บันทึกข้อความ

ส่วนราชการ ฝ่ายตรวจสอบ ๒ กลุ่มตรวจสอบภายใน โทร. ๐๒-๕๙๐๔๑๐๒ โทรสาร. ๐๒-๕๙๐๔๑๐๑
ที่ สธ ๐๙๒๕.๐๓/ พิเศษ **วันที่** ๒๗ พฤษภาคม ๒๕๖๑
เรื่อง สรุปรายงานการอบรม CGIA หลักสูตร Advance ด้าน Performance Operation and Management

เรียน ผู้อำนวยการกลุ่มตรวจสอบภายใน (ผ่านหัวหน้าฝ่ายตรวจสอบ ๒)

ตามที่กลุ่มตรวจสอบภายใน ได้อนุมัติให้ดิฉัน เข้ารับการอบรมประกาศนียบัตรผู้ตรวจสอบภายในภาครัฐ (CGIA) หลักสูตร Advanced ด้าน Performance Operation and Management ครั้งที่ ๑ ในวันที่ ๑๙ – ๒๕ มีนาคม ๒๕๖๑ ณ โรงแรมนารายณ์ กรุงเทพฯ นั้น สรุปผลการเข้ารับการอบรม ดังนี้

- หัวข้อวิชา เทคนิคและเครื่องมือการบริหารจัดการ โดย ดร.บัญญัติ บุญญา

๑. การบริหารจัดการ (Good Governance) ได้แก่ การมีส่วนร่วมของสาธารณชน ความสุจริตและโปร่งใส พันธะความรับผิดชอบต่อสังคม กลไกทางการเมืองที่ชอบธรรม กฎเกณฑ์ที่ยุติธรรมและชัดเจน ประสิทธิภาพและประสิทธิผล

๒. ทำไมต้องมีการบริหารจัดการ (Good Governance) เนื่องจากโลกยุคโลกาภิวัฒน์ สังคมเศรษฐกิจเป็นยุคแห่งการเรียนรู้ งานของรัฐมากขึ้น ยากขึ้น รัฐเล็กลง ลดเงิน ลดคน ลดอำนาจ และที่สำคัญต้องเปิดให้มีส่วนร่วม ต้องโปร่งใส พร้อมถูกตรวจสอบ

๓. เครื่องมือการบริหารจัดการ ได้แก่ การปรับกลยุทธ์ต้องมีความชัดเจน การบริหารบุคคลควรมีการพัฒนาบุคลากรของหน่วยงานอยู่เสมอ การเรียนรู้และปรับปรุงอย่างต่อเนื่อง การใช้ IT ได้เกิดประโยชน์ การบริหารเวลา การบริหารต้นทุน

๔. องค์กรที่มุ่งเน้นยุทธศาสตร์ ประกอบด้วย

๔.๑ การบริหารกระบวนการ ได้แก่ การพัฒนาขั้นตอนการทำงานให้ดีขึ้น เพื่อให้เกิดประสิทธิภาพ (Efficiency) ได้แก่ การลดรอบระยะเวลาดำเนินการ ลดต้นทุนและความสูญเสีย การเพิ่มผลผลิต

๔.๒ กระบวนการบริหารลูกค้า ได้แก่ การดูแลผู้รับบริการ ความโปร่งใส และมีส่วนร่วมเพื่อให้เกิดคุณภาพ (Quality)

๔.๓ การวางระบบบริหารจัดการสินทรัพย์ที่จับต้องได้ ได้แก่ ทุนมนุษย์ ทุนข้อมูลสารสนเทศและทุนความรู้ ทุนองค์กร เพื่อให้เกิดขีดสมรรถนะ (Capacity building) และเพิ่มความพร้อมเชิงยุทธศาสตร์

ซึ่งทั้ง ๓ กระบวนการเป็นการบริหารการเปลี่ยนแปลง ก่อให้เกิดการเพิ่มคุณค่า (Value Creation) เกิดประสิทธิผล (Effectiveness)

๕. การบริหารมุ่งผลสัมฤทธิ์ (RBM) คือ ผลผลิต (Output) คือ การดำเนินการที่เกิดจากการจัดทำกิจกรรม และผลลัพธ์ (Outcome) คือ การดำเนินงานที่เกิดจากการนำผลผลิตไปใช้ ซึ่งทั้งผลผลิต และ ผลลัพธ์ ก่อให้เกิดผลสัมฤทธิ์ (Results)

๖. การจัดการเชิงกลยุทธ์ คือ การจัดการองค์การที่เน้น

๖.๑ การกำหนดวิสัยทัศน์ ภารกิจ กลยุทธ์ ซึ่งเป็นทิศทางขององค์กรในระยะยาวให้ สอดคล้องกับสภาพแวดล้อมทั้งภายนอก สภาพการณ์ภายในองค์การ ชัดเจน เป็นที่เข้าใจ ยอมรับทั่วกัน

๖.๒ การดำเนินการปรับทุกส่วนขององค์การเพื่อนำกลยุทธ์ไปปฏิบัติ

๖.๓ การติดตาม ประเมินผล เพื่อปรับปรุงการดำเนินงานให้บรรลุตามวิสัยทัศน์ ภารกิจ และกลยุทธ์ที่กำหนดไว้

