บันทึกข้อความ

กองการเจ้าหน้าที่
เลขรับที่ ๕๐๑
วันที่ - ๑ ส.ค. ๒๕๖๘
เวลา ..... น.
☐ ฝ่ายบริหารและบรรจุแต่งตั้ง
☑ ฝ่ายส่งเสริมและพัฒนาบุคลากร

ส่วนราชการ หน่วยตรวจสอบภายใน เทศบาลเมืองหนองปรือ

ที่ นตภ. ๕๗/ ๒๕๖๘ **วันที่** ๑ สิงหาคม ๒๕๖๘

เรื่อง ขอเพิ่มประกาศการผ่านโครงการฝึกอบรมฯ ในทะเบียนประวัติพนักงานเทศบาล (ก.พ.๗)

เรียน ปลัดเทศบาลเมืองหนองปรือ

ตามที่ข้าพเจ้านางสาวสุดารัตน์ พิกุล พนักงานเทศบาล ตำแหน่ง นักวิชาการตรวจสอบภายใน ระดับ ปฏิบัติการ เลขที่ตำแหน่ง ๐๘-๒-๑๒-๓๒๐๕-๐๐๒ สังกัด หน่วยตรวจสอบภายใน ได้รับอนุมัติให้เข้าร่วมโครงการฝึกอบรมหลักสูตร “การพัฒนาทักษะของผู้ตรวจสอบภายในยุคดิจิทัล : Future-Ready Auditing” ประจำปี พ.ศ. ๒๕๖๘ ระหว่าง วันที่ ๓ – ๔ กรกฎาคม พ.ศ. ๒๕๖๘ ณ โรงแรมการ์เด้นซีวิว พัทยา จังหวัดชลบุรี บัดนี้ ข้าพเจ้าได้สำเร็จหลักสูตรการฝึกอบรม เมื่อวันที่ ๔ กรกฎาคม ๒๕๖๘

ข้าพเจ้ามีความประสงค์ขอเพิ่มประกาศนียบัตร โครงการฝึกอบรมตามหลักสูตรดังข้างต้น ในทะเบียนประวัติพนักงานเทศบาล (ก.พ.๗) ทั้งนี้ได้แนบหลักฐานการสำเร็จหลักสูตรการฝึกอบรมมาพร้อมเอกสารนี้

จึงเรียนมาเพื่อโปรดทราบ และพิจารณาดำเนินการต่อไป

(นางสาวสุดารัตน์ พิกุล)
นักวิชาการตรวจสอบภายในปฏิบัติการ
หัวหน้าหน่วยตรวจสอบภายใน

เรียน นายกเทศมนตรีเมืองหนองปรือ
☐ เพื่อโปรดทราบ
☐ เพื่อโปรดอนุมัติ
☐ เพื่อโปรดพิจารณา เสนอ กจ. พิจารณา

(นายศราวุธ อมรธรรมสิน)
ปลัดเทศบาลเมืองหนองปรือ

(นางอัญมณี ตำจันทร์)
รองนายกเทศมนตรี ปฏิบัติราชการแทน
นายกเทศมนตรีเมืองหนองปรือ

ทราบ/ดำเนินการ

(นายวินัย อินทร์พิทักษ์)
นายกเทศมนตรีเมืองหนองปรือ

สำนักบริการวิชาการ มหาวิทยาลัยบูรพา

มอบวุฒิบัตรนี้ไว้เพื่อแสดงว่า

นางสาวสุดารัตน์ พิกุล

ได้ผ่านการฝึกอบรม

โครงการอบรมเชิงปฏิบัติการ หลักสูตร "การพัฒนาทักษะ
ของผู้ตรวจสอบภายในยุคดิจิทัล : Future-Ready Auditing" ประจำปี พ.ศ. 2568

ระหว่างวันที่ 3 - 4 กรกฎาคม พ.ศ. 2568

ณ โรงแรมการ์เดน ซีวิว รีสอร์ท พัทยา จังหวัดชลบุรี

ให้ไว้ ณ วันที่ 4 กรกฎาคม พ.ศ. 2568

ดร.พีรพัฒน์ มั่งคั่ง

ผู้อำนวยการสำนักบริการวิชาการ มหาวิทยาลัยบูรพา

สำเนาถูกต้อง

(นางสาวสุดารัตน์ พิกุล)

ศึกวิชาการตรวจสอบภายในปฏิบัติการ

บันทึกข้อความ

สวนราชการ หน่วยตรวจสอบภายใน เทศบาลเมืองหนองปรือ

ที่ นตภ. ๕๓ / ๒๕๖๘ **วันที่** ๒๙ กรกฎาคม ๒๕๖๘

เรื่อง รายงานผลการฝึกอบรม

เรียน นายกเทศมนตรีเมืองหนองปรือ

ตามบันทึกข้อความ หน่วยตรวจสอบภายใน ที่ นตภ. ๓๓/๒๕๖๘ ลงวันที่ ๒๓ พฤษภาคม ๒๕๖๘ เรื่องขออนุญาตเข้ารับการฝึกอบรม และขออนุมัติเบิกค่าลงทะเบียน โดยอนุญาต ให้นางสาวสุดารัตน์ พิกุล ตำแหน่ง นักวิชาการตรวจสอบภายใน เดินทางไปราชการเพื่อเข้าร่วมฝึกอบรม โครงการอบรมเชิงปฏิบัติการหลักสูตร "การพัฒนาทักษะของผู้ตรวจสอบภายในยุคดิจิทัล : Future-Ready Auditing " ประจำปี พ.ศ. ๒๕๖๘ ซึ่งมีกำหนดการระหว่างวันที่ ๓ -๔ กรกฎาคม ๒๕๖๘ ณ โรงแรมการ์เด้นซีวิว พัทยา อำเภอบางละมุง จังหวัดชลบุรี นั้น

บัดนี้การฝึกอบรมเสร็จสิ้นแล้ว ผู้เข้ารับการฝึกอบรม ได้เดินทางกลับถึงสถานที่ราชการ แล้ว เพื่อให้เป็นไปตามระเบียบกระทรวงมหาดไทยว่าด้วยค่าใช้จ่ายในการฝึกอบรม และการเข้ารับการฝึกอบรมของเจ้าหน้าที่ท้องถิ่น พ.ศ.๒๕๕๗ แก้ไขเพิ่มเติมถึงฉบับปัจจุบัน ข้อ ๑๐ "ให้ผู้เข้ารับการฝึกอบรมหรือผู้สังเกตการณ์ที่เข้ารับการฝึกอบรมหรือเข้าร่วมสังเกตการณ์ที่หน่วยงานอื่นของรัฐหรือหน่วยงานอื่นจัดการฝึกอบรม จัดทำรายงานผลการฝึกอบรมหรือเข้าร่วมสังเกตการณ์เสนอผู้มีอำนาจอนุมัติตามข้อ ๙ ภายใน หกสิบวัน นับแต่วันเดินทางกลับถึงสถานที่ราชการ" จึงขอรายงานผลการฝึกอบรม รายละเอียดตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ

(นางสาวสุดารัตน์ พิกุล)
นักวิชาการตรวจสอบภายในปฏิบัติการ

(นายศราวุธ อมรธรรมสิน)
ปลัดเทศบาลเมืองหนองปรือ

(นางอัญมณี [illegible])
รองนายกเทศมนตรีเมืองหนองปรือ

ทราบ

(นายวินัย อินทร์พิทักษ์)
นายกเทศมนตรีเมืองหนองปรือ

แบบรายงานผลการเข้ารับการฝึกอบรม/เข้าร่วมสังเกตการณ์ (ทั้งในประเทศ/ต่างประเทศ)

๑. ชื่อ – สกุล .....นางสาวสุดารัตน์.....พิกุล.....
ตำแหน่ง.....นักวิชาการตรวจสอบภายใน.....**ระดับ**.....ปฏิบัติการ.....
สังกัด.....หน่อยตรวจสอบภายใน.....

๒. โครงการ/หลักสูตร โครงการอบรมเชิงปฏิบัติการหลักสูตร "การพัฒนาทักษะของผู้ตรวจสอบภายในยุคดิจิทัล : Future-Ready Auditing " ประจำปี พ.ศ. ๒๕๖๘

จัดโดย สำนักบริการวิชาการ ร่วมกับ สำนักงานตรวจสอบภายใน มหาวิทยาลัยบูรพา

๓. ระยะเวลาเดินทางไปเข้ารับการฝึกอบรม/เข้าร่วมสังเกตการณ์

ระหว่าง วันที่ ๓ -๔ กรกฎาคม ๒๕๖๘

๔. สถานที่ฝึกอบรม ณ โรงแรมการ์เด้นซีวิว พัทยา อำเภอบางละมุง จังหวัดชลบุรี

๕. วัตถุประสงค์ในการเข้ารับการฝึกอบรม/เข้าร่วมสังเกตการณ์

๕.๑ เพื่อเสริมสร้างความเข้าใจเกี่ยวกับบทบาทและความสำคัญของผู้ตรวจสอบภายใน ในยุคดิจิทัล
๕.๒ เพื่อพัฒนาทักษะด้านการใช้เทคโนโลยีดิจิทัลในการตรวจสอบ
๕.๓ เพื่อฝึกการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) และการนำ AI มาใช้ในการตรวจสอบ
๕.๔ เพื่อเรียนรู้แนวทางการบริหารความเสี่ยงทางไซเบอร์ และการป้องกันการทุจริตในระบบดิจิทัล
๕.๕ เพื่อพัฒนาทักษะการสื่อสาร และการนำเสนอผลการตรวจสอบอย่างมีประสิทธิภาพ

๖. งบประมาณในการฝึกอบรม/เข้าร่วมสังเกตการณ์

๖.๑ ค่าลงทะเบียนฝึกอบรม จำนวน ๕,๙๐๐ บาท

๗. สรุปเนื้อหาที่ได้รับจากการฝึกอบรม

๑. แนวทางการตรวจสอบภายในสำหรับสถาบันการศึกษา

การตรวจสอบระบบการจัดการเรียนการสอน (Academic Management System) ในสถาบันการศึกษาเป็นกระบวนการสำคัญในการประเมินประสิทธิภาพและการปฏิบัติตามมาตรฐานการศึกษาเพื่อให้มั่นใจว่าสถาบันการศึกษามีการจัดการที่โปร่งใสและมีคุณภาพ โดยสามารถตรวจสอบได้ทั้งในเชิงโครงสร้างองค์กร การปฏิบัติงานและกระบวนการต่าง ๆ ที่เกี่ยวข้องกับการเรียนการสอน

ขั้นตอนการตรวจสอบระบบการจัดการเรียนการสอน

๑. การตรวจสอบกระบวนการออกแบบหลักสูตร โดยตรวจสอบว่า หลักสูตรการศึกษาตรงตามมาตรฐานการศึกษาและข้อกำหนดของกระทรวงศึกษาธิการหรือหน่วยงานที่เกี่ยวข้อง ประเมินการมีส่วนร่วมของคณาจารย์ ในการออกแบบหลักสูตร และการปรับปรุงหลักสูตรตามผลการประเมินผลการเรียนการสอน ตรวจสอบการดำเนินงานตามหลักสูตรที่ได้รับการอนุมัติรวมถึงการทบทวนและปรับปรุงหลักสูตรในทุก ๆ ปี

๒. การตรวจสอบกระบวนการลงทะเบียนและการบริหารจัดการข้อมูลนักศึกษาโดยการตรวจสอบระบบ การลงทะเบียนนักศึกษา เช่น การลงทะเบียนวิชาเรียน การเลือกวิชาเลือกตามหลักสูตร ประเมินการจัดการข้อมูล ประวัติ

การศึกษาของนักศึกษา และการออกใบรับรองหรือประกาศนียบัตร ตรวจสอบว่าข้อมูลนักศึกษาได้รับการจัดเก็บอย่างปลอดภัยและเป็นไปตามมาตรฐานการปกป้องข้อมูลส่วนบุคคล

๓. การตรวจสอบระบบการจัดการการประเมินผลตรวจสอบกระบวนการ การประเมินผลการเรียน เช่น การสอบ การประเมินผลรายวิชา และการประเมินโดยใช้เครื่องมือออนไลน์ ตรวจสอบการจัดการ คะแนนการสอบ รวมถึงการบันทึกและการคำนวณคะแนนให้มีความถูกต้อง โปร่งใส และไม่มีการทุจริต ประเมินการรีวิวและปรับปรุงวิธีการประเมินให้เหมาะสมกับสถานการณ์การศึกษาและความคิดเห็นของผู้เรียน

๔. การตรวจสอบการจัดการห้องเรียนและการสอน โดยตรวจสอบกระบวนการ การจัดห้องเรียนโดยคำนึงถึงจำนวนผู้เรียน, การจัดสถานที่เรียน, และอุปกรณ์การเรียนที่จำเป็น ประเมินการใช้เทคโนโลยีการสอน เช่น ระบบการเรียนออนไลน์ (Learning Management System - LMS) เช่น Moodle, Google Classroom หรือ Microsoft Teams ตรวจสอบการจัดการคลังทรัพยากรการเรียนการสอน เช่น หนังสือเรียน เครื่องมือการเรียนการสอน หรือฐานข้อมูลออนไลน์

๕. การตรวจสอบการฝึกอบรมและพัฒนาศักยภาพของคณาจารย์ โดยตรวจสอบโปรแกรมการอบรมและพัฒนาคณาจารย์ เพื่อให้ทันกับการเปลี่ยนแปลงในเทคโนโลยีการเรียนการสอน ประเมินการจัดทำคู่มือหรือแนวทางการสอน เพื่อให้คณาจารย์มีความเข้าใจตรงกัน ตรวจสอบการติดตามผลการสอนของอาจารย์และการรับข้อเสนอแนะจากนักศึกษา

๖. การตรวจสอบระบบการรับข้อเสนอแนะจากนักศึกษา โดยตรวจสอบว่าสถาบันการศึกษามีระบบในการเก็บข้อมูลข้อเสนอแนะจากนักศึกษาเกี่ยวกับการสอนและการเรียนการสอน การประเมินการจัดการระบบข้อร้องเรียนและการดำเนินการแก้ไขปัญหาที่นักศึกษาแจ้ง ตรวจสอบการใช้ข้อมูลจากข้อเสนอแนะมาเป็นข้อมูลในการปรับปรุงการเรียนการสอน

๗. การตรวจสอบความคุ้มค่าและประสิทธิภาพของระบบการเรียนการสอน โดยการประเมินประสิทธิภาพการใช้ทรัพยากร เช่น บุคลากร, เวลา, งบประมาณ, อุปกรณ์การเรียน และการตรวจสอบผลลัพธ์การเรียนการสอนและผลสำเร็จของนักศึกษา เช่น อัตราการสำเร็จการศึกษา, อัตราการหางานทำหลังจบการศึกษา

ตัวอย่างคำถามสำหรับการตรวจสอบ

๑. คำถามด้านกระบวนการการออกแบบหลักสูตร
- หลักสูตรที่เปิดสอนมีการปรับปรุงอย่างสม่ำเสมอ
- หลักสูตรมีการตอบสนองต่อความต้องการของตลาดแรงงาน
- ผู้มีส่วนเกี่ยวข้องในการออกแบบหลักสูตร ได้แก่ คณาจารย์ นักศึกษาหรือผู้เชี่ยวชาญภายนอก

๒. คำถามด้านการประเมินผลการเรียน
- มีระบบตรวจสอบความถูกต้องของการประเมินผลนักศึกษา
- ผลการประเมินถูกนำมาปรับปรุงกระบวนการเรียนการสอน
- นักศึกษามีโอกาสในการให้ข้อเสนอแนะเกี่ยวกับการประเมินผล

