รายงานสรุปผลการจัดกิจกรรมและสรุปผลการประเมินความพึงพอใจของผู้เข้าร่วมกิจกรรม
หัวข้อ "การบริหารความเสี่ยงด้านระบบสารสนเทศในองค์กร
และการตรวจสอบระบบสารสนเทศ (IT Audit)"
ภายใต้โครงการจัดการความรู้เพื่อสร้างเครือข่ายในการทำงาน (KM Networking)
ประจำปีงบประมาณ พ.ศ. ๒๕๖๐ ครั้งที่ ๓

กลุ่มตรวจสอบภายใน (กตส.) ได้ดำเนินโครงการจัดการความรู้เพื่อสร้างเครือข่ายในการทำงาน (KM Networking) ประจำปีงบประมาณ พ.ศ. ๒๕๖๐ โดยจัดอบรมครั้งที่ ๓ หัวข้อ "การบริหารความเสี่ยงด้านระบบสารสนเทศในองค์กร และการตรวจสอบระบบสารสนเทศ (IT Audit)" ระหว่างวันที่ ๖-๗ มิถุนายน ๒๕๖๐ สรุปสาระสำคัญของการจัดกิจกรรมได้ ดังนี้

๑. วัตถุประสงค์ของการอบรม คือ

๑.๑ เพื่อให้บุคลากร สบน. มีความรู้และความเข้าใจเรื่องความเสี่ยง การบริหารความเสี่ยงและการควบคุมภายในด้านสารสนเทศ

๑.๒ เพื่อให้ผู้ตรวจสอบภายใน สบน. รวมทั้งเครือข่าย กตส. ทราบเทคนิคและวิธีการตรวจสอบด้านระบบสารสนเทศ

๒. ขอบเขตการอบรม จำนวน ๒ วัน ดังนี้

๒.๑ การอบรมวันแรก เป็นการอบรมภาพรวมของความเสี่ยงและการควบคุมภายในระบบสารสนเทศในองค์กร กลุ่มเป้าหมาย คือ ผู้ตรวจสอบภายใน และเจ้าหน้าที่ผู้ใช้งานระบบหรือดูแลระบบสารสนเทศ สบน. เช่น ระบบฐานข้อมูลหนี้สาธารณะ (GFMIS-TR) ระบบบริหารจัดการโครงการลงทุนด้านโครงสร้างพื้นฐาน (IIPM) ระบบบริหารจัดการข้อมูลการบริหารการชำระหนี้ (DMTR) ระบบฐานข้อมูลการวิเคราะห์ความเสี่ยงทางเครดิต เป็นต้น โดยมีผู้เข้าอบรม จำนวน ๔๔ คน (ข้าราชการ ๓๐ คน พนักงานราชการและลูกจ้าง ๑๔ คน)

๒.๒ การอบรมวันที่สอง เป็นการอบรมเฉพาะด้านตรวจสอบภายในระบบสารสนเทศ โดยมีกลุ่มเป้าหมาย คือ ผู้ตรวจสอบภายในของ สบน. และเครือข่าย กตส. จากสำนักงานปลัดกระทรวงการคลัง สำนักงานเศรษฐกิจการคลัง และสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ โดยมีผู้เข้าร่วมอบรม จำนวน ๑๘ คน (ข้าราชการ ๑๓ คน พนักงานราชการและลูกจ้าง ๕ คน)

๓. วิทยากร ได้แก่ นางสาววรางคณา มุสิกะสังข์ (ISACA) และทีมงาน จากบริษัทบริษัท ไพรซ์วอเทอร์เฮาส์ คูเปอส์ ประเทศไทย (PwC)

๔. รายละเอียดการอบรม สรุปได้ ดังนี้

๔.๑ การกำกับดูแลกิจการ (Governance) ความเสี่ยง (Risk) และการควบคุม (Control) โดยคุณณฤดี คอศิริ

๑) ความเชื่อมโยงของการกำกับดูแลกิจการ (Governance) ความเสี่ยง (Risk) และการควบคุม (Control)

การกำกับดูแลกิจการเป็นหน้าที่ของผู้บริหารในการกำหนด อนุมัติ และติดตามกลยุทธ์ขององค์กร เพื่อให้องค์กรบรรลุวัตถุประสงค์และเป้าหมายที่กำหนด โดยผู้บริหารจะต้องระบุ ประเมินปัญหาหรือความเสี่ยงที่อาจมีผลต่อการบรรลุวัตถุประสงค์ขององค์กร เพื่อใช้ในการกำหนดวิธีการจัดการ รวมทั้งติดตามความเสี่ยง (การบริหารความเสี่ยง) นอกจากนี้ ต้องกำหนดนโยบายและวิธีการต่างๆ ให้บุคลากรของหน่วยงานนำไปปฏิบัติเพื่อลดโอกาส และ/หรือผลกระทบของความเสี่ยง (การควบคุมภายใน) โดยมีกระบวนการตรวจสอบและประเมินความมีประสิทธิผลของการควบคุมภายในโดยผู้ตรวจสอบภายใน (การตรวจสอบภายใน) และผู้บริหาร/ผู้ปฏิบัติงาน

/ที่รับผิดชอบ...

