ฝทบ.

เลขที่.................

วันที่.................

....

ศตส.1 490

สส. 31/8/59

.1 ผชก. (สายใน)

เลขที่ 1350

DCS -

วันที่ 1 ก.ย.59

เวลา 13:19

ฝทบ.

เลขที่ 4938

วันที่ 31 ส.ค.2559

เวลา 13:53

รายงานสรุปการฝึกอบรม/สัมมนาภายนอก ประจำปี 2559

เลขที่ 2369

วันที่ 1/9/59

เวลา 15.27

1512

14.07

เรียน รผบ. ผ่าน ผชก.(นายสุชินฯ) ผอ.ฝทบ. ผอ.สตส ผอ.กตส

1. ข้าพเจ้า นาย ภณ วัชรินทร์ ตำแหน่ง พนักงานตรวจสอบ 4 แผนก ตส.2 กอง กตส. ฝ่าย สตส. ได้รับอนุมัติให้ไปเข้าร่วมการฝึกอบรม/สัมนาหลักสูตร/เรื่อง IT Audit for Non - IT Auditor Master Class จัดโดย สถาบันวิทยาการ สวทช ระหว่างวันที่ 25-29 ก.ค.2559 สถานที่จัด โรงแรมแกรนด์ สุขุมวิท ซอย 6 ค่าลงทะเบียนอบรม/สัมมนา ☑ เสียค่าใช้จ่าย 21,400 บาท ☐ ไม่เสียค่าใช้จ่าย

2. ข้าพเจ้าขอรายงานสรุปการฝึกอบรม/สัมมนา ดังนี้

2.1 สรุปรายละเอียดเนื้อหาของหลักสูตร (ไม่เขียนเฉพาะหัวข้อ ควรมีการบรรยายสรุป พร้อมแนบเอกสารประกอบการอบรม เพื่อถ่ายทอดองค์ความรู้ต่อไป)

อบรมวันที่ 1 หัวข้อ สารสนเทศสำหรับผู้ตรวจสอบ

เรียนรู้องค์ประกอบของระบบเทคโนโลยีสารสนเทศ ฐานข้อมูล เครือข่าย เทคโนโลยีที่เกี่ยวข้อง เรียนรู้กระบวนการ ขั้นตอนและเครื่องมือที่ใช้ในการพัฒนาระบบสารสนเทศ รวมทั้งการดำเนินงานและติดตามโครงการพัฒนาระบบสารสนเทศเพื่อสร้างความรู้ความเข้าใจในการพัฒนาระบบ

- นิยามของ Policy ถึง Procedure ได้แก่

1. นโยบาย (Policy) เป็นสิ่งสำคัญสำหรับกระบวนการทำงานที่กำหนดโดยองค์กรเพื่อจะประกาศให้บุคคลากรในหน่วยงานทราบเกี่ยวกับ มาตรฐาน (Standard) มาตรวัด (Baseline) แนวทาง (Guideline) และ ขั้นตอน (Procedure) ที่องค์กรจะนำมาใช้ในการชี้วัดประสิทธิภาพและคุณภาพของงานภายในองค์กร

2. มาตรฐาน (Standard) เป็นเสมือนข้อตกลงที่จะต้องประกาศให้คนในองค์กรรับรู้กันเกี่ยวกับเป้าหมายขององค์กรซึ่งองค์กรแต่ละองค์กรสามารถสร้างมาตรฐานของตนเองได้ถ้าหากมีลักษณะงานที่เป็นรูปแบบเฉพาะไม่เหมือนองค์กรอื่นหรือไม่มีองค์กรใดที่มีกระบวนการทำงานที่คล้ายกัน แต่หลายๆ องค์กรมักมีกระบวนการทำงานที่คล้ายกันในเฉพาะเรื่องจึงมีองค์กรส่วนกลางที่เรียกว่า International Organization for Standardization หรือ ISO เป็นผู้กำหนดมาตรฐานกลางหรือกระบวนการการทำงานที่ดีที่ได้รับการยอมรับจากหลายองค์กรทั่วโลกที่จะแสดงให้เห็นถึงกระบวนการทำงานในเฉพาะเรื่อง ซึ่งในแต่ละมาตรฐานจะมีจุดเด่นแตกต่างกัน ขึ้นอยู่กับการนำมาตรฐานในแต่ละเรื่องมาปรับใช้ให้ตรงกับกระบวนการนั้นๆ ขององค์กร โดยในบางมาตรฐานจะมีผู้ตรวจสอบภายนอก ที่สอบผ่านคุณสมบัติผู้ออกใบรับรองมาตร ฐานในแต่ละหัวข้อ เป็นผู้ตรวจสอบและออกใบรับรอง certificate ในแต่ละมาตรฐานให้กับองค์กรที่ผ่านคุณสมบัติที่มาตรฐานกำหนด การผ่านมาตรฐานในระดับสากล ไม่ได้เป็นตัวชี้วัดว่าองค์กรนั้นมีกระบวนการการทำงานที่ดี

