



International Professional
Practices Framework

Supplemental Guidance Practice Guide

การวางแผนสำหรับงานที่ได้รับมอบหมาย

การกำหนดวัตถุประสงค์และขอบเขต

สารบัญ

บทสรุปผู้บริหาร.....	3
บทนำ.....	4
ขั้นตอนการวางแผนสำหรับงานที่ได้รับมอบหมาย.....	6
การทำความเข้าใจบริบทและวัตถุประสงค์ของงานที่ได้รับมอบหมาย.....	6
การรวบรวมข้อมูล.....	9
การทบทวนผลการประเมินในครั้งก่อน.....	10
การทำความเข้าใจและจัดทำแผนผังกระบวนการและการควบคุมต่างๆ.....	11
การสัมภาษณ์ผู้มีส่วนได้เสียที่เกี่ยวข้อง.....	12
การระดมความคิดเกี่ยวกับสถานการณ์ความเสี่ยงต่างๆ ที่อาจเกิดขึ้น.....	14
การจัดทำบันทึกข้อมูลที่ได้รวบรวมมา.....	14
การประเมินความเสี่ยงในเบื้องต้น.....	15
การระบุความเสี่ยงและการควบคุม: ตารางความเสี่ยงและการควบคุม.....	15
การจัดลำดับความเสี่ยง: แผนผังความเสี่ยง.....	19
การกำหนดวัตถุประสงค์ของงานที่ได้รับมอบหมาย.....	21
วัตถุประสงค์ของงานการให้ความเชื่อมั่น.....	21
วัตถุประสงค์ของงานให้คำปรึกษา.....	23
การกำหนดขอบเขตของงานที่ได้รับมอบหมาย.....	23
ขอบเขตของงานการให้ความเชื่อมั่น.....	24
ขอบเขตของงานให้คำปรึกษา.....	26
การจัดสรรทรัพยากร.....	27
การจัดทำเอกสารบันทึกแผนงาน.....	28
ภาคผนวก ก มาตรฐานของสมาคมผู้ตรวจสอบภายในที่เกี่ยวข้อง.....	30
ภาคผนวก ข ภาคอธิธานศัพท์.....	33
กิตติกรรมประกาศ.....	35

บทสรุปผู้บริหาร

การวางแผนเป็นส่วนหนึ่งของวิธีการตรวจสอบภายในอย่างเป็นระบบ เป็นระเบียบ และเป็นไปตามความเสี่ยง และได้ถูกบัญญัติไว้ใน *มาตรฐานการปฏิบัติงานวิชาชีพการตรวจสอบภายในที่เป็นสากล*. การวางแผนสำหรับงานตรวจสอบภายในที่ได้รับมอบหมายนั้นจะเกี่ยวข้องกับการพิจารณากลยุทธ์และวัตถุประสงค์ต่างๆ ของบริเวณหรือกระบวนการที่จะทำการสอบทาน การจัดลำดับความเสี่ยงต่างๆ ที่เกี่ยวข้องกับการปฏิบัติงานที่ได้รับมอบหมาย การกำหนดวัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมาย และการจัดทำเอกสารบันทึกแนวทางต่างๆ แนวปฏิบัติฉบับนี้จะประกอบด้วยขั้นตอนที่จำเป็นในการวางแผนสำหรับงานที่ได้รับมอบหมาย เพื่อให้บรรลุผลตามมาตรฐาน 2200 เรื่องการวางแผนสำหรับงานที่ได้รับมอบหมาย ไปจนถึงมาตรฐาน 2220 เรื่องขอบเขตของงานที่ได้รับมอบหมาย รวมถึงมาตรฐานด้านการนำไปใช้ปฏิบัติสำหรับการบริการให้ความเชื่อมั่น (.A) และการบริการให้คำปรึกษา (.C)

ลำดับและรายละเอียดของการวางแผนสำหรับงานที่ได้รับมอบหมาย ซึ่งรวมถึงการกำหนดวัตถุประสงค์และขอบเขต อาจมีความแตกต่างกันออกไปตามความต้องการของแต่ละองค์กร แต่หน่วยงานตรวจสอบภายในและแต่ละงานที่ได้รับมอบหมายดังกล่าว อย่างไรก็ตาม ขั้นตอนการวางแผนโดยทั่วไปมีดังนี้

- ทำความเข้าใจบริบทและวัตถุประสงค์ของงานที่ได้รับมอบหมาย
- รวบรวมข้อมูลเพื่อทำความเข้าใจบริเวณหรือกระบวนการที่จะทำการสอบทาน
- ทำการประเมินความเสี่ยงต่างๆ ที่เกี่ยวข้องในเบื้องต้น
- กำหนดวัตถุประสงค์สำหรับงานที่ได้รับมอบหมาย
- กำหนดขอบเขตสำหรับงานที่ได้รับมอบหมาย
- จัดสรรทรัพยากรอย่างเหมาะสมและเพียงพอ
- จัดทำเอกสารบันทึกแผนงาน

ในการวางแผนสำหรับงานที่ได้รับมอบหมายให้มีประสิทธิผลนั้น ผู้ตรวจสอบภายในจะต้องเริ่มจากการทำความเข้าใจบริบทและวัตถุประสงค์ของงานดังกล่าว สาเหตุที่งานดังกล่าวถูกบรรจุไว้ในแผนการตรวจสอบภายในประจำปี ตลอดจนพันธกิจ วิสัยทัศน์วัตถุประสงค์ในเชิงกลยุทธ์ และองค์ประกอบอื่นๆ ขององค์กรนั้นมีความสอดคล้องกับบริเวณหรือกระบวนการที่จะทำการสอบทานอย่างไร นอกจากนี้ ผู้ตรวจสอบภายในยังต้องพิจารณาด้วยว่างานที่ได้รับมอบหมายนั้น เป็นการร้องขอรับบริการให้ความเชื่อมั่นหรือการให้คำปรึกษา

Practice Guide / Engagement Planning: Establishing Objectives and Scope

เนื่องจากความคาดหวังของผู้มีส่วนได้เสียและข้อกำหนดของมาตรฐานนั้นมีความแตกต่างกัน ทั้งนี้ ขึ้นอยู่กับประเภทของงานที่ได้รับมอบหมายดังกล่าว

จากนั้น ผู้ตรวจสอบภายในจะต้องเก็บข้อมูลเกี่ยวกับบริเวณหรือกระบวนการที่จะทำการสอบทาน เพื่อพิจารณากำหนดวัตถุประสงค์ ขอบเขตและแผนสำหรับงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในอาจตรวจสอบเอกสารจากงานบริการให้ความเชื่อมั่นในครั้งก่อนหน้า สอบทานนโยบายและขั้นตอนการปฏิบัติงานที่ใช้บังคับ ตลอดจนสัมภาษณ์ผู้มีส่วนได้เสียที่เกี่ยวข้อง เพื่อทำความเข้าใจและจัดทำแผนผังกระบวนการและการควบคุมต่างๆ ในบริเวณหรือกระบวนการที่จะทำการสอบทาน