๗. การบริหารความเสี่ยง คือ

๗.๑ วิธีการบริหารจัดการที่เป็นไปเพื่อการคาดการณ์ และลดผลเสียของความไม่แน่นอน ที่จะเกิดขึ้นกับองค์กร ทั้งนี้เพื่อให้องค์กรสามารถบรรลุวัตถุประสงค์ได้โดยมีประสิทธิภาพมากขึ้น

๗.๒ เป็นกลวิธีที่เป็นเหตุเป็นผลที่นำมาใช้ในการบ่งชี้วิเคราะห์ ประเมิน จัดการติดตาม และสื่อสารความเสี่ยงที่เกี่ยวข้องกับกิจกรรม หรือกระบวนการดำเนินงานขององค์กร เพื่อช่วยให้องค์กรลดความเสี่ยงให้เหลือน้อยที่สุด

๗.๓ เป็นการทำนายอนาคตอย่างมีเหตุมีผล มีหลักการ และหาทางลดหรือป้องกันความเสียหายในการทำงานของโครงการแต่ละขั้นตอนไว้ก่อนล่วงหน้า

๘. ทำไมต้องนำการบริหารความเสี่ยงมาใช้ในภาคราชการ เพราะพระราชกฤษฎีการว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. ๒๕๔๖ (Good Governance : GG) มุ่งหวังให้การบริหารราชการเป็นไปเพื่อประโยชน์สุขของประชาชน

๙. กระบวนการบริหารความเสี่ยง ได้แก่ การกำหนดวัตถุประสงค์ การบ่งชี้ความเสี่ยง การประเมินความเสี่ยง การจัดการความเสี่ยง การติดตามผล

๑๐. การบริหารความขัดแย้งในหน่วยงาน จำแนกเป็น ๕ วิธี ได้แก่ การหลีกเลี่ยง การปรองดอง การต่อสู้ การร่วมมือร่วมใจ การประนีประนอมหรือการเจรจาต่อรอง

๑๑. องค์ประกอบของ Competency คือ คุณลักษณะทั้งในด้านทักษะ ความรู้และพฤติกรรมของบุคคล ซึ่งจำเป็นต่อการปฏิบัติงานในตำแหน่งงานหนึ่งให้ประสบความสำเร็จ ได้แก่ skill attributes knowledge

๑๒. การจัดการความรู้ (KM) คือ ความรู้หรือบทสรุปของความเข้าใจเนื้อหาเป็นความจริงที่ผ่านการพิสูจน์และทดลอง สามารถตั้งเป็นกฎ นำไปปฏิบัติงานได้จริง หรือสามารถนำไปประกอบการตัดสินใจ รวมทั้งสามารถทำนายผลได้ สิ่งสำคัญของการบริหารจัดการองค์ความรู้ คือ การแลกเปลี่ยนความรู้ (Sharing) ระหว่างบุคคลทั้งเป็นทางการและอย่างไม่เป็นทางการ เช่น การพบปะ พูดคุยเพื่อแลกเปลี่ยนความคิดเห็น

๑๓. การพัฒนาองค์กรสู่การเป็นผู้นำเชิงกลยุทธ์ (๔ H) ได้แก่ ความคิด (Head) จิตสำนึก (Heart) พฤติกรรม/การแสดงออก (Hand) และการมีสุขภาพที่ดี (Health)

๑๔. ยุทธศาสตร์สู่ผลงานการบริหารเชิงยุทธศาสตร์ ได้แก่ การรุก การป้องกันตัว การถอย และการพลิกฟื้นสถานการณ์

- หัวข้อวิชา การประเมินผลการดำเนินงาน โดย อาจารย์สุรพงษ์ ชูรังสฤษฎ์

๑. ทำไมผู้ตรวจสอบภายในจึงต้องเรียนรู้การประเมินผลการดำเนินงาน (Performance Management)

๑.๑ เพราะเป็นส่วนหนึ่งของการควบคุมและ**กระบวนการกำกับดูแล** (Governance Process) กระบวนการกำกับดูแลที่ดีของหน่วยตรวจสอบภายใน คือ การมีจริยธรรม จรรยาบรรณ

๑.๒ เพราะต้อง**บริหารผลงานของหน่วยตรวจสอบภายใน** คือ ปกป้องผลประโยชน์ของหน่วยงานในองค์กร และเพิ่มคุณค่าให้กับผู้มีส่วนได้เสียในองค์กร

๒. การประเมินผลการดำเนินงาน สะท้อนให้เห็นถึง

๒.๑ ความสามารถในการจัดการองค์กร เพื่อให้บรรลุวัตถุประสงค์/เป้าหมายองค์กร

๒.๒ นำไปสู่กระบวนการปรับปรุงด้านประสิทธิภาพและประสิทธิผล

๒.๓ ทำให้ทราบจุดอ่อนของการดำเนินงานที่ผ่านมา

๒.๔ ผลการประเมินสามารถใช้ในการกำหนดแผนงานได้อย่างต่อเนื่อง

๓. การนำกระบวนการ PDCA มาใช้ในการบริหารงาน

กระบวนการ PDCA คือ กระบวนการปฏิบัติงานเพื่อให้ได้ผลและมีประสิทธิภาพมาใช้ขับเคลื่อน สำหรับการปฏิบัติงาน ประกอบด้วย P (Plan) การวางแผนในอนาคต โดยการกำหนดวัตถุประสงค์และตั้งเป้าหมาย D (Do) การลงมือปฏิบัติตามแผน C (Check) การตรวจสอบเพื่อติดตามความคืบหน้า และเปรียบเทียบผลสำเร็จของงานกับแผน การทบทวนแผน A (Act) การดำเนินการให้เหมาะสม หากการปฏิบัติเป็นที่น่าพอใจ ก็จัดให้เป็นมาตรฐานเพื่อเป็นแนวทางให้ปฏิบัติต่อไป หากการปฏิบัติมีข้อควรปรับปรุงก็ให้กำหนดวิธีการปรับปรุงต่อไป