ที่สุด แต่เป็นตัวบ่งบอกว่า องค์กรเราได้ปฏิบัติตามกระบวนการต่างๆที่เป็นขั้นต่ำที่องค์กรในระดับสากลได้ปฏิบัติกันอยู่

3. มาตรวัด (Baseline) หมายถึง ค่าที่เป็นตัวเลขหรือสามารถวัดได้อาจจะหมายถึง ค่าสูงสุด ค่าต่ำสุด ค่าเฉลี่ย หรือ ค่าใดๆก็ตามที่สามารถชี้วัดได้ว่าหากอยู่ในระยะดังกล่าวถือว่าอยู่ในมาตรฐานหรือองค์กรสามารถยอมรับได้

4. แนวทาง (Guideline) หมายถึงตัวอย่างที่เป็นเป้าหมายเพื่อให้ปฏิบัติตามเพื่อให้บรรลุวัตถุประสงค์ตามนโยบายที่องค์กรตั้งไว้

5. ขั้นตอน (Procedure) หมายถึงรายละเอียดในแต่ละเรื่องเปรียบเสมือนเฉลยวิธีในการปฏิบัติขั้นตอนในแต่ละอย่างที่องค์กรกำหนดเพื่อให้บรรลุเป้าหมายในแต่ละเรื่อง

- องค์ประกอบของการตรวจสอบ ประกอบด้วย 5 องค์ประกอบ ดังนี้

1. สภาพที่เกิดขึ้นจริง ได้แก่ สิ่งที่ผู้ตรวจสอบประมวลผลข้อเท็จจริงจากการสังเกตการณ์

2. เกณฑ์การตรวจสอบ ได้แก่ หลักเกณฑ์ที่จะใช้ในการตรวจสอบ โดยกำหนดจากกฎหมาย มาตรฐานการปฏิบัติงาน แผนงานที่กำหนด หรือหลักการปฏิบัติงานที่ดี

3. ผลกระทบ ได้แก่ ข้อมูลแสดงโอกาสความเสี่ยง หรือผลเสียหายที่จะเกิดขึ้นจากปัญหานั้นโดยระบุในเชิงปริมาณ จำนวนความเสียหาย จำนวนวันที่ล่าช้า การระบุผลกระทบที่ชัดเจนมีสาระสำคัญ เป็นปัจจัยที่จะทำให้ข้อตรวจพบได้รับความสนใจจากผู้ที่เกี่ยวข้อง

4. สาเหตุ ได้แก่ ข้อมูลแสดงสาเหตุ สาเหตุที่เกิดปัญหานั้นเกิดจากระบบการควบคุมภายในที่ไม่ดี หรือการปฏิบัติตามกฎระเบียบ ข้อบังคับ ระบบ นโยบาย มาตรฐาน ที่หน่วยงานกำหนด

5. ข้อเสนอแนะ เป็นข้อมูลตามความเห็นของผู้ตรวจสอบที่เสนอแนะขึ้น โดยอาจจะเสนอตามความเห็นของผู้ตรวจสอบ ผู้เชี่ยวชาญ และผู้ที่เกี่ยวข้อง เพื่อให้ข้อเสนอแนะนั้นมีคุณค่าเป็นที่ยอมรับและปฏิบัติได้

- ขั้นตอนและเครื่องมือในการพัฒนาระบบสารสนเทศ System Development Methodology

1. Waterfall Model เป็นต้นแบบการพัฒนาระบบที่เหมาะกับงานที่มีการกำหนดขอบเขตความต้องการ ขั้นตอนการปฏิบัติงานที่ชัดเจน และมักเกิดขึ้นซ้ำๆ

2. Prototype Model เป็นต้นแบบการพัฒนาระบบที่เหมาะกับงานที่มีการกำหนดขอบเขตงานความต้องการ ขั้นตอนการปฏิบัติงานที่อาจจะต้องมีการปรับเปลี่ยนจากต้นแบบหลักเล็กน้อย อาจจะต้องใช้ระยะเวลาในการเก็บความต้องการจากผู้ใช้งานเพิ่มเติมในช่วงแรกของกระบวนการทำงาน และปรับเปลี่ยนตามความต้องการ (เฉพาะช่วงแรกในการขอเท่านั้น)

3. Spiral Model เป็นต้นแบบการพัฒนาระบบที่เหมาะกับระบบงานที่ไม่เคยเกิดขึ้นมาก่อนตลอดกระบวนการพัฒนาระมีการพัฒนาไปพร้อมๆกับการทดสอบระบบเป็นระยะและมีการปรับเปลี่ยนข้อกำหนดต่างๆได้ตลอดกระบวนการพัฒนา