การประเมินความเสี่ยงต่างๆ ในเบื้องต้นจะช่วยผู้ตรวจสอบภายในในการจัดลำดับความเสี่ยงที่จะต้องประเมินในระหว่างปฏิบัติงานที่ได้รับมอบหมาย การใช้แผนผังแสดงกระบวนการ (process maps) และการระดมสมองเกี่ยวกับสถานการณ์ความเสี่ยงต่างๆ ที่อาจเกิดขึ้นเป็นเทคนิคสองอย่างที่จะช่วยผู้ตรวจสอบภายในในการระบุความเสี่ยงและวิธีการควบคุมต่างๆ ที่เกี่ยวข้องกับบริเวณหรือกระบวนการที่จะทำการสอบทาน แนวปฏิบัติฉบับนี้จะอธิบายถึงวิธีการที่ผู้ตรวจสอบภายในสามารถนำตารางความเสี่ยงและการควบคุม (Risk and Control Matrix) รวมทั้งแผนผังความเสี่ยง (Heat Map) มาใช้ในการจัดลำดับความเสี่ยง จากนั้นก็นำผลลัพธ์ที่ได้มาใช้ในการกำหนดวัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมาย ด้วยวิธีการที่สอดคล้องเป็นไปตามมาตรฐาน นอกจากนี้ แนวปฏิบัติฉบับนี้ยังจะกล่าวถึงวิธีการจัดสรรทรัพยากรต่างๆ การจัดทำบันทึกเอกสารกระบวนการวางแผน ตลอดจนการกำหนดวัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมายดังกล่าวอีกด้วย

บทนำ

การวางแผนนั้นเป็นส่วนหนึ่งของแนวทางในการปฏิบัติงานของหน่วยงานตรวจสอบภายในที่เป็นระบบ เป็นระเบียบ และอาศัยความเสี่ยงเป็นพื้นฐาน และได้มีการบัญญัติไว้ในมาตรฐาน ในมาตรฐาน 2200 เรื่องการวางแผนสำหรับงานที่ได้รับมอบหมาย ซึ่งได้กำหนดให้ผู้ตรวจสอบภายในต้องจัดทำและบันทึกแผนสำหรับงานที่ได้รับมอบหมายแต่ละงาน ดังนั้นจึงเป็นสิ่งสำคัญที่ผู้ตรวจสอบภายในจะต้องมีความเข้าใจในกระบวนการวางแผนสำหรับงานที่ได้รับมอบหมาย ซึ่งใช้โดยหน่วยงานตรวจสอบภายในขององค์กร โดยมักจะกำหนดและอธิบายไว้ในนโยบายและคู่มือการปฏิบัติงานตรวจสอบภายใน

การวางแผนสำหรับงานที่ได้รับมอบหมายจะมีความเกี่ยวข้องกับการพิจารณาถึงกลยุทธ์และวัตถุประสงค์ของบริเวณหรือกระบวนการที่จะทำการสอบทาน รวมถึงการจัดลำดับความเสี่ยงที่เกี่ยวข้องกับงานที่ได้รับ

Practice Guide / Engagement Planning: Establishing Objectives and Scope

มอบหมายนั้นๆ แผนงานจะต้องประกอบด้วยวัตถุประสงค์ ขอบเขต ระยะเวลา และการจัดสรรทรัพยากร การกำหนดวัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมายจะช่วยให้ผู้ตรวจสอบภายในมุ่งเน้นไปที่ความเสี่ยงที่มีนัยสำคัญในบริเวณหรือกระบวนการที่จะทำการสอบทาน จัดทำแนวการปฏิบัติงานสำหรับงานที่ได้รับมอบหมายและสื่อสารอย่างชัดเจนไปยังฝ่ายบริหารและคณะกรรมการ

วัตถุประสงค์ของงานที่ได้รับมอบหมายจะเป็นข้อความกว้างๆ ที่กำหนดโดยผู้ตรวจสอบภายใน ซึ่งจะเป็นตัวกำหนดถึงผลสำเร็จของงานดังกล่าวที่ได้ตั้งใจไว้ ขอบเขตจะเป็นตัวกำหนดสิ่งที่มุ่งเน้นและขอบข่ายของงานที่ได้รับมอบหมาย โดยจะระบุถึงกิจกรรม กระบวนการ ระบบงาน ช่วงเวลา และองค์ประกอบอื่นๆ ที่จะทำการสอบทาน นอกจากนี้ วัตถุประสงค์และขอบเขตยังเป็นพื้นฐานที่จะช่วยผู้ตรวจสอบภายในสามารถพิจารณา กำหนดระยะเวลา งบประมาณ และทรัพยากรที่ต้องใช้สำหรับงานที่ได้รับมอบหมายได้อีกด้วย

การที่ไม่สามารถกำหนดวัตถุประสงค์ของงานที่ได้รับมอบหมายไว้อย่างเหมาะสม จะนำมาซึ่งความเสี่ยงต่างๆ ที่ส่งผลกระทบต่อความสามารถของหน่วยงานตรวจสอบภายในที่จะดำเนินการในเรื่องต่อไปนี้

- การจัดลำดับความเสี่ยงต่างๆ ในระดับของงานที่ได้รับมอบหมายให้สอดคล้องกับความเสี่ยงขององค์กร
- การตอบสนองความคาดหวังขององค์กรและ/หรือผู้มีส่วนได้เสีย
- การปกป้องและเพิ่มคุณค่าขององค์กรโดยการให้ความเชื่อมั่น คำแนะนำและข้อมูลในเชิงลึก
- การปรับปรุงกระบวนการกำกับดูแล การบริหารความเสี่ยงและการควบคุมขององค์กร

ในทำนองเดียวกัน หากขอบเขตของงานที่ได้รับมอบหมายไม่ได้รับการกำหนดไว้อย่างเหมาะสมก่อนเริ่มปฏิบัติงาน หน่วยงานตรวจสอบภายในจะมีความเสี่ยงเกี่ยวกับความไม่มีประสิทธิภาพและความไม่เพียงพอในการดำเนินการเรื่องต่างๆ เช่น

- ไม่สามารถระบุความเสี่ยงที่มีนัยสำคัญสำหรับบริเวณหรือกระบวนการที่จะทำการสอบทาน
- ไม่สามารถมั่นใจได้ว่าฝ่ายบริหารหรือบุคลากรในบริเวณหรือกระบวนการที่จะทำการสอบทานมีความเข้าใจในขอบเขตและวัตถุประสงค์ของงานที่ได้รับมอบหมายดังกล่าว
- เกิดการทำงานซ้ำซ้อน หรือปฏิบัติงานที่ไม่เพิ่มคุณค่า
- จัดสรรทรัพยากรไม่เพียงพอต่อการปฏิบัติงานที่ได้รับมอบหมายให้แล้วเสร็จ

