หลักสูตร Risk Based Audit

วันที่ 18 - 19 มิถุนายน 2565

ณ โรงแรมเดอะเบอร์เคลีย์ ประตูน้ำ

จัดโดยสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย

การตรวจสอบด้วยระบบการบริหารความเสี่ยง (Risk Management Based Auditing)

องค์ประกอบของการตรวจสอบตามความเสี่ยง

1. เข้าใจวัตถุประสงค์ของการดำเนินงาน
2. ระบุความเสี่ยงในการบรรลุวัตถุประสงค์
3. หาวิธีการที่จะควบคุมความเสี่ยง

กลยุทธ์ในการติดตามความเสี่ยง

1. รู้ความเสี่ยงที่สำคัญ
2. ประเมินความเสี่ยง
3. มีการลดความเสี่ยงที่สมควร

การบริหารจัดการความเสี่ยงองค์กร

1. ผสมผสานและบูรณาการเป็นหนึ่งเดียว สอดคล้องกับเป้าหมายและแผนงานยุทธศาสตร์ขององค์กร
2. ครอบคลุมเความเสี่ยงในทุก ๆ ด้าน
3. มุ่งเน้นควบคุมป้องกันและเตรียมพร้อมกับการเผชิญความเสี่ยง
4. ทุกคนมีส่วนร่วมและสนับสนุนส่งเสริมซึ่งกันและกัน

การวางแผนด้วย Risk Assessment

การประเมินความเสี่ยงเป็นเครื่องมือของการวางแผนอย่างหนึ่งเพื่อ

1. ทำให้เข้าใจกิจกรรม และกระบวนการที่จะตรวจสอบอย่างละเอียดก่อนการตรวจสอบ
2. สามารถจัดการงานตรวจสอบโดยให้ความสำคัญกับกิจกรรที่มีความเสี่ยงสูง
3. ทำให้เข้าใจกิจกรรมการควบคุมของแต่ละขั้นตอนว่าควรปรับปรุงหรือไม่
4. ทำให้ได้ประสานงานและร่วมมือกับผู้รับการตรวจ
5. กำหนดวัตถุประสงค์และวิธีการตรวจสอบได้ตรงประเด็น

ประโยชน์ของการวางแผนด้วยการประเมินความเสี่ยง

1. เข้าใจกระบวนการต่าง ๆ ของการปฏิบัติงาน
2. มุ่งเน้นหน่วยงานหรือกิจกรรมที่มีความเสี่ยง
3. การตรวจสอบมีความคุ้มค่า น่าเชื่อถือและมีมาตรฐานวิชาชีพ
4. ส่งเสริมความร่วมมือและความเข้าใจร่วมกันมากกว่าอดีต

บทบาทของผู้ตรวจสอบภายใน

ผู้ตรวจสอบภายใน ทำหน้าที่เป็นผู้ช่วยฝ่ายบริหาร และคณะกรรมการการตรวจสอบ เพื่อ

1. การทดสอบ
2. การประเมินผล
3. การรายงานความเพียงพอและประสิทธิผลของกระบวนการบริหารความเสี่ยง
4. การให้ความเห็นเพื่อการปรับปรุงระบบการบริหารความเสี่ยงที่เหมาะสม

ขอบเขตของงานตรวจสอบ (Audit Universe)

1. Audit Universe จะถูกกำหนดและปรับปรุงโดยพิจารณาจากประเด็นความเสี่ยงของของกิจกรรมตรวจสอบที่เป็นไปได้
2. โครงการหรืองานที่จะตรวจสอบในแต่ละปีจะมาจากระดับความเสี่ยง เช่น
   2.1 โครงการ
   2.2 หน่วยงาน
   2.3 กระบวนการ
   2.4 ยุทธศาสตร์ หรือวัตถุประสงค์ของยุทธศาสตร์ หรือวัตถุประสงค์ของโครงการ ฯลฯ

การกำหนดงานตรวจสอบ

1. Functional หรือ แผนกงาน
2. กระบวนการ เช่น การจัดซื้อ การผลิต การบริหารพัสดุ เป็นต้น
3. ระบบฐานข้อมูล
4. กฎหมาย ระเบียบ ข้อบังคับ
5. สายผลิตภัณฑ์หรือบริการ หรือกลุ่มลูกค้า
6. สัญญาหรือโครงการต่าง ๆ
7. แผนงานหลักหรือแผนปฏิบัติงาน
8. อื่น ๆ

การระบุปัจจัยเสี่ยง

1. เข้าใจวัตถุประสงค์ และปัจจัยที่ส่งผบกระทบต่อผลสำเร็จ
2. ความเสี่ยงโดยทั่วไปของกิจกรรมที่เกี่ยวข้อง
3. จำนวนปัจจัยเสี่ยงขึ้นกับดุลพินิจ ต้องมีความพอดี
4. กระบวนการประเมินและระบุความเสี่ยงต้องมีการเก็บข้อมูล
5. ปัจจัยเสี่ยงต้อง
   5.1 หลากหลายและสะท้อนความเสี่ยงทั่วทั้งองค์กร
   5.2 บ่งชี้ถึงความเสี่ยงที่สำคัญต่อองค์กร
   5.3 มีความหมายหรือมีน้ำหนักต่อความสำเร็จ
   5.4 เป็นเหตุเป็นผล อธิบายได้ถ้าเกิดแล้วเป็นอย่างไร

