IPPF

International Professional Practices Framework

Supplemental Guidance

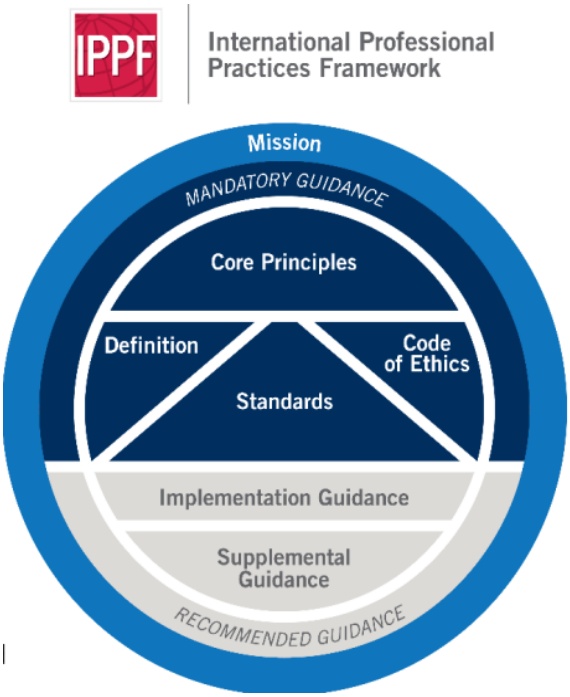
Practice Guide

การพัฒนาแผนการตรวจสอบภายในที่อาศัยความเสี่ยง

The Institute of Internal Auditors | Global

เกี่ยวกับ IPPF

กรอบโครงสร้างการปฏิบัติงานวิชาชีพสากล (IPPF®) คือ กรอบโครงสร้างการทำงานตามแนวคิดที่ IIA ได้ประกาศใช้เพื่อเป็นแนวทางปฏิบัติสำหรับวิชาชีพตรวจสอบภายในทั่วโลก



แนวทางภาคบังคับ (Mandatory Guidance) ถูกพัฒนาขึ้นตามกระบวนการการศึกษาอย่างละเอียดลึกซึ้ง ซึ่งได้มีการเปิดเผยต่อสาธารณะเพื่อที่ผู้มีส่วนได้เสียจะได้ให้ข้อมูลความคิดเห็นได้ องค์ประกอบภาคบังคับของ IPPF ประกอบไปด้วย

- หลักการพื้นฐานที่สำคัญ (Core principles) สำหรับการปฏิบัติงานวิชาชีพตรวจสอบภายใน
- คำจำกัดความ (Definition) ของการตรวจสอบภายใน
- ประมวลจรรยาบรรณ (Code of Ethics)
- มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน *(Standards)*

ในส่วนที่เป็น**แนวทางที่แนะนำ**จะประกอบไปด้วย แนวทางการนำมาตรฐานไปใช้ปฏิบัติ (Implementation Guidance) และ แนวทางเสริม (Supplemental Guidance) แนวทางการนำมาตรฐานไปใช้ปฏิบัติ ได้รับการออกแบบมาเพื่อช่วยให้ผู้ตรวจสอบภายในเข้าใจว่าจะนำเอาข้อกำหนดต่างๆ ในแนวทางภาคบังคับไปประยุกต์ใช้และปฏิบัติให้สอดคล้องกับข้อกำหนดเหล่านั้นได้อย่างไร

เกี่ยวกับแนวทางเสริม (Supplemental Guidance)

แนวทางเสริมจะให้ข้อมูลเพิ่มเติม คำแนะนำ และ วิธีปฏิบัติที่เป็นเลิศสำหรับการปฏิบัติงานให้บริการตรวจสอบภายใน เอกสารนี้จะช่วยสนับสนุนมาตรฐาน โดยได้ระบุประเด็นต่างๆ ตามหัวข้อ และประเด็นของแต่ละธุรกิจเฉพาะอย่าง โดยให้รายละเอียดมากกว่าแนวทางการนำมาตรฐานไปใช้ปฏิบัติ และ ได้รับการรับรองโดย IIA โดยผ่านการการทบทวนและกระบวนการอนุมัติอย่างเป็นทางการมาแล้ว

แนวปฏิบัติ (Practice Guides)

แนวปฏิบัติ เป็นรูปแบบหนึ่งของแนวทางเสริม ซึ่งจะให้วิถีทางโดยละเอียด กระบวนการแต่ละขั้นตอน พร้อมทั้งตัวอย่างที่จะช่วยสนับสนุนผู้ตรวจสอบภายในทุกคน บางแนวปฏิบัติจะเน้นไปที่:

- การให้บริการทางการเงิน
- ภาครัฐ
- เทคโนโลยีสารสนเทศ (GTAG®)

สำหรับภาพรวมข้อมูลเกี่ยวกับเอกสารของแนวปฏิบัติที่จัดทำโดย IIA โปรดดูได้ที่ www.globaliia.org/standards-guidance

สารบัญ

บทสรุปสำหรับผู้บริหาร

ในสภาพแวดล้อมทางธุรกิจในทุกวันนี้การตรวจสอบภายในที่มีประสิทธิผลจำเป็นต้องมีการวางแผนพร้อมทั้งมีการตอบสนองอย่างว่องไวต่อความเสี่ยงที่กำลังเปลี่ยนแปลงไปอย่างรวดเร็ว เพื่อที่จะเพิ่มคุณค่าและปรับปรุงประสิทธิผลขององค์กร ลำดับความสำคัญของตรวจสอบภายในจะต้องสอดคล้องกับวัตถุประสงค์ขององค์กร และควรระบุความเสี่ยงที่มีแนวโน้มสูงสุดที่จะส่งผลต่อความสามารถขององค์กรในการบรรลุวัตถุประสงค์เหล่านั้นได้

ข้อสังเกต: ภาคผนวก ก ได้ให้รายการแหล่งข้อมูลอื่นๆ ของ IIA ซึ่งเกี่ยวข้องกับแนวปฏิบัตินี้ คำที่เน้นตัวหนาได้มีคำอธิบายไว้ใน **ภาคผนวก ข**

การทำให้มั่นใจในความสอดคล้องนี้ เป็นแก่นแท้ของมาตรฐาน 2010 – การวางแผนมาตรฐาน 2010.A1 มาตรฐาน 2010.A2 และมาตรฐาน 2010.C1 ซึ่งเป็นงานของหัวหน้าหน่วยงานตรวจสอบภายใน (CAE) ที่มาพร้อมภาระหน้าที่ในการสร้างแผนงานที่ตรวจสอบภายในจะต้องปฏิบัติโดยอาศัยการประเมินความเสี่ยงเป็นพื้นฐานซึ่งการวางแผนนี้ต้องกระทำอย่างน้อยปีละครั้ง

แนวปฏิบัติฉบับนี้อธิบายถึงแนวทางที่เป็นระบบ ในการสร้างและคงไว้ซึ่งแผนการตรวจสอบภายในที่อาศัยความเสี่ยงเป็นพื้นฐาน CAE และผู้ตรวจสอบภายในที่ได้รับมอบหมายจะร่วมกันทำงานเพื่อ:

- เข้าใจในองค์กร
- ระบุ ประเมิน และจัดลำดับความสำคัญของความเสี่ยง
- ประสานงานกับผู้ให้บริการรายอื่นๆ
- ประมาณการทรัพยากร
- เสนอแผนและขอความคิดเห็นตอบกลับ
- สรุปและสื่อสารแผน
- ประเมินความเสี่ยงอย่างต่อเนื่อง
- ปรับปรุงแผนให้เป็นปัจจุบันและสื่อสารเกี่ยวกับการปรับปรุง

แนวปฏิบัติฉบับนี้ได้ให้แนวทางทั่วๆ ไปพอที่จะไปประยุกต์ใช้ในสถานการณ์ ความจำเป็น และความต้องการของแต่ละองค์กรได้ ในการประยุกต์ใช้แนวปฏิบัตินี้ ผู้ตรวจสอบภายในควรคำนึงถึงระดับวุฒิภาวะขององค์กรของตน โดยเฉพาะระดับการบูรณาการของการกำกับดูแลและการบริหารความเสี่ยง ผู้ตรวจสอบภายในอาจจำเป็นต้องดัดแปลงแนวปฏิบัตินี้ให้เข้ากับอุตสาหกรรมเฉพาะอย่างบางชนิด สถานที่ตั้งทางภูมิศาสตร์ และขอบเขตอำนาจทางการเมืองที่องค์กรของตนดำเนินงานอยู่

บทนำ

การวางแผนโดยอาศัยความเสี่ยงเป็นพื้นฐานอย่างครอบคลุมนั้น จะช่วยให้หน่วยงานตรวจสอบภายในสามารถจัดทิศทางและทุ่มเททรัพยากรที่มีอยู่อย่างจำกัดได้อย่างเหมาะสม เพื่อการให้บริการความเชื่อมั่นและให้คำปรึกษาเชิงรุกที่ลึกซึ้ง และมองอนาคตเป็นหลักในเรื่องที่องค์กรกำลังมีปัญหามากที่สุด และ CAE มีภาระหน้าที่ในการสร้างแผนสำหรับ**งานที่ได้รับมอบหมาย**ของตรวจสอบภายในโดยอาศัย**การประเมินความสี่ยง**เป็นพื้นฐาน ซึ่งต้องกระทำอย่างน้อยปีละครั้ง (มาตรฐาน 2010 – การวางแผน และมาตรฐาน 2010.A1)

ในขณะที่การประเมินความเสี่ยงปีละครั้งเป็นข้อกำหนดขั้นต่ำในมาตรฐาน แต่ความเสี่ยงในปัจจุบันที่เปลี่ยนแปลงไปอย่างรวดเร็วทำให้ผู้ตรวจสอบภายในต้องประเมินความเสี่ยงบ่อยๆ หรือแม้กระทั่งต้องประเมินอย่างต่อเนื่อง แผนการตรวจสอบโดยอาศัยความเสี่ยงเป็นพื้นฐานนั้น ควรแคล่วคล่องและว่องไว เพื่อบรรลุได้ถึงคุณสมบัติเหล่านั้น CAE บางท่าน จะปรับปรุงแผนเป็นรายไตรมาส (หรือเป็นตารางเวลาที่คล้ายคลึงกัน) และ CAE ท่านอื่นๆ ก็จะถือว่าแผนของตนมีลักษณะ “หมุนเวียน (rolling)” เมื่อมีการเปลี่ยนแปลงเพียงเล็กน้อยเกิดขึ้น

การสื่อสารถึงแผนที่อาศัยความเสี่ยง

เมื่อทำการวางแผนงานตรวจสอบภายใน CAE ควรคิดว่าจะบริหารผู้มีส่วนได้เสียอย่างไร แล้วสร้างแผนงานตรวจสอบภายในที่สร้างคุณค่าของผู้มีส่วนได้เสียได้มากที่สุด ข้อควรพิจารณาได้แก่:

- งานของตรวจสอบภายในประเภทใดที่จะให้ความเชื่อมั่นและคำปรึกษาแก่ผู้บริหารระดับสูงและ

ใครมีหน้าที่รับผิดชอบในแผนการตรวจสอบภายในที่อาศัยความเสี่ยงเป็นพื้นฐาน?

- ขณะที่ CAE มีหน้าที่รับผิดชอบในแผนงานตรวจสอบภายใน ผู้จัดการและผู้ตรวจสอบที่มีประสบการณ์อาจจะเป็นผู้กระทำกิจกรรมต่างๆ ในกระบวนการวางแผน แนวปฏิบัติฉบับนี้จะพูดถึงบทบาท และภาระหน้าที่ของ CAE ผู้จัดการตรวจสอบภายใน ผู้ตรวจสอบภายในโดยรวม อย่างไรก็ตาม ไม่มีแนวทางใดที่จะเหมาะสมไปได้กับทุกองค์กร และการจัดการย่อมแตกต่างกันไปในแต่ละองค์กร (เช่นอาจขึ้นอยู่กับขนาด และทรัพยากรที่หน่วยงานตรวจสอบภายในมีอยู่)
- *มาตรฐาน*ที่กล่าวถึงข้อกำหนดเกี่ยวกับการวางแผนงานที่ต้องปฏิบัติ โดยอาศัยความเสี่ยงของ CAE (มาตรฐานชุด 2000) และมาตรฐานที่เกี่ยวกับการวางแผนงานที่ได้รับมอบหมายแต่ละงาน (มาตรฐานชุด 2200) แนวปฏิบัติฉบับนี้จะกล่าวถึงเฉพาะการวางแผนงานตรวจสอบภายในโดยอาศัยความเสี่ยงเป็นพื้นฐานของ CAE เท่านั้น สำหรับแนวปฏิบัติเรื่อง “การวางแผนงานที่ได้รับมอบหมาย: การกำหนดวัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมาย” จะอธิบายถึงวิธีการวางแผนสำหรับงานที่ได้รับมอบหมายแต่ละงาน

คณะกรรมการได้อย่างเพียงพอว่า ความเสี่ยงที่สำคัญได้รับการบรรเทาอย่างมีประสิทธิผลแล้ว?

- หน่วยงานตรวจสอบภายในจะสื่อสารการประเมินความเสี่ยงและแผนงานตรวจสอบที่อาศัยความเสี่ยงเป็นพื้นฐานอย่างไร? วิธีการแสดงภาพให้เห็นได้ด้วยตาประเภทใดที่จะช่วยส่งเสริมการสื่อสารที่มีประสิทธิผลได้?
- ผู้บริหารระดับสูงและคณะกรรมการคาดหวังอะไรบ้างจากหน่วยงานตรวจสอบภายใน? CAE ควรหารือกับผู้บริหารระดับสูงและคณะกรรมการเป็นการล่วงหน้าว่าคาดหวังว่าควรรายงานถี่มากน้อยเพียงใด และเกณฑ์ที่ใช้ตัดสินว่าสมควรมีการรายงานและการอนุมัติการเปลี่ยนแปลงในแผนงานตรวจสอบ (ได้แก่ ความสำคัญและความรีบด่วนของประเด็นเหล่านั้น) ตามที่ได้บรรยายไว้ในมาตรฐาน 2060 – การรายงานต่อผู้บริหารระดับสูงและคณะกรรมการ นโยบายและวิธีการปฏิบัติงานควรกล่าวถึงเรื่องการรักษาความลับโดยให้เป็นไปตามประมวลจรรยาบรรณและ*มาตรฐาน* (มาตรฐาน 2040 – นโยบายและวิธีการปฏิบัติงาน และมาตรฐานชุดที่เริ่มจากมาตรฐาน 2330 – การจัดทำเอกสารข้อมูล และมาตรฐานชุดที่เริ่มจากมาตรฐาน 2440 – การเผยแพร่ผลการปฏิบัติงาน)

การเปลี่ยนแปลงแผน

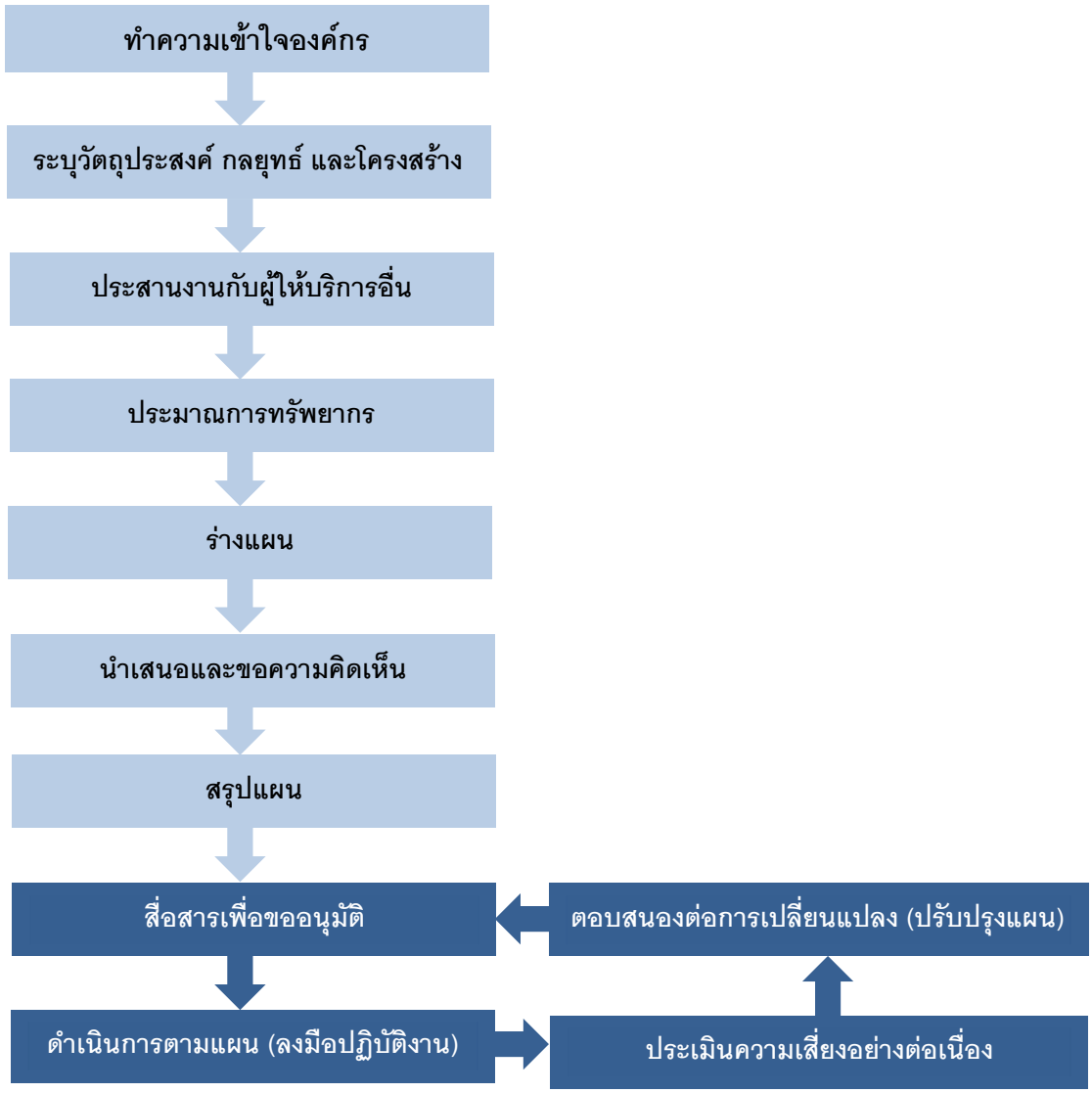
แนวปฏิบัติฉบับนี้อธิบายขั้นตอนที่นำไปสู่การสร้างแผนงานตรวจสอบภายในตั้งแต่แรกเริ่ม รวมทั้งข้อกำหนดสำหรับการอนุมัติแผนอย่างเป็นทางการ ซึ่งอาจเกิดขึ้นตามที่ได้กำหนดไว้ล่วงหน้า หรือตามช่วงตารางเวลา นอกจากนี้ หน่วยงานตรวจสอบภายในจะต้องตอบสนองต่อการเปลี่ยนแปลงต่างๆ ทั้งภายในและภายนอกที่ส่งผลกระทบต่อวัตถุประสงค์ขององค์กรและลำดับความสำคัญของความเสี่ยง องค์กรต่างๆ และสภาพการณ์ภายนอกกำลังมีการเปลี่ยนแปลงอยู่อย่างต่อเนื่อง และข้อมูลความเสี่ยงใหม่ๆ หรือรายละเอียดเกี่ยวกับความเสี่ยงที่มากขึ้นอาจเกิดขึ้นได้ในระหว่างการปฏิบัติงานที่ได้รับมอบหมายใดก็ได้ ผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกอาจค้นพบข้อมูลใหม่ๆ ในระหว่างการปฏิบัติงาน ซึ่งจะทำให้เกิดการเปลี่ยนแปลงการประเมินความเสี่ยงอย่างครอบคลุมของตรวจสอบภายในและแผนงานตรวจสอบภายในได้ทันทีทันใด

การเปลี่ยนแปลงดังกล่าวจะชี้ให้เห็นชัดถึงความจำเป็นที่ต้องมีการประเมินความเสี่ยงอย่างต่อเนื่อง การประเมินการจัดลำดับความสำคัญของความเสี่ยงซ้ำอีก และปรับแผนงานเพื่อรองรับลำดับความสำคัญเร่งด่วนอันใหม่ มาตรฐาน 2010 – การวางแผน ได้แนะนำให้ CAE ต้องทบทวนและปรับปรุงแผนเพื่อตอบสนองต่อการเปลี่ยนแปลงทางธุรกิจ ความเสี่ยง การปฏิบัติงาน โครงการ ระบบ และวิธีการควบคุมต่างๆ ขององค์กร ในช่วงหลังๆ ของแนวปฏิบัติฉบับนี้ได้ให้รายละเอียดเพิ่มเติมว่า CAE ควรจะบริหารการเปลี่ยนแปลงในแผนอย่างไร

ภาพรวมของการพัฒนาแผนงานตรวจสอบ

กระบวนการจัดให้มีแผนงานการตรวจสอบภายในโดยทั่วไปจะประกอบด้วยระยะต่างๆ ดังภาพที่ตามมา อย่างไรก็ตาม ผู้อ่านควรจะตีความแนวคิดเกี่ยวกับระยะต่างๆ นั้นโดยไม่ต้องเคร่งครัดมากเกินไป เนื่องจากรายละเอียดต่างๆ ของการวางแผนจะแตกต่างกันไปตามแต่ละหน่วยงานตรวจสอบภายในและองค์กร ผู้ตรวจสอบภายในจำนวนมากอาจทำงานไปพร้อมๆ กันเพื่อจัดทำแผนงานการตรวจสอบภายใน ซึ่งรวมถึงการประเมินความเสี่ยงที่ใช้สนับสนุนด้วย ดังนั้น ระยะบางระยะอาจจะทับซ้อนกันได้เป็นบางครั้ง CAE หลายๆ ท่านมักจะบันทึกแนวทางที่ตนชอบไว้ในนโยบายและวิธีปฏิบัติงานของหน่วยงานตรวจสอบภายใน (มาตรฐาน 2040) แนวปฏิบัติฉบับนี้ได้แยกแยะระยะต่างๆ ของการวางแผนตามที่แสดงไว้ในภาพที่ 1 ผู้ตรวจสอบภายในควรมองภาพวงจรของการจัดทำแผนทั้งหมดว่าเป็นความพยายามที่ครอบคลุมที่ตอบสนองต่อการเปลี่ยนแปลงในทางองค์กรต่างๆ

ภาพที่ 1: วงจรการพัฒนาแผนงานตรวจสอบภายใน



การทำความเข้าใจองค์กร

การระบุวัตถุประสงค์ กลยุทธ์ และโครงสร้าง

การทำความเข้าใจในกระบวนการบริหารความเสี่ยงขององค์กรจำเป็นต้องมีการระบุว่าบทบาทและภาระหน้าที่ของการบริหารความเสี่ยงกับการกำกับดูแลมีการประสานงานกันอย่างไร โดยมากการประสานงานนี้มักเกี่ยวข้องกับ:

