รายงานการไปศึกษา/ดูงาน/ฝึกอบรม/ประชุมและสัมมนา

๑. ชื่อ นางทักษอร อินทุเศรษฐ ตำแหน่งนักวิชาการตรวจสอบภายในชำนาญการ
ที่ทำงาน กลุ่มตรวจสอบภายใน กรมส่งเสริมการเกษตร
ไป (ดูงาน/ฝึกอบรม/ประชุมหรือสัมมนา) หลักสูตรระดับ ๒ การตรวจสอบภายในเฉพาะด้าน (Audit Specialist) การตรวจสอบการกำกับดูแล การบริหารความเสี่ยงและการควบคุมภายใน (Governance, Risk Management and Control Audit Specialist) ณ โรงแรมเซ็นทารา ไลฟ์ ศูนย์ราชการ และคอนเวนชันเซ็นเตอร์ แจ้งวัฒนะ กรุงเทพมหานคร
จัดโดยกรมบัญชีกลาง ฝึกอบรมระหว่างวันที่ ๒๓ – ๒๕ กรกฎาคม ๒๕๖๘
รวมระยะเวลา .....-..... ปี .....-..... เดือน .....๓..... วัน
ผู้ดำเนินการจัด กรมบัญชีกลาง
๒. ค่าใช้จ่ายที่ใช้ไประหว่างฝึกอบรม/ดูงาน/สัมมนา/ประชุม

ค่าเบี้ยเลี้ยง	.....-.....บาท
ค่าที่พัก	.....-.....บาท
ค่าพาหนะ	.....๕๐๐.....บาท
อื่น ๆ (ค่าลงทะเบียน)	....๖,๐๐๐.....บาท

๓. รายละเอียดการดูงาน ฝึกอบรม ประชุม สัมมนา ฯลฯ ที่สมควรรายงานให้มีรายละเอียดและเนื้อหามากที่สุดเท่าที่จะทำได้ โดยบรรยายสิ่งที่ได้สังเกต รู้ เห็น หรือได้รับถ่ายทอดมาให้ชัดเจน ถ้ามีเอกสารต่างหากให้แนบไปด้วย

<u>เนื้อหาวิชาการ</u>

โครงการอบรมหลักสูตรประกาศนียบัตรผู้ตรวจสอบภายใน (CGIA) หลักสูตรระดับ ๒ การตรวจสอบภายในเฉพาะด้าน (Audit Specialist) หลักสูตรการตรวจสอบการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายใน (Governance, Risk Management and Control Audit Specialist) มีดังนี้

หัวข้อที่ ๑ การตรวจสอบการบริหารจัดการความเสี่ยงด้านการทุจริต
หัวข้อที่ ๒ การตรวจสอบด้านการกำกับ ดูแล
หัวข้อที่ ๓ การตรวจสอบด้านระบบการควบคุมภายในและการบริหารจัดการความเสี่ยง
หัวข้อที่ ๔ การให้บริการให้คำปรึกษา
หัวข้อที่ ๕ หลักการคิดวิเคราะห์สำหรับผู้ตรวจสอบภายใน (Analytical Thinking)

โดยมีรายละเอียดดังนี้

หัวข้อที่ ๑ การตรวจสอบการบริหารจัดการความเสี่ยงด้านการทุจริต

บรรยายโดย อาจารย์ศิวะรักษ์ พินิจารมณ์ ภาคเอกชน

การตรวจสอบการบริหารความเสี่ยงด้านการทุจริต

๑. ความเสี่ยงโดยธรรมชาติ (Inherent Risk) ความเสี่ยงที่เกิดขึ้นโดยธรรมชาติของธุรกิจ กิจกรรม หรือกระบวนการใด ๆ ก่อนที่จะมีการนำระบบควบคุมภายในหรือมาตรการบรรเทาความเสี่ยงใด ๆ มาใช้

๒. ความเสี่ยงจากการควบคุม (Control risk) ในบริบทของการตรวจสอบบัญชีหรือการบริหารความเสี่ยงโดยทั่วไป หมายถึง ความเสี่ยงที่ระบบการควบคุมภายในขององค์กรจะไม่สามารถป้องกัน, ตรวจพบ, หรือแก้ไขข้อผิดพลาดหรือการทุจริตที่มีสาระสำคัญได้อย่างทันท่วงที

๓. ความเสี่ยงในการตรวจจับ (Detection Risk) ในการสอบบัญชี คือ ความเสี่ยงที่ผู้สอบบัญชีจะไม่สามารถตรวจพบการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ (Material Misstatement) ที่มีอยู่ในงบการเงินได้ แม้ว่าการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงนั้นจะเกิดขึ้นจริงก็ตาม

๔. ความเสี่ยงในการสอบบัญชี (Audit Risk) หมายถึง ความเสี่ยงที่ผู้สอบบัญชีจะแสดงความเห็นที่ไม่เหมาะสมต่องบการเงินที่แสดงข้อมูลที่ขัดต่อข้อเท็จจริงอันเป็นสาระสำคัญ (Material Misstatement) ทั้ง ๆ ที่งบการเงินนั้นมีความผิดพลาดอย่างมีนัยสำคัญ

ความหมายการทุจริต

COSO (The Committee of Sponsoring Organizations of the Treadway Commission) องค์กรเอกชนหลักที่เกี่ยวข้องกับวิชาชีพบัญชีและการเงิน เพื่อให้คำแนะนำและจัดทำกรอบการทำงานเกี่ยวกับการบริหารความเสี่ยงองค์กร (Enterprise Risk Management - ERM) การควบคุมภายใน (Internal Control) และการป้องกันการทุจริต (Fraud Deterrence) และ ACFE (Association of Certified Fraud Examiners) (สมาคมผู้ตรวจสอบการฉ้อโกงที่ผ่านการรับรอง)

การทุจริต

- เจตนากระทำหรือละเว้นไม่กระทำ
- ออกแบบเพื่อหลอกลวงผู้อื่น
- เกิดความเสียหาย
- ผู้กระทำได้รับผลประโยชน์ส่วนตน

ทุจริตต่อหน้าที่

- ปฏิบัติหรือละเว้นการปฏิบัติ
- ในตำแหน่งหน้าที่หรือผู้อื่นเชื่อว่าอยู่ในตำแหน่งหน้าที่
- เพื่อแสวงหาผลประโยชน์มิควรได้โดยมิชอบเพื่อตนและผู้อื่น

หมวดของการทุจริต มีจำนวน ๓ หมวด คือ

๑. คอร์รัปชั่น (การทุจริต)

- ความขัดแย้งทางผลประโยชน์ (โครงการจัดซื้อจัดจ้าง แบบแผน)
- การติดสินบน/เงินใต้โต๊ะ Kickbacks (เงินหรือผลประโยชน์อื่น ๆ ที่จ่ายคืนให้กับบุคคลหรือหน่วยงาน เพื่อแลกกับการได้รับบริการ, สัญญา, หรือสิทธิพิเศษบางอย่าง ซึ่งมักจะเป็นการกระทำที่ผิดกฎหมายหรือไม่โปร่งใส ตัวอย่างเช่น การจ่าย "ค่าน้ำร้อนน้ำชา" หรือ "เงินส่วนแบ่ง" จากกำไรให้กับเจ้าหน้าที่เพื่อแลกกับการได้รับงานหรือการอนุมัติ) และการเสนอราคาเสื้อผ้า
- เงินบำเหน็จที่ผิดกฎหมาย การขู่กรรโชกทรัพย์

๒. การนำทรัพย์สินขององค์กรไปใช้อย่างไม่เหมาะสม

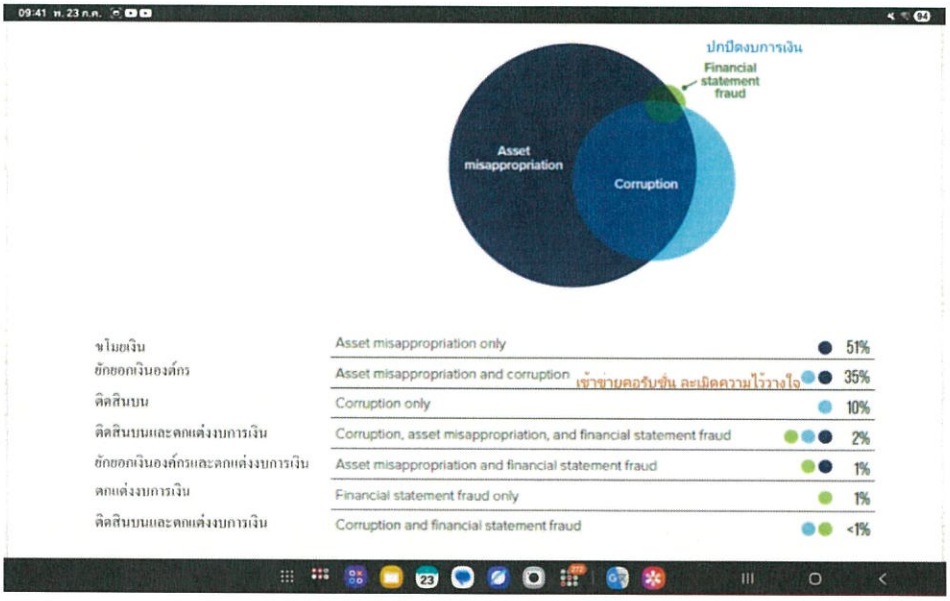
- การยักหยอกทรัพย์สิน

๑. เงินสด ๑.๑ โจรกรรมเงินสดในมือ ๑.๒ การขโมยใบเสร็จรับเงิน ตกแต่งใบเสร็จ ๑.๓ การฉ้อโกงการจ่ายเงิน

๒. สินค้าคงคลังและสินค้าอื่น ๆ

๓. การบิดเบือนรายงาน (การฉ้อโกงงบการเงิน)

การทุจริตอาจเข้าข่ายมากกว่าหนึ่งหมวด



กรอบโครงสร้างความเสี่ยงด้านการทุจริตของภาคราชการ เช่น การฮั้วประมูล การรวมหัวกันกำหนดราคา พนักงาน Corruption ใช้ทรัพย์สินไม่เหมาะสม ติดสินบน Kickback กรรโชก รีดไถ รายงานเท็จ ปลอมเอกสาร คู่ค้าปลอม โกงเงินช่วยเหลือ จ่ายเงินไม่เหมาะสม ขโมยข้อมูลส่วนบุคคล ขโมยสินทรัพย์ทางปัญญา ขโมยข้อมูลส่วนบุคคลผ่าน IP ผิดกฎหมาย FCPA ฟอกเงิน เปิดเผยข้อมูลลับ ขโมยข้อมูลลับ อาชญากรรม Cyber จารกรรม Phishing Ransomware ทุจริต Email ธุรกิจ/บัญชี เขาถึงระบบโดยไม่ได้รับอนุญาต ขโมยข้อมูล เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ขโมยข้อมูลที่เป็นความลับ การโกงเลือกตั้ง การเล่นพรรคเล่นพวก การใช้อิทธิพลมืด องค์กรอาชญากรรม การรวมกลุ่มเพื่อผูกขาดธุรกิจ

- การฮั้วประมูล
- การรวมหัวกันกำหนดราคา
- พนักงาน Corruption
- ใช้ทรัพย์สินไม่เหมาะสม
- ติดสินบน
- Kickback
- กรรโชก รีดไถ
- รายงานเท็จ
- ปลอมเอกสาร
- คู่ค้าปลอม
- โกงเงินช่วยเหลือ
- จ่ายเงินไม่เหมาะสม
- ขโมยข้อมูลส่วนบุคคล
- ขโมยสินทรัพย์ทางปัญญา
- ขโมยข้อมูลส่วนบุคคลผ่าน IP
- ผิดกฎหมาย FCPA
- ฟอกเงิน
- เปิดเผยข้อมูลลับ
- ขโมยข้อมูลลับ
- อาชญากรรม Cyber
- จารกรรม
- Phishing
- Ransomware
- ทุจริต Email ธุรกิจ/บัญชี
- เข้าถึงระบบโดยไม่ได้รับอนุญาต
- ขโมยข้อมูล
- เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
- ขโมยข้อมูลที่เป็นความลับ

เพิ่มเติม:

- การโกงเลือกตั้ง
- การเล่นพรรคเล่นพวก
- การใช้อิทธิพลมืด
- องค์กรอาชญากรรม
- การรวมกลุ่มเพื่อผูกขาดธุรกิจ

*Fraud Risk Management, AICPA & CIMA

การทุจริตในภาคราชการ ระดับชาติ ๔๗ % รัฐและจังหวัด ๒๙ % และท้องถิ่น ๒๓ % ในแต่ละระดับ ผู้บริหาร ๑๙ % ผู้จัดการ ๓๙ % และ พนักงาน ๓๙ % ถึงผู้บริหารกระทำผิดในองค์กรของรัฐแค่ ๑๙ % เท่านั้น แต่ผู้ฉ้อโกงอยู่บนสุดกลับก่อให้เกิดความศูนย์เสียมากที่สุด

Domains ของมาตรฐานการตรวจสอบภายในสากล Global internal Audit Standards

๑. purpose of internal auditing วัตถุประสงค์ของการตรวจสอบภายใน

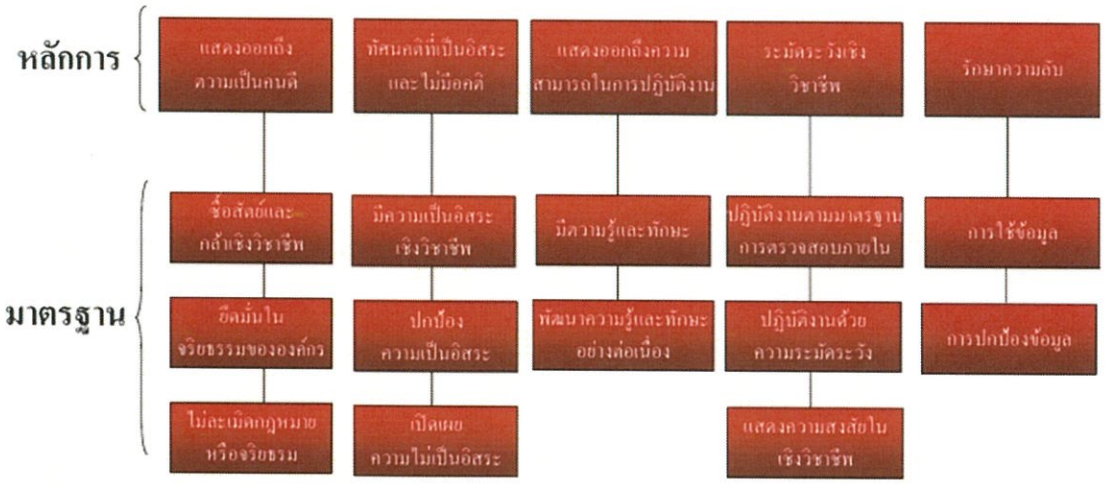
๒. Ethics & professionalism จริยธรรมและความเป็นมืออาชีพ มี ๕ หลักการ ๑๓ มาตรฐาน

๓. Governing the internal Audit Function การกำกับดูแลการทำงานตรวจสอบภายใน

๔. Managing the internal Audit Function การจัดการทำงานตรวจสอบภายใน

๕. Performing internal Audit Services แสดงการบริการตรวจสอบภายใน

จริยธรรมและความเป็นมืออาชีพ



ความท้าทายของผู้ตรวจสอบภายในภาคราชการ

๑. การเมืองและสภาพแวดล้อมทางการเมือง

- การเปลี่ยนแปลงผู้นำทางการเมือง
- การเปลี่ยนแปลงข้าราชการและแนวทางของระบบราชการ

๒. ความท้าทายของผู้ตรวจสอบภายใน

- การปฏิบัติงานตรวจสอบภายใน
- การแก้ไขปรับปรุงขอแนะนำของผู้ตรวจสอบภายใน

๓. การยึดมั่นจริยธรรมวิชาชีพของผู้ตรวจสอบภายใน

- ๕ มาตรฐานใน Domain ๒ ของ The IIA Global
- ความโปร่งใสสร้างความมั่นใจให้กับสาธารณชนและผู้มีส่วนได้เสีย
- ยึดมั่นในจริยธรรมของวิชาชีพสูงกว่าภาคเอกชนเนื่องจากค่าตอบแทนมาจากประชาชน

การปฏิบัติตามจริยธรรม ผู้ตรวจสอบภายในควรตัดสินใจด้วยตนเองในการปฏิบัติตามหลักการที่กำหนดไว้

ความระมัดระวังเชิงวิชาชีพ คือ พิจารณาความเป็นไปได้ที่การผิดพลาดจะเกิดจากเจตนาในทุกเรื่องที่อยู่ในแผนการตรวจสอบ

ระบบร้องเรียนที่มีประสิทธิผล

การบริหารระบบร้องเรียน (Speak Up & Listen Up)

ภาคราชการและส่วนใหญ่ของภาคเอกชนควรมีระบบร้องเรียนโดยปฏิบัติตามหลักการสากล ๑๙ แนวทางดังต่อไปนี้

ขอบเขต :

๑. การกระทำที่ละเมิดกฎหมาย หรือเป็นเหตุให้เกิดอันตรายต่อองค์กร

๒. การกระทำที่เกี่ยวข้องกับการปฏิบัติงานภายในองค์กร

๓. ปกป้องผู้ร้องเรียนโดยเชื่อว่า การร้องเรียนอยู่บนพื้นฐานของความจริง ณ เวลาที่ร้องเรียน

หน้าที่และความรับผิดชอบ :

๔. ผู้บริหารระดับสูงจัดตั้งระบบร้องเรียนและสนับสนุน Speak Up & Listen Up

๕. องค์กรกำหนดใหม่หน่วยงานและทรัพยากรดูแลระบบร้องเรียน

ข้อมูลและการสื่อสาร :

๖. ข้อมูลของระบบร้องเรียนต้องมีการสื่อสารและแพร่หลายในทุกระดับขององค์กร

๗. องค์กรควรรายงานต่อสาธารณชนถึงวัฒนธรรม Speak Up & Listen Up

ระเบียบวิธีปฏิบัติ :

๘. ระบบร้องเรียนควรมีหลายช่องทางในการรายงานและมีผู้รับในระดับผู้จัดการขึ้นไป

๙. ระบบร้องเรียนควรมีการติดตามและรายงานผล

๑๐. ผู้ร้องเรียนควรทราบสถานะตลอดกระบวนการ และโอกาสในการให้ข้อมูลเพิ่มเติม

๑๑. ข้อมูลของการร้องเรียนและการติดตามผลควรเป็นเอกสารในรูปแบบของการตรวจสอบและสามารถเรียกดูได้ในเวลาที่เหมาะสม

การสนับสนุนและการป้องกันผู้ร้องเรียน :