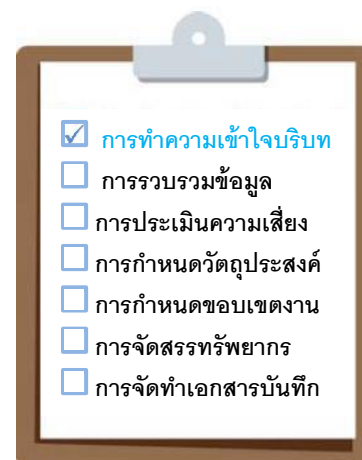
ขั้นตอนการวางแผนสำหรับงานที่ได้รับมอบหมาย

มีขั้นตอนต่างๆ ในการวางแผนมากมายที่มีส่วนช่วยในการจัดทำวัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมาย รายละเอียดโดยเฉพาะของขั้นตอนและลำดับในการปฏิบัติอาจมีการปรับเปลี่ยนให้เหมาะสมกับความต้องการของแต่ละหน่วยงานตรวจสอบภายใน แต่ละองค์กร และแต่ละงานที่ได้รับมอบหมาย ตัวอย่างเช่น หน่วยงานตรวจสอบภายในแห่งหนึ่ง อาจเริ่มต้นจากการกำหนดวัตถุประสงค์เบื้องต้นก่อนปฏิบัติขั้นตอนอื่นๆ ที่จำเป็นในอันที่จะทำให้ได้วัตถุประสงค์ที่เสร็จสมบูรณ์ อย่างไรก็ตาม การวางแผนสำหรับงานที่ได้รับมอบหมาย โดยทั่วไปแล้วมักจะประกอบด้วยขั้นตอนต่างๆ ดังนี้

- ทำความเข้าใจบริบทและวัตถุประสงค์ของงานที่ได้รับมอบหมาย
- รวบรวมข้อมูลเพื่อทำความเข้าใจกิจกรรมหรือกระบวนการที่จะทำการสอบทาน
- ทำการประเมินความเสี่ยงของกิจกรรมหรือกระบวนการที่จะทำการสอบทานในเบื้องต้น
- กำหนดวัตถุประสงค์สำหรับงานที่ได้รับมอบหมาย
- กำหนดขอบเขตสำหรับงานที่ได้รับมอบหมาย
- จัดสรรทรัพยากรต่างๆ
- จัดทำเอกสารบันทึกแผนงาน

การทำความเข้าใจบริบทและวัตถุประสงค์ของงานที่ได้รับมอบหมาย

การทำความเข้าใจบริบทและวัตถุประสงค์ของงานที่ได้รับมอบหมายจะช่วยให้ผู้ตรวจสอบภายในสามารถวางแผนได้อย่างมีประสิทธิภาพ ตลอดจนเชื่อมั่นได้ว่าเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ในแผนการตรวจสอบภายในประจำปีนั้นได้บรรลุผลสำเร็จ ผู้ตรวจสอบภายในควรเริ่มต้นจากการทำความเข้าใจแผนการตรวจสอบภายในประจำปี การวางแผนและการหารือที่นำไปสู่การจัดทำแผนดังกล่าว รวมถึงเหตุผลที่งานแต่ละงานถูกกำหนดไว้ในแผนการตรวจสอบภายในประจำปีนั้น งานซึ่งรวมอยู่ในแผนการตรวจสอบภายในนั้นเกิดจากการประเมินความเสี่ยงแบบทั่วทั้งองค์กร ซึ่งจัดทำอย่างน้อยปีละครั้ง โดยหน่วยงานตรวจสอบภายใน



Practice Guide / Engagement Planning: Establishing Objectives and Scope

เมื่อผู้ตรวจสอบภายในเริ่มปฏิบัติงานที่ได้รับมอบหมาย จะต้องคำนึงถึงความเสี่ยงต่างๆ ที่เกี่ยวข้องกับงานนั้นๆ และสอบถามว่ามีการเปลี่ยนแปลงใดๆ ที่ได้เกิดขึ้นนับตั้งแต่มีการจัดทำแผนการตรวจสอบภายในประจำปีขึ้น ทั้งนี้ การทบทวนผลการประเมินความเสี่ยงแบบทั่วทั้งองค์กร ตลอดจนผลการประเมินความเสี่ยงอื่นๆ ที่ได้ประเมินไปแล้ว (เช่นที่ได้ดำเนินการโดยฝ่ายบริหาร) อาจช่วยให้ผู้ตรวจสอบภายในระบุความเสี่ยงต่างๆ ที่เกี่ยวข้องกับบริเวณหรือกระบวนการที่จะทำการสอบทานได้

เพื่อให้เกิดความเข้าใจในบริบทของงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในควรตรวจสอบความเกี่ยวข้องและสอดคล้องกันระหว่างตัวองค์กรกับพื้นที่หรือกระบวนการที่จะทำการตรวจสอบ โดยเฉพาะในองค์ประกอบต่อไปนี้

- พันธกิจ วิสัยทัศน์ และวัตถุประสงค์ต่างๆ ในเชิงกลยุทธ์
- โครงสร้างและกระบวนการต่างๆ ที่เกี่ยวข้องกับการกำกับดูแล การบริหารความเสี่ยงและการควบคุม
- นโยบายและขั้นตอนการปฏิบัติงานต่างๆ
- ลำดับความสำคัญของความเสี่ยงต่างๆ

นอกจากนี้ ผู้ตรวจสอบภายในยังควรพิจารณาด้วยว่างานที่ได้รับมอบหมายนั้น เป็นการร้องขอเพื่อบริการให้ความเชื่อมั่นหรือการให้คำปรึกษา เนื่องจากความคาดหวังของผู้มีส่วนได้เสียและข้อกำหนดของ มาตรฐาน นั้นมีความแตกต่างกัน โดยขึ้นอยู่กับประเภทของงานที่ได้รับมอบหมายดังกล่าว จุดมุ่งหมาย วัตถุประสงค์และขอบเขตของงานให้ความเชื่อมั่นอาจมีความแตกต่างกันอย่างมีนัยสำคัญจากงานให้คำปรึกษา สำหรับงานให้ความเชื่อมั่นนั้น วัตถุประสงค์และขอบเขตจะถูกพิจารณากำหนดในเบื้องต้นโดยผู้ตรวจสอบภายใน ในขณะที่สำหรับงานให้คำปรึกษานั้นจะถูกกำหนดโดยผู้รับบริการ ทั้งนี้ มาตรฐานด้านการนำไปใช้ปฏิบัติต่างๆ ที่เกี่ยวข้องกับการวางแผนสำหรับงานให้ความเชื่อมั่นและงานให้คำปรึกษาแสดงอยู่ในตารางในหน้า 8

ข้อกำหนดของมาตรฐานสำหรับงานให้บริการความเชื่อมั่นและงานให้คำปรึกษา

การให้ความเชื่อมั่น

ในการวางแผนการปฏิบัติงานสำหรับกลุ่มบุคคลภายนอกองค์กร ผู้ตรวจสอบภายในต้องทำความเข้าใจกับผู้รับบริการเป็นลายลักษณ์อักษรเกี่ยวกับวัตถุประสงค์ ขอบเขต ภาระหน้าที่ของแต่ละฝ่าย และความคาดหวังอื่น ๆ ของผู้รับบริการ (มาตรฐาน 2201.A1)