4. RAD Model เป็นต้นแบบการพัฒนาที่มีข้อดีคือสามารถสื่อสารกับผู้ให้ขอบเขตงานได้ตลอดเวลาเพื่อป้องกันการพัฒนาระบบไม่ตรงกับความต้องการของผู้ใช้งาน โดยข้อจำกัดของต้นแบบนี้อาจจะต้องให้ผู้ใช้งานหรือผู้พัฒนาระบบมีการประสานงานกันตลอดเวลาที่ดำเนินโครงการซึ่งเป็นไปได้ยากที่ผู้ใช้งานจะอยู่ร่วมกับผู้พัฒนาระบบตลอดนอกเสียจากให้ผู้พัฒนาระบบมาทำงานอยู่สถานที่เดียวกับผู้ใช้งานตลอดกระบวนการพัฒนาระบบ

5. Packaged Software Model เป็นต้นแบบการพัฒนาระบบโดยใช้วิธีการเลือกซื้อระบบที่ถูกพัฒนาเสร็จแล้ว ในช่วงแรกของกระบวนการจะใช้ระยะเวลาในการศึกษาความต้องการของผู้ใช้งานและความสามารถของระบบที่มีขาย ความยากของต้นแบบนี้คือการคำนวนค่าใช้จ่ายในการปรับปรุง Software ให้ตรงตามความต้องการของผู้ใช้งาน กรณีที่ค่าใช้จ่ายในการปรับปรุงสูงกว่าการพัฒนาระบบใหม่ ให้เลือกการพัฒนาระบบใหม่จะเป็นการประหยัดต้นทุนมากกว่า

อบรมวันที่ 2 หัวข้อ ISO 27001 กับการบริหารความเสี่ยงเทคโนโลยีสารสนเทศ และกฎหมายไอซีที

ศึกษามาตรฐาน ISO 27001 เพื่อนำมาใช้วิเคราะห์ความเสี่ยงและประยุกต์ใช้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมทั้งหลักกฎหมายที่เกี่ยวข้องกับการกระทำผิดด้านคอมพิวเตอร์ และกรณีศึกษาที่น่าสนใจของสถาบันการเงินกับการควบคุมความเสี่ยงผ่านหลักเกณฑ์การควบคุมความเสี่ยงของธนาคารแห่งประเทศไทย

- ความมั่นคงปลอดภัยของระบบสารสนเทศ หมายถึง การรักษาไว้ซึ่ง ความลับของข้อมูล ความครบถ้วนของข้อมูล สภาพความพร้อมใช้ของข้อมูล เพื่อป้องกันทรัพย์สินสารสนเทศ จากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลง แก้ไข ทำลาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ (พรฎ.ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2553)
- มาตรฐาน ISO 27001 เป็นมาตรฐานที่ให้ความสำคัญกับการบริหารความเสี่ยงเทคโนโลยีสารสนเทศให้อยู่ในเกณฑ์ที่สามารถยอมรับได้ โดยมีข้อกำหนดต่างๆให้ปฏิบัติ และติดตามเฝ้าระวังความเสี่ยง รวมถึงการประเมินความเสี่ยงในทุกๆรอบปี
- วัตถุประสงค์การควบคุมและมาตรการควบคุมตามมาตรฐาน ISO 27001:2013 ประกอบด้วย 14 องค์ประกอบ ได้แก่

A5 นโยบายการรักษาความมั่นคงปลอดภัย จะต้องมีการระบุทิศทางการบริหารจัดการและการสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศโดยสอบคล้องกับความต้องการทางธุรกิจ กฎหมาย และระเบียบข้อบังคับที่เกี่ยวข้อง โครงสร้างของนโยบายประกอบด้วย

- นโยบาย เป็นเอกสารกำหนดทิศทาง และกรอบการบริหารจัดการ
- มาตรฐาน เป็นเอกสารกำหนดขอบเขตและวิธีการในการดำเนินการเพื่อให้เป็นไปตามนโยบาย ตลอดจนกำหนดหน้าที่และความรับผิดชอบของส่วนงานและบุคคลที่เกี่ยวข้อง
- ขั้นตอนการปฏิบัติ เป็นเอกสารกำหนดขั้นตอนการปฏิบัติแสดงถึงความสัมพันธ์ของผู้ดำเนินการ เอกสารที่เกี่ยวข้องระหว่างขั้นตอนการปฏิบัติให้สอดคล้องกับนโยบาย และมาตรฐานต่างๆ

A6 **โครงสร้างความมั่นคงปลอดภัยสารสนเทศ** เพื่อให้มีการแบ่งแยกหน้าที่ความรับผิดชอบที่จะทำให้ขัดต่อการปฏิบัติงานโดยทำให้การเปลี่ยนแปลงทรัพย์สินขององค์กรหรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์ โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาก็ตาม ต้องมีการแยกหน้าที่ดังกล่าวออกจากกันเพื่อลดความเสี่ยงในการเกิดปัญหาภายหลัง