สิ่งสำคัญมากที่สุดของการนำกระบวนการ PDCA มาใช้ คือ ผู้บริหารสูงสุดของหน่วยงานในการขับเคลื่อนกระบวนการดังกล่าว

๔. เครื่องมือที่ใช้ในการประเมินผลการดำเนินงาน ได้แก่ Balanced Scorecard (BSC) ซึ่งทำให้ผู้บริหารระดับสูงเห็นภาพรวมขององค์กรได้ชัดเจนขึ้น และช่วยให้ศึกษาผลการปฏิบัติงานที่ผ่านมาและปรับปรุงกลยุทธ์ขององค์กรให้ครบถ้วนในทุก ๆ ด้าน ด้วยการวัดผล ๔ ด้าน คือ

- ด้านการเงิน (Financial) เมื่อก่อนผลสำเร็จของงานจะวัดด้านการเงินเพียงอย่างเดียว ซึ่งไม่ใช่สิ่งที่ทำให้องค์กรอยู่รอดได้อย่างยั่งยืน
- ความพึงพอใจของลูกค้า (Customer)
- กระบวนการภายใน (Internal Process) วัดที่คุณภาพ เวลาตอบสนอง และต้นทุน
- การเรียนรู้ และนวัตกรรม (Learning and Growth) การเรียนรู้สิ่งใหม่ ๆ ทันโลก และชนะใจลูกค้า โดยเอาเทคโนโลยีมาช่วยในการตรวจสอบ

๕. ปัจจัยแห่งความสำเร็จ (Key Success Factor) ประกอบด้วย

๕.๑ การกำหนดเป้าหมาย มี ๒ แบบ ได้แก่

- การกำหนดเป้าหมายในแนวดิ่ง เริ่มจากบนลงล่าง (Top – down) ดังนั้นเป้าหมายขององค์กรต้องมีความชัดเจน ไม่เช่นนั้นเป้าหมายของหน่วยงานจะไม่สอดคล้องกับองค์กร
- การกำหนดเป้าหมายแนวระนาบ คือ หน่วยงานต้องสนับสนุนซึ่งกันและกันต้องกำหนดเป้าหมายร่วมกันให้มีความสอดคล้องกัน ดังนั้น งานตรวจสอบภายในจึงอยู่ในแนวระนาบ

๕.๒ การจัดทำแผน

๕.๓ การวินิจฉัยผลงาน ซึ่งการวินิจฉัยผลงานเป็นขั้นตอนที่สำคัญ เพราะเป็นการติดตามผลและนำผลที่เกิดขึ้นในระยะเวลาหนึ่งมาพิจารณา และหาความแตกต่างระหว่างเป้าหมายกับผลที่เกิดขึ้นจริงโดยต้องหาเหตุผลสนับสนุนและอธิบายได้

- หัวข้อวิชา การประมวลผลข้อมูลที่ได้จากการตรวจพบการกระทำผิด โดย อาจารย์มานิต พาณิชย์กุล

การตรวจสอบการทุจริต (Fraud Indicators)

๑. การทุจริต เกิดขึ้นได้จาก ๓ ปัจจัย คือ สิ่งกระตุ้น/สิ่งบีบคั้น โอกาส และการตั้งใจใช้อุบายหรือนิสัย

๒. ผู้ตรวจสอบให้บริการอะไรเกี่ยวกับการทุจริต

- จัดทำ Audit Program เพื่อประเมินระบบการควบคุมภายในเกี่ยวกับความเสี่ยงด้านการทุจริต
- คำนึงถึงความเสี่ยงเกี่ยวกับการทุจริตในแผนการตรวจสอบ

๓. สิ่งที่ทำให้การทุจริตลดน้อยลง ได้แก่ การมีจริยธรรมที่สามารถทนต่อสิ่งยั่วยุได้

ยกตัวอย่าง ถ้าสิ่งกระตุ้นสูง โอกาสสูง จริยธรรมต่ำ ทำให้เกิดการทุจริตได้

๔. วัฒนธรรมองค์กรที่เชิญชวนให้ทำทุจริต ได้แก่

๔.๑ วัตถุประสงค์องค์กรเน้นการสร้างกำไร และใช้กำไรเป็นเกณฑ์ในการประเมินผลงาน

๔.๒ สร้างวัฒนธรรมองค์กรให้ทุกคนให้ความสำคัญในเรื่องของต้นทุน ทุก ๆ อย่างแต่ไม่ให้คุณค่าของความสุจริต