ข้อเสนอแนะหลังการตรวจสอบ

หลังจากทำการตรวจสอบแล้ว ผู้ตรวจสอบภายในสามารถให้ข้อเสนอแนะ ดังนี้ ปรับปรุงระบบการประเมินผลเพื่อให้สามารถประเมินผลได้อย่างรอบด้านและมีความเป็นธรรม โดยใช้เทคโนโลยีในการสนับสนุนการเรียนการสอนให้มีประสิทธิภาพมากขึ้น (เช่น LMS, การเรียนออนไลน์) สร้างช่องทางให้คณาจารย์และนักศึกษาสามารถแสดงความคิดเห็นและข้อเสนอแนะได้สะดวกยิ่งขึ้น การตรวจสอบระบบการจัดการเรียนการสอนจะช่วยเพิ่มประสิทธิภาพในการให้บริการการศึกษา รวมถึงการเสริมสร้างคุณภาพการเรียนการสอนในสถาบันการศึกษาให้มีมาตรฐานและเหมาะสมกับการเปลี่ยนแปลงทางการศึกษาในยุคปัจจุบัน

๒. แนวทางการตรวจสอบการใช้เทคโนโลยีในการบริหารจัดการ

IT Audit คือ การตรวจสอบและประเมินประสิทธิภาพ ประสิทธิผล ความถูกต้อง และความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Systems) ที่องค์กรนำมาใช้ในการบริหารจัดการ โดยมีวัตถุประสงค์หลักเพื่อป้องกันทรัพย์สินจากการทุจริตและข้อผิดพลาด ตรวจสอบว่าระบบ IT มีการควบคุมที่เพียงพอเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต การแก้ไขข้อมูลโดยไม่ถูกต้อง หรือการทุจริต รักษาความถูกต้องของข้อมูลและความปลอดภัยของฐานข้อมูลหลัก ตรวจสอบว่าข้อมูลที่ถูกจัดเก็บ ประมวลผล และส่งผ่านระบบ IT มีความถูกต้อง ครบถ้วน และปลอดภัยจากการถูกทำลายหรือเปิดเผยโดยไม่ได้รับอนุญาต ประเมินประสิทธิผลของระบบงาน: ตรวจสอบว่าระบบ IT สนับสนุนการดำเนินงานขององค์กรให้บรรลุเป้าหมายได้อย่างมีประสิทธิภาพ ประเมินประสิทธิภาพในการใช้ทรัพยากรของระบบ ตรวจสอบว่ามีการใช้ทรัพยากร IT (เช่น Hardware, Software, Network) อย่างคุ้มค่าและมีประสิทธิภาพสูงสุด ระบุและจัดการความเสี่ยงด้าน IT ค้นหาช่องโหว่และจุดอ่อนในระบบ IT ที่อาจนำไปสู่ความเสี่ยง เช่น การหยุดชะงักของระบบ การโจมตีทางไซเบอร์ การสูญหายของข้อมูล ตรวจสอบการปฏิบัติตามกฎระเบียบและนโยบาย: ตรวจสอบว่าการใช้เทคโนโลยีเป็นไปตามกฎหมาย ข้อบังคับ และนโยบายภายในขององค์กร การตรวจสอบ IT Audit โดยทั่วไปจะครอบคลุมหลายด้าน ดังนี้

๑. การวางแผน (Planning) ระบุขอบเขตของการตรวจสอบและกำหนดเป้าหมาย/วัตถุประสงค์ที่ชัดเจน ประเมินความเสี่ยงด้าน IT ที่สำคัญขององค์กร (IT Risk Assessment) เพื่อกำหนดจุดที่ต้องให้ความสำคัญ จัดทำแผนการตรวจสอบและกำหนดทรัพยากรที่ต้องใช้การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls - ITGC) นโยบายและขั้นตอนปฏิบัติ มีการกำหนดนโยบายและขั้นตอนปฏิบัติในการใช้ IT ที่ชัดเจนและเป็นลายลักษณ์อักษรหรือไม่

๒. การแบ่งแยกหน้าที่ (Segregation of Duties) มีการแบ่งแยกหน้าที่งานในระบบ IT ที่เหมาะสมเพื่อป้องกันการทุจริตหรือไม่ (เช่น ผู้พัฒนาระบบไม่ควรเป็นผู้ดูแลระบบ)

๓. การพัฒนาและการเปลี่ยนแปลงระบบงาน (Program Development and Change Management) มีกระบวนการควบคุมการพัฒนา การเปลี่ยนแปลง และการนำระบบงานใหม่ไปใช้งานอย่างรัดกุมหรือไม่ การรักษาความปลอดภัยระบบสารสนเทศ (Information Security): มีมาตรการควบคุมการเข้าถึงระบบ (Access Control), การป้องกันมัลแวร์, การเข้ารหัสข้อมูล, และการจัดการภัยคุกคามทางไซเบอร์ที่เพียงพอหรือไม่ การปฏิบัติการคอมพิวเตอร์ (Computer Operations): มีขั้นตอนการปฏิบัติงานประจำวันของศูนย์คอมพิวเตอร์ที่เหมาะสม (เช่น การสำรองข้อมูล, การบำรุงรักษา) หรือไม่

๔. แผนการกู้คืนระบบ (Disaster Recovery/Business Continuity Plan - DRP/BCP): มีแผนรองรับและขั้นตอนการกู้คืนระบบในกรณีที่เกิดเหตุการณ์ไม่คาดฝัน (เช่น ภัยพิบัติ ระบบล่ม) หรือไม่

- การควบคุมเฉพาะระบบงาน (Application Controls)

- การนำเข้าข้อมูล (Input Controls) ตรวจสอบว่าข้อมูลที่ป้อนเข้าระบบมีความถูกต้อง ครบถ้วน และได้รับอนุญาต

- การประมวลผล (Processing Controls) ตรวจสอบว่าระบบประมวลผลข้อมูลได้อย่างถูกต้องตามที่กำหนด

- การส่งออกข้อมูล (Output Controls) ตรวจสอบว่าผลลัพธ์ที่ได้จากการประมวลผลมีความถูกต้องและมีการนำไปใช้งานอย่างเหมาะสม

- การเชื่อมโยงข้อมูลระหว่างระบบ (Interface Controls): ตรวจสอบความถูกต้องและปลอดภัยในการรับส่งข้อมูลระหว่างระบบงานต่างๆ

การดำเนินการตรวจสอบ (Execution) ตรวจสอบและทดสอบการควบคุมภายในของระบบ IT ตามที่วางแผนไว้ เก็บรวบรวมหลักฐานและข้อมูลจากการตรวจสอบ (เช่น บันทึกการเข้าถึง, Log files, เอกสารนโยบาย) สัมภาษณ์บุคลากรที่เกี่ยวข้อง ใช้เครื่องมือและเทคนิคการตรวจสอบต่างๆ การรายงานผล (Reporting) จัดทำรายงานผลการตรวจสอบ สรุปข้อค้นพบ (Findings), ข้อบกพร่องของการควบคุม (Control Deficiencies), และความเสี่ยงที่ระบุได้ เสนอแนะแนวทางแก้ไขและปรับปรุงเพื่อลดความเสี่ยงและเพิ่มประสิทธิภาพ การติดตามผล (Follow-up) ติดตามผลการดำเนินงานตามข้อเสนอแนะที่ให้ไว้ เพื่อให้มั่นใจว่าปัญหาได้รับการแก้ไขอย่างเหมาะสม

ประโยชน์ของการตรวจสอบเทคโนโลยีสารสนเทศ (IT Audit) เพิ่มความมั่นใจในความถูกต้องของข้อมูล สร้างความน่าเชื่อถือให้กับข้อมูลที่ใช้ในการตัดสินใจทางธุรกิจ ปรับปรุงประสิทธิภาพการดำเนินงาน: ค้นหาโอกาสในการปรับปรุงกระบวนการทำงานให้รวดเร็วและมีประสิทธิภาพมากขึ้นด้วยการใช้เทคโนโลยีลดความเสี่ยงด้าน IT ช่วยระบุและบรรเทาความเสี่ยงด้านความปลอดภัยของข้อมูล การหยุดชะงักของระบบ และการโจมตีทางไซเบอร์ ส่งเสริมการปฏิบัติตามกฎระเบียบ ช่วยให้องค์กรมั่นใจว่าการดำเนินงานด้าน IT เป็นไปตามกฎหมาย ข้อบังคับ และมาตรฐานที่เกี่ยวข้อง เพิ่มความโปร่งใสและความรับผิดชอบ สร้างความรับผิดชอบในการบริหารจัดการ IT ภายในองค์กร สนับสนุนการตัดสินใจเชิงกลยุทธ์ ให้ข้อมูลเชิงลึกที่ช่วยผู้บริหารในการวางแผนและตัดสินใจเกี่ยวกับการลงทุนและการใช้เทคโนโลยี

เครื่องมือและมาตรฐานที่ใช้ในการตรวจสอบระบบสารสนเทศ

มาตรฐานและกรอบการทำงาน (Frameworks) COBIT (Control Objectives for Information and Related Technologies) เป็นกรอบการทำงานที่ได้รับการยอมรับอย่างกว้างขวางสำหรับการกำกับดูแลและการบริหารจัดการ IT ขององค์กร

๑. ISO/IEC ๒๗๐๐๑ (Information Security Management System - ISMS) มาตรฐานสากลสำหรับการจัดการความมั่นคงปลอดภัยของข้อมูล

๒. ITIL (Information Technology Infrastructure Library) แนวปฏิบัติสำหรับการจัดการบริการด้าน IT

๓. NIST Cybersecurity Framework กรอบการทำงานด้านความปลอดภัยทางไซเบอร์

เครื่องมือช่วยในการตรวจสอบ (Audit Tools):Data Analytics Tools เช่น

- ACL (Audit Command Language), IDEA, Python, R เพื่อวิเคราะห์ข้อมูลจำนวนมาก ค้นหาความผิดปกติ และระบุรูปแบบ

- Vulnerability Scanners เครื่องมือสำหรับสแกนหาช่องโหว่ด้านความปลอดภัยในระบบเครือข่ายและแอปพลิเคชัน

- Penetration Testing Tools (Pentest Tools) เครื่องมือที่ใช้จำลองการโจมตีเพื่อทดสอบความแข็งแกร่งของระบบ

- Configuration Management Tools สำหรับตรวจสอบการตั้งค่าของระบบและอุปกรณ์

- Log Management Systems สำหรับรวบรวมและวิเคราะห์ Log เพื่อตรวจจับเหตุการณ์ผิดปกติ

สรุป การตรวจสอบการใช้เทคโนโลยีในการบริหารจัดการ หรือที่รู้จักกันในชื่อ IT Audit (การตรวจสอบเทคโนโลยีสารสนเทศ) เป็นกระบวนการที่มีความสำคัญอย่างยิ่งในยุคปัจจุบันที่เทคโนโลยีเข้ามามีบทบาทในทุกมิติของการดำเนินธุรกิจและองค์กร การตรวจสอบการใช้เทคโนโลยีในการบริหารจัดการเป็นกระบวนการที่สำคัญและจำเป็นอย่างยิ่งสำหรับองค์กรในยุคดิจิทัล เพื่อให้มั่นใจว่าการลงทุนและการใช้เทคโนโลยีเป็นไปอย่างมีประสิทธิภาพ ปลอดภัย และสนับสนุนเป้าหมายทางธุรกิจขององค์กรได้อย่างยั่งยืน

เทคนิคและทักษะผู้ตรวจสอบภายในของสถาบันการศึกษา

ผู้ตรวจสอบภายในของสถาบันการศึกษา มีบทบาทสำคัญในการประเมินและให้คำแนะนำเกี่ยวกับการควบคุมภายใน การบริหารความเสี่ยง และการกำกับดูแลกิจการ เพื่อให้สถาบันดำเนินงานอย่างมีประสิทธิภาพ โปร่งใส และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง

๑. ความรู้ด้านระเบียบและกฎหมาย เข้าใจระเบียบกระทรวงศึกษาธิการ พระราชบัญญัติการศึกษาแห่งชาติ ระเบียบงบประมาณ การเงิน บัญชี และพัสดุภาครัฐ กฎหมายว่าด้วยความโปร่งใสและการตรวจสอบได้ (เช่น พ.ร.บ. ข้อมูลข่าวสาร)

๒. ทักษะการวางแผนและการจัดลำดับความสำคัญ การวางแผนการตรวจสอบตามความเสี่ยง (Risk-based audit) กำหนดวัตถุประสงค์ ขอบเขต และวิธีการตรวจสอบให้สอดคล้องกับเป้าหมายของสถาบัน บริหารเวลาการตรวจสอบให้มีประสิทธิภาพ

๓. ทักษะการสื่อสารและมนุษย์สัมพันธ์ สื่อสารอย่างชัดเจนและสร้างความร่วมมือกับหน่วยงานที่ถูกตรวจสอบ ให้คำแนะนำที่สร้างสรรค์ และเน้นการปรับปรุงไม่ใช่เพียงการจับผิด เขียนรายงานการตรวจสอบให้อ่านง่าย มีข้อเสนอแนะที่นำไปปฏิบัติได้จริง

๔. ความสามารถด้านการวิเคราะห์ข้อมูล วิเคราะห์ข้อมูลทางการเงิน งบประมาณ และผลการดำเนินงาน ใช้เครื่องมือ Excel หรือซอฟต์แวร์อื่น ๆ เพื่อประเมินความผิดปกติของข้อมูล ประเมินประสิทธิภาพและประสิทธิผลของโครงการต่าง ๆ ในสถาบัน

๕. ทักษะด้านจริยธรรมและความเป็นอิสระ ปฏิบัติหน้าที่อย่างเป็นกลาง ไม่ลำเอียง ยึดมั่นในจรรยาบรรณผู้ตรวจสอบภายใน รักษาความลับของข้อมูลที่ได้รับระหว่างการตรวจสอบ

๖. ความสามารถในการตรวจสอบด้านไอที เข้าใจระบบสารสนเทศและการบริหารจัดการข้อมูลของสถาบัน (เช่น ระบบทะเบียนนักศึกษา, ระบบบัญชีการเงิน) รู้จักความเสี่ยงด้านไอที เช่น การสำรองข้อมูล การควบคุมสิทธิ์ผู้ใช้

๗. การพัฒนาตนเองอย่างต่อเนื่อง ติดตามแนวโน้มการบริหารจัดการ การกำกับดูแล และมาตรฐานการตรวจสอบภายในใหม่ ๆ เข้าร่วมอบรม สัมมนา หรือหลักสูตรของสำนักตรวจสอบภายใน หรือองค์กรวิชาชีพ (เช่น IIA)

๓. การตรวจสอบความปลอดภัยไซเบอร์

การตรวจสอบความปลอดภัยไซเบอร์ (Cybersecurity Audit) เป็นกระบวนการประเมินความมีประสิทธิภาพของการควบคุมและมาตรการด้านความปลอดภัยทางไซเบอร์ขององค์กร เพื่อระบุช่องโหว่ ความเสี่ยง และข้อบกพร่องที่อาจนำไปสู่การโจมตีทางไซเบอร์ การละเมิดข้อมูล หรือการหยุดชะงักของระบบ