วัตถุประสงค์ของงานให้ความเชื่อมั่นจะต้องสอดคล้องกับผลการประเมินความเสี่ยงเบื้องต้นที่เกี่ยวข้องกับพื้นที่หรือกระบวนการที่จะตรวจสอบ (มาตรฐาน 2210.A1)

ในการพิจารณากำหนดวัตถุประสงค์ของงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในต้องคำนึงถึงความเป็นไปได้ที่จะเกิดข้อผิดพลาด การทุจริต การไม่ปฏิบัติตามกฎระเบียบ และความเสี่ยงอื่น ๆ ที่มีนัยสำคัญ (มาตรฐาน 2210.A2)

ผู้ตรวจสอบภายในต้องกำหนดเกณฑ์ที่เพียงพอและเหมาะสมเพื่อใช้ประเมินว่าได้มีการบรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้แล้ว (มาตรฐาน 2210.A3)

การให้คำปรึกษา

ผู้ตรวจสอบภายในและผู้รับบริการงานให้คำปรึกษาต้องเห็นชอบกับวัตถุประสงค์ ขอบเขต ความคาดหวัง และความรับผิดชอบของแต่ละฝ่าย รวมทั้งบันทึกข้อตกลงนี้ไว้เป็นลายลักษณ์อักษร ในกรณีที่เป็นงานที่สำคัญ (มาตรฐาน 2201.C1)

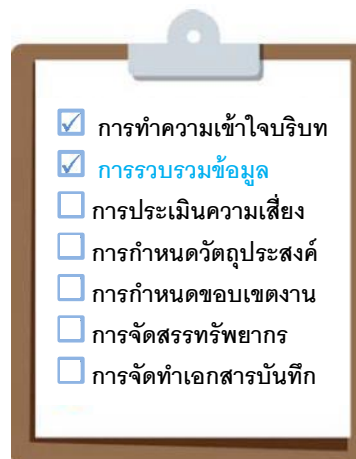
วัตถุประสงค์ของงานให้คำปรึกษาจะต้องระบุถึงกระบวนการกำกับดูแล การบริหารความเสี่ยงและการควบคุม โดยอยู่ภายในขอบเขตที่ได้ตกลงไว้กับผู้รับบริการ (มาตรฐาน 2210.C1)

วัตถุประสงค์ของงานให้คำปรึกษาต้องสอดคล้องกับคุณค่า กลยุทธ์และวัตถุประสงค์ขององค์กร (มาตรฐาน 2210.C2)

ในระหว่างการปฏิบัติงานให้คำปรึกษา ผู้ตรวจสอบภายในต้องระบุถึงวิธีการควบคุมให้สอดคล้องกับวัตถุประสงค์ของงานที่ได้รับมอบหมายและต้องเตรียมพร้อมต่อประเด็นการควบคุมที่มีนัยสำคัญ (มาตรฐาน 2220.C2)

การรวบรวมข้อมูล

ในฐานะที่เป็นส่วนหนึ่งของการวางแผนสำหรับงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในต้องเก็บรวบรวมข้อมูลเกี่ยวกับบริเวณหรือกระบวนการที่จะทำการสอบทาน เช่น วัตถุประสงค์ทางธุรกิจ กระบวนการที่มีอยู่เพื่อให้บรรลุวัตถุประสงค์นั้นๆ ความเสี่ยงที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์นั้นๆ ตลอดจนวิธีการควบคุมที่มีเพื่อจัดการกับความเสี่ยงดังกล่าว การทำความเข้าใจวัตถุประสงค์ในทางธุรกิจจะช่วยให้พื้นฐานแก่ผู้ตรวจสอบภายในในการระบุความเสี่ยงต่างๆ ที่ควรรวมไว้ในการประเมินความเสี่ยง ณ ทุกระดับของงานที่ได้รับมอบหมายในเบื้องต้น (ตามที่กำหนดไว้ในมาตรฐาน 2210.A1)



ในการเก็บรวบรวมข้อมูล ผู้ตรวจสอบภายในมักจะดำเนินการดังต่อไปนี้:

- ทบทวนการประเมินผลในครั้งก่อนของบริเวณหรือกระบวนการที่จะทำการสอบทาน
- ทำความเข้าใจและกำหนดแผนผังกระบวนการและการควบคุมต่างๆ ในบริเวณหรือกระบวนการที่จะทำการสอบทาน
- สัมภาษณ์ผู้มีส่วนได้เสียที่เกี่ยวข้อง
- ระดมสมองเกี่ยวกับสถานการณ์ความเสี่ยงที่อาจเกิดขึ้น

เพื่อให้เป็นไปตามมาตรฐาน 2200 เรื่องการวางแผนสำหรับงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในต้องจัดทำบันทึกข้อมูลที่เก็บรวบรวมได้มาในขณะที่จัดทำแผนไว้เป็นลายลักษณ์อักษร ซึ่งจะช่วยให้สามารถสังเกตเห็นได้ถึงการปฏิบัติที่ได้กล่าวข้างต้นไม่ได้เป็นไปตามลำดับขั้นตอนที่เหมาะสม อย่างไรก็ตาม หลายๆ สิ่งที่ต้องปฏิบัติ เช่น การจัดทำแผนผังกระบวนการ และการจัดทำเอกสารบันทึกข้อมูล เป็นสิ่งที่ต้องปฏิบัติอย่างต่อเนื่องตลอดช่วงของการวางแผนสำหรับงานที่ได้รับมอบหมาย

การทบทวนผลการประเมินในครั้งก่อน

ข้อมูลบางอย่างเกี่ยวกับบริเวณหรือกระบวนการที่จะทำการสอบทานอาจรวบรวมได้มาจากเอกสารต่างๆ ขององค์กร การประเมินครั้งล่าสุดที่เกี่ยวข้องกับงานที่ได้รับมอบหมายและรายงานต่างๆ อาจมีข้อมูลให้ผู้ตรวจสอบภายในสามารถนำไปรวมไว้ในแผนงานได้

กระดาษทำการจากงานตรวจสอบในครั้งก่อน – ผู้ตรวจสอบภายในจะทบทวนกระดาษทำการจากงานตรวจสอบภายในครั้งล่าสุดสำหรับบริเวณหรือกระบวนการที่จะทำการสอบทาน เพื่อรวบรวมข้อมูลเกี่ยวกับกระบวนการและการควบคุมที่มีอยู่ในระหว่างการตรวจสอบครั้งหลังสุด การทบทวนกระดาษทำการในครั้งก่อนยังจะช่วยให้ผู้ตรวจสอบภายในสามารถสอบถามเกี่ยวกับการปรับปรุงแก้ไขที่ได้ดำเนินการโดยฝ่ายบริหารตามข้อสังเกตจากการตรวจสอบในครั้งก่อน

การประเมินความเสี่ยงแบบทั่วทั้งองค์กร – ผู้ตรวจสอบภายในควรสอบถามลำดับความสำคัญของความเสี่ยงต่างๆ ที่องค์กรได้ระบุไว้ เพื่อพิจารณาว่า มีความเสี่ยงใดบ้างที่ควรถูกรวมไว้เป็นส่วนหนึ่งของงานที่ได้รับมอบหมายในครั้งปัจจุบันหรือไม่