๔.๓ วัฒนธรรมองค์กรที่ให้ความสำคัญต่อผลประโยชน์ตอบแทนเป็นแรงจูงใจเพียงอย่างเดียว

๔.๔ องค์กรที่มีความล้มเหลวในการสร้างหรือสื่อสารเรื่องจริยธรรมในองค์กร

๔.๕ มีการมอบหรือกระจายอำนาจในการบริหารโดยไม่มีการติดตามการปฏิบัติตามอำนาจ

๔.๖ องค์การที่ไม่สนใจต่อข้อร้องเรียน

๔.๗ มีความล้มเหลวในการเฝ้าระวังในเรื่องการใช้อำนาจของผู้บริหารเพื่อข้ามระบบการควบคุมภายใน

๔.๘ มีระบบการสื่อสารแบบทางเดียว ลักษณะจากระดับจัดการลงมาโดยการสื่อสารแบบ ๒ ทาง ทำให้เกิดการ feedback กลับมาได้

๕. การตรวจสอบการทุจริต เน้นเรื่อง ข้อแตกต่าง ความผิดแปลก การบัญชีที่ไม่เป็นไปตามเกณฑ์ วิธีการกำกับ ไม่ใช่ข้อผิดพลาดหรือละเลย

๖. การตรวจสอบการทุจริต เป็นการค้นหาจุดอ่อนในการควบคุม

๗. ขั้นตอนในการตรวจสอบการทุจริต ได้แก่

๗.๑ การกำหนดประเด็นทุจริตให้ชัดเจน

๗.๒ ประเมิน วิธี เรื่องที่ต้องพิสูจน์เพื่อสนับสนุนประเด็น

๗.๓ รวบรวมเอกสารและประเมินเกี่ยวกับประเด็นที่สงสัยว่ามีการทุจริต

๗.๔ พบผู้เกี่ยวข้องทั้งหมด เพื่อประเมินในความเป็นไปได้

๗.๕ เมื่อประเมินรวมแล้วกำหนดแนวทางการดำเนินการต่อ เช่น การกำหนดหลักฐาน/ข้อมูลเพื่อใช้พิสูจน์ การสัมภาษณ์

๗.๖ ประเมินสภาพแวดล้อมของการปฏิบัติงาน

๗.๗ ประเมินผลการตรวจสอบ และหลักฐานว่าเพียงพอ และเชื่อถือได้

๗.๘ แจ้งผู้บังคับบัญชา เพื่อยืนยันและแสดงหลักฐานเป็นการภายใน

๗.๙ รายงานผู้บริหาร พร้อมแสดงหลักฐานจากการตรวจสอบโดยเร็ว

๗.๑๐ ระบุจุดอ่อนที่มี และแนวทางในการปรับปรุงแก้ไข

๘. โอกาสในการก่อทุจริต ได้แก่ ขาดการควบคุมภายในและการตรวจสอบภายใน มอบหมายความรับผิดชอบมากเกินไปให้กับผู้ปฏิบัติงานคนเดียว กระจายอำนาจมากเกินไป ล้มเหลวในการลงโทษผู้ทุจริต การลงโทษ ไม่สมกับความผิด หรือไม่ได้รับการเปิดเผย

๙. ความล้มเหลวในการตรวจจับทุจริต ทุจริตส่วนใหญ่ถูกจับได้ แต่มักปล่อยให้ลอยนวลไป โดยไม่ฟ้องร้องดำเนินคดีอาญา

๑๐. การสร้างสภาพแวดล้อมเพื่อสกัดกั้นทุจริต ได้แก่ ความซื่อสัตย์ในระดับบริหาร ชื่อเสียงในทางที่ดี ขั้นตอนการว่าจ้างพนักงานใหม่ต้องมีกระบวนการคัดสรรและจ้างพนักงานตรวจสอบประวัติอาชญากรรม โปรแกรมเรื่องจริยธรรม นโยบายปราบปรามทุจริต

การบ่งชี้การทุจริต

๑. **การป้องปรามการทุจริต** จะประกอบด้วยมาตรการที่ปรามการเตรียมการทุจริตและจำกัดโอกาสในการที่จะทำการทุจริต

การป้องปรามการทุจริต คือ ระบบการควบคุมภายใน ซึ่งผู้บริหารองค์กรมีหน้าที่จะต้องสร้างและรักษาไว้ ซึ่งระบบการควบคุมภายใน

๒. ผู้ตรวจสอบภายในมีหน้าที่ ช่วยในการสอบทานและประเมินความเพียงพอ และความมีประสิทธิภาพของการควบคุมภายในว่าเพียงพอที่จะช่วยลดโอกาสการกระทำการทุจริต

๓. เมื่อผู้ตรวจสอบภายในสงสัยว่ามีการทำผิด ผู้ตรวจสอบภายในต้องแจ้งผู้มีอำนาจหน้าที่ที่เหมาะสมขององค์กรนั้น

๔. การรายงานกรณีทุจริต กระทำได้ดังนี้ รายงานด้วยวาจา รายงานเป็นระยะ ๆ รายงานเมื่อสอบสวนสิ้นสุดแล้ว

๕. ฝ่ายจัดการหรือหัวหน้าส่วนราชการ มีหน้าที่สร้างและรักษาไว้ซึ่งระบบการควบคุมที่มีประสิทธิภาพ

๖. สิ่งที่บอกเหตุว่าเกิดการทุจริต เนื่องจากระบบการควบคุมภายในที่ไม่เพียงพอ ได้แก่ ไม่ได้เปรียบเทียบสินทรัพย์กับของจริง ไม่ปฏิบัติตามอำนาจในการดำเนินการ ขาดบุคลากร บุคลากรขาดคุณสมบัติ ร่วมกันทุจริต มีสินทรัพย์มูลค่าสูงที่จับต้องง่าย ไม่แยกอำนาจและหน้าที่