A7 **ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล** เพื่อให้พนักงานและผู้ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบ ตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย รวมทั้งเพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยนหรือสิ้นสุดการจ้างงาน

A8 **การบริหารจัดการทรัพย์สิน** ต้องมีการกำหนดบัญชีทรัพย์สิน ผู้รับผิดชอบต่อทรัพย์สินที่ถือครอง เพื่อกำหนดให้มีการใช้ทรัพย์สินอย่างเหมาะสม รวมถึงการคืนทรัพย์สินเมื่อสิ้นสุดการจ้างงาน

A9 **การควบคุมการเข้าถึง** ต้องมีการกำหนดชั้นของการเข้าถึงสารสนเทศ เพื่อป้องกันการเข้าถึงระบบและบริหารโดยไม่ได้รับอนุญาต และให้ผู้ที่มีสิทธิ์ในการใช้ระบบและบริการสามารถใช้งานได้เฉพาะหน้าที่ๆตนได้รับมอบหมายเท่านั้น

A10 **การเข้ารหัสข้อมูล** เพื่อให้สามารถป้องกันความลับ การปลอมแปลง หรือคงไว้ซึ่งความถูกต้องของข้อมูลสารสนเทศ ต้องมีมาตรฐานการเข้ารหัสข้อมูลในส่วนที่มีความสำคัญอย่างเหมาะสม

A11 **ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม** ต้องมีการกำหนดพื้นที่ๆต้องการการรักษาความปลอดภัย (Secure Areas) ยกตัวอย่างเช่น Data Center เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

A12 **ความมั่นคงปลอดภัยสำหรับการดำเนินงาน** ต้องมีการกำหนดขั้นตอนการปฏิบัติงานหน้าที่ความรับผิดชอบ การป้องกันโปรแกรมที่ไม่ประสงค์ดี การสำรองข้อมูล การบันทึกล็อกและการเฝ้าระวัง การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริหาร การบริหารจัดการช่องโหว่ทางเทคนิค เช่น กรณีที่มีการพัฒนาระบบ จะต้องมีการแยกสภาพแวดล้อมสำหรับการพัฒนาระบบ การทดสอบ และการให้บริการออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

A13 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล เพื่อให้มีการรักษาความมั่นคงปลอดภัยต่อการสื่อสารกันภายในองค์กรและหน่วยงานภายนอก เช่น กำหนดให้มีการแบ่งแยกเครือข่ายระหว่างสารสนเทศภายในและภายนอก ปกป้องข้อมูลการถ่ายโอนสารสนเทศภายในองค์กร และการถ่ายโอนกับหน่วยงานภายนอก จะต้องมีการกำหนด นโยบาย ขั้นตอนการปฏิบัติ ข้อตกลง สำหรับการถ่ายโอนสารสนเทศ รวมทั้งข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ

A14 การจัดหา พัฒนา และบำรุงรักษาระบบ ต้องมีการวิเคราะห์และกำหนดความต้องการด้านความมั่นคงความปลอดภัยของระบบสารสนเทศ เพื่อความมั่นคงปลอดภัยของบริการบนเครือข่าย ป้องกันการธุรกรรมของบริการสารสนเทศ ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน รวมถึงการปกป้องข้อมูลที่ใช้ในการทดสอบระบบด้วยการจำลองข้อมูลชุดใหม่โดยไม่ใช่ข้อมูลจริงในการทดสอบระบบ

A15 ความสัมพันธ์กับผู้ให้บริการภายนอก เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก รวมทั้งรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงการให้บริการของผู้ให้บริการภายนอก

A16 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริการจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยให้ได้รับทราบ

A17 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ เพื่อให้มีการจัดทำแผนการบริหารความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรในการรับมือกับภัยที่มีความเสี่ยงที่จะเกิดขึ้นและสามารถบริหารจัดการได้อย่างเป็นระบบ

A18 ความสอดคล้อง เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับหรือสัญญาจ้าง ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และที่เป็นความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ควรมีการระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง เช่น สิทธิในทรัพย์สินทางปัญญา การป้องกันข้อมูล ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล รวมทั้ง การทบทวนความมั่นคงปลอดภัยสารสนเทศให้มีความสอดคล้องกับนโยบายและขั้นตอนการปฏิบัติขององค์กรอย่างสม่ำเสมอ

- กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ได่แก่
    - พ.ร.บ.ลิขสิทธิ์ พ.ศ.2537 และ พ.ร.บ.ลิขสิทธิ์ (ฉบับที่2) พ.ศ.2558
    - พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ.2540
    - พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 และ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่2) พ.ศ.2551
        - พ.ร.ฎ.กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2551