๑๒. ตัวตนและข้อมูลของผู้ร้องเรียนควรจำกัดการเปิดเผยเฉพาะที่ผู้ร้องเรียนยินยอม

๑๓. องค์กรควรยอมรับและติดตามผลรายงานของกลุ่มนิรนามและปกป้องผู้ร้องเรียน

๑๔. องค์กรควรป้องกันอันตรายหรือการรบกวนที่อาจเกิดขึ้นกับผู้ร้องเรียน

๑๕. องค์กรควรมีขั้นตอนในการป้อง และการควบคุมอันตรายที่อาจเกิดขึ้นกับผู้ร้องเรียน

๑๖. ระบบควรมีการใช้บังคับ โปร่งใสและมีกลไกที่ทันเวลาในกิจกรรมต่อไปนี้

- รับรู้และติดตามอันตราย การรบกวน หรือการเปิดเผยความลับที่อาจเกิดกับผู้ร้องเรียน
- ลงโทษผู้ทำอันตราย รบกวนหรือเปิดเผยความลับของผู้ร้องเรียน
- ชดใช้ผู้ร้องเรียนที่ถูกแกล้งโดยการบรรเทาผลกระทบ และจ่ายค่าตอบแทน

๑๗. องค์กรควรสนับสนุนผู้ร้องเรียนจากอันตรายที่กระทบสุขภาพและอาชีพการงาน

<u>การป้องกันบุคคลที่ถูกร้องเรียน :</u>

๑๘. องค์กรควรป้องกันบุคคลที่ถูกแกล้งจากการร้องเรียน และลงโทษผู้ร้องเรียนที่เจตนาให้ข้อมูลเท็จ

<u>ตรวจติดตามและสอบทานอย่างต่อเนื่อง :</u>

๑๙. องค์กรควรจัดให้มีการสอบทานระบบร้องเรียนอย่างน้อยปีละครั้ง แก้ไขปรับปรุงให้มีประสิทธิผลมากขึ้น โดยมั่นใจว่าระบบมีความทันสมัยอยู่ในกรอบของกฎหมายและอยู่ในแนวทางเชิงปฏิบัติที่ดีที่สุด

ความคุ้มค่าของระบบร้องเรียน :

๑. แสดงความมุ่งมั่นต่อสาธารณะถึงความเป็นข้าราชการที่ดีและรับผิดชอบต่อสังคม

๒. ป้องกัน และลดหรือบรรเทาภาระผูกพัน

๓. ป้องกัน และลดหรือบรรเทาภาระผูกพันด้านความเสียหายทางการเงิน

๔. ปรับปรุงการปฏิบัติตามกฎหมาย และการบริหารความเสี่ยงอย่างต่อเนื่อง

๕. สร้างชื่อเสียงขององค์กรให้มีความเข้มแข็งมากขึ้น

๖. เพิ่มประสิทธิภาพให้กับการพัฒนาสู่วัฒนธรรมขององค์กร

มาตรฐานการตรวจสอบภายในด้านการทุจริต

ข้อ ๑๒๑๐.A๑-๑ CAE ต้องขอความช่วยเหลือหรือขอคำแนะนำ ถ้าผู้ตรวจสอบภายในขาดความรู้ ความสามารถที่จำเป็นในการปฏิบัติงานตรวจสอบความช่วยเหลือและคำแนะนำอาจได้จากผู้เชี่ยวชาญที่อยู่ภายนอกองค์กร เช่น นักกฎหมาย นักบัญชี ผู้สอบการทุจริต หรืออื่น ๆ ผู้สอบการทุจริตอาจช่วยเหลือและให้คำแนะนำในเรื่องการสอบสวนการทุจริตหรือความปลอดภัยขององค์กรในด้านต่าง ๆ

ข้อ ๑๒๑๐-๑ ผู้ตรวจสอบภายในควรมีความรู้ในการบ่งชี้สิ่งบอกเหตุของการทุจริต

ข้อ ๑๒๑๐.A๒ ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอในการประเมินความเสี่ยงในเรื่องการทุจริต และลักษณะที่องค์กรจัดการกับความเสี่ยงดังกล่าว อย่างไรก็ดี ผู้ตรวจสอบภายในต้องไม่ถูกคาดหวังว่าจะมีความเชี่ยวชาญเท่ากับผู้ที่รับผิดชอบโดยตรงในด้านการตรวจสอบและสอบสวนการทุจริต

- สามารถระบุสิ่งบอกเหตุที่อาจนำไปสู่การทุจริต
- เข้าใจลักษณะและเทคนิคที่ใช้ทำทุจริต รวมทั้งรูปแบบและสถานการณ์ที่เกิดการทุจริต
- สามารถตัดสินใจได้ว่าควรทำอย่างไรต่อไป หรือควรเสนอให้ตั้งคณะกรรมการสอบสวนหรือไม่
- ประเมินประสิทธิผลของการควบคุมที่ใช้ป้องกันและตรวจจับการทุจริต รวมทั้งโอกาสในการปรับปรุง

ข้อ ๑๒๒๐.A๑ ผู้ตรวจสอบภายในต้องทำ Due Professional Care โดยการพิจารณาจาก :

- การขยายงานเพื่อให้บรรลุวัตถุประสงค์ของการตรวจสอบ
- ความซับซ้อนหรือสาระสำคัญของเรื่องที่จะให้ความมั่นใจ
- ความเพียงพอและประสิทธิผลของกระบวนการการกำกับดูแลความเสี่ยงและการควบคุม
- ความเป็นไปได้ที่จะเกิดความผิดพลาด การทุจริต และการละเมิดกฎระเบียบ
- ต้นทุนของการเพิ่มระบบควบคุมเปรียบเทียบกับผลกำไรที่คาดว่าจะได้รับ

ข้อ ๒๐๖๐ CAE ต้องรายงานผู้บริหารระดับสูงและคณะกรรมการบริษัทให้ทราบถึงวัตถุประสงค์ อำนาจดำเนินการ ความรับผิดชอบและผลการตรวจสอบเปรียบเทียบกับแผนงานเป็นระยะรายงานดังกล่าวต้องครอบคลุมความเสี่ยงที่มีสาระสำคัญและการควบคุมที่มีอยู่รวมทั้งความสี่ยงในเรื่องการทุจริตประเด็นการกำกับดูแลและเรื่องอื่น ๆ ที่ผู้บริหารระดับสูงและคณะกรรมการบริษัทกำหนดให้ปฏิบัติ

ข้อ ๒๑๒๐.A๒ ผู้ตรวจสอบภายในต้องประเมินความเป็นไปได้ที่จะเกิดการทุจริตและพิจารณาด้วยว่าองค์กรได้จัดการกับความเสี่ยงนั้นอย่างไร

ข้อ ๒๒๑๐.A๒ ผู้ตรวจสอบภายในต้องคำนึงถึงความเป็นไปได้ที่จะเกิดข้อบกพร่องที่มีสาระสำคัญ การทุจริตการละเมิดกฎระเบียบและความเสี่ยงอื่น ๆ ในขณะที่พัฒนาวัตถุประสงค์ในการตรวจสอบ

ผู้ตรวจสอบภายในไม่ควรรับผิดชอบในเรื่อง Fraud Investigation (สืบสวนการฉ้อโกง) เนื่องจาก :

- ต้องประเมินประสิทธิผลของกระบวนการ Fraud Investigation
- ขาด Resource (ขาดทรัพยากร) เช่น Investigators and Forensic Specialists

อย่างไรก็ดี ผู้ตรวจสอบภายในอาจรับผิดชอบเป็น Fraud Investigator ก็ได้แต่ต้องรับภาระหน้าที่ให้ชัดเจนใน Fraud Policy และ Internal Audit Charter

บทบาทของการตรวจสอบภายในเชิงปฏิบัติ ความรับผิดชอบของกิจกรรมตรวจสอบภายด้านการสืบสวนสอบสวน ควรกำหนดในกฎบัตร และนโยบาย และระเบียบปฏิบัติ :

๑. ผู้ตรวจสอบภายในอาจรับผิดชอบเบื้องต้น เป็นแหล่งทรัพยากรที่สนับสนุน หลีกเลี่ยงเพราะเป็นผู้ประเมินการสืบสวนสอบสวนหรือขาดทักษะ

๒. บทบาทใด ๆ แม้ขาดความอิสระ ยอมรับได้ ถ้ามีการเปิดเผย และบริหารจัดการอย่างเหมาะสม

๓. ผู้ตรวจสอบภายในปกติไม่เพียงประเมินการสบสวนสอบสวนแต่ยังให้คำแนะนำผู้บริหารในการปรับปรุงกระบวนการควบคุม

๔. ทีมสืบสวนสอบสวนต้องมีความรู้ ในรูปแบบของการทุจริต วิธีการสืบสวนสอบสวน และกฎหมายที่เกี่ยวข้อง

๕. กิจกรรมตรวจสอบภายในอาจใช้บุคลากรภายใน ภายนอก หรือทั้งสองแบบ

การควบคุมภายในตามแนวทางของ COSO-IC

องค์ประกอบการควบคมภายในของ COSO

๑. สภาพแวดล้อมในการควบคุม
๒. การประเมินความเสี่ยง
๓. กิจกรรมการควบคุม
๔. เทคโนโลยีและการสื่อสาร
๕. กิจกรรมการตรวจติดตาม

องค์ประกอบและหลักการของ COSO-IC

การประเมินความเสี่ยงด้านการทุจริต

๑. พิจารณาการทุจริตแบบต่าง ๆ

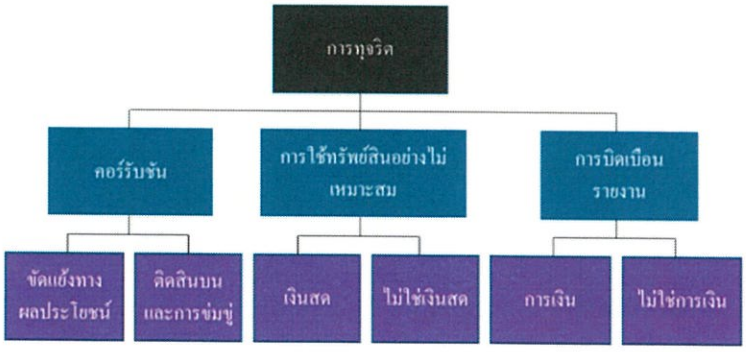
๒. ประเมินแรงจูงใจ ความกดดันและทัศนคติ

๓. ประเมินโอกาสหรือช่องทางที่อาจเกิดการทุจริต

๔. จัดให้มีมาตรการเพื่อป้องกันและแก้ไขการทุจริต

๕. สื่อสารให้มีการปฏิบัติตามนโยบายและแนวปฏิบัติ

การทุจริตแบบต่างๆ



องค์ประกอบของ COSO-FRM

๑. การกำกับดูแลความเสี่ยงด้านการทุจริต

๒. การประเมินความเสี่ยงด้านการทุจริต

๓. กิจกรรมการควบคุมความเสี่ยงด้านการทุจริต

๔. การสอบสวนการทุจริตและการแก้ไข

๕. กิจการการตรวจติดตามการบริหารความเสี่ยงด้านการทุจริต

หลักการของ COSO-FRM*

๑. จัดตั้งและสื่อสาร FRMP** ที่มุ่งมั่นในคุณค่าของคุณธรรมและจริยธรรม

๒. ระบุความเสี่ยงการทุจริตแต่ละประเภท & ควบคุมความเสี่ยงที่เหลืออยู่

๓. พัฒนาและใช้การควบคุมเพื่อป้องกันและการตรวจจับการทุจริต

๔. จัดตั้งกระบวนการเพื่อหาข้อมูล สอบสวนและแก้ไขการทุจริต

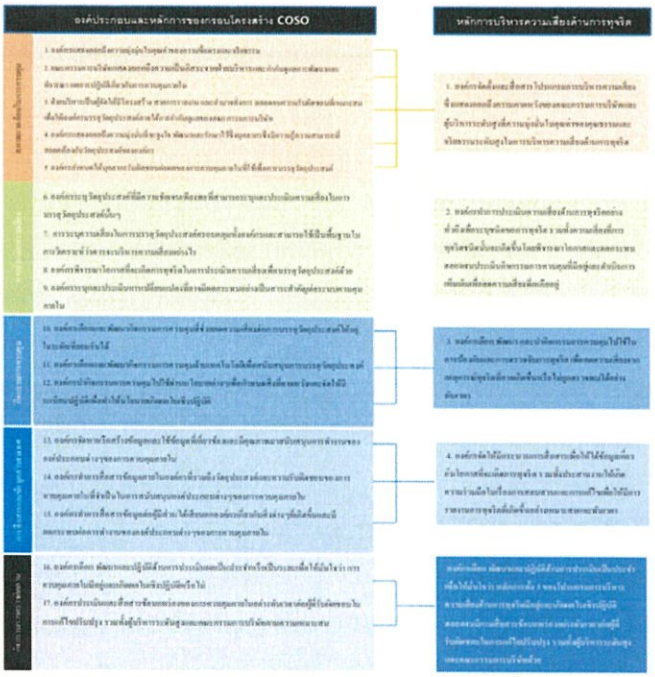
๕. ตรวจติดตามหลักการบริหารความเสี่ยงและ FRMP เพื่อแก้ไขข้อบกพร่อง

แนวทางการบริหารความเสี่ยง

๑. กรอบแนวทางการบริหารความเสี่ยงด้านการทุจริตออกแบบมาให้มีส่วนคล้ายกับผู้ที่เคยใช้กรอบโครงสร้างของ COSO โดยเสนอหลักการและจุดเน้น หลักการทั้ง ๕ ของแนวทางจึงสามารถเชื่อมต่อได้กับ ๕ องค์ประกอบ และ ๑๗ หลักการของ COSO

ความสัมพันธ์ระหว่าง 5 องค์ประกอบและ 17 หลักการของกรอบโครงสร้างการควบคุมภายในของ COSO กับ 5 หลักการของการบริหารความเสี่ยงด้านการทุจริต

COSO ได้ปรับปรุงกรอบโครงสร้างการควบคุมภายในปี 1992 ในปี 2013 โดยเพิ่ม 17 หลักการที่ชัดเจนจาก 5 องค์ประกอบที่มีอยู่เดิม ซึ่งแนวทางของการบริหารความเสี่ยงด้านการทุจริตที่ COSO ออกมาในปี 2016 ก็มีโครงสร้างคล้ายกันโดยมีองค์ประกอบและหลักการที่เชื่อมต่อกับ 17 หลักการของ COSO 2013 ดังจะเห็นได้จากการเชื่อมความสัมพันธ์ระหว่างหลักการที่กล่าวถึงดังต่อไปนี้



๒. บทสรุปขององค์ประกอบและหลักการของการบริหารความเสี่ยงด้านการทุจริต

๒.๑ การควบคุมดูแลด้านความเสี่ยงของการทุจริต (Fraud Risk Governance Component) การกำกับ ดูแล ด้านความเสี่ยงของการทุจริตเป็นองค์ประกอบที่เชื่อมต่อกับการกำกับ ดูแล ขององค์กร และสภาพแวดล้อมในการควบคุมภายใน การกำกับ ดูแล ขององค์กรแสดงลักษณะที่คณะกรรมการบริษัทและฝ่ายบริหารได้ปฏิบัติภารกิจในการบรรลุเป้าหมายขององค์กร ซึ่งรวมถึงการสร้างความสัมพันธ์อันดีการรายงานและการแสดงออกถึงความรับผิดชอบทางด้านกฎหมายต่อผู้มีส่วนได้เสียส่วนสภาพแวดลอมในการควบคุมภายในช่วยสร้างวินัยที่สนับสนุนการประเมินความเสี่ยงต่อการบรรลุวัตถุประสงค์ขององค์กร องค์กรจัดตั้งและสื่อสารโปรแกรมการบริหารความเสี่ยงด้านการทุจริตซึ่งแสดงออกถึงความคาดหวังและความมุ่งมั่นของคณะกรรมการบริษัท และผู้บริหารระดับสูงในเรื่องคุณค่าของความซื่อตรงและจริยธรรมในการบริหารความเสี่ยงด้านการทุจริต

๒.๒ การประเมินความเสี่ยงด้านการทุจริต (Fraud Risk Assessment Component) การประเมินความเสี่ยงด้านการทุจริตเป็นกระบวนการที่เคลื่อนไหวและต่อเนื่องในการระบุและประเมินความเสี่ยงด้านการทุจริตขององค์กร การประเมินความเสี่ยงด้านการทุจริตนี้ ทำให้เห็นความเสี่ยงของการตกแต่งรายงานทางการเงินหรือที่ไม่ใช่รายงานทางการเงิน การนำทรัพย์สินไปใช้อย่างไม่เหมาะสม และการกระทำผิดกฎหมาย (รวมทั้งคอร์รัปชัน) แนวทางนี้สามารถนำไปใช้ให้เหมาะสมและสอดคล้องตามความจำเป็น ตามความซับซ้อน และตามลักษณะที่กำหนดเป็นเป้าหมายขององค์กร การบริหารความเสี่ยงด้านการทุจริตไม่เพียงเชื่อมต่อกับองค์ประกอบของกรอบโครงสร้าง COSO ในเรื่องการบริหารความเสี่ยงและการควบคุมภายในแต่ยังเชื่อมต่อโดยเฉพาะกับหลักการที่ ๘ ของกรอบโครงสร้าง COSO ๒๐๑๓ ด้วยองค์กรทำการประเมินความเสี่ยงด้านการทุจริตเพื่อระบุชนิดของการทุจริต รวมทั้งความเสี่ยงที่การทุจริตชนิดนั้นจะเกิดขึ้นโดยพิจารณาโอกาสและผลกระทบตลอดจนประเมินกิจกรรมการควบคุมที่มีอยู่ในปัจจุบันและดำเนินการเพิ่มเติมเพื่อลดความเสี่ยงที่ยังคงเหลืออยู่

๒.๓ กิจกรรมการควบคุมการทุจริต (Fraud Control Activity Component) กิจกรรมการควบคุมการทุจริตเป็นการกระทำที่จัดตั้งขึ้นโดยผ่านนโยบายและระเบียบปฏิบัติที่ช่วยให้มั่นใจว่าแนวทางของฝ่ายบริหารในการลดความเสี่ยงด้านการทุจริตเกิดขึ้นในเชิงปฏิบัติ กิจกรรมการควบคุมการทุจริตเป็นระเบียบปฏิบัติหรือกระบวนการที่มีเจตนาเฉพาะเพื่อป้องกันการเกิดขึ้นของการทุจริต หรือตรวจจับได้อย่างรวดเร็วเมื่อเกิดการทุจริตขึ้น กิจกรรมการควบคุมการทุจริตโดยทั่วไปอาจมองได้ว่าเป็นทั้งส่วนที่ใช้ป้องกัน (ออกแบบเพื่อหลีกเลี่ยงเหตุการณ์ทุจริตหรือรายการที่จะนำไปสู่การทุจริต) หรือส่วนที่ใช้ตรวจจับ (ออกแบบเพื่อให้สามารถค้นพบเหตุการณ์หรือรายการทุจริตหลังผ่านกระบวนการขั้นต้นที่นำไปสู่การทุจริต) การเลือกพัฒนานำมาใช้และตรวจติดตามกิจกรรมการควบคุมเพื่อการป้องกันและตรวจจับการทุจริตเป็นส่วนสำคัญของการบริหารความเสี่ยงด้านการทุจริต กิจกรรมการควบคุมการทุจริตเป็นเอกสารที่กำหนดวิธีปฏิบัติและผู้รับผิดชอบในการระบุความเสี่ยงและชนิดของการทุจริต กิจกรรมการควบคุมการทุจริตจึงเป็นส่วนหนึ่งขององค์ประกอบการบริหารความเสี่ยงด้านการทุจริตของการควบคุมภายใน