๗. สิ่งที่บอกเหตุว่าเกิดการทุจริต เนื่องจากพฤติกรรมที่อาจนำไปสู่การทุจริต ได้แก่ ชอบกล่าวร้ายคนอื่น ไม่ยอมลาพักผ่อน ชอบแก้ไขเอกสาร ถือเงินสดเป็นจำนวนมาก สนิทสนมกับคู่ค้า

๘. สิ่งที่บอกเหตุว่ามีการทุจริตเกิดขึ้น ได้แก่ การกระทบตัวเลขล่าช้า ลูกค้ามักร้องเรียน รายได้มักตกต่ำ ปรับปรุงตัวเลขทางบัญชีบ่อยครั้ง สินค้าหายโดยไม่สอบสวน ขวัญและกำลังใจพนักงานต่ำ

๙. สาเหตุในระดับผู้บริหาร ได้แก่ ตั้งเป้าหมายสูงเกินไป ต้องการความสำเร็จ ต้องการผลประโยชน์ ต้องการสร้างกำไร คุมทั้งสินทรัพย์ และการบันทึกบัญชีโดยไม่แบ่งแยกกัน

๑๐. ปัจจัยที่มีส่วนหรือก่อให้เกิดการทุจริตได้ ได้แก่

๑๐.๑ การควบคุมภายในที่ไม่มีประสิทธิผล ได้แก่ การแบ่งแยกหน้าที่ที่รับผิดชอบ ข้อจำกัดในการเข้าถึงสินทรัพย์ การบันทึกรายงาน การระบุเรื่องความรับผิดชอบในหน้าที่ การกระทบยอดสินทรัพย์กับบัญชี การทำรายงานตามอำนาจที่กำหนด การกำหนดเงื่อนไขในการควบคุม เนื่องจาก ขาดคน หรือมีคนที่ไม่มีคุณภาพ ขาดผู้เชี่ยวชาญด้านคอมพิวเตอร์ ทำหน้าที่กำกับควบคุม ทำให้เกิดการฉวยโอกาส การใช้โปรแกรมระบบงานที่ไม่ผ่านการทดสอบ

๑๐.๒ ความร่วมมือกันของพนักงาน หลีกเลี่ยงการควบคุม
๑๐.๓ การถือครองเงินสด/ครองเงินสดไว้สูง ทำให้เกิดโอกาสการทุจริต
๑๑. การควบคุมที่สำคัญ ได้แก่ ความสามารถและความซื่อสัตย์ของพนักงาน ที่มีความรับผิดชอบในหน้าที่ชัดเจนและอำนาจที่เหมาะสม การแบ่งแยกหน้าที่ให้เกิดการคานอำนาจ กระบวนการที่เหมาะสมและการให้อำนาจเป็นชั้น ๆ

- **หัวข้อวิชา เทคนิคการให้บริการในวิชาชีพตรวจสอบ โดย อาจารย์มานิต พาณิชย์กุล**

๑. การตรวจสอบภายใน คือ การให้ความเชื่อมั่นและการให้คำปรึกษา อย่างเที่ยงธรรม เป็นอิสระ เพิ่มคุณค่า ปรับปรุงการดำเนินงาน บรรลุวัตถุประสงค์ด้วยการประเมิน ปรับปรุงประสิทธิภาพของกระบวนการบริหารความเสี่ยง การควบคุม กำกับดูแลอย่างเป็นระบบ ระเบียบ

๒. การให้บริการของการตรวจสอบภายใน ได้แก่ การเสนอวิธีการ/กลยุทธ์การทำงานเป็นระบบ ระเบียบ มีวินัย ในการทำงาน ประเมิน/ปรับปรุงประสิทธิผล เรื่อง ความโปร่งใส บริหารความเสี่ยง การควบคุม

๓. IPPF : International Professional Practices Framework คือ มาตรฐานสากลการปฏิบัติงานวิชาชีพการตรวจสอบภายใน

๔. มาตรฐานด้านคุณสมบัติ ได้แก่ ให้หัวหน้าผู้ตรวจสอบภายในรายงานตรงต่อคณะกรรมการหรือหัวหน้า ส่วนราชการ

๕. การตรวจสอบภายในมีลักษณะ ให้บริการความเชื่อมั่นและคำปรึกษา ควรระบุไว้ใน กฎบัตร

๖. หากการตรวจสอบสูญเสียความเป็นอิสระและเที่ยงธรรม รายละเอียดการขาดอิสระและเที่ยงธรรมควรถูกเปิดเผยให้แก่ผู้ที่เหมาะสมทราบ

๗. หัวหน้าหน่วยตรวจสอบภายในควรปฏิเสธงานให้คำปรึกษา หรือเสาะหาคำแนะนำ หรือความช่วยเหลือ กรณีเจ้าหน้าที่ตรวจสอบภายในขาดความรู้ ทักษะ และความสามารถอื่น ๆ ที่จำเป็นในการปฏิบัติงานไม่ว่าบางส่วนหรือทั้งหมด