ที่รับผิดชอบงานนั้นๆ (การประเมินการควบคุมด้วยตนเอง) เพื่อให้มั่นใจว่า องค์กรจะสามารถดำเนินการได้บรรลุวัตถุประสงค์

๒) <u>การควบคุมภายใน</u>

แนวคิดการควบคุมภายในตามกรอบของ COSO ปี ๒๐๑๓ คือ กระบวนการ (Process) ที่กำหนดขึ้นและนำมาใช้โดยคณะกรรมการ ฝ่ายบริหาร เพื่อให้เกิดความมั่นใจอย่างสมเหตุสมผลว่า องค์กรจะสามารถบรรลุวัตถุประสงค์ (Objective) ใน ๓ เรื่อง คือ (๑) การปฏิบัติงาน (Operations) (๒) การรายงาน (Reporting) และ (๓) การปฏิบัติตามกฎ ระเบียบ (Compliance) โดยมีองค์ประกอบของการควบคุมภายใน ๕ องค์ประกอบ ได้แก่ (๑) สภาพแวดล้อมการควบคุม (๒) การประเมินความเสี่ยง (๓) กิจกรรมควบคุม (๔) สารสนเทศและการสื่อสาร และ (๕) การติดตามประเมินผล

สภาพแวดล้อมการควบคุม : ผู้บริหารควรปฏิบัติตัวเป็นแบบอย่างที่ดีให้กับบุคลากรในองค์กร บุคลากรมีความเข้าใจเกี่ยวกับพฤติกรรมที่เป็นที่ยอมรับหรือพฤติกรรมที่ไม่เป็นที่ยอมรับ และสิ่งที่ต้องดำเนินการหากพบเห็นพฤติกรรมที่ไม่เหมะสม องค์กรควรมีการกำหนดนโยบายและขั้นตอนการปฏิบัติงานสำหรับกระบวนการทำงานที่มีความสำคัญ มีการสื่อสารให้ผู้เกี่ยวข้องทราบ รวมทั้งมีการทบทวนและปรับปรุงอย่างสม่ำเสมอ

การประเมินความเสี่ยง : เพื่อจัดลำดับความสำคัญของความเสี่ยงก่อนพิจารณากำหนดกิจกรรมควบคุมตามระดับความเสี่ยงที่ประเมินได้

กิจกรรมควบคุม : เป็นได้ทั้งแบบ Manual Controls และ/หรือ Automated Controls

สารสนเทศและการสื่อสาร : สารสนเทศทั้งจากภายในและภายนอกองค์กร โดยการสื่อสารที่ดีต้องเป็นการสื่อสาร ๒ ทาง (Two-way Communication) และคุณภาพของสารสนเทศไม่ได้พิจารณาเฉพาะเนื้อหาเท่านั้น ยังรวมถึงความถูกต้อง ครบถ้วน เป็นปัจจุบัน และทันเวลาด้วย

การติดตามประเมินผล : การติดตามประเมินผลความเพียงพอและประสิทธิผลของการควบคุมภายในที่วางไว้ซึ่งเป็นหน้าที่ของผู้บริหารและเจ้าหน้าที่ผู้ปฏิบัติงาน สำหรับผู้ตรวจสอบภายในจะมีหน้าที่สอบทานความเพียงพอเหมาะสมเท่านั้น

๓) <u>ความเสี่ยงและการควบคุมภายในของกระบวนการปฏิบัติงานที่สำคัญ</u>

กิจกรรมการควบคุม (Control Activities) ตัวอย่างเช่น การอนุมัติ (Approvals) อำนาจการอนุมัติ (Authorizations) การตรวจสอบ (Verifications) การกระทบยอด (Reconciliations) การสอบทานผลการปฏิบัติงาน (Reviews of Operating Performance) การเก็บรักษาทรัพย์สิน (Security of Asset) การแบ่งแยกหน้าที่ (Segregation of Duties)

การควบคุมมี ๒ ด้าน คือ (๑) Hard Controls เช่น นโยบาย ขั้นตอนการปฏิบัติงาน โครงสร้างองค์กร การกำหนดอำนาจการอนุมัติ เป็นต้น (๒) Soft Controls เช่น ความซื่อสัตย์ จริยธรรม วัฒนธรรม ความรู้/ความเข้าใจ เป็นต้น

ประเภทของการควบคุมภายใน ได้แก่

(๑) เชิงป้องกัน (Preventive) คือ เพื่อป้องกันหรือลดความเสี่ยงจากความผิดพลาด/เสียหาย เช่น การแบ่งแยกหน้าที่ การควบคุมการเข้าถึงทรัพย์สิน

(๒) เชิงค้นพบ (Detective) คือ ค้นพบความผิดพลาด/เสียหายที่เกิดขึ้นแล้ว เช่น การกระทบยอด การตรวจนับสินค้าคงเหลือ

(๓) เชิงแก้ไข (Corrective) คือ แก้ไขความผิดพลาด/เสียหายที่เกิดขึ้นให้ถูกต้อง หรือลดความเสียหาย เช่น แผนฉุกเฉิน การกู้ข้อมูล

/(๔) เชิงส่งเสริม...