- การนำระบบการควบคุมภายในไปใช้ปฏิบัติโดยผู้บริหารด้านการปฏิบัติงานและสายงาน
- การให้ความมั่นใจว่าระบบการบริหารความเสี่ยงและการควบคุมได้ถูกออกแบบมาอย่างมีประสิทธิผลและทำงานได้ตามที่ออกแบบมา หน่วยงานที่ทำหน้าที่บริหารความเสี่ยง **การกำกับดูแลให้ปฏิบัติตามกฎ** หน่วยงานควบคุมคุณภาพ และหน่วยงานอื่นที่คล้ายคลึงกันที่ให้ความเชื่อมั่นเช่นกัน
- การให้ความเชื่อมั่นและให้คำปรึกษาอย่างเป็นอิสระเกี่ยวกับกระบวนการการกำกับดูแล การบริหารความเสี่ยง และการควบคุมโดยหน่วยงานตรวจสอบภายใน

การสอบทานเอกสารหลัก

ก่อนจะเริ่มการประเมินความเสี่ยง CAE อาจสอบทานเอกสารหลักๆ เป็นต้นว่า ผังองค์กรและแผนกลยุทธ์ CAE อาจสอบทานเอกสารเหล่านี้ เพื่อทำความเข้าใจอย่างลึกซึ้งเกี่ยวกับกระบวนการทางธุรกิจและความเสี่ยงที่อาจเกิดขึ้นรวมทั้งจุดควบคุมต่างๆ ขององค์กร ถ้าฝ่ายบริหารได้นำเครื่องมืออัตโนมัติในการเฝ้าระวังความเสี่ยงอย่างต่อเนื่องมาใช้ ดังนั้นแล้ว ผู้ตรวจสอบภายในอาจจะรวบรวมข้อมูลจากรายงานความเสี่ยงที่ผลิตออกมาอย่างอัตโนมัติได้ ข้อมูลเพิ่มเติมอาจได้มาจากการประเมินครั้งก่อนๆ และรายงานที่ผลิตโดยผู้ตรวจสอบภายในและผู้สอบบัญชี เอกสารที่คล้ายคลึงกันสำหรับแต่ละ**หน่วยที่สามารถรับการตรวจสอบได้ / หน่วยรับตรวจ** (auditable units) อาจมีรายละเอียดเกี่ยวกับกระบวนการปฏิบัติงานและหน่วยงานบริการที่ทำหน้าที่เป็นหน่วยสนับสนุนกระบวนการเหล่านั้น ภาพที่ 2 ได้แสดงรายการตัวอย่างของข้อมูลและเอกสารที่ผู้ตรวจสอบภายในอาจจะต้องรวบรวมมา

ภาพที่ 2 แหล่งเอกสารสำหรับการรวบรวมข้อมูล

ข้อมูลที่ต้องรวบรวม	แหล่งที่มาของเอกสารที่อาจเป็นไปได้
▪ บทบาทในการควบคุมและการให้ความเชื่อมั่นใดที่กำลังทำหน้าที่อยู่ในองค์กร (ซึ่งก็คือ แนวป้องกันด่านที่หนึ่งและที่สอง)? ▪ ภาระหน้าที่ของแต่ละบทบาทคืออะไร? ▪ องค์กรได้นำกรอบการบริหารความเสี่ยงแบบทั่วทั้งองค์กร (ERM) มาใช้หรือยัง?	▪ ผังองค์กร ▪ รายงานการประชุมกับผู้บริหารระดับสูง ผู้บริหารในแนวป้องกันด่านที่สอง และคณะอนุกรรมการบริหารความเสี่ยง
▪ วัตถุประสงค์หลักขององค์กรคืออะไร? ▪ มีการเสนอโครงการใหม่ๆ หรือการเปลี่ยนแปลงใหญ่ๆ ในเวลาที่จะมาถึงอันใกล้หรือไม่?	▪ แผนกลยุทธ์ขององค์กร ▪ แผนกลยุทธ์สำหรับบริเวณที่มีความสำคัญยิ่งแต่ละที่ และโครงการใหม่ๆ ที่สำคัญ ▪ รายงานการประชุมของผู้บริหารระดับสูงและของคณะกรรมการ
▪ กระบวนการทางธุรกิจหลักขององค์กรคืออะไร? ▪ ในแต่ละกระบวนการนั้นมีความเสี่ยงที่อาจเกิดขึ้นได้และวิธีการควบคุมอะไรบ้าง? ▪ กลยุทธ์ วัตถุประสงค์และแผนเป็นจริงได้หรือไม่? ▪ มีการระบุความเสี่ยงที่เกี่ยวข้องได้ทั้งหมดแล้วหรือไม่?	▪ รายงานประจำปี (Annual reports) และรายงานที่จะต้องยื่นต่อสาธารณะ / ทางการ ▪ ทะเบียนรายการความเสี่ยงทั้งหมด (หรือที่เรียกกันว่า risk universe)[1] ▪ ทะเบียนรายการความเสี่ยงของฝ่ายบริหาร (หรือที่เรียกว่า คลังความเสี่ยง - risk inventories) และการประเมินความเสี่ยง ซึ่งรวมถึง การประเมินการควบคุมโดยตนเอง (control self-assessments) ซึ่งกระทำโดยหัวหน้าหน่วยธุรกิจแต่ละหน่วย (การประเมินความเสี่ยงด้านการดำเนินงาน) ▪ ผลจากการเฝ้าระวังความเสี่ยงโดยอัตโนมัติ หากได้มีการนำระบบอัตโนมัติมาใช้ ▪ การประเมินและรายงานครั้งก่อนๆ จากผู้ให้บริการการให้ความเชื่อมั่นหลายๆ ราย (หน่วยงานในแนวป้องกันด่านที่สอง ผู้ตรวจสอบภายใน และผู้สอบบัญชี) ▪ เอกสารที่แสดงรายละเอียดในการปฏิบัติงาน (เช่น แผนผังของกระบวนการ)

1. Rick A. Wright, Jr., หนังสือ *The Internal Auditor's Guide to Risk Assessment,* พิมพ์ครั้งที่ 2. (Lake Mary, FL: Internal Audit Foundation, 2018), หน้า 51.

การปรึกษากับผู้มีส่วนได้เสียหลัก

CAE จะต้องปรึกษาหารือกับผู้มีส่วนได้เสียหลัก เพื่อที่จะบรรลุข้อกำหนดในมาตรฐาน ตามมาตรฐาน 2010 – การวางแผน การสื่อสารอย่างต่อเนื่องเป็นสิ่งสำคัญยิ่ง ที่จะช่วยในการปรับปรุงแผนได้อย่างว่องไว เมื่อมีการเปลี่ยนแปลง นอกจากนี้แล้ว การสื่อสารอย่างต่อเนื่องจะช่วยให้มั่นใจได้ว่าผู้บริหารระดับสูง คณะกรรมการ และหน่วยงานตรวจสอบภายในมีความเข้าใจที่ตรงกันเกี่ยวกับความเสี่ยง และลำดับความสำคัญในการให้ความเชื่อมั่นขององค์กร

การพบปะกับคณะกรรมการและคณะกรรมการกำกับดูแล

CAE ควรเข้าร่วมประชุมกับคณะกรรมการและคณะกรรมการกำกับดูแลหลัก (เช่น คณะกรรมการตรวจสอบ คณะอนุกรรมการความเสี่ยง) และอาจเข้าพบกับแต่ละท่านอย่างเป็นอิสระได้ การเข้าร่วมประชุมดังกล่าวจะช่วยให้ CAE ได้รับทราบเกี่ยวกับพัฒนาการล่าสุดที่เกิดขึ้นในองค์กรและจะได้ตื่นตัวกับความเสี่ยงที่อาจเกิดขึ้นซึ่งสามารถเป็นผลจากการเปลี่ยนแปลงต่างๆ ได้

การพบปะกับผู้บริหาร

นอกจากจะต้องพบปะกับคณะกรรมการแล้ว CAE (หรือผู้ตรวจสอบภายในที่ได้รับมอบหมาย) ควรเข้าร่วมประชุมที่จัดเป็นประจำ (ทางโทรศัพท์ เว็บ หรือตัวเป็นๆ) กับผู้บริหารระดับสูงและ/หรือผู้ที่รายงานตรงต่อผู้บริหารระดับสูง (อันได้แก่ ผู้ที่ทำหน้าที่เป็นด่านที่สอง เช่น หน่วยงานกำกับดูแล บริหารความเสี่ยง และควบคุมคุณภาพ) CAE ควรได้พูดคุยกับผู้บริหารระดับสูงแต่ละท่านอย่างเป็นอิสระ

การปรึกษากับผู้มีส่วนได้เสียหลัก

ผู้มีส่วนได้เสียที่ควรพิจารณา

- คณะกรรมการ: คณะกรรมการตรวจสอบ คณะกรรมการกำกับดูแล สมาชิกในคณะกรรมการแต่ละท่าน
- ผู้บริหารระดับสูง หัวหน้าผู้บริหารงานความเสี่ยง (chief risk officer)
- หน่วยงานที่อยู่ในแนวป้องกันด่านที่สอง (Second line functions)
- ผู้บริหารด้านปฏิบัติการ / สายงาน
- ทรัพยากรบุคคล
- การตลาด
- พนักงานที่ทำงานปฏิบัติการที่เป็นงานสำคัญ
- ผู้สอบบัญชี / ผู้ตรวจสอบจากทางการ ตามที่ระบุไว้ (เฉพาะในแต่ละภาคอุตสาหกรรม)

วิธีการสื่อสาร

- การประชุมแบบประจันหน้า
- การประชุมทางโทรศัพท์ / ออนไลน์
- การทำสำรวจ
- การสัมภาษณ์
- การระดมสมองกลุ่ม การฝึกปฏิบัติ
- การสื่อสารที่ไม่เป็นทางการอย่างต่อเนื่อง

ในบางอุตสาหกรรมหรือบางภาคส่วนที่มีการควบคุมจากทางการโดยเข้มงวด CAE อาจจะต้องพบกับผู้สอบบัญชีและ/หรือเจ้าหน้าที่จากทางการด้วย

เพื่อให้เข้าใจในกระบวนการทางธุรกิจและความท้าทายต่างๆ ในการที่จะบรรลุเป้าหมายที่สำคัญทางธุรกิจได้ดียิ่งขึ้น ผู้ตรวจสอบภายในอาจจะพบปะกับผู้ปฏิบัติงานหลัก ๆ หรือผู้บริหารสายงาน เป็นต้นว่า รองประธานบริหาร และผู้อำนวยการในแต่ละหน่วยธุรกิจรวมทั้งพนักงานที่ทำงานด้านปฏิบัติการด้วย

การสื่อสารแบบไม่เป็นทางการ

ข้อมูลที่ได้มาอย่างไม่เป็นทางการอาจจะเติมเต็มความเข้าใจในองค์กรของผู้ตรวจสอบภายในได้ สามารถให้รายละเอียดที่เป็นจริงซึ่งไม่มีการเปิดเผยอย่างเป็นทางการ ความสัมพันธ์มักจะดีขึ้นได้เมื่อผู้ตรวจสอบภายในได้รับมอบหมายให้ไปปฏิบัติงานเฉพาะในบางสายธุรกิจ หน้าที่งาน หรือสถานที่ตั้ง และ/หรือบางนิติบุคคล การมีปฏิสัมพันธ์กับผู้บริหารและทีมงานตลอดทั่วทั้งหน่วยธุรกิจและหน้าที่งานต่างๆ ซึ่งรวมถึงฝ่ายงานเช่น ฝ่ายทรัพยากรบุคคลและฝ่ายการตลาดจะช่วยให้หน่วยงานตรวจสอบภายในปะติดปะต่อภาพรวมที่ครอบคลุมแผนองค์กรและสภาพแวดล้อมการควบคุมขององค์กรได้

มักจะเกิดได้บ่อยๆ ที่การสื่อสารอย่างไม่เป็นทางการจะสร้างความไว้วางใจ เพิ่มความเป็นไปได้ที่พนักงานจะหยิบยกความกังวลต่างๆ มาพูดกับผู้ตรวจสอบภายในตรงๆ ซึ่งอาจจะไม่ได้มีการกล่าวถึงในการประชุมที่เป็นทางการ การเปิดใจเช่นนั้นจะทำให้ความสามารถในการประเมินสภาพแวดล้อมการควบคุมของตรวจสอบภายในดีขึ้นได้ การหมุนเวียนผู้ตรวจสอบภายในสำหรับงานตรวจสอบภายในดังกล่าวจะถ่วงดุลระหว่างประโยชน์ของการสื่อสารอย่างไม่เป็นทางการกับความจำเป็นที่ต้องปกป้องความเป็นอิสระและความเที่ยงธรรมของผู้ตรวจสอบภายใน (มาตรฐาน 1130 – การเสื่อมเสียความเป็นอิสระหรือความเที่ยงธรรม)

การสำรวจ การสัมภาษณ์ การระดมสมอง การวิจัย

เครื่องมืออื่นๆ สำหรับการหาข้อมูล ได้แก่ การสำรวจ การสัมภาษณ์ และการฝึกปฏิบัติการเป็นกลุ่ม (เช่น การระดมสมอง และการสนทนากลุ่ม) เครื่องมือเหล่านี้มีประโยชน์โดยเฉพาะสำหรับการระบุความเสี่ยงเกิดใหม่ และความเสี่ยงของการเกิดการทุจริต)

CAE และสมาชิกในหน่วยงานตรวจสอบภายในอาจจะเพิ่มความตระหนักรู้เกี่ยวกับความเสี่ยงเกิดใหม่ที่เป็นไปได้ ด้วยการทำวิจัยข่าวสารในแวดวงอุตสาหกรรม แนวโน้ม การเปลี่ยนแปลงในข้อกำหนดจากทางการ การร่วมเครือข่ายกับผู้เชี่ยวชาญด้านอื่นๆ และการแสวงหาความรู้ที่เกี่ยวข้องเพิ่มเติมอย่างต่อเนื่อง

คำถามที่ควรพิจารณาได้แก่:

- วัตถุประสงค์สูงสุด 10 ข้อขององค์กรเชื่อมโยงกับวัตถุประสงค์หลักของฝ่ายอย่างไร?
- กลยุทธ์อะไรที่ถูกนำมาใช้เพื่อให้บรรลุวัตถุประสงค์เหล่านั้น?
- ความเสี่ยงใด หากเกิดขึ้นสามารถเข้ามาแทรกแซงความสามารถขององค์กรในการบรรลุวัตถุประสงค์เหล่านั้นได้?

แหล่งของข้อมูลความเสี่ยงเกิดใหม่

- การเปลี่ยนแปลงในลำดับความสำคัญของฝ่ายบริหาร กระบวนการทางธุรกิจ เทคโนโลยี (ไอที) และการปฏิบัติงานต่างๆ
- ระบบจริยธรรม / การแจ้งเบาะแสเกี่ยวกับความเสี่ยงของการทุจริต
- พัฒนาการของภูมิรัฐศาสตร์ (Geopolitical)
- การเปลี่ยนแปลงในทางกฎหมายข้อกำหนดจากทางการ
- คำขอจากผู้บริหารระดับสูง และคณะกรรมการ
- โครงการใหม่ๆ และการเปลี่ยนแปลงโปรแกรม
- การประเมินความเสี่ยงจากฝ่ายบริหารและหน่วยงานตรวจสอบภายใน (ซึ่งรวมถึง การทุจริต ไอที และวิธีการควบคุมทางการเงิน)

การสร้างหรือแก้ไขหัวข้อการตรวจสอบทั้งหมด (Audit Universe)

เมื่อได้ระบุกลยุทธ์และวัตถุประสงค์หลักแล้ว CAE อาจจะต้องการสร้างหรือทบทวน audit universe ซึ่งเป็นรายการหรือแค็ตตาล็อกของหน่วยงานในองค์กรที่สามารถรับการตรวจได้ (auditable units) หน่วยงานในองค์กรที่สามารถรับการตรวจได้นั้นเป็นได้ตั้งแต่ “หัวข้อ ประเด็น กรณี โครงการ ฝ่ายงาน กระบวนการ กิจการ หน้าที่งาน หรือบริเวณซึ่งมีความเสี่ยงอยู่และอาจสมควรที่จะให้มีการตรวจสอบ”

สำหรับ audit universe นั้นจะช่วยลดความยุ่งยากในการระบุและประเมินความเสี่ยงทั่วทั้งองค์กร มันคือขั้นตอนไปสู่การค้นพบว่า หน่วยรับตรวจใดที่มีระดับความเสี่ยงที่สมควรได้รับการสอบทานต่อไป ในการปฏิบัติงานตรวจสอบ **ภาคผนวก ค** ได้ให้ตัวอย่างของกระดาษทำการที่ใช้เชื่อมโยงวัตถุประสงค์และกลยุทธ์กับประเภทต่างๆ ใน audit universe

ถ้าหากไม่มี audit universe อยู่ ผู้ตรวจสอบภายในจะเริ่มจากการทำความเข้าใจว่า องค์กรมองและจัดประเภทกิจกรรม ความเสี่ยงและวิธีการควบคุมอย่างไร และองค์กรได้รับความเชื่อมั่นในการบริหารความเสี่ยงและกระบวนการควบคุมอย่างไร ซึ่งในขั้นนี้จะรวมถึงการพิจารณากรอบโครงสร้างที่ใช้โดยองค์กร การใช้โครงสร้างที่สอดคล้องกับแนวทางของฝ่ายบริหารมากที่สุดจะช่วยให้เพิ่มการทำงานร่วมกันระหว่างหน่วยงานตรวจสอบภายในและผู้ให้บริการความเชื่อมั่นและ**บริการให้คำปรึกษา**รายอื่นได้มากที่สุด โดยเฉพาะหากว่าองค์กรได้นำเอา

มั่นใจได้ในความครบถ้วนสมบูรณ์ของ Audit Universe

เพื่อให้มั่นใจได้ในความครบถ้วนสมบูรณ์ของ audit universe CAE ควรพิจารณาแหล่งข้อมูลความเสี่ยงต่อไปนี้:

- กลยุทธ์ขององค์กร และห่วงโซ่ของการสร้างคุณค่า (chain of value)
- บริเวณ หน่วยงาน ฝ่ายงาน และโครงการหลัก รวมทั้งกลยุทธ์ วัตถุประสงค์ และกระบวนการ ของหน่วยงานเหล่านั้น (ที่ระดับสูง จากแผนผังองค์กร ฝ่ายกฎหมาย และ/หรือกรอบโครงสร้างการบริหารความเสี่ยงทั่วทั้งองค์กร – ERM)
- ผู้ขายที่เป็นบุคคลที่สาม (จากหน่วยงานกฎหมาย จัดซื้อ หรือหน่วยงานที่ทำหน้าที่บริหารสัญญา)
- กระบวนการ และกระบวนการย่อยของหน่วยงานหลักทั้งหมด (จากกิจกรรมการทำแผนผังกระบวนการ เช่นที่กำหนดไว้โดย ISO)
- แอพพลิเคชันหลักๆ และสินทรัพย์ระบบข้อมูล ซึ่งรวมถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลที่มีอยู่ในสินทรัพย์เหล่านั้น (จากฝ่ายบริหารด้านไอที)
- ข้อกำหนดในทางกฎหมายและจากทางการซึ่งใช้บังคับองค์กร
- ตัวชี้วัดผลการดำเนินงานที่ไม่ใช่ตัวชี้วัดทางการเงิน (เช่น สิ่งแวดล้อม สุขภาพ และความปลอดภัย สังคม และการกำกับดูแล)

กระบวนการบริหารความเสี่ยงแบบทั่วทั้งองค์กรไปใช้ปฏิบัติแล้ว audit universe ที่จัดโครงสร้างมาเป็นอย่างดี จะทำให้การประเมินความเสี่ยงของตรวจสอบภายใน และแผนงานการตรวจสอบมีประโยชน์และมีคุณค่าต่อองค์กรมากยิ่งขึ้น

การทำให้มั่นใจได้ว่า audit universe จะจับภาพความเสี่ยงได้ทั้งหมดเป็นเรื่องท้าทาย เนื่องจากความเสี่ยงบางตัวจะมีอยู่ในช่วงรอยต่อระหว่างหน่วยงานต่างๆ ในองค์กร หรือระหว่างองค์กรกับสิ่งแวดล้อมภายนอก การมอง audit universe โดยแยกตามกระบวนการมักจะช่วยเผยให้เห็นความเสี่ยงเหล่านั้นได้ ในแถบด้านข้างภายใต้หัวข้อ “มั่นใจได้ในความครบถ้วนสมบูรณ์ของ Audit Universe” ได้ให้รายการแหล่งที่มาของข้อมูลความเสี่ยงที่ CAE ทั้งหลายควรพิจารณา

CAE ควรหารือกับผู้บริหารระดับสูงเพื่อที่จะมั่นใจได้ว่า audit universe จะสะท้อนโมเดลทางธุรกิจขององค์กรได้อย่างถูกต้อง เมื่อได้สร้าง audit universe ขึ้นแล้วมันก็อาจจะถูกหยิบยกไปใช้ในโอกาสหน้าได้ อย่างไรก็ตาม หัวข้อเหล่านั้นควรจะต้องได้รับการปรับปรุงบ่อยๆ เพื่อที่จะได้รวมเอาการเปลี่ยนแปลงต่างๆ ทั้งภายในและภายนอกเข้าไปด้วย ซึ่งการเปลี่ยนแปลงเหล่านั้นอาจนำมาซึ่งความเสี่ยงใหม่ๆ เมื่อใดก็ได้ audit universe จะช่วยให้จัดระเบียบบริเวณที่สมควรได้รับการตรวจ (auditable areas) สำหรับการประเมินความเสี่ยงและขอบเขตในการให้ความเชื่อมั่นได้อย่างครอบคลุม

การประเมินความเสี่ยงของตรวจสอบภายใน

การทำความเข้าใจนัยสำคัญของการประเมินที่เป็นอิสระ

การประเมินความเสี่ยงทั่วทั้งองค์กรจะช่วยให้ CAE สามารถเพ่งความสนใจไปที่ความเสี่ยงที่ได้ถูกจัดอันดับไว้ในระดับที่มีนัยสำคัญสูงสุดเหล่านั้นได้ และเพื่อที่จะได้ระบุงานตรวจสอบซึ่งบริหารจัดการได้ในเวลาอันควร และเป็นงานตรวจสอบที่เพิ่มคุณค่าซึ่งสะท้อนให้เห็นถึงลำดับความสำคัญขององค์กรได้ สิ่งนี้มักจะปรากฏออกมาในแผนที่ระบุหน่วยงานในองค์กรที่สามารถรับการตรวจได้ (auditable units) ได้ออกมาโดยเฉลี่ยประมาณ 15 งาน