การประเมินความเสี่ยงด้านการทุจริตและเอกสารต่างๆ ที่เกี่ยวข้อง – ผู้ตรวจสอบภายในควรสื่อสารกับผู้ที่มีหน้าที่รับผิดชอบในการจัดการกับความเสียหายจากการทุจริต ข้อกล่าวหา และรายละเอียดเหตุการณ์ที่เกิดขึ้น (เช่น หน่วยงานกฎหมาย ทรัพยากรบุคคล บริหารความเสี่ยงจากการทุจริต) นอกจากการหารือเกี่ยวกับเหตุการณ์ทุจริตที่เกิดขึ้น หรือการสอบสวนข้อกล่าวหาที่เกิดขึ้นภายในบริเวณหรือกระบวนการที่จะทำการสอบทานแล้ว ผู้ตรวจสอบภายในจะต้องสอบถามเอกสารที่เกี่ยวข้องเพื่อทำความเข้าใจข้อเท็จจริงในข้อกล่าวหาหรือจากการสอบสวน รวมทั้งผลลัพธ์ที่ได้ ผู้ตรวจสอบภายในอาจจำกัดการค้นหาข้อมูลให้อยู่ภายในช่วงระยะเวลาที่เหมาะสมสำหรับเหตุการณ์การทุจริตที่เกิดขึ้นและได้รับการยืนยันแล้ว ตลอดจนข้อกล่าวหาที่ได้รับการสอบสวนแล้วแต่ไม่พบข้อเท็จจริงใดๆ

รายงานโดยผู้ให้บริการงานให้ความเชื่อมั่นและงานให้คำปรึกษาอื่นๆ – ผู้ตรวจสอบภายในอาจพึ่งพาผลงานที่ดำเนินการโดยผู้ให้บริการความเชื่อมั่นและคำปรึกษาทั้งภายในหรือภายนอกอื่นๆ แทนที่จะไปปฏิบัติงานเอง ทำให้เกิดการงานซ้ำซ้อน ความสามารถของผู้ตรวจสอบภายในที่จะพึ่งพาผลงานของผู้อื่นนั้นขึ้นอยู่กับว่าผู้ตรวจสอบภายในพอใจกับความเป็นอิสระและความสามารถที่เพียงพอ ของผู้ให้บริการ ตลอดจนงานที่ได้กระทำไปแล้วมีความเกี่ยวข้องและเชื่อถือได้ ผู้ให้บริการงานให้ความเชื่อมั่นและงานให้คำปรึกษาอาจหมาย

Practice Guide / Engagement Planning: Establishing Objectives and Scope

รวมถึงผู้ที่มีหน้าที่รับผิดชอบเกี่ยวกับการบริหารความเสี่ยง การกำกับดูแลการปฏิบัติงาน อาชีวอนามัยและความปลอดภัย เทคโนโลยีสารสนเทศ จริยธรรม กฎหมาย การรักษาความปลอดภัย คุณภาพและอื่นๆ ผู้ให้บริการยังอาจรวมถึงหน่วยงานภายนอก เช่น ผู้สอบบัญชีหรือบุคคลที่สามที่ได้ทำสัญญาว่าจ้าง ผู้ตรวจสอบภายในอาจพบปะกับผู้ให้บริการงานให้ความเชื่อมั่นและงานให้คำปรึกษาเพื่อสอบทานและหารือเกี่ยวกับรายงานและ/หรือเอกสารอื่นๆ ที่เกี่ยวข้องกับงานที่ได้ดำเนินการภายในบริเวณหรือกระบวนการที่จะทำการสอบทาน ทั้งนี้ ในมาตรฐาน 2050 เรื่องการประสานงานและการพึ่งพาผลงานผู้อื่น ได้ให้ข้อมูลเพิ่มเติมเกี่ยวกับการประสานความร่วมมือกันกับผู้ให้บริการงานให้ความเชื่อมั่นและงานให้คำปรึกษาอื่นๆ

การทำความเข้าใจและจัดทำแผนผังกระบวนการและการควบคุมต่างๆ

ในการระบุความเสี่ยงต่างๆ ที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ในทางธุรกิจ ผู้ตรวจสอบภายในจะต้องมีความเข้าใจในบริเวณหรือกระบวนการที่จะทำการสอบทาน ทั้งนี้ แผนผังกระบวนการในระดับสูง (high-level process map) ซึ่งแสดงถึงปัจจัยนำเข้ากระบวนการและผลผลิตที่ออกมาจากกระบวนการแบบกว้างๆ (เช่น กิจกรรมต่างๆ ทางเดินของงาน และการประมวลผลสารสนเทศที่สำคัญ) อาจนำมาช่วยได้ ผู้ตรวจสอบภายในอาจสร้างผังกระบวนการหรืออ้างอิงจากเอกสารที่มีอยู่แล้ว หากได้ตรวจสอบแล้วว่าเอกสารดังกล่าวมีความถูกต้องและเป็นปัจจุบัน

แผนผังกระบวนการจะช่วยให้ผู้ตรวจสอบภายในสามารถระบุและเข้าใจมากขึ้นในสิ่งต่อไปนี้:

- ระบบงานและข้อมูลที่ควรนำมาพิจารณาเมื่อจะกำหนดวัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมาย ความเกี่ยวข้องและความพึ่งพาซึ่งกันและกัน ตลอดจนแหล่งจัดเก็บข้อมูลที่สำคัญ (เช่น เก็บไว้ในระบบเดียว หรือหลายระบบ)
- การนำสารสนเทศที่สำคัญมาใช้ในบริเวณหรือกระบวนการที่จะสอบทานเป็นอย่างไร ข้อมูล/สารสนเทศใดบ้างที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย และจะประเมินผลสารสนเทศดังกล่าวอย่างไร (เช่น การทดสอบมาตรฐาน การวิเคราะห์ข้อมูล และการใช้ดัชนีชี้วัดผลหรือความสำเร็จ)
- ใครคือผู้ที่สามารถเข้าถึงสารสนเทศที่มีความสำคัญได้
- จุดต่างๆ ในกระบวนการซึ่งขาดวิธีการควบคุมที่มีประสิทธิภาพ หรือไม่ได้ออกแบบวิธีการควบคุมมาอย่างดีพอ หรือจุดที่มีโอกาสที่จะปรับปรุงกระบวนการให้ดีขึ้นได้