- พ.ร.ฎ.ว่าด้วยการควบคุมดูแลธุรกิจบริการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ.2551
- พ.ร.ฎ.ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2553

* พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

อบรมวันที่ 3 หัวข้อ3.1 บทบาทหน้าที่ของผู้ตรวจสอบเทคโนโลยีสารสนเทศ (IT Auditor)

ศึกษาและทำความเข้าใจบทบาทหน้าที่ความรับผิดชอบของ General Auditor และ IT Auditor รวมทั้งความต้องการของผู้บริหารและผู้มีส่วนได้ส่วนเสียขององค์กร (Stakeholders)

งานตรวจสอบภายในเป็นลักษณะงานสนับสนุนผู้รับผิดชอบในการปฏิบัติหน้าที่งานตรวจสอบจึงไม่ควรมีอำนาจสั่งการหรือมีอำนาจบริหาร งานในสายงานที่ตรวจสอบ และต้องมีความ เป็นอิสระในกิจกรรมที่ตนตรวจสอบ เพื่อให้การปฏิบัติงานเป็นไปอย่างอิสระทั้งในการปฏิบัติงานและทัศนคติของผู้ตรวจสอบ ความเป็นอิสระมีองค์ประกอบที่สำคัญ 2 ส่วน ได้แก่

1. สถานภาพในองค์กรของผู้ตรวจสอบภายใน และความสนับสนุนที่ผู้ตรวจสอบภายในได้รับจากฝ่ายบริหาร นับว่าเป็นปัจจัยที่สำคัญยิ่งที่ ส่งผลกระทบต่อระดับคุณภาพ และคุณค่าของบริการที่ผู้ตรวจสอบภายในจะให้แก่ฝ่ายบริหาร

2. ผู้ตรวจสอบภายในไม่ควรเข้าไปมีส่วนได้เสีย หรือส่วนร่วมในการปฏิบัติงานขององค์กร ในกิจกรรมที่ผู้ตรวจสอบภายในต้องตรวจสอบหรือประเมินผล ผู้ตรวจสอบภายในต้องมีความเป็นอิสระทั้งในการปฏิบัติงานและการเสนอความเห็นในการตรวจสอบ ดังนั้น จึงมิควรเป็นกรรมการในคณะกรรมการ ใด ๆ ขององค์กร หรือหน่วยงานในสังกัดอันมีผลกระทบต่อความเป็นอิสระในการปฏิบัติงานและการเสนอความเห็น

อบรมวันที่ 3 หัวข้อ 3.2 การตรวจสอบธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

ศึกษากรอบแนวคิด GRC (Governance ,Risk and Compliance) ทั้งระดับนโยบาย ระดับกลยุทธ์ และระดับปฏิบัติการ เพื่อมุ่งสู่การบริหารกิจการที่ดีสร้างมูลค่าให้แก่องค์กรภายใต้เกณฑ์ความเสี่ยงทั่วไปและความเสี่ยงด้านเทคโนโลยีสารสนเทศในระดับที่ยอมรับได้ รวมทั้งแนวทางการตรวจสอบธรรมาภิบาลด้านเทคโนโลยีสารสนเทศกับมาตรฐาน PMBOK และ Six Sigma

- โครงการในด้าน IT ต้องมีการวัดคุณค่า โดยใช้เกณฑ์ที่สามารถวัดได้ เช่น E-mail ต้องมีการวัดจำนวนในการส่งต่อวัน ระบบสารบรรณ ต้องมีการวัด จำนวนการค้นหาและการอัพโหลดดาวน์โหลดเอกสาร
- การตั้งวัตถุประสงค์ของโครงการ IT เมื่อมีการตั้งวัตถุประสงค์ไม่ว่าจะเพื่ออะไรก็ตามสิ่งที่ได้กำหนดไว้ในวัตถุประสงค์ เมื่อโครงการเสร็จสิ้นผลที่เกิดขึ้นภายใต้วัตถุประสงค์ที่ได้เขียนไว้จะต้องเกิดขึ้น

- ต้องมีการประเมินความคุ้มค่าในระบบงานและโครงการที่สำคัญโดยเฉพาะโครงการที่ใช้งบประมาณสูง เพื่อใช้ในการวัดคุณค่าของโครงการ
- เครื่องมือที่ใช้ในการขับเคลื่อนแผนงานต่างๆให้อยู่ในวิธีการปฏิบัติงานที่ดีคือ COBIT 5
- สิ่งที่ยากที่สุดของการบริหารโครงการคือการติดตามประเมินความเสี่ยงต้องทำเป็นประจำ
- Project Management Body of Knowledge (PMBOK) เป็นกระบวนการในการควบคุมและบริหารจัดการโครงการตั้งแต่ขั้นตอนการอนุมัติให้จัดทำโครงการ การวางแผนโปรเจค การดำเนินโครงการ ตลอดจนการปิดโครงการ โดนส่วนที่ PMBOK เน้นมากที่สุดคือการควบคุมทรัพยากร คน เงิน เวลา ความเสี่ยง และขอบเขตของโครงการ
- SIX SIGMA เป็นกระบวนการในการพัฒนาคุณภาพเป้าหมายของ Six Sigma คือการ ลดปริมาณข้อบกพร่อง หรือความสูญเสียต่อสินค้าและบริหาร พัฒนาประสิทธิภาพการผลิต การเพิ่มความพึงพอใจของลูกค้า การเพิ่มรายได้สุทธิ คุณภาพในความหมายของทฤษฎีนี้จะเกิดขึ้นได้ เมื่อมีการลดข้อบกพร่องหรือลดต้นทุน โดยอาศัยวิธีทางสถิติในรูปแบบของการกระจายแนวโน้มจากมาตรฐานกลาง