องค์กรที่ได้นำเอา ERM ไปใช้ปฏิบัติแล้ว อาจสร้างทะเบียนความเสี่ยงที่ครอบคลุม (ซึ่งเป็นที่รู้จักกันว่าเป็นรายการคลังความเสี่ยงหรือความเสี่ยงทั้งหมด – risk inventory / risk universe) ผู้ตรวจสอบภายในอาจใช้ข้อมูลของผู้บริหารโดยถือว่าเป็นข้อมูลส่วนหนึ่งในการทำการประเมินความเสี่ยงทั่วทั้งองค์กรของตรวจสอบภายในก็ได้ อย่างไรก็ตาม เพื่อให้สอดคล้องกับหลักการในประมวลจรรยาบรรณเรื่องความเที่ยงธรรม และมาตรฐาน 1100 – ความเป็นอิสระและความเที่ยงธรรม ผู้ตรวจสอบภายในควรปฏิบัติงานใน

ส่วนของตนเพื่อยืนยันว่า ได้มีการบันทึกความเสี่ยงหลักทั้งหมดไว้แล้ว และความมีนัยสำคัญของความเสี่ยงที่เกี่ยวเนื่องได้ถูกสะท้อนให้เห็นอย่างถูกต้องแล้ว

การทำความเข้าใจในวัตถุประสงค์ทางธุรกิจ กลยุทธ์ และความเสี่ยง

ความเสี่ยงที่เกี่ยวกับวัตถุประสงค์ทางธุรกิจ

เพื่อที่จะระบุความเสี่ยงที่ร้ายแรงหรือความเสี่ยงหลัก หน่วยงานตรวจสอบภายในควรระบุและทำความเข้าใจมิใช่เพียงแค่วัตถุประสงค์หรือกลยุทธ์ที่อยู่ในระดับสูงเท่านั้น แต่ควรรวมถึงวัตถุประสงค์ทางธุรกิจเฉพาะอย่างและกลยุทธ์ที่ใช้เพื่อให้บรรลุวัตถุประสงค์เหล่านั้น องค์กรบางแห่งอาจจัดประเภทวัตถุประสงค์ทางธุรกิจเป็นดังนี้ วัตถุประสงค์เชิงกลยุทธ์ วัตถุประสงค์ตามหน้าที่งาน หรือวัตถุประสงค์ที่ระดับกระบวนการ[2] ความเสี่ยง แต่บางแห่งอาจใช้ประเภทตามที่มีระบุในกรอบโครงสร้างการควบคุมฉบับ Committee of Sponsoring Organizations (COSO) Internal Control — Integrated Framework คือ: วัตถุประสงค์ด้านการปฏิบัติงาน การรายงาน และการปฏิบัติตามกฎระเบียบ

การใช้ประโยชน์จากโอกาส

กรอบการบริหารความเสี่ยงและการกำกับดูแลในยุคสมัยนี้จะเน้นถึงความสำคัญของการใช้ประโยชน์จากโอกาส เพื่อความมั่นใจในเรื่องนวัตกรรม การเจริญเติบโต ความมั่นคงทางการเงิน (financial viability)

กรอบโครงสร้างฉบับ COSO's ERM ได้นิยามคำว่า โอกาส ไว้ว่า "การกระทำหรือ การกระทำที่เป็นไปได้ ที่สร้างหรือเปลี่ยนแปลงเป้าหมายหรือแนวทางในการสร้าง รักษาไว้ และการตระหนักถึงคุณค่า"

ความเสี่ยงรวมถึงโอกาส

ผู้ตรวจสอบภายในควรคำนึงถึงธรรมชาติของความเสี่ยงในหลายๆ แง่มุม เมื่อทำการตัดสินใจว่าจะระบุและประเมินความเสี่ยงเหล่านั้นอย่างไร เนื่องจากแต่ละองค์กรย่อมมีกลยุทธ์และวัตถุประสงค์ทางธุรกิจที่ต่างกัน ไม่มีแบบเช็คสอบความเสี่ยง (risk checklist) ใดเพียงแบบเดียวที่จะใช้ได้กับทุกองค์กร รายการคลังความเสี่ยงแตกต่างกันไปในแต่ละองค์กรและสามารถเปลี่ยนแปลงได้เมื่อเวลาเปลี่ยนไป

2. Wright, หนังสือ*The Internal Auditor's Guide*, หน้า 60.

ยิ่งไปกว่านั้น ผู้ตรวจสอบภายในควรคำนึงว่า “ความเสี่ยงจะแสดงให้เห็นถึง อุปสรรคขวากหนามในการประสบความสำเร็จ เช่นเดียวกับโอกาส ซึ่งอาจช่วยให้บรรลุวัตถุประสงค์เหล่านั้นได้”[3] โดยแท้จริงแล้ว “ความเสี่ยงอาจเกี่ยวข้องกับการป้องกันสิ่งชั่วร้ายไม่ให้เกิดขึ้น (การบรรเทาความเสี่ยง) หรือ การที่ไม่สามารถทำให้เชื่อมั่นได้ว่าสิ่งดีๆ จะเกิดขึ้น (ซึ่งก็คือ การใช้ประโยชน์ หรือแสวงหาโอกาส)”

การจัดทำเอกสารความเสี่ยง

ประเภทความเสี่ยง

แต่ละหน่วยธุรกิจหรือแต่ละหน้าที่งานในองค์กรอาจมีวิธีการมองและวัดวัตถุประสงค์ทางธุรกิจ กระบวนการ และความเสี่ยงที่แตกต่างกัน การจัดประเภทความเสี่ยงจะนำมาซึ่งความน่าเชื่อถือ และความสม่ำเสมอไปทั่วองค์กร เมื่อทำการระบุ สื่อสาร รวมทั้งการวิเคราะห์ เกี่ยวกับความเสี่ยงและกระบวนการบริหารความเสี่ยง

กรอบบางกรอบ แนวทางและอุตสาหกรรมเฉพาะอย่างอาจแนะนำหรือกำหนดให้ใช้การแบ่งประเภทบางอย่าง ถ้าองค์กรใช้กรอบการบริหารความเสี่ยงใด หน่วยงานตรวจสอบภายในก็ควรจัดประเภทให้สอดคล้องกับประเภทต่างๆ ในกรอบนั้น หากไม่มีกรอบหรือการจัดประเภทความเสี่ยงอยู่ ผู้ตรวจสอบภายในสามารถหารือระดมสมองกับฝ่ายบริหารเกี่ยวกับความเสี่ยงที่เกี่ยวข้องกับองค์กรโดยเริ่มจากการจัดหมวดหมู่ของประเภทความเสี่ยงต่างๆ ซึ่งเป็นที่รู้จักกันดีในองค์กรส่วนใหญ่ เป็นต้นว่า ความเสี่ยงด้านกลยุทธ์ ความเสี่ยงด้านการปฏิบัติงาน ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ และความเสี่ยงด้านการเงิน[4]

ความเสี่ยงภายใน ความเสี่ยงภายนอก และความเสี่ยงทางกลยุทธ์

ในแต่ละประเภทกว้างๆ ของความเสี่ยง ผู้ตรวจสอบภายในควรพิจารณาแหล่งที่มาของความเสี่ยงทั้งภายในและภายนอก ซึ่งสามารถก่อให้เกิดรายการที่ยาวมากได้ ผู้ตรวจสอบภายในจะประเมินความเสี่ยงเพื่อทำให้รายการนั้นแคบลง และจัดลำดับความสำคัญความเสี่ยงที่ควรรวมอยู่ในการวางแผนงานของตรวจสอบภายใน สำหรับความเสี่ยงด้านกลยุทธ์ หากว่าผู้บริหารไม่บริหารจัดการให้ดีพอ จะมีแนวโน้มสูงสุดที่จะส่งผลกระทบต่อความสามารถขององค์กรในการบรรลุเป้าหมายได้[5]

---

3. Urton L. Anderson และอื่นๆ. หนังสือ *Internal Auditing: Assurance and Advisory Services*, พิมพ์ครั้งที่ 4. (Lake Mary, FL: Internal Audit Foundation, 2017), หน้า 4-3.

4. Wright, หนังสือ *The Internal Auditor's Guide*, หน้า 13.

5. Wright, หนังสือ *The Internal Auditor's Guide*, หน้า 21.

ความเสี่ยงด้านไอที

แผนงานการตรวจสอบที่ครอบคลุมจะรวมถึงไอทีด้วย ซึ่งหมายความว่า ความเสี่ยงด้านไอทีจะต้องถูกรวมอยู่ในการประเมินความเสี่ยงทั้งหมด ความเสี่ยงด้านไอทีอาจจะจัดแบ่งเป็นประเภทย่อย ซึ่งได้แก่ โครงสร้างพื้นฐาน การปฏิบัติงาน และแอพพลิเคชันต่างๆ และมักจะไม่ผูกติดกับกระบวนการทางธุรกิจใดโดยเฉพาะเสมอไป แท้จริงแล้ว ทุกกิจกรรมทางธุรกิจจะพึ่งพาเทคโนโลยีไม่มากก็น้อย เทคโนโลยีจะสนับสนุนกระบวนการทางธุรกิจ และมักจะเป็นส่วนประกอบที่สำคัญยิ่งในการควบคุมกระบวนการ ในขณะที่กระบวนการควบคุมเป็นระบบอัตโนมัติมากขึ้น ข้อบกพร่องต่างๆ ในเทคโนโลยีสนับสนุนการทำงานอาจส่งผลกระทบต่อการปฏิบัติงานขององค์กรและต่อวัตถุประสงค์ทางธุรกิจอย่างมีนัยสำคัญได้

ตามมาตรฐาน 2110.A2 หน่วยงานตรวจสอบภายในต้องประเมินว่า **การกำกับดูแลเทคโนโลยีสารสนเทศ** — ซึ่งก็คือ ภาวะผู้นำ โครงสร้างองค์กร และกระบวนการ — สนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรหรือไม่ การทำความเข้าใจในแผนกลยุทธ์ด้านไอทีควรช่วยให้ผู้ตรวจสอบภายในระบุได้ว่า ไอทีจะสนับสนุนองค์กรในการนำเอากลยุทธ์ไปปฏิบัติและบรรลุวัตถุประสงค์ได้อย่างไร

หน่วยงานตรวจสอบภายในควรประเมินความยืดหยุ่นของกลยุทธ์ด้านไอที — เป็นต้นว่า ความสามารถในการสนับสนุนการเจริญเติบโตขององค์กรในอนาคต — และการตอบสนองของการบริหารความเสี่ยงด้านไอที และกระบวนการควบคุมในการป้องกัน ตรวจหา และตอบโต้ภัยต่อความมั่นคงปลอดภัยทางไซเบอร์

สิ่งแวดล้อม สังคม และความเสี่ยงด้านการกำกับดูแล

นักลงทุน ผู้บริโภค และสาธารณชน ต่างมุ่งหวังให้องค์กรวัดและรายงาน เกี่ยวกับการดำเนินความพยายามในเรื่องสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG) ขององค์กรตน โดยที่เป็นส่วนหนึ่งในการตัดสินใจลงทุน นักลงทุนมักจะมองหาข้อมูลที่ไม่ใช่ข้อมูลที่ต้องเปิดเผยตามข้อบังคับทางการซึ่งเกี่ยวกับประเด็น ESG มากขึ้น ไม่ว่าจะเป็นในรูปรายงานความยั่งยืนที่แยกมาต่างหาก หรือแถลงการณ์ต่อสาธารณชนเกี่ยวกับการบริหารความเสี่ยงที่ไม่ใช่ทางการเงินซึ่งมีอยู่ในแบบนำส่งงบการเงิน หรือแถลงการณ์ที่ส่งตรงไปยังผู้มีส่วนได้เสียอื่นๆ (สถาบันจัดอันดับความน่าเชื่อถือ) การรายงานที่ไม่ใช่ทางการเงินอาจส่งผลกระทบถึงชื่อเสียงขององค์กรที่มีต่อผู้ลงทุน พันธมิตรทางธุรกิจ และพนักงานที่คาดว่าจะดึงมาร่วมงาน

ข้อกำหนดเกี่ยวกับสิ่งแวดล้อมและความเสี่ยงเกี่ยวกับการปฏิบัติตามกฎที่ใช้กับห่วงโซ่อุปทาน (supply chain) ผลิตภัณฑ์ และบริการ การทุจริตที่เกี่ยวกับสิ่งแวดล้อม เช่น การโกหกในเรื่องมาตรฐานการปล่อยมลพิษ กำลังได้รับความสนใจไม่เพียงแต่จากทางการแต่ประชาชนก็ให้ความสนใจมากขึ้น ความเสี่ยงทางสังคมเกี่ยวข้องกับผลกระทบที่องค์กรส่งถึงพนักงาน ลูกค้า ผู้ค้าส่งวัตถุดิบ และชุมชน การรักษาความสัมพันธ์ที่ดีกับผู้มีส่วนได้เสียเหล่านี้จะทำให้ความเชื่อมั่นในองค์กรจากสาธารณชนดำรงอยู่ได้ ความเสี่ยงด้านการกำกับดูแลเกี่ยวข้องกับ กลยุทธ์ นโยบาย และการควบคุมดูแลในเรื่องความยั่งยืน โครงสร้าง

และองค์ประกอบของคณะกรรมการ ค่าตอบแทนผู้บริหารระดับสูง การล็อบบี้ทางการเมือง การติดสินบน คอรัปชั่น และการทุจริต

ผู้ตรวจสอบภายในควรมีส่วนในการหารือเกี่ยวกับ ESG และทำความเข้าใจการดำเนินความพยายามขององค์กรในเรื่อง ESG โดยเฉพาะการดำเนินการเหล่านั้นเป็นไปในทิศทางเดียวกันกับความคาดหวังของผู้มีส่วนได้เสียอย่างไร ในองค์กรที่ไม่มีเกณฑ์และการรายงานเรื่อง ESG หน่วยงานตรวจสอบภายในมีโอกาสที่จะช่วยองค์กรเพิ่มความตระหนักรู้เกี่ยวกับ ESG เกณฑ์และมาตรวัด ESG ที่ผสมผสานกับกระบวนการในการเฝ้าระวัง และสอบยันข้อมูลจะประกอบด้วยกระบวนการควบคุมหลักในการรายงาน ESG องค์กรระดับโลก ได้แก่ สหประชาชาติ (United Nations) องค์กรเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจ (Organisation for Economic Co-operation and Development — OECD) และคณะกรรมการว่าด้วยมาตรฐานทางบัญชีความยั่งยืน (Sustainability Accounting Standards Board: SASB) ได้จัดให้มีเกณฑ์การวัด ESG ที่ใช้วัดได้ รวมทั้งรายละเอียดเกี่ยวกับความเสี่ยง โอกาส และการรายงานที่เกี่ยวกับ ESG

ความเสี่ยงจากผู้ให้บริการที่เป็นกลุ่มบุคคลที่สาม (Third-party Risks)

บางโครงสร้าง กระบวนการ และแอพพลิเคชันขององค์กร อาจจะมีอยู่อย่างน้อยก็บางส่วนที่อยู่ในสภาวะเสมือนจริง และ/หรือมีการใช้บริการจากผู้ให้บริการที่เป็นกลุ่มบุคคลที่สาม ในการสอบทานของหน่วยงานตรวจสอบภายในควรคำนึงถึง ความเสี่ยงที่มีมากับผู้ให้บริการที่เป็นกลุ่มบุคคลที่สามที่องค์กรพึ่งพาอยู่ (เช่น บริการการเก็บข้อมูลบนคลาวด์ และระบบบริหารจัดการข้อมูล เป็นต้น) แนวปฏิบัติของ IIA เรื่อง “การตรวจสอบการบริหารความเสี่ยงที่มีมากับผู้ให้บริการที่เป็นกลุ่มบุคคลที่สาม — Auditing Third-party Risk Management” ได้ให้ข้อมูลที่เป็นประโยชน์เกี่ยวกับการประเมินความเสี่ยงที่มีมากับผู้ให้บริการที่เป็นกลุ่มบุคคลที่สาม

ความเสี่ยงของการทุจริต (Fraud Risks)

หน่วยงานตรวจสอบภายในมีภาระหน้าที่ในการประเมินกระบวนการบริหารความเสี่ยงขององค์กรและประสิทธิผลของมันซึ่งรวมถึงกระบวนการต่างๆ ที่เกี่ยวข้องกับความเสี่ยงของการทุจริตด้วย (มาตรฐาน 2120.A2) เนื่องจากความเสี่ยงของการทุจริตรูปแบบใหม่ๆ สามารถเกิดขึ้นเมื่อใดก็ได้ ดังนั้น ผู้ตวจสอบภายในควรจะต้องประมินความเสี่ยงของการทุจริตด้วยในขณะที่ทำการวางแผนสำหรับงานการให้ความเชื่อมั่นแต่ละงาน (มาตรฐาน 2210.A1 และ 2210.A2) การระดมสมองร่วมกับผู้มีส่วนได้เสียภายในองค์กรเป็นส่วนสำคัญยิ่งของการประเมินความเสี่ยงของการทุจริต เนื่องจากการทำทุจริตจะเกี่ยวข้องกับการใช้อุบายหลบเลี่ยงวิธีการควบคุมที่มีอยู่ CAE หลายท่านจะทุ่มเทให้กับการประเมินความเสี่ยงของการทุจริตโดยแยกออกมาต่างหาก ไม่ว่าจะค้นพบข้อมูลใดๆ โดยใช้กระบวนการใดก็ตาม ก็ควรนำข้อมูลเหล่านั้นมาผนวกรวมในการประเมินความเสี่ยงที่ครอบคลุมทั้งหมดและในแผนงานการตรวจสอบ แนว

ปฏิบัติของ IIA เรื่อง “การวางแผนงานที่ได้รับมอบหมาย: การประเมินความเสี่ยงของการทุจริต — Engagement Planning: Assessing Fraud Risks” ได้เสนอแนวทางที่เป็นระบบในประเมินความเสี่ยงของการทุจริตไว้แล้ว

แนวทางการประเมินความเสี่ยง

แนวทางที่ใช้กันอยู่ทั่วๆ ไปในการระบุ จัดทำเอกสาร และประเมินความเสี่ยงคือ “แนวทางความเสี่ยงเฉพาะ — specific-risk approach” “แนวทางที่แยกความเสี่ยงตามกระบวนการ — risk-by-process approach” และ “แนวทางที่ใช้**ปัจจัยเสี่ยง** — risk factor approach” CAE หลายท่าน อาจจะปรับแต่งแนวทางของตนให้เหมาะกับการประเมินความเสี่ยงทั่วทั้งองค์กร และหลายๆ ท่านอาจจะใช้วิธีผสม (ซึ่งก็คือ ใช้หลายๆ แนวทางผสมกัน) ข้อมูลตอบกลับจากผู้บริหารระดับสูงและคณะกรรมการ (รวมทั้งคณะอนุกรรมการอื่นๆ ที่เกี่ยวข้องของแต่ละกลุ่ม)[6] ควรถูกนำมาพิจารณาด้วยในตอนที่ทำการเลือกแนวทางและเกณฑ์สำหรับการประเมินความเสี่ยงที่ครอบคลุมทั้งหมด

การประเมินความเสี่ยงโดยทั่วไปมักจะใช้แนวทางทั้งที่เป็นเชิงปริมาณและเชิงคุณภาพผสมกัน ปัจจุบันมีซอฟต์แวร์ให้เลือกมากมายที่จะนำมาช่วยหน่วยงานตรวจสอบภายในทำการประเมินความเสี่ยงซึ่งให้ผลลัพธ์ทั้งที่เป็นข้อมูลเชิงปริมาณและเชิงคุณภาพ

แนวทางความเสี่ยงเฉพาะ (A specific-risk approach) อาจจะถือได้ว่า เป็นการทำจากล่างสู่บน (bottom-up) เนื่องจากจะเกี่ยวข้องกับการระบุความเสี่ยงที่มีมากับเฉพาะบางหน่วยรับตรวจแต่ละหน่วยใน audit universe ความเสี่ยงจะถูกระบุโดยเชื่อมโยงกับวัตถุประสงค์ทางธุรกิจ ซึ่งมักได้มาจากการประชุมหารือกับผู้บริหารที่เกี่ยวข้องโดยเฉพาะกับวัตถุประสงค์นี้ โดยอาศัยเกณฑ์ที่ผสมกัน (เช่น ผลกระทบ โอกาสเกิด) ค่าคะแนนความเสี่ยงแบบผสมจะถูกคำนวณไปให้แต่ละหน่วยรับตรวจ แนวทางนี้มักใช้สำหรับการประเมินความเสี่ยงที่เกี่ยวข้องกับแต่ละงานที่ได้รับมอบหมายแต่ก็อาจจะยุ่งยากเมื่อขยายไปสู่ระดับองค์กรเมื่อจำนวนหน่วยรับตรวจและความเสี่ยงเพิ่มขึ้นเป็นจำนวนมากมาย รูปแบบง่ายๆ ของแนวทางนี้ได้แสดงไว้ใน**ภาคผนวก ง**

6. ตามคำจำกัดความใน IPPF คำว่า “คณะกรรมการ” ได้แก่ คณะอนุกรรมการที่เกี่ยวข้องหรือองค์คณะอื่นใดที่ทางองค์คณะซึ่งมีหน้าที่กำกับดูแลได้มอบหมายหน้าที่บางอย่างให้ ดังนั้น การใช้คำว่า "คณะกรรมการ" ในแนวปฏิบัติฉบับนี้ ควรได้รับการตีความให้รวมถึงคณะอนุกรรมการของคณะกรรมการด้วย

แนวทางที่แยกความเสี่ยงตามกระบวนการ (A risk-by-process approach) จะคล้ายๆ กับแนวทางความเสี่ยงเฉพาะ (specific risk approach) ผู้ตรวจสอบภายในและผู้บริหารจะเริ่มต้นโดยถือว่ากระบวนการต่างๆ ในองค์กรทั้งหมดเป็นหน่วยรับตรวจ ความเสี่ยงหลักๆ จะถูกจับคู่เทียบกับแต่ละกระบวนการ นอกจากนี้แล้ว ผู้ตรวจสอบภายในจะตัดสินว่า กระบวนการใดที่มีบทบาทสำคัญในการบรรลุวัตถุประสงค์ และความเสี่ยงต่อกระบวนการต่างๆ เหล่านั้นได้รับการจัดการอย่างมีประสิทธิผลเพียงใด กระบวนการที่มีความเสี่ยงที่เหลืออยู่ (residual risk) ในระดับสูงสุดจะได้รับการจัดลำดับความสำคัญเพื่อที่จะนำไปรวมอยู่ในแผนงานการตรวจสอบภายใน[7]

แนวทางที่ใช้ปัจจัยเสี่ยง (A risk-factor approach) ถือได้ว่า เป็นการทำจากบนสู่ล่าง (top-down) เนื่องจากจะมองสภาพการณ์ในระดับสูงที่มีอยู่เหมือนๆ กันในหน่วยรับตรวจเป็นส่วนใหญ่ แนวทางนี้มักจะถูกนำมาใช้เมื่อต้องประเมินความเสี่ยงที่ครอบคลุมทั่วทั้งองค์กร เนื่องจากจะให้มุมมองในระดับมหภาค (macro-level view) ผู้ตรวจสอบภายในจะระบุปัจจัยร่วม (common factors) ของหน่วยรับตรวจทั้งหมดที่มีผลต่อความสามารถขององค์กรในการบรรลุวัตถุประสงค์ได้ ปัจจัยเสี่ยงไม่ใช่ความเสี่ยงด้วยตัวของมันเอง แต่มันคือสภาพการณ์ที่เกี่ยวเนื่องมากับความเสี่ยงเมื่อมีความเสี่ยงอยู่แล้ว หรือกล่าวอีกนัยหนึ่งก็คือ สภาพการณ์ที่ชี้ให้เห็นถึงความน่าจะเป็นของผลกระทบที่มีนัยสำคัญ