Practice Guide / Engagement Planning: Establishing Objectives and Scope

ข้อมูลบางอย่างที่จำเป็นต้องระบุไว้ในแผนผังกระบวนการอาจได้มาจากเอกสารต่างๆ ขององค์กร เช่น คู่มือพนักงาน คู่มือการปฏิบัติงาน และ/หรือเว็บไซต์ภายในขององค์กรซึ่งรวบรวมนโยบายและขั้นตอนกระบวนการต่างๆ ไว้ ตัวอย่างเช่น วิทยาลัย ศักดิ์ พิษณุภาค วัตถุประสงค์ทางธุรกิจ และกลยุทธ์ต่างๆ ที่เกี่ยวข้องกับบริเวณหรือกระบวนการที่จะทำการสอบทานซึ่งมักจะมีการจัดทำไว้เป็นเอกสาร อย่างไรก็ตาม สิ่งเหล่านี้ก็อาจได้มาจากการสัมภาษณ์กับฝ่ายบริหารก็ได้

การสัมภาษณ์ผู้มีส่วนได้เสียที่เกี่ยวข้อง

การสัมภาษณ์ผู้มีส่วนได้เสียที่เกี่ยวข้อง ถือเป็นขั้นตอนที่สำคัญยิ่งที่จะช่วยให้ผู้ตรวจสอบภายในมีความเข้าใจเกี่ยวกับวัตถุประสงค์ การออกแบบ การดำเนินงาน และสภาพแวดล้อมในการควบคุมของบริเวณหรือกระบวนการที่จะสอบทานได้ดียิ่งขึ้น ทั้งนี้ แผนผังโครงสร้างขององค์กรมักจะมีส่วนช่วยให้ผู้ตรวจสอบภายในสามารถระบุได้ถึงผู้มีส่วนได้เสียที่เกี่ยวข้อง

คำถามปลายเปิดจะส่งเสริมให้เกิดการสนทนาที่มีคุณค่าระหว่างผู้ตรวจสอบภายในและผู้มีส่วนได้เสียต่างๆ เนื่องจากจะทำให้ผู้มีส่วนได้เสียสามารถให้รายละเอียดเพิ่มเติม ตลอดจนเปิดโอกาสให้มีการสอบถามได้ทันที ผู้ตรวจสอบภายในมักจะสัมภาษณ์ผู้มีส่วนได้เสียต่างๆ เช่น ผู้ปฏิบัติงานในขั้นตอนต่างๆ ในกระบวนการ ฝ่ายบริหาร บุคลากรด้านเทคโนโลยีสารสนเทศ ที่ปรึกษากฎหมาย เจ้าหน้าที่กำกับดูแลการปฏิบัติงาน บุคคลที่สามที่ได้ทศัญญาว่าจ้าง รวมถึงผู้มีส่วนได้เสียอื่นๆ

ผู้ปฏิบัติขั้นตอนต่างๆ ในกระบวนการ – ข้อมูลในเชิงลึกอาจได้รับการสัมภาษณ์กับบุคลากรในทุกระดับของกระบวนการ เนื่องจากเป็นผู้ที่สามารถให้ข้อมูลที่มีลักษณะเฉพาะเกี่ยวกับวิธีการทำงานจริงของกระบวนการ ไม่ใช่แต่เพียงวิธีการที่ถูกออกแบบมาเพื่อให้ทำงาน ข้อมูลดังกล่าวจะมีประโยชน์อย่างมากสำหรับใช้ในการระบุความเสี่ยงจากการทุจริต เนื่องจากผู้มีหน้าที่รับผิดชอบในการปฏิบัติงานในกระบวนการมักจะมี ความเข้าใจเกี่ยวกับวิธีการควบคุม รวมถึงวิธีการที่จะหลีกเลี่ยงหรือเอาชนะวิธีควบคุมต่างๆ เหล่านั้นได้เป็นอย่างดีที่สุด

ฝ่ายบริหาร – ผู้จัดการซึ่งมีหน้าที่รับผิดชอบในบริเวณหรือกระบวนการที่จะทำการสอบทานอาจให้ภาพรวมได้ดีที่สุดเกี่ยวกับวิธีที่กระบวนการถูกออกแบบมาเพื่อให้ทำงาน ข้อมูลเกี่ยวกับกระบวนการอาจได้รับการจัดทำเป็นลายลักษณ์อักษรในรูปของนโยบาย ขั้นตอนการปฏิบัติงาน และแบบประเมินตนเอง นอกจากนี้ เอกสารที่มีอยู่อาจบรรยายถึงวัตถุประสงค์ทางธุรกิจและดัชนีชี้วัดผลการดำเนินงานของกิจกรรม (เช่น เกณฑ์ที่ใช้วัดว่ามี

Practice Guide / Engagement Planning: Establishing Objectives and Scope

การบรรลุวัตถุประสงค์หรือไม่) ตลอดจนสิ่งเหล่านี้จะช่วยสนับสนุนวัตถุประสงค์ขององค์กรได้อย่างไร การสัมภาษณ์ฝ่ายบริหารอาจช่วยให้ผู้ตรวจสอบภายในสามารถระบุได้ว่าความเข้าใจของฝ่ายบริหารเกี่ยวกับขั้นตอนต่างๆ ในแต่ละกระบวนการนั้นมีความแตกต่างจากความเข้าใจของผู้ปฏิบัติงานหรือไม่ การสัมภาษณ์เหล่านี้ อาจช่วยให้ผู้ตรวจสอบภายในสามารถระบุหลักเกณฑ์ที่จะนำมาใช้ในการประเมินระบบการกำกับดูแลการบริหารความเสี่ยงและการควบคุมของบริเวณหรือกระบวนการที่จะทำการสอบทาน ตามที่เป็นข้อกำหนดของงานให้ความเชื่อมั่นได้ (มาตรฐาน 2210.A3)

บุคลากรด้านเทคโนโลยีสารสนเทศ - เนื่องจากความเสี่ยงทางด้านเทคโนโลยีสารสนเทศและความปลอดภัยเป็นเรื่องสำคัญ ผู้ตรวจสอบภายในจึงควรทำการศึกษาเกี่ยวกับความเสี่ยงทางด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นให้มากที่สุดเท่าที่จะเป็นไปได้ การสัมภาษณ์ผู้มีส่วนได้เสียที่เกี่ยวข้องในกระบวนการต่างๆ ทางด้านเทคโนโลยีสารสนเทศที่อาจมีผลกระทบต่อบริเวณหรือกระบวนการที่จะทำการสอบทานนั้น จะช่วยให้มั่นใจได้ว่าระบบทั้งหมดที่นำมาใช้อยู่นั้นได้รับการคำนึงถึง และอาจเผยให้เห็นถึงจุดที่ขาดวิธีการควบคุม มีการควบคุมไม่เพียงพอ หรือถูกหลีกเลี่ยงได้