(๔) เชิงส่งเสริม (Directive) คือ ส่งเสริมหรือกระตุ้นให้เกิดผลตามต้องการ เช่น การให้นโยบาย/กำหนดเป้าหมาย การให้รางวัลจูงใจ

ข้อพิจารณาสำคัญ คือ การควบคุมต้องมีความสอดคล้องกับความเสี่ยง คำนึงถึงต้นทุนในการควบคุมที่มีความสัมพันธ์กับระดับความเสี่ยง

๔.๒ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ และกรอบการดำเนินงาน มาตรฐาน และกฎหมายที่เกี่ยวข้อง โดยคุณวรางคณา มุสิกะสังข์

๑) ความเสี่ยงขององค์กร ประกอบด้วย

ความเสี่ยงด้านกลยุทธ์ คือ ความเสี่ยงที่มีผลต่อความอยู่รอดขององค์กร เช่น การสูญเสียทางการเงิน ศักยภาพในการแข่งขัน เป็นต้น

ความเสี่ยงด้านการปฏิบัติงาน คือ ความเสี่ยงที่มีผลกระทบต่อการดำเนินงานขององค์กร อันเนื่องมาจากความผิดพลาดในการปฏิบัติงานของบุคลากร ระบบ หรือ กระบวนการ โดยอาจเกิดจากปัจจัยภายนอกหรือภายในก็ได้

ความเสี่ยงด้านการเงิน คือ ความเสี่ยงที่เกิดจากความผันผวนของตัวแปรทางการเงิน เช่น อัตราดอกเบี้ย อัตราแลกเปลี่ยน สภาพคล่องทางการเงิน และเครดิตความน่าเชื่อถือในการกู้ยืมเงิน เป็นต้น ซึ่งก่อให้เกิดการสูญเสียทางการเงิน

ความเสี่ยงด้านกฎ ระเบียบ คือ ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติตามกฎ ระเบียบ ข้อบังคับต่างๆ ที่เกี่ยวข้องกับองค์กร

๒) ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT) คือ ความเป็นไปได้ที่จะเกิดเหตุการณ์ไม่คาดคิดที่จะสูญเสียหรือไม่ได้มาซึ่งข้อมูลที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร หรือผลกระทบในวงกว้างต่อผู้เกี่ยวข้อง ถือเป็นส่วนหนึ่งของความเสี่ยงด้านการปฏิบัติงาน

จากผลการสำรวจในปี ๒๐๑๖ และ ๒๐๑๗ พบว่า ความเสี่ยงด้าน IT เป็นความเสี่ยงอันดับต้นๆ ของความเสี่ยงทางธุรกิจ (Top ๑๐ Global Business Risks) โดยในปี ๒๐๑๗ แนวโน้มของความเสี่ยงด้าน IT ได้แก่ ระบบ IT หลักเสียหายหรือไม่มีการลงทุนด้าน IT ที่เพียงพอ (Critical information Infrastructure Breakdown) การโจมตีทาง Cyber (Cyber Attacks) การใช้เทคโนโลยีไม่คุ้มค่า (Misuse of Technologies) การทุจริต/การถูกขโมยข้อมูล (Data Fraud or Theft) องค์กรจำเป็นต้องจัดทำแผนความปลอดภัยของข้อมูลและควบคุมความเสี่ยงด้าน IT

ความเสี่ยงด้าน IT ได้แก่ ข้อมูลไม่ถูกต้อง ข้อมูลไม่ปลอดภัย การหยุดชะงักของระบบ มีสาเหตุมาจากการใช้งานโดยบุคคลที่ไม่ได้รับอนุญาต ข้อผิดพลาดของโปรแกรม ข้อผิดพลาดของการนำเข้าข้อมูล การขัดข้องของระบบ การปฏิบัติงานด้าน IT ไม่มีประสิทธิภาพ ระบบที่มีไม่เหมาะสมสอดคล้องกับการปฏิบัติงานขององค์กร ส่งผลกระทบต่อองค์กร เช่น เกิดการทุจริต เกิดความเสียหายจากข้อผิดพลาด การตัดสินใจผิดพลาด การหยุดชะงักของธุรกิจ เป็นต้น

ความเสี่ยงอุบัติใหม่ (Emerging Risks) :

- Cyber Risk เช่น โจรสลัดไซเบอร์ที่เรียกค่าไถ่เป็น Bit Coin /มัลแวร์ Wannacry
- Social Media Risk

/๓) การจัดการ...

๓) การจัดการความเสี่ยงด้าน IT

ประโยชน์ของการควบคุมด้าน IT คือ เพื่อจัดการความเสี่ยงด้าน IT ให้อยู่ในระดับที่ยอมรับได้ ผู้บริหารและผู้ใช้งานมีความมั่นใจต่อความปลอดภัย ความถูกต้องครบถ้วน และความพร้อมใช้ของข้อมูลและระบบ IT ประกอบด้วย

(๑) การควบคุมทั่วไป (IT General control) คือ นโยบายและระเบียบปฏิบัติที่ใช้ในการบริหารจัดการด้าน IT และสภาพแวดล้อมของระบบคอมพิวเตอร์รวมทั้งระบบงานสารสนเทศต่างๆ และช่วยสนับสนุนความมีประสิทธิผลของระบบงาน เป็นการควบคุมพื้นฐานของระบบ IT เพื่อให้มั่นใจว่า ระบบ IT โดยรวมขององค์กรมีการจัดการที่ดี และเป็นส่วนหนึ่งที่จะก่อให้เกิด IT Governance โดยเป็นการควบคุมพื้นฐานที่ต้องมีเพื่อทำให้การควบคุมระบบงานมีประสิทธิภาพและประสิทธิผล มีผลต่อความถูกต้องของข้อมูลในทุกระบบงาน ได้แก่