อบรมวันที่ 4 หัวข้อ แนวปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศ

ศึกษาแนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศโดยใช้มาตรฐานระดับสากล ในการตรวจสอบ บริหารจัดการและควบคุมความเสี่ยงขององค์กร

แนวทางการปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศตาม COBIT 5 แบ่งออกเป็น 5 ส่วนใหญ่ๆได้แก่

- Evaluate, Direct and Monitor (EDM) เป็นส่วนของการกำหนดนโยบายจากผู้มีอำนาจในการสั่งการสูงสุดขององค์กรเพื่อสร้างความมั่นใจให้แก่ผู้มีส่วนได้ส่วนเสียขององค์กร
- Align, Plan and Organize (APO) เป็นส่วนของการกำกับ วางแผน แนวทางในการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายของผู้บริหาร
- Build, Acquire and Implement (BAI) เป็นส่วนของตอนการปฏิบัติตามแผนงาน และแนวทางการปฏิบัติงานที่ได้กำหนดไว้ โดยดำเนินการสร้าง จัดหา พัฒนา และใช้งานระบบให้ตรงตามความต้องการขององค์กร
- Deliver, Service and Support (DSS) เป็นส่วนของการส่งมอบโครงการ การดูแลและสนับสนุนการใช้บริการของระบบ โดยปฏิบัติตาม Service Level Agreement ตามที่องค์กรได้กำหนดไว้
- Monitor, Evaluate and Assess (MEA) เป็นส่วนของการเฝ้าติดตามการปฏิบัติตามนโยบาย ขั้นตอนการปฏิบัติงาน และข้อกำหนดต่างๆที่องค์กรได้ประกาศไว้รวมถึง การวัดผลความคุ้มค่า และการประเมินผลการปฏิบัติงาน

อบรมวันที่ 5

หัวข้อ 5.1 เทคนิคการตรวจประเมินตามมาตรฐาน ISO 19011 และประสบการณ์การตรวจสอบด้านเทคโนโลยีสารสนเทศ

หลักการ ขั้นตอน และเทคนิคการตรวจสอบประเมินที่เป็นสากลตามมาตรฐาน ISO 19011 และประสบการณ์การตรวจสอบด้านเทคโนโลยีสารสนเทศ เทคนิคการตรวจสอบความเสี่ยงที่ควรระวัง ปัญหาและอุปสรรคในการตรวจสอบ

- หลักการที่ใช้ในการตรวจสอบได้แก่ หลักการ 3P ประกอบด้วย Paper Physical and People เป็นหลักฐานในการตรวจสอบ 3 อย่างที่สามารถใช้ในการประกอบการตรวจสอบ
- เกณฑ์ที่ใช้ในการตรวจประเมิน แบ่งออกเป็น 2 ประเภท
    - External Criteria ได้แก่ มาตรฐานต่างๆ COBIT5, GRC, ISO/IEC20000, ISO/IEC27001, ISO22301, กฎหมาย ICT และอื่นๆ
    - Internal Criteria ได้แก่ วิสัยทัศน์, พันธกิจม นโยบาย IT/Security ขององค์กร
- การพิจารณาและแยกแยะระหว่าง Nonconformity และ Observation จะใช้การพิจารณาโดยใช้เกณฑ์การพิจารณาดังนี้
    - ขั้นตอนการปฏิบัติใดๆที่ไม่สอดคล้องกับ Internal Criteria ถือว่าเป็น Nonconformity ผู้ปฏิบัติจะต้องมีการปรับปรุงกระบวนการทำงานเพื่อให้สอดคล้องกับนโยบายขององค์กรที่ได้ประกาศไว้
    - ขั้นตอนการปฏิบัติใดๆที่ไม่ได้ถูกกำหนดไว้ใน Internal Criteria แต่ผู้ตรวจสอบตรวจพบว่ามีแนวทางในการปฏิบัติที่ดีกว่าเดิมโดยสามารถแนะนำเพิ่มเติมได้ อ้างอิงตาม External Criteria ถือว่าเป็น Observation ซึ่งผู้ปฏิบัติจะปฏิบัติตามหรือไม่ก็ได้ขึ้นอยู่กับการพิจารณาของผู้บริหารที่รับผิดชอบดูแลขั้นตอนนั้นๆ