๒.๔ การสอบสวนการทุจริตและการแก้ไขปรับปรุง (Fraud Investigation and Corrective Action Component) กิจกรรมการควบคุมปกติไม่สามารถให้ความมั่นใจในเรื่องการทุจริตได้อย่างเต็มที่ผลคือคณะกรรมการฯ หรือผู้มีบทบาทในการกำกับ ดูแล ควรพิจารณาเพิ่มความมั่นใจโดยการพัฒนาและนำมาใช้ซึ่งระบบที่มีการสอบทานอย่างเป็นความลับ มีความรวดเร็ว บุคลากรมีความรู้ความสามารถและมีการสอบสวนเพื่อหาข้อสรุปเมื่อมีการละเมิดหรือการกล่าวหาเกี่ยวกับการกระทำผิด หรือการทุจริต ประโยชน์ที่ได้จากการสอบสวนยังช่วยให้องค์กรสามารถปรับปรุงเพื่อเพิ่มโอกาสในการเรียกทรัพย์สินที่เสียไปคืนมาลดความเสี่ยงในด้านพิธีการทางกฎหมายหรือชื่อเสียงเสียหายโดยการจัดตั้งและจัดเตรียมแผนอย่างระมัดระวังองค์กรจัดตั้งและสื่อสารโปรแกรมการบริหารความเสี่ยงเพื่อแสดงความคาดหวังของคณะกรรมการบริษัทและผู้บริหารระดับสูงถึงความมุ่งมั่นในคุณค่าของความซื่อตรงและจริยธรรมในการบริหารความเสี่ยงด้านการทุจริต

๒.๕ กิจกรรมตรวจติดตามการบริหารความเสี่ยงด้านการทุจริต (Fraud Risk Management Monitoring Activities Component) ถูกใช้เพื่อให้มั่นใจว่าหลักการแต่ละหลักการของการบริหารความเสี่ยงด้านการทุจริตมีอยู่และเกิดผลในเชิงปฏิบัติตามที่ได้ออกแบบมาและยังสามารถระบุการเปลี่ยนแปลงเมื่อเกิดความจำเป็นได้อย่างทันท่วงที

หัวข้อที่ ๒ การตรวจสอบด้านการกำกับ ดูแล

บรรยายโดย อาจารย์ไพรัช ศรีวิไลฤทธิ์ ผู้ช่วยกรรมการผู้จัดการใหญ่อาวุโส สายงานการกำกับ ดูแล กิจการและเลขานุการ บริษัท ทิสโก้ไฟแนนเชียลกรุ๊ป จำกัด (มหาชน)

มาตรฐานการตรวจสอบภายในที่เกี่ยวข้อง

NEW Global Internal Audit Standards ของ International Professional Practices Framework (IPPF) ๒๐๒๔

Domain I. จุดมุ่งหมายของงานตรวจสอบภายใน

ถ้อยแถลงเกี่ยวกับจุดมุ่งหมายของงานตรวจสอบภายใน

การตรวจสอบภายในเสริมความเข้มแข็งให้องค์กรในเรื่อง

- การสร้าง ปกป้อง และดำรงคุณค่า
- กระบวนการกำกับดูแล บริหารความเสี่ยง และการควบคุม
- การตัดสินใจและบังคับบัญชา
- ชื่อเสียงและความน่าเชื่อถือต่อผู้มีส่วนได้เสีย

- ความสามารถในการยังประโยชน์แก่ส่วนรวมขององค์กร

Domain II. จริยธรรมและความเป็นมืออาชีพ

- Standard ๔.๒ ความระมัดระวังเยี่ยงวิชาชีพ

ผู้ตรวจสอบต้องใช้ความระมัดระวังเยี่ยงวิชาชีพ โดยประเมินสถานการณ์ ข้อกำหนด ต้นทุน และประโยชน์ของบริการตรวจสอบที่จะมอบให้ ซึ่งรวมถึง

- กลยุทธ์และวัตถุประสงค์ขององค์กร
- ประโยชน์หรือส่วนได้เสียของผู้รับบริการ และผู้ที่เกี่ยวข้อง
- ความพอเพียงและประสิทธิผลของกระบวนการกำกับดูแล บริหารความเสี่ยง และการควบคุม

Domain IV. การบริหารจัดการหน่วยงานตรวจสอบภายใน

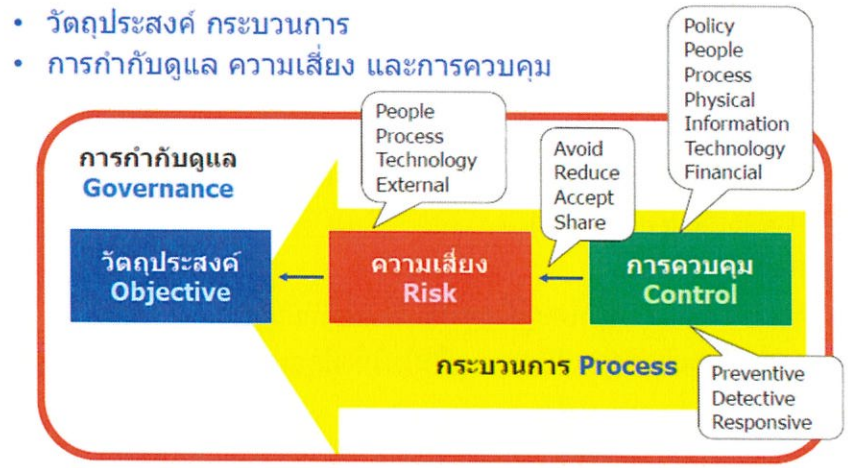
- Standard ๙.๑ ทำความเข้าใจกระบวนการ GRC

“เพื่อที่จะพัฒนากลยุทธ์และแผนการตรวจสอบ หัวหน้าหน่วยงานตรวจสอบภายใน ต้องทำความเข้าใจในกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุม (GRC) ขององค์กร”

“เพื่อที่จะเข้าใจ กระบวนการกำกับดูแล หัวหน้าหน่วยงานตรวจสอบภายใน ต้องพิจารณาถึงวิธีการที่องค์กร”

- กำหนดเป้าหมายเชิงกลยุทธ์ และตัดสินใจ
- กำกับการบริหารความเสี่ยงและการควบคุม
- ปลูกฝังจริยธรรมและวัฒนธรรมองค์กร
- บริหารผลงานและความรับผิดชอบ
- วางโครงสร้างการบริหารจัดการ
- สื่อสารข้อมูลความเสี่ยงและการควบคุม
- ประสานงานระหว่างคณะกรรมการ ผู้ให้ความเชื่อมั่นและฝ่ายบริหาร"

แนวคิดเรื่อง GRC



แนวคิดเรื่อง GRC ซึ่งย่อมาจาก:

G = Governance (ธรรมาภิบาล)

R = Risk (ความเสี่ยง)

C = Control (การควบคุม)

๑. Governance (**การกำกับดูแล**)

- เป็นพื้นฐานที่ช่วยให้องค์กรบรรลุ **วัตถุประสงค์** (Objective)
- ครอบคลุมการตั้งเป้าหมายอย่างชัดเจน และแน่ใจว่าการดำเนินงานสอดคล้องกับเป้าหมาย
- มีความรับผิดชอบ โปร่งใส และตรวจสอบได้

๒. Risk (**ความเสี่ยง**)

- เมื่อองค์กรมีวัตถุประสงค์ ก็จะต้องประเมิน **ความเสี่ยงที่อาจเกิดขึ้นระหว่างทาง**
- ความเสี่ยงมีแหล่งที่มา เช่น: People (บุคลากร) Process (กระบวนการ) Technology (เทคโนโลยี) **และ** External (ปัจจัยภายนอก)

แนวทางจัดการความเสี่ยง ได้แก่:

- Avoid = หลีกเลี่ยง
- Reduce = ลดระดับ
- Accept = ยอมรับ
- Share = กระจายความเสี่ยง เช่น ทำประกัน

๓. Control (**การควบคุม**)

คือ การตั้ง **มาตรการหรือระบบควบคุมภายใน** เพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ควบคุมในด้านต่าง ๆ เช่น: Policy, People, Process, Physical, Information, Technology, Financial

ประเภทของการควบคุม:

- Preventive ป้องกันไม่ให้เกิด
- Detective ตรวจจับเมื่อเกิด
- Responsive ตอบสนอง/แก้ไขหลังเกิด

๔. **กระบวนการ** (Process)

วงจรการจัดการทั้งหมดนี้ถือเป็น “**กระบวนการ**” ที่เกี่ยวเนื่องกัน เริ่มจาก **ตั้งวัตถุประสงค์ ⟶ ประเมินความเสี่ยง ⟶ วางการควบคุม** ↻ **ความเชื่อมโยง**

- Governance ช่วยกำหนด **วัตถุประสงค์**
- จากนั้นประเมิน Risk ที่อาจส่งผลกระทบ
- แล้วใช้ Control มาควบคุมความเสี่ยงนั้น เพื่อให้ยังคงบรรลุวัตถุประสงค์เดิมได้

สรุป :

GRC เป็นแนวคิดที่ใช้บริหารองค์กรอย่างมีประสิทธิภาพ โดยบูรณาการ **เป้าหมาย**, **ความเสี่ยง**, และ **การควบคุม** เข้าไว้ด้วยกันอย่างเป็นระบบ

การกำกับดูแลใน GRC

กระบวนการกำกับสอดส่องโดยผู้มีส่วนได้เสีย เพื่อให้มั่นใจว่า

- การกำหนดเป้าหมายที่ชัดเจน เป็นไปได้ มีคุณภาพ สอดคล้องกับกลยุทธ์ มีความสมดุล และคำนึงถึงความยั่งยืน
- การออกแบบกระบวนการ ตอบโจทย์ แก้ปัญหาได้อย่างตรงจุดและมีประสิทธิภาพ มีการนำทรัพยากร เครื่องมือ เทคโนโลยีและนวัตกรรม มาใช้อย่างคุ้มค่าและเหมาะสม
- มีการศึกษา ระบุ ประเมิน ตอบสนอง และวางหรือปรับปรุงมาตรการจัดการ ให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ รวมถึงมีการติดตามรายงานสถานะอยู่เสมอ

- มีการวางระบบการควบคุม เพื่อจัดการความเสี่ยงและช่วยเพิ่มโอกาสในการบรรลุเป้าหมาย และทุกองค์ประกอบของการควบคุมทำงานร่วมกันอย่างมีประสิทธิผล

- โครงสร้างและกลไกการกำกับดูแล-ภายใน-มีประสิทธิผล

การทำงานร่วมกันของ GRC

ความเข้าใจใน GRC มีความสำคัญต่องานตรวจสอบภายใน เพราะ GRC ต้องทำงานร่วมกันเสมอ

- **ขาด C** หรือ การควบคุม องค์กรจะล้มเหลว ไม่บรรลุเป้าหมายเกิดความผิดพลาด ทุจริต เสียหาย ร้องเรียน ปัญหาคุณภาพ

- **ขาด R** หรือ การบริหารความเสี่ยง องค์กรจะเต็มไปด้วยการควบคุมที่ล้าสมัยหรือไม่จำเป็น เทอะทะ ขาดประสิทธิภาพ ไม่พัฒนา มีต้นทุนและค่าใช้จ่ายสูง เกิดช่องโหว่ ไม่มีการคาดการณ์และป้องกันความเสี่ยง หมดทรัพยากรส่วนใหญ่ไปกับการแก้ปัญหา

- **ขาด G** หรือ การกำกับดูแล องค์กรจะไม่ตอบสนองความต้องการของสังคมและผู้มีส่วนได้เสีย ไม่สร้างคุณค่า เกิดปัญหาเดิม ๆ ซ้ำซาก ต่างคนต่างทำ ไม่ปรับตัว ผลงาน บุคลากร และวัฒนธรรมองค์กรจะถดถอยลงเรื่อย ๆ และถูกละเลยไม่ได้รับความสนใจจากผู้มีส่วนได้เสียในที่สุด

การกำกับดูแลมีในทุกระดับ

หลักของ Governance คือการขับเคลื่อนให้เกิด GRC ในทุกระดับ

- ประเทศ กฎหมาย รัฐบาล องค์กรอิสระ องค์กรภาคประชาสังคม

- อุตสาหกรรม กฎระเบียบ เกณฑ์ แนวปฏิบัติ องค์กรกำกับดูแลสภาอุตสาหกรรม องค์กรวิชาชีพ องค์กรคุ้มครองผู้บริโภค

- องค์กร การประชุมผู้ถือหุ้น ข้อบังคับ คณะกรรมการคณะกรรมการชุดย่อย นโยบาย ระเบียบ กฎบัตร ผู้สอบบัญชี งบการเงิน การเปิดเผยข้อมูล รายงานการประชุม รายงานประจำปี ช่องทางรับข้อร้องเรียน การจัดโครงสร้างองค์กร

- หน่วยงาน คณะอนุกรรมการ คณะทำงาน, supervisory review, การรายงาน การสอบทานโดยหน่วยงานกำกับตรวจสอบ

- กระบวนการ คู่มือ ระบบงาน การเก็บ log ไว้ตรวจ dashboard

- กิจกรรม การแบ่งแยกหน้าที่ การสอบทานงาน ทะเบียน ใบเสร็จ

นิยามของการกำกับดูแลที่ดี

แตกต่างไปขึ้นกับระดับและผู้ที่พิจารณา แต่อาจนิยามกว้าง ๆ ได้ว่า

- การกำกับดูแลที่ดี จะสร้างคุณค่าอย่างยั่งยืน และช่วยสร้างความเชื่อมั่นแก่ผู้มีส่วนได้เสีย

- เป็นการจัดโครงสร้างและความสัมพันธ์ ระหว่างผู้รับผิดชอบกระบวนการ ผู้ทำหน้าที่กำกับดูแล รวมถึงผู้มีส่วนได้เสียทั้งภายในและภายนอก

- มีการวางโครงสร้างในการกำหนดเป้าหมาย วิธีการไปสู่เป้าหมายนั้น และการติดตามผล

- มีการกำหนดกลไกเพื่อกำกับการบริหารจัดการ และการตัดสินใจของผู้รับผิดชอบ

- มีกลไกปลูกฝังวัฒนธรรมและจริยธรรม ที่เน้นพื้นฐานเรื่องความซื่อสัตย์ เป็นธรรม โปร่งใส มุ่งมั่นรับผิดชอบงานในบทบาทหน้าที่ และรับผิดชอบต่อผลการกระทำและตัดสินใจของตน

นิยามของการกำกับดูแลของกองทุนตลาดหลักทรัพย์

การกำกับดูแลกิจการ หมายถึง ความสัมพันธ์ในเชิงการกำกับดูแล รวมทั้งกลไกมาตรการที่ใช้กำกับการตัดสินใจของคนในองค์กรให้เป็นไปตามวัตถุประสงค์ ซึ่งรวมถึง

๑. การกำหนดวัตถุประสงค์และเป้าหมายหลัก

๒. การกำหนดกลยุทธ์ นโยบาย และพิจารณาอนุมัติแผนงานและงบประมาณ, และ

๓. การติดตามประเมิน และดูแลการรายงานผลการดำเนินงาน

การกำกับดูแลกิจการที่ดี หมายถึง การกำกับดูแลกิจการที่เป็นไปเพื่อการสร้างคุณค่าให้กิจการอย่างยั่งยืน นอกเหนือจากการสร้างความเชื่อมั่นให้แก่ผู้ลงทุน ซึ่งคณะกรรมการควรกำกับดูแลกิจการให้นำไปสู่ผลอย่างน้อยดังต่อไปนี้

๑. สามารถแข่งขันได้และมีผลประกอบการที่ดีโดยคำนึงถึงผลกระทบในระยะยาว

๒. ประกอบธุรกิจอย่างมีจริยธรรม เคารพสิทธิและมีความรับผิดชอบต่อผู้ถือหุ้นและผู้มีส่วนได้เสีย

๓. เป็นประโยชน์ต่อสังคม และพัฒนาหรือลดผลกระทบด้านลบต่อสิ่งแวดล้อม

๔. สามารถปรับตัวได้ภายใต้ปัจจัยการเปลี่ยนแปลง

นิยามของการกำกับดูแลของตลาดหลักทรัพย์

การกำกับดูแลกิจการ หมายถึง การบริหารจัดการบริษัทที่มีประสิทธิภาพ โปร่งใสตรวจสอบได้ และคำนึงถึงผู้มีส่วนได้เสียทุกฝ่าย ซึ่งการกำกับดูแลกิจการที่ดีจะช่วยเสริมสร้างประสิทธิภาพในการดำเนินธุรกิจขององค์กร โดยการเพิ่มขีดความสามารถในการแข่งขันทางธุรกิจและสร้างความเชื่อมั่นให้แก่ผู้ถือหุ้นในระยะยาว

หลักพื้นฐานการกำกับดูแลกิจการที่ดี ๕ ประการ ได้แก่

๑. ความซื่อสัตย์ คือ การบริหารจัดการด้วยความซื่อสัตย์สุจริตน่าเชื่อถือ และยึดมั่นในความถูกต้อง

๒. ความยุติธรรม คือ การปฏิบัติต่อผู้มีส่วนได้เสียขององค์กรอย่างเป็นธรรม

๓. ความโปร่งใส คือ การดำเนินงานที่มีการเปิดเผยข้อมูลอย่างโปร่งใสแก่ผู้ที่เกี่ยวข้องและสามารถตรวจสอบได้

๔. ความรับผิดชอบ คือ การปฏิบัติตามบทบาทหน้าที่ที่อยู่ในความรับผิดชอบของตนด้วยสติปัญญาและความสามารถอย่างเต็มกำลัง มุ่งมั่นให้งานสำเร็จและพัฒนางานให้ดีขึ้น

๕. ภาระรับผิดชอบ คือ ความรับผิดและรับชอบในผลของการกระทำที่เกิดขึ้น อันเนื่องจากการกระทำ การสั่งการ การมอบหมาย และการตัดสินใจ ตามบทบาทหน้าที่ของตนเอง โดยสามารถชี้แจงและอธิบายการตัดสินใจนั้นได้