- การวางแผนด้าน IT เพื่อใช้เป็นแผนแม่บทในการจัดทำแผนการดำเนินงานด้าน IT เพื่อให้ระบบ IT สามารถตอบสนองต่อความต้องการทางธุรกิจและเกิดประโยชน์สูงสุดต่อองค์กร โดยต้องคำนึงถึงวัตถุประสงค์ระยะสั้นและระยะยาวขององค์กร และมีการติดตามความคืบหน้าของงาน

- การจัดโครงสร้างงาน IT เพื่อให้มั่นใจว่าหน่วยงานคอมพิวเตอร์มีการแบ่งแยกหน้าที่งาน IT ที่สำคัญออกจากกันอย่างเหมาะสม ทำให้สามารถสอบทานงานระหว่างกันได้ ลดโอกาสความผิดพลาด หรือการปฏิบัติงานที่ไม่ได้รับอนุญาตอย่างทันกาล เช่น แบ่งแยกหน้าที่งานด้านการวางแผนออกจากการพัฒนาและเปลี่ยนแปลงระบบ เป็นต้น

- การพัฒนาและเปลี่ยนแปลงแก้ไขระบบ IT เพื่อให้มั่นใจว่ามีการพัฒนาระบบงาน/การเปลี่ยนแปลงระบบแก้ไขงานตรงกับความต้องการทางธุรกิจ มีการบริหารจัดการโครงการพัฒนาระบบอย่างมีประสิทธิผล มีการกำหนดกระบวนการหรือระเบียบปฏิบัติที่เหมาะสมและเป็นมาตรฐานเดียวกัน มีการควบคุมเพื่อลดผลกระทบอันเกิดจากความผิดพลาดของการแก้ไข/เปลี่ยนแปลงโปรแกรมโดยไม่ได้รับอนุญาต

- การรักษาความปลอดภัยระบบ IT เพื่อให้มั่นใจว่ามีการกำหนดนโยบายหรือกระบวนการรักษาความปลอดภัยระบบ IT มีการกำหนดการควบคุมในการเข้าถึงโปรแกรมและข้อมูล มีการพิสูจน์ตัวตนของผู้ใช้ระบบอย่างเหมาะสม มีการกำหนดเจ้าของระบบ IT และบทบาทหน้าที่อย่างชัดเจน มีการกำหนดผู้ดูแลความปลอดภัยของระบบ IT และบทบาทหน้าที่อย่างชัดเจน มีมาตรการที่ดีเพียงพอในการรักษาความปลอดภัยระบบ IT ทั้งในระดับ Logical และ Physical

- การปฏิบัติการคอมพิวเตอร์ เพื่อให้มั่นใจว่ามีการควบคุมการปฏิบัติงานของฝ่ายปฏิบัติการเพื่อสนับสนุนการทำงานของระบบประจำวันอย่างเพียงพอ การประมวลผลมีความครบถ้วนถูกต้อง การประมวลผลที่ผิดพลาดสามารถถูกค้นพบและแก้ไขได้ทันการณ์ ข้อมูลและระบบ IT มีความพร้อมใช้งานอยู่เสมอ (มีการบำรุงรักษาอุปกรณ์และระบบงาน)

- การสำรองข้อมูลและการทำแผนกู้คืนระบบ IT เพื่อให้มั่นใจว่ามีมาตรการในการกู้ระบบ IT ให้กลับมาใช้งานได้ทันการณ์และเพียงพอหลังจากเกิดเหตุการณ์

(๒) การควบคุมเฉพาะระบบงาน (Applications control) เป็นการควบคุมโดยบุคคล (Manual) หรือโดยระบบ (Automate) ซึ่งเป็นการควบคุมระดับกระบวนการหรือรายการทางธุรกิจ เพื่อให้มั่นใจว่าการอนุมัติ การบันทึกเข้า และการประมวลผลถูกต้อง สมบูรณ์เพียงครั้งเดียว ในเวลาที่เหมาะสม

- การควบคุมการนำเข้า (Input Controls) มีความสำคัญเนื่องจากเป็นต้นทางของความถูกต้องเชื่อถือได้ของข้อมูล เพื่อให้มั่นใจว่า ทุกรายการได้รับการอนุมัติก่อนการประมวลผล ทุกรายการที่ได้รับ

/การอนุมัติ...

การอนุมัติให้นำเข้ามีความถูกต้อง ครบถ้วน รายการที่ระบบปฏิเสธการประมวลผลได้รับการแก้ไขและนำเข้าใหม่ภายในเวลาที่เหมาะสม

- การควบคุมการประมวลผล (Processing Controls) เพื่อให้มั่นใจว่ารายการต่างๆ รวมทั้งรายการที่สร้างขึ้นโดยอัตโนมัติได้รับการประมวลผลอย่างเหมาะสม รายการไม่สูญหาย ไม่เพิ่มเติม ไม่ประมวลผลซ้ำ หรือมีการเปลี่ยนแปลงอย่างไม่เหมาะสม ข้อผิดพลาดจากการประมวลผลถูกตรวจพบและแก้ไขภายในระยะเวลาที่กำหนด