๘. ผู้ตรวจสอบภายในควรระมัดระวังในการประกอบวิชาชีพอย่างเหมาะสม โดยพิจารณาถึง
๘.๑ ขอบเขตการตรวจสอบที่จำเป็น เพื่อบรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมาย
๘.๒ ความซับซ้อน มีนัยสำคัญ ความสำคัญ ที่ใช้กระบวนการความเชื่อมั่นประเมิน
๘.๓ ความเพียงพอ มีประสิทธิภาพ ในการจัดการความเสี่ยง ควบคุม กำกับดูแล
๘.๔ ความเป็นไปได้ที่เกิดข้อผิดพลาด ผิดปกติ ที่ไม่ปฏิบัติตามระเบียบ
๘.๕ ต้นทุนการให้ความเชื่อมั่นเทียบผลประโยชน์ที่ได้รับ

๙. ผู้ตรวจสอบภายในควรระมัดระวังอย่างเหมาะสม ในการให้คำปรึกษา โดยคำนึงถึง
๙.๑ ความจำเป็น ความคาดหวังของผู้รับบริการ รวมทั้งลักษณะช่วงเวลาสื่อสารถึงผลการปฏิบัติงาน
๙.๒ ความสลับซับซ้อน ขอบเขตงานที่จำเป็น
๙.๓ ต้นทุนการให้คำปรึกษาเทียบผลประโยชน์ที่ได้รับ

๑๐. หัวหน้าหน่วยงานตรวจสอบควรสร้าง/รักษา โปรแกรมการประกันคุณภาพและปรับปรุงงานให้ครอบคลุม ทุกงาน ลักษณะโปรแกรมควรออกแบบเพื่อเพิ่มคุณค่า ปรับปรุงงานให้เกิดความเชื่อมั่นในการปฏิบัติงาน ตามมาตรฐานและหลักจรรยาบรรณของผู้ตรวจสอบภายใน

๑๑. การประเมินโปรแกรมคุณภาพ มี ๒ ส่วน ได้แก่ ประเมินภายใน และประเมินภายนอก

๑๒. หัวหน้าหน่วยงานตรวจสอบควรแจ้งแผนงานกิจกรรมการตรวจสอบภายใน ทรัพยากร การเปลี่ยนแปลงระหว่างกาลให้ผู้บริหารระดับสูงและคณะกรรมการ

๑๓. หัวหน้าหน่วยงานตรวจสอบควรรายงานคณะกรรมการและผู้บริหารระดับสูงเป็นระยะ ๆ ในเรื่องดังนี้ วัตถุประสงค์ อำนาจหน้าที่ความรับผิดชอบ ผลการปฏิบัติงานตามแผน ความเสี่ยงที่มีสาระสำคัญ จุดควบคุม กำกับดูแลกิจการอื่น ๆ ที่จำเป็นหรือถูกร้องขอจากคณะกรรมการหรือผู้บริหารระดับสูง

หัวข้อวิชา IT Governance & Importance IT Governance Frameworks and Standards
โดย อาจารย์มานิตย์ พาณิชย์กุล และ ดร.พรเทพ อนุสสรนิติสาร

๑. What is COBIT ? COBIT : Control Objective for Information and related Technologies

๒. แนวคิดการควบคุมด้าน IT ระดับสูง
๒.๑ ต้องเข้าใจธุรกิจ (เข้าใจการให้บริการหน่วยงาน)
๒.๒ แนะนำแนวปฏิบัติที่ดี (Good Practices) ในการปฏิบัติงาน IT
๒.๓ เน้นการควบคุม (Control) แต่ไม่เน้นรายละเอียดเป็นกรอบใหญ่
๒.๔ ช่วยให้หน่วยงานประสบผลสำเร็จในการลงทุน หรืองบประมาณด้าน IT
๒.๕ ช่วยบอกวิธีการแก้ปัญหาถ้ามีข้อผิดพลาดเกิดขึ้น

๓. Who does COBIT serve ?
๓.๑ Stakeholders (หัวหน้าส่วนราชการ ประชาชน ลูกค้า)
๓.๒ ผู้มาใช้บริการภายในและภายนอก
๓.๓ ผู้ทำหน้าที่ควบคุมและรับผิดชอบความเสี่ยงทั้งภายในและภายนอก

๔. ประโยชน์ของการใช้ COBIT
๔.๑ ความสอดคล้องกับกลยุทธ์ เช่น แผนกลยุทธ์ทางด้าน IT ต้องเข้ากันกับแผนธุรกิจหรือหน่วยงาน
๔.๒ การสร้างคุณค่าเพิ่ม เช่น สะสางบทบาทหน้าที่ของแต่ละคน ธรรมาภิบาลบอกว่าใครทำหน้าที่อะไร
๔.๓ การบริหารความเสี่ยง เช่น เป็นที่ยอมรับของผู้มารับบริการ
๔.๔ การวัดผลการดำเนินงาน เป็นตัวบอกแนวคิดวิธีการบริหารจัดการด้าน IT ทั่วไป
๔.๕ การบริหารทรัพยากร โดย COBIT ใช้หลักการควบคุมของ COSO ด้วย

๕. COBIT มาจากพื้นฐานของธรรมาภิบาลหลายตัว เช่น ITIL , ISO ๑๗๗๙๙ , CMM , COSO
สรุป COBIT เป็น High Level ไม่เน้นรายละเอียด ประกอบด้วย ISO ๑๗๗๙๙ , CMM , ITIL จะมีขอบเขตตั้งแต่ Process Control จนถึง Strategic