หลักธรรมาภิบาลในการบริหารองค์กร

ประยุกต์ใช้ในการดำเนินงาน เพื่อส่งเสริมองค์กรให้มีศักยภาพและประสิทธิภาพสอดคล้องกับความรู้สึกและความต้องการของสาธารณะชนประกอบด้วยหลักสำคัญ ๖ ประการ

หลักนิติธรรม การตรากฎหมาย กฎระเบียบ ข้อบังคับต่าง ๆ ให้ทันสมัยและเป็นธรรม เป็นที่ยอมรับและถือปฏิบัติร่วมกันอย่างเสมอภาค ไม่เลือกปฏิบัติ

หลักคุณธรรม การยึดมั่นในความถูกต้องดีงาม สร้างค่านิยมสำนึกในหน้าที่ซื่อสัตย์ มีระเบียบวินัย เสียสละ อดทนขยันหมั่นเพียร และเคารพสิทธิผู้อื่น

หลักความโปร่งใส สร้างความไว้วางใจ มีการให้และรับข้อมูล ที่สะดวก เป็นจริง ทันการณ์ เท่าเทียม มีระบบตรวจสอบและประเมินผลที่มีประสิทธิภาพ

หลักการมีส่วนร่วม เปิดให้ประชาชนมีส่วนร่วมรับรู้ และเสนอความเห็นในการตัดสินใจสำคัญ ๆ ของสังคม สร้างความสามัคคีและความร่วมมือกันในสังคม

หลักความรับผิดชอบ ตั้งใจปฏิบัติภารกิจตามหน้าที่ รับผิดชอบต่อความบกพร่องในหน้าที่ที่ตนรับผิดชอบ และพร้อมที่จะปรับปรุงแก้ไข

หลักความคุ้มค่า บริหารจัดการและใช้ทรัพยากรที่มีจำกัดอย่างคุ้มค่า เพื่อให้เกิดประโยชน์สูงสุดแก่ส่วนรวม

บทบาทและความรับผิดชอบ

การกำกับดูแลองค์กร เป็นบทบาทหลักและความรับผิดชอบของคณะกรรมการ ในการกำหนด กำกับติดตาม และจัดการให้มีการเปิดเผยข้อมูลต่อผู้มีส่วนได้เสีย

บุคคลอื่นที่มีบทบาทสำคัญในกระบวนการกำกับดูแล

คือ ประธานคณะกรรมการและคณะกรรมการชุดย่อย

ผู้บริหารสูงสุดจากการแต่งตั้ง/เลือกตั้งขององค์กรภาครัฐ

ผู้บริหารสูงสุดในสายงานกำกับดูแล สายงานทรัพยากรบุคคลสายงานจริยธรรมและจรรยาบรรณ สายงานบริหารความเสี่ยงและการควบคุมภายใน สายงานกำกับการปฏิบัติตามกฎเกณฑ์และสายงานตรวจสอบภายใน

การตรวจสอบการกำกับดูแลองค์กร

๑. ศึกษามาตรฐาน กรอบ โมเดล แนวทาง หลักเกณฑ์ กฎระเบียบ และหลักการกำกับดูแลที่ดีที่เหมาะสม หรือกำหนดไว้สำหรับองค์กร ในลักษณะ ประเภทธุรกิจ หรืออุตสาหกรรมเดียวกัน

๒. ระบุสิ่งที่องค์กรปฏิบัติอยู่ และประเมินว่ากระบวนการกำกับดูแลขององค์กรมีระดับวุฒิภาวะ (Maturity Level) อยู่ในระดับใด

โครงสร้างการกำกับดูแล ตลอดจนรายละเอียดของกระบวนการและวิธีปฏิบัติซึ่งอาจแตกต่างกันได้ตามประเภท ขนาด ความซับซ้อน โครงสร้าง และระดับวุฒิภาวะของกระบวนการ รวมถึงกฎระเบียบที่บังคับใช้กับองค์กร

ศึกษากฎบัตร วาระ และรายงานการประชุม คณะกรรมการและคณะกรรมการชุดย่อย เพื่อเข้าใจบทบาทของคณะกรรมการ/ฝ่ายบริหาร ในกระบวนการกำกับดูแลและการตัดสินใจขององค์กร

สัมภาษณ์ผู้มีบทบาทหลักในกระบวนการกำกับดูแล

ศึกษารายงานหรือผลการประเมินการกำกับดูแลองค์กร และต้องทำควบคู่ไปกับการตรวจสอบด้านจริยธรรมและวัฒนธรรม

การประเมินวุฒิภาวะกระบวนการธุรกิจ

คำอธิบายระดับวุฒิภาวะ (Maturity Level) ตาม CMMI (Capability Maturity Model Integration) แบ่ง**ออกเป็น ๕ ระดับ**

*วุฒิภาวะระดับ ๑ - เริ่มต้น: Initial ยังไม่มีกระบวนการ หรือมี แต่เป็นกระบวนการแบบเฉพาะกิจและวุ่นวาย การจัดการยังเน้นแก้ไขปัญหาเฉพาะหน้า ไม่สม่ำเสมอ คาดการณ์ไม่ได้ ล่าช้า ต้นทุนสูง คุณภาพต่ำ

*วุฒิภาวะระดับ ๒ - มีการจัดการ: Repeatable กำหนดแนวปฏิบัติเพียงบางกระบวนการหรือโครงการ การจัดการยังขาดหน่วยงานรับผิดชอบชัดเจน

* วุฒิภาวะระดับ ๓ - กำหนด: Defined กำหนดกระบวนการหลักได้และมีการควบคุมเป็นมาตรฐานทั่วองค์กร เริ่มใช้ข้อมูลมาจัดการกระบวนการ

* วุฒิภาวะระดับ ๔ - จัดการเชิงปริมาณ: Managed มีมาตรวัดคุณภาพและสมรรถนะของกระบวนการที่ดี มีการเก็บข้อมูลอย่างสม่ำเสมอ และใช้ข้อมูลสถิติ ในการตั้งเป้าหมาย วางแผน ควบคุมและตัดสินใจ

* วุฒิภาวะระดับ ๕ - การเพิ่มประสิทธิภาพ: Optimizing มุ่งมั่นสู่ความเป็นเลิศ องค์กรปรับปรุงสมรรถนะการบริหารจัดการอย่างต่อเนื่อง ยึดแนวปฏิบัติที่ดีสร้างนวัตกรรม เพิ่มประสิทธิภาพ สามารถคาดการณ์และปรับตัวรับความเปลี่ยนแปลงได้

ตัวอย่างระดับวุฒิภาวะของ GRC ที่มา : Gartner

Maturity Level	การตัดสินใจ (Decision-Making Style)	ผลลัพธ์ธุรกิจ (Business Outcomes)	การวางแผนกลยุทธ์ (Strategic Planning)	ความเป็นผู้นำ (Leadership Style)	บริหารความเสี่ยง (Risk Approach)	บริหารการเงินการคลัง (Fiscal Approach)
Level 1: None	ตัดสินใจแบบตามสะดวก มากกว่าจะทำอย่างรอบคอบหรือมีการประสานงาน	ตอบสนองการแข่งขันได้ช้า จัดการทรัพยากรไม่ดี ไม่โปร่งใส	แทบไม่มีการวางแผนเชิงกลยุทธ์เลย หรือมีก็น้อยมาก	ลีเส้น ไม่แทรกแซงงานคนอื่นหรือข้ามสายงาน	ละเว้นหรือปฏิเสธความเสี่ยง	กระจายงบประมาณโดยไม่มีการควบคุมจากส่วนกลางหรือการควบคุมอ่อนแอ
Level 2: Isolated Competency	การตัดสินใจเป็นไปอย่างรอบคอบเฉพาะกรณีวิกฤตหรือความเสี่ยงสูง	ประสิทธิภาพปรับปรุงดีขึ้นเฉพาะในขอบเขตบางพื้นที่ในองค์กรเท่านั้น	มุ่งเน้นระยะสั้น และจำกัดขอบเขตเพียงโครงการสำคัญเท่านั้น	โฟกัสแต่เรื่องสำคัญหรือมีปัญหา และมอบหมายเรื่องที่เหลือให้ระดับล่างดูแล	ตอบสนองตอความเสี่ยงเมื่อจวนตัวจริงๆ เท่านั้น	จัดสรรเงินทุนให้แค่กับบางหน่วยหรือบางโครงการ
Level 3: Risk Mitigation	การตัดสินใจตามกรอบทรัพยากรหรือการปฏิบัติตามกฎระเบียบ	ลดต้นทุนและลดการสิ้นเปลืองทรัพยากร มีการปฏิบัติตามกฎระเบียบที่ดีขึ้น	มีแผนกลยุทธ์ แต่เพื่อตอบสนองแค่เหตุการณ์หรือเงื่อนไขที่เฉพาะเจาะจง	เน้นที่การควบคุมและระมัดระวัง รอบคอบ โดยแทบไม่มอบหมายงานให้ผู้อื่น	ระบุและจัดการความเสี่ยงเชิงรุก สำหรับต้นทุน การปฏิบัติตามกฎระเบียบ และความต่อเนื่องปลอดภัย	ทำบัญชีและควบคุมต้นทุนอย่างละเอียดเข้มงวด โดยไม่เน้นความคล่องตัวของงบประมาณ
Level 4: Benefit Optimization	กระบวนการตัดสินใจถูกขับเคลื่อนจากบนสู่ล่าง โดยมีกลยุทธ์และหลักการที่ชัดเจน	คาดการณ์ ROI และการเติบโตได้ และวัดผลการปรับปรุงการดำเนินงานได้	แผนกลยุทธ์มุ่งเน้นระยะยาว โดยใช้ประโยชน์จากการประสานการทำงานร่วมกันทั่วองค์กร	กระจายอำนาจโดยให้ลำดับความสำคัญและคำแนะนำอย่างชัดเจนแก่ระดับล่าง	ยอมรับความเสี่ยงและจัดการความเสี่ยงทางธุรกิจ ตามแบบจำลอง ROI	บริหารจัดการ IT Portfolio โดยแบ่งตามระดับ Run / Grow / Transform
Level 5: Competitive Innovation	การตัดสินใจทำอย่างมีพลวัต (dynamic) และรวดเร็ว	สร้างนวัตกรรมใหม่ๆ และความได้เปรียบในทุกสภาวะการแข่งขันหรือเศรษฐกิจ	พลิกแพลงกลยุทธ์ได้อย่างรวดเร็วเพื่อตอบสนองการแข่งขัน	เน้นไปที่นวัตกรรม ทดลองสิ่งใหม่ๆ และแก้ไขปัญหา	ยินดียอมรับความเสี่ยงหลังจากคำนวณได้แล้ว เพื่อความได้เปรียบในการแข่งขัน	ใช้แนวทางธุรกิจเงินร่วมลงทุน (Venture capital) ในการบริหารจัดการด้านการเงิน

การสร้างวัฒนธรรมองค์กรที่เน้นจริยธรรม

ถือเป็นรากฐานสำคัญของการกำกับดูแลและการควบคุม

๑. ระบุคุณค่าหลักที่สนับสนุนวัฒนธรรมองค์กร เช่น ความซื่อสัตย์

๒. จัดทำคู่มือจรรยาบรรณและความประพฤติ ใช้เป็นแนวทาง

๓. ประเมินความเสี่ยงของการละเมิดจรรยาบรรณและทุจริต

๔. จัดทำนโยบายจริยธรรมและจรรยาบรรณธุรกิจเผยแพร่

๕. จัดฝึกอบรมเพื่อสร้างความตระหนักและหมั่นทบทวน

๖. เปิดช่องทางปรึกษา และแจ้งเบาะแสหรือเหตุต้องสงสัย

๗. รณรงค์เพื่อย้ำเตือนและยกระดับความใส่ใจด้านจริยธรรม

๘. ประเมินและปรับปรุงโปรแกรมจริยธรรมและวัฒนธรรมองค์กร

๙. ผู้บริหารระดับสูงเน้นย้ำความสำคัญของความซื่อสัตย์ และการปฏิบัติตามกฎหมายกฎระเบียบ และแสดงความมุ่งมั่นที่จะปลูกฝังวัฒนธรรมและจริยธรรม โดยกระทำตนเป็นตัวอย่าง

การตรวจสอบด้านจริยธรรมและวัฒนธรรม โดยหลักจะเป็นการตรวจสอบหลักฐานจากกระบวนการ เช่น

๑. มีเอกสารคุณค่าหลัก/คู่มือจรรยาบรรณ/นโยบายเกี่ยวกับความขัดแย้งทางผลประโยชน์ที่อนุมัติโดยคณะกรรมการ มีหลักฐานการเผยแพร่นโยบายคู่มือทั่วถึงทั้งองค์กร

๒. นโยบายจริยธรรม/จรรยาบรรณ สอดคล้องกับความเสี่ยง

๓. จำนวนผู้เข้าอบรมและผลสัมฤทธิ์การอบรม

๔. ทำแบบสำรวจภายในองค์กร ว่าบุคลากรรู้ว่ามีช่องทางแจ้งเบาะแสและมีความไว้วางใจว่าจะได้รับความคุ้มครองหรือไม่

๕. เบาะแสที่ได้รับแจ้งมีการสอบสวน ดำเนินการทางวินัย และแจ้งผลกลับให้ผู้แจ้งเบาะแสทราบ

๖. ประเมินประสิทธิผลของโปรแกรมรณรงค์ กิจกรรม และการสื่อสาร

๗. หลักฐานการสื่อสารจากผู้บริหารระดับสูงและคณะกรรมการ

๘. หลักฐานการประเมินและปรับปรุงโปรแกรมจริยธรรม

๙. คำวิจารณ์ ความคิดเห็น และข้อเสนอแนะ จากผู้มีส่วนได้เสีย/สาธารณะชน ข่าวธรรมาภิบาล คดีฟ้องร้อง

หัวข้อที่ ๓ การตรวจสอบด้านระบบการควบคุมภายในและการบริหารจัดการความเสี่ยง

บรรยายโดย อาจารย์พรศิริ ปุณเกษม อนุกรรมการตรวจสอบ สำนักงานเลขาธิการ

ความหมายของการตรวจสอบภายใน AUDIT / ASSURANCE DEFINITION คืออะไร

คือ การตรวจสอบภายในเป็นกิจกรรมที่ให้ความเชื่อมั่น และ ให้คำปรึกษาแก่องค์กรอย่างเที่ยงธรรม และเป็นอิสระ เพื่อเพิ่มคุณค่าในการปรับปรุงการดำเนินงานขององค์กรให้ดียิ่งขึ้น ช่วยให้องค์กรบรรลุวัตถุประสงค์ โดยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยงการควบคุม และการกำกับดูแล อย่างเป็นระบบและมีระเบียบ

โครงสร้างของ Global Internal Audit Standards™ หรือ "มาตรฐานการตรวจสอบภายในระดับสากล" ฉบับปรับปรุงล่าสุดของ สถาบันผู้ตรวจสอบภายในสากล (The IIA) ซึ่งประกาศใช้เมื่อ มกราคม ๒๐๒๔ และมีผลบังคับใช้ ๑ มกราคม ๒๐๒๕ (ปรับปรุงล่าสุด) ซึ่งประกอบด้วย **๕ องค์ประกอบหลัก ๑๕ หลักการ (Principles)** ที่เป็นกรอบแนวทางในการดำเนินงานของหน่วยงานตรวจสอบภายในอย่างมีประสิทธิภาพ ดังนี้

๑. PURPOSE - **วัตถุประสงค์**

- เป็นหัวใจสำคัญของมาตรฐาน
- เน้นบทบาทของการตรวจสอบภายในในการสร้างคุณค่าให้แก่องค์กร
- มุ่งเน้นการเสริมสร้างความเชื่อมั่น และการปรับปรุงกระบวนการดำเนินงาน

๒. ETHICS & PROFESSIONALISM - **จริยธรรมและความเป็นมืออาชีพ**

- กำหนดหลักจริยธรรมและพฤติกรรมที่พึงประสงค์ของผู้ตรวจสอบภายใน เช่น ความซื่อสัตย์ ความเป็นอิสระ ความลับ และความสามารถในการให้บริการอย่างมืออาชีพ
- เน้นย้ำจรรยาบรรณของวิชาชีพตรวจสอบภายใน

๓. GOVERNING - **ธรรมาภิบาล**

- ครอบคลุมบทบาทของผู้บริหารระดับสูงและคณะกรรมการในการสนับสนุนงานตรวจสอบภายใน
- ส่งเสริมความเป็นอิสระ การรายงานโดยตรง และการสนับสนุนทรัพยากรที่เหมาะสม (งบประมาณ)

๔. MANAGING – การบริหารจัดการงานตรวจสอบภายใน

- กล่าวถึงวิธีการบริหารงานตรวจสอบภายใน เช่น การจัดทำแผนงาน การบริหารความเสี่ยง การจัดสรรทรัพยากร

- การสร้างระบบคุณภาพและการพัฒนาอย่างต่อเนื่องของทีมตรวจสอบภายใน

๕. PERFORMING – การปฏิบัติงานตรวจสอบภายใน

- ครอบคลุมกระบวนการตั้งแต่การวางแผนงานตรวจสอบ การปฏิบัติงานภาคสนาม การสื่อสารผลการตรวจสอบ

- รวมถึงการติดตามผลการปรับปรุงของฝ่ายที่รับตรวจ

โครงสร้างของ Global Internal Audit Standards™ หรือ "มาตรฐานการตรวจสอบภายในระดับสากล" ประกอบด้วย ๕ องค์ประกอบ (Domains) และ ๑๕ หลักการ (Principles) ดังนี้

๕ องค์ประกอบ (Domains)	๑๕ หลักการ (Principles)
๑: วัตถุประสงค์และอำนาจหน้าที่ (Purpose of Internal Auditing and Foundational Principles)	กิจกรรมการตรวจสอบภายในจัดตั้งขึ้นเพื่อให้ความเชื่อมั่น (assurance) คำแนะนำ (insight) และค่านิยมเพิ่มพูน (foresight/value) โดยดำเนินการอย่างอิสระและเป็นกลาง
๒: จริยธรรมและความเป็นมืออาชีพ (Ethics and Professionalism) (๕ หลักการ)	หลักการที่ ๑ Demonstrate Integrity (แสดงความซื่อสัตย์) หลักการที่ ๒ Maintain Objectivity (รักษาความเป็นกลาง) หลักการที่ ๓ Demonstrate Competency (แสดงความสามารถ) หลักการที่ ๔ Exercise Due Professional Care (ใช้ความระมัดระวังอย่างมืออาชีพ) หลักการที่ ๕ Maintain Confidentiality (รักษาความลับ) ความขยันขันแข็งในการปฏิบัติ
๓: การกำกับดูแล ความเป็นอิสระและความเท่าเทียม (Governance, Independence, and Objectivity) (๓ หลักการ)	หลักการที่ ๖ Authorized by the Board (ได้รับอนุญาตจากคณะกรรมการ) หลักการที่ ๗ Positioned Independently (อยู่ในตำแหน่งที่เป็นอิสระ) หลักการที่ ๘ Overseen by the Board (อยู่ภายใต้การกำกับดูแลของคณะกรรมการ)
๔: การบริหารจัดการกิจกรรมการตรวจสอบภายใน (Managing the Internal Audit Function) (๔ หลักการ)	หลักการที่ ๙ Plan Strategically (วางแผนเชิงกลยุทธ์) หลักการที่ ๑๐ Manage Resources (บริหารจัดการทรัพยากร) หลักการที่ ๑๑ Communicate Effectively (สื่อสารอย่างมีประสิทธิภาพ) หลักการที่ ๑๒ Enhance Quality (เพิ่มประสิทธิภาพคุณภาพ)
๕: การปฏิบัติงานตรวจสอบภายใน (Performing Internal Audit Services) (๓ หลักการ)	หลักการที่ ๑๓: Plan Engagement Effectively (วางแผนการปฏิบัติงานอย่างมีประสิทธิภาพ) ๑๓.๑ Engagement Communication (มาตรฐาน ๑๓.๑ การสื่อสารการปฏิบัติงาน) ๑๓.๒ Engagement Risk Assessment (มาตรฐาน ๑๓.๒ การประเมินความเสี่ยงของการปฏิบัติงาน)