หัวข้อ 5.2 Integrated Audit in Practice

การบูรณาการการตรวจสอบทั่วไป และการตรวจสอบด้านเทคโนโลยีสารสนเทศเพื่อมุ่งสู่การเป็น Integrated Auditor

ในอดีตกระบวนการทำงานของ Auditor มีการแบ่งความรับผิดชอบออกเป็นส่วนงานต่างๆโดยมีความสามารถในการตรวจสอบที่เป็นงานเฉพาะด้านเช่น ตรวจสอบทั่วไป ตรวจสอบบัญชีการเงิน ตรวจสอบไอทีเป็นต้น การบูรณาการการตรวจสอบให้เป็นกระบวนการเดียวกันสามารถทำได้โดยอาศัยแนวการปฏิบัติที่ดีที่ได้กำหนดไว้ภายใต้มาตรฐาน ทำให้ผู้ปฏิบัติงาน และผู้ตรวจสอบสามารถเข้าใจกระบวนการทำงานที่เป็นรูปแบบเดียวกันได้ โดยอาศัยเครื่องมือในการทำงาน เช่น COBIT5 และอื่นๆ ทั้งนี้ความสำคัญขึ้นอยู่กับผู้มีอำนาจในการกำหนดทิศทางขององค์กร นั้นคือ ผู้ที่จะกำหนดแนวทางการใช้เครื่องมือแบบแผนที่เป็นรูปแบบเดียวกันทั้งองค์กรจะทำให้กระบวนการทำงานมีความชัดเจนและตรวจสอบติดตามได้อย่างเป็นระบบ

2.2 ข้อเสนอแนะในการนำความรู้ตามหลักสูตร/เรื่องจากการฝึกอบรม/สัมมนาครั้งนี้ มาประยุกต์ใช้กับองค์การ

การบูรณาการการทำงานจะสามารถดำเนินการได้ จะต้องอาศัยผู้มีอำนาจกำหนดนโยบายขององค์กรที่จะกำหนดทิศทางในการใช้เครื่องมือในการปฏิบัติงาน รวมทั้งวางแผน โดยอ้างอิงจาก Best practice ที่เป็นสากล และให้ความสำคัญกับมาตรฐานสากลต่างๆ เพื่อความก้าวหน้ายิ่งขึ้นขององค์กร เพราะมาตรฐาน คือ เกณฑ์ขั้นต่ำที่องค์กรทั่วโลกได้ให้การยอมรับและมีการปฏิบัติตาม โดยองค์กรสามารถใช้เกณฑ์การปฏิบัติตามข้อบังคับต่างๆของมาตรฐาน ชี้วัดความสำเร็จในแต่ละด้านขององค์กรได้เป็นอย่างดี

2.3 ความคิดเห็นเกี่ยวกับการฝึกอบรม/สัมมนา

(1) หลักสูตรที่ฝึกอบรม/สัมมนาครั้งนี้ช่วยเพิ่มพูนความรู้ของท่าน

☑ มาก ☐ ปานกลาง ☐ น้อย

(2) ท่านคิดว่าการฝึกอบรม/สัมมนาครั้งนี้มีประโยชน์กับตัวท่านและองค์การเพียงใด

☑ มาก ☐ ปานกลาง ☐ น้อย

ระบุเหตุผล (ตอบได้มากกว่า 1 ข้อ)

☑ เนื้อหาเกี่ยวข้องโดยตรงและสามารถนำไปใช้กับการปฏิบัติงานได้อย่างดี

☐ เนื้อหาไม่เกี่ยวข้องกับการปฏิบัติงาน

☑ เป็นความรู้เสริม และมีประโยชน์ในการปฏิบัติงาน

☑ ได้แลกเปลี่ยนประสบการณ์กับบุคคลนอกองค์การ

☑ วิทยากรมีความรู้ ความสามารถ และประสบการณ์ ในการบรรยายเป็นอย่างดี

☐ เนื้อหาการอบรมไม่ตรงกับหัวข้อการบรรยาย

☐ อื่น ๆ .....