- การควบคุมผลลัพธ์ที่ได้จากการประมวลผล (Output Controls) เป็นการควบคุมระยะสุดท้ายเพื่อให้ได้ข้อมูล และรายงานที่ถูกต้องจากระบบ เพื่อให้มั่นใจว่า ผลลัพธ์จากการประมวลผลถูกต้อง มีการจำกัดการเข้าถึงหรือใช้ข้อมูลที่ส่งออกจากระบบเฉพาะผู้ที่ได้รับอนุญาต การส่งข้อมูลออกจากระบบไปยังบุคคลที่ได้รับอนุมัติอย่างทันเวลา

- การควบคุมด้วยแฟ้มร่องรอยการตรวจสอบ (Audit Trails) แฟ้มทะเบียนร่องรอยที่สร้างขึ้นเพื่อบันทึกกิจกรรมในระบบงาน หรือผู้ใช้งาน โดยหากมีการออกแบบและใช้งานที่ดี จะเป็นวิธีการควบคุมเชิงตรวจสอบที่มีประสิทธิภาพ เช่น การบันทึกเหตุการณ์สำคัญของผู้ใช้งาน ความพยายามเข้าระบบทรัพยากรบนระบบที่ใช้งาน

๔) กรอบการดำเนินงาน มาตรฐาน และกฎหมายที่เกี่ยวข้องกับ IT

กรอบมาตรฐานในการกำกับดูแลและการบริหารองค์กรด้าน IT ที่เป็นหลักสากล คือ COBIT Framework (Control Objective for Information and Related Technology) ซึ่งพัฒนาและปรับปรุงโดย ISACA ปัจจุบันได้มีการพัฒนาและปรับปรุง Version COBIT5 ซึ่งกล่าวถึง การตรวจสอบและการให้ความเชื่อมั่นด้าน IT การบริหารความเสี่ยงด้าน IT ความมั่นคงปลอดภัยด้าน IT กฎระเบียบที่เกี่ยวข้อง และการกำกับดูแลองค์กรที่เกี่ยวข้องกับ IT

มาตรฐานการบริหารความมั่นคงปลอดภัยสารสนเทศ ได้แก่ ISO 27000, ISO27001:2513, ISO27002:2513 กล่าวถึง นโยบายความมั่นคงปลอดภัย การจัดองค์กร การจัดการทรัพย์สินสารสนเทศ การบริหารการสื่อสารและการดำเนินการของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบสารสนเทศ การควบคุมการเข้าถึงระบบ การจัดหา การพัฒนา และบำรุงรักษาระบบสารสนเทศ การจัดการเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ เป็นต้น

กฎหมายและพระราชบัญญัติที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ กำหนดมาตรการในการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๖๐ เนื่องจาก e-Doc ได้รับการรับรองให้มีความเท่าเทียมกับเอกสาร โดย e-Doc ใช้เป็นหลักฐาน/พยานในศาลได้

๔.๓ การตรวจสอบภายใน โดยคุณอาทิตย์ เตชะสินกุล

๑) ความคาดหวังของผู้มีส่วนได้ส่วนเสียต่อผู้ตรวจสอบภายใน

ผู้ตรวจสอบภายใน (Internal Audit: IA) ควรเป็นมากกว่าผู้ให้ความเชื่อมั่น (Assurance Provider) โดยจะต้องสามารถเป็นนักแก้ปัญหา (Problem Solver) ต้องเข้าใจองค์กรในเชิงลึก (Insight Generator) และให้คำปรึกษาโดยผู้บริหารให้ความเชื่อมั่น (Trusted Advisor) จากผลการสำรวจของ PwC พบว่า ความคาดหวังใน IA ลดลง จากร้อยละ ๕๔ ในปี ๒๐๑๖ เป็นร้อยละ ๔๔ ในปี ๒๐๑๗ เนื่องจากกฎระเบียบใหม่ๆ ที่เพิ่มขึ้น การเปลี่ยนแปลงรูปแบบธุรกิจและกลยุทธ์ขององค์กร และเทคโนโลยี เป็นต้น ทำให้ IA ขาดทักษะใหม่ๆ และ

/ก้าวไม่ทัน...

ก้าวไม่ทันต่อการเปลี่ยนแปลง ดังนั้น IA ควรต้องมีการเตรียมการและปรับตัวให้ทันต่อเทคโนโลยี และควรนำเครื่องมือใหม่ๆ มาช่วยสนับสนุนการทำงาน เช่น ACL Program เป็นต้น

๒) ทักษะที่จำเป็นสำหรับ IA

- ทักษะส่วนบุคคล : การวิเคราะห์หาสาเหตุ และการสื่อสาร
- ทักษะเฉพาะด้าน : การคำนวณ/บัญชี การบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ (พื้นฐาน) ความรู้/ความเข้าใจในองค์กร และการวิเคราะห์/สรุปข้อมูล

การพัฒนาทักษะให้เกิดประสิทธิภาพสูงสุด ควรพัฒนาโดย On the Job Training: Coaching: Classroom ในสัดส่วน ๗๐: ๒๐: ๑๐

๓) การวางแผนการตรวจสอบตามแนวความเสี่ยง (Risk-Based IA Plan)

การประเมินความเสี่ยงเพื่อวางแผนการตรวจสอบ เริ่มจากการวิเคราะห์กลยุทธ์ขององค์กร ประเมินความเสี่ยงที่คาดว่าจะมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร (ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงด้านการเงิน ความเสี่ยงด้านกฎระเบียบ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ) ประเมินระบบการควบคุมภายในที่มีอยู่ขององค์กร และจัดทำ Risk Map โดยพิจารณาจากโอกาส (Likelihood) และผลกระทบ (Impact) พร้อมทั้งจัดลำดับความเสี่ยง เพื่อใช้วางแผนการตรวจสอบและจัดสรรทรัพยากรที่จะใช้ในการตรวจสอบ