การตรวจสอบความปลอดภัยไซเบอร์มีวัตถุประสงค์หลัก ดังนี้ ระบุและประเมินความเสี่ยง ค้นหาจุดอ่อนในระบบ โครงสร้างพื้นฐาน แอปพลิเคชัน และกระบวนการที่อาจถูกโจมตีได้ ตรวจสอบการปฏิบัติตามนโยบายและมาตรฐาน ตรวจสอบว่าองค์กรปฏิบัติตามนโยบายความปลอดภัยภายใน มาตรฐานอุตสาหกรรม (เช่น ISO ๒๗๐๐๑, NIST Cybersecurity Framework) และข้อกำหนดทางกฎหมาย (เช่น PDPA, GDPR) หรือไม่ ประเมินประสิทธิภาพของการควบคุม วิเคราะห์ว่ามาตรการควบคุมความปลอดภัยที่มีอยู่สามารถป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพหรือไม่ ให้คำแนะนำในการปรับปรุง เสนอแนวทางแก้ไขและปรับปรุงเพื่อเสริมสร้างความปลอดภัยทางไซเบอร์ขององค์กร สร้างความมั่นใจ สร้างความเชื่อมั่นให้กับผู้บริหาร ลูกค้า และผู้มีส่วนได้ส่วนเสียว่าข้อมูลและระบบขององค์กรได้รับการปกป้องอย่างเพียงพอ

ขอบเขตของการตรวจสอบความปลอดภัยไซเบอร์

การตรวจสอบความปลอดภัยไซเบอร์สามารถครอบคลุมหลายด้าน ขึ้นอยู่กับความต้องการและลักษณะขององค์กร การประเมินโครงสร้างพื้นฐานเครือข่าย ตรวจสอบการตั้งค่าไฟร์วอลล์, เราเตอร์, สวิตช์, และอุปกรณ์เครือข่ายอื่น ๆ เพื่อหาช่องโหว่และจุดเข้าถึงที่ไม่ปลอดภัย การประเมินระบบปฏิบัติการและเซิร์ฟเวอร์ ตรวจสอบการตั้งค่าความปลอดภัยของ Windows, Linux, และระบบปฏิบัติการเซิร์ฟเวอร์อื่น ๆ รวมถึงการจัดการแพตช์และการควบคุมการเข้าถึง การประเมินแอปพลิเคชัน ตรวจสอบความปลอดภัยของแอปพลิเคชันทั้งที่พัฒนาเองและที่จัดซื้อ รวมถึงการทดสอบช่องโหว่ของเว็บแอปพลิเคชัน (Web Application Penetration Testing) และ API การจัดการข้อมูล ตรวจสอบมาตรการในการปกป้องข้อมูลที่ละเอียดอ่อน ทั้งข้อมูลที่จัดเก็บ (data at rest) และข้อมูลที่กำลังส่งผ่าน (data in transit) รวมถึงการเข้ารหัส, การสำรองข้อมูล, และการจัดการสิทธิ์การเข้าถึง การจัดการตัวตนและการเข้าถึง (Identity and Access Management - IAM) ตรวจสอบนโยบายการสร้างรหัสผ่านที่รัดกุม, การรับรองความถูกต้องแบบหลายปัจจัย (MFA), และการจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน การจัดการช่องโหว่และการแพตช์ (Vulnerability and Patch Management):** ตรวจสอบกระบวนการในการระบุ, ประเมิน, และแก้ไขช่องโหว่ด้านความปลอดภัยอย่างสม่ำเสมอ การจัดการเหตุการณ์และการตอบสนอง (Incident Management and Response) ประเมินแผนและกระบวนการขององค์กรในการตรวจจับ, ตอบสนอง, และฟื้นตัวจากเหตุการณ์ด้านความปลอดภัย ความตระหนักด้านความปลอดภัยของพนักงาน (Security Awareness Training) ตรวจสอบว่าพนักงานได้รับการฝึกอบรมด้านความปลอดภัยอย่างเพียงพอหรือไม่ เพื่อลดความเสี่ยงจากการโจมตีแบบวิศวกรรมสังคม (Social Engineering) การตรวจสอบการปฏิบัติตามกฎระเบียบ (Compliance Audit):** ตรวจสอบว่าองค์กรปฏิบัติตาม

ข้อกำหนดของกฎหมายและมาตรฐานที่เกี่ยวข้องหรือไม่ เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA), HIPAA, PCI DSS

กระบวนการตรวจสอบความปลอดภัยไซเบอร์ โดยทั่วไป กระบวนการตรวจสอบความปลอดภัยไซเบอร์ประกอบด้วยขั้นตอนดังนี้

๑. การวางแผนและกำหนดขอบเขต (Planning and Scoping) กำหนดวัตถุประสงค์ ขอบเขต และทรัพยากรที่จำเป็นสำหรับการตรวจสอบ

๒. การเก็บรวบรวมข้อมูล (Information Gathering) รวบรวมเอกสาร, นโยบาย, ขั้นตอนปฏิบัติ, ผังเครือข่าย, และข้อมูลการตั้งค่าระบบ. สัมภาษณ์บุคลากรที่เกี่ยวข้อง

๓. การประเมินและการทดสอบ (Assessment and Testing)

๑. การตรวจสอบเอกสาร (Documentation Review) ตรวจสอบนโยบายและขั้นตอนปฏิบัติว่าครบถ้วนและเหมาะสมหรือไม่

๒. การสแกนช่องโหว่ (Vulnerability Scanning) ใช้เครื่องมืออัตโนมัติเพื่อระบุช่องโหว่ในระบบและเครือข่าย

๓. การทดสอบการเจาะระบบ (Penetration Testing - Pentest) จำลองการโจมตีจากผู้ไม่หวังดีเพื่อทดสอบความแข็งแกร่งของระบบ

๔. การตรวจสอบการตั้งค่า (Configuration Review) ตรวจสอบการตั้งค่าความปลอดภัยของอุปกรณ์และซอฟต์แวร์

๕. การตรวจสอบบันทึกเหตุการณ์ (Log Review) วิเคราะห์บันทึกเหตุการณ์เพื่อหาความผิดปกติหรือกิจกรรมที่น่าสงสัย

๔. การวิเคราะห์และการระบุข้อค้นพบ (Analysis and Findings Identification) วิเคราะห์ข้อมูลที่รวบรวมได้เพื่อระบุช่องโหว่ ความเสี่ยง และข้อบกพร่องด้านความปลอดภัย

๕. การรายงานผล (Reporting) จัดทำรายงานผลการตรวจสอบที่ครอบคลุมข้อค้นพบ, ระดับความเสี่ยง, และข้อเสนอแนะในการปรับปรุง

๖. การติดตามผล (Follow-up) ติดตามเพื่อให้มั่นใจว่าข้อเสนอแนะได้รับการดำเนินการและแก้ไขปัญหาตามที่ตกลงไว้

เครื่องมือและเทคนิคที่ใช้ในการตรวจสอบ

- เครื่องมือสแกนช่องโหว่ Nessus, OpenVAS, Qualys.
- เครื่องมือทดสอบการเจาะระบบ Metasploit, Kali Linux, Nmap.
- เครื่องมือวิเคราะห์ Log Splunk, ELK Stack (Elasticsearch, Logstash, Kibana).
- เครื่องมือจัดการการเข้าถึง Active Directory tools, Identity and Access Management (IAM) solutions.
- มาตรฐานและกรอบการทำงาน ISO ๒๗๐๐๑, NIST Cybersecurity Framework, CIS Controls, OWASP Top ๑๐

การตรวจสอบความปลอดภัยไซเบอร์เป็นกระบวนการที่ต้องทำอย่างต่อเนื่องและสม่ำเสมอ เพื่อให้องค์กรสามารถปรับตัวและรับมือกับภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปอย่างรวดเร็ว

๔. การตรวจสอบการใช้ข้อมูลและการวิเคราะห์ข้อมูล

การตรวจสอบการใช้ข้อมูลและการวิเคราะห์ข้อมูล (Data Usage and Data Analytics Audit) เป็นกระบวนการที่สำคัญในการประเมินว่าองค์กรมีการใช้ข้อมูลและเครื่องมือวิเคราะห์ข้อมูลอย่างมีประสิทธิภาพ ถูกต้อง ปลอดภัย และเป็นไปตามข้อกำหนดทางกฎหมายและนโยบายหรือไม่

วัตถุประสงค์ของการตรวจสอบการใช้ข้อมูลและการวิเคราะห์ข้อมูล

การตรวจสอบนี้มีวัตถุประสงค์หลักเพื่อ ความถูกต้องและความสมบูรณ์ของข้อมูล ตรวจสอบให้แน่ใจว่าข้อมูลที่ใช้ในการวิเคราะห์มีความถูกต้อง ครบถ้วน และเชื่อถือได้ ความปลอดภัยของข้อมูล ประเมินมาตรการที่ใช้ในการปกป้องข้อมูลจากการเข้าถึง การใช้งาน การเปิดเผย การแก้ไข หรือการทำลายโดยไม่ได้รับอนุญาต การปฏิบัติตามกฎระเบียบ ตรวจสอบว่าการเก็บรวบรวม การประมวลผล การใช้งาน และการเปิดเผยข้อมูลเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (เช่น PDPA, GDPR), มาตรฐานอุตสาหกรรม, และนโยบายภายในองค์กร

ประสิทธิภาพและประสิทธิผลของการวิเคราะห์ ประเมินว่ากระบวนการวิเคราะห์ข้อมูลและผลลัพธ์ที่ได้นั้นมีความถูกต้อง มีประโยชน์ และสามารถนำไปใช้ในการตัดสินใจทางธุรกิจได้อย่างมีประสิทธิภาพ การบริหารจัดการข้อมูลที่ดี ตรวจสอบการดำเนินการเกี่ยวกับธรรมาภิบาลข้อมูล (Data Governance), การจัดการคุณภาพข้อมูล (Data Quality Management), และการบริหารจัดการวงจรชีวิตข้อมูล (Data Lifecycle Management) การระบุความเสี่ยง ค้นหาช่องโหว่และจุดอ่อนที่อาจนำไปสู่ความเสี่ยงด้านข้อมูล เช่น ข้อมูลรั่วไหล, การใช้ข้อมูลผิดวัตถุประสงค์, หรือการตัดสินใจที่ผิดพลาดจากข้อมูลที่ไม่ถูกต้อง

ขอบเขตของการตรวจสอบการใช้ข้อมูลและการวิเคราะห์ข้อมูล

๑. การกำกับดูแลข้อมูล (Data Governance) นโยบายและมาตรฐานข้อมูลมีการกำหนดนโยบายและมาตรฐานสำหรับการจัดเก็บ การเข้าถึง การใช้งาน และการทำลายข้อมูลที่ชัดเจนและมีการบังคับใช้หรือไม่ บทบาทและความรับผิดชอบ มีการกำหนดบทบาทและความรับผิดชอบสำหรับเจ้าของข้อมูล ผู้ดูแลข้อมูล และผู้ใช้งานข้อมูลอย่างชัดเจนหรือไม่ การจัดการวงจรชีวิตข้อมูล มีกระบวนการจัดการข้อมูลตั้งแต่การสร้าง การจัดเก็บ การใช้งาน ไปจนถึงการจัดเก็บถาวรและการทำลายข้อมูลอย่างเหมาะสมหรือไม่

๒. คุณภาพข้อมูล (Data Quality) ความถูกต้อง (Accuracy) ข้อมูลมีความถูกต้องและเป็นปัจจุบันหรือไม่ ความสมบูรณ์ (Completeness) ข้อมูลมีครบถ้วนตามที่จำเป็นสำหรับการวิเคราะห์หรือไม่ ความสอดคล้อง (Consistency) ข้อมูลมีความสอดคล้องกันทั่วทั้งระบบและแหล่งข้อมูลต่างๆ หรือไม่ ความเป็นปัจจุบัน (Timeliness) ข้อมูลพร้อมใช้งานและทันเวลาสำหรับการตัดสินใจหรือไม่ ความถูกต้องตามรูปแบบ (Validity) ข้อมูลเป็นไปตามรูปแบบและข้อกำหนดที่กำหนดไว้หรือไม่ กระบวนการตรวจสอบคุณภาพข้อมูล มีการตรวจสอบและแก้ไขปัญหาคุณภาพข้อมูลอย่างสม่ำเสมอหรือไม่

๓. ความปลอดภัยของข้อมูล (Data Security) การควบคุมการเข้าถึง (Access Controls) มีการจำกัดการเข้าถึงข้อมูลตามบทบาทและความจำเป็น (Role-Based Access Control) และมีการตรวจสอบการเข้าถึงหรือไม่ การเข้ารหัสข้อมูล (Data Encryption) มีการเข้ารหัสข้อมูลทั้งที่จัดเก็บ (data at rest) และข้อมูลที่กำลังส่งผ่าน (data in transit) หรือไม่ การป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention - DLP) มีมาตรการป้องกันการส่งออกหรือเปิดเผยข้อมูลที่ละเอียดอ่อนโดยไม่ได้รับอนุญาตหรือไม่ การสำรองและกู้คืนข้อมูล (Backup and Recovery) มีการสำรองข้อมูลอย่างสม่ำเสมอและมีแผนการกู้คืนข้อมูลในกรณีเกิดเหตุการณ์ไม่คาดฝันหรือไม่ การปกป้องข้อมูลส่วนบุคคล (Privacy Protection) มีมาตรการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายและนโยบายหรือไม่ (เช่น การไม่ระบุตัวตน, การทำให้ข้อมูลเป็นนามแฝง)

๔. การใช้และการวิเคราะห์ข้อมูล (Data Usage and Analytics) วัตถุประสงค์ในการใช้ข้อมูล มีการใช้ข้อมูลตามวัตถุประสงค์ที่ได้แจ้งไว้และได้รับความยินยอม (หากจำเป็น) หรือไม่ เครื่องมือและเทคนิคการวิเคราะห์ เครื่องมือและเทคนิคที่ใช้ในการวิเคราะห์ข้อมูลมีความเหมาะสมและให้ผลลัพธ์ที่เชื่อถือได้หรือไม่ ความถูกต้องของแบบจำลอง (Model Accuracy) หากมีการใช้แบบจำลองทางสถิติหรือ AI/ML ในการวิเคราะห์ มีการตรวจสอบความถูกต้องและอคติ (bias) ของแบบจำลองหรือไม่ การนำเสนอผลลัพธ์ผลการวิเคราะห์ข้อมูลถูกนำเสนอในรูปแบบที่ชัดเจน เข้าใจง่าย และสามารถนำไปใช้ในการตัดสินใจได้หรือไม่ การติดตามและประเมินผลมีการติดตามและประเมินผลกระทบจากการใช้ข้อมูลและการวิเคราะห์ข้อมูลต่อการดำเนินธุรกิจหรือไม่

๕. การปฏิบัติตามกฎระเบียบ (Compliance) กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA/GDPR) ตรวจสอบการปฏิบัติตามข้อกำหนดเกี่ยวกับการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล กฎหมายเฉพาะอุตสาหกรรม ตรวจสอบการปฏิบัติตามกฎระเบียบเฉพาะสำหรับอุตสาหกรรมนั้นๆ (เช่น HIPAA สำหรับข้อมูลสุขภาพ, PCI DSS สำหรับข้อมูลบัตรเครดิต) ข้อตกลงและสัญญา ตรวจสอบการปฏิบัติตามข้อตกลงและสัญญาที่เกี่ยวข้องกับการใช้ข้อมูลกับบุคคลที่สาม

กระบวนการตรวจสอบการใช้ข้อมูลและการวิเคราะห์ข้อมูล

๑. การวางแผนและกำหนดขอบเขต กำหนดวัตถุประสงค์ ขอบเขตของการตรวจสอบ (เช่น ข้อมูลประเภทใด ระบบใด) และทีมผู้ตรวจสอบ

๒. การทำความเข้าใจกระบวนการ ทำความเข้าใจว่าองค์กรมีการรวบรวม จัดเก็บ ประมวลผล วิเคราะห์ และใช้งานข้อมูลอย่างไร

๓. การประเมินความเสี่ยงระบุความเสี่ยงที่สำคัญที่เกี่ยวข้องกับการใช้ข้อมูลและการวิเคราะห์ข้อมูล.