๖. IT Governance จะสำเร็จได้อยู่ที่ Top คือ เป็นความรับผิดชอบของผู้บริหารระดับสูงและคณะกรรมการที่กำกับดูแล

๗. คุณลักษณะที่สำคัญของ COBIT ประกอบด้วย
๗.๑ Business – Focus
๗.๒ Process – Oriented
๗.๓ Control – Based
๗.๔ Measurement – Driven

๘. Business – Focus คือ ทุกอย่างต้องเชื่อมเป้าหมายทางธุรกิจ เน้นความต้องการของธุรกิจ จะใช้วงจรคุณภาพเข้ามาจัดการ (Plan - Do - Check - Act) โดยมีพื้นฐาน IT ประกอบด้วย ข้อมูล (Information) ระบบงาน (Application) เครือข่าย (Infrastructure) บุคลากร (People)

๙. Process – Oriented เน้นกระบวนการในการบริหารงาน IT เพื่อการจัดการที่ดี เช่น การปรับใช้ IT ให้เข้ากับธุรกิจ (Alignment) ทำให้ธุรกิจง่ายขึ้น ทำให้เกิดความน่าเชื่อถือ ทำให้เกิดการบริหารความเสี่ยงที่เหมาะสม

๑๐. Control – Based คือ การควบคุมและการกำกับดูแล ดังนี้

๑๐.๑ ต้องควบคุมในเชิงเป้าหมายธุรกิจ โดยการออกกฎหมาย ระเบียบ นโยบายปฏิบัติ การควบคุมระบบกระบวนการ การควบคุม IT ทั่วไป

๑๐.๒ การควบคุมด้าน IT มี ๒ Controls คือ IT General Control : ด้านทั่วไป และ Application Controls : ภายในระบบ

๑๑. Measurement – Driven แนวคิดการขับเคลื่อนโดยการวัดผลใช้เครื่องมือ ดังนี้

๑๑.๑ Dashboard : เป็นกระบวนการติดตามอย่างต่อเนื่องในเรื่องของเป้าหมายกับผลการปฏิบัติ โดยการเปรียบเทียบเป็นระยะ ๆ เพื่อแก้ไขปรับปรุง

๑๑.๒ Balance Scorecard : กำหนดให้มี ๔ ตัวชี้วัดในการวัดผลโดยจัดทั้ง ๔ ตัว แล้วแต่ให้น้ำหนักตัวไหนแต่ต้องให้มีการจัดทั้ง ๔ ตัว คือ Financial , Customer , Process , Learning and Development

๑๑.๓ Benchmarking : เทียบกับหน่วยงานที่ทำแล้วได้ดี

๑๒. IT Governance Focus Areas คือ เป้าหมาย ๕ เรื่อง ดังนี้

๑๒.๑ Strategic Alignment คามสอดคล้องกับกลยุทธ์

๑๒.๒ Value Delivery การสร้างคุณค่า ผลตอบแทน

๑๒.๓ Risk Management การบริหารความเสี่ยง

๑๒.๔ Performance Measurement การวัดผลการดำเนินงาน

๑๒.๕ Resource Management การบริหารทรัพยากร

๑๓. ต้นเหตุความเสี่ยงด้านระบบ IT

๑๓.๑ ขาดประสิทธิภาพในการบริหารจัดการระบบ IT

๑๓.๒ การขยายตัวของความซับซ้อนของระบบ IT

๑๓.๓ ความไม่ใส่ใจต่อความเสี่ยงด้าน IT เช่น ขาดความรู้ ความชำนาญ โครงสร้างพื้นฐานของระบบ IT ไม่ดี ความไม่ใส่ใจต่อความเสี่ยงของเจ้าหน้าที่ การขาดระบบในเตือนภัย

๑๔. อุปสรรคของการบริหารความเสี่ยงด้าน IT ระดับองค์กร คือ การขาดภาพรวมของการดำเนินการของระบบ IT ที่เชื่อมโยงกับการดำเนินงานและเป้าหมายขององค์กร

๑๕. ประเภทของการตัดสินใจหลักที่เกี่ยวข้องกับการบริหารจัดการระบบ IT เป็นบทบาทของระบบ IT ที่เกี่ยวข้องกับกลยุทธ์ขององค์กร

๑๕.๑ IT Principles : ด้านยุทธศาสตร์ของระบบ

๑๕.๒ IT Architecture : ด้านสถาปัตยกรรม เป็นทางเลือกด้านเทคนิคที่จะช่วยผลักดันให้องค์กรบรรลุเป้าหมาย (Network →Internet ภาครัฐ เป็น Mobile)

๑๕.๓ IT Infrastructure : ด้านโครงสร้างพื้นฐานของระบบ ซึ่งเป็นปัจจัยพื้นฐานที่สะท้อนให้เห็นถึงศักยภาพของระบบ เช่น ความเร็วของ IT