	๑๓.๓ Engagement Objectives and Scope (มาตรฐาน ๑๓.๓ วัตถุประสงค์และขอบเขตของการปฏิบัติงาน) ๑๓.๔ Evaluation Criteria (มาตรฐาน ๑๓.๔ เกณฑ์การประเมิน) ๑๓.๕ Engagement Resources (มาตรฐาน ๑๓.๕ ทรัพยากรการปฏิบัติงาน) ๑๓.๖ Work Program (มาตรฐาน ๑๓.๖ แผนการปฏิบัติงาน) หลักการที่ ๑๔: Conduct Engagement Work (ปฏิบัติงานตรวจสอบ) หลักการที่ ๑๕: Communicate Engagement Results and Monitor Action Plans (สื่อสารผลการปฏิบัติงานและติดตามแผนปฏิบัติการ)

การควบคุมภายใน คือ กระบวนการปฏิบัติงานที่ถูกกำหนดร่วมกันโดยคณะกรรมการ ผู้บริหาร บุคลากรขององค์กร ทุกระดับ เพื่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลต่อ **การบรรลุวัตถุประสงค์ ใน ๓ ด้าน** ต่อไปนี้

๑. ด้านการดำเนินงาน (ประสิทธิภาพและประสิทธิผลของการดาเนินงานและ ความปลอดภัยของทรัพย์สิน)

๒. ด้านรายงาน (ความน่าเชื่อถือของรายงานทั้งการเงินและไม่ใช่การเงิน)

๓. ด้านการปฏิบัติตามกฎระเบียบข้อบังคับที่เกี่ยวข้อง

ตามกรอบแนวคิดการควบคุมภายในของ COSO ๒๐๑๓ กำหนดองค์ประกอบการควบคุมภายในไว้ **๕ องค์ประกอบ** คือ

(๑) สภาพแวดล้อมของการควบคุม

(๒) การประเมินความเสี่ยง

(๓) กิจกรรมการควบคุม

(๔) สารสนเทศและการสื่อสาร

(๕) การติดตามผล

วิธีการปฏิบัติ อย่างเป็นขั้นตอน นำไปสู่ผลสำเร็จ แทรกอยู่ในแต่ละกระบวนการทำงานขององค์กร โดยเชื่อมโยงประสานกัน ให้มั่นใจว่าสิ่งที่ควรเกิดควรเป็น **จะเกิด และเป็น**ตามนั้น และสิ่งที่ไม่ควรเกิด **ก็ไม่ควรเกิด**

บทบาทของผู้ตรวจสอบภายในกับการควบคุมภายใน

ตามมาตรฐานสากลการปฏิบัติวิชาชีพการตรวจสอบภายใน ระบุบทบาทของการควบคุมในงานของผู้ตรวจสอบภายในคือ **ผู้ตรวจสอบภายในต้องสนับสนุนองค์กร ให้มีระบบการควบคุมอย่างมีประสิทธิผล โดยการประเมินประสิทธิภาพและประสิทธิผลเพื่อปรับปรุงอย่างต่อเนื่อง**

การประเมินความเพียงพอของการควบคุม

การควบคุมเพียงพอ หมายถึง การที่ฝ่ายจัดการได้วางแผนและจัดการในลักษณะที่ให้ความเชื่อมั่นอย่างสมเหตุผล ว่าฝ่ายจัดการได้ปฏิบัติงานอย่างมีประสิทธิภาพ ประหยัด บรรลุเป้าหมายและวัตถุประสงค์

ฝ่ายจัดการทุกระดับสามารถนำ COSO ๒๐๑๓ ไปใช้ได้ตั้งแต่ (๔ ขั้นตอนของระบบควบคุมภายใน)

Design ⟶ วางระบบ

Implement ⟶ นำไปใช้

Conduct ⟶ ดำเนินการควบคุม

Assess ⟶ ประเมินความมีประสิทธิภาพ

ตรวจสอบภายใน ประเมินระบบการควบคุม โดย

๑. กำหนดในแผนการตรวจสอบ

๒. ประเมินการออกแบบการควบคุม

๓. ประเมินการออกแบบการควบคุมในช่วงการทดสอบประสิทธิผล

๔. ประเมินประสิทธิผลระบบในภาคสนาม

การบรรลุวัตถุประสงค์ ๓ ด้าน ขององค์กร โดยเน้นที่ **วัตถุประสงค์ในการดำเนินงาน (Operations objectives)** ซึ่งเป็นเหตุผลพื้นฐานที่องค์กรดำรงอยู่ และสามารถแตกต่างกันไปขึ้นอยู่กับการตัดสินใจของผู้บริหารว่าจะดำเนินการอย่างไร ที่ไหน และควรมีผลการปฏิบัติงานอย่างไร

วัตถุประสงค์ในการดำเนินงานอาจเกี่ยวข้องกับ

- คุณภาพ (Quality)
- ผลิตภาพ (Productivity)
- นวัตกรรม (Innovation)
- ความพึงพอใจของลูกค้า (Customer satisfaction)

นอกจากนี้ การปกป้องทรัพย์สิน หรือการคุ้มครองและรักษาทรัพย์สิน ก็จัดอยู่ในหมวดหมู่ของวัตถุประสงค์ในการดำเนินงานเช่นกัน วัตถุประสงค์ในการดำเนินงานยังถูกแบ่งย่อยออกเป็น ๓ ด้านหลัก ซึ่งสอดคล้องกับภาพประกอบ:

- **Efficiency (ประสิทธิภาพ)**: เกี่ยวข้องกับการดำเนินงาน (Operational)
- **Effectiveness (ประสิทธิผล)**: อาจเกี่ยวข้องกับด้านการเงิน (Financial)
- **Safety (ความปลอดภัย)**: เกี่ยวข้องกับการปกป้องทรัพย์สิน (Safeguarding asset)

วัตถุประสงค์ของการรายงาน (Reporting Objectives) ซึ่งเป็นการเตรียมรายงานสำหรับองค์กรและบุคคลภายนอก เช่น ผู้มีส่วนได้เสีย รายงานเหล่านี้ แบ่งออกเป็น ๓ ประเภทหลัก ที่แสดงเป็นรูปฟันเฟืองที่เชื่อมโยงกัน

๑. Nonfinancial (ไม่ใช่ทางการเงิน) รายงานภายใน (Internal reporting) ถูกใช้โดยฝ่ายบริหารภายในองค์กร เพื่อช่วยในการตัดสินใจที่เกี่ยวข้องกับตัวชี้วัดประสิทธิภาพ การดำเนินงาน และกลยุทธ์

๒. Financial (ทางการเงิน) ไม่ได้ระบุรายละเอียดเฉพาะในภาพสำหรับส่วนนี้ แต่โดยทั่วไปหมายถึงรายงานที่เกี่ยวข้องกับข้อมูลทางการเงิน

๓. Internal or external (ภายในหรือภายนอก) รายงานภายนอก (External reports) มักจะถูกกำหนดโดยหน่วยงานกำกับดูแลภายนอกและหน่วยงานกำหนดมาตรฐาน

ตามกรอบแนวคิดการควบคุมภายในของ COSO ๒๐๑๓ กำหนดองค์ประกอบการควบคุมภายในไว้ ๕ องค์ประกอบ มีหลักการควบคุม รวมทั้งสิ้น ๑๗ หลักการ

COSO ๒๐๑๓ ประกอบด้วย ๕ องค์ประกอบ ๑๗ Principles (หลักการ) ดังนี้		
๕ องค์ประกอบ	**๑๗ หลักการ**	**อักษรย่อ**
๑. สภาพแวดล้อมการควบคุม (Control Environment) (๕ หลักการ)	๑. แสดงให้เห็นการมุ่งเน้นคุณค่าความซื่อสัตย์จริยธรรม จากท่าทีของคณะกรรมการและผู้บริหาร	CE๑
	๒. คณะกรรมการมีความเป็นอิสระจากฝ่ายบริหาร และทำหน้าที่กำกับดูแล (OVERSIGHT) และพัฒนาการดำเนินการด้านการควบคุมภายใน	CE๒
	๓. กำหนดโครงสร้าง อำนาจหน้าที่ และความรับผิดชอบ	CE๓

๕ องค์ประกอบ	๑๗ หลักการ	อักษรย่อ
	๔. แสดงให้เห็นความมุ่งมั่นต่อความรู้ความสามารถ	CE๔
	๕. บังคับให้มีความรับผิดชอบต่อผลการปฏิบัติงานตามหน้าที่	CE๕
๒. การประเมินความเสี่ยง (Risk Assessment) (๕ หลักการ)	๖. องค์กรกำหนดวัตถุประสงค์ไว้อย่างชัดเจนเพียงพอ เพื่อให้สามารถระบุและประเมินความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับการบรรลุวัตถุประสงค์ขององค์กร	RA๖
	๗. ระบุและวิเคราะห์ความเสี่ยง	RA๗
	๘. ประเมินความเสี่ยงจากการทุจริต	RA๘
	๙. ระบุและวิเคราะห์การเปลี่ยนแปลงที่มีนัยสำคัญ	RA๙
๓. กิจกรรมการควบคุม (Control Activities) (๓ หลักการ)	๑๐. เลือกและพัฒนากิจกรรมการควบคุม (Selects and develops control activities)	CA๑
	๑๑. เลือกและพัฒนาการควบคุมทั่วไปด้านเทคโนโลยี (Selects and develops general controls over technology)	CA๒
	๑๒. นำไปปฏิบัติโดยกำหนดเป็นนโยบายและวิธีปฏิบัติงาน (Deploys through policies and procedures)	CA๓
๔. สารสนเทศและการสื่อสาร (Information and Communication) (๓ หลักการ)	๑๓. การใช้ข้อมูลที่เกี่ยวข้อง (Uses relevant information)	IC๑
	๑๔. การสื่อสารภายในองค์กร (Communicates internally)	IC๒
	๑๕. การสื่อสารภายนอกองค์กร (Communicates externally)	IC๓
๕. กิจกรรมการติดตามผล (Monitoring Activities) (๒ หลักการ)	๑๖. การประเมินอย่างต่อเนื่อง และการประเมินโดยอิสระ (Conducts ongoing and/or separate evaluations)	MA๑
	๑๗. การประเมิน และการรายงานข้อผิดพลาดหรือส่วนที่แตกต่าง (Evaluates and communicates deficiencies)	MA๒

กิจกรรมการควบคุม (Control Activities) ซึ่งเป็นส่วนหนึ่งของการควบคุมด้านเทคโนโลยีสารสนเทศ (IT Control) โดยแบ่งออกเป็น ๒ ประเภทหลัก ได้แก่:

๑. การควบคุมคอมพิวเตอร์ทั่วไป (General Computer Control)

- **การเข้าถึง (Access / Operations)**: เกี่ยวข้องกับการควบคุมการเข้าถึงระบบคอมพิวเตอร์และการดำเนินงานต่าง ๆ
- **การจัดหา พัฒนา บำรุงรักษาระบบ (Application Acquisition and Maintenance)**: ครอบคลุมการควบคุมกระบวนการได้มา การพัฒนา และการบำรุงรักษาระบบแอปพลิเคชัน
- **การเปลี่ยนแปลง (Changes)**: เกี่ยวข้องกับการควบคุมการเปลี่ยนแปลงที่เกิดขึ้นกับระบบ
- **ความปลอดภัย (Cyber Security)**: เน้นการควบคุมด้านความปลอดภัยทางไซเบอร์

๒. การควบคุมแอปพลิเคชัน (Application Control)

- **Input (ข้อมูลเข้า)**: การควบคุมที่เกี่ยวข้องกับข้อมูลที่ป้อนเข้าสู่ระบบ
- **Processing (การประมวลผล)**: การควบคุมที่เกี่ยวข้องกับกระบวนการประมวลผลข้อมูลภายในแอปพลิเคชัน
- **Output (ผลลัพธ์)**: การควบคุมที่เกี่ยวข้องกับข้อมูลผลลัพธ์ที่ได้จากแอปพลิเคชัน

การควบคุมด้วยมือ (Manual Control) โดยเน้นที่หลักการ **การแบ่งแยกหน้าที่ (Segregation of Duties)** ซึ่งเป็นแนวคิดสำคัญในการควบคุมภายใน เพื่อลดโอกาสเกิดข้อผิดพลาด การฉ้อโกง หรือการทุจริต โดยแบ่งหน้าที่หลักออกเป็น ๓ ส่วน และมีการแยกย่อยดังนี้ RCA

- **Recording / Accounting (การบันทึก / การทำบัญชี)**
- **Reconciliation (การกระทบยอด)** เป็นกิจกรรมที่เกี่ยวข้องกับการตรวจสอบความถูกต้องของข้อมูลโดยการเปรียบเทียบข้อมูลจากแหล่งต่าง ๆ เพื่อให้มั่นใจว่าข้อมูลตรงกันและถูกต้อง
- **Custody (การดูแลรักษา / การเก็บรักษาทรัพย์สิน)**
- **Operation Responsibility (ความรับผิดชอบในการดำเนินงาน)** เกี่ยวข้องกับหน้าที่ในการดำเนินงานหรือจัดการทรัพย์สิน
- **System development (การพัฒนาระบบ)** เกี่ยวข้องกับการสร้างหรือปรับปรุงระบบที่อาจส่งผลต่อการดูแลรักษาทรัพย์สินหรือข้อมูล
- **Computer Operations (การดำเนินงานคอมพิวเตอร์)** เกี่ยวข้องกับการจัดการและการดำเนินงานระบบคอมพิวเตอร์ ซึ่งอาจเกี่ยวข้องกับการเข้าถึงข้อมูลหรือทรัพย์สิน
- **Authorization (การอนุมัติ)** :

ประเภทของการควบคุม มี ๓ ประเภท ดังนี้

ประเภทของการควบคุม	คำอธิบาย	ตัวอย่าง
Preventive Controls (การควบคุมเชิงป้องกัน)	ป้องกันรายการ เหตุการณ์ที่ไม่พึงประสงค์ ป้องกันเหตุผิดพลาดที่อาจเกิดขึ้น ก่อนเกิดข้อผิดพลาด (ป้องกันไม่ให้เกิดความผิดพลาดหรือทุจริตตั้งแต่ต้น)	การแยกหน้าที่, การอนุมัติล่วงหน้า, การกำหนดรหัสผ่าน
Detective Controls (การควบคุมเชิงตรวจพบ)	การตรวจสอบ/สอบทาน กรณีการควบคุมเชิงป้องกัน ไม่เป็นผลหรือโดนมองข้าม ก่อให้เกิดความผิดพลาด เพื่อการวางแนวทางแก้ไขต่อไป หลังเกิดข้อผิดพลาดแล้ว (ตรวจพบความผิดพลาดหรือความผิดปกติหลังจากเกิดขึ้น)	การกระทบยอดบัญชี, รายงานการตรวจสอบ, กล้องวงจรปิด
Corrective Controls (การควบคุมเชิงแก้ไข)	การควบคุมเพื่อแก้ไขเหตุการณ์เพื่อลดความผิดพลาดหรือผลกระทบเสียหายที่เกิดจากเหตุการณ์ รายการที่ผิดพลาด (แก้ไขข้อผิดพลาดที่เกิดขึ้นแล้ว เพื่อไม่ให้เกิดซ้ำ)	การปรับปรุงกระบวนการหลังการสอบทาน, การฝึกอบรมเพิ่มเติม

และอีก ๓ ประเภทของการควบคุมภายในเพิ่มเติม ได้แก่

ประเภทการควบคุม	ลักษณะเด่น	เป้าหมาย	ตัวอย่าง
Directive Control	แนะนำ/ชี้นำ	ให้ปฏิบัติถูกต้องตามแนวทาง	ทางม้าลาย, SOP
Compensating Control	ทดแทนการควบคุมหลักที่ขาด	คงไว้ซึ่งระดับการควบคุม	กล้องวงจรปิดแทนคนเฝ้า
Complementary Control	เสริมกันหลายชั้น	เพิ่มความแข็งแกร่งของระบบควบคุม	กล้อง + ยามรักษาการ

Transaction Processing Cycles หรือ วัฏจักรการประมวลผลรายการ หมายถึง กระบวนการหลักในการทำธุรกรรมขององค์กร ซึ่งถูกแบ่งออกเป็น วัฏจักร หรือ “รอบ” ตามลักษณะของกิจกรรมทางธุรกิจ โดยทั่วไปแบ่งออกเป็น ๔ วัฏจักรหลัก ดังนี้

๑. Revenue Cycle - วัฏจักรรายได้ คือ กระบวนการตั้งแต่การขายสินค้า/บริการ ไปจนถึงการเก็บเงินจากลูกค้า

ตัวอย่างระบบที่เกี่ยวข้อง เช่น ระบบขาย, ระบบบัญชีลูกหนี้ (AR), ระบบเงินสด

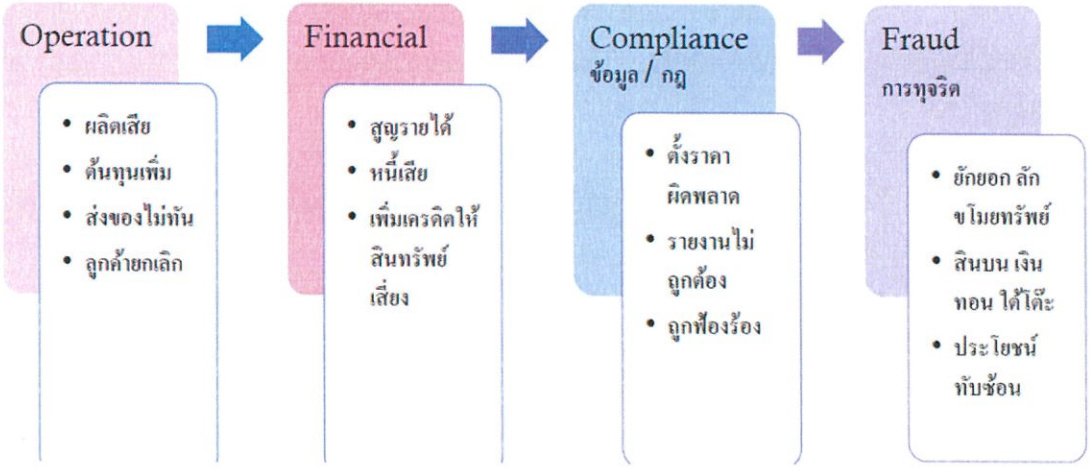
๒. Expenditure Cycle - วัฏจักรค่าใช้จ่าย คือ กระบวนการตั้งแต่การจัดซื้อวัสดุ อุปกรณ์ หรือบริการไปจนถึงการ