๔. การทดสอบและการรวบรวมหลักฐาน ตรวจสอบเอกสารนโยบาย, ขั้นตอนปฏิบัติ, รายงานการวิเคราะห์, เอกสารสถาปัตยกรรมข้อมูล สัมภาษณ์บุคลากรที่เกี่ยวข้องกับข้อมูลและการวิเคราะห์ ตรวจสอบระบบและเครื่องมือการตั้งค่าฐานข้อมูล, เครื่องมือ BI/Analytics, ระบบจัดการข้อมูล วิเคราะห์ข้อมูลใช้เครื่องมือวิเคราะห์ข้อมูล (Data Analytics Tools) เพื่อตรวจสอบคุณภาพข้อมูล, รูปแบบการใช้งาน, และความผิดปกติ ทดสอบการควบคุมทดสอบว่าการควบคุมการเข้าถึง, การเข้ารหัส, และมาตรการรักษาความปลอดภัยอื่นๆ ทำงานตามที่ออกแบบไว้หรือไม่

๕. การระบุข้อค้นพบและข้อเสนอแนะ สรุปช่องโหว่, ความเสี่ยง, และข้อบกพร่องที่พบ พร้อมเสนอแนะแนวทางแก้ไขที่เป็นรูปธรรม

๖. การจัดทำรายงาน นำเสนอรายงานผลการตรวจสอบแก่ผู้บริหารและผู้มีส่วนได้ส่วนเสีย

๗. การติดตามผล ติดตามการดำเนินการแก้ไขตามข้อเสนอแนะเพื่อให้มั่นใจว่าปัญหาได้รับการแก้ไขอย่างเหมาะสม

เครื่องมือและเทคนิคที่ใช้ในการตรวจสอบ

๑. เครื่องมือวิเคราะห์ข้อมูล (Data Analytics Tools) เช่น SQL, Python (Pandas, NumPy), R, Excel, Power BI, Tableau สำหรับวิเคราะห์ชุดข้อมูลขนาดใหญ่เพื่อตรวจสอบคุณภาพข้อมูล รูปแบบการใช้งาน และความผิดปกติ

๒. เครื่องมือตรวจสอบคุณภาพข้อมูล (Data Quality Tools) สำหรับการโปรไฟล์ข้อมูล, การทำความสะอาดข้อมูล, และการตรวจสอบความสอดคล้อง

๓. เครื่องมือจัดการข้อมูลประจำหลัก (Master Data Management - MDM) และธรรมาภิบาลข้อมูล (Data Governance Platforms) เพื่อตรวจสอบว่ามีการปฏิบัติตามหลักธรรมาภิบาลข้อมูลหรือไม่

๔. เครื่องมือสแกนช่องโหว่และทดสอบการเจาะระบบ หากการตรวจสอบครอบคลุมความปลอดภัยของโครงสร้างพื้นฐานข้อมูล

๕. รายการตรวจสอบ (Checklists) และกรอบการทำงาน (Frameworks) เช่น COBIT, DAMA-DMBOK (Data Management Body of Knowledge) สำหรับแนวทางการจัดการข้อมูล, NIST Privacy Framework สำหรับความเป็นส่วนตัวของข้อมูล

การตรวจสอบการใช้ข้อมูลและการวิเคราะห์ข้อมูลเป็นสิ่งสำคัญอย่างยิ่งในยุคที่ข้อมูลเป็นทรัพย์สินที่มีค่าขององค์กร การตรวจสอบนี้ไม่เพียงแต่ช่วยให้องค์กรปฏิบัติตามข้อกำหนดต่างๆ แต่ยังช่วยเพิ่มประสิทธิภาพในการใช้ข้อมูลเพื่อขับเคลื่อนการเติบโตและสร้างความได้เปรียบทางการแข่งขันอีกด้วย

๕. การตรวจสอบระบบการจัดการการเงิน

การตรวจสอบระบบการจัดการการเงิน (Financial Management System Audit) เป็นกระบวนการประเมินความมีประสิทธิภาพ ความถูกต้อง และความน่าเชื่อถือของระบบและกระบวนการที่องค์กรใช้ในการบริหารจัดการด้านการเงิน ตั้งแต่การบันทึกบัญชี การรายงานทางการเงิน ไปจนถึงการควบคุมงบประมาณและการจัดการกระแสเงินสด

วัตถุประสงค์ของการตรวจสอบระบบการจัดการการเงิน

การตรวจสอบนี้มีวัตถุประสงค์หลักเพื่อ ความถูกต้องและความน่าเชื่อถือของข้อมูลทางการเงิน ตรวจสอบให้แน่ใจว่าข้อมูลทางการเงินที่บันทึกและรายงานมีความถูกต้อง ครบถ้วน และเชื่อถือได้ การปฏิบัติตามมาตรฐานและกฎระเบียบประเมินว่าระบบและกระบวนการทางการเงินปฏิบัติตามมาตรฐานการบัญชี (เช่น TFRS, IFRS), กฎหมายและข้อบังคับที่เกี่ยวข้อง (เช่น กฎหมายภาษี), และนโยบายภายในองค์กรหรือไม่ ประสิทธิภาพของการควบคุมภายในตรวจสอบว่ามีการควบคุมภายในที่เพียงพอและทำงานได้อย่างมีประสิทธิภาพ เพื่อป้องกันการทุจริต ข้อผิดพลาด และการสูญเสียทางการเงิน การประเมินความเสี่ยงทางการเงินระบุความเสี่ยงที่สำคัญที่อาจส่งผลกระทบต่อความมั่นคงทางการเงินขององค์กร เช่น ความเสี่ยงด้านสภาพคล่อง ความเสี่ยงด้านปฏิบัติการ หรือความเสี่ยงด้านการฉ้อโกง ประสิทธิภาพและประสิทธิผลของระบบประเมินว่าระบบการจัดการการเงินสนับสนุนการดำเนินงานขององค์กรได้อย่างมีประสิทธิภาพ และใช้ทรัพยากรทางการเงินอย่างคุ้มค่าหรือไม่ การตัดสินใจเชิงกลยุทธ์สร้างความมั่นใจว่าข้อมูลทางการเงินที่ใช้ในการตัดสินใจของผู้บริหารมีความแม่นยำและทันเวลา

ขอบเขตของการตรวจสอบระบบการจัดการการเงิน

การตรวจสอบนี้สามารถครอบคลุมหลายด้าน ขึ้นอยู่กับโครงสร้างและความซับซ้อนของระบบการเงินขององค์กร

๑. การควบคุมภายในทางการเงิน (Financial Internal Controls) การแบ่งแยกหน้าที่ (Segregation of Duties) มีการแบ่งแยกหน้าที่ความรับผิดชอบในการทำธุรกรรมทางการเงินอย่างเหมาะสมหรือไม่ เช่น ผู้บันทึกบัญชีไม่ควรเป็นผู้อนุมัติการจ่ายเงิน การอนุมัติและการรับรอง (Authorization and Approval) มีกระบวนการอนุมัติธุรกรรมทางการเงินที่ชัดเจนและเป็นไปตามระดับอำนาจที่กำหนดหรือไม่ การกระทบยอด (Reconciliation) มีการกระทบยอดบัญชีต่างๆ (เช่น บัญชีธนาคาร, ลูกหนี้, เจ้าหนี้) อย่างสม่ำเสมอหรือไม่ การดูแลทรัพย์สิน (Safeguarding Assets) มีมาตรการในการปกป้องทรัพย์สินขององค์กรจากการสูญหาย การขโมย หรือการนำไปใช้โดยไม่ได้รับอนุญาตหรือไม่ การบันทึกบัญชี (Recording Transactions) ธุรกรรมทางการเงินทั้งหมดได้รับการบันทึกอย่างถูกต้องครบถ้วน และทันเวลาหรือไม่

๒. ระบบบัญชีและซอฟต์แวร์ (Accounting Systems and Software) การทำงานของระบบ (System Functionality) ระบบบัญชีสามารถรองรับความต้องการทางธุรกิจและมีการประมวลผลธุรกรรมได้อย่างถูกต้องหรือไม่ การควบคุมการเข้าถึงระบบ (System Access Controls) มีการจำกัดการเข้าถึงระบบบัญชีตามบทบาทและสิทธิ์ของผู้ใช้งานอย่างเหมาะสมหรือไม่ ความสมบูรณ์ของข้อมูล (Data Integrity) ข้อมูลที่ป้อนเข้าสู่ระบบและข้อมูลที่ประมวลผลมีความถูกต้องและสมบูรณ์หรือไม่ การสำรองและกู้คืนข้อมูล (Backup and Recovery) มีการสำรองข้อมูลทางการเงินและมีแผนการกู้คืนระบบในกรณีที่เกิดข้อผิดพลาดหรือภัยพิบัติหรือไม่ การจัดการการเปลี่ยนแปลง (Change Management) มีกระบวนการควบคุมการเปลี่ยนแปลง การปรับปรุง หรือการอัปเกรดระบบบัญชีอย่างเหมาะสมหรือไม่

๓. กระบวนการทางการเงินที่สำคัญ (Key Financial Processes) วงจรรายได้ (Revenue Cycle) การออกใบแจ้งหนี้, การบันทึกรายได้, การรับชำระเงิน วงจรค่าใช้จ่าย (Expenditure Cycle) การจัดซื้อจัดจ้าง, การรับสินค้า/บริการ, การบันทึกค่าใช้จ่าย, การจ่ายชำระหนี้ วงจรสินทรัพย์ (Asset Cycle) การได้มาซึ่งสินทรัพย์, การคิดค่าเสื่อมราคา, การจำหน่ายสินทรัพย์ วงจรค่าจ้างเงินเดือน (Payroll Cycle) การคำนวณเงินเดือน, การจ่ายเงินเดือน, การหักภาษีและประกันสังคม การจัดการสินค้าคงคลัง (Inventory Management) การบันทึก, การตีราคา, และการควบคุมสินค้าคงคลัง การจัดการกระแสเงินสดและงบประมาณ (Cash Flow and Budget Management) การจัดทำงบกระแสเงินสด, การควบคุมงบประมาณ, การพยากรณ์ทางการเงิน

๔. การรายงานทางการเงิน (Financial Reporting) ความถูกต้องของรายงาน รายงานทางการเงิน (งบแสดงฐานะการเงิน, งบกำไรขาดทุน, งบกระแสเงินสด) มีความถูกต้องและเป็นไปตามมาตรฐานการบัญชีหรือไม่ การเปิดเผยข้อมูล (Disclosures) มีการเปิดเผยข้อมูลที่เพียงพอและจำเป็นในหมายเหตุประกอบงบการเงินหรือไม่ ความทันเวลา (Timeliness) รายงานทางการเงินจัดทำและนำเสนออย่างทันเวลาหรือไม่ การควบคุมการนำเสนอรายงาน มีกระบวนการตรวจสอบและอนุมัติรายงานทางการเงินก่อนการเผยแพร่หรือไม่

กระบวนการตรวจสอบระบบการจัดการการเงิน

๑. การวางแผนและกำหนดขอบเขต (Planning and Scoping) โดยกำหนดวัตถุประสงค์ ขอบเขต และทรัพยากรที่จำเป็นสำหรับการตรวจสอบ ทำความเข้าใจโครงสร้างองค์กร ระบบการเงิน และกระบวนการทางธุรกิจที่เกี่ยวข้อง และประเมินความเสี่ยงของการควบคุมที่สำคัญ

๒. การทำความเข้าใจและการประเมินการควบคุมภายใน (Understanding and Evaluating Internal Controls) โดนการตรวจสอบนโยบาย ขั้นตอนปฏิบัติ และแผนผังกระแสงาน (Flowcharts) ของระบบการเงิน สัมภาษณ์บุคลากรที่เกี่ยวข้องเพื่อทำความเข้าใจการดำเนินงานจริง ประเมินการออกแบบการควบคุมว่ามีประสิทธิภาพเพียงพอในการป้องกันหรือตรวจจับข้อผิดพลาด/การทุจริตหรือไม่

๓. การทดสอบการควบคุม (Testing Controls) การทดสอบการปฏิบัติงาน (Test of Operating Effectiveness) ตรวจสอบว่าการควบคุมที่ออกแบบไว้นั้นมีการปฏิบัติงานจริงและมีประสิทธิภาพตามที่คาดหวังหรือไม่ (เช่น ทดสอบการอนุมัติ, การกระทบยอด) การทดสอบสาระสำคัญ (Substantive Testing) ตรวจสอบความถูกต้องของยอดคงเหลือในบัญชีและรายการธุรกรรมทางการเงินโดยตรง (เช่น ตรวจสอบเอกสารประกอบการจ่ายเงิน, การยืนยันยอดลูกหนี้/เจ้าหนี้) อาจใช้เทคนิค CAATs (Computer Assisted Audit Techniques) เช่น Data Analytics Tools เพื่อวิเคราะห์ข้อมูลทางการเงินขนาดใหญ่

๔. การระบุข้อค้นพบและข้อบกพร่อง (Identification of Findings and Deficiencies) โดยการสรุปข้อบกพร่องของการควบคุมภายใน, ข้อผิดพลาดในการบันทึกบัญชี, หรือความเสี่ยงที่อาจเกิดขึ้น และจัดลำดับความสำคัญของข้อค้นพบตามระดับความรุนแรงและผลกระทบ

๕. การจัดทำรายงาน (Reporting) จัดทำรายงานผลการตรวจสอบที่ครอบคลุมข้อค้นพบ, ความเสี่ยงที่เกี่ยวข้อง, และข้อเสนอแนะในการปรับปรุง รายงานควรชัดเจน กระชับ และเน้นข้อเสนอแนะที่ปฏิบัติได้จริง

๖. การติดตามผล (Follow-up) ติดตามเพื่อให้มั่นใจว่าผู้บริหารได้ดำเนินการแก้ไขตามข้อเสนอแนะที่ให้ไว้และปัญหาได้รับการแก้ไขอย่างเหมาะสม

ประโยชน์ของการตรวจสอบระบบการจัดการการเงิน

๑. เพิ่มความน่าเชื่อถือของข้อมูลทางการเงิน ทำให้ข้อมูลที่ใช้ในการตัดสินใจมีความถูกต้องและเชื่อถือได้

๒. ลดความเสี่ยงจากการทุจริตและข้อผิดพลาด ช่วยให้องค์กรมีระบบควบคุมที่แข็งแกร่งขึ้นเพื่อป้องกันการสูญเสียทางการเงิน

๓. ส่งเสริมการปฏิบัติตามกฎระเบียบ มั่นใจว่าองค์กรปฏิบัติตามกฎหมายและมาตรฐานการบัญชีที่เกี่ยวข้อง

๔. ปรับปรุงประสิทธิภาพการดำเนินงาน ระบุจุดที่สามารถปรับปรุงกระบวนการทางการเงินให้มีประสิทธิภาพมากขึ้น

๕. สนับสนุนการตัดสินใจ ให้ข้อมูลที่แม่นยำและทันเวลาแก่ผู้บริหารสำหรับการตัดสินใจเชิงกลยุทธ์และการวางแผน

การตรวจสอบระบบการจัดการการเงินเป็นการลงทุนที่คุ้มค่าสำหรับองค์กรทุกขนาด เพื่อให้มั่นใจในความมั่นคงทางการเงิน ความโปร่งใส และการเติบโตอย่างยั่งยืน

๖. การตรวจสอบการปฏิบัติตามกฎหมายและมาตรฐาน

การตรวจสอบการปฏิบัติตามกฎหมายและมาตรฐาน (Regulatory Compliance Audit) คือ กระบวนการที่เป็นระบบและเป็นอิสระในการประเมินว่าองค์กรได้ดำเนินกิจกรรมและกระบวนการต่างๆ เป็นไปตามข้อกำหนดทางกฎหมาย กฎระเบียบ ข้อบังคับ มาตรฐาน และนโยบายภายในที่เกี่ยวข้องหรือไม่ การตรวจสอบนี้มีความสำคัญอย่างยิ่งในการช่วยให้องค์กรหลีกเลี่ยงความเสี่ยงทางกฎหมาย บทลงโทษทางการเงิน ความเสียหายต่อชื่อเสียง และผลกระทบเชิงลบอื่นๆ