ผลการประเมินความเสี่ยงจะเป็นส่วนหนึ่งของการวางแผนการตรวจสอบ อย่างไรก็ตามต้องพิจารณาองค์ประกอบอื่นๆ ร่วมด้วย เช่น ข้อกังวลของผู้บริหาร ประเด็นข้อสงสัยหรือข้อตรวจพบของสำนักงานการตรวจเงินแผ่นดิน เป็นต้น

๔) องค์ประกอบของรายงานการตรวจสอบภายในที่ดี

คุณภาพของการรายงานตาม IIA Standard ๒๔๒๐ คือ การรายงานผลต้องมีความถูกต้อง เที่ยงธรรม ชัดเจน รัดกุม (กระชับ) สร้างสรรค์ ครบถ้วน และทันกาล

๔.๔ การจัดการความเสี่ยงด้านการปฏิบัติงาน IT โดยคุณวรางคณา มุสิกะสังข์

๑) Risk Based IT Audit approach ประกอบด้วย

- การรวบรวมข้อมูลและแผนที่เกี่ยวข้อง เช่น ความรู้ที่เกี่ยวข้องกับองค์กรและอุตสาหกรรม ผลการตรวจสอบปีที่ผ่านมา ข้อมูลทางการเงิน กฎระเบียบที่เกี่ยวข้อง การประเมินความเสี่ยงขององค์กร เป็นต้น
- ทำความเข้าใจระบบควบคุมภายใน ได้แก่ สภาพแวดล้อมการควบคุม กระบวนการควบคุม การประเมินความเสี่ยง กิจกรรมควบคุม ผลการประเมินความเสี่ยง
- Compliance Tests เช่น ทดสอบการปฏิบัติตามนโยบาย IT ทดสอบปฏิบัติตามหน้าที่ที่แบ่งแยก เป็นต้น
- Substantive Tests เช่น วิเคราะห์กระบวนการ ทดสอบ account balances เป็นต้น
- สรุปผลการตรวจสอบ ให้ข้อเสนอแนะ และจัดทำรายงานผลการตรวจสอบ

๒) IT Audit Scope

- IT General Review : ตรวจสอบสภาพแวดล้อมด้าน IT การพัฒนาระบบ การเปลี่ยนแปลงระบบ การเข้าถึงระบบและข้อมูล การปฏิบัติงานด้านคอมพิวเตอร์
- Application Controls : ตรวจสอบการอนุมัติผู้ใช้งานระบบและข้อมูล การกำหนดสิทธิการเข้าระบบ การบันทึกข้อมูล การประมวลผล ผลลัพธ์ที่ได้จากระบบ การเชื่อมข้อมูลระหว่างระบบ

/- Computer...

- Computer Assisted Audit Techniques (CAATs) : ใช้เครื่องมือ/โปรแกรมช่วยในการทดสอบระบบ

๕. สรุปผลการประเมินความพึงพอใจในการจัดกิจกรรม

กตส. ได้สำรวจความพึงพอใจของผู้เข้าร่วมกิจกรรม KM Networking ครั้งที่ ๓ โดยใช้แบบประเมินผลการอบรม/สัมมนาของสำนักงานเลขานุการกรม เพื่อนำไปปรับปรุงการดำเนินโครงการในปีต่อไป โดยมีรายละเอียด ดังนี้

๔.๑ หัวข้อตามแบบประเมินผล ประกอบด้วย ๕ ประเด็นหลัก ดังนี้

๑) การบรรลุวัตถุประสงค์ของโครงการ ได้แก่ หัวข้อเรื่องมีความสอดคล้องและสนับสนุนการปฏิบัติงานในภารกิจของ กตส. และหัวข้อเรื่องมีความสอดคล้องและสนับสนุนการปฏิบัติงานในภารกิจของสำนัก ศูนย์ กลุ่ม

๒) ความรู้ความเข้าใจก่อนและหลังฝึกอบรม

๓) การนำความรู้ไปปรับใช้ในการปฏิบัติงาน

๔) ความพึงพอใจต่อภาพรวมของโครงการ ประกอบด้วย

(๑) ด้านกระบวนการ ได้แก่ การแจ้งรายละเอียด การกำหนดรูปแบบ/กิจกรรม การกำหนดกลุ่มเป้าหมายชัดเจน จำนวนคนเข้าร่วมเหมาะสม สื่อประกอบการสอนเหมาะสม อุปกรณ์การสอนเหมาะสม

(๒) ด้านเจ้าหน้าที่ที่ให้บริการ ได้แก่ การให้ข้อมูลโครงการที่ครบถ้วน การตอบข้อซักถามที่ชัดเจน ตรงประเด็น กิริยามารยาท การแต่งกายเหมาะสม เจ้าหน้าที่กระตือรือร้นเต็มใจให้บริการ