ชำระเงินให้กับผู้ขาย คือ ตัวอย่างระบบที่เกี่ยวข้อง เช่น ระบบจัดซื้อ, ระบบบัญชีเจ้าหนี้ (AP), ระบบคลังสินค้า

๓. Production Cycle - วัฏจักรการผลิต คือ: กระบวนการในการวางแผน ควบคุม และดำเนินการผลิตสินค้าหบริการ ตัวอย่างระบบที่เกี่ยวข้อง เช่น ระบบการผลิต (ERP), ระบบสินค้าคงคลัง, ระบบ BOM (Bill of Materials)

๔. Finance Cycle - วัฏจักรการเงิน คือ: กระบวนการบริหารจัดการด้านการเงินขององค์กร ทั้งด้านเงินทุน รายจ่าย และการวิเคราะห์การเงิน ตัวอย่างระบบที่เกี่ยวข้อง เช่น ระบบบัญชีแยกประเภททั่วไป (GL), ระบบงบประมาณ, ระบบวิเคราะห์ทางการเงิน

ความเสี่ยงหรือผลกระทบจากการควบคุมภายในที่ไม่เพียงพอและขาดประสิทธิผล



ข้อจำกัดของการควบคุมภายใน

การควบคุมภายในที่ดี ต้องอาศัยการมีระบบที่ดี มีบุคลากรที่ซื่อสัตย์และมีความสามารถ มีนโยบายและวิธีปฏิบัติงานที่เหมาะสม อย่างไรก็ตามการควบคุมภายในไม่อาจให้ความมั่นใจได้อย่างสมบูรณ์ เพียงให้ความเชื่อมั่นอย่างสมเหตุผลเท่านั้น ข้อจำกัดของการควบคุมภายใน มีดังนี้

๑. กิจการต้องการให้มีการควบคุมที่คุ้มค่า โดยมีต้นทุนที่ต่ำกว่าผลประโยชน์จากการลดความเสียหายที่อาจเกิด

๒. การควบคุมมีไว้สำหรับรายการที่คาดว่าจะเกิดตามปกติ

๓. ความผิดพลาดเกิดจากคนประมาท เข้าใจผิด หรือความไม่เข้าใจ

๔. การร่วมมือกันทุจริต หรือหลีกเลี่ยงระบบการควบคุมที่มีอยู่

๕. ผู้ปฏิบัติไม่ปฏิบัติตามระบบ หรือละเว้นการปฏิบัติ

๖. วิธีการควบคุมที่มีอยู่อาจไม่เหมาะกับสถานการณ์ที่เปลี่ยนไป

ประโยชน์ของการควบคุมภายใน

การควบคุมภายในที่ดี เป็นประโยชน์ช่วยเพิ่มคุณค่าให้องค์กร และเป็นประโยชน์ต่อฝ่ายต่าง ๆ ดังนี้

๑. ผู้บริหาร เกิดความมั่นใจในประสิทธิผลของการปฏิบัติงานให้บรรลุเป้าหมาย การปฏิบัติงานมีประสิทธิภาพ รายงานข้อมูลที่ได้รับมีความน่าเชื่อถือ และมั่นใจในความปลอดภัยของทรัพย์สินยิ่งขึ้น

๒. พนักงาน มีความมั่นใจในประสิทธิภาพของการปฏิบัติงาน

๓. ผู้ตรวจสอบภายใน และผู้สอบบัญชีภายนอก ใช้การประเมินการควบคุมภายใน ถ้าการควบคุมภายในเพียงพอและมีประสิทธิผล สามารถลดขอบเขตการตรวจสอบลงได้และเน้นการตรวจสอบเรื่องที่มีความเสี่ยงสำคัญได้มากขึ้น

คำอธิบายรหัสหมวดหมู่ COSO ๒๐๑๓:

- **CE** (Control Environment): สภาพแวดล้อมของการควบคุม (หลักการที่ ๑–๕)
- **RA** (Risk Assessment): การประเมินความเสี่ยง (หลักการที่ ๖–๙)
- **CA** (Control Activities): กิจกรรมการควบคุม (หลักการที่ ๑๐–๑๒)
- **IC** (Information & Communication): สารสนเทศและการสื่อสาร (หลักการที่ ๑๓–๑๕)
- **M** (Monitoring): การติดตามประเมินผล (หลักการที่ ๑๖–๑๗)

การบริหารความเสี่ยงจากมุมมองของฝ่ายบริหาร

Management Perspective - Key Concepts

- การระบุความเสี่ยง => สิ่งนี้เกี่ยวข้องกับการตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นซึ่งอาจส่งผลกระทบต่อวัตถุประสงค์ขององค์กร เทคนิคต่าง ๆ ได้แก่ การระดมความคิด การวิเคราะห์ SWOT และการทบทวนข้อมูลในอดีต

- การประเมินความเสี่ยง => เมื่อระบุแล้ว ความเสี่ยงจะได้รับการประเมินตามผลกระทบและความเป็นไปได้ที่อาจเกิดขึ้นซึ่งมักเกี่ยวข้องกับการวิเคราะห์เชิงคุณภาพและเชิงปริมาณ เช่น เมทริกซ์ความเสี่ยงหรือตารางกริดความน่าจะเป็น ผลกระทบ

- การจัดลำดับความสำคัญของความเสี่ยง => หลังจากการประเมินแล้ว ความเสี่ยงจะถูกจัดลำดับความสำคัญเพื่อมุ่งเน้นไปที่ภัยคุกคามที่สำคัญที่สุด ซึ่งช่วยในการจัดสรรทรัพยากรอย่างมีประสิทธิภาพเพื่อจัดการความเสี่ยงเหล่านี้

- การลดความเสี่ยง => มีการพัฒนากลยุทธ์เพื่อลดผลกระทบของความเสี่ยงให้เหลือน้อยที่สุด ซึ่งอาจรวมถึงการหลีกเลี่ยงความเสี่ยง ลดโอกาสหรือผลกระทบ การโอนความเสี่ยง (เช่น ผ่านการประกันภัย) หรือการยอมรับ

- การติดตามและการรายงานความเสี่ยง => การติดตามความเสี่ยงอย่างต่อเนื่องและประสิทธิผลของกลยุทธ์การบรรเทาผลกระทบถือเป็นสิ่งสำคัญ การรายงานอย่างสม่ำเสมอทำให้มั่นใจได้ว่าผู้มีส่วนได้ส่วนเสียจะได้รับแจ้งเกี่ยวกับสถานะความเสี่ยงและการเปลี่ยนแปลงใด ๆ ในสภาพแวดล้อมที่มีความเสี่ยง

- วัฒนธรรมความเสี่ยง => การสร้างวัฒนธรรมที่คำนึงถึงความเสี่ยงภายในองค์กร โดยที่พนักงานทุกระดับเข้าใจถึงความสำคัญของการบริหารความเสี่ยงและบทบาทของพวกเขาในนั้น

- การกำกับ ดูแล และการปฏิบัติตามข้อกำหนด => ตรวจสอบให้แน่ใจว่าแนวทางปฏิบัติในการบริหารความเสี่ยงสอดคล้องกับข้อกำหนดด้านกฎระเบียบและนโยบายองค์กร ซึ่งเกี่ยวข้องกับการจัดตั้งโครงสร้างการกำกับ ดูแล เช่น คณะกรรมการความเสี่ยง และการกำหนดบทบาทและความรับผิดชอบ

- การจัดการภาวะวิกฤติ => การพัฒนาแผนและขั้นตอนในการตอบสนองต่อเหตุการณ์ ความเสี่ยงเมื่อเกิดขึ้นอย่างมีประสิทธิผล ซึ่งรวมถึงแผนการสื่อสาร กลยุทธ์การกู้คืน และการวางแผนความต่อเนื่องทางธุรกิจ

- การบริหารความเสี่ยงเชิงกลยุทธ์ => บูรณาการการบริหารความเสี่ยงเข้ากับการวางแผนเชิงกลยุทธ์และกระบวนการตัดสินใจเพื่อให้แน่ใจว่าความเสี่ยงที่อาจเกิดขึ้นได้รับการพิจารณาในเป้าหมายและกลยุทธ์ระยะยาว

- เทคโนโลยีและเครื่องมือ => การใช้เทคโนโลยี เช่น ซอฟต์แวร์การจัดการความเสี่ยง เพื่อปรับปรุงกระบวนการ ระบุ การประเมิน การติดตาม และการรายงานความเสี่ยง

การบริหารความเสี่ยงจากมุมมองของการตรวจสอบภายใน

Internal Audit Perspective -Key Concepts

- การตรวจสอบตามความเสี่ยง => การตรวจสอบภายในได้รับการวางแผนและดำเนินการตามโปรไฟล์ความเสี่ยงขององค์กร ซึ่งหมายถึงการมุ่งเน้นทรัพยากรการตรวจสอบในพื้นที่ที่มีความเสี่ยงสูงสุดต่อองค์กร

- การประเมินการควบคุมภายใน => การประเมินประสิทธิผลของการควบคุมภายในที่ออกแบบมาเพื่อลดความเสี่ยง สิ่งนี้เกี่ยวข้องกับการทดสอบการออกแบบและประสิทธิภาพการทำงานของการควบคุม

- การประเมินความเสี่ยง => ผู้ตรวจสอบภายในจะทบทวนและตรวจสอบกระบวนการประเมินความเสี่ยงขององค์กรเพื่อให้แน่ใจว่าสามารถระบุและจัดลำดับความสำคัญของความเสี่ยงได้อย่างถูกต้อง

- บทบาทการให้ความเชื่อมั่นและที่ปรึกษา => ให้ความมั่นใจในกระบวนการบริหารความเสี่ยงและเสนอบริการให้คำปรึกษาเพื่อช่วยปรับปรุงแนวทางปฏิบัติในการบริหารความเสี่ยง

- การกำกับ ดูแล และการปฏิบัติตามข้อกำหนด => ตรวจสอบให้แน่ใจว่ากระบวนการบริหารความเสี่ยงเป็นไปตามกฎหมาย ข้อบังคับ และนโยบายภายในที่บังคับใช้ ซึ่งรวมถึงการประเมินโครงสร้างการกำกับ ดูแลด้านการบริหารความเสี่ยง

Internal Audit Perspective - Activities

- การวางแผน => การพัฒนาแผนการตรวจสอบตามการประเมินความเสี่ยงอย่างละเอียด ซึ่งรวมถึงการทำความเข้าใจวัตถุประสงค์เชิงกลยุทธ์ขององค์กรและระบุความเสี่ยงหลักที่อาจส่งผลกระทบต่อวัตถุประสงค์เหล่านี้

- การทบทวนกรอบการบริหารความเสี่ยง => ประเมินกรอบการบริหารความเสี่ยงโดยรวมเพื่อให้มั่นใจว่ามีการนำไปปฏิบัติอย่างครอบคลุมและมีประสิทธิผล ซึ่งรวมถึงการทบทวนนโยบาย ขั้นตอน และเครื่องมือบริหารความเสี่ยง

- การทดสอบการควบคุม => ดำเนินการทดสอบการควบคุมเพื่อตรวจสอบประสิทธิภาพในการลดความเสี่ยงที่ระบุ ซึ่งเกี่ยวข้องกับทั้งการออกแบบและการทดสอบประสิทธิภาพการปฏิบัติงาน

- การรายงาน => สื่อสารผลการตรวจสอบและข้อเสนอแนะไปยังฝ่ายบริหารและคณะกรรมการ ซึ่งรวมถึงการเน้นย้ำถึงช่องว่างหรือจุดอ่อนในกระบวนการบริหารความเสี่ยงและเสนอแนะการปรับปรุง

- การติดตามผล => ติดตามการดำเนินการตามคำแนะนำการตรวจสอบเพื่อให้แน่ใจว่าปัญหาที่ระบุได้รับการแก้ไขและลดความเสี่ยง

- การติดตามอย่างต่อเนื่อง => การประเมินสภาพแวดล้อมความเสี่ยงและการควบคุมภายในอย่างต่อเนื่อง ซึ่งเกี่ยวข้องกับการใช้การวิเคราะห์ข้อมูลและเครื่องมืออื่น ๆ เพื่อติดตามตัวบ่งชี้ความเสี่ยงหลักและควบคุมประสิทธิภาพอย่างต่อเนื่อง

- การมีส่วนร่วมของผู้มีส่วนได้ส่วนเสีย => ทำงานร่วมกับการบริหารความเสี่ยง การปฏิบัติตามกฎระเบียบ และหน้าที่อื่น ๆ เพื่อให้มั่นใจว่าแนวทางการประสานงานในการบริหารความเสี่ยงรวมถึงการสื่อสารอย่างสม่ำเสมอกับคณะกรรมการตรวจสอบและผู้บริหารระดับสูง

- การฝึกอบรมและการตระหนักรู้ => การส่งเสริมวัฒนธรรมที่ตระหนักถึงความเสี่ยงภายในองค์กรผ่านโปรแกรมการฝึกอบรมและการตระหนักรู้ ผู้ตรวจสอบภายในสามารถช่วยให้ความรู้แก่พนักงานเกี่ยวกับหลักการและแนวปฏิบัติในการบริหารความเสี่ยง

- การเปรียบเทียบ => การเปรียบเทียบแนวทางปฏิบัติในการบริหารความเสี่ยงขององค์กรกับมาตรฐานอุตสาหกรรมและแนวทางปฏิบัติที่ดีที่สุด เพื่อระบุประเด็นที่ต้องปรับปรุง

- บริการให้คำปรึกษา => ให้บริการให้คำปรึกษาแก่ฝ่ายบริหารในการบริหารความเสี่ยง เช่น วิธีการประเมินความเสี่ยง การออกแบบการควบคุม และกลยุทธ์การลดความเสี่ยง

เทคนิคการตรวจสอบภายใน

การประเมินความเสี่ยง

- วัตถุประสงค์ : เพื่อระบุและจัดลำดับความสำคัญของความเสี่ยงตามโอกาสและผลกระทบ
- เทคนิค : เมทริกซ์ความเสี่ยง, การวิเคราะห์ SWOT, บันทึกความเสี่ยงการประเมินการควบคุมภายใน
- วัตถุประสงค์ : เพื่อประเมินการออกแบบและประสิทธิผลของการควบคุมภายใน
- เทคนิค : ควบคุมการทดสอบ, บทสรุป, ควบคุมการประเมินตนเองการวิเคราะห์ข้อมูล
- วัตถุประสงค์ : เพื่อระบุแนวโน้ม, ความผิดปกติ, และปัญหาที่อาจเกิดขึ้นในข้อมูล
- เทคนิค : การทำเหมืองข้อมูล, การวิเคราะห์ทางสถิติ, การวิเคราะห์แนวโน้มการสุ่มตัวอย่าง
- วัตถุประสงค์ : เพื่อสรุปเกี่ยวกับประชากรโดยพิจารณาจากชุดย่อยของข้อมูล
- เทคนิค : การสุ่มตัวอย่าง, การสุ่มตัวอย่างแบบแบ่งชั้น, การสุ่มตัวอย่างแบบตัดสินการสัมภาษณ์และการสำรวจ
- วัตถุประสงค์ : เพื่อรวบรวมข้อมูลเชิงคุณภาพเกี่ยวกับกระบวนการ, การควบคุม, และความเสี่ยง
- เทคนิค : การสัมภาษณ์แบบมีโครงสร้าง, แบบสำรวจปลายเปิด, การสนทนากลุ่มการทำแผนที่กระบวนการ
- วัตถุประสงค์ : เพื่อทำความเข้าใจและบันทึกของกระบวนการและระบุจุดควบคุม (Flowchart)
- เทคนิค : ผังงาน, แผนภาพกระบวนการ, คำอธิบายการเล่าเรื่อง

บทสรุป

- วัตถุประสงค์ : เพื่อทำความเข้าใจผังกระบวนการและระบุจุดอ่อนในการควบคุม
- เทคนิค : ติดตามธุรกรรมตั้งแต่เริ่มต้นจนเสร็จสิ้น

ข้อสังเกต

- วัตถุประสงค์ : เพื่อตรวจสอบการมีอยู่และการทำงานของการควบคุมโดยดูการทำงานจริง
- เทคนิค : การสังเกตนอกสถานที่, การแชโดว์พนักงานการเปรียบเทียบ
- วัตถุประสงค์ : เพื่อเปรียบเทียบกระบวนการและการควบคุมขององค์กรกับแนวทางปฏิบัติที่ดีที่สุดหรือมาตรฐานอุตสาหกรรม
- เทคนิค : การเปรียบเทียบประสิทธิภาพ, การทบทวนแนวทางปฏิบัติที่ดีที่สุด

การวิเคราะห์สถานการณ์

- วัตถุประสงค์ : เพื่อประเมินว่าสถานการณ์ต่าง ๆ อาจส่งผลกระทบต่อโปรไฟล์ความเสี่ยงขององค์กรอย่างไร
- เทคนิค : การทดสอบความเครียด, การวิเคราะห์ความไว, การวิเคราะห์ “จะเป็นอย่างไร”

การประเมินความเสี่ยงจากการทุจริต

- วัตถุประสงค์ : เพื่อระบุพื้นที่ที่อาจเกิดการฉ้อโกง

- เทคนิค : แบบสอบถามความเสี่ยงจากการฉ้อโกง, แบบจำลองการตรวจจับการฉ้อโกง, การวิเคราะห์ทางนิติวิทยาศาสตร์

การทดสอบการปฏิบัติตามข้อกำหนด

- วัตถุประสงค์ : เพื่อให้มั่นใจว่ามีการปฏิบัติตามกฎหมาย, ข้อบังคับ, และนโยบายภายใน

- เทคนิค : รายการตรวจสอบการปฏิบัติตามข้อกำหนด, การตรวจสอบข้อกำหนดด้านกฎระเบียบ, การทดสอบการปฏิบัติตามนโยบาย

หัวข้อที่ ๔ การให้บริการให้คำปรึกษา

บรรยายโดย อาจารย์ฉันทนา สืบสิน (ภาคเอกชน CIA)