วัตถุประสงค์ของการตรวจสอบการปฏิบัติตามกฎหมายและมาตรฐาน

ระบุและประเมินการปฏิบัติตามข้อกำหนด ตรวจสอบว่าองค์กรเข้าใจและปฏิบัติตามกฎหมาย กฎระเบียบและมาตรฐานที่บังคับใช้อย่างถูกต้อง ลดความเสี่ยง ค้นหาและประเมินความเสี่ยงที่อาจเกิดขึ้นจากการไม่ปฏิบัติตาม ซึ่งอาจนำไปสู่บทลงโทษ ค่าปรับ คดีความ หรือความเสียหายต่อชื่อเสียง ปรับปรุงกระบวนการ ระบุจุดอ่อนในกระบวนการทำงานที่อาจทำให้เกิดการไม่ปฏิบัติตาม และเสนอแนะแนวทางแก้ไขเพื่อปรับปรุงประสิทธิภาพและความสอดคล้อง สร้างความน่าเชื่อถือและความโปร่งใส แสดงให้เห็นถึงความมุ่งมั่นขององค์กรในการดำเนินธุรกิจอย่างมีจริยธรรมและรับผิดชอบต่อผู้มีส่วนได้ส่วนเสีย สนับสนุนการตัดสินใจ ให้ข้อมูลเชิงลึกแก่ผู้บริหารเพื่อใช้ในการตัดสินใจและวางแผนกลยุทธ์ที่สอดคล้องกับข้อกำหนด สร้างวัฒนธรรมการปฏิบัติตาม ส่งเสริมให้บุคลากรทุกคนมีความตระหนักและเข้าใจถึงความสำคัญของการปฏิบัติตามกฎระเบียบ

ขอบเขตของการตรวจสอบการปฏิบัติตามกฎหมายและมาตรฐาน

ขอบเขตของการตรวจสอบจะขึ้นอยู่กับประเภทของธุรกิจ อุตสาหกรรมที่องค์กรดำเนินงาน และลักษณะเฉพาะของกฎหมายและมาตรฐานที่เกี่ยวข้อง ซึ่งอาจรวมถึงกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Data Privacy Laws):** เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของไทย, General Data Protection Regulation (GDPR) ของสหภาพยุโรป. ตรวจสอบการเก็บรวบรวม การใช้ การเปิดเผย และการจัดเก็บข้อมูลส่วนบุคคล กฎหมายและข้อบังคับทางการเงิน เช่น มาตรฐานการรายงานทางการเงิน (TFRS/IFRS), กฎระเบียบของตลาดหลักทรัพย์, กฎหมายป้องกันและปราบปรามการฟอกเงิน (AML/CFT) กฎหมายแรงงานและสิทธิมนุษยชน การปฏิบัติตามกฎหมายแรงงานเกี่ยวกับการจ้างงาน ค่าจ้าง สภาพการทำงาน สิทธิประโยชน์ และการไม่เลือกปฏิบัติ กฎหมายสิ่งแวดล้อม สุขภาพ และความปลอดภัย (EHS) การจัดการของเสีย, การควบคุมมลพิษ, มาตรฐานความปลอดภัยในที่ทำงาน, ใบอนุญาตต่างๆ ที่เกี่ยวข้องกับสิ่งแวดล้อมและอาชีวอนามัย กฎหมายการแข่งขันทางการค้า การไม่กระทำการผูกขาดหรือจำกัดการแข่งขันที่เป็นธรรม กฎหมายและมาตรฐานเฉพาะอุตสาหกรรม เช่น อุตสาหกรรมการเงิน กฎระเบียบของธนาคารแห่งประเทศไทย, สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) อุตสาหกรรมสุขภาพ มาตรฐานโรงพยาบาล, กฎหมายยาและเครื่องมือแพทย์ (เช่น HIPAA ในสหรัฐอเมริกา) อุตสาหกรรมการผลิต มาตรฐาน ISO ต่างๆ (เช่น ISO ๙๐๐๑ สำหรับคุณภาพ, ISO ๑๔๐๐๑ สำหรับสิ่งแวดล้อม, ISO ๔๕๐๐๑ สำหรับอาชีวอนามัยและความปลอดภัย), Good Manufacturing Practices (GMP) นโยบายและขั้นตอนภายในองค์กร:** ตรวจสอบว่าพนักงานและกระบวนการทำงานปฏิบัติตามนโยบายและขั้นตอนที่องค์กรกำหนดขึ้นเอง (ซึ่งมักจะอ้างอิงจากกฎหมายและมาตรฐานภายนอก)

กระบวนการตรวจสอบการปฏิบัติตามกฎหมายและมาตรฐาน

๑. การวางแผนและกำหนดขอบเขต ระบุกฎหมายและมาตรฐานที่เกี่ยวข้อง ทำรายการกฎหมาย กฎระเบียบและมาตรฐานทั้งหมดที่องค์กรต้องปฏิบัติตาม กำหนดวัตถุประสงค์และขอบเขต ระบุว่าการตรวจสอบจะครอบคลุมส่วนใดขององค์กร กระบวนการใด และกฎระเบียบใดบ้าง จัดตั้งทีมตรวจสอบบุคลากรที่มีความเชี่ยวชาญในด้านกฎหมาย/มาตรฐานที่เกี่ยวข้องและทักษะการตรวจสอบ

๒. การทำความเข้าใจและการรวบรวมข้อมูล ศึกษาเอกสารทบทวนนโยบาย, ขั้นตอนปฏิบัติ, สัญญา, รายงานการปฏิบัติงาน, และบันทึกต่างๆ ที่เกี่ยวข้อง สัมภาษณ์บุคลากร พูดคุยกับผู้บริหารและพนักงานที่เกี่ยวข้องกับกระบวนการและกิจกรรมที่อยู่ภายใต้การตรวจสอบ เพื่อทำความเข้าใจวิธีการทำงานและการปฏิบัติตามข้อกำหนด สังเกตการณ์การปฏิบัติงานจริงในพื้นที่ที่เกี่ยวข้อง

๓. การประเมินและการทดสอบ ประเมินการออกแบบการควบคุม (Design Effectiveness) ตรวจสอบว่ามาตรการควบคุมที่องค์กรมีอยู่นั้นถูกออกแบบมาอย่างเหมาะสมเพื่อป้องกันการไม่ปฏิบัติตาม ทดสอบประสิทธิภาพการปฏิบัติงาน (Operating Effectiveness) ตรวจสอบว่ามาตรการควบคุมเหล่านั้นถูกนำไปปฏิบัติจริงและทำงานได้อย่างมีประสิทธิภาพ ตรวจสอบหลักฐาน ตรวจสอบเอกสาร หลักฐานการอนุมัติ บันทึกการฝึกอบรม หรือบันทึกอื่นๆ ที่แสดงถึงการปฏิบัติตามข้อกำหนด

๔. การวิเคราะห์และระบุข้อค้นพบ ระบุช่องว่าง/ข้อบกพร่อง (Gaps/Deficiencies) ค้นหาจุดที่องค์กรยังไม่ปฏิบัติตามกฎหมายหรือมาตรฐาน ประเมินความเสี่ยง วิเคราะห์ผลกระทบและความรุนแรงของข้อบกพร่องที่พบ ค้นหาสาเหตุหลัก ระบุสาเหตุที่แท้จริงของการไม่ปฏิบัติตาม (เช่น ขาดความรู้, ไม่มีกระบวนการ, ระบบไม่รองรับ)

๕. การจัดทำรายงาน นำเสนอรายงานผลการตรวจสอบที่ชัดเจน ครอบคลุมข้อค้นพบ, ความเสี่ยง, และข้อเสนอแนะในการแก้ไขและปรับปรุง นำเสนอแก่ผู้บริหารระดับสูงและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

๖. การติดตามผล ติดตามความคืบหน้าของการดำเนินการแก้ไขตามข้อเสนอแนะ ตรวจสอบให้แน่ใจว่าปัญหาที่ระบุได้รับการแก้ไขอย่างมีประสิทธิภาพและยั่งยืน

ประโยชน์ของการตรวจสอบการปฏิบัติตามกฎหมายและมาตรฐาน

๑. ป้องกันบทลงโทษและค่าปรับ ลดความเสี่ยงในการถูกปรับหรือถูกฟ้องร้องจากหน่วยงานกำกับดูแล

๒. ปกป้องชื่อเสียงองค์กร สร้างความเชื่อมั่นและความไว้วางใจให้กับลูกค้า คู่ค้า และสาธารณชน

๓. เพิ่มประสิทธิภาพการดำเนินงาน การปฏิบัติตามกฎระเบียบมักจะนำไปสู่กระบวนการที่ชัดเจนและมีประสิทธิภาพมากขึ้น

๔. ลดความเสี่ยงทางธุรกิจ ช่วยให้องค์กรระบุและจัดการความเสี่ยงที่เกี่ยวข้องกับการไม่ปฏิบัติตามได้อย่างรวดเร็ว

๕. สร้างความได้เปรียบในการแข่งขัน การแสดงให้เห็นถึงการปฏิบัติตามมาตรฐานสูงสามารถเป็นจุดเด่นทางการตลาด

๖. ส่งเสริมธรรมาภิบาลที่ดี สนับสนุนการบริหารจัดการองค์กรที่ดีและมีความรับผิดชอบ

การตรวจสอบการปฏิบัติตามกฎหมายและมาตรฐานไม่ใช่แค่การทำตามข้อบังคับ แต่เป็นการลงทุนที่สำคัญในการสร้างความมั่นคง ความยั่งยืน และความน่าเชื่อถือให้กับองค์กรในระยะยาว

๗. การตรวจสอบความโปร่งใสและการรายงานผล

การตรวจสอบความโปร่งใสและการรายงานผล (Transparency and Reporting Audit) เป็นกระบวนการที่สำคัญในการประเมินว่าองค์กรมีการเปิดเผยข้อมูลอย่างตรงไปตรงมา ครบถ้วน และทันเวลาเพียงพอหรือไม่ รวมถึงตรวจสอบความถูกต้องและความน่าเชื่อถือของรายงานผลการดำเนินงานต่างๆ การตรวจสอบนี้ช่วยสร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสีย ทั้งผู้ถือหุ้น พนักงาน ลูกค้า คู่ค้า และสาธารณชน

วัตถุประสงค์ของการตรวจสอบความโปร่งใสและการรายงานผล

การตรวจสอบความโปร่งใสและการรายงานผลมีวัตถุประสงค์หลักดังนี้ สร้างความเชื่อมั่น ทำให้ผู้มีส่วนได้ส่วนเสียมั่นใจว่าข้อมูลที่องค์กรเปิดเผยนั้นถูกต้อง เป็นจริง และไม่บิดเบือน สนับสนุนการตัดสินใจ ตรวจสอบว่ารายงานผลการดำเนินงานมีความน่าเชื่อถือเพียงพอสำหรับการตัดสินใจเชิงกลยุทธ์และการลงทุน ป้องกันการทุจริตและข้อผิดพลาด การเปิดเผยข้อมูลอย่างโปร่งใสช่วยลดโอกาสในการปกปิดการทุจริตหรือข้อผิดพลาด ปฏิบัติตามกฎระเบียบ ตรวจสอบว่าองค์กรปฏิบัติตามข้อกำหนดของกฎหมายและหน่วยงานกำกับดูแลเกี่ยวกับการเปิดเผยข้อมูลและการรายงานผล (เช่น ข้อกำหนดของตลาดหลักทรัพย์, กฎหมายคุ้มครองข้อมูลส่วนบุคคล) เสริมสร้างธรรมาภิบาลส่งเสริมหลักการกำกับดูแลกิจการที่ดี (Good Corporate Governance) ด้วยการสร้างวัฒนธรรมองค์กรที่เน้นความซื่อสัตย์สุจริตและความรับผิดชอบ ปรับปรุงชื่อเสียงองค์กร องค์กรที่มีความโปร่งใสสูงมักจะได้รับความไว้วางใจและมีภาพลักษณ์ที่ดีในสายตาของสาธารณชน

ขอบเขตของการตรวจสอบความโปร่งใสและการรายงานผล

การตรวจสอบนี้สามารถครอบคลุมได้หลากหลายด้าน ขึ้นอยู่กับประเภทและขนาดขององค์กร รวมถึงข้อกำหนดเฉพาะของอุตสาหกรรมนั้นๆ

๑. การรายงานทางการเงิน (Financial Reporting) งบการเงิน ตรวจสอบความถูกต้อง ครบถ้วน และความสอดคล้องของงบแสดงฐานะการเงิน งบกำไรขาดทุน งบกระแสเงินสด และงบการเปลี่ยนแปลงส่วนของผู้ถือหุ้น กับมาตรฐานการบัญชีที่ยอมรับโดยทั่วไป (เช่น TFRS, IFRS) หมายเหตุประกอบงบการเงิน ตรวจสอบว่ามีการเปิดเผยข้อมูลสำคัญอย่างเพียงพอและเหมาะสมตามที่กำหนด รายงานประจำปี (Annual Report) ประเมินว่าข้อมูลในรายงานประจำปีมีความสอดคล้องกับงบการเงินและให้ภาพรวมที่ถูกต้องของผลการดำเนินงาน รายงานภายใน (Internal Reports) ตรวจสอบความน่าเชื่อถือและความแม่นยำของรายงานทางการเงินที่ใช้ภายในองค์กร เช่น รายงานงบประมาณ, รายงานต้นทุน

๒. การรายงานที่ไม่ใช่ทางการเงิน (Non-Financial Reporting) รายงานความยั่งยืน/ESG (Environmental, Social, and Governance) ตรวจสอบความถูกต้องของข้อมูลที่เกี่ยวข้องกับผลกระทบต่อสิ่งแวดล้อม สังคม และการกำกับดูแลกิจการ (เช่น การปล่อยก๊าซเรือนกระจก, ความหลากหลายของพนักงาน, จริยธรรมทางธุรกิจ) รายงานความรับผิดชอบต่อสังคม (CSR Report) ประเมินความน่าเชื่อถือของข้อมูลเกี่ยวกับกิจกรรมเพื่อสังคมและการมีส่วนร่วมกับชุมชน รายงานการกำกับดูแลกิจการที่ดี (Corporate Governance Report) ตรวจสอบว่ามีการเปิดเผยข้อมูลเกี่ยวกับโครงสร้างการกำกับดูแล, คณะกรรมการ, ค่าตอบแทนผู้บริหาร, และนโยบายที่เกี่ยวข้อง ข้อมูลผลิตภัณฑ์และบริการ ความถูกต้องของข้อมูลที่เปิดเผยเกี่ยวกับผลิตภัณฑ์ บริการ และข้อกำหนดและเงื่อนไขต่างๆ

๓. กระบวนการและระบบที่เกี่ยวข้องกับการรายงาน (Reporting Processes and Systems) ระบบรวบรวมข้อมูล ตรวจสอบว่าระบบที่ใช้ในการรวบรวมข้อมูลสำหรับการรายงานมีความถูกต้อง เชื่อถือได้ และมีการควบคุมที่เพียงพอ กระบวนการตรวจสอบและอนุมัติ มีการกำหนดกระบวนการตรวจสอบและอนุมัติข้อมูลก่อนการเปิดเผยที่ชัดเจนและรัดกุมหรือไม่ การควบคุมภายใน ประเมินประสิทธิภาพของการควบคุมภายในที่ออกแบบมาเพื่อป้องกันข้อผิดพลาดหรือการบิดเบือนข้อมูลในการรายงาน การจัดการข้อมูล ตรวจสอบว่ามีการบริหารจัดการข้อมูลอย่างเหมาะสม ตั้งแต่การเก็บ การประมวลผล ไปจนถึงการจัดเก็บถาวร