3. วิทยากรที่ให้ความรู้ในหลักสูตรนี้ ได้แก่

ชื่อ-สกุล	จากสถาบัน/หน่วยงาน	ระดับความสามารถของวิทยากร		
3.1 อ.ชยากร ปิยบัญฑิตกุล	สวทช.	☑ ดีมาก	☐ ดี	☐ พอใช้
3.2 อ.ภิญโญ ตรีเพชราภรณ์	สวทช.	☑ ดีมาก	☐ ดี	☐ พอใช้
3.3 อ.เมธา สุวรรณสาร	สวทช.	☑ ดีมาก	☐ ดี	☐ พอใช้
3.4 ดร.บรรจง หะรังษี	สวทช.	☑ ดีมาก	☐ ดี	☐ พอใช้
3.5 อ.พิทักษ์พงษ์ อินเสือ	สวทช.	☑ ดีมาก	☐ ดี	☐ พอใช้

4. ข้อเสนอแนะในการส่งพนักงานเข้ารับการฝึกอบรม/สัมมนาตามหลักสูตร/เรื่องนี้สำหรับครั้งต่อไป

ควรมีการจัดฝึกอบรมหลักสูตรนี้อีก โดยเฉพาะการเชิญวิทยากรเพื่อบรรยายให้ความรู้แก่บุคคลากรในองค์กรและสำคัญยิ่งที่จะต้องได้รับความร่วมมือจากผู้บริหารที่มีอำนาจสั่งการ เนื่องจากการขับเคลื่อนองค์กรที่สำคัญจะต้องมาจากผู้บริหารที่มีอำนาจในการเปลี่ยนแปลงองค์กร เพื่อให้วิทยากรบรรยายภาพรวมและชี้ให้เห็นถึงความสัมพันธ์ของกระบวนการทำงานที่เป็นมาตรฐาน รวมถึงความเข้าใจในกระบวนการทำงานที่เป็นมาตรฐานระดับสากล เนื่องการปฏิบัติตามมาตรฐาน บุคคลากรในองค์กรจำเป็นต้องมีความเข้าใจในกระบวนการทำงานในภาพรวมขององค์กร หากองค์กรสามารถปรับกระบวนการทำงานให้มีความคล้ายคลึงกับ Best practice ของมาตรฐานสากล จะช่วยเพิ่มประสิทธิ์ภาพในการทำงานและเป็นแนวทางการปฏิบัติงานที่เป็นแบบแผนเดียวกัน จะช่วยให้ง่ายต่อการปฏิบัติตามกระบวนการทำงานที่เป็นไปตามแนวปฏิบัติที่องค์กรกำหนดไว้ และง่ายต่อการฝึกอบรมบุคคลากรใหม่ที่จะเข้ามาปฏิบัติงานในอนาคต

จึงเรียนมาเพื่อโปรดทราบ

ลงชื่อ .....
(นายรณ วัชรินทร์)
วันที่ 31 ส.ค. 59

หมายเหตุ

1. การส่งรายงานสรุปผลการฝึกอบรม/สัมมนา ควรสรุปรายละเอียดเนื้อหาหลักสูตรผ่านผู้บังคับบัญชาในสังกัดของตนเอง และนำเสนอเรียนถึง รผบ. ผ่าน ผชก.(นายสุชินฯ) ผอ.ฝทบ ตามสายบังคับบัญชาถึงระดับรองผู้ว่าการ (ต้องแนบเอกสารประกอบการฝึกอบรมทุกครั้งและแนบวุฒิบัตร หากไม่มีให้แนบใบเซ็นชื่อเข้ารับการฝึกอบรมอย่างเคร่งครัด)

2. เมื่อ รผบ. พิจารณาเรื่องรายงานการฝึกอบรมภายนอกเรียบร้อยแล้ว กรุณาส่งเรื่องดังกล่าวไปที่ พบ.กพร.ฝทบ. เพื่อ ฝทบ. จะบันทึกประวัติการฝึกอบรมเป็น "ผ่าน" และนำรายงานเผยแพร่องค์ความรู้ใน Web HRD และ Web KM ของ รฟม. ต่อไป

3. สอบถามข้อมูลเพิ่มเติมได้ที่ แผนกพัฒนาทรัพยากรบุคคล กองพัฒนาบุคลากรและระบบงาน ฝ่ายทรัพยากรบุคคล คุณรัชกร โทร 1224 คุณอัจฉรา โทร 1213 คุณมณฑิชา โทร 1275 และคุณจิตปภา โทร 1214

เรียน ☐ ผอ.กทบ. ☐ ผอ.กสผ. ☑ ผอ.กพร.
☐ เพื่อทราบ ☑ เพื่อดำเนินการ
☐ เพื่อพิจารณา ☐ เพื่อตรวจสอบ
☐ รวบรวม ☐ เรียน
☐ .....

(นายสุทัศน์ ศิริยงค์)
ผอ.กทบ.

เรียน ☐ ผอ. ฝกม. ☐ ผอ. ฝกท.
☐ ผอ. ฝจบ. ☑ ผอ. ฝทบ.
☐ อื่นๆ.....
เพื่อโปรด ☑ ทราบ ☐ พิจารณา
☑ ดำเนินการ ☐ ตรวจสอบ
☐ ถือปฏิบัติ ☐ .....

(นายฉุทธิกา สุภารัตน์)