การบริการให้ความเชื่อมั่น

- เกี่ยวกับหน่วยงาน/องค์กร การปฏิบัติงาน หน้าที่ กระบวนการ ระบบงาน หรือเรื่องอื่นใดที่เป็นประเด็น
- ผู้ตรวจสอบภายในจะเป็นผู้กำหนดลักษณะและขอบเขตของงานแต่ละงานเอง
- โดยทั่วไปแล้วการบริการให้ความเชื่อมั่นจะมีผู้ที่เกี่ยวข้อง ๓ ฝ่าย คือ
  ๑) เจ้าของกระบวนการ
  ๒) บุคคลหรือกลุ่มบุคคลที่ทำการประเมินซึ่งก็คือ ผู้ตรวจสอบภายใน และ
  ๓) บุคคลหรือกลุ่มบุคคลที่ใช้ผลการประเมินซึ่งเรียกว่า ผู้ใช้

การบริการให้คำปรึกษา - CONSULTING SERVICES : อภิธานศัพท์

การบริการให้คำปรึกษา แนะนำ และบริการอื่น ๆ ที่เกี่ยวข้อง โดยลักษณะและขอบเขตของงานจะเป็นไปตามข้อตกลงที่ทำขึ้นร่วมกันกับผู้รับบริการและมีจุดประสงค์เพื่อเพิ่มคุณค่าให้กับหน่วยงานของรัฐ โดยการปรับปรุงกระบวนกำกับ ดูแล การบริหารความเสี่ยง และการควบคุม ของหน่วยงานของรัฐให้ดีขึ้น เช่น ให้คำปรึกษา แนะนำเรื่องความคล่องตัวในการดำเนินงานการออกแบบระบบงานวิธีการต่าง ๆ ในการปฏิบัติงาน และการฝึกอบรม เป็นต้น

- มีลักษณะเป็นการให้คำแนะนำ และโดยทั่วไป จะให้บริการก็ต่อเมื่อได้รับการร้องขอจากผู้รับบริการเป็นการเฉพาะ
- ลักษณะและขอบเขตของงานการให้คำปรึกษาจะขึ้นอยู่กับข้อตกลงกับผู้รับบริการ
- มีผู้ที่เกี่ยวข้อง ๒ ฝ่าย คือ
  ๑) บุคคลหรือกลุ่มบุคคลที่เป็นผู้ให้คำปรึกษาซึ่งก็คือผู้ตรวจสอบภายใน และ
  ๒) บุคคลหรือกลุ่มบุคคลที่แสวงหาและรับคำปรึกษา ซึ่งก็คือผู้รับบริการ
- ผู้ตรวจสอบภายในควรรักษาความเที่ยงธรรม และไม่เข้าไปรับหน้าที่เป็นผู้บริหารเสียเอง

มาตรฐานวิชาชีพที่เกี่ยวข้อง

๑๐๐๐ - วัตถุประสงค์ อำนาจและภาระหน้าที่

๑๐๐๐.C๑ - ต้องกำหนดลักษณะของบริการให้คำปรึกษาไว้ในกฎบัตรของหน่วยงานตรวจสอบภายใน

๑๑๓๐ - การเสื่อมเสียความเป็นอิสระหรือความเที่ยงธรรม

๑๑๓๐.C๑ – ผู้ตรวจสอบภายในสามารถให้บริการด้านการให้คำปรึกษาในงานที่ตนเองเคยรับผิดชอบมาก่อนด้วยความเที่ยงธรรม

๑๑๓๐.C๒ - ในกรณีที่มีเหตุหรือข้อจำกัดในอันที่จะทำให้ผู้ตรวจสอบภายในไม่สามารถให้คำปรึกษาได้อย่างอิสระหรือความเที่ยงธรรม ผู้ตรวจสอบภายในต้องเปิดเผย เหตุหรือข้อจำกัดดังกล่าว ให้กับผู้มอบหมายงานหรือผู้รับบริการทราบก่อนจะยอมรับงานนั้น

๑๒๐๐ - ความเชี่ยวชาญและการใช้ความระมัดระวังในการประกอบวิชาชีพ

๑๒๐๐.C๑ - หัวหน้าหน่วยงานตรวจสอบภายในต้องไม่รับงานบริการให้คำปรึกษา หรือให้คำแนะนำและความช่วยเหลือ หากทีมงานขาดความรู้ ทักษะ และความสามารถอื่นที่จำเป็นในการปฏิบัติงานในเรื่องนั้น ๆ ไม่ว่าเพียงบางส่วนหรือทั้งหมด

๑๒๒๐ - ความระมัดระวังในทางวิชาชีพ

๑๒๒๐.C๑ - ผู้ตรวจสอบภายในต้องปฏิบัติงานบริการด้วยความระมัดระวังอย่างรอบคอบเยี่ยงผู้ประกอบวิชาชีพ โดยคำนึงถึงสิ่งต่อไปนี้

- ความต้องการและความคาดหวังของผู้มอบหมายงายและผู้รับบริการ ซึ่งรวมถึงลักษณะของเรื่องที่จะให้คำปรึกษาเวลาที่ใช้ในการปฏิบัติงานและการรายงานผลการตรวจสอบ
- ความซับซ้อนของของขอบเขตงานที่จาจเป็นเพื่อให้งานที่ได้รับ มอบหมายบรรลุผลสำเร็จตามวัตถุประสงค์
- ความคุ้มค่าของค่าใช้จ่ายที่เกิดขึ้นในการให้บริการคำปรึกษา เปรียบเทียบกับประโยชน์ที่คาดว่าหน่วยงานของรัฐจะได้รับ

๒๐๑๐ - การวางแผน

๒๐๑๐.C๑ - หัวหน้าหน่วยงานตรวจสอบภายใน ควรให้มีงานบริการให้คำปรึกษา เพื่อช่วยให้เกิดโอกาสในการปรับปรุง การบริหารจัดการความเสี่ยง การสร้างมูลค่าเพิ่ม และปรับปรุงการดำเนินงานของหน่วยงานของรัฐ ซึ่งต้องกำหนดงานบริการให้คำปรึกษาดังกล่าวไว้ในแผนการตรวจสอบด้วย

๒๑๒๐ - การบริหารความเสี่ยง บทตีความ

๒๑๒๐.C๑ - ระหว่างปฏิบัติงานการให้คำปรึกษา ผู้ตรวจสอบภายในต้องระบุ (Address - จัดการปัญหา) ความเสี่ยงที่สอดคล้องกับวัตถุประสงค์ของงานที่ได้รับมอบหมาย และต้องระมัดระวังความเสี่ยงอื่น ๆ ที่มีนัยสำคัญที่อาจเกิดขึ้นได้

๒๑๒๐.C๒ - ผู้ตรวจสอบภายใน ต้องนำเอาความรู้ในเรื่องของความเสี่ยงที่ได้รับจากการให้บริการให้คำปรึกษาไปใช้ในการประเมินกระบวนการบริหารความเสี่ยงของหน่วยงาน

๒๑๒๐.C๓ - การให้ความช่วยเหลือฝ่ายบริหารในการจัดให้มีหรือปรับปรุงกระบวนการบริหารความเสี่ยง ผู้ตรวจสอบภายในต้องพึงละเว้นการในส่วนของการดำเนินการซึ่งเป็นหน้าที่ความรับผิดชอบของฝ่ายบริหาร

๒๑๓๐ - การควบคุม

๒๑๓๐.C๑ - ผู้ตรวจสอบภายในต้องนำความรู้ในเรื่องของการควบคุมที่ได้รับจากการ ให้บริการให้คำปรึกษาไปใช้ในการประเมินผลการควบคุมของหน่วยงานของรัฐ

๒๒๐๐ - การวางแผนสำหรับงานที่ได้รับมอบหมาย

๒๒๐๑.C๑ – การปฏิบัติงานให้คำปรึกษาผู้ตรวจสอบภายในต้องทำความเข้าใจกับผู้รับบริการเกี่ยวกับ วัตถุประสงค์ ขอบเขต ความรับผิดชอบความคาดหวังอื่น ๆ ของผู้รับบริการในกรณีที่เป็นงานที่สำคัญต้องบันทึกความเข้าใจนี้ไว้เป็นลายลักษณ์อักษร

๒๒๑๐ - วัตถุประสงค์ของงานที่ได้รับมอบหมาย

๒๒๑๐.C๑ - วัตถุประสงค์ของงานให้คำปรึกษา ผู้ตรวจสอบภายในต้องคำนึงถึง (ใช้คำว่า Address ไม่ใช่ระบุ) กระบวนการกำกับ ดูแล การบริหารความเสี่ยง และการควบคุมโดยอยู่ภายในขอบเขตที่ได้ตกลงไว้กับผู้รับบริการ

๒๒๑๐.C๒ - วัตถุประสงค์ของงานให้คำปรึกษาต้องสอดคล้องกับการสร้างคุณค่า ยุทธศาสตร์และวัตถุประสงค์ หรือเป้าหมายของหน่วยงานของรัฐ

๒๒๒๐ - ขอบเขตของงานที่ได้รับมอบหมาย

๒๒๒๐.C๑ - ในการปฏิบัติงานให้คำปรึกษา ผู้ตรวจสอบภายในต้องมั่นใจว่าได้กำหนดขอบเขตของงานที่ได้รับมอบหมายไว้เพียงพอที่จะบรรลุวัตถุประสงค์ที่ได้ตกลงไว้ หากผู้ตรวจสอบภายในได้กำหนดเงื่อนไขเกี่ยวกับขอบเขตขึ้นมาในระหว่างการปฏิบัติงานจะต้องมีการหารือถึงเงื่อนที่ปรับปรุงนั้นกับผู้รับบริการว่าจะยังคงต้องการให้ปฏิบัติงานต่อไปหรือไม่

๒๒๒๐.C๒ - ในระหว่างการปฏิบัติงานให้คำปรึกษา ผู้ตรวจสอบภายในต้องระบุ (Address) การควบคุมที่สอดคล้องกับวัตถุประสงค์ของงานที่ได้รับมอบหมายและต้องระมัดระวังต่อประเด็นการควบคุมที่มีนัยสำคัญ

๒๒๔๐ - แนวการปฏิบัติงาน (Engagement Work Program) - ผู้ตรวจสอบภายในต้องพัฒนาและจัดทำแนวการปฏิบัติงานเป็นลายลักษณ์อักษร เพื่อให้การปฏิบัติงานบรรลุวัตถุประสงค์ที่กำหนด

๒๒๔๐.C๑ - แนวการปฏิบัติงานสำหรับงานการให้คำปรึกษาอาจมีรูปแบบและเนื้อหาที่แตกต่างกันไปขึ้นอยู่กับลักษณะของการปฏิบัติงาน

๒๓๓๐ - การจัดทำเอกสารข้อมูล

๒๓๓๐.C๑ - หัวหน้าหน่วยงานตรวจสอบ ต้องกำหนดนโยบายในการเก็บและรักษาบันทึกข้อมูลที่ได้จากการปฏิบัติงานให้คำปรึกษารวมทั้งการเผยแพร่ต่อบุคคลภายในและภายนอกหน่วยงานของรัฐ นโยบายเหล่านี้ต้องสอดคล้องกับแนวทางของหน่วยงานของรัฐ ระเบียบและหลักเกณฑ์ที่เกี่ยวข้อง

๒๔๑๐ - เกณฑ์สำหรับการสื่อสาร

๒๔๑๐.C๑ - การสื่อสารถึงความคืบหน้าและผลของงานให้คำปรึกษาอาจมีรูปแบบและเนื้อหาแตกต่างกันไป ขึ้นอยู่กับลักษณะของงานแต่ละงานและความต้องการของผู้รับบริการ

๒๔๔๐ - การเผยแพร่ผลการปฏิบัติงาน

๒๔๔๐.C๑ - หัวหน้าหน่วยงานตรวจสอบภายในเป็นผู้รับผิดชอบในการสื่อสารผลการให้บริการให้คำปรึกษาชุดสมบูรณ์ให้แก่ผู้รับบริการ

๒๔๔๐.C๒ - ระหว่างการให้บริการให้คำปรึกษาอาจมีการพบประเด็นเกี่ยวกับการกำกับ ดูแล การบริหารความเสี่ยง และการควบคุม หากประเด็นนั้น ๆ มีนัยสำคัญต่อองค์กร ผู้ตรวจสอบต้องรายงานให้ผู้บริหารระดับสูงและคณะกรรมการทราบ

๒๕๐๐ - การเฝ้าติดตามผล - หัวหน้าหน่วยงานตรวจสอบภายในต้องกำหนดและติดตามการปฏิบัติตามข้อเสนอแนะในรายงานการตรวจสอบ

๒๕๐๐.C๑ - หน่วยงานตรวจสอบภายในต้องมีการติดตามการปฏิบัติตามผลของการบริการให้คำปรึกษาตามขอบเขตการปฏิบัติงานที่ได้ตกลงไว้กับผู้รับบริการ

๔ TYPES OF CONSULTING SERVICE

Consulting Engagements are limited by the need of organization and the resources so long as they do not impair the independence of IA function or objectivity of internal auditors

There are ๔ types of Consulting Engagement :

๑. Advisory Consulting Engagement

๒. Training Consulting Engagement

๓. Facilitative Consulting Engagement

๔. Blended Engagement (Combining assurance and consulting service in a single audit can yield significant efficiencies for practitioners)

เหตุผลที่ต้องรับบริการจากที่ปรึกษา

- มีปัญหา ที่ต้องการแก้ไข
- มีข้อจำกัด ทำเองไม่ได้
- ต้องการความช่วยเหลือ
- ให้ช่วยแนะนำแนวทาง/วิธีการ
- แก้ปัญหา หรือ “หาทางออก”

คุณสมบัติที่สำคัญของผู้ตรวจสอบ

- เข้าใจ “การควบคุม” เป็นอย่างดี
- เข้าใจ และสามารถ วิเคราะห์ และ ระบุวัตถุประสงค์ของการควบคุมได้
- วิเคราะห์ Workflow/Flowchart
- ละเอียด รอบคอบ
- Positive and Logical Thinking

แนวทางในการเสนอให้บริการด้านที่ปรึกษา

- ประมวลประเด็นที่ตรวจพบ ที่เกิดขึ้นบ่อย เป็นประเด็นซ้ำ (CommonFinding)
- ประเด็นซ้ำของผู้ตรวจสอบภายนอก (ผู้ตรวจการ - สตง./ผู้สอบบัญชี)
- ข้อร้องเรียนซ้ำเกี่ยวกับการปฏิบัติงาน

DESIGNED TO ADD VALUE

“add value” The internal audit activities add value to organization (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management and control process

ปัญหา

เหตุการณ์/สิ่งที่เกิดขึ้นแล้วทำให้เกิด

- ความยุ่งยาก
- เสียหายต่อองค์กร
- ไม่ได้ผลตามที่คาดหวัง/วัตถุประสงค์
- ความผิดพลาด ล่าช้า

CONSULTING SERVICE GUIDELINE :

- หลักเกณฑ์ของงานที่ให้บริการได้
- ขั้นตอนการให้บริการ
- ผู้อนุมัติให้บริการ
- ความรับผิดชอบของผู้ตรวจสอบและหน่วยงานตรวจสอบภายใน
- การรายงานผล (รูปแบบ ผู้รับรายงาน)
- แบบฟอร์ม/กระดาษทำการต่าง ๆ ที่ใช้

ขั้นตอนการปฏิบัติงาน (ENGAGEMENT WORK PROGRAM)

บรรยายลักษณะของปัญหา : ระบุปัญหา (State the Problem) เป็นจุดเริ่มต้นที่สำคัญก่อนเข้าขั้นตอนหาแนวทางในการแก้ไข

- อะไรที่เป็นปัญหา
- ที่ไหน (สถานที่/พื้นที่ที่เกิดปัญหา)

- ลักษณะของ (รายการ) ที่เป็นปัญหา
- มากน้อยแค่ไหน
- เวลาที่เกิดรายการที่มีปัญหา
- ผู้เกี่ยวข้องกับรายที่ที่เกิดปัญหาเกี่ยวข้องอย่างไร
- รายการที่ไม่มีปัญหา
- ลักษณะรายการ เวลา ผู้เกี่ยวข้อง

หัวข้อที่ ๕ หลักการคิดวิเคราะห์สำหรับผู้ตรวจสอบภายใน (Analytical Thinking)

บรรยายโดยอาจารย์ ดร.เจษฎา ช.เจริญยิ่ง (ภาคเอกชน)

การเสริมสร้างทักษะการคิดอย่างเป็นระบบและการวิเคราะห์ (Enhancing Systematic Thinking and Analytical Skills)

ความสำคัญ (Key Words)

- Systematic Thinking การคิดอย่างเป็นระบบ มีลำดับ ขั้นตอน มีโครงสร้าง และมีตรรกะชัดเจน โดยพิจารณาทุกองค์ประกอบของปัญหา ความสัมพันธ์ระหว่างองค์ประกอบ

- System or Systemic Thinking การคิดอย่างเป็นระบบหรือเชิงระบบ (เรียบเรียง สรุป และถ่ายทอด)

- Analytical Thinking การคิดเชิงวิเคราะห์ (แยกแยะ) ข้อมูลหรือปัญหาออกเป็นส่วนย่อย ๆ เพื่อทำความเข้าใจ และหาสาเหตุ ที่แท้จริงของสิ่งที่เกิดขึ้นอย่างเป็นระบบ

- Synthesis or Synthetical Thinking การคิดเชิงสังเคราะห์หรือการสังเคราะห์ (การสรุป) กระบวนการทางความคิดที่เกี่ยวข้องกับการรวมเอาแนวคิดข้อมูลหรือองค์ประกอบย่อย ๆ ที่แตกต่างกันเข้าด้วยกัน เพื่อสร้างความเข้าใจใหม่หรือสิ่งใหม่ทั้งหมด

- Critical Thinking การคิดอย่างมีวิจารณญาณ กระบวนการคิดอย่างมีเหตุผลและหลักฐาน ในการวิเคราะห์ ตรวจสอบ และประเมินข้อมูลสถานการณ์ หรือข้อเสนอหลาย ๆ อย่างรอบด้าน

Top ๗ ทักษะที่ CAEs ต้องการ

Personal Skills ทักษะส่วนตัว

๑. Analytical/ critical thinking การคิดเชิงวิเคราะห์/วิจารณญาณ

๒. Communication การสื่อสาร

Technical Skills ทักษะทางเทคนิค

๑. Accounting บัญชี

๒. Risk Management assurance การประกันการจัดการความเสี่ยง

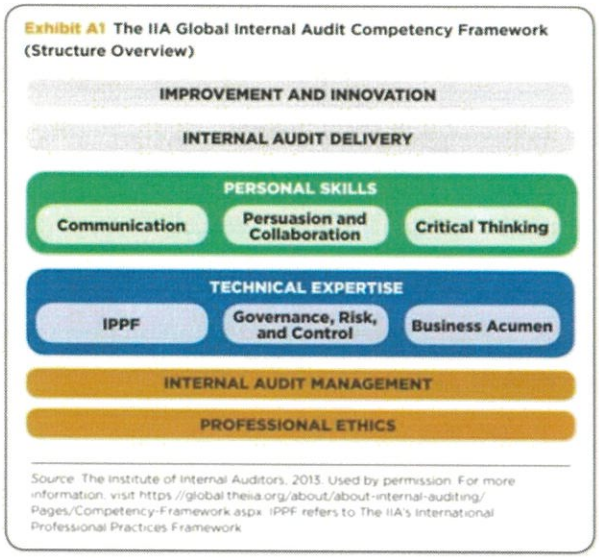
๓. Information technology (general) เทคโนโลยีสารสนเทศ (ทั่วไป)

๔. Industry-specific knowledge ความรู้เฉพาะด้านอุตสาหกรรม ความเข้าใจในข้อมูล แนวทางปฏิบัติเกี่ยวข้องกับสาขาหรือส่วนธุรกิจใดโดยเฉพาะ

๕. Data mining and analytics การวิเคราะห์และการทำเหมืองข้อมูล เป็นสองกระบวนการที่เกี่ยวข้องกันอย่างใกล้ชิดในการจัดการและใช้ประโยชน์จากข้อมูลขนาดใหญ่ เพื่อให้ได้ข้อมูลเชิงลึกที่มีค่าและสนับสนุนการตัดสินใจเชิงธุรกิจ

The Iia Global Internal Audit Competency Framework (Structure Overview) กรอบความสามารถในการตรวจสอบภายในระดับโลกของ IIA (โครงสร้าง)

The IIA Global Internal Audit Competency Framework encompasses the overall skills needs of the profession.