ที่ปรึกษากฎหมายและผู้มีหน้าที่กำกับดูแลการปฏิบัติตามกฎระเบียบ - ในหลายๆ บริเวณหรือกระบวนการ มักจะต้องเกี่ยวข้องกับปฏิบัติตามกฎหมายและระเบียบข้อบังคับ ดังนั้น ผู้ตรวจสอบภายในอาจเลือกที่จะพบปะกับที่ปรึกษากฎหมายและผู้จัดการด้านความเสี่ยงเพื่อขอข้อมูลที่ได้รับผ่านโครงการการแจ้งเบาะแส (whistleblower programs) รวมถึงข้อมูลเกี่ยวกับเหตุการณ์ที่มีความผิดปกติและคดีความ (ทั้งในอดีตและปัจจุบัน) ที่มีความเกี่ยวข้องกับงานที่ได้รับมอบหมาย การสัมภาษณ์ผู้มีหน้าที่กำกับดูแลการปฏิบัติตามกฎระเบียบ หรือผู้มีหน้าที่รับผิดชอบในการดำเนินการของระบบการควบคุมอาจให้ข้อมูลเชิงลึกได้ว่าการปฏิบัติตามนโยบายและขั้นตอนการปฏิบัติงานนั้นจะตอบสนองต่อกฎหมายและระเบียบข้อบังคับอย่างมีประสิทธิภาพได้เพียงใด ทั้งนี้ กฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องอาจประกอบด้วยส่วนที่เป็นเกณฑ์ที่จะใช้ในการประเมินว่ากิจกรรมนั้นจะสามารถบรรลุวัตถุประสงค์ในทางธุรกิจได้อย่างไรก็ได้ (มาตรฐาน 2210.A3)

ผู้มีส่วนได้เสียอื่นๆ - ผู้ตรวจสอบภายในอาจสัมภาษณ์หรือทำการสำรวจความคิดเห็นจากลูกค้าหรือหน่วยงานทางธุรกิจอื่นๆ ที่มีความเกี่ยวข้องกับบริเวณหรือกระบวนการที่จะทำการสอบทาน เพื่อทำความเข้าใจประเด็นปัญหาต่างๆ ในอดีตและ/หรือปัจจุบันที่อาจบ่งชี้ถึงความเสี่ยงที่อาจเกิดขึ้นได้

การระดมความคิดเกี่ยวกับสถานการณ์ความเสี่ยงต่างๆ ที่อาจเกิดขึ้น

ผู้ตรวจสอบภายในอาจจะดมสมองร่วมกับบุคคลต่างๆ หรือในกลุ่ม หรือหน่วยงานที่ได้คัดเลือกมา โดยในระหว่างการระดมสมองเพื่อระบุความเสี่ยงที่เกี่ยวข้องนั้น ผู้ตรวจสอบภายในอาจถามว่า “สิ่งใดที่จะทำให้ไม่สามารถบรรลุวัตถุประสงค์ทางธุรกิจได้” นอกจากนี้ เพื่อระบุความเสี่ยงที่อยู่ตามธรรมชาตินั้น ผู้ตรวจสอบภายในอาจถามว่า “จะมีสิ่งผิดปกติใดเกิดขึ้นบ้าง หากไม่มีวิธีการควบคุมอยู่เลย”

เนื่องจากความมีนัยสำคัญของความเสี่ยงจากการทุจริต มาตรฐาน 2210.A2 จึงกำหนดให้ต้องนำเรื่องการทุจริตมาร่วมพิจารณาเมื่อจะทำการกำหนดวัตถุประสงค์สำหรับงานให้ความเชื่อมั่น การระดมสมองเกี่ยวกับสถานการณ์ความเสี่ยงจากการทุจริตต่างๆ นั้นจะมีประโยชน์อย่างยิ่ง เนื่องจากจะช่วยให้ผู้ตรวจสอบภายในได้ทราบถึงมุมมองต่างๆ ที่หลากหลายในการพิจารณาสิ่งจูงใจหรือแรงกดดันที่อาจนำไปสู่การทุจริต โอกาสในการกระทำทุจริต (เช่น จุดอ่อนของการควบคุม) ตลอดจนวิธีการที่ฝ่ายบริหารและหน่วยงานอื่นๆ อาจก้าวข้ามและ/หรือหลีกเลี่ยงการควบคุมต่างๆ ได้

การจัดทำบันทึกข้อมูลที่ได้รวบรวมมา

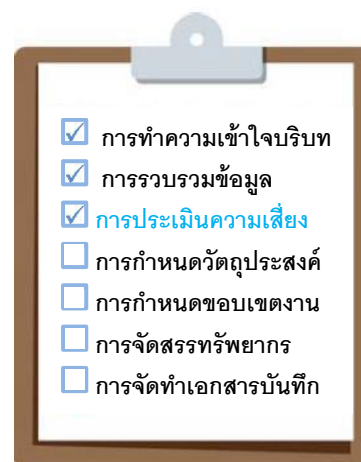
โดยการจัดทำเอกสารบันทึกข้อมูลที่ได้รวบรวมมาในระหว่างการวางแผนสำหรับงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในจะสามารถประเมินข้อมูลที่เก็บรวบรวมมา เพื่อให้ได้มุมมองในเรื่องดังต่อไปนี้:

- วัตถุประสงค์ของกิจกรรมที่จะทำการสอบทาน
- กลยุทธ์ต่างๆ ที่นำมาใช้เพื่อให้บรรลุวัตถุประสงค์เหล่านั้น
- ความเสี่ยงต่างๆ ที่จะทำให้ไม่บรรลุวัตถุประสงค์เหล่านั้น
- กระบวนการและวิธีการควบคุมที่สำคัญ
- เทคโนโลยีสารสนเทศและระบบอื่นๆ ที่เกี่ยวข้องกับบริเวณหรือกระบวนการที่จะทำการสอบทาน
- แหล่งข้อมูลต่างๆ และความเชื่อถือได้ของข้อมูลที่นำเข้าและข้อมูลที่ออกมาจากบริเวณหรือกระบวนการที่จะทำการสอบทาน

การมีความเข้าใจโดยละเอียดเกี่ยวกับองค์กรและบริเวณหรือกระบวนการที่จะทำการสอบทาน จะช่วยให้ผู้ตรวจสอบภายในสามารถทำการประเมินเกี่ยวกับความเสี่ยงต่างๆ ในเบื้องต้น ตามที่กำหนดไว้ในมาตรฐาน 2210.A1 ได้

การประเมินความเสี่ยงในเบื้องต้น

เนื่องจากข้อจำกัดทางด้านเวลาและทรัพยากร จึงทำให้ไม่สามารถสอบถามความเสี่ยงทั้งหมดได้ในระหว่างปฏิบัติงานที่ได้รับมอบหมาย ดังนั้น ผู้ตรวจสอบภายในจึงต้องประเมินความเสี่ยงในเบื้องต้นและจัดลำดับความเสี่ยงต่างๆ ตามความมีนัยสำคัญ ซึ่งจะวัดได้จากการนำปัจจัยความเสี่ยงต่างๆ มารวมกัน