๔. การสื่อสารและการเปิดเผยข้อมูล (Communication and Disclosure) ช่องทางการสื่อสาร ตรวจสอบว่ามีการใช้ช่องทางการสื่อสารที่เหมาะสมและเข้าถึงได้ง่ายสำหรับผู้มีส่วนได้ส่วนเสีย (เช่น เว็บไซต์,ข่าวประชาสัมพันธ์) ความทันเวลา ข้อมูลถูกเปิดเผยอย่างทันเวลาตามข้อกำหนดหรือไม่ ความชัดเจนและเข้าใจง่าย ข้อมูลที่เปิดเผยมีความชัดเจน ตรงไปตรงมา และเข้าใจง่ายหรือไม่ การปฏิบัติตามกฎหมายที่เกี่ยวข้อง ตรวจสอบการเปิดเผยข้อมูลว่าเป็นไปตามกฎหมายและข้อกำหนดของหน่วยงานกำกับดูแลที่เกี่ยวข้องหรือไม่

กระบวนการตรวจสอบความโปร่งใสและการรายงานผล

๑. การวางแผนและกำหนดขอบเขต ระบุประเภทของรายงานและข้อมูลที่จะตรวจสอบ (เช่น รายงานทางการเงิน, รายงาน ESG) กำหนดวัตถุประสงค์ของการตรวจสอบ (เช่น เพื่อรับรองความถูกต้องของรายงาน ESG) ทำความเข้าใจข้อกำหนดการเปิดเผยข้อมูลของหน่วยงานกำกับดูแลและมาตรฐานที่เกี่ยวข้อง

๒. การทำความเข้าใจกระบวนการรวบรวมและรายงานข้อมูล ศึกษาแผนผังกระบวนการ (Flowcharts) และเอกสารขั้นตอนการทำงานที่เกี่ยวข้องกับการสร้างรายงาน สัมภาษณ์บุคลากรที่มีส่วนร่วมในการรวบรวม ประมวลผล และจัดทำรายงาน ทำความเข้าใจระบบและเครื่องมือที่ใช้ในการจัดเก็บและวิเคราะห์ข้อมูล

๓. การประเมินและการทดสอบ การตรวจสอบเอกสาร ทบทวนรายงานต่างๆ ที่องค์กรเผยแพร่ รวมถึงหลักฐานอ้างอิงของข้อมูลที่ระบุในรายงาน การทดสอบการควบคุมภายใน ตรวจสอบว่าการควบคุมที่ออกแบบมาเพื่อรับรองความถูกต้องของข้อมูล (เช่น การอนุมัติ, การกระทบยอด) ทำงานได้อย่างมีประสิทธิภาพ การทดสอบความถูกต้องของข้อมูล เลือกตัวอย่างข้อมูลจากรายงานและทำการยืนยันความถูกต้องกับแหล่งข้อมูลต้นฉบับหรือหลักฐานภายนอก การวิเคราะห์ข้อมูล ใช้เทคนิคการวิเคราะห์ข้อมูลเพื่อหาความผิดปกติหรือความไม่สอดคล้องกันของข้อมูลในรายงาน การประเมินการเปิดเผยข้อมูล ตรวจสอบว่าข้อมูลที่เปิดเผยครบถ้วน ชัดเจน และเป็นไปตามข้อกำหนดหรือไม่

๔. การระบุข้อค้นพบและข้อบกพร่อง สรุปข้อผิดพลาด, ความไม่สอดคล้อง, หรือช่องว่างในการเปิดเผยข้อมูลที่พบ ระบุสาเหตุของข้อบกพร่อง และประเมินผลกระทบที่อาจเกิดขึ้น (เช่น ผลกระทบทางการเงิน, ผลกระทบต่อชื่อเสียง)

๕. การจัดทำรายงาน จัดทำรายงานผลการตรวจสอบที่ครอบคลุมข้อค้นพบ, ระดับความรุนแรงของปัญหา, และข้อเสนอแนะในการปรับปรุง รายงานควรเป็นกลาง ตรงไปตรงมา และเน้นข้อมูลที่ช่วยให้องค์กรสามารถปรับปรุงได้

๖. การติดตามผล ติดตามความคืบหน้าของการดำเนินการแก้ไขตามข้อเสนอแนะ ตรวจสอบให้แน่ใจว่าข้อบกพร่องได้รับการแก้ไขอย่างเหมาะสมและมีการปรับปรุงกระบวนการอย่างยั่งยืน

ประโยชน์ของการตรวจสอบความโปร่งใสและการรายงานผล

๑. เพิ่มความน่าเชื่อถือ สร้างความมั่นใจให้กับนักลงทุน ลูกค้า และสาธารณชนว่าองค์กรดำเนินงานด้วยความซื่อสัตย์

๒. เสริมสร้างภาพลักษณ์ที่ดี องค์กรที่โปร่งใสมีแนวโน้มที่จะได้รับความไว้วางใจและมีชื่อเสียงที่ดีในตลาด

๓. ลดความเสี่ยงทางกฎหมายและชื่อเสียง ลดโอกาสในการถูกฟ้องร้อง ถูกปรับ หรือได้รับความเสียหายต่อชื่อเสียงจากการเปิดเผยข้อมูลที่ไม่ถูกต้อง

๔. ดึงดูดการลงทุน นักลงทุนมักจะมองหาบริษัทที่มีความโปร่งใสในการดำเนินงานและรายงานผล

๕. ปรับปรุงการตัดสินใจภายใน ข้อมูลที่ถูกต้องและเชื่อถือได้ช่วยให้ผู้บริหารตัดสินใจได้อย่างแม่นยำยิ่งขึ้น

๖. ส่งเสริมวัฒนธรรมองค์กรที่ดี กระตุ้นให้พนักงานตระหนักถึงความสำคัญของความซื่อสัตย์สุจริตและความรับผิดชอบในการทำงาน

การตรวจสอบความโปร่งใสและการรายงานผลไม่ได้เป็นเพียงแค่การปฏิบัติตามข้อกำหนด แต่เป็นการลงทุนที่สำคัญในการสร้างความยั่งยืนและความสำเร็จให้กับองค์กรในระยะยาว

วันที่ ๔ กรกฎาคม ๒๕๖๘

บรรยายโดย อ.พัทยา ปานสุวรรณ ผู้อำนวยการกองการตรวจสอบระบบสารสนเทศ สำนักงานตรวจสอบ การประปานครหลวง (กปน.)

เหตุผลที่ผู้ตรวจสอบภายในต้องเข้าใจการเขียนโปรแกรม

ตรวจสอบระบบอัตโนมัติ
เข้าใจการทำงานของระบบและตรรกะโปรแกรมที่ใช้ในสถาบัน

วิเคราะห์ข้อมูลปริมาณมาก
ประมวลผลข้อมูลจำนวนมากได้อย่างมีประสิทธิภาพ

ตรวจจับความผิดปกติ
สร้างอัลกอริทึมค้นหารูปแบบผิดปกติในข้อมูล

สร้างเครื่องมืออัตโนมัติ
พัฒนา script ช่วยงานตรวจสอบประจำให้ทำงานเร็วขึ้น

เหตุผลที่ผู้ตรวจสอบภายในจำเป็นต้องมีความเข้าใจในการเขียนโปรแกรมนั้นมีหลากหลายและมีความสำคัญอย่างยิ่งในยุคดิจิทัลเช่นปัจจุบัน ไม่ใช่แค่เรื่องของเทคโนโลยีเท่านั้น แต่ยังรวมถึงความสามารถในการทำงานให้มีประสิทธิภาพและประสิทธิผลมากขึ้นด้วย

๑. เข้าใจการทำงานของระบบและข้อมูลเชิงลึกการเขียนโปรแกรมช่วยให้ผู้ตรวจสอบเข้าใจ ตรรกะการทำงาน (Logic) ของระบบซอฟต์แวร์และแอปพลิเคชันต่างๆ ได้ลึกซึ้งขึ้น เช่น ระบบ ERP, CRM หรือระบบการเงิน การรู้หลักการเขียนโค้ดทำให้สามารถวิเคราะห์ flow ของข้อมูล มองเห็นเส้นทางการไหลของข้อมูลตั้งแต่ต้นจนจบ ทำให้เข้าใจว่าข้อมูลถูกป้อน ประมวลผล และส่งออกอย่างไร ระบุช่องโหว่ด้านตรรกะ ไม่ใช่แค่ช่องโหว่ด้านเทคนิค แต่รวมถึงข้อผิดพลาดในการออกแบบระบบหรือตรรกะทางธุรกิจที่อาจนำไปสู่การทุจริตหรือข้อผิดพลาด เข้าใจความสัมพันธ์ของข้อมูล รู้ว่าข้อมูลจากตารางต่างๆ เชื่อมโยงกันอย่างไร ซึ่งสำคัญต่อการตรวจสอบความถูกต้องของข้อมูล

๒. เพิ่มประสิทธิภาพในการเข้าถึงและวิเคราะห์ข้อมูลในอดีตผู้ตรวจสอบอาจต้องพึ่งพาฝ่าย IT ในการดึงข้อมูล แต่เมื่อมีความรู้ด้านการเขียนโปรแกรม (เช่น SQL สำหรับฐานข้อมูล หรือ Python/R สำหรับการวิเคราะห์ข้อมูล) จะทำให้ดึงข้อมูลได้เองไม่ต้องรอให้ฝ่าย IT ช่วย ทำให้กระบวนการตรวจสอบรวดเร็วขึ้นและลดภาระงานของฝ่ายอื่น วิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) สามารถเขียนสคริปต์เพื่อประมวลผลข้อมูลจำนวนมหาศาล เพื่อค้นหาความผิดปกติ รูปแบบ หรือแนวโน้มที่บ่งชี้ถึงความเสี่ยงหรือการทุจริต (Data Analytics for Audit) สร้างรายงานอัตโนมัติ พัฒนาเครื่องมือเล็กๆ เพื่อสร้างรายงานการตรวจสอบซ้ำๆ ได้โดยอัตโนมัติ ช่วยลดเวลาและข้อผิดพลาด

๓. ประเมินความปลอดภัยของระบบแอปพลิเคชันและข้อมูลความรู้ด้านการเขียนโปรแกรมเป็นพื้นฐานสำคัญในการตรวจสอบความปลอดภัยทางไซเบอร์ โดยเฉพาะอย่างยิ่งในส่วนของแอปพลิเคชัน (Application Security) ทำให้ผู้ตรวจสอบสามารถตรวจสอบโค้ดเบื้องต้น แม้ไม่ได้เป็นผู้เชี่ยวชาญด้านความปลอดภัยโค้ดโดยตรง แต่การเข้าใจโครงสร้างโค้ดจะช่วยให้ระบุรูปแบบโค้ดที่อาจเป็นอันตราย (เช่น SQL Injection, Cross-Site Scripting) หรือช่องโหว่พื้นฐานได้ เข้าใจการตั้งค่าความปลอดภัย รู้ว่าการตั้งค่าต่างๆ ในระบบมีผลต่อการทำงานของโค้ดอย่างไร และส่งผลต่อความปลอดภัยหรือไม่ สื่อสารกับผู้เชี่ยวชาญด้าน IT ได้ดีขึ้นใช้ภาษาเดียวกันกับนักพัฒนาหรือวิศวกรความปลอดภัย ทำให้การสื่อสารมีประสิทธิภาพและประเด็นการตรวจสอบชัดเจนขึ้น

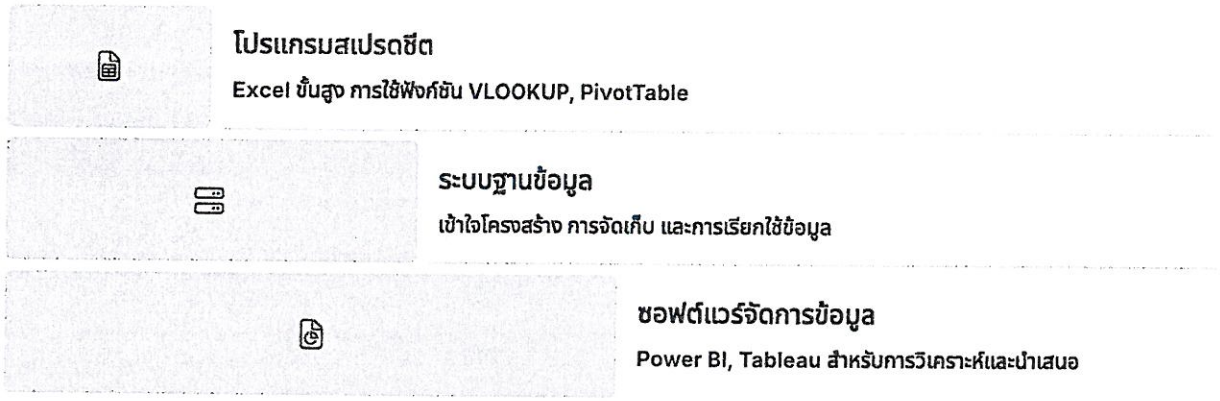
๔. พัฒนาเครื่องมือตรวจสอบอัตโนมัติ (Automated Audit Tools) ผู้ตรวจสอบภายในที่มีทักษะการเขียนโปรแกรมสามารถสร้างสคริปต์การตรวจสอบ (Audit Scripts) พัฒนาสคริปต์เพื่อตรวจสอบการควบคุมภายในที่ทำซ้ำๆ ได้โดยอัตโนมัติ เช่น การตรวจสอบสิทธิ์การเข้าถึง, การตรวจสอบบันทึกการเปลี่ยนแปลง (Log files) พัฒนา CAATs (Computer Assisted Audit Techniques) ใช้ความรู้ด้านการเขียนโปรแกรมในการสร้างหรือปรับแต่งเครื่องมือเพื่อช่วยในการตรวจสอบข้อมูลและระบบ ทำงานร่วมกับเทคโนโลยีใหม่ๆ เมื่อองค์กรนำเทคโนโลยีใหม่ๆ เช่น AI, Machine Learning, Blockchain มาใช้ ผู้ตรวจสอบที่เข้าใจหลักการเขียนโปรแกรมจะสามารถทำความเข้าใจและตรวจสอบเทคโนโลยีเหล่านี้ได้ดียิ่งขึ้น

๕. เป็นที่ปรึกษาและผู้สร้างคุณค่าเพิ่มการเข้าใจการเขียนโปรแกรมทำให้ผู้ตรวจสอบภายในสามารถก้าวข้ามบทบาทจากการเป็นเพียงผู้จับผิด ไปสู่การเป็น ที่ปรึกษาเชิงกลยุทธ์ (Strategic Advisor) ได้ โดยการให้คำแนะนำที่มีคุณภาพ เสนอแนะแนวทางแก้ไขปัญหาที่ปฏิบัติได้จริงและมีประสิทธิภาพมากขึ้น เพราะเข้าใจข้อจำกัดทางเทคนิคและโอกาสในการปรับปรุง ระบุโอกาสในการปรับปรุงกระบวนการ มองเห็นโอกาสในการใช้เทคโนโลยีเพื่อปรับปรุง

ประสิทธิภาพและประสิทธิผลของกระบวนการทางธุรกิจ เพิ่มคุณค่าให้กับองค์กรไม่ใช่แค่การค้นหาปัญหา แต่ยังช่วยองค์กรให้เติบโตและปรับตัวในยุคดิจิทัลได้อย่างมั่นคง