ครอบคลุมถึงความต้องการทักษะโดยรวมของวิชาชีพ

- การปรับปรุงและนวัตกรรม
- การส่งมอบงานตรวจสอบภายใน
- ทักษะส่วนบุคคล ๑. การสื่อสาร ๒. ความระมัดระวังและความร่วมมือทำงานเป็นทีม ๓. คิดอย่างมีวิจารณญาณ (มีเหตุผล)
- ทักษะเชี่ยวชาญด้านเทคนิค ๑. IPPF ๒. ควบคุม, ความเสี่ยง และการจัดการ ๓. เป้าหมาย/โครงสร้างขององค์กรเพื่อประโยชน์อะไร กฎหมาย ฯ
- การจัดการการตรวจสอบภายใน
- จริยธรรมวิชาชีพ

มาตรฐานที่เกี่ยวข้อง

มาตรฐาน ๒๓๐๐ - การปฏิบัติงานที่ได้รับมอบหมาย

ผู้ตรวจสอบภายในจะต้องระบุปัญหา (identify) วิเคราะห์ (analyze) ประเมินผล (evaluate) และบันทึก (document) ข้อมูล (information) อย่างเพียงพอเพื่อให้บรรลุวัตถุประสงค์ของงานได้

มาตรฐาน ๒๓๒๐ - การวิเคราะห์และประเมินผล ผู้ตรวจสอบภายในต้องสรุปผลการปฏิบัติงานโดยตั้งอยู่บนพื้นฐานของการวิเคราะห์และการประเมินที่เหมาะสม

Analytical Procedures

Practice Advisory ๒๓๒๐ - ๑ : วิธีการเชิงวิเคราะห์ (Analytical procedures)

๑. ผู้ตรวจสอบภายในอาจใช้วิธีการเชิงวิเคราะห์ในการค้นหาหลักฐานของการตรวจสอบวิธีการเชิงวิเคราะห์เป็นการศึกษาและเปรียบเทียบความสัมพันธ์ระหว่างทั้งข้อมูลทางการเงินและข้อมูลในทางการปฏิบัติงาน การใช้วิธีการเชิงวิเคราะห์นี้จะอยู่บนพื้นฐานที่ว่าในกรณีที่ไม่ทราบได้ถึงสถานการณ์ที่เป็นไปในทางตรงกันข้ามความสัมพันธ์ระหว่างข้อมูลก็ควรจะคาดได้ว่าน่าจะยังคงมีอยู่และต่อเนื่อง ตัวอย่างของสภาพการณ์ที่เป็นไปในทางตรงข้าม ได้แก่ รายการหรือเหตุการณ์ผิดปกติหรือไม่เกิดซ้ำ การเปลี่ยนแปลง

ทางบัญชีทางองค์กร ทางการปฏิบัติงานสิ่งแวดล้อมและเทคโนโลยี ความไม่มีประสิทธิภาพ ความไม่มีประสิทธิผล ความผิดพลาด การทุจริต หรือการกระทำผิดกฎหมาย เป็นต้น

๒. การตรวจสอบเชิงวิเคราะห์ จะช่วยทำให้ผู้ตรวจสอบภายในมีวิธีการที่มีประสิทธิภาพและประสิทธิผลในการหาหลักฐานที่เก็บรวบรวมได้จากการตรวจสอบ การประเมินผลที่ได้จากการเปรียบเทียบข้อมูลกับสิ่งที่คาดหวังไว้ซึ่งได้กำหนดหรือจัดทำขึ้นโดยผู้ตรวจสอบภายใน

วิธีการเชิงวิเคราะห์มีประโยชน์ในการค้นหาสิ่งต่าง ๆ เหล่านี้ :

- ผลต่างที่ไม่ได้คาดคิดว่าจะเกิด
- การไม่ปรากฏผลต่างตามที่ได้คาดไว้
- ข้อบกพร่อง หรือความผิดพลาดที่อาจเป็นไปได้
- การปฏิบัติที่ไม่ถูกต้องตามกฎระเบียบ หรือการกระทำผิดกฎหมายที่อาจเกิดขึ้นได้
- รายการ หรือเหตุการณ์ที่ไม่ปกติ หรือไม่เคยเกิด

๓. วิธีการตรวจสอบเชิงวิเคราะห์ ได้แก่ : การเปรียบเทียบข้อมูลในงวดปัจจุบันกับสิ่งที่คาดไว้โดยอาศัยข้อมูลทำนองเดียวกันของงวดก่อน หรือกับงบประมาณหรือสิ่งที่ได้พยากรณ์ไว้ การศึกษาความสัมพันธ์ของข้อมูลทางการเงินกับข้อมูลที่ไม่ได้เป็นตัวเงินที่เหมาะสมกัน (ตัวอย่าง เช่น ค่าใช้จ่ายเงินเดือนที่บันทึกไว้เปรียบเทียบกับการเปลี่ยนแปลงในจำนวนเฉลี่ยของพนักงาน) การศึกษาความสัมพันธ์ระหว่างองค์ประกอบของข้อมูล (ตัวอย่าง เช่น การเพิ่มขึ้นหรือลดลงของค่าใช้จ่ายดอกเบี้ยที่ได้บันทึกไว้ เปรียบเทียบกับการเปลี่ยนแปลงในยอดคงเหลือของภาระหนี้ที่เกี่ยวข้องกัน) การเปรียบเทียบข้อมูลขององค์กรกับสิ่งที่คาดโดยอาศัยข้อมูลทำนองเดียวกันกับของธุรกิจหรือของอุตสาหกรรมที่องค์กรประกอบกิจการอยู่

๔. วิธีการตรวจสอบเชิงวิเคราะห์ อาจจะทำโดยใช้หน่วยเงินตรา ปริมาณที่นับได้อัตราส่วนหรือเปอร์เซ็นต์ วิธีการตรวจสอบเชิงวิเคราะห์ที่เฉพาะเจาะจงบางอย่าง ได้แก่ อัตราส่วน แนวโน้ม และการวิเคราะห์เชิงถดถอย การทดสอบความสมเหตุสมผล การเปรียบเทียบงวดต่องวด การเปรียบเทียบกับงบประมาณ การพยากรณ์ และข้อมูลทางเศรษฐกิจภายนอก วิธีการตรวจสอบเชิงวิเคราะห์จะช่วยให้ผู้ตรวจสอบภายในในการระบุสภาพการณ์หรือต้องใช้วิธีการตรวจสอบอื่นที่จะตามมาภายหลัง ผู้ตรวจสอบภายในจะใช้วิธีการตรวจสอบเชิงวิเคราะห์ ในการวางแผนปฏิบัติงานโดยเป็นไปตามแนวทางที่มีอยู่ในมาตรฐาน ๒๒๐๐

๕. ในระหว่างการตรวจสอบ ผู้ตรวจสอบภายในอาจใช้วิธีการตรวจสอบเชิงวิเคราะห์เพื่อก่อให้เกิดหลักฐานสนับสนุนในระหว่างการปฏิบัติงานตรวจสอบในการกำหนดขอบเขตวิธีนี้ ผู้ตรวจสอบภายในควรจะพิจารณา

ปัจจัยที่จะกล่าวต่อไปนี้ :

- ความสำคัญของประเด็นที่ต้องตรวจสอบ
- การประเมินถึงกระบวนการบริหารความเสี่ยงของบริเวณที่กำลังได้รับการตรวจ
- ความเพียงพอของระบบการควบคุมภายใน
- ความพร้อม และความเชื่อถือได้ของข้อมูลทางการเงิน และข้อมูลที่ไม่ใช่ข้อมูลทางการเงิน

การวิเคราะห์

การวิเคราะห์ หมายถึง การจำแนกแยกแยะองค์ประกอบของสิ่งใดสิ่งหนึ่งออกเป็นส่วนเพื่อค้นหาว่าทำมาจากอะไร มีองค์ประกอบอะไรประกอบขึ้นมาได้อย่างไร เชื่อมโยงสัมพันธ์กันอย่างไร

ความหมายของการคิดเชิงวิเคราะห์ คือ ความสามารถในการจำแนกแจกแจงองค์ประกอบต่าง ๆ ของสิ่งใดสิ่งหนึ่งหรือเรื่องใดเรื่องหนึ่งและหาความสัมพันธ์เชิงเหตุผลระหว่างองค์ประกอบเหล่านั้น เพื่อค้นหาสาเหตุที่แท้จริงของสิ่งที่เกิดขึ้นการคิดเชิงวิเคราะห์เปรียบเหมือนการเห็น “ผลลัพธ์” ของบางสิ่ง แล้วไม่ด่วนสรุปทันที

ว่ามันเกิดจากสาเหตุใด มีองค์ประกอบใด มีความเป็นมาอย่างไร แต่พยายามหาข้อเท็จจริงที่ถูกต้องเสียก่อนว่าผลลัพธ์ที่เราเห็นนั้น เกิดจาก “สาเหตุที่แท้จริงคืออะไร” โดยมาจากสมมติฐานที่ว่า ทุกสิ่งที่เกิดขึ้นมานั้นย่อมมีที่มาที่ไป ย่อมมีเหตุมีผล และมีองค์ประกอบย่อย ๆ ซ่อนอยู่ภายใน ซึ่งอาจจะสอดคล้องหรือตรงกันข้ามกับสิ่งที่ปรากฏภายนอก ดังนั้น การจะเข้าใจสภาพที่แท้จริงจึงจำเป็นต้องมีการวิเคราะห์ เพื่อตอบคำถามว่า “สิ่งนี้เป็นมาจากอะไร และเพราะเหตุใดจึงเป็นเช่นนั้น” ก่อนที่เราจะสรุปความหรือตัดสินใจบางอย่างเกี่ยวกับเรื่องนั้น

Analytical thinking

การคิดวิเคราะห์ คือ ความสามารถในการพินิจพิเคราะห์และแยกแยะความจริงให้เข้าใจจุดแข็ง จุดอ่อน จุดเด่น จุดด้อย หรือ สาเหตุ รูปแบบ ของปัญหา หรือเหตุการณ์ หรือสถานการณ์ที่เกิดขึ้น

Importance to use

Synthesis thinking with Analytical thinking

- เมื่อเราวิเคราะห์ลงลึกในรายละเอียด ย่อมยากที่จะเข้าใจความสัมพันธ์ของกิจกรรมหรือปัจจัยที่เราวิเคราะห์

- เราจำเป็นต้องมีทั้ง การคิดแบบ Analysis and Synthesis Critical thinking Definition

Critical thinking

การคิดอย่างมีวิจารณญาณ is the ability to analyze facts, generate and organize ideas, defend opinion, make comparisons, draw inferences, evaluate arguments and solve problems (Chance, ๑๙๘๖ p.๖)

Problem Solving : Needed Skills

- Analytical and critical thinking skills
  - help you to evaluate the problem and to make decisions
- Solving the problems involves both analytical and creative skills
- Which particular skills are needed will vary, depending on the problem and your role in the organization, but the following skills are key to problem - solving :
- Analytical Ability
- Lateral Thinking การคิดที่แตกต่าง คิดนอกกรอบ หักมุมจากความคิดทั่วไป
- Initiative
- Logical Reasoning
- Persistence มีความวิริยะอุตสาหะ

Getting to the "Root" of the Problem

- Sometimes the thing we think is a problem is not the real problem, so to get at the real problem, probing is necessary
- Root Cause Analysis is an effective method of probing – it helps identify what, how, and why something happened
- Definition of root cause :
  - Specific underlying cause
  - Those that can reasonably be identified
  - Those that management has control to fix

Analytical Techniques

- Benchmarking - Compare and measure a process or activity against an internal or external source
- SWOT Analysis - Assessment of strengths, weaknesses, opportunities, and threats
- Cost Benefit Analysis - Compare total equivalent costs (all the minuses) against equivalent value in benefits (all the pluses)
- Impact Analysis - What if type analysis to assess the impact of change on an agency
- Pareto Chart - Bar Chart for categorizing issues or other attributes in terms of importance

Summary

- Analytical Thinking follows the Scientific Approach
- Five Step Process for improvement :
  - Define the Problem
  - Test in the form of Hypothesis
  - Focus on Facts
  - Analysis (Various Analytical Tools)
  - Recommend a Solution

<u>วิธีการนำเสนอเนื้อหาของวิทยากร</u>

เป็นการนำเสนอโดยวิธีบรรยายประกอบ Power Point

๔. สรุปข้อคิดเห็นประโยชน์ที่ได้รับและข้อเสนอแนะ หรือสิ่งที่คิดว่าจะนำมาปรับปรุงใช้ให้เป็นประโยชน์

๔.๑ ประโยชน์ที่ได้รับ

๔.๑.๑ ผู้ตรวจสอบภายใน มีความรู้ความเข้าใจในกระบวนการ เทคนิคและวิธีการตรวจสอบภายใน การกำกับ ดูแล การบริหารความเสี่ยง และการควบคุมภายใน (Governance, Risk Management and Control Audit Specialist) และสามารถนำไปปฏิบัติงานได้

๔.๑.๒ ได้แลกเปลี่ยนความรู้และประสบการณ์ในการปฏิบัติงานตรวจสอบกับผู้เข้ารับการฝึกอบรมหน่วยงานอื่น ๆ

๔.๑.๓ ได้รู้จักและมีเครือข่ายในการปฏิบัติงานเพิ่มขึ้นกับเพื่อนร่วมอาชีพเดียวกัน เจ้าหน้าที่ตรวจสอบภายใน เพื่อแชร์ประสบการณ์ หรือปัญหา และแนวทางแก้ไขของแต่ละพื้นที่ เพื่อเป็นกรณีศึกษาต่อไป

๔.๒ <u>ข้อเสนอแนะ</u> (เกี่ยวกับการพัฒนาบุคลากรในด้านนี้)

องค์กรควรสนับสนุนให้บุคลากรของกลุ่มตรวจสอบภายในทุกท่านได้รับความรู้ ความเข้าใจในเรื่องของการตรวจสอบภายในเฉพาะด้าน (Audit Specialist) ในหลักสูตรต่าง ๆ อย่างต่อเนื่อง เพื่อพัฒนาองค์ความรู้ ความสามารถ และปฏิบัติงานของผู้ตรวจสอบภายในให้มีประสิทธิภาพยิ่งขึ้น

๔.๓ <u>สิ่งที่คิดว่าจะนำมาใช้ในการปฏิบัติงานในภารกิจที่รับผิดชอบ</u> (โปรดระบุเป็นรายบุคคล)

นางทักษอร อินทุเศรษฐ

๑. ได้มีความรู้ความเข้าใจในการตรวจสอบด้านระบบการควบคุมภายในและการบริหารจัดการความเสี่ยงในมุมมองจากภาคเอกชน เพื่อนำมาปรับใช้ให้เข้ากับหน่วยงานภาครัฐ

๒. นำความรู้เรื่องการตรวจสอบทุจริต มาเป็นแนวทางในการปฏิบัติงานตรวจสอบการทุจริตของหน่วยงานต่อไป

๓. นำความรู้ในหัวข้อการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายใน (Governance, Risk Management and Control Audit Specialist) มาเป็นแนวทางในการตรวจสอบด้านการบริหารความเสี่ยง ตั้งแต่ขั้นตอนการวางแผนการตรวจสอบ การประเมินความเสี่ยง การปฏิบัติงานตรวจสอบ การรายงานผลการปฏิบัติ และการติดตาม

๔. นำความรู้เทคนิคการตรวจสอบด้านการบริหาร/การดำเนินงานมาเป็นแนวทางในการออกแบบการตรวจสอบและวิธีการรวบรวมหลักฐานการตรวจสอบภายใน การตั้งคำถามให้สอดคล้องกับวัตถุประสงค์เพื่อได้ข้อตรวจพบที่แสดงข้อเท็จจริงทั้งในด้านดีและที่ควรได้รับการแก้ไข วิธีการดำเนินการแก้ไข รวมทั้งความเห็นต่าง ๆ ให้หน่วยรับตรวจ

๕. ได้มีความรู้ความเข้าใจการให้บริการให้คำปรึกษา ทำให้ทราบถึงหลักเกณฑ์ของงาน ที่ให้บริการ ขั้นตอนการให้บริการ ผู้อนุมัติ ให้บริการ ความรับผิดชอบของ ผู้ตรวจสอบและหน่วยงานตรวจสอบภายใน การรายงานผล (รูปแบบ ผู้รับรายงาน) และแบบฟอร์ม/กระดาษทำการต่าง ๆ ที่ใช้มาเป็นแนวทางในการให้บริการให้คำปรึกษาภายในองค์กร

ลงชื่อ ..... ผู้รายงาน
(นางทักษอร อินทุเศรษฐ)
นักวิชาการตรวจสอบภายในชำนาญการ

๕. ความเห็นของผู้บังคับบัญชา (ระดับผู้อำนวยการกอง/สำนัก/เกษตรจังหวัด หรือเทียบเท่า ขึ้นไป)
ให้ผู้เข้าร่วมการฝึกอบรม นำความรู้ที่ได้ร่วม ปรับปรุง พัฒนางานต่อไป
.....
.....
.....
.....
.....
.....

(นางสาวบังเอิญ แก้วพระโต)
นักวิชาการตรวจสอบภายในชำนาญการพิเศษ
ปฏิบัติหน้าที่ผู้อำนวยการกลุ่มตรวจสอบภายใน