<u>การกำหนดระดับความเสี่ยง</u>

1. ให้ระดับทุกปัจจัยเสี่ยงแบบที่ง่าย มีความเหมายและเข้าใจตรงกัน
2. ระดับที่ให้ 3 หรือ 5 ระดับ แต่ไม่ควรเกิน 7
    2.1 ค่าน้อยควรแสดงระดับความเสี่ยงที่น้อย
    2.2 ค่ามากควรแสดงระดับความเสี่ยงที่มาก
3. การกำหนดระดับความเสี่ยงต้องพิจารณา
    3.1 ผลกระทบที่คาดว่าจะได้รับ (Risk Impact)
    3.2 โอกาสที่จะเกิดความเสี่ยงนั้น ๆ (Risk likelihood)

<u>แหล่งข้อมูลของความเสี่ยง</u>

1. รายงานและผลการตรวจสอบที่ผ่านมา
2. การศึกษาโครงการต่าง ๆ และการขอคำปรึกษาเรื่องต่าง ๆ จากภายนอก
3. ประเด็นข่าวสาร เหตุการณ์ปัจจุบัน
4. นโยบาย และกฎ ระเบียบ เทคโนโลยี
5. การสัมภาษณ์ผู้บริหาร หรือแบบสอบถามต่าง ๆ
6. อื่น ๆ

<u>เครื่องมือและวิธีการประเมินความเสี่ยง</u>

1. รูปแบบไม่จำเป็นแต่ต้องมี ต้องง่ายและทำได้ทุกคนแต่ต้องได้ข้อมูลครบถ้วน
2. วิธีการขึ้นอยู่กับ
    2.1 ลักษณะข้อมูลและปริมาณข้อมูล
    2.2 ความซับซ้อนหรือความยุ่งยากของการเก็บข้อมูล
    2.3 ต้นทุน ความคุ้มค่าด้านเวลาและงบประมาณ
    2.4 สภาพแวดล้อมภายในองค์กร
    2.5 โครงสร้างและวัฒนธรรมองค์กร
    2.6 อื่น ๆ

<u>การกำหนดแผนการตรวจสอบ</u> ต้องพิจารณาปัจจัยต่าง ๆ เพิ่มเติมดังนี้

1. จำนวนทรัพยากรบุคคล ความรู้ ทักษะ ความชำนาญ และประสบการณ์
2. งบประมาณ
3. อุปกรณ์ เครื่องมือเครื่องใช้ที่จำเป็น
4. เป้าหมายของการปฏิบัติงาน
5. ความต้องการของผู้บริหารและหรือคณะกรรมการตรวจสอบ
6. ขนาดขององค์กร และขนาดของหน่วยงานตรวจสอบ
7. ความต้องการของลูกค้าภายในองค์กรและผู้มีส่วนได้เสีย

การประเมินความเสี่ยง

1. การประเมินความเสี่ยงต้องพิจารณา Soft control ด้วย
2. จุดอ่อนของ Soft control จะมีผลทำให้ความเสี่ยงเพิ่มขึ้น เช่น
   2.1 วัฒนธรรมองค์กร ค่านิยมร่วมของบุคลากร
   2.2 การสื่อสารภายใน
   2.3 รูปแบบและนโยบายการจัดการ Tone at the top
   2.4 อื่น ๆ
   สิ่งเหล่านี้จะนำไปสู่ความสูญเสียในระยะยาว

การประเมินความเสี่ยง ควรทำเมื่อ

1. เมื่อทำแผนงานประจำปี
2. เมื่อจะทำการตรวจสอบเพื่อกำหนดวัตถุประสงค์และ Audit Program โดยจะศึกษากระบวนการของกิจกรรมที่จะตรวจสอบอย่างละเอียด

กระบวนการประเมินความเสี่ยง

1. วิเคราะห์กิจกรรมที่จะตรวจสอบว่ามีกระบวนการหรือวิธีการอย่างไร
2. ในแต่ละขั้นตอนและกระบวนการมีวัตถุประสงค์เพื่ออะไร
3. อะไรเป็นความเสี่ยงที่จะทำให้ขั้นตอนหรือกระบวนการไม่บรรลุวัตถุประสงค์ได้บ้าง
4. กำหนดเกณฑ์หรือระดับความเสี่ยง
5. จัดลำดับความเสี่ยง
6. เลือกกิจกรรมที่มีความเสี่ยงสูงมาทำการกำหนดวัตถุประสงค์การตรวจสอบและกำหนดวิธีการตรวจสอบ
   สิ่งสำคัญคือ ควรให้ผู้รับการตรวจสอบมีส่วนร่วมในการประเมินความเสี่ยงด้วย

****

จัดทำโดย นางสาวจุฑารัตน์ ลอยโคกสูง
กลุ่มตรวจสอบภายใน