(๓) ด้านวิทยากร ได้แก่ ความรอบรู้ในหัวข้อวิชาของวิทยากร การจัดลำดับความสัมพันธ์ของเนื้อหาวิชาเหมาะสม วิทยากรมีเทคนิค/วิธีการในการถ่ายทอดให้เข้าใจง่าย เอกสารประกอบการสอนครบถ้วน ชัดเจน การยกตัวอย่าง/กิจกรรมในการฝึกอบรม การสรุปและทบทวนให้เข้าใจยิ่งขึ้น

(๔) ด้านสิ่งอำนวยความสะดวก ได้แก่ ขนาดห้องเหมาะสมกับจำนวนผู้เข้าร่วมโครงการ การจัดห้องเหมาะสมกับหัวข้อการสอน ความสะดวกในการเดินทาง อาหารและเครื่องดื่มเหมาะสม

(๕) ด้านคุณภาพ ได้แก่ ความสอดคล้องของเนื้อหาหลักสูตรกับความต้องการ เนื้อหาหลักสูตรเป็นปัจจุบันทันต่อการเปลี่ยนแปลง ความรู้ที่ได้รับสามารถนำไปปรับใช้ในการปฏิบัติงานได้ ความคุ้มค่าของการฝึกอบรม

๕) ความเหมาะสมของระยะเวลาการจัดฝึกอบรม

โดยกำหนดระดับคะแนนเป็นระดับ ๑ - ๕ โดยระดับ ๑ คะแนน แสดงถึงความพึงพอใจน้อยที่สุด ไล่ไปตามลำดับจนถึงระดับ ๕ คะแนน ที่แสดงถึงความพึงพอใจมากที่สุด

๔.๒ เกณฑ์การประเมินผล ใช้วิธีการทางสถิติเบื้องต้นในการวิเคราะห์ข้อมูล ได้แก่ วิธีค่าเฉลี่ยเลขคณิตถ่วงน้ำหนัก (Weighted arithmetic mean) และวิธีค่าเฉลี่ยเลขคณิต (Arithmetic mean) โดยมีเกณฑ์การประเมินผลตามตารางที่ ๑ ดังนี้

/ตารางที่ ๑...

ตารางที่ ๑ เกณฑ์การประเมิน

คะแนน	ร้อยละ	เกณฑ์
ตั้งแต่ ๔ ขึ้นไป - ๕	๘๐% ขึ้นไป	พึงพอใจมากที่สุด
ตั้งแต่ ๓ ขึ้นไป – ๔	๖๐% ขึ้นไป – ๘๐%	พึงพอใจมาก
ตั้งแต่ ๒ ขึ้นไป - ๓	๔๐% ขึ้นไป – ๖๐%	พึงพอใจปานกลาง
ตั้งแต่ ๑ ขึ้นไป - ๒	๒๐% ขึ้นไป – ๔๐%	พึงพอใจน้อย
ตั้งแต่ ๐ - ๑	๐% – ๒๐%	ไม่พึงพอใจ

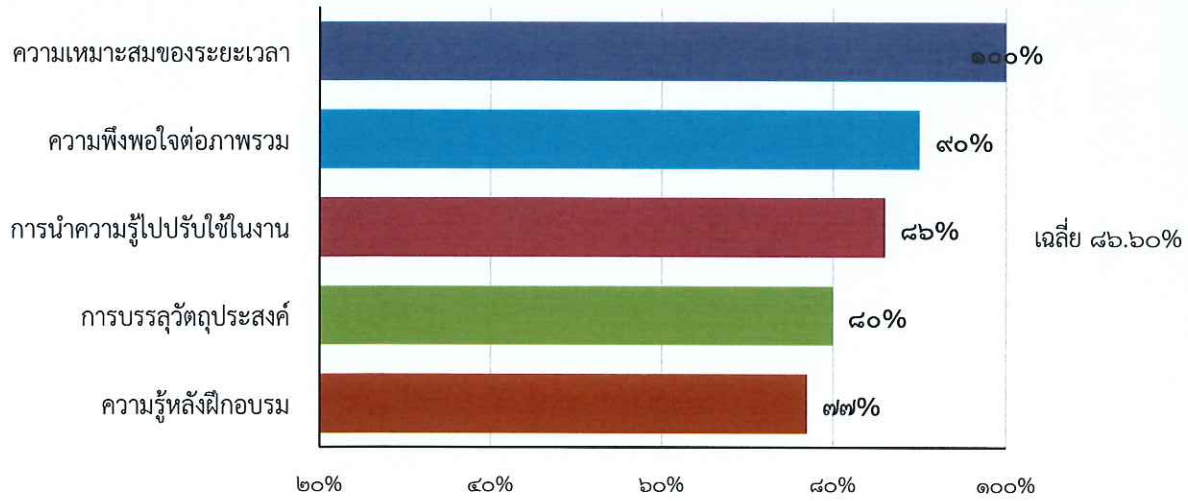
๔.๓ ตัวชี้วัด คือ ความพึงพอใจในการเข้าร่วมกิจกรรมไม่น้อยกว่าร้อยละ ๘๐

๔.๔ สรุปผลการประเมิน

มีผู้ตอบแบบประเมิน จำนวน ๒๒ ชุด จากทั้งหมด ๔๔ ชุด หรือคิดเป็นร้อยละ ๕๐ เนื่องจากได้มีการเปลี่ยนรูปแบบการประเมินโดยใช้แบบสอบถาม Online ผ่าน Application Line บนโทรศัพท์มือถือ ทำให้ไม่สามารถติดตามว่าผู้เข้ารับการอบรมทำการประเมินให้หรือยัง ทำได้เพียงการประชาสัมพันธ์และขอความร่วมมือในการตอบแบบประเมิน