บทสรุป ในโลกที่ขับเคลื่อนด้วยเทคโนโลยี การที่ผู้ตรวจสอบภายในมีความเข้าใจในการเขียนโปรแกรม ไม่ได้หมายความว่าทุกคนจะต้องเป็นนักพัฒนาซอฟต์แวร์ แต่หมายถึงการมีความเข้าใจในแนวคิดพื้นฐาน (Fundamental Concepts) และสามารถประยุกต์ใช้เครื่องมือการเขียนโปรแกรมง่ายๆ เพื่อเพิ่มขีดความสามารถในการทำงานของตนเอง การมีทักษะนี้จะช่วยให้งานตรวจสอบภายในมีความทันสมัย มีประสิทธิภาพ และสามารถสร้างมูลค่าเพิ่มให้กับองค์กรได้อย่างแท้จริง

ทักษะด้านเทคโนโลยีที่จำเป็น



ในยุคที่เทคโนโลยีเข้ามามีบทบาทสำคัญในทุกมิติของธุรกิจและองค์กร ทักษะด้านเทคโนโลยีจึงเป็นสิ่งจำเป็นอย่างยิ่งสำหรับทุกคน ไม่เว้นแม้แต่ผู้บริหารและพนักงานในสายงานที่ไม่ใช่เทคนิคโดยตรง โดยเฉพาะอย่างยิ่งผู้ที่อยู่ในตำแหน่งงานที่ต้องใช้ข้อมูลและระบบในการทำงานและการตัดสินใจ ต่อไปนี้คือทักษะด้านเทคโนโลยีที่จำเป็นในตลาดแรงงานปัจจุบันและอนาคต:

๑. ทักษะพื้นฐานดิจิทัล (Digital Literacy) คือทักษะตั้งต้นที่ทุกคนควรมี เป็นรากฐานสำคัญในการต่อยอดไปสู่ทักษะอื่น ๆ ที่ซับซ้อนขึ้น การใช้คอมพิวเตอร์และอินเทอร์เน็ต เข้าใจการทำงานพื้นฐานของระบบปฏิบัติการ, การใช้งานเว็บเบราว์เซอร์, การค้นหาข้อมูล การใช้งานโปรแกรมสำนักงาน ความสามารถในการใช้โปรแกรมประมวลผลคำ (เช่น Microsoft Word, Google Docs), โปรแกรมตารางคำนวณ (เช่น Microsoft Excel, Google Sheets), และโปรแกรมนำเสนอข้อมูล (เช่น Microsoft PowerPoint, Google Slides) ในการสร้าง จัดการ และวิเคราะห์ข้อมูลเบื้องต้น การทำงานร่วมกันแบบออนไลน์ ใช้เครื่องมือสำหรับการทำงานร่วมกัน เช่น Google Workspace, Microsoft ๓๖๕, Zoom, Microsoft Teams เพื่อการสื่อสารและการทำงานเป็นทีมที่มีประสิทธิภาพ ความมั่นคงปลอดภัยไซเบอร์เบื้องต้น เข้าใจภัยคุกคามไซเบอร์พื้นฐาน (เช่น ฟิชชิ่ง, มัลแวร์), การป้องกันตนเอง (เช่น การตั้งรหัสผ่านที่รัดกุม, การระวังการคลิกลิงก์ที่ไม่รู้จัก), และความสำคัญของการปกป้องข้อมูลส่วนบุคคล

๒. ทักษะการวิเคราะห์ข้อมูล (Data Analytics) ในโลกที่เต็มไปด้วยข้อมูล องค์กรจำเป็นต้องใช้ข้อมูลในการตัดสินใจ การมีทักษะในการวิเคราะห์ข้อมูลจึงเป็นสิ่งสำคัญอย่างยิ่งความเข้าใจด้านข้อมูล (Data Understanding) รู้จักประเภทของข้อมูล, แหล่งที่มาของข้อมูล, และความสำคัญของคุณภาพข้อมูล การใช้เครื่องมือวิเคราะห์ข้อมูล โปรแกรมตารางคำนวณขั้นสูง (Advanced Excel) การใช้สูตรที่ซับซ้อน, PivotTable, การสร้างกราฟและแผนภูมิเพื่อแสดงผลข้อมูล เครื่องมือ BI (Business Intelligence Tools) เช่น Power BI, Tableau, Looker Studio (Google Data Studio) ในการสร้างแดชบอร์ดและรายงานที่เข้าใจง่าย ภาษาโปรแกรมเพื่อการวิเคราะห์ข้อมูล Python (พร้อมไลบรารีเช่น Pandas, NumPy) และ R เป็นภาษาที่นิยมใช้สำหรับการจัดการข้อมูล, การวิเคราะห์เชิงสถิติ, และการสร้างแบบจำลอง SQL (Structured Query Language) ภาษาสำหรับเรียกใช้ จัดการ และวิเคราะห์ข้อมูลจากฐานข้อมูล ซึ่งเป็นทักษะสำคัญสำหรับผู้ที่ต้องทำงานกับข้อมูลจำนวนมาก การตีความข้อมูลสามารถตีความผลการวิเคราะห์เพื่อหา insight และแปลงข้อมูลให้เป็นข้อมูลที่นำไปใช้ในการตัดสินใจได้

๓. ทักษะความปลอดภัยไซเบอร์ (Cybersecurity) ภัยคุกคามทางไซเบอร์เป็นความเสี่ยงสำคัญสำหรับทุกองค์กร ทักษะด้านความปลอดภัยจึงเป็นสิ่งจำเป็นเพื่อปกป้องข้อมูลและระบบการบริหารจัดการความเสี่ยงไซเบอร์การระบุ, ประเมิน, และบรรเทาความเสี่ยงด้านความปลอดภัยของข้อมูลและระบบ การประเมินช่องโหว่และการทดสอบการเจาะระบบ (Vulnerability Assessment & Penetration Testing - VAPT) เข้าใจหลักการและกระบวนการในการค้นหาช่องโหว่ในระบบเครือข่าย, แอปพลิเคชัน, และโครงสร้างพื้นฐาน การตอบสนองต่อเหตุการณ์ (Incident Response) ความเข้าใจในการจัดการและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยเมื่อเกิดการโจมตี การปฏิบัติตามมาตรฐานความปลอดภัย เข้าใจมาตรฐานและกรอบการทำงานด้านความปลอดภัย เช่น ISO ๒๗๐๐๑, NIST Cybersecurity Framework

๔. ทักษะการเข้าใจและประยุกต์ใช้เทคโนโลยีเกิดใหม่ (Emerging Technologies) การทำความเข้าใจเทคโนโลยีใหม่ๆ ที่กำลังเข้ามามีบทบาทจะช่วยให้องค์กรสามารถปรับตัวและสร้างความได้เปรียบ ปัญญาประดิษฐ์ (Artificial Intelligence - AI) และ Machine Learning (ML) ความเข้าใจพื้นฐานรู้ว่า AI/ML ทำงานอย่างไร, ประเภทของ AI, และกรณีการใช้งานในธุรกิจ (เช่น การวิเคราะห์เชิงคาดการณ์, การทำงานอัตโนมัติ) Prompt Engineering ทักษะในการสร้างคำสั่ง (prompt) ที่มีประสิทธิภาพเพื่อดึงศักยภาพของ AI (เช่น Generative AI อย่าง ChatGPT) มาใช้งาน คลาวด์คอมพิวติ้ง (Cloud Computing) เข้าใจหลักการทำงานของบริการคลาวด์ (เช่น IaaS, PaaS, SaaS) และแพลตฟอร์มคลาวด์ยอดนิยม (เช่น AWS, Azure, Google Cloud) รวมถึงความสำคัญด้านความปลอดภัยและการจัดการข้อมูลบนคลาวด์ บล็อกเชน (Blockchain) ความเข้าใจพื้นฐานเกี่ยวกับเทคโนโลยีบล็อกเชนและศักยภาพในการสร้างความโปร่งใสและตรวจสอบย้อนกลับได้ในธุรกิจ IoT (Internet of Things) เข้าใจว่าอุปกรณ์เชื่อมต่อทำงานร่วมกันอย่างไร และข้อมูลจาก IoT สามารถนำมาใช้ประโยชน์ในธุรกิจได้อย่างไร

๕. ทักษะด้านการเขียนโปรแกรมพื้นฐาน (Basic Programming/Scripting) แม้ไม่จำเป็นต้องเป็นนักพัฒนาเต็มตัว แต่การมีความเข้าใจในการเขียนโปรแกรมพื้นฐานจะช่วยเพิ่มประสิทธิภาพในการทำงานได้อย่างมาก Python เป็นภาษาที่ได้รับความนิยมอย่างมากเนื่องจากเรียนรู้ง่ายและใช้งานได้หลากหลาย ทั้งการวิเคราะห์ข้อมูล, การทำงานอัตโนมัติ, และการสร้างแอปพลิเคชันขนาดเล็ก Visual Basic for Applications (VBA) สำหรับการทำงานอัตโนมัติในโปรแกรม Microsoft Office (เช่น Excel Macros) ซึ่งยังคงมีประโยชน์ในหลายองค์กร ความเข้าใจใน Logic และ Algorithms การคิดเชิงตรรกะและเข้าใจกระบวนการทำงานแบบเป็นขั้นตอน ซึ่งเป็นหัวใจสำคัญของการเขียนโปรแกรม

๖. ทักษะการจัดการกระบวนการอัตโนมัติ (Process Automation / RPA) Robotic Process Automation (RPA) การใช้ซอฟต์แวร์หุ่นยนต์เพื่อทำงานซ้ำๆ หรืองานที่มีกฎเกณฑ์ชัดเจนให้เป็นอัตโนมัติ ช่วยลดความผิดพลาดและเพิ่มประสิทธิภาพในการทำงาน. การเข้าใจ RPA จะช่วยให้สามารถระบุงานที่เหมาะสมกับการทำ Automation และประเมินผลกระทบได้

การพัฒนาทักษะเหล่านี้อย่างต่อเนื่องจะช่วยให้บุคคลมีความสามารถในการปรับตัวเข้ากับการเปลี่ยนแปลงทางเทคโนโลยี และเป็นที่ต้องการในตลาดแรงงานที่เปลี่ยนแปลงอย่างรวดเร็ว

การนำความรู้โปรแกรมไปประยุกต์ใช้จริง

โดยแบ่งออกเป็น ๓ หัวข้อหลัก พร้อมตัวอย่างการประยุกต์ใช้ในแต่ละด้าน

๑. ตรวจสอบข้อมูลเงิน (Financial Data Verification) สร้าง script เปรียบเทียบข้อมูลเงินระหว่างระบบต่างๆ ผู้ที่เข้าใจการเขียนโปรแกรมสามารถเขียนโปรแกรมหรือสคริปต์เพื่อดึงข้อมูลทางการเงินจากระบบที่แตกต่างกัน (เช่น ระบบบัญชี, ระบบธนาคาร, ระบบ CRM) มาเปรียบเทียบกันโดยอัตโนมัติ เพื่อให้มั่นใจว่าข้อมูลมีความสอดคล้องกันและไม่มีข้อผิดพลาด ค้นหารายการที่ไม่ตรงกัน หรือมีความผิดปกติ สคริปต์ที่สร้างขึ้นสามารถช่วยระบุรายการธุรกรรมทางการเงินที่ไม่สอดคล้องกัน หรือมีรูปแบบที่ผิดปกติ ซึ่งอาจเป็นสัญญาณของการทุจริต, ข้อผิดพลาดในการบันทึกข้อมูล, หรือปัญหาในกระบวนการทำงาน

๒. ตรวจสอบการปฏิบัติตามระเบียบ (Compliance Verification) สร้างระบบตรวจจับเอกสารที่ไม่ครบตามระเบียบ สามารถเขียนโปรแกรมเพื่อตรวจสอบเอกสารหรือข้อมูลที่จำเป็นตามระเบียบข้อบังคับต่างๆ ว่ามีการจัดเก็บครบถ้วนหรือไม่ เช่น เอกสารสัญญา, ใบอนุญาต, หรือข้อมูลที่ต้องเปิดเผยตามกฎหมาย ค้นหารายการที่อาจมีความเสี่ยงด้านการปฏิบัติตามกฎ โปรแกรมสามารถช่วยวิเคราะห์ข้อมูลและระบุธุรกรรมหรือกิจกรรมที่อาจขัดต่อกฎหมาย นโยบาย หรือข้อบังคับที่กำหนดไว้ เช่น การจ่ายเงินที่ไม่ได้รับอนุมัติ, การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต, หรือการดำเนินการที่ไม่เป็นไปตามขั้นตอนที่กำหนด

๓. วิเคราะห์แนวโน้มและรูปแบบ (Trend and Pattern Analysis) สร้างกราฟและรายงานอัตโนมัติจากข้อมูลการตรวจสอบ ผู้ที่มีความรู้ด้านโปรแกรมสามารถเขียนโค้ดเพื่อดึงข้อมูลจากการตรวจสอบมาสร้างกราฟและรายงานผลแบบอัตโนมัติ ทำให้ไม่ต้องเสียเวลาในการจัดทำรายงานด้วยมือ และช่วยให้เห็นภาพรวมของข้อมูลได้ง่ายขึ้น ระบุแนวโน้มหรือรูปแบบที่อาจบ่งชี้ปัญหา การวิเคราะห์ข้อมูลด้วยโปรแกรมสามารถช่วยระบุแนวโน้มที่น่าสนใจหรือรูปแบบที่ผิดปกติในชุดข้อมูล ซึ่งอาจบ่งชี้ถึงปัญหาที่ซ่อนอยู่ เช่น การเพิ่มขึ้นของข้อผิดพลาดในบางกระบวนการ, การใช้ทรัพยากรที่สูงเกินจริง, หรือประสิทธิภาพที่ลดลง

โดยรวมแล้ว ประโยชน์ของการนำความรู้ด้านการเขียนโปรแกรมมาใช้ในงานตรวจสอบภายในและงานควบคุมคุณภาพ เพื่อเพิ่มประสิทธิภาพ ความถูกต้อง และความสามารถในการค้นหาปัญหาหรือความเสี่ยงที่อาจเกิดขึ้นได้อย่างรวดเร็วและแม่นยำยิ่งขึ้น

เส้นทางการพัฒนาทักษะสำหรับผู้ตรวจสอบภายใน

โดยนำเสนอทักษะที่ควรพัฒนาเรียงลำดับจากพื้นฐานไปสู่ระดับที่ซับซ้อนขึ้น และแสดงถึงระดับความเชี่ยวชาญหรือการลงทุนด้านเวลาที่ควรให้กับแต่ละทักษะโดยประมาณ (แกนนอนอาจหมายถึงระดับความเชี่ยวชาญ/เวลา/ความสำคัญสัมพัทธ์) ความสำคัญของการพัฒนาทักษะด้านเทคโนโลยีและข้อมูลสำหรับผู้ตรวจสอบภายในเพื่อให้สามารถทำงานได้อย่างมีประสิทธิภาพและทันสมัยในยุคดิจิทัล โดยมีทักษะหลักที่ระบุไว้ดังนี้

๑. พื้นฐาน Excel ขั้นสูง คือจุดเริ่มต้นที่สำคัญที่สุดสำหรับผู้ตรวจสอบภายในทุกคน แม้ว่าจะมีเครื่องมือที่ซับซ้อนกว่า แต่ Excel ยังคงเป็นเครื่องมือหลักในการจัดการและวิเคราะห์ข้อมูลเบื้องต้น ผู้ตรวจสอบควรมีทักษะในการใช้ฟังก์ชันที่ซับซ้อน, PivotTable, การสร้างกราฟ, และการจัดการข้อมูลจำนวนมากใน Excel ได้อย่างคล่องแคล่ว