รายการปัจจัยเสี่ยงที่เป็นไปได้อาจจะมีเยอะแยะไปหมดซึ่งทำให้กระบวนการประเมินความเสี่ยงยุ่งยากตามไปด้วย CAE หลายๆ ท่านอาจจัดกลุ่มปัจจัยเสี่ยงเป็นประเภทต่างๆ เช่น ด้านกลยุทธ์ ด้านการปฏิบัติตามกฎระเบียบ และด้านการเงิน ในบางองค์กร ผู้บริหารระดับสูงและคณะกรรมการอาจให้คำแนะนำแก่หน่วยงานตรวจสอบภายในเกี่ยวกับปัจจัยเสี่ยงที่พวกเขาเชื่อว่าเกี่ยวข้องมากที่สุดก็ได้ ปัจจัยเสี่ยงบางตัวอาจเชื่อมโยงกับประเภทต่างๆ ได้หลายประเภท อย่างไรก็ตาม การจัดประเภทปัจจัยเสี่ยงอาจทำได้สะดวกในตอนทำการสรุปผลการประเมินความเสี่ยงให้แก่ฝ่ายบริหารระดับสูงและคณะกรรมการ

ตัวอย่างของปัจจัยเสี่ยง และประเภทของปัจจัยเสี่ยง ได้แก่:

- ระดับของกิจกรรมที่เกี่ยวเนื่องกัน (เช่น จำนวนรายการค้า)
- ความมีสาระสำคัญ (ขนาดของรายได้หรือรายจ่าย)
- สภาพคล่องของสินทรัพย์ที่เกี่ยวข้อง
- ผลกระทบต่อยี่ห้อ / ตราสินค้า (การรับรู้ของสาธารณชน ชื่อเสียง)
- การไม่สามารถบรรลุเป้าหมาย
- ความสามารถ ผลการปฏิบัติงาน อัตราการเข้า-ออกของผู้บริหาร
- ข้อบกพร่องที่ทราบอยู่แล้ว (ผลจากการปฏิบัติงานครั้งก่อนที่ออกมาอย่างไม่น่าพึงพอใจ)

7. Anderson, หนังสือ *Internal Auditing: Assurance and Advisory Services, หน้า 120.*

- ระดับการเปลี่ยนแปลงในระบบ นโยบาย วิธีการปฏิบัติงาน สัญญา และความสัมพันธ์
- ความอ่อนไหวต่อการทุจริต
- ความสลับซับซ้อนในการปฏิบัติงาน
- ระดับการพึ่งพากลุ่มบุคคลที่สาม
- ความเข้มแข็งของวิธีการควบคุมภายใน และสภาพแวดล้อมการควบคุม
- ระดับความเกี่ยวพันกับทางการ และปัญหาด้านการปฏิบัติตามกฎระเบียบ
- ระยะเวลาตั้งแต่การประเมินครั้งก่อน หรือการตรวจสอบครั้งก่อน[8]

ภาคผนวก จ ได้ให้ตัวอย่างของการประเมินความเสี่ยง โดยใช้แนวทางที่ใช้ปัจจัยเสี่ยง

การวัดค่าความเสี่ยง

ความเสี่ยงตามธรรมชาติ (Inherent Risk)

ในการประเมินความเสี่ยง ผู้ตรวจสอบภายในควรประมาณการทั้งความเสี่ยงตามธรรมชาติ (ซึ่งก็คือ ความเสี่ยงที่ไม่มีวิธีการควบคุมอยู่) และความเสี่ยงที่เหลืออยู่ (residual risk) ความแตกต่างนี้เป็นสิ่งสำคัญ เพราะผู้บริหารมักจะคิดถึงความเสี่ยงที่เหลืออยู่ในเบื้องต้น แต่ผู้ตรวจสอบภายในจำเป็นต้องสามารถพิจารณาได้ว่าเทคนิคการบรรเทาความเสี่ยงได้รับการออกแบบและทำงานได้อย่างมีประสิทธิผลหรือไม่ การประเมินความเสี่ยงของผู้ตรวจสอบภายในจะเริ่มต้นที่การพิจารณาถึงความเสี่ยงตามธรรมชาติ การผสมกันระหว่างความเสี่ยงภายในและภายนอกในสภาพที่บริสุทธิ์ปราศจากการควบคุม

กลยุทธ์การบริหารความเสี่ยงและความเสี่ยงที่เหลืออยู่

ความเสี่ยงที่เหลืออยู่ หรือความเสี่ยงสุทธิ (net risk) คือส่วนของความเสี่ยงตามธรรมชาติที่คงเหลืออยู่หลังจากผู้บริหารได้ใช้กลยุทธ์การบริหารความเสี่ยงของตนแล้ว[9] ด้วยความช่วยเหลือของฝ่ายบริหาร ผู้ตรวจสอบภายในจะระบุกลยุทธ์การบริหารความเสี่ยง และกระบวนการควบคุม แล้วแปลงให้เป็นรูปแบบในทางการปฏิบัติงานหรือที่สามารถวัดค่าได้ เพื่อที่จะตัดสินถึงความเสี่ยงที่เหลืออยู่ CAE หรือผู้ตรวจสอบที่ได้รับมอบหมายควรบันทึกเหตุผลที่พวกเขาตัดสินว่าเป็นความเสี่ยงที่เหลืออยู่ เหตุผลนี้จะสนับสนุนมุมมองของตรวจสอบภายในในการจัดลำดับความสำคัญของความเสี่ยง ซึ่งเป็นสิ่งสำคัญยิ่งในกรณีที่ดุลพินิจของตรวจสอบภายใน อาจจะขัดแย้งกับการตีความผลการจัดอันดับความเสี่ยงที่เข้มงวด

8. Wright, หนังสือ *The Internal Auditor's Guide*, หน้า 68 และ 98.

9. Anderson, หนังสือ *Internal Auditing*, หน้า 487.

การจัดอันดับความเสี่ยงที่มีมากับแต่ละหน่วยรับตรวจจะช่วยให้ CAE สามารถจัดลำดับความสำคัญของความครอบคลุมหรือขอบเขต (audit coverage) ของหน่วยรับตรวจนั้นได้[10] การวัดค่ามักจะต้องมีการกำหนดศัพท์เฉพาะ นิยาม และลักษณะจำเพาะ ให้ทั่วทั้ง audit universe (เช่น การจัดอันดับความเสี่ยง ความมีสาระสำคัญ เป็นต้น) ให้เป็นมาตรฐาน การกำหนดมาตรฐานนี้ อาจเกี่ยวข้องกับความสอดคล้องกับกรอบโครงสร้างการบริหารความเสี่ยงขององค์กร ถ้าหากมีอยู่แล้ว

การจัดอันดับผลกระทบและโอกาสเกิด (Impact and Likelihood Ratings)

ผลกระทบและโอกาสเกิดคือสองตัววัดที่ได้รับการยอมรับให้อยู่ในคำจำกัดความของคำว่าความเสี่ยงของ IIA นอกจากนี้แล้ว CAE อาจคำนึงถึง หรือนำตัววัดค่าผลกระทบหรือความรุนแรงอื่นมารวมพิจารณาด้วย เป็นต้นว่า ตัววัดต่างๆ ที่ได้รับการยอมรับในกรอบโครงสร้าง ERM ของ COSO (ซึ่งก็คือ ความสามารถในการปรับตัว (adaptability) ความสลับซับซ้อน (complexity) ความคงทน (persistence) การกู้คืน (recoverability) และความเร็ว (velocity)) การจัดอันดับความเสี่ยงอาจเป็นตัวเลข (เช่น กำหนดมาตราส่วน (scale) ตั้งแต่ 1 ถึง 3 หรือ ตั้งแต่ 1 ถึง 5) หรือจัดเป็นประเภท (เช่น ผลกระทบอาจจัดได้เป็น ไม่มีนัยสำคัญ มีสาระสำคัญ และร้ายแรงสุด โอกาสเกิด อาจจัดเป็น ต่ำ ปานกลาง และสูง)

ไม่ว่าจะเลือกใช้รูปแบบใด ควรมีการกำหนดเกณฑ์เฉพาะสำหรับแต่ละตัววัด ตัวอย่างเช่น เกณฑ์สำหรับผลกระทบอาจได้แก่ ผลกระทบในทางกฎหมาย การปฏิบัติตามข้อกำหนด / ทางการ ผลกระทบด้านชื่อเสียง ด้านการปฏิบัติงาน และความมีสาระสำคัญในเกณฑ์ทางการเงิน (มูลค่าที่ซึ่งผลกระทบต่อรายได้สามารถส่งผลถึงการบรรลุวัตถุประสงค์ขององค์กรได้) เกณฑ์ในการกำหนดโอกาสเกิด ได้แก่ ประสิทธิผลของการควบคุม และความสลับซับซ้อนของกระบวนการปฏิบัติงาน

ตัวอย่างของมาตราส่วนของผลกระทบและโอกาสเกิดพร้อมทั้งเกณฑ์ได้แสดงไว้ใน**ภาคผนวก ง** การจัดอันดับผลกระทบและโอกาสเกิดได้ถูกรวมกันเพื่อก่อให้เกิดการจัดอันดับความเสี่ยงที่ครอบคลุมซึ่งแสดงให้เห็นถึงความสำคัญโดยรวมของความเสี่ยงแต่ละตัวที่อยู่ในแต่ละหน่วยรับตรวจ / บริเวณที่สามารถตรวจได้ (auditable unit/area)

ปัจจัยเสี่ยงและค่าคะแนนความเสี่ยงทั้งหมด

ปัจจัยเสี่ยงคือองค์ประกอบที่โดยทั่วไปแล้วจะเพิ่มผลกระทบจากความเสี่ยงหรือโอกาสเกิดความเสี่ยงให้แก่หน่วยรับตรวจที่เกี่ยวข้อง และในแนวทางที่ใช้ปัจจัยเสี่ยง (risk-factor approach) นั้น การจัดอันดับความเสี่ยงจะถูกกำหนดให้กับปัจจัยเสี่ยงโดยตรง แทนที่จะจัดระดับของผลกระทบหรือโอกาสเกิด อย่างไรก็ตาม อาจจัดกลุ่มปัจจัยเสี่ยงโดยแยกว่า ปัจจัยเสี่ยงเหล่านั้น ส่งผลต่อผลกระทบหรือโอกาสเกิดหรือไม่

10. Wright, หนังสือ *The Internal Auditor's Guide,* หน้า 85.

การถ่วงน้ำหนัก ค่าคะแนนความเสี่ยงรวม (Weighting, total risk score) – ปัจจัยเสี่ยงบางปัจจัย มีนัยสำคัญต่อการบรรลุวัตถุประสงค์ มากกว่าปัจจัยอื่น และดังนั้น อาจจะต้องได้รับการถ่วงน้ำหนัก (ในเชิงตัวเลข) แต่ละหน่วยรับตรวจจะมีการจัดอันดับให้แต่ละปัจจัยเสี่ยง และการจัดอันดับปัจจัยเสี่ยงจะถูกรวบรวมมาเป็นค่าคะแนนรวมเพียงค่าเดียวสำหรับหน่วยรับตรวจนั้น ซึ่งเรียกว่าเป็นค่าคะแนนความเสี่ยงรวม ค่าคะแนนนี้ก่อให้เกิดพื้นฐานในการเปรียบเทียบสำหรับการจัดลำดับความสำคัญ หรือจัดลำดับหน่วยรับตรวจต่างๆ

การคำนวณตามที่ทางการกำหนด (Regulated calculations) – ในบางอุตสาหกรรม หน่วยงานทางการที่มีหน้าที่กำกับดูแล อาจจะกำหนดกรอบความเสี่ยงโดยเฉพาะโดยมีรูปแบบและ/หรือกระบวนวิธีที่เป็นทางการ[11] CAE อาจอ้างถึงการจัดอันดับความเสี่ยงของผู้บริหารที่ได้วัดเทียบกับกรอบที่เป็นทางการ และแล้ว CAE จึงค่อยให้ความเห็นว่า หน่วยงานตรวจสอบภายในเห็นด้วยหรือไม่กับการจัดอันดับของผู้บริหาร

ประเภทของความเสี่ยงและปัจจัยเสี่ยง ควรได้รับการทบทวนเป็นระยะ เพื่อที่จะเชื่อมั่นได้ว่าเหมาะสมกับขนาดและความซับซ้อนขององค์กร ควรเก็บหลักฐานของการทบทวนไว้กับบันทึกอื่นๆ ที่ใช้ในการวางแผนงานการตรวจสอบภายใน

ฮีทแมพ (Heat Map)

ผลจากการประเมินความเสี่ยงที่มีระดับความเสี่ยงสำหรับแต่ละหน่วยรับตรวจนั้น อาจจะแสดงเป็นกราฟในรูปของฮีทแมพ หรือแผนภูมิอื่นใดที่คล้ายคลึงกันเพื่อช่วยแสดงถึงลำดับความสำคัญ ฮีทแมพจะมีประโยชน์มากโดยเฉพาะเมื่อเกณฑ์บางเกณฑ์ได้รับการถ่วงน้ำหนักมากเกินกว่าเกณฑ์อื่นๆ รวมทั้งมีประโยชน์ในการนำเสนอผลการประเมินต่อคณะกรรมการหรือผู้บริหารระดับสูงด้วย

การสอบยันการประเมินความเสี่ยงกับผู้บริหาร

หน่วยงานตรวจสอบภายในจะคำนึงถึงความคิดเห็นจากผู้มีส่วนได้เสียตลอดช่วงของการจัดทำแผนงานการตรวจสอบภายใน และข้อมูลตอบกลับนี้จะให้ข้อมูลแก่การประเมินความเสี่ยงของหน่วยงานตรวจสอบภายใน ในขณะเดียวกัน หน่วยงานตรวจสอบภายในก็ต้องดำรงไว้ซึ่งความเป็นอิสระและความเที่ยงธรรม — ไม่มีอคติโดยทางการบริหาร — ซึ่งรวมถึงในการประเมินความเสี่ยงของหน่วยงานตรวจสอบภายในด้วย CAE ควรพบปะกับผู้บริหารระดับสูงเพื่อทบทวนการประเมินความเสี่ยงของหน่วยงานตรวจสอบภายในทำให้มั่นใจได้ในเรื่องความละเอียดถี่ถ้วน และความเข้าใจซึ่งกันและกัน และปรึกษาหารือถึงเหตุผลสำหรับ

11. ตัวอย่างเช่น ในอุตสาหกรรมการธนาคารของสหรัฐอเมริกา จะต้องคำนึงถึงความเสี่ยงเก้าประเภทและจัดอันดับสำหรับแต่ละประเด็น/บริเวณหรือกระบวนการที่กำลังได้รับการสอบทาน

สิ่งที่เห็นไม่ตรงกันที่มีนัยสำคัญในการมองภาพความเสี่ยงหรือการให้คะแนน CAE หลายๆ ท่านอาจจะอธิบายถึงระดับความตระหนักรู้ในความเสี่ยงของฝ่ายบริหารโดยแสดงออกเป็นปัจจัยเสี่ยงปัจจัยหนึ่ง และเพิ่มหรือลดค่าคะแนนในค่าคะแนนความเสี่ยงรวม เพื่อที่จะเพิ่มหรือลดความมีนัยสำคัญของความเสี่ยงที่เกี่ยวข้องกับหน่วยรับตรวจหน่วยหนึ่งก็ได้

ข้อควรพิจารณาเพิ่มเติมในการวางแผน

การสนองตอบต่อคำขอของฝ่ายบริหารและคณะกรรมการ

ผู้บริหารระดับสูงและ/หรือคณะกรรมการ อาจจะขอใช้บริการการให้ความเชื่อมั่นและการให้คำปรึกษา และ CAE ก็ควรตอบสนองต่อคำร้องขอเหล่านี้ บริการที่ปรึกษา/ให้คำแนะนำ อาจถูกร้องขอในประเด็นหรือกระบวนการซึ่งไม่ปรากฏอยู่ในพวกที่มีลำดับความสำคัญสูงสุดในการประเมินความเสี่ยง มักจะเป็นโอกาสสำหรับหน่วยงานตรวจสอบภายในที่จะให้คำแนะนำที่จะทำให้โอกาสเกิดความเสี่ยงในอนาคตลดลงได้ ตัวอย่างเช่น ผู้ตรวจสอบภายในอาจได้รับการร้องขอให้หาสาเหตุที่แท้จริง (root cause) ของการตรวจสอบจากภายนอกที่ล้มเหลว หรือขอให้สอบทานการนำเอากระบวนการหรือเทคโนโลยีใหม่ๆ ไปใช้จริง

ดังนั้น CAE หลายท่าน มักจะสำรองสัดส่วนไว้ในแผนงานการตรวจสอบเพื่องานให้คำปรึกษารวมทั้งงานเฉพาะกิจที่เกิดขึ้นในช่วงระหว่างเวลาที่ทำการประเมินความเสี่ยงและช่วงที่ทำการปรับแผนด้วย การลงทุนในทรัพยากรตรวจสอบภายในในการปฏิบัติงานให้คำปรึกษาควรสะท้อนอยู่ในงบประมาณและแผนของตรวจสอบภายใน

ข้อกำหนดใน IPPF สำหรับแผน

มาตรฐาน 2010.A2 – หัวหน้าหน่วยงานตรวจสอบต้องระบุ และคำนึงถึงความคาดหวังของผู้บริหารระดับสูง คณะกรรมการ และผู้มีส่วนได้เสียอื่น ที่มีต่อความเห็นของการตรวจสอบภายในและข้อสรุปอื่นๆ

มาตรฐาน 2010.C1 – หัวหน้าหน่วยงานตรวจสอบภายในควรพิจารณารับงานให้คำปรึกษาที่เสนอมา โดยคำนึงถึงแนวโน้มที่งานนั้นจะสามารถทำให้เกิดการปรับปรุงการบริหารความเสี่ยง เพิ่มคุณค่า และปรับปรุงการปฏิบัติงานขององค์กร รวมทั้งต้องบรรจุงานที่ได้ยอมรับมาแล้วไว้ในแผนด้วย

ความถี่ของการปฏิบัติงานและช่วงจังหวะเวลา

ไม่ใช่ว่าหน่วยรับตรวจทั้งหมดจะสามารถหรือควรได้รับการสอบทานได้ครบในทุกวงรอบการตรวจสอบตามหลักแล้ว ความถี่ของการตรวจสอบจะขึ้นอยู่กับการประเมินความเสี่ยง CAE ทั้งหลายควรพิจารณาว่า

งานใดจะช่วยส่งเสริมความสามารถขององค์กรในการบรรลุวัตถุประสงค์ได้มากที่สุด และงานใดมีแนวโน้มที่จะเพิ่มคุณค่าได้มากที่สุด

การกำหนดความถี่โดยอาศัยความเสี่ยง

ในแผนงานการตรวจสอบภายในที่อาศัยความเสี่ยงล้วนๆ CAE อาจจะใช้หนึ่งในสองกลยุทธ์เพื่อให้ได้มาซึ่งความถี่ที่เหมาะสมของการปฏิบัติงานตรวจสอบที่ได้วางแผนไว้

1. แผนงานการตรวจสอบอาจอาศัยการประเมินความเสี่ยงอย่างต่อเนื่องโดยไม่มีการกำหนดความถี่สำหรับการปฏิบัติงานไว้ก่อนล่วงหน้า จากการที่ในปัจจุบันลักษณะความเสี่ยงมีการเปลี่ยนแปลงเป็นไปในอัตราเร่ง หลายๆ องค์กรกำลังเริ่มใช้การตรวจสอบแบบต่อเนื่อง (continuous auditing) ซึ่งจะช่วยให้สามารถตอบสนองต่อการเปลี่ยนแปลงได้อย่างรวดเร็วและไม่หยุดนิ่งตลอดทั้งปี ทำการเปลี่ยนแผนงานการตรวจสอบเป็นระยะได้ตามความจำเป็น แผนงานการตรวจสอบเหล่านี้เรียกว่าเป็น “แผนหมุนเวียน (rolling)” “แผนลื่นไหล (fluid)” และ/หรือ “แผนพลวัต (dynamic)”
2. ความถี่ในการตรวจสอบที่อาศัยระดับของความเสี่ยงที่เหลืออยู่ซึ่งได้กำหนดไว้ในการประเมินความเสี่ยง ตัวอย่างเช่น หน่วยรับตรวจซึ่งได้รับการจัดอันดับว่ามีระดับความเสี่ยงสูงอาจจะถูกตรวจอย่างน้อยปีละครั้ง (หรือทุกๆ 12 ถึง 18 เดือน) พวกที่ได้รับการจัดอันดับว่ามีระดับความเสี่ยงปานกลางอาจได้รับการตรวจสอบทุกๆ 19 ถึง 24 เดือน และพวกที่ได้รับการจัดอันดับว่ามีระดับความเสี่ยงต่ำอาจจะได้รับการตรวจสอบทุกๆ 25 ถึง 36 เดือน (หรือไม่ต้องตรวจเลยก็ได้)

เพื่อที่จะมั่นใจได้ว่า แผนงานการตรวจสอบจะครอบคลุมงานที่ต้องทำและมีพื้นฐานมาจากความเสี่ยงทั้งหมด สิ่งที่ผู้ตรวจสอบภายในควรพิจารณาคือ:

- งานทั้งหลายที่กำหนดโดยกฎหมายหรือข้อกำหนดต่างๆ
- งานที่สำคัญต่อพันธกิจ
- เวลาและทรัพยากรที่จำเป็นต้องใช้สำหรับการปฏิบัติงานภาคบังคับและงานที่มีลำดับความเสี่ยงสูง
- ผู้ให้บริการการให้ความเชื่อมั่นได้กำหนดของเขตความครอบคลุมความเสี่ยงที่มีนัยสำคัญทั้งหมดไว้อย่างเพียงพอหรือไม่
- เปอร์เซนต์ของแผนซึ่งควรสำรองไว้ สำหรับโครงการพิเศษ การให้บริการให้คำปรึกษา หรืองานเฉพาะกิจที่ได้รับการร้องขอมา

ความถี่ของรอบวงจรการตรวจในภาคอุตสาหกรรมที่มีการควบคุมจากทางการสูง

ในบางภาคอุตสาหกรรม เช่น บริการด้านการเงิน องค์กรต้องปฏิบัติตามข้อบังคับซึ่งกำหนดให้องค์กรต้องกำหนด audit/risk universe ค่าความเสี่ยง และจัดอันดับความเสี่ยง และเพื่อที่จะให้คงรอบขั้นต่ำของการตรวจสอบได้ แม้ว่าความเสี่ยงตามธรรมชาติของการปฏิบัติตามกฎระเบียบจะเป็นเพียงเล็กน้อยก็ตาม งาน