วิธีที่มีประสิทธิภาพวิธีหนึ่งในการดำเนินการและจัดทำเอกสารการประเมินความเสี่ยงเบื้องต้น ณ ระดับของงานที่ได้รับมอบหมายนั้น คือ การจัดทำแผนภูมิที่แสดงถึงความเกี่ยวข้องกันระหว่างความเสี่ยงและวิธีการควบคุม เช่น ตารางแมทริกซ์ความเสี่ยงและการควบคุม ซึ่งตารางนี้เป็นเครื่องมือที่ผู้ตรวจสอบภายในใช้กันโดยทั่วไปในการระบุ จัดระเบียบ และประเมินความเสี่ยงที่อาจส่งผลกระทบต่อวัตถุประสงค์ในทางธุรกิจของกิจกรรมที่จะทำการสอบทาน ตลอดจนการควบคุมเพื่อจัดการกับความเสี่ยงดังกล่าว แมทริกซ์ความเสี่ยงและการควบคุมสามารถจัดทำในรูปของสเปรดชีท (Spreadsheet) เอกสารจาก word processing หรือมาจากโปรแกรมการตรวจสอบสำเร็จรูป นัยสำคัญของความเสี่ยงแต่ละตัวสามารถแสดงได้ด้วยแผนภูมิพื้นฐาน เช่น แผนที่ความเสี่ยง (Heat Map)

ในการจัดทำแผนที่ความเสี่ยงนั้น ผู้ตรวจสอบภายในจะต้องกำหนดความเสี่ยงแต่ละความเสี่ยงตามตัวแปรที่สำคัญสองตัว ได้แก่ ผลกระทบและโอกาสที่จะเกิดความเสี่ยง วิธีนี้จะช่วยสร้างเอกสารที่มีความชัดเจน ซึ่งสามารถจัดเก็บไว้เป็นส่วนหนึ่งของกระดาษทำการสำหรับงานที่ได้รับมอบหมายได้ รวมถึงเป็นส่วนหนึ่งของแนวการปฏิบัติงานที่ได้รับมอบหมาย (มาตรฐาน 2240 เรื่องแนวการปฏิบัติงาน) เอกสารดังกล่าวยังถือเป็น “ข้อมูลที่เพียงพอ เชื่อถือได้ เกี่ยวข้องและเป็นประโยชน์” ซึ่งจำเป็นเพื่อสนับสนุนผลและข้อสรุปของงานที่ได้รับมอบหมาย ตามมาตรฐาน 2330 เรื่องการจัดทำเอกสารข้อมูล

การระบุความเสี่ยงและการควบคุม: ตารางความเสี่ยงและการควบคุม

ตารางแมทริกซ์ความเสี่ยงและการควบคุมจะประกอบด้วยข้อมูลที่เก็บรวบรวมมาตลอดกระบวนการวางแผนสำหรับงานที่ได้รับมอบหมาย **ภาพที่ 1** หน้า 16 แสดงตัวอย่างวิธีจัดทำตารางแมทริกซ์ความเสี่ยงและการควบคุมสำหรับงานให้ความเชื่อมั่นของบัญชีเจ้าหนี้ ทั้งนี้ รูปแบบของตารางความเสี่ยงและการควบคุมอาจมีความแตกต่างกันออกไป

ภาพที่ 1: ตารางความเสี่ยงและการควบคุมสำหรับบัญชีเจ้าหนี้

วัตถุประสงค์ทางธุรกิจ	ความเสี่ยงตามธรรมชาติ	ผลกระทบ (ต่ำ, กลาง, สูง)	โอกาสที่จะเกิด (ต่ำ, กลาง, สูง)	การควบคุม
A. ค่าใช้จ่ายพนักงานมีความเหมาะสมและได้รับการอนุมัติ	A.1 มีการออกบัตรเครดิตขององค์กร อย่างไม่เหมาะสม ส่งผลให้เกิดการทุจริต ค่าใช้จ่าย	กลาง	กลาง	มีการแบ่งแยกหน้าที่
	A.2 พนักงานไม่ได้รับการชี้แนะเกี่ยวกับ นโยบายการใช้บัตรเครดิตและค่าใช้จ่าย ขององค์กร ส่งผลให้เกิดค่าใช้จ่ายที่ไม่เหมาะสม	ต่ำ	กลาง	นโยบายค่าใช้จ่ายได้รับการสื่อสารไปยังผู้มีอำนาจในการใช้จ่ายขององค์กร
	A.3 ไม่ได้นำส่ง/ตรวจสอบ รายงานค่าใช้จ่ายอย่างเหมาะสม แก่เวลา ส่งผลให้เกิด ค่าใช้จ่ายที่ไม่เหมาะสม	สูง	สูง	ไม่มีวิธีการควบคุมใดๆ
	A.4 รายงานค่าใช้จ่ายพร้อมใบเสร็จรับเงินไม่ได้รับการสอบทานและอนุมัติโดยบุคคลที่เหมาะสม ส่งผลให้เกิด ค่าใช้จ่ายที่ไม่เหมาะสม	สูง	กลาง	การอนุมัติขึ้นอยู่กับลำดับชั้นของฝ่ายบริหาร รายงานค่าใช้จ่ายจะไม่ได้รับการนำเสนอจนกว่าจะได้รับการอนุมัติจากผู้จัดการ ทีมค่าใช้จ่ายจะดำเนินการสอบทานเป็นประจำทุกเดือน
B. ค่าใช้จ่ายในการดำเนินงานมีความเหมาะสมและได้รับการอนุมัติ	B.1 ผู้ขายปลอมได้ถูกสร้างไว้ในระบบ ส่งผลให้เกิดการทุจริตค่าใช้จ่าย	สูง	ต่ำ	มีการแบ่งแยกหน้าที่
	B.2 ผู้ขายนำส่งใบแจ้งหนี้ที่ไม่ถูกต้อง ทำซ้ำหรือปลอมแปลง ซึ่งไม่ได้รับการตรวจสอบและ	สูง	กลาง	การอนุมัติใบแจ้งหนี้เป็นไปตามระดับอำนาจอนุมัติ ค่าใช้จ่าย

 Practice Guide / Engagement Planning: Establishing Objectives and Scope

วัตถุประสงค์ทางธุรกิจ	ความเสี่ยงตามธรรมชาติ	ผลกระทบ (ต่ำ, กลาง, สูง)	โอกาสที่จะเกิด (ต่ำ, กลาง, สูง)	การควบคุม
	อนุมัติโดยบุคคลที่เหมาะสม			
	B.3 ค่าใช้จ่ายไม่ได้รับการอนุมัติก่อนดำเนินการ ส่งผลให้เกิดค่าใช้จ่ายที่ไม่เหมาะสม	กลาง	ต่ำ	ไม่มีวิธีการควบคุมใดๆ
C. การจ่ายชำระเงินมีความถูกต้องและตรงเวลา	C.1 การจ่ายชำระเงินภายหลังจากวันครบกำหนดชำระ ส่งผลให้ถูกคิดดอกเบี้ยและเบี้ยปรับ	ต่ำ	กลาง	ไม่มีวิธีการควบคุมใดๆ
	C.2 ไม่ได้รับส่วนลด เนื่องจากจ่ายชำระเงินภายหลังจากระยะเวลาที่จะได้รับส่วนลด	ต่ำ	สูง	ไม่มีการควบคุมใดๆ

ตัวอย่างในหน้า 16 ประกอบด้วยห้าคอลัมน์ซึ่งมีรายละเอียดดังนี้:

- **วัตถุประสงค์ทางธุรกิจ** - แต่ละวัตถุประสงค์ของบริเวณที่จะสอบทาน (ตามที่