นทอนดุลยพินิจของผู้ประกอบวิชาชีพ
- ✓ เปิดเผยความจริงทั้งหมดที่ทราบ ซึ่งหากละเว้นไม่เปิดเผยแล้วอาจทำให้รายงานผลการตรวจสอบบิดเบือนไป

การรักษาความลับ (Confidentiality)



- ✓ รอบคอบในการใช้ และปกป้องสารสนเทศที่ได้มาระหว่างการปฏิบัติหน้าที่
- ✓ ไม่ใช้สารสนเทศที่ได้มาเพื่อผลประโยชน์ส่วนตนหรือเพื่อการใดที่ขัดต่อกฎหมายหรือขัดต่อวัตถุประสงค์ที่ถูกต้องตามกฎหมายและหลักจริยธรรมขององค์กร

ความสามารถในหน้าที่ (Competency)



- ✓ ปฏิบัติหน้าที่เฉพาะในงานส่วนที่ตนมีความรู้ ทักษะ และประสบการณ์ที่จำเป็นสำหรับงานส่วนนั้นเท่านั้น
- ✓ ปฏิบัติงานตรวจสอบภายในโดยยึดมาตรฐานสากลการปฏิบัติงานวิชาชีพการตรวจสอบภายใน (International Standards for the Professional Practice of Internal Auditing) เป็นหลัก
- ✓ พัฒนาความชำนาญ ประสิทธิผล และคุณภาพของบริการอย่างต่อเนื่อง