เหล่านี้จะต้องถูกรวมอยู่ใน audit universe เพื่อที่จะมั่นใจได้ว่า หน่วยงานตรวจสอบภายในได้ปฏิบัติงานโดยใช้ความระมัดระวังอย่างเหมาะสม และมีความสามารถอย่างมืออาชีพ

เมื่อกฎหมาย ข้อกำหนด หรือมาตรฐานอุตสาหกรรมกำหนดให้มีการปฏิบัติงานตรวจสอบบางอย่างตามรอบวงจร CAE อาจวางแผนสำหรับหลายๆ ปีเพื่อที่จะบันทึกช่วงเวลา และทรัพยากรพิเศษหรือที่ต้องเพิ่มเติมเมื่อจำเป็น นอกจากจะต้องประสานข้อมูลต่างๆ ที่ได้รวบรวมมาแล้ว ผู้ตรวจสอบภายในควรร่วมงานกับผู้สอบบัญชีเพื่อที่จะทำให้ช่วงเวลาที่จะปฏิบัติงานสอดคล้องกันเพื่อที่จะมั่นใจได้ว่าจะรบกวนการปฏิบัติงานขององค์กรน้อยที่สุด

ถึงแม้ว่ามีการกำหนดให้ปฏิบัติงานตามรอบวงจร แต่งานเหล่านั้นจะแย่งเอาทรัพยากรไปจากงานที่กำหนดขึ้นตามระดับความเสี่ยง ซึ่งดูเหมือนจะขัดแย้งกับแนวคิดเรื่องการตรวจสอบโดยอาศัยความเสี่ยงเป็นพื้นฐานในระดับหนึ่ง โดยเฉพาะเมื่อหน่วยงานตรวจสอบภายในและผู้บริหารได้กำหนดกระบวนการในการบริหารความเสี่ยงและการให้ความเชื่อมั่นในบริเวณที่มีความเสี่ยงซึ่งได้กำหนดไว้แล้ว

เพื่อจัดการกับปัญหานี้ CAE อาจจะ:

- ลดขอบเขตของงานตรวจภาคบังคับให้แตะเฉพาะประเด็น/บริเวณที่กำหนด โดยไม่ต้องทุ่มทรัพยากรไปให้เกินกว่าข้อกำหนดขั้นต่ำ
- ขยายช่วงเวลาของแผนระยะยาว (เช่น เป็นจ็ดปี) เพื่อบันทึกงานภาคบังคับ ในขณะเดียวกันก็ประเมินความเสี่ยงอย่างต่อเนื่องและปรับแผนระยะสั้นให้ถี่ขึ้น เพื่อจัดลำดับความสำคัญของงานโดยให้เชื่อมโยงกับความเสี่ยงที่มีนัยสำคัญ
- ประสานและพึ่งพาผู้ให้บริการความเชื่อมั่นรายอื่นๆ

ในขณะที่การปฏิบัติงานตามรอบวงจรจะมีข้อมูลนำเข้าในแผนเพียงแค่ครั้งเดียว CAE ต้องระมัดระวังไม่ไปพึ่งพาแผนระยะยาวมากนัก ในยุคปัจจุบันที่ภาพมุมมองความเสี่ยงเปลี่ยนแปลงไปอย่างรวดเร็ว เมื่อแผนระยะยาวได้ถูกกำหนดขึ้น แผนของปีปัจจุบันก็ควรได้รับการวางแผนโดยมีรายละเอียดมากขึ้น มีการทบทวนอย่างน้อยไตรมาสละครั้ง และปรับแก้ตามสมควร

การประมาณการทรัพยากร

CAE ต้องกำหนดทรัพยากรที่จำเป็นในการลงมือปฏิบัติตามแผน ทรัพยากรอาจ ได้แก่ คน (เช่น ชั่วโมงทำงานและทักษะของคนงาน) เทคโนโลยี (เช่น เครื่องมือและเทคนิคในการตรวจสอบ) ช่วงเวลา/ตารางงาน (ความพร้อมของทรัพยากร) และเงินทุน CAE จะต้องประมาณการขอบเขตของงานและทักษะ เวลา รวมทั้งงบประมาณที่จำเป็นจะต้องใช้ในการปฏิบัติงานเหล่านั้น CAE อาจสะท้อนให้เห็นถึงลักษณะและความซับซ้อนของงานแต่ละงาน ทรัพยากรที่ใช้ไปเทียบกับงานซึ่งเทียบเคียงกันได้ที่ได้ปฏิบัติไปแล้วก่อนหน้านั้น และวันที่ของการตรวจสอบในบริเวณหรือกระบวนการนั้นๆ ล่าสุด

การประเมินทักษะ

มาตรฐาน 2030 ได้อธิบายคำว่า “ทรัพยากรที่เหมาะสม” ในแง่ของความรู้ ทักษะ และความสามารถในหน้าที่ด้านต่างๆ *มาตรฐาน*ได้ให้ความสนใจเป็นอย่างมากในเรื่องความสามารถของหน่วยงานตรวจสอบภายใน และความสามารถในหน้าที่นี้ก็เป็นหนึ่งในสี่หลักการของประมวลจรรยาบรรณของ IIA โดยถือว่าเป็นส่วนหนึ่งในการวางแผน CAE จะต้องทราบถึงความสามารถในหน้าที่ของทีมตรวจสอบภายใน CAE อาจจัดทำและดูแลทะเบียนรายการทักษะพิเศษและความรู้ของผู้ตรวจสอบภายในแต่ละคน ควบคู่ไปกับเกณฑ์เปรียบเทียบทักษะที่จำเป็นในการตอบสนองความคาดหวัง ความต้องการ และคำขอจากองค์กร และอุตสาหกรรม ในบางภาคอุตสาหกรรมที่ถูกควบคุมจากทางการอย่างเข้มงวดอาจถึงกับมีการกำหนดรายการทักษะขั้นต่ำที่คาดหวัง และกำหนดให้ต้องทำการวิเคราะห์ทักษะเป็นประจำ

เกณฑ์เปรียบเทียบที่กำหนดขึ้นนั้น สามารถปรับแต่งเพื่อให้ระบุได้ถึงทักษะเฉพาะบางอย่างที่จำเป็นในการทำงานได้ตามแผนงานการตรวจสอบภายใน CAE ควรจัดให้ทักษะที่ปรากฏในทีมงานตรวจสอบภายในสอดคล้องกับทักษะต่างๆ ที่จำเป็นในการตอบสนองความคาดหวังและปฏิบัติงานที่มีอยู่ในแผนได้

ความต้องการในทรัพยากรตรวจสอบภายใน

มาตรฐาน 2030 – การบริหารทรัพยากร

หัวหน้าหน่วยงานตรวจสอบภายในต้องมั่นใจว่าทรัพยากรสำหรับงานตรวจสอบมีความเหมาะสม เพียงพอและถูกนำมาใช้อย่างมีประสิทธิผลเพื่อให้บรรลุตามแผนงานที่ได้รับอนุมัติมาได้

บทตีความ:

ความเหมาะสม หมายถึง การผสมผสานระหว่างความรู้ ทักษะ และความสามารถด้านต่างๆ ที่จำเป็นในการปฏิบัติตามแผนงาน ความเพียงพอ หมายถึง ปริมาณของทรัพยากรที่จำเป็นต่อการบรรลุแผนงาน ทรัพยากรจะถูกนำไปใช้ได้อย่างมีประสิทธิผลก็ต่อเมื่อมีการนำไปใช้ในลักษณะที่ก่อให้เกิดความสำเร็จตามแผนงานที่ได้รับอนุมัติได้สูงสุด

การประสานงานกับผู้ให้บริการการให้ความเชื่อมั่นและให้คำปรึกษารายอื่น

หน่วยงานตรวจสอบภายในเพิ่มคุณค่าได้มากที่สุดด้วยการให้บริการความเชื่อมั่นและให้คำปรึกษาในที่ๆ มีความเสี่ยงที่เหลืออยู่สูงสุด อย่างไรก็ตาม ในองค์กรซึ่งมีวุฒิภาวะพร้อมและถูกทางการควบคุมอย่างเข้มงวด บางบริเวณที่มีความเสี่ยงสูงอาจมีการควบคุมอย่างมีประสิทธิผลแล้วโดยแนวป้องกันด่านที่หนึ่ง และอาจมีการให้ความเชื่อมั่นที่ครอบคลุมเพียงพอโดยแนวป้องกันด่านที่สอง ดังเช่น หน่วยงานบริหารความเสี่ยง และหน่วยงานกำกับดูแล รวมทั้งความครอบคลุมเพิ่มเติมโดยผู้สอบบัญชี หัวหน้าหน่วยงานข้อมูล (chief information officer) และหัวหน้าหน่วยงานความปลอดภัยของข้อมูล (chief information security officer) ขององค์กรอาจประเมินความเสี่ยงด้านไอที และหน่วยงานตรวจสอบภายในอาจเป็นผู้ยืนยันผลการประเมิน

เพื่อให้การใช้ทรัพยากรอันมีค่าเกิดประโยชน์สูงสุด CAE ควรประสานกิจกรรมต่างๆ แบ่งปันข้อมูล และพิจารณาการพึ่งพาผลงานของผู้ให้บริการให้ความเชื่อมั่นและให้คำปรึกษารายอื่นทั้งจากภายในและภายนอก (มาตรฐาน 2050 – การประสานงานและการพึ่งพาผลงานของผู้อื่น) การพึ่งพาผลงานของผู้ให้บริการรายอื่นแทนที่จะครอบคลุมเรื่องเดียวกัน จะช่วยลดการทำงานซ้ำซ้อน และเพิ่มประสิทธิภาพด้วยความเชื่อมั่นที่ได้ให้ไป

แผนที่การให้ความเชื่อมั่น (Assurance Maps)

แผนที่การให้ความเชื่อมั่น เป็นเอกสารที่บันทึกการประสานงานในความครอบคลุมของการให้ความเชื่อมั่น แผนที่นี้จะมีรายการประเภทความเสี่ยงต่างๆ ที่มีนัยสำคัญและเชื่อมโยงกับแหล่งการให้ความเชื่อมั่นที่เกี่ยวข้องแหล่งต่างๆ จากข้อมูลที่ได้รวบรวมมา ความเข้มข้น หรือ ระดับของความครอบคลุมที่ได้ให้บริการไปแล้วนั้นสามารถจัดอันดับได้ว่าเป็น พอเพียง หรือไม่พอเพียง แล้วจะเห็นช่องว่างและความซ้ำซ้อนได้ชัดเจนขึ้น

การสร้างแผนที่การให้ความเชื่อมั่นเกี่ยวข้องกับผู้ให้บริการการให้ความเชื่อมั่นที่หลากหลายซึ่งต้องร่วมมือกัน จากมุมมองแบบองค์รวมทั่วทั้งองค์กร การระบุจุดที่งานของผู้ให้บริการรายอื่นทับซ้อนกับขอบเขตของตรวจสอบภายในจะช่วยยืนยันการตัดสินใจของ CAE ได้ว่า งานใดควรรวมอยู่ในแผน หรืองานใดควรถูกกัน

เรียนรู้เกี่ยวกับแผนที่การให้ความเชื่อมั่น

แนวปฏิบัติของ IIA (IIA's Practice Guide) เรื่อง “การประสานงานและการพึ่งพา: การพัฒนาแผนที่การให้ความเชื่อมั่น – Coordination and Reliance: Developing an Assurance Map” ได้ให้รายละเอียด แนวทางที่แนะนำ พร้อมทั้งตัวอย่างของการสร้างและการใช้ประโยชน์จาก แผนที่การให้ความเชื่อมั่น

ออกไปจากแผนงานการตรวจสอบภายใน แผนที่นี้ยังเป็นหลักฐานของช่องว่างในการให้ความเชื่อมั่นที่ชัดเจนซึ่งอาจจะต้องการทรัพยากรเพิ่มเติมเพื่อปิดช่องว่าง

การตอบสนองความต้องการทักษะเพิ่มเติม

หากหน่วยงานตรวจสอบภายในขาดความรู้หรือทักษะที่จำเป็นในการปฏิบัติงานการให้ความเชื่อมั่นบางงานให้ลุล่วงได้ CAE อาจร้องขอให้ผู้เชี่ยวชาญหรือผู้ชำนาญการจากภายในองค์กรเพื่อให้ทำงานที่ต้องใช้ความเชี่ยวชาญทางเทคนิคและในขณะเดียวกันก็จะได้ถ่ายทอดความรู้ใหม่ๆ ให้แก่ทีมงานตรวจสอบภายใน

อีกทางเลือกหนึ่งคือการใช้ cosourcing ซึ่งผู้เชี่ยวชาญจากภายนอกองค์กรจะปฏิบัติงานพิเศษบางอย่างภายใต้การกำกับดูแลของผู้ตรวจสอบภายในที่มีประสบการณ์ และใช้วิธี outsourcing สำหรับงานที่ต้องดำเนินการโดยผู้ให้บริการจากภายนอกตั้งแต่ต้นจนจบ CAE ควรบันทึกการจัดเตรียมทีมงานในลักษณะนี้ไว้ในงบประมาณของแผนด้วย

การคำนวณชั่วโมงในแผน

เพื่อที่จะคำนวณจำนวนชั่วโมงที่ตรวจสอบภายใน “มีอยู่ – available” CAE จะคำนวณชั่วโมงทั้งหมดซึ่งผู้ตรวจสอบภายในแต่ละคนในทีมสามารถทำงานเพื่อให้เป็นไปตามแผนได้ในช่วงเวลาหนึ่งที่กำหนด (ซึ่งมักจะเป็นหนึ่งปี) จำนวนชั่วโมงที่มีอยู่จะคำนึงถึงผลของการประเมินทักษะ การใช้ทรัพยากรจากภายนอก และงานย่อยๆ ที่ไม่ช่วยให้งานสำเร็จตามแผนได้ด้วย

ตัวอย่างเช่น CAE อาจเริ่มต้นด้วยการตั้งสมมติฐานว่า พนักงานเต็มเวลาคนหนึ่ง จะมีเวลาทำงานเท่ากับจำนวนชั่วโมงทั้งหมด 2,080 ชั่วโมง (ซึ่งก็คือ 40 ชั่วโมงต่อสัปดาห์ 52 สัปดาห์ต่อปี)[12] แล้ว CAE อาจจะลบด้วยข้อต่อไปนี้ เพื่อหาจำนวนชั่วโมงที่มีอยู่คงเหลือ:

- **ลบ**เวลาสำหรับงานที่ไม่ใช่งานตรวจสอบ (nonaudit) หรือเวลาของงานที่ไม่ก่อให้เกิดประโยชน์ ซึ่งเป็นกิจกรรมที่ไม่มีส่วนช่วยให้การปฏิบัติงานที่ได้รับมอบหมายสำเร็จและเป็นไปตามแผนงานตรวจสอบได้
  - ช่วงวันหยุดที่จ่ายเงิน (เช่น วันหยุด วันลาพักผ่อน วันลาป่วย)
  - การฝึกอบรมและการพัฒนาบุคลากร
  - การประชุม (กับทีมตรวจสอบภายใน และกับผู้บริหารและคณะกรรมการ)
  - ความริเริ่มโครงการประกันคุณภาพและปรับปรุงงานของหน่วยงานตรวจสอบภายใน
  - อัตราการใช้งานที่ลดลงสำหรับคนที่คาดว่าจะจ้างใหม่ในปีที่กำหนด

12. CAEs ควรปรับสมมติฐานเพื่อให้สะท้อนสถานการณ์ที่แท้จริงของจำนวนพนักงานตรวจสอบภายในและองค์กร

- เวลาที่ใช้ในการหารือประเด็นปัญหากับผู้เชี่ยวชาญในการพัฒนากรอบ / กลยุทธ์การตรวจสอบ
- อัตราการลาออกในระหว่างปีที่ไม่ได้คาดไว้ (เรียกว่า “ปัจจัยความว่าง หรือ vacancy factor” โดยปกติใช้สำหรับทีมงานที่มีพนักงานจำนวนมาก)
- สำรองสำหรับงานที่ไม่ใช่งานตรวจสอบที่ยังไม่ได้มีการมอบหมาย

- หักเวลาที่ใช้ในการช่วยเหลือผู้ให้บริการการให้ความเชื่อมั่นรายอื่น เช่น ผู้สอบบัญชี หากมี
- หักเวลาของ CAE ที่เผื่อไว้ในการควบคุมบังคับบัญชาและกิจกรรมอื่นๆ ที่เกี่ยวข้อง (เช่น ประมาณไว้ที่ 80 เปอร์เซนต์)
- หักชั่วโมงที่ใช้ประโยชน์ได้ซึ่งจะใช้สำหรับงานตามคำร้องขอที่กำลังดำเนินไป การเฝ้าระวัง การวิเคราะห์ข้อมูล งานติดตามผลที่ได้ปฏิบัติเสร็จสิ้นไปแล้ว และสำรองเผื่อไว้สำหรับคำขอที่มีมาเป็นครั้งคราว หมายเหตุ: CAE บางท่านก็รวมเอาการเฝ้าติดตามผล / การตรวจสอบในขณะที่งานดำเนินไปเป็นส่วนหนึ่งของชั่วโมงที่ใช้ประโยชน์ได้ที่มีอยู่
- ส่วนที่เหลือก็คือ จำนวนชั่วโมงที่มีอยู่ (ชั่วโมงการตรวจสอบ หรือชั่วโมงที่คิดค่าบริการ) ที่จะใช้ในการปฏิบัติงานที่ได้รับมอบหมาย (ซึ่งรวมถึง การประเมินความเสี่ยง การวิเคราะห์และประเมินผล การจัดทำเอกสาร และการรายงาน) เพื่อที่จะทำตามแผนงานการตรวจสอบภายในที่อาศัยความเสี่ยงได้สำเร็จ

การร่างแผนงานการตรวจสอบภายใน

งานที่ได้เตรียมการมาทั้งหมดมาถึงจุดที่แผนงานการตรวจสอบภายในฉบับร่างจะถูกนำเอาไปเสนอ หารือและแก้ไข และหาข้อสรุปเพื่อการอนุมัติ แผนงานการตรวจสอบภายในที่นำเสนออาจประกอบไปด้วยส่วนต่างๆ ดังนี้:

บทสรุปสำหรับผู้บริหาร (Executive summary) – ส่วนนี้จะเป็นบทสรุปภาพรวมประเด็นสำคัญสั้นๆ ซึ่งมักจะเป็นบทสรุปเพียงหนึ่งหน้าถึงความเสี่ยงที่มีนัยสำคัญที่สุด งานที่ได้วางแผนไว้ กำหนดเวลาเบื้องต้น และแผนการจัดกำลังคนลงไปในงาน

นโยบายและกระบวนการ (Policies and processes) – ส่วนนี้จะเป็นภาพรวมเพื่อให้คณะกรรมการเข้าใจถึงการทำงานตรวจสอบและความละเอียดถี่ถ้วนของนโยบายและแนวทางการวางแผนงานตรวจสอบภายใน อันประกอบไปด้วยคำบรรยายพื้นฐานเกี่ยวกับกระบวนการต่างๆ ที่ใช้ในการสร้าง audit universe การทำการประเมินความเสี่ยง ความครอบคลุมในการให้ความเชื่อมั่นที่ประสานกัน และแผนกำลังคน อาจเน้นย้ำถึงการเปลี่ยนแปลงใดๆ ในนโยบายและวิธีการทำงานเพื่อใช้ในการหารือก็ได้

บทสรุปเกี่ยวกับการประเมินความเสี่ยง (Risk assessment summary) – คำบรรยายถึงกระบวนการประเมินความเสี่ยงและผลจากการประเมิน จะช่วยยกระดับความเข้าใจของคณะกรรมการเกี่ยวกับลำดับความสำคัญของงานตรวจสอบภายในได้ ข้อมูลต่างๆ อาจได้แก่:

- กลยุทธ์ขององค์กร บริเวณสำคัญที่ต้องใส่ใจ ความเสี่ยงที่สำคัญ และกลยุทธ์การให้ความเชื่อมั่นที่เกี่ยวข้องในแผนงานการตรวจสอบ
- บทสรุปความเสี่ยงต่างๆ
- บทวิเคราะห์ (หรือบทสรุป) ระดับความเสี่ยงตามธรรมชาติหรือความเสี่ยงที่เหลืออยู่ของหน่วยรับตรวจต่างๆ (auditable units)
- ค่าคะแนน / อันดับของความเสี่ยงสำหรับหน่วยรับตรวจต่างๆ
- แผนที่ความเสี่ยง (Heat map) สำหรับ audit universe ทั้งหมด โดยชี้ให้เห็นถึงลำดับความสำคัญ การรวมและการยกเว้นใดๆ ด้วย

ภาพรวมของงานต่างๆ ในแผน –

- รายการงานตรวจสอบต่างๆ ที่เสนอ (และคุณสมบัติเฉพาะที่ถือว่าโดยลักษณะแล้วเป็นงานการให้ความเชื่อมั่นหรืองานให้คำปรึกษา)
- ขอบเขตและวัตถุประสงค์เบื้องต้นของงานที่ได้รับมอบหมาย
- ช่วงเวลาและระยะเวลาที่ใช้ในเบื้องต้น (ไทม์ไลน์ที่แสดงว่างานที่ได้รับมอบหมายใดบ้างที่จะปฏิบัติในไตรมาสใด และจะต้องใช้เวลานานเท่าไรงานจึงจะเสร็จ)

ความครอบคลุมและข้อยกเว้นในการให้ความเชื่อมั่น (Assurance coverage and exclusions) – ในส่วนนี้อาจจะรวมถึง แผนที่การให้ความเชื่อมั่น ข้อสรุป หรือเครื่องมืออื่นใดที่ใช้ในการสื่อสารถึงความครอบคลุมของการให้ความเชื่อมั่นในบริเวณที่มีความเสี่ยงที่มีนัยสำคัญ ส่วนข้อยกเว้นนั้นจะยอมรับถึงหน่วยรับตรวจหรือบริเวณเสี่ยงที่ไม่ได้กล่าวถึง และหากไม่ได้ครอบคลุมถึงบริเวณที่มีความเสี่ยงสูง (เช่น เนื่องมาจากข้อจำกัดด้านทรัพยากร) แล้ว ในส่วนนี้อาจใส่ข้อเสนอแนะแก่คณะกรรมการเพื่อให้แสวงหาความเชื่อมั่นจากแหล่งอื่น เช่น โดยผ่านการว่าจ้างบุคคลภายนอกมาร่วมทำงาน (cosourcing) หรือว่าจ้างบุคคลภายนอกให้มาทำงานใดงานหนึ่งทั้งหมด (outsourcing)

เหตุผลที่รวมหรือไม่รวม (Rationale for inclusions and exclusions) – คำอธิบายในส่วนนี้สำคัญยิ่งโดยเฉพาะถ้าการจัดอันดับความเสี่ยงหรือการกำหนดความถี่ได้ถูกข้ามไป เหตุผลอาจจะรวมถึง การเปลี่ยนแปลงในการจัดอันดับความเสี่ยง ระยะห่างตั้งแต่การตรวจครั้งก่อน การเปลี่ยนแปลงทางการบริหาร และอื่นๆ