ผลการประเมินความพึงพอใจ ๕ ประเด็นหลัก พบว่า ประเด็นที่ได้รับความพึงพอใจมากที่สุด คือ ความเหมาะสมของระยะเวลา โดยได้รับความพึงพอใจร้อยละ ๑๐๐ และประเด็นที่ได้รับความพึงพอใจน้อยที่สุด คือ ความรู้ที่ได้รับหลังการฝึกอบรม โดยได้รับความพึงพอใจร้อยละ ๗๗ และมีผลการประเมินความพึงพอใจเฉลี่ยใน ๕ ประเด็นหลักอยู่ที่ ร้อยละ ๘๕.๖๐ อยู่ในเกณฑ์พึงพอใจมากที่สุด รายละเอียดตามแผนภาพที่ ๑

แผนภาพที่ ๑ : ผลการประเมินความพึงพอใจในการเข้าร่วมกิจกรรม ครั้งที่ ๓



รายละเอียดในแต่ละประเด็นย่อย สรุปได้ดังนี้

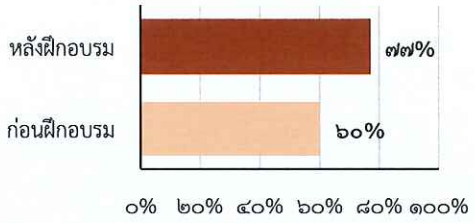
- การบรรลุวัตถุประสงค์ของโครงการ พบว่า มีความสอดคล้องกับภารกิจของ กตส. ร้อยละ ๘๖ และสอดคล้องกับภารกิจของผู้เข้าร่วมกิจกรรม ร้อยละ ๘๐ รายละเอียดตามแผนภาพที่ ๒

/- ความรู้...

- ความรู้ความเข้าใจก่อนและหลังฝึกอบรม พบว่า ผู้เข้าร่วมกิจกรรมมีความรู้ความเข้าใจก่อนการฝึกอบรม ร้อยละ ๖๐ และผู้เข้าร่วมกิจกรรมมีความรู้ความเข้าใจหลังการฝึกอบรม ร้อยละ ๗๗ เพิ่มขึ้นร้อยละ ๑๗ รายละเอียดตามแผนภาพที่ ๓

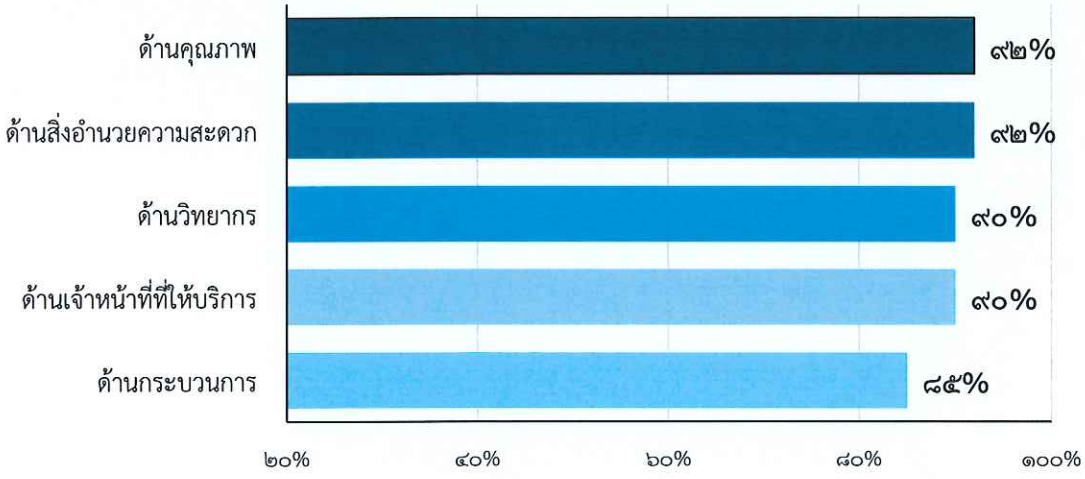
แผนภาพที่ ๒ ผลการประเมินการบรรลุวัตถุประสงค์ของโครงการ

แผนภาพที่ ๓ ผลการประเมินความรู้ความเข้าใจก่อนและหลังฝึกอบรม



- ความพึงพอใจต่อภาพรวม พบว่า ประเด็นที่พึงพอใจมากที่สุด คือ ด้านคุณภาพ ร้อยละ ๙๒ และประเด็นที่พึงพอใจน้อยที่สุด คือ ด้านกระบวนการ ซึ่งประกอบด้วย การแจ้งรายละเอียด การกำหนดรูปแบบ/กิจกรรม การกำหนดกลุ่มเป้าหมายชัดเจน จำนวนคนเข้าร่วมเหมาะสม สื่อประกอบการสอนเหมาะสม อุปกรณ์การสอนเหมาะสม ร้อยละ ๘๕ รายละเอียดตามแผนภาพที่ ๔

แผนภาพที่ ๔ ผลการประเมินความพึงพอใจของภาพรวมของโครงการ



กลุ่มตรวจสอบภายใน
สำนักงานบริหารหนี้สาธารณะ
๑๑ สิงหาคม ๒๕๖๐