๑๕.๔ Business Application Need : ด้านความต้องการขององค์กร ซึ่งเป็นรูปแบบของระบบที่จะช่วยสนับสนุนกิจกรรมขององค์กร

๑๕.๕ Prioritization and Investment : ลำดับความสำคัญและการลงทุน เช่น การกำหนดงบประมาณการลงทุนที่จุดใด

๑๖. ลักษณะโครงสร้างการตัดสินใจในการจัดการระบบ IT

๑๖.๑ Business Monarchy : เป็นระบบรวมศูนย์ที่สุด คือ CEO หรือ CIO ตัดสินใจโดยลำพัง

๑๖.๒ IT Monarchy : การตัดสินใจโดยผู้เกี่ยวข้องด้าน IT เท่านั้น

๑๖.๓ Federal : การตัดสินใจร่วมกันในหลาย ๆ ฝ่าย รวมทั้งแผนก IT ในรูปแบบคณะกรรมการ

๑๖.๔ IT Duopoly : การตัดสินใจร่วมกันสองส่วน ซึ่งมักจะเป็นแผนก IT กับ หัวหน้าหน่วยงานที่ใช้ระบบ

๑๗. Public Value แบ่งเป็น ๓ ด้าน ดังนี้ การให้บริการ (Services) ผลการดำเนินงาน (Perfornance) ความเชื่อถือ (Trust)

๑๘. กรอบการประเมินเหตุความเสี่ยงด้าน IT (๔ A Framework) ได้แก่ ความพร้อมใช้ (Availability) การเข้าถึงระบบ (Access) ความถูกต้อง (Accuracy) และความว่องไว (Agility)

๑๙. ประโยชน์ของ ๔A Framework คือ นำไปใช้แลกเปลี่ยนความคิดเห็นระหว่างผู้บริหารกับ IT ได้พูดคุยหารือปรึกษาและเข้าใจความเสี่ยงที่เกิดขึ้น

๒๐. Where to start IT risk ? (การเริ่มต้นประเมินความเสี่ยง) ดำเนินการได้ดังนี้

๒๐.๑ ดูพื้นฐานของระบบ IT (Foundation) ทำให้ง่าย ไม่ซับซ้อน

๒๐.๒ ดูกระบวนการ (Process) การจัดการความเสี่ยงและติดตาม

๒๐.๓ ดูความตื่นตัว (Awareness) วัฒนธรรมขององค์กร

๒๑. ขั้นตอนในการปรับปรุงโครงสร้างพื้นฐาน (Foundation) เริ่มจาก การจัดการกับความพร้อมใช้ (Availability Risk) ค้นหาปัญหาและรับแก้ไข และพัฒนา ประยุกต์ใช้แนวทางควบคุมในการติดตามสถานะของระบบ IT

๒๒. เครื่องมือที่ใช้ในการปรับปรุงความพร้อมใช้ (Availability Risk) คือ BCP หรือ BCM (Business Continuity Management) เป็นความเข้าใจและการลดผลกระทบอันเกิดจากเหตุการณ์ที่ร้ายแรงที่ส่งผลต่อการดำเนินการที่สำคัญขององค์กร

๒๓. ในการบริหารความเสี่ยงระบบ IT จะต้องมี Feedback เป็นการติดตามความเสี่ยง (Monitor and Track Risk)

๒๔. Organizational structure in IT risk governance process (โครงสร้างขององค์กรในกระบวนการบริหารความเสี่ยงระบบ IT) ประกอบด้วย

- ผู้บริหาร ซึ่งต้องมีบทบาทสร้างความตื่นตัวในองค์กร (Risk – aware culture)
- IT risk management team บทบาท คือ ทบทวนติดตามความเสี่ยง
- Local manager and experts บทบาท คือ เป็นผู้ใช้และเป็นผู้บริหารความเสี่ยง เพื่อ Feedback on policies and processes / reduce risk เป็นผู้ควบคุมหรือลดผลกระทบด้านความเสี่ยงเมื่อเกิดปัญหาขึ้น

๒๕. ทำไมเราต้องมาสนใจการจัดทำระบบ IT Governance

๒๕.๑ เพราะระบบการดำเนินการขององค์กรต่าง ๆ ต้องอาศัยระบบคอมพิวเตอร์เป็นกลไกหลักในการดำเนินการ เช่น ระบบ GFMIS

๒๕.๒ มูลค่าในการลงทุนระบบ IT มีแนวโน้มสูงขึ้นเรื่อย ๆ ในอนาคต

๒๕.๓ มีความเสี่ยงต่อการมีปัญหาด้านความปลอดภัย เช่น ไวรัส e-mailขยะ ระบบถูกบุกรุก

๒๖. องค์ประกอบสำคัญในการสร้างคุณค่าทางสังคม (Public Value) ของรัฐบาลอิเล็กทรอนิกส์ (e - Government) ได้แก่ การให้บริการต่าง ๆ (Citizen Service Applications) คุณภาพและประสิทธิภาพการให้บริการ ความน่าเชื่อถือ (Trust)

จึงเรียนมาเพื่อโปรดทราบ จะเป็นพระคุณ

(นางจรัญญา สะเริญรัมย์)
นักวิชาการตรวจสอบภายในปฏิบัติการ

เรียน ผู้อำนวยการกลุ่มตรวจสอบภายใน

เพื่อโปรดทราบรายงานสรุปผลการอบรม CGIA ด้าน Advance Per. ด้วย จะเป็นพระคุณ

(นางสาวอรุณี มนประณีต)
นักวิชาการตรวจสอบภายในชำนาญการ
หัวหน้าฝ่ายตรวจสอบ ๒

- ทราบ
- นำขึ้น web site กตส.

๒๒ ก.พ. ๖๑

(นางสาวพิมพ์ภาวดี ศรีจันทร์)
ผู้อำนวยการกลุ่มตรวจสอบภายใน