แผนทรัพยากร (Resource plan) – ส่วนนี้จะระบุประเภทและจำนวนทรัพยากรที่จำเป็นต้องใช้ในการปฏิบัติตามแผน อาจจะบรรยายถึงจำนวนพนักงานที่ต้องการที่จะใช้เพื่อให้แผนการตรวจสอบกระทำได้สำเร็จ (สมรรถนะ) จำนวนพนักงานสนับสนุนที่ต้องการ ผลการประเมินทักษะโดยย่อ และแผนที่จะดำเนินการกับช่องว่างเรื่องทักษะ

งบประมาณทางการเงิน (Financial budget requirements) – แผนจะรวมถึงงบประมาณทางการเงินเพื่อจ่ายเงินเดือนพนักงานตรวจสอบภายใน รวมทั้งต้นทุนในการว่าจ้างบุคคลภายนอกมาให้บริการแบบ cosourced และหรือ outsourced เครื่องมือ (ซึ่งก็คือเทคโนโลยี) การฝึกอบรม และค่าใช้จ่ายอื่นๆ

IPPF และมาตรฐานที่เกี่ยวข้อง (IPPF and relevant standards) – การอ้างอิงในการปฏิบัติให้สอดคล้องกับมาตรฐานใน IPPF และแนวทางต่างๆ จะช่วยสนับสนุนการหารือกับผู้บริหารระดับสูงและคณะกรรมการเกี่ยวกับความสำคัญของแผนที่จัดทำโดยอาศัยความเสี่ยงของตรวจสอบภายในรวมทั้งแง่มุมอื่นๆ ของการวางแผน (เช่น การสื่อสาร การประสานงาน และการพึ่งพาผลงานของผู้อื่น)

บริเวณที่ได้รับการอนุมัติ (Approval sign-off area) – ผู้บริหารระดับสูงและคณะกรรมการต้องอนุมัติแผน

ส่วนย่อย หรือ แผนย่อย (Subsections, or subplans) – ภายในแผนโดยรวม ความเสี่ยงต่างๆ จากหน่วยรับตรวจทั้งหมด อาจนำมารวมกันเป็นประเภทๆ โดยมีความครอบคลุมในการให้ความเชื่อมั่นที่เกี่ยวข้องกับแต่ละพื้นที่เสี่ยงหลักที่ได้ระบุไว้

- ด้านการปฏิบัติงาน
- ด้านการเงิน
- ด้านการปฏิบัติตามกฎระเบียบ
- ไอที / ความมั่นคงปลอดภัยทางไซเบอร์
- วัฒนธรรม
- บริการให้คำปรึกษา (เช่น ความคิดริเริ่มด้านกลยุทธ์ การประเมินระบบใหม่ในเบื้องต้น)
- งานพิเศษที่ถูกร้องขอมา (เช่น การสอบสวน)
- การติดตามผล (ซึ่งก็คือ การติดตามการนำเอาข้อเสนอแนะไปลงมือปฏิบัติ)

ภาคผนวก ฉ แสดงตัวอย่างของบทสรุปสำหรับผู้บริหาร สำหรับแผนงานการตรวจสอบภายในระยะสามปี ซึ่งในปีที่สองและปีที่สามอาจมีการเปลี่ยนแปลงได้ขึ้นอยู่กับผลจากการประเมินความเสี่ยง

การนำเสนอแผนและการขอความคิดเห็น

เมื่อแผนการตรวจสอบตามความเสี่ยงเบื้องต้นได้ถูกสร้างขึ้น CAE หรือผู้จัดการตรวจสอบภายในมักจะหารือกับฝ่ายบริหารระดับสูงก่อนทำให้แผนเป็นทางการเพื่อนำเสนอต่อคณะกรรมการตรวจสอบและ/หรือคณะกรรมการทั้งชุด CAE มักนำเอากระบวนการมาตรฐานมาใช้ในการทบทวนร่วมกันนี้ และอาจจะพบกับผู้บริหารระดับสูงแต่ละท่านเป็นรายบุคคลด้วย CAE อาจจะปรึกษากับคณะอนุกรรมการบางชุด เช่น ชุดที่มีหน้าที่ในการบริหารความเสี่ยง การปฏิบัติตามกฎระเบียบ จรรยาบรรณ และอื่นๆ อาจจะกำหนดเวลาประชุมกับเจ้าของกระบวนการแต่ละคนเพื่อที่จะหารือเกี่ยวกับขอบเขตเบื้องต้นและช่วงเวลาของการปฏิบัติงานที่ได้รับมอบหมาย

ในการหารือ CAE ควรสื่อสารผลของการประเมินความเสี่ยง ความเสี่ยงที่มีนัยสำคัญจะส่งผลต่อวัตถุประสงค์ขององค์กรอย่างไร และผลนั้นช่วยในการกำหนดแผนที่จะตรวจงานตรวจสอบต่างๆ ได้อย่างไร CAE ควรอธิบายถึงการกำหนดทรัพยากร เป็นต้นว่า บริเวณต่างๆ ที่หน่วยงานตรวจสอบจะให้ความเชื่อมั่น และบริเวณใดที่จะใช้บริการการให้ความเชื่อมั่นจากผู้อื่น ในระหว่างการประชุม CAE สามารถกล่าวถึงความกังวลของฝ่ายบริหารระดับสูงได้ แผนอาจมีการเปลี่ยนแปลงได้ขึ้นอยู่กับการหารือถึงความเสี่ยงที่ยอมรับได้ (risk appetite) และขอบเขต และ/หรือช่วงเวลาที่ครอบคลุมของการให้ความเชื่อมั่น (ขึ้นอยู่กับการประสานงานกับผู้ให้บริการรายอื่น) CAE และฝ่ายบริหารระดับสูงจะร่วมกันพิจารณาใคร่ครวญคำถามต่างๆ เป็นต้นว่า:

- ความเสี่ยงและหน่วยรับตรวจทั้งหมดได้รับการพิจารณาอย่างละเอียดถี่ถ้วนแล้วหรือไม่?
- จะมีการเปลี่ยนแปลง (เช่น การซื้อกิจการ การควบรวมกิจการ การอัพเกรดระบบ ผู้จัดส่งสินค้ากลุ่มบุคคลที่สาม หรือการนำเอาซอฟต์แวร์ไปใช้) ที่กำลังจะมาถึงซึ่งเรายังไม่ได้พิจารณาอย่างเป็นกิจจะลักษณะหรือไม่?
- งานที่ได้กำหนดในแผนเชื่อมโยงกับวัตถุประสงค์และความเสี่ยงสูงสุดขององค์กรอย่างไร?
- งานที่มีในแผนเพิ่มคุณค่าให้แก่ฝ่ายบริหารระดับสูงและองค์กรอย่างไร?
- การประสานของความครอบคลุมของการให้ความเชื่อมั่นและตารางงาน / ช่วงเวลาของงานต่างๆ สมเหตุสมผลหรือไม่?
- หากมีคำร้องขอใดที่ไม่ได้รับการพิจารณาให้บรรจุในแผนทำไมจึงไม่?

ข้อจำกัดของความครอบคลุมของการให้ความเชื่อมั่นที่เกี่ยวกับงบประมาณ

ในการสื่อสารแผนงานและความต้องการทรัพยากรของหน่วยงานตรวจสอบภายใน CAE ควรอธิบายถึงความสัมพันธ์ระหว่างความเสี่ยงที่องค์กรกำลังเผชิญและงบประมาณที่มีให้กับความครอบคลุมของการให้

ความเชื่อมั่น CAE ควรให้ความสนใจกับบริเวณที่เสี่ยงสูงที่ไม่ได้กำหนดความครอบคลุมของการให้ความเชื่อมั่นไว้พอและควรเตรียมพร้อมที่จะร้องขอทรัพยากรเพิ่มเติม เมื่อมีความจำเป็น

การสื่อสารเพื่อสรุปแผน

การนำเสนอต่อคณะกรรมการตรวจสอบ

CAE จะประเมินผลความคิดเห็นที่ตอบกลับมาจากผู้บริหารระดับสูง และนำไปรวมกับข้อมูลที่เกี่ยวข้องเพื่อที่จะมั่นใจได้ว่าแผนงานได้สะท้อนให้เห็นถึงลำดับความสำคัญขององค์กรอย่างเหมาะสม และมั่นใจว่าฝ่ายบริหารสนับสนุนการนำเอาแผนไปลงมือปฏิบัติ แผนที่ปรับแก้แล้วจะถูกนำเสนอต่อคณะกรรมการตรวจสอบเพื่อให้ทบทวนอีกครั้ง คณะกรรมการตรวจสอบอาจแนะนำให้ปรับแผนโดยขึ้นอยู่กับมุมมองเกี่ยวกับความเสี่ยงที่องค์กรยอมรับได้ของคณะกรรมการตรวจสอบ การประชุมจะเปิดโอกาสให้ CAE ได้อธิบายถึงงบประมาณและความเกี่ยวพันกับความครอบคลุมของการให้ความเชื่อมั่น โดยมีหมายเหตุเกี่ยวกับช่องว่างของการไม่ครอบคลุมที่มีนัยสำคัญหากมี

การนำเสนอต่อคณะกรรมการเต็มคณะ

เพื่อสื่อสารกับคณะกรรมการ CAE มักจะจัดทำการนำเสนอที่สรุปงานต่างๆ ที่มีอยู่ในแผน อธิบายถึงการประเมินความเสี่ยงที่อยู่เบื้องหลังการเลือก และกล่าวถึงคุณค่าของการให้ความเชื่อมั่นและให้คำปรึกษาอย่างเป็นอิสระและเที่ยงธรรมที่ให้โดยหน่วยงานตรวจสอบภายใน ประธานคณะกรรมการตรวจสอบอาจจะนำเสนอข้อมูลสรุปต่อคณะกรรมการเพื่อการอนุมัติขั้นสุดท้าย เมื่อฝ่ายบริหารระดับสูงและคณะกรรมการได้อนุมัติแผนแล้ว หน่วยธุรกิจต่างๆ ที่ได้รับผลกระทบทั้งหมดจะได้รับสำเนาแผนชุดหนึ่งด้วย

การสื่อสารอย่างต่อเนื่อง

ในบางองค์กร CAE จะสื่อสารเป็นรายไตรมาสโดยผ่านทางรายงานที่เป็นทางการ ช่วงจังหวะเวลาของการนำเสนอต่อฝ่ายบริหารระดับสูงและคณะกรรมการ (คณะกรรมการตรวจสอบ) อาจส่งผลถึงการที่ผู้มีส่วนได้ส่วนเสียทั้งสองกลุ่มคิดต่อหน่วยงานตรวจสอบภายในอย่างไร ข้อมูลที่มากเกินไปและถูกเอามานำเสนอในคราวเดียว (เช่น เมื่อสิ้นไตรมาส) สามารถลดการเปิดใจรับข้อมูลที่ได้จากหน่วยงานตรวจสอบภายในของผู้มีส่วนได้เสียได้ ผู้ตรวจสอบภายในพึงใส่ใจที่จะสื่อสารกับฝ่ายบริหารระดับสูงอย่างสม่ำเสมอ และเมื่อมีการเปลี่ยนแปลงใดๆ ในแผนงานการตรวจสอบภายในก็ควรแจ้งเตือนล่วงหน้าพอสมควรเพื่อเปิดโอกาสให้มีการหารือได้

การสื่อสารถึงการเปลี่ยนแปลงที่เสนอ

ถ้าแผนงานการตรวจสอบภายในและ/หรือความต้องการทรัพยากรมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ CAE ต้องสื่อสารการเปลี่ยนแปลงเหล่านั้นให้ฝ่ายบริหารระดับสูงและคณะกรรมการได้รับทราบ และขออนุมัติโดยให้เป็นไปตามมาตรฐาน 2020 – การสื่อสารและการอนุมัติ ถึงแม้ว่าจะมีการปรับแผนเพียงเล็กน้อย ก็อาจเป็นโอกาสให้คนสามกลุ่มมาพูดคุยหารือกันเกี่ยวกับการตระหนักรู้ถึงความเสี่ยงต่างๆ เพื่อปรับปรุงความถูกต้องของข้อมูลที่ใช้ร่วมกัน และเพื่อทำให้ลำดับความสำคัญของการบริหารความเสี่ยงของพวกเขาเหล่านั้นสอดคล้องกัน

CAE บางท่านหรือผู้จัดการตรวจสอบจะสอบทานแผนงานการตรวจสอบภายในเป็นรายเดือน เขาเหล่านั้นจะประเมินว่ามีการเปลี่ยนแปลงในรูปแบบความเสี่ยงใดสมควรที่จะมาแทนที่งานตรวจสอบที่ได้รับมอบหมายหรือไม่ และมีทรัพยากรอยู่เพียงพอให้แก่งานตรวจสอบงานใหม่ที่จะเพิ่มเติมเข้าไปในแผนหรือไม่

ถึงแม้ว่าไม่ได้กำหนดให้มีการสื่อสารถึงการปลี่ยนแปลงเหล่านี้เป็นรายไตรมาส CAE หลายๆ ท่านก็เลือกที่จะกำหนดที่จะรายงานเป็นรายไตรมาสเพื่อความสม่ำเสมอ บทสนทนาในการสื่อสารอาจเป็นการร้องขอทรัพยากร ผู้ตรวจสอบภายในจะพิจารณาคำถามต่างๆ เป็นต้นว่า “การเปลี่ยนแปลงในแผนจะเป็นเหตุการณ์ที่ไม่เหมือนใครหรือไม่ หรือจำเป็นต้องมีการปรับงบประมาณระยะยาวหรือไม่” เพื่อรองรับงานชิ้นใหม่ภายในงบประมาณที่มี หน่วยงานตรวจสอบภายในอาจจำเป็นต้องตัดบางสิ่งบางอย่างออกจากแผนก็ได้ CAE หรือผู้จัดการตรวจสอบอาจสร้างกรณีศึกษาทางธุรกิจสำหรับการเปลี่ยนแปลงที่ต้องการ หรืออาจจะถามฝ่ายบริหารระดับสูงและคณะกรรมการว่าโครงการใดที่พวกเขาเต็มใจจะยกเลิกเพื่อให้ทรัพยากรว่างพอสำหรับการเปลี่ยนแปลง

เหตุผลที่ต้องมีการปรับแผน

การเปลี่ยนแปลงในทางองค์กร ที่อาจเปลี่ยน**รูปแบบความเสี่ยง**ได้ ได้แก่:

- การซื้อหรือขายหน่วยธุรกิจหรือสินทรัพย์
- การเปลี่ยนตัวคณะกรรมการเจ้าของกิจการ หรือผู้นำองค์กร
- การเปลี่ยนแปลงกฎหมาย ข้อบังคับ หรือมาตรฐานอุตสาหกรรม ที่อาจนำมาซึ่งความเสี่ยงในการปฏิบัติตามกฎหมาย
- การเปลี่ยนแปลงโครงการเชิงกลยุทธ์ ซึ่งรวมถึงการแสวงหาโอกาสใหม่ๆ
- การค้นพบตัวชี้วัดความเสี่ยงที่คาดไม่ถึงมาก่อน
- การเปลี่ยนแปลงภายนอก เช่น การเมือง หรือพัฒนาการของสิ่งแวดล้อม
- การนำเอาระบบใหม่มาใช้

ภาคผนวก ก. มาตรฐานและแนวปฏิบัติของ IIA ที่เกี่ยวข้อง

ข้อมูลของ IIA ต่อไปนี้ ได้ถูกใช้อ้างอิงตลอดแนวปฏิบัตินี้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการนำ *มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน*ไปใช้ปฏิบัติ ขอให้ดูได้ที่**แนวทางการนำมาตรฐานไปใช้ปฏิบัติ** (Implementation Guidance – IG) ของ IIA

ประมวลจรรยาบรรณ
หลักการข้อที่ 1: คุณธรรม
หลักการข้อที่ 2: ความเที่ยงธรรม
หลักการข้อที่ 3: การรักษาความลับ
หลักการข้อที่ 4: ความสามารถในหน้าที่
มาตรฐาน
มาตรฐาน 1000 – วัตถุประสงค์ อำนาจและภาระหน้าที่
มาตรฐาน 1100 – ความเป็นอิสระและความเที่ยงธรรม
มาตรฐาน 1130 – การเสื่อมเสียความเป็นอิสระหรือความเที่ยงธรรม
มาตรฐาน 2010 – การวางแผน
มาตรฐาน 2020 – การสื่อสารและอนุมัติแผนงานตรวจสอบ
มาตรฐาน 2030 – การบริหารทรัพยากร
มาตรฐาน 2040 – นโยบายและวิธีการปฏิบัติงาน
มาตรฐาน 2050 – การประสานงานและการพึ่งพาผลงานของผู้อื่น
มาตรฐาน 2060 – การรายงานต่อผู้บริหารระดับสูงและคณะกรรมการ
มาตรฐาน 2110 – การกำกับดูแล
มาตรฐาน 2330 – การจัดทำเอกสารข้อมูล
มาตรฐาน 2440 – การเผยแพร่ผลการปฏิบัติงาน
แนวปฏิบัติ (Practice Guide)
แนวทางการตรวจสอบเทคโนโลยีระดับโลก (Global Technology Audit Guide/GTAG) “การกำกับดูแลด้านไอที” ปี 2561
แนวปฏิบัติเรื่อง “การประเมินกระบวนการบริหารความเสี่ยง” ปี 2562
แนวปฏิบัติเรื่อง “การประสานงานและการพึ่งพาผลงานของผู้อื่น: การสร้างแผนที่การให้ความเชื่อมั่น” ปี 2561
แนวปฏิบัติเรื่อง “การแสดงออกถึงหลักการสำคัญสำหรับการปฏิบัติงานวิชาชีพตรวจสอบภายใน” ปี 2562
แนวปฏิบัติเรื่อง “การวางแผนสำหรับงานที่ได้รับมอบหมาย: กำหนดวัตถุประสงค์และขอบเขต” ปี 2560
แนวปฏิบัติเรื่อง “การวางแผนสำหรับงานที่ได้รับมอบหมาย: การประเมินความเสี่ยงของการทุจริต” ปี 2560
แนวปฏิบัติเรื่อง “ตรวจสอบภายในและแนวป้องกันด่านที่สอง” ปี 2559

ภาคผนวก ข. อภิธานศัพท์

คำศัพท์ที่มีเครื่องหมายดอกจัน (*) กำกับอยู่ ได้มาจาก “ภาคอภิธานศัพท์” ของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากลของ IIA (The IIA’s International Professional Practices Framework® ฉบับปี 2560) นอกจากนั้นแล้ว แหล่งที่มาได้ระบุไว้ที่เชิงอรรถ (footnotes)

auditable unit (**หน่วยที่สามารถรับการตรวจสอบได้/หน่วยรับตรวจ**) – หัวข้อ ประเด็น โครงการ ฝ่าย กระบวนการ นิติบุคคล หน้าที่งาน หรือบริเวณอื่นใด โดยเฉพาะที่หากมีความเสี่ยงแล้วอาจทำให้มีหตุผลสมควรที่จะได้รับการตรวจสอบ[13]

board* (**คณะกรรมการ**) – คณะบุคคลในระดับสูงสุดที่ทำหน้าที่ในการกำกับดูแลองค์กร (ตัวอย่างเช่น คณะกรรมการองค์กร (Board of Directors) คณะกรรมการกำกับดูแล (Supervisory Board) หรือคณะกรรมการนโยบาย หรือทรัสตี (Board of Governors or Trustees) ซึ่งมีหน้าที่ในการสั่งการและ/หรือสอดส่องดูแลกิจกรรมขององค์กร และพิจารณาความรับผิดชอบในผลงานการบริหารของผู้บริหารระดับสูงถึงแม้การจัดระบบการกำกับดูแลอาจแตกต่างกันไปตามแต่ละขอบเขตอำนาจของแต่ละรัฐ หรือในแต่ละภาคส่วน โดยมากแล้ว คณะกรรมการจะรวมถึงสมาชิกที่ไม่ได้มีส่วนในการบริหารหากในองค์กรไม่มีคณะกรรมการแล้ว คำว่า “คณะกรรมการ” ที่ใช้ในมาตรฐานนี้จะหมายถึง กลุ่มคนหรือบุคคลที่ทำหน้าที่กำกับดูแลองค์กรนอกจากนั้น คำว่า “คณะกรรมการ” ที่ใช้ในมาตรฐานนี้ อาจหมายถึง คณะหรือองค์คณะอื่นใดที่ทางองค์คณะซึ่งมีหน้าที่กำกับดูแลได้มอบหมายหน้าที่บางอย่างให้ (เช่น คณะกรรมการตรวจสอบ)

chief audit executive* (**หัวหน้าหน่วยงานตรวจสอบภายใน**) – คำว่า หัวหน้าหน่วยงานตรวจสอบภายใน จะหมายถึง บทบาทของบุคคลซึ่งอยู่ในตำแหน่งงานที่อยู่ในระดับสูง ซึ่งรับผิดชอบในการบริหารหน่วยงานตรวจสอบภายในให้มีประสิทธิผลโดยสอดคล้องกับกฎบัตรของหน่วยงานตรวจสอบภายใน และ องค์ประกอบส่วนที่เป็นภาคบังคับของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล หัวหน้าหน่วยงานตรวจสอบภายใน หรือบุคคลที่ต้องรายงานต่อหัวหน้าหน่วยงานตรวจสอบภายใน ควรมีประกาศนียบัตรทางวิชาชีพและคุณสมบัติที่เหมาะสม อย่างไรก็ตามชื่อตำแหน่งและ/หรือภาระหน้าที่สำหรับหัวหน้าหน่วยงานตรวจสอบภายใน อาจแตกต่างกันในแต่ละองค์กร

compliance* (**การปฏิบัติตามกฎระเบียบ**) – การยึดถือและปฏิบัติตามนโยบาย แผนงาน วิธีการปฏิบัติงาน กฎหมาย ระเบียบข้อบังคับ สัญญา ตลอดจนข้อกำหนดอื่นๆ