๒. SQL เบื้องต้น การเข้าใจ SQL (Structured Query Language) เป็นทักษะถัดไปที่จำเป็น เพราะข้อมูลส่วนใหญ่ในองค์กรถูกจัดเก็บอยู่ในฐานข้อมูล การที่ผู้ตรวจสอบสามารถเขียนคำสั่ง SQL เบื้องต้นได้ จะช่วยให้สามารถดึงข้อมูล (Query Data) เลือกดึงข้อมูลที่ต้องการจากฐานข้อมูลได้ด้วยตนเอง โดยไม่ต้องพึ่งพาฝ่าย IT กรองและจัดเรียงข้อมูล จัดการข้อมูลที่ดึงมาเพื่อให้ง่ายต่อการวิเคราะห์เข้าใจโครงสร้างฐานข้อมูลทำให้เข้าใจว่าข้อมูลถูกจัดเก็บและเชื่อมโยงกันอย่างไร

๓. Python สำหรับข้อมูล Python เป็นภาษาโปรแกรมที่ได้รับความนิยมอย่างมากสำหรับการจัดการและวิเคราะห์ข้อมูล เนื่องจากเรียนรู้ง่ายและมีไลบรารี (libraries) ที่ทรงพลัง (เช่น Pandas, NumPy) ผู้ตรวจสอบที่เข้าใจ Python จะสามารถประมวลผลข้อมูลขนาดใหญ่ จัดการและทำความสะอาดข้อมูลจำนวนมหาศาลได้อย่างมีประสิทธิภาพ วิเคราะห์ข้อมูลเชิงลึก ทำการวิเคราะห์ทางสถิติ, สร้างแบบจำลอง, และค้นหารูปแบบหรือแนวโน้มที่ซับซ้อนในข้อมูล ทำงานอัตโนมัติบางอย่างเขียนสคริปต์เพื่อทำงานที่ซ้ำซากให้เป็นอัตโนมัติ

๔. Power BI / Tableau ทักษะเหล่านี้คือเครื่องมือสำหรับ Business Intelligence (BI) หรือการแสดงผลข้อมูล (Data Visualization) ซึ่งสำคัญมากในการสื่อสารผลการตรวจสอบและข้อมูลเชิงลึกได้อย่างมีประสิทธิภาพ สร้างแดชบอร์ด (Dashboards) ออกแบบแดชบอร์ดที่สวยงามและโต้ตอบได้ เพื่อแสดงผลลัพธ์การวิเคราะห์ข้อมูลทางการเงิน, การปฏิบัติตามกฎระเบียบ, หรือแนวโน้มต่างๆ นำเสนอข้อมูลที่ซับซ้อนให้เข้าใจง่ายแปลงข้อมูลดิบให้เป็นภาพที่เข้าใจง่าย ช่วยให้ผู้บริหารและผู้มีส่วนได้ส่วนเสียเข้าใจประเด็นสำคัญได้รวดเร็ว

๕. Audit Automation คือจุดสูงสุดของเส้นทางการพัฒนาทักษะที่นำเสนอ ซึ่งหมายถึงการนำเทคโนโลยีและโปรแกรมมาใช้เพื่อทำให้กระบวนการตรวจสอบเป็นไปโดยอัตโนมัติมากที่สุดเท่าที่จะเป็นไปได้การใช้ Robotic Process Automation (RPA) นำซอฟต์แวร์หุ่นยนต์มาทำงานซ้ำๆ เช่น การดึงข้อมูล, การเปรียบเทียบข้อมูล, หรือการตรวจสอบความถูกต้องของเอกสาร การพัฒนาสคริปต์ตรวจสอบอัตโนมัติ เขียนโค้ดหรือสคริปต์เพื่อทำการทดสอบการควบคุมภายในแบบอัตโนมัติอย่างต่อเนื่อง (Continuous Auditing) หรือตามตารางเวลาที่กำหนด การรวมระบบ (Integration) เชื่อมโยงเครื่องมือและระบบต่างๆ เข้าด้วยกัน เพื่อให้การไหลของข้อมูลและการตรวจสอบเป็นไปอย่างราบรื่น

โดยสรุปแล้ว ผู้ตรวจสอบภายในในปัจจุบันควรเป็นผู้ขับเคลื่อนด้วยข้อมูล (Data-Driven) และมีความสามารถในการใช้เทคโนโลยีเพื่อเพิ่มประสิทธิภาพและคุณค่าให้กับงานตรวจสอบ การเริ่มต้นจากทักษะพื้นฐานและค่อยๆ พัฒนาไปสู่ทักษะขั้นสูงจะช่วยให้ผู้ตรวจสอบสามารถก้าวทันโลกยุคดิจิทัลและเป็นที่ต้องการในสายงานนี้

เทคนิคการวิเคราะห์ข้อมูลเบื้องต้นสำหรับผู้ตรวจสอบภายใน

การวิเคราะห์แนวโน้ม (Trend Analysis) เทคนิคนี้เน้นการศึกษา รูปแบบและทิศทางของข้อมูลตลอดช่วงเวลา เพื่อทำความเข้าใจการเปลี่ยนแปลงที่เกิดขึ้นและคาดการณ์สิ่งที่จะเกิดขึ้นในอนาคต ผู้ตรวจสอบภายในสามารถใช้เทคนิคนี้เพื่อเปรียบเทียบผลการดำเนินงานรายเดือน/รายปี ตรวจสอบว่าผลการดำเนินงานทางการเงินหรือตัวชี้วัดสำคัญอื่นๆ มีการเปลี่ยนแปลงไปในทิศทางใดเมื่อเทียบกับช่วงเวลาที่ผ่านมา การเปลี่ยนแปลงที่สำคัญอาจบ่งชี้ถึงประสิทธิภาพที่ดีขึ้น ปัญหาที่กำลังก่อตัว หรือการเปลี่ยนแปลงที่ผิดปกติ ติดตามการเปลี่ยนแปลงของค่าใช้จ่าย วิเคราะห์ว่าค่าใช้จ่ายในหมวดหมู่ต่างๆ มีแนวโน้มเพิ่มขึ้นหรือลดลงอย่างไร เพื่อระบุค่าใช้จ่ายที่อาจสูงเกินไป หรือไม่สอดคล้องกับกิจกรรมทางธุรกิจวิเคราะห์อัตราการเติบโตหรือลดลง ประเมินอัตราการเปลี่ยนแปลงของตัวแปรต่างๆ เช่น ยอดขาย, ต้นทุน, หรือจำนวนข้อผิดพลาด เพื่อทำความเข้าใจพลวัตของธุรกิจและระบุพื้นที่ที่ต้องการการตรวจสอบเพิ่มเติม

การตรวจจับความผิดปกติ (Anomaly Detection) เทคนิคนี้มุ่งเน้นการค้นหาข้อมูลที่แตกต่างจากรูปแบบปกติ ซึ่งอาจเป็นสัญญาณของปัญหา ข้อผิดพลาด หรือการทุจริต ผู้ตรวจสอบภายในสามารถใช้เทคนิคนี้เพื่อตรวจสอบรายการที่มีมูลค่าสูงผิดปกติ ค้นหารายการธุรกรรมทางการเงินหรือกิจกรรมที่มีมูลค่าสูงเกินกว่าค่าเฉลี่ยหรือขีดจำกัดที่กำหนดไว้ ซึ่งอาจต้องมีการตรวจสอบเพิ่มเติมเพื่อยืนยันความถูกต้อง ระบุความถี่ของธุรกรรมที่ผิดแปลก วิเคราะห์รูปแบบความถี่ของการเกิดธุรกรรม เช่น การซื้อซ้ำๆ จากผู้ขายรายเดิมในเวลาอันสั้น หรือการอนุมัติหลายรายการโดยบุคคลคนเดียว ซึ่งอาจบ่งชี้ถึงความเสี่ยง หาความเบี่ยงเบนจากมาตรฐาน เปรียบเทียบข้อมูลจริงกับมาตรฐาน นโยบาย หรือเกณฑ์ที่กำหนดไว้ เพื่อระบุข้อมูลหรือกิจกรรมที่ไม่เป็นไปตามข้อกำหนด เช่น การอนุมัติที่ไม่มีเอกสารประกอบครบถ้วน หรือการจ่ายเงินที่ไม่ตรงตามเงื่อนไขสัญญา

โดยรวมแล้ว เทคนิคทั้งสองนี้เป็นพื้นฐานสำคัญที่ช่วยให้ผู้ตรวจสอบภายในสามารถใช้ข้อมูลในการค้นหาประเด็นที่น่าสงสัย วิเคราะห์สถานการณ์ และวางแผนการตรวจสอบเชิงลึกได้อย่างมีประสิทธิภาพมากยิ่งขึ้น การผสมผสานการวิเคราะห์แนวโน้มกับการตรวจจับความผิดปกติจะช่วยให้ผู้ตรวจสอบมีมุมมองที่ครอบคลุมและสามารถระบุความเสี่ยงและปัญหาที่อาจเกิดขึ้นได้อย่างแม่นยำ

ตรวจสอบการจัดซื้อจัดจ้าง (Procurement Audit)

โดยแบ่งออกเป็น ๔ ด้านหลักที่สำคัญในกระบวนการตรวจสอบ

๑. การตรวจสอบการจัดซื้อจัดจ้าง เป็นกระบวนการที่สำคัญเพื่อให้แน่ใจว่ากิจกรรมการจัดซื้อขององค์กรเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และปฏิบัติตามกฎระเบียบ โดยครอบคลุมด้านต่างๆ ดังนี้

๑.๑ รวบรวมข้อมูลใบสั่งซื้อ เน้นข้อมูลการจัดซื้อจัดจ้างทั้งหมด ขั้นตอนแรกของการตรวจสอบคือการรวบรวมข้อมูลที่เกี่ยวข้องกับการจัดซื้อจัดจ้างทั้งหมด ซึ่งรวมถึงใบสั่งซื้อ (Purchase Orders - POs), สัญญา, ใบแจ้งหนี้, เอกสารขออนุมัติ, บันทึกการรับสินค้า/บริการ และเอกสารอื่นๆ ที่เกี่ยวข้องกับกระบวนการจัดซื้อทั้งหมด การรวบรวมข้อมูลที่ครบถ้วนและเป็นระบบจะช่วยให้ผู้ตรวจสอบมีภาพรวมที่ชัดเจนและสามารถนำไปวิเคราะห์ต่อได้

๑.๒ ตรวจสอบการชำระเงิน เปรียบเทียบใบสั่งซื้อกับการชำระเงินจริง ในขั้นตอนนี้ ผู้ตรวจสอบจะทำการเปรียบเทียบข้อมูลในใบสั่งซื้อกับบันทึกการชำระเงินจริงที่เกิดขึ้น เพื่อตรวจสอบความถูกต้องและความสอดคล้องกันของตัวเลข ตัวอย่างเช่น ตรวจสอบว่าจำนวนเงินที่จ่ายตรงกับที่ระบุในใบสั่งซื้อและใบแจ้งหนี้หรือไม่

รวมถึงเงื่อนไขการชำระเงิน การตรวจสอบนี้มีวัตถุประสงค์เพื่อระบุข้อผิดพลาด, การชำระเงินเกิน, การชำระเงินซ้ำ, หรือการชำระเงินที่ไม่ได้รับอนุญาต

๑.๓ วิเคราะห์คู่ค้า ตรวจสอบประวัติและความสัมพันธ์ของคู่ค้า ผู้ตรวจสอบจะวิเคราะห์ข้อมูลเกี่ยวกับคู่ค้าหรือผู้ขายที่องค์กรมีการทำธุรกรรมด้วย ซึ่งรวมถึงประวัติการทำธุรกิจ, ความน่าเชื่อถือ, ชื่อเสียง, และความสัมพันธ์ที่อาจมีกับบุคลากรภายในองค์กร การวิเคราะห์นี้มีวัตถุประสงค์เพื่อระบุความเสี่ยงที่อาจเกิดขึ้นจากการสมยอมกัน (collusion), การมีผลประโยชน์ทับซ้อน (conflict of interest), หรือการเลือกคู่ค้าที่ไม่เหมาะสม. อาจรวมถึงการตรวจสอบรายชื่อผู้ขายที่ไม่ควรทำธุรกิจด้วย (เช่น Blacklist) หรือการตรวจสอบ KYC (Know Your Customer) เบื้องต้น

๑.๔ ตรวจสอบความสอดคล้อง ยืนยันการปฏิบัติตามระเบียบการจัดซื้อจัดจ้าง เป็นการตรวจสอบที่สำคัญที่สุดส่วนหนึ่ง เพื่อให้แน่ใจว่ากระบวนการจัดซื้อจัดจ้างทั้งหมดได้ปฏิบัติตามนโยบายและขั้นตอนปฏิบัติภายในขององค์กร รวมถึงกฎหมายและข้อบังคับที่เกี่ยวข้องภายนอก (เช่น กฎหมายการแข่งขันทางการค้า, กฎหมายป้องกันการทุจริต, ระเบียบการจัดซื้อจัดจ้างภาครัฐหากเกี่ยวข้อง). การตรวจสอบนี้ครอบคลุมตั้งแต่ขั้นตอนการวางแผน, การกำหนดคุณสมบัติ, การประมูล, การคัดเลือกผู้ขาย, การอนุมัติ, และการทำสัญญา

โดยรวมแล้ว การตรวจสอบการจัดซื้อจัดจ้างเป็นการประเมินที่ครอบคลุมหลายมิติ ตั้งแต่การรวบรวมข้อมูลไปจนถึงการวิเคราะห์เชิงลึก เพื่อให้มั่นใจว่ากระบวนการจัดซื้อเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และปราศจากการทุจริตหรือข้อผิดพลาด

๘. ประโยชน์ที่ทางราชการ/ประชาชนได้รับจากการฝึกอบรม/เข้าร่วมสังเกตการณ์

๘.๑ สามารถปรับตัวสู่การตรวจสอบภายในยุคดิจิทัล เข้าใจแนวโน้มของเทคโนโลยีที่มีผลกระทบต่อการตรวจสอบภายใน เช่น AI, Data Analytics, Blockchain และ Cloud Computing

๘.๒ สามารถเรียนรู้เครื่องมือ เทคนิค และแนวทางปรับปรุงกระบวนการตรวจสอบให้สอดคล้องกับยุคดิจิทัล

๘.๓ เพิ่มประสิทธิภาพการตรวจสอบภายในให้สอดคล้องกับการเปลี่ยนแปลงในยุคดิจิทัล

๙. ข้อเสนอแนะ แนวคิดที่นำไปปรับใช้ในการปฏิบัติงานหรือพัฒนางานที่สอดคล้องกับข้อ ๘

การตรวจสอบงบประมาณและการใช้จ่าย สามารถวิเคราะห์การจัดสรรงบประมาณ การเบิกจ่าย และการใช้จ่ายจริง เพื่อตรวจสอบความสอดคล้องกับแผนงานและระเบียบที่กำหนด รวมถึงการตรวจจับการใช้จ่ายที่ผิดปกติหรือเกินความจำเป็น ตรวจสอบกระบวนการจัดซื้อจัดจ้าง ตั้งแต่การกำหนด TOR การเปรียบเทียบราคา การคัดเลือกผู้เสนอราคา ไปจนถึงการส่งมอบงาน เพื่อให้มั่นใจว่าเป็นไปอย่างโปร่งใสและคุ้มค่า เพิ่มประสิทธิภาพและความรวดเร็วในการวิเคราะห์ข้อมูลจำนวนมาก (Big Data Analysis): AI สามารถประมวลผลและวิเคราะห์ข้อมูลทางการเงิน เอกสาร และรายงานต่างๆ ของเทศบาลเมืองหนองปรือ ได้อย่างรวดเร็วและแม่นยำกว่ามนุษย์ ซึ่งจะช่วยให้ค้นพบความผิดปกติ รูปแบบ หรือแนวโน้มที่น่าสงสัยได้ง่ายขึ้น

๑๐. รูปภาพประกอบการฝึกอบรม