13. Wright, หนังสือ *The Internal Auditors Guide*, หน้า 149.

consulting services* (**การบริการให้คำปรึกษา**) – กิจกรรมการให้คำปรึกษา แนะนำ และบริการที่เกี่ยวเนื่องแก่ผู้รับบริการ โดยลักษณะและขอบเขตของงานจะเป็นไปตามข้อตกลงที่ทำขึ้นร่วมกันกับผู้รับบริการโดยมุ่งหมายที่จะเพิ่มคุณค่าและปรับปรุงกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุมขององค์กร โดยผู้ตรวจสอบภายในต้องไม่เข้าไปรับภาระหน้าที่ในทางการบริหาร ตัวอย่าง ได้แก่ การให้คำปรึกษา คำแนะนำ การอำนวยความสะดวก และการฝึกอบรม

control processes* (**กระบวนการควบคุม**) – นโยบาย วิธีการปฏิบัติ (ทั้งที่ทำด้วยมือหรือโดยระบบอัตโนมัติ) และกิจกรรมต่างๆ ขององค์กรซึ่งเป็นส่วนหนึ่งของกรอบโครงสร้างการควบคุมที่ได้รับการออกแบบมาและใช้ปฏิบัติจริง เพื่อที่จะเชื่อมั่นได้ว่าความเสี่ยงได้ถูกจำกัดให้อยู่ในระดับที่ยอมรับได้

engagement* (**งานที่ได้รับมอบหมาย**) – งานตรวจสอบภายในหรือกิจกรรมการสอบทานที่ได้รับมอบหมายให้ทำแต่ละงาน ตัวอย่างเช่น งานตรวจสอบภายใน งานสอบทานการประเมินการควบคุมด้วยตนเอง (Control Self-Assessment หรือ CSA) การตรวจสอบการทุจริต หรืองานบริการให้คำปรึกษา งานที่ได้รับมอบหมาย อาจประกอบด้วยงานย่อยๆ หลายๆ งานหรือหลายๆ กิจกรรมที่ออกแบบมาเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวข้องชุดใดชุดหนึ่งโดยเฉพาะ

fraud* (**การทุจริต**) – การกระทำผิดกฎหมายใดๆ ที่มีลักษณะของการฉ้อฉลหลอกลวง ปกปิด หรือทำลายความเชื่อมั่น การกระทำเหล่านี้ไม่จำเป็นต้องเป็นการคุกคามโดยใช้ความรุนแรงหรือการใช้กำลังบังคับ การทุจริตอาจกระทำโดยกลุ่มบุคคลและองค์กร เพื่อให้ได้มาซึ่งเงินทองทรัพย์สินหรือบริการ เพื่อเลี่ยงการจ่ายเงินหรือการสูญเสียบริการ หรือเพื่อปกป้องผลประโยชน์ของบุคคลหรือผลประโยชน์ทางธุรกิจ

governance* (**การกำกับดูแล**) – การผสมผสานของกระบวนการและโครงสร้างต่างๆ ที่คณะกรรมการนำมาใช้เพื่อบอกกล่าว สั่งการ บริหาร และเฝ้าติดตามกิจกรรมต่างๆ ภายในองค์กรเพื่อให้บรรลุวัตถุประสงค์ขององค์กร

information technology governance* (**การกำกับดูแลด้านเทคโนโลยีสารสนเทศ**) — ประกอบด้วยภาวะความเป็นผู้นำ โครงสร้างขององค์กร และกระบวนการที่สร้างความมั่นใจได้ว่า เทคโนโลยีสารสนเทศขององค์กรสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กร

internal audit activity* (**หน่วยงานตรวจสอบภายใน**) – ฝ่าย สายงาน คณะที่ปรึกษา หรือ ผู้ปฏิบัติหน้าที่อื่นๆ ที่ให้บริการการให้ความเชื่อมั่นและการให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระ ซึ่งออกแบบมาเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานขององค์กร หน่วยงานตรวจสอบภายในช่วยให้องค์กรบรรลุเป้าหมายได้ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุม อย่างเป็นระบบและเป็นระเบียบ

risk* **(ความเสี่ยง)** – ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่จะส่งผลกระทบต่อการบรรลุเป้าหมายขององค์กร ความเสี่ยงวัดได้จากผลกระทบจากเหตุการณ์และโอกาสที่จะเกิดเหตุการณ์นั้น

risks (plural) **(ความเสี่ยงต่าง ๆ)** (พหูพจน์) – "หมายถึงเหตุการณ์หนึ่งหรือมากกว่าหนึ่งเหตุการณ์ซึ่งอาจเกิดขึ้นได้ ที่อาจส่งผลกระทบถึงการบรรลุวัตถุประสงค์ได้ 'ความเสี่ยง' (เอกพจน์) หมายถึงเหตุการณ์ซึ่งอาจเกิดขึ้นทั้งหมดโดยรวมแล้วอาจจะส่งผลกระทบถึงการบรรลุวัตถุประสงค์ได้"[14]

risk appetite* **(ระดับความเสี่ยงที่ยอมรับได้)** – ระดับความเสี่ยงที่องค์กรเต็มใจที่จะยอมรับ

risk assessment (การประเมินความเสี่ยง) – การจำแนกแยกแยะและวิเคราะห์ (มักจะในแง่ของผลกระทบและโอกาสเกิด) ความเสี่ยงต่างๆ ที่เกี่ยวข้องกับการบรรลุวัตถุประสค์ขององค์กรหนึ่งๆ ซึ่งก่อให้เกิดพื้นฐานในการตัดสินใจว่า ควรจัดการความเสี่ยงต่างๆ นั้นอย่างไร[15]

risk factor (ปัจจัยเสี่ยง) – สภาพการณ์ที่สัมพันธ์กับความน่าจะเป็นและผลกระทบจากความเสี่ยงที่สูงขึ้น (ซึ่งก็คือ ตัวชี้วัดนำของการที่มีความไม่แน่นอน)[16]

risk management* **(การบริหารความเสี่ยง)** – กระบวนการในการระบุ ประเมิน จัดการ และควบคุมเหตุการณ์หรือสถานการณ์ไม่พึงประสงค์ที่อาจจะเกิดขึ้น เพื่อก่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ขององค์กร

risk profile (รูปแบบความเสี่ยง) – มุมมองความเสี่ยงโดยรวมที่ต้องแบกรับในเฉพาะบางระดับของกิจการหรือในบางแง่มุมของธุรกิจที่ทำให้ฝ่ายบริหารต้องพิจารณาถึงประเภท ความรุนแรง และความเกี่ยวโยงซึ่งกันและกันของความเสี่ยงต่างๆ และความเสี่ยงเหล่านั้นจะส่งผลกระทบต่อผลการปฏิบัติงานที่เกี่ยวกับกลยุทธ์และวัตถุประสงค์ในทางธุรกิจได้อย่างไร[17]

strategic risk (ความเสี่ยงเชิงกลยุทธ์) – ความเป็นไปได้ของการเกิดเหตุการณ์หรือสภาพการณ์ที่จะส่งเสริมหรือเป็นภัยต่อความเจริญรุ่งเรืองและความคงอยู่ขององค์กรในระยะยาว[18]

---

14. PwC for Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrating Strategy with Performance (2017),* หน้า 110.

15. Anderson, หนังสือ *Internal Auditing,* หน้า 495.

16. Wright, หนังสือ *The Internal Auditor's Guide,* หน้า 66.

17. COSO, *Enterprise Risk Management ─ Integrating Strategy and Performance (2017),* หน้า 110.

18. Wright, หนังสือ *The Internal Auditor's Guide,* หน้า 13.

ภาคผนวก ค. เชื่อมโยงวัตถุประสงค์ กลยุทธ์ และ Audit Universe

ภาพที่ ค 1: วัตถุประสงค์ในทางองค์กร กลยุทธ์ ที่เกี่ยวข้องกับ Audit Universe

วัตถุประสงค์ขององค์กร	
วัตถุประสงค์ที่ 1	.....
วัตถุประสงค์ที่ 2	.....
วัตถุประสงค์ที่ 3	.....
วัตถุประสงค์ที่ 4	.....
วัตถุประสงค์ที่ 5	.....
วัตถุประสงค์ที่ 6	.....

กลยุทธ์	การเชื่อมโยงกับวัตถุประสงค์	โครงการที่	การเชื่อมโยงกับ Audit Universe
กลยุทธ์ 1	วัตถุประสงค์ที่ 1, 6	1.1 1.2 1.3 1.4	การปฏิบัติงาน / พัฒนาบริการ, ไอที กฎหมาย, การเงิน, การปฏิบัติตามกฎ การกำกับดูแล การปฏิบัติงาน, ไอที
กลยุทธ์ 2	วัตถุประสงค์ที่ 1, 2, 3, 4	2.1 2.2 2.3	การปฏิบัติงาน, การเงิน การกำกับดูแล, กฎหมาย การปฏิบัติงาน
กลยุทธ์ 3	วัตถุประสงค์ที่ 4	3.1 3.2 3.3 3.4 3.5	การกำกับดูแล หน่วยงานสนับสนุน / ทรัพยากรบุคคล หน่วยงานสนับสนุน / การตลาด การปฏิบัติงาน / พัฒนาบริการ, ไอที การปฏิบัติงาน, ไอที
กลยุทธ์ 4	วัตถุประสงค์ที่ 5, 6	4.1 4.2 4.3 4.4	การกำกับดูแล, หน่วยงานสนับสนุน / การตลาด การกำกับดูแล, การบริหารความเสี่ยง หน่วยงานสนับสนุน / จัดซื้อ หน่วยงานสนับสนุน / บริหารอาคาร

ภาคผนวก ง. การประเมินความเสี่ยง: แนวทางสำหรับความเสี่ยงเฉพาะอย่าง

ขั้นตอนที่ 1. กำหนดมาตราส่วนการวัดและเกณฑ์วัดความเสี่ยง

แนวทางสำหรับความเสี่ยงเฉพาะอย่าง (specific-risk approach) ตามตัวอย่างนี้ ขั้นตอนแรก ก็คือต้องกำหนดเกณฑ์ที่จะใช้จัดอันดับความเสี่ยงแต่ละตัว ในแง่ของผลกระทบและโอกาสเกิด เกณฑ์สามเกณฑ์ที่เลือกมาสำหรับตัวอย่างนี้ คือ ด้านกฎหมาย ด้านการปฏิบัติงาน และด้านการเงิน ผลกระทบจะถูกให้คะแนนตั้งแต่ 5 ซึ่งหมายถึง หายนะ ไปจนถึง 1 ซึ่งหมายถึง ต่ำ โอกาสเกิดจะถูกจัดอันดับตามมาตราส่วนตั้งแต่ 5 ซึ่งหมายถึง สูงมาก ไปจนถึง 1 ซึ่งหมายถึง ต่ำมาก

ภาพที่ ง.1: มาตราส่วนและเกณฑ์ของผลกระทบจากความเสี่ยง

คำอธิบายผลกระทบ	คะแนนผลกระทบ	เกณฑ์ด้านกฎหมาย	เกณฑ์ด้านการปฏิบัติงาน	เกณฑ์ด้านการเงิน
หายนะ	5	สภาพแวดล้อมที่ซับซ้อน มีการควบคุมจากทางการสูงด้วยการบังคับใช้กฎหมายอย่างเข้มงวด ผลกระทบจากการไม่ปฏิบัติตามกฎระเบียบน่าจะส่งผลให้เกิดภาระหนี้สินทางกฎหมายและค่าปรับ ซึ่งอาจส่งผลให้ต้องปิดโรงงานทั้งหมดหรือบางส่วน มีผลกระทบด้านการเงินและด้านชื่อเสียงอย่างมีนัยสำคัญ	หน่วยธุรกิจหนึ่งหน่วยหรือมากกว่านั้น หรือทั้งองค์กรอาจจะไม่สามารถดำเนินงานได้ ผลกระทบต่อชื่อเสียง	มากกว่า 25 ล้านเหรียญ
มีนัยสำคัญสูง	4	สภาพแวดล้อมที่อยู่ภายใต้กฎหมายที่ซับซ้อน ภาระหนี้สินทางกฎหมายและค่าปรับจากการไม่ปฏิบัติตามกฎหมายอาจจะเป็นจุดสนใจของสาธารณชน และจะมีผลกระทบด้านการเงินและชื่อเสียงอย่างยาวนาน	หลายๆ หน่วยธุรกิจอาจได้รับผลกระทบ ความสามารถขององค์กรในการดำเนินงานหรือให้บริการอาจลดลงเป็นอย่างมาก ผลกระทบต่อชื่อเสียง	10 ถึง 25 ล้านเหรียญ
มีนัยสำคัญ	3	มีการบังคับใช้กฎหมายและข้อกำหนดต่างๆ อย่างสม่ำเสมอ ภาระหนี้สินทางกฎหมายและค่าปรับจากการไม่ปฏิบัติตามกฎหมายมีสาระสำคัญ (material)	หนึ่งหน่วยธุรกิจหรือมากกว่านั้นอาจได้รับผลกระทบอย่างมีสาระสำคัญ ความสามารถขององค์กรในการดำเนินงานหรือให้บริการอาจลดลงอย่างมีนัยสำคัญผลกระทบต่อชื่อเสียง	5 ถึง 10 ล้านเหรียญ (มีสาระสำคัญ)
ปานกลาง	2	สภาพแวดล้อมการกำกับดูแลจากทางการที่แข็งขัน มีการเก็บค่าปรับเพียงเล็กน้อยถึงปานกลางสำหรับการไม่ปฏิบัติตามกฎหมาย	ประสิทธิผลและประสิทธิภาพในการดำเนินงานเสียหายปานกลาง	1 ถึง 5 ล้านเหรียญ
ต่ำ	1	สภาพแวดล้อมทางกฎหมายยังหละหลวม หรือค่าปรับสำหรับการไม่ปฏิบัติตามกฎหมายเป็นจำนวนน้อยมาก	ประสิทธิผลหรือประสิทธิภาพในการดำเนินงานยังสามารถปรับปรุงได้ แต่การปฏิบัติงานต่างๆ ยังคงดำเนินไปได้อย่างต่อเนื่อง	น้อยกว่า 1 ล้านเหรียญ

ภาพที่ ง.2: มาตราส่วนของโอกาสเกิดความเสี่ยง และคำอธิบาย

อันดับ	คะแนน	คำอธิบาย	เกณฑ์
สูงมาก	5	โอกาสเกิดความเสี่ยงค่อนข้างสูงมาก	กระบวนการปฏิบัติงานซับซ้อนและวิธีการควบคุมไม่มีประสิทธิผล
สูง	4	โอกาสเกิดความเสี่ยงค่อนข้างสูง	กระบวนการปฏิบัติงานซับซ้อนและมีการสังเกตเห็นจุดอ่อนของการควบคุมบางจุด
ปานกลาง	3	โอกาสเกิดความเสี่ยงค่อนข้างปานกลาง	กระบวนการปฏิบัติงานค่อนข้างซับซ้อน มีการสังเกตเห็นจุดอ่อนของการควบคุมเพียงเล็กน้อย
ต่ำ	2	โอกาสเกิดความเสี่ยงค่อนข้างต่ำ	กระบวนการปฏิบัติงานไม่ซับซ้อน วิธีการควบคุมต่างๆ มีประสิทธิผล
ต่ำมาก	1	โอกาสเกิดความเสี่ยงค่อนข้างต่ำมาก	กระบวนการปฏิบัติงานไม่ซับซ้อน วิธีการควบคุมต่างๆ มีประสิทธิผล

ขั้นตอนที่ 2. แจงรายการหน่วยรับตรวจตามแนวตั้งและความเสี่ยงเฉพาะตามแนวนอน แล้วจัดอันดับผลกระทบและโอกาสเกิดสำหรับความเสี่ยงแต่ละตัวสำหรับแต่ละหน่วยรับตรวจ

รูปภาพที่ ง.3 แสดงถึงตัวอย่างที่ได้กำหนดขึ้นเอง โดยที่มีหน่วยรับตรวจแต่ละหน่วยในแถวแนวนอน และมีความเสี่ยงแต่ละตัวในหนึ่งคอลัมน์ ในแต่ละคอลัมน์ของความเสี่ยงจะแบ่งย่อยออกเป็น ค่าของผลกระทบและโอกาสเกิดที่เป็นของแต่ละหน่วยรับตรวจโดยเฉพาะ ค่าที่ปรากฏในตารางนี้ไม่ได้มีการถ่วงน้ำหนัก ดังนั้น ค่าผลกระทบและโอกาสเกิดสำหรับความเสี่ยงแต่ละตัวในแต่ละหน่วยรับตรวจจึงได้ถูกบวกรวมเข้าด้วยกันเพื่อให้ได้ค่าความเสี่ยงรวมสำหรับหน่วยรับตรวจนั้น ค่าคะแนนความเสี่ยงรวมจะบ่งชี้ระดับความเสี่ยงที่สัมพันธ์กันสำหรับแต่ละหน่วยรับตรวจ ตัวอย่างนี้เป็นเพียงตัวอย่างที่ทำให้เข้าใจได้ง่าย แต่ในทางปฏิบัติจริงรูปแบบตารางจะแตกต่างกันไปมาก และโดยทั่วไปแล้วควรให้น้ำหนักกับผลกระทบให้มากกว่าโอกาสเกิด

ภาพที่ ง.3: แนวทางความเสี่ยงเฉพาะ พร้อมค่าคะแนนความเสี่ยงรวม

L= Likelihood I= Impact	ความเสี่ยง 1		ความเสี่ยง 2		ความเสี่ยง 3		ความเสี่ยง 4		ความเสี่ยง 5		ความเสี่ยง 6		ความเสี่ยง 7		ความเสี่ยง 8		คะแนนรวม	ระดับ
	L	I	L	I	L	I	L	I	L	I	L	I	L	I	L	I		
หน่วยรับตรวจที่ 1	3	2	2	4	3	5	2	3	1	5	1	3	1	2	2	5	44	M
หน่วยรับตรวจที่ 2	2	3	1	4	1	5	2	2	1	3	1	1	2	3	2	2	35	M
หน่วยรับตรวจที่ 3	1	3	1	3	2	3	3	3	2	1	1	1	3	4	1	4	36	M
หน่วยรับตรวจที่ 4	4	4	3	5	2	5	1	2	1	5	3	2	2	5	2	5	51	H
หน่วยรับตรวจที่ 5	1	3	2	4	3	4	3	3	4	4	2	4	2	5	1	4	49	H
หน่วยรับตรวจที่ 6	1	1	1	2	2	1	1	3	2	1	2	2	2	3	1	2	27	L
หน่วยรับตรวจที่ 7	4	5	4	5	4	5	4	4	4	5	4	5	3	5	3	5	69	E
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
การจัดอันดับสำหรับช่วงค่าคะแนน																		
ต่ำ (L)= 0 ถึง 32			ปานกลาง (M) = 33 ถึง 45						สูง (H) = 46 ถึง 59						สูงสุด (E) = 60+			

ขั้นที่ 3. ให้คะแนนประสิทธิผลของการบริหารความเสี่ยงและวิธีการควบคุม

ภาพที่ ง.4: เกณฑ์ในการประเมินกระบวนการบริหารความเสี่ยงและวิธีการควบคุม

การประเมินการออกแบบ	เกณฑ์สำหรับการบริหารความเสี่ยงและกระบวนการควบคุม
พอเพียง	▪ กระบวนการการบริหารความเสี่ยง การควบคุม และการกำกับดูแล กำลังทำงานอย่างมีประสิทธิผล อาจมีประสิทธิภาพ หรือยังพอมีสิ่งที่จะปรับปรุงได้อีกเพื่อเพิ่มประสิทธิภาพ ▪ มีการกำหนดผู้เป็นเจ้าของความเสี่ยงไว้อย่างชัดเจนและยังคงปฏิบัติหน้าที่อยู่ ▪ ฝ่ายบริหารแก้ไขข้อบกพร่องในการควบคุมหรือประเด็นอื่นๆ ที่ตรวจพบโดยผู้ตรวจสอบและทางการผู้กำกับดูแล ▪ ผู้บริหารระบุและบรรเทาความเสี่ยงในเชิงรุก (proactive)
จำเป็นต้องปรับปรุง	▪ กระบวนการบริหารความเสี่ยงและการควบคุมบางกระบวนการกำลังทำงานอย่างมีประสิทธิผล แต่มีหลายๆ กระบวนการที่ไม่ได้จัดทำเอกสารหรือเฝ้าติดตามประเมินผล ▪ ความเสี่ยงหลักๆ ส่วนใหญ่ได้รับการบรรเทาให้อยู่ในระดับที่ยอมรับได้ ▪ ความเสี่ยงแค่บางตัวที่มีเจ้าของ
ไม่พอเพียง	▪ กระบวนการการบริหารความเสี่ยงและวิธีการควบคุมได้รับการออกแบบมาอย่างไม่เหมาะสม นำไปดำเนินการอย่างไม่คงเส้นคงวา หรือไม่มีอยู่ ▪ ไม่ได้ทำเอกสารข้อมูลความเสี่ยง และความเสี่ยงต่างๆ ไม่ได้รับการแก้ไขอย่างเต็มที่ ▪ การบริหารความเสี่ยงเป็นไปในเชิงรับ (reactive)

ขั้นที่ 4. การหาความเสี่ยงที่เหลืออยู่

การประเมินความเสี่ยงตามธรรมชาติ ประสิทธิผลของการควบคุม และความเสี่ยงที่เหลืออยู่ อาจแสดงได้เป็นแผนภูมิ (หรือเมทริกซ์) ซึ่งมีคอลัมน์หนึ่งที่กำหนดระดับความเสี่ยงในรูปของความเสี่ยงตามธรรมชาติ คอลัมน์หนึ่งกำหนดระดับประสิทธิผลของการตอบโต้ความเสี่ยงและวิธีการควบคุมที่เกี่ยวข้องกัน และอีกคอลัมน์หนึ่งสำหรับระดับความเสี่ยงที่เหลืออยู่ของแต่ละหน่วย รูปภาพที่ ง.5 แสดงตัวอย่างของตาราง

ภาพที่ ง.5: การหาความเสี่ยงที่เหลืออยู่

หน่วยรับตรวจ	ระดับความเสี่ยงตามธรรมชาติ	ประสิทธิผลของการควบคุม	ระดับความเสี่ยงที่เหลืออยู่
หน่วยรับตรวจที่ 1	ปานกลาง	จำเป็นต้องปรับปรุง	ปานกลาง
หน่วยรับตรวจที่ 2	ปานกลาง	พอเพียง	ต่ำ
หน่วยรับตรวจที่ 3	ปานกลาง	ไม่พอเพียง	สูง
หน่วยรับตรวจที่ 4	สูง	พอเพียง	ต่ำ
หน่วยรับตรวจที่ 5	สูง	จำเป็นต้องปรับปรุง	สูง
หน่วยรับตรวจที่ 6	ต่ำ	พอเพียง	ต่ำ
หน่วยรับตรวจที่ 7	สูงมาก	จำเป็นต้องปรับปรุง	สูงมาก
...	...	...	...

ภาคผนวก จ. ตัวอย่าง: การประเมินความเสี่ยงตามแนวทางการใช้ปัจจัยเสี่ยง (Risk Factor Approach)

ภาพที่ จ.1: ตัวอย่างของการกำหนดปัจจัยเสี่ยง เกณฑ์ และการจัดอันดับ

ชื่อปัจจัยเสี่ยง	ข้อพิจารณา / เกณฑ์	การจัดอันดับและคำอธิบาย
ความสูญเสีย / ปัจจัยเสี่ยงที่มีสาระสำคัญ	▪ มูลค่าความเสี่ยงที่เป็นตัวเงิน (value at risk) ▪ ค่าใช้จ่ายในการดำเนินงาน ▪ จำนวนรายการ ▪ ผลกระทบต่อบริเวณอื่นในองค์กร ▪ ระดับการพึ่งพาไอที	5 = ปัจจัยเสี่ยงสูง 4 = ปัจจัยเสี่ยงสูงกว่าค่าเฉลี่ย 3 = ปัจจัยเสี่ยงโดยเฉลี่ย 2 = ปัจจัยเสี่ยงต่ำกว่าค่าเฉลี่ย 1 = ปัจจัยเสี่ยงน้อยมาก
ความเสี่ยงเชิงกลยุทธ์	▪ การรับรู้ของสาธารณชน / ชื่อเสียง ▪ สภาพเศรษฐกิจในประเทศ ▪ ความผันผวน ▪ ความมีนัยสำคัญต่อกลยุทธ์ ▪ ระดับของกฎระเบียบจากภายนอก ▪ การเปลี่ยนแปลงในกฎระเบียบข้อบังคับหรือการตรวจสอบจากทางการ ▪ การเปลี่ยนแปลงในสายธุรกิจหรือบริการ ▪ สัญญาที่ทำใหม่ที่มีนัยสำคัญ	5 = เสี่ยงสูง 4 = เสี่ยงสูงกว่าค่าเฉลี่ย 3 = เสี่ยงโดยเฉลี่ย 2 = เสี่ยงต่ำกว่าค่าเฉลี่ย 1 = เสี่ยงน้อยมาก
สภาพแวดล้อมการควบคุม (CE)	▪ ระดับความโดดเดี่ยวของกระบวนการ ▪ ระดับของความเป็นทางการและความสอดคล้องกับวัตถุประสงค์ ▪ การนำกระบวนการ / ระบบใหม่มาใช้ ▪ กระบวนการภายในองค์กร หรือว่าจ้างกลุ่มบุคคลที่สาม ▪ อัตราการเข้าออกของผู้บริหารระดับปฏิบัติการ ▪ มีระดับของการเฝ้าติดตามประเมินผลการปฏิบัติงานอยู่ ▪ ทัศนคติที่สื่อจากฝ่ายบริหาร ▪ ความเป็นทางการของกระบวนการ / วิธีปฏิบัติงาน ▪ ผลกระทบต่อลูกค้า	5 = เสี่ยงสูง (CE อ่อนแอมาก) 4 = เสี่ยงสูงกว่าค่าเฉลี่ย (CE อ่อนแอ) 3 = โดยเฉลี่ย (CE โดยเฉลี่ย) 2 = เสี่ยงต่ำกว่าค่าเฉลี่ย (CE แข็งแรง) 1 = เสี่ยงต่ำ (CE แข็งแกร่งมาก)
ความซับซ้อน	▪ ระดับการใช้ระบบอัตโนมัติ ▪ ระดับของความเชี่ยวชาญพิเศษที่ต้องใช้ในการปฏิบัติงาน ▪ ระดับของรายละเอียดทางเทคนิค ▪ ความซับซ้อนของโครงสร้าง / สถาปัตยกรรมที่เกี่ยวข้อง ▪ ความถี่ของการเปลี่ยนแปลง	5 = ความซับซ้อนสูง 4 = ความซับซ้อนสูงกว่าค่าเฉลี่ย 3 = ความซับซ้อนโดยเฉลี่ย 2 = ซับซ้อนต่ำกว่าค่าเฉลี่ย 1 = เรียบง่าย

ภาพที่ จ.1: ตัวอย่างของการกำหนดปัจจัยเสี่ยง เกณฑ์ และการจัดอันดับ (ต่อ)

ชื่อปัจจัยเสี่ยง	ข้อพิจารณา / เกณฑ์	การจัดอันดับและคำอธิบาย
ความครอบคลุมในการให้ความเชื่อมั่น	▪ ประเภทของงานตรวจสอบที่ได้รับมอบหมาย ▪ การตรวจสอบอื่นๆ (การตรวจสอบจากภายนอกทางการ) ▪ ความครอบคลุมในด้านที่สอง ▪ มีการติดตามผลอยู่แล้ว	5 = ไม่ได้ถูกสอบทานมา 4 ปีแล้ว (3 ปีสำหรับการปฏิบัติตามกฎ หรือความเสี่ยงที่มีผลกระทบสูง) 4 = ไม่ได้ถูกสอบทานมา 3 - 4 ปีแล้ว (2-3 ปีสำหรับการปฏิบัติตามกฎ หรือความเสี่ยงที่มีผลกระทบสูง) 3 = ได้รับการสอบทาน 2 - 3 ปีมาแล้ว (1-2 ปีสำหรับการปฏิบัติตามกฎ หรือความเสี่ยงที่มีผลกระทบสูง) 2 = ได้รับการสอบทาน 1 - 2 ปีมาแล้ว (1 ปีสำหรับการปฏิบัติตามกฎ ผลกระทบสูง) 1 = ได้รับการสอบทานในปีที่แล้ว หรือกำลังมีความคิดที่จะตรวจในปัจจุบัน
ความตระหนักรู้ของผู้บริหาร	▪ ความกังวลที่ตอบกลับมาในแบบสำรวจ ▪ ความกังวลที่ตอบมาในการสัมภาษณ์ ▪ ระดับความตระหนักรู้ในเรื่องความเสี่ยง	5 = ความกังวลของผู้บริหารมีประเด็นและเหตุผลเฉพาะ 4 = ความกังวลของผู้บริหารเป็นเรื่องทั่วไป 3 = ผู้บริหารรู้สึกกลางๆ 2 = ผู้บริหารไม่มีข้อกังวลที่เจาะจง 1 = ผู้บริหารสามารถแสดงออกถึงการควบคุมความเสี่ยงที่มีประสิทธิผลได้

ภาพที่ จ.2: ตัวอย่างของการหาค่าคะแนนความเสี่ยงรวม

	ปัจจัยเสี่ยงที่เกี่ยวกับผลกระทบ			ปัจจัยเสี่ยงที่เกี่ยวกับโอกาสเกิด					
หน่วยรับตรวจ	**ความสูญเสีย/ปัจจัยเสี่ยงที่มีสาระสำคัญ**	**ความเสี่ยงเชิงกลยุทธ์**	**ยอดรวมย่อย**	**สภาพแวดล้อมการควบคุม (CE)**	**ความซับซ้อน**	**ความครอบคลุมในการให้ความเชื่อมั่น**	**ความตระหนักรู้ของผู้บริหาร**	**ยอดรวมย่อย**	**ยอดรวมค่าคะแนนความเสี่ยงทั้งหมด**
ถ่วงน้ำหนัก	*50%*	*50%*		*35%*	*35%*	*20%*	*10%*		
หน่วยที่ 1	1	2	1.5	2	1	3	1	1.75	3.25
หน่วยที่ 2	5	5	5	3	1	5	1	2.5	7.5
หน่วยที่ 3	1	5	3	4	5	4	2	4.15	7.15
หน่วยที่ 4	5	5	5	5	4	5	4	4.55	9.55
หน่วยที่ 5	5	2	3.5	4	2	2	4	2.9	6.4
...	...	...	...	...	...	...	...	...	...

ดัชนีคะแนนความเสี่ยงทั้งหมด	2 ถึง 4 = ต่ำ	4.1 ถึง 6.5 = ปานกลาง	6.6 ถึง 8.5 = สูง	8.6 ถึง 10 = สูงมาก

สเกลการจัดอันดับ: 1 คือ ต่ำสุด; 5 คือ สูงสุด; ยอดรวมคะแนนต่ำสุดที่เป็นไปได้ = 2; ยอดรวมคะแนนสูงสุดที่เป็นไปได้ = 10

ภาคผนวก ฉ. ตัวอย่าง: สรุปย่อแผนงานตรวจสอบภายใน

ตัวอย่างสรุปแผนงานการตรวจสอบภายในแบบง่ายๆ นี้ แสดงหน่วยรับตรวจตามแถวแนวนอน แต่ละแถวจะถูกขยายออกเพื่อใส่ข้อมูลความเสี่ยงที่ชี้ถึงลำดับความสำคัญของหน่วยรับตรวจ รวมทั้งปี และไตรมาสที่จะมีการปฏิบัติงาน กำหนดเวลาตามที่เสนอสำหรับปีที่ตามมาภายหลังปีปัจจุบันนั้นสามารถเปลี่ยนแปลงได้ ทั้งนี้ ขึ้นอยู่กับการประเมินความเสี่ยงให้เป็นปัจจุบัน ในแต่ละช่องสี่เหลี่ยมที่แสดงถึงงานตรวจสอบที่ได้รับมอบหมายแต่ละงานจะถูกใส่รหัสสี โดยมีคำอธิบายที่ชี้ให้เห็นถึงประเภทของงานตรวจสอบ ตัวเลขที่อยู่ในแต่ละบล็อค แสดงถึงจำนวนชั่วโมงที่จำต้องใช้ในงาน จำนวนชั่วโมงทั้งหมดจะถูกรวมยอดไว้ด้านล่างสุดของแต่ละคอลัมน์ ซึ่งแสดงให้เห็นถึงทรัพยากรทั้งหมดที่ต้องการอย่างชัดเจน มีการคำนวณสรุปที่แสดงถึงจำนวนชั่วโมงที่ต้องใช้สำหรับงานย่อยๆ ซึ่งไม่เกี่ยวกับงานตรวจสอบที่ได้รับมอบหมาย

ภาพที่ ฉ.1: สรุปแผนงานการตรวจสอบภายในโดยอาศัยความเสี่ยงสำหรับระยะเวลาสามปี

(สามารถเปลี่ยนแปลงได้ขึ้นอยู่กับการประเมินความเสี่ยง)

ตรวจ | ตรวจบางประเด็น

การประเมินความเสี่ยงในปัจจุบัน				ปีที่มีการทบทวนที่ผ่านมา			จำนวนชั่วโมงของพนักงานที่เสนอในปีปัจจุบัน			กำหนดเวลาปฏิบัติงานที่นำเสนอสำหรับปีปัจจุบัน					กำหนดเวลาปฏิบัติงานที่นำเสนอสำหรับปีหน้า					กำหนดเวลาปฏิบัติงานที่นำเสนอสำหรับสองปีข้างหน้านับจากปี				
อันดับที่	หน่วยรับตรวจ	คะแนนความเสี่ยงที่เหลืออยู่	ลำดับความสำคัญ	สามปีมาแล้ว	สองปีมาแล้ว	ปีที่แล้ว	ผู้ให้บริการอื่น	IAA	รวม	Q1	Q2	Q3	Q4	รวมจำนวนชั่วโมงที่ใช้ของปี	Q1	Q2	Q3	Q4	รวมจำนวนชั่วโมงที่ใช้ของปี	Q1	Q2	Q3	Q4	รวมจำนวนชั่วโมงที่ใช้ของปี
1	หน่วยรับตรวจที่ 6	4.5	สูง	✓	✓		15	20	35	20	15					5	15							
2	หน่วยรับตรวจที่ 3	4.4	สูง	✓		✓	20	20	40	20	20													25	
3	หน่วยรับตรวจที่ 7	4.2	สูง	✓	✓		20	20	40		20	20			15	5									
4	หน่วยรับตรวจที่ 5	3.1	ปานกลาง	✓		✓		30	30			20	10										25		
5	หน่วยรับตรวจที่ 11	3.0	ปานกลาง		✓											30	10							
6	หน่วยรับตรวจที่ 8	2.8	ปานกลาง		✓										5	10								
7	หน่วยรับตรวจที่ 9	2.6	ปานกลาง		✓												15	15						
8	หน่วยรับตรวจที่ 1	2.2	ปานกลาง		✓											25	10							
9	หน่วยรับตรวจที่ 2	2.1	ปานกลาง			✓															10	20		
10	หน่วยรับตรวจที่ 4	1.2	ต่ำ			✓																	15	5	
11	หน่วยรับตรวจที่ 10	1.0	ต่ำ		✓																		15	5	
							55	90	145	40	55	40	10	145	20	75	50	15	160	10	20	55	35	120
บริเวณที่ไม่ใช่การตรวจ																								
1	การเตรียมการสำหรับการประชุม AC และคณะอนุกรรมการบริหารความเสี่ยง							90	90	9	7	7	7		9	7	7	7		9	7	7	7	
2	การปรับปรุงการประเมินความเสี่ยงและแผนงานการตรวจสอบภายใน							150	150		15	15	20			15	15	20			15	15	20	
3	งานให้คำปรึกษาและงานโครงการอื่นๆ							45	45	10	5				10	5				10	5			
4	การตรวจติดตามผล							240	240	20	20	20	20		20	20	20	20		20	20	20	20	
5	การฝึกอบรมพนักงาน							90	90	10	10	10			10	10	10			10	10	10		
6	ความริเริ่มทางกลยุทธ์						20	125	145	20	20	0	25		10	10	10	10		10	10	10	10	
7	งานที่ยกยอดไป							30	30	10					10					10				
8	การประกันคุณภาพ							45	45				15					15					15	
จำนวนชั่วโมงทำงานที่ต้องใช้ทั้งหมดใน 1 ปี							75	905	980	119	132	92	97	440	89	142	112	87	430	79	87	117	107	390

ภาคผนวก ช. ภาพรวมของเอกสารตรวจสอบภายใน

การบันทึกข้อมูลที่ได้มาในแต่ละระยะของการวางแผนนั้น เป็นส่วนหนึ่งของแนวทางที่เป็นระบบระเบียบซึ่งบ่งบอกความเป็นหน่วยงานตรวจสอบภายใน ผู้ตรวจสอบภายในและ CAE อาจจะจัดทำเอกสารดังต่อไปนี้แล้วรวบรวมให้เป็นพื้นฐานที่สนับสนุนแผนงานการตรวจสอบภายในได้อย่างครอบคลุมและสอดประสานกัน

ภาพที่ ช.1: เอกสารของตรวจสอบภายในที่เกี่ยวกับแต่ละระยะของการวางแผน

ระยะของการวางแผน	เอกสารของตรวจสอบภายใน
เข้าใจองค์กร	▪ กฎบัตรของตรวจสอบภายใน ที่บันทึกความคาดหวังของฝ่ายบริหารและคณะกรรมการ และข้อกำหนดต่างๆ ที่ตรวจสอบภายในต้องปฏิบัติสอดคล้องกับ IPPF รวมทั้งการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับต่างๆ และข้อกำหนดในอุตสาหกรรมด้วย ▪ กรอบการบริหารความเสี่ยงขององค์กร (ประเภทความเสี่ยง และความเสี่ยงแต่ละตัวพร้อมทั้งคำอธิบาย) ▪ ทะเบียนที่ครอบคลุมความเสี่ยงทั้งหมด (risk universe)
ระบุ ประเมิน และจัดลำดับความสำคัญความเสี่ยง	▪ Audit universe ที่แสดงรายการของหน่วยรับตรวจ ▪ บันทึกเกี่ยวกับการระดมสมองและการประเมินความเสี่ยงใหม่ๆ และความเสี่ยงของการทุจริต ▪ การประเมินความเสี่ยงรวมทั้งการวิเคราะห์ความมีนัยสำคัญของความเสี่ยง ▪ รายการปัจจัยเสี่ยงพร้อมคำบรรยายและการวัดค่า ▪ แผนผัง / เมทริกซ์ ความเสี่ยงและการควบคุม ซึ่งแสดงถึงการจัดอันดับความเสี่ยงต่างๆ ▪ ฮีทแมพ (Heat map) ▪ อันดับของหน่วยรับตรวจเพื่อบรรจุในแผน ▪ เกณฑ์สำหรับลำดับความสำคัญและความถี่ของการตรวจสอบโดยขึ้นอยู่กับความเสี่ยงที่เหลืออยู่
การประสานงานกับผู้ให้บริการอื่น	▪ แผนที่การให้ความเชื่อมั่น (Assurance map)

ระยะของการวางแผน	เอกสารของตรวจสอบภายใน
ประมาณการทรัพยากร	▪ แผนการรับพนักงาน ซึ่งรวมถึง ○ ทะเบียนรายการทักษะของพนักงานที่มีอยู่ ○ การคาดคะเนถึงทักษะที่จำเป็นเพื่อให้งานสำเร็จ ○ บันทึกสมมติฐานและการคาดคะเน ○ สรุปจำนวนชั่วโมงของคนที่ต้องทุ่มให้กับหน้าที่งานที่ไม่ใช่งานตรวจสอบและงานย่อยๆ
นำเสนอแผนและขอความคิดเห็น	▪ วาระและรายงานการประชุม ▪ บันทึกช่วยจำสำหรับการประชุมที่ไม่เป็นทางการ ▪ แบบสำรวจ
สรุปและสื่อสารแผน	▪ หน่วยรับตรวจใน audit universe ▪ อันดับของความเสี่ยงตามธรรมชาติและความเสี่ยงที่เหลืออยู่ของแต่ละหน่วยรับตรวจ ▪ ตัวบ่งชี้ (Descriptor) ซึ่งชี้ให้เห็นถึงความสำคัญของงานตรวจสอบของแต่ละหน่วยรับตรวจ ▪ กำหนดเวลาของงานต่างๆ (หลายๆ ปี และระยะสั้น ตามปีปฏิทิน) ▪ ขอบเขตและวัตถุประสงค์งานที่เสนอ ▪ ชั่วโมงคนทำงานและทรัพยากรที่จำเป็นสำหรับงานแต่ละงาน ▪ การมอบหมายงานให้แก่พนักงาน ▪ สรุปทรัพยากร: จำนวนชั่วโมงคนที่ใช้ทั้งหมด และจำนวนงานที่ได้รับมอบหมายต่อปี
ประเมินความเสี่ยงอย่างต่อเนื่อง	▪ ประเมินความเสี่ยงเป็นรายไตรมาส และ/หรือ เทคโนโลยีที่สามารถช่วยในการอัพเดทจากการเฝ้าระวังความเสี่ยง
ปรับปรุงแผนให้เป็นปัจจุบัน และสื่อสารการปรับปรุงนั้น	▪ กฎบัตรการตรวจสอบภายในที่ระบุเกณฑ์ของการเปลี่ยนแปลงต่างๆ ที่ต้องมีการสื่อสาร

ภาคผนวก ซ. อ้างอิงและอ่านเพิ่มเติม

อ้างอิง

Wright, Rick A., Jr. Internal Auditor's Guide to Risk Assessment. 2nd ed. Lake Mary, FL: Internal Audit Foundation. 2018. https://bookstore.theiia.org/the-internal-auditors-guide-to-risk-assessment-2nd-edition

Urton L. Anderson, Michael J. Head, Sridhar Ramamoorti, Cris Riddle, Mark Salamasick, and Paul J. Sobel. Internal Auditing: Assurance and Advisory Services, 4th ed. Lake Mary, FL: Internal Audit Foundation. 2017. https://bookstore.theiia.org/internal-auditing-assurance-advisory-services-fourth-edition-2

อ่านเพิ่มเติม

แนวปฏิบัติจาก Committee of Sponsoring Organizations of the Treadway Commission (COSO)

- Enterprise Risk Management — Integrating Strategy and Performance. 2017. https://www.coso.org/Pages/erm.aspx
- Internal Control – Integrated Framework. 2013. https://www.coso.org/Pages/ic.aspx

แหล่งข้อมูลจาก ISACA

- COBIT 2019 Framework: Introduction and Methodology. https://www.isaca.org/resources/cobit
- COBIT 2019 Framework: Governance and Management Objectives. https://www.isaca.org/resources/cobit
- The Risk IT Framework. https://www.isaca.org/bookstore/bookstore-risk-digital/writf

กิตติกรรมประกาศ

ทีมพัฒนาแนวปฏิบัติ (Guidance Development Team)

Alp Buluc, CIA, CCSA, CRMA, Turkey

David Dominguez, CIA, CRMA, United States

Susan Haseley, United States

Charlotta Hjelm, CIA, QIAL, Sweden

Hazem Keshk, CIA, CRMA, Canada

Suzan Sgaier, CIA, United States

Faris Theyab, CIA, United Arab Emirates

ผู้ให้คำแนะนำจากทั่วโลก (Global Guidance Contributors)

Awad Elkarim Mohamed Ahmed, CIA, CCSA, CRMA, United Arab Emirates

Travis Finstad, United States

Renee Jaenicke, CIA, United States

James Paterson, CIA, United Kingdom

IIA Global Standards and Guidance

Anne Mercer, CIA, CFSA, Director (Project Lead)

Jim Pelletier, CIA, CGAP, Vice President

Cassian Jae, Managing Director

Michael Padilla, CIA, Director

Christopher Polke, CGAP, Director

Jeanette York, CCSA, Director

Shelli Browning, Technical Editor

Lauressa Nelson, Technical Editor

Vanessa Van Natta, Standards and Guidance Specialist

ทาง IIA ขอขอบคุณหน่วยงานกำกับดูแลต่อไปนี้สำหรับการสนับสนุน: คณะกรรมการพัฒนาแนวปฏิบัติ (Guidance Development Committee) สภาที่ปรึกษาเกี่ยวกับแนวทางปฏิบัติในทางวิชาชีพ (Professional Guidance Advisory Council) คณะกรรมการมาตรฐานการตรวจสอบภายในสากล (International Internal Audit Standards Board) คณะกรรมการกำกับดูแลหน้าที่และจริยธรรมในทางวิชาชีพ (Professional Responsibility and Ethics Committee) และสภาผู้ดูแลกรอบการปฏิบัติงานวิชาชีพสากล (International Professional Practices Framework Oversight Council)

เกี่ยวกับสมาคม

สมาคมผู้ตรวจสอบภายใน (IIA) เป็นหน่วยงานด้านการตรวจสอบภายในที่ได้รับการยอมรับอย่างกว้างขวางในการเป็นผู้ให้การสนับสนุน ผู้ให้ความรู้ และผู้กำหนดมาตรฐาน แนวทางปฏิบัติต่างๆ และวุฒิบัตรรับรองคุณวุฒิต่างๆ ที่เกี่ยวข้องกับวิชาชีพตรวจสอบภายใน สมาคมก่อตั้งขึ้นในปีพ.ศ. 2484 ในปัจจุบัน IIA ได้ให้บริการสมาชิกมากกว่า 200,000 คน จากมากกว่า 170 ประเทศและดินแดน สำนักงานใหญ่ของสมาคมตั้งอยู่ที่เลคแมรี่ (Lake Mary) มลรัฐฟลอริดา สหรัฐอเมริกา สำหรับข้อมูลเพิ่มเติมโปรดเยี่ยมชม www.globaliia.org

ข้อความปฏิเสธความรับผิดชอบ

IIA ตีพิมพ์เอกสารนี้เพื่อจุดประสงค์ในการให้ข้อมูลและเพื่อการศึกษาเท่านั้น และไม่ได้มีวัตถุประสงค์เพื่อให้คำตอบที่ชัดเจนที่สุดสำหรับสถานการณ์เฉพาะแต่ละสถานการณ์ ดังนั้น จึงมีวัตถุประสงค์เพียงเพื่อใช้เป็นแนวทางในการปฏิบัติงานเท่านั้น IIA จึงใคร่แนะนำให้ท่านขอคำปรึกษาจากผู้เชี่ยวชาญอิสระซึ่งมีความรู้เกี่ยวข้องโดยตรงกับสถานการณ์เฉพาะนั้นๆ IIA จะไม่รับผิดชอบใดๆ ต่อการที่ผู้ใดก็ตามเชื่อและอาศัยคำแนะนำนี้แต่เพียงอย่างเดียว

ลิขสิทธิ์

พฤษภาคม 2563

The Institute of Internal Auditors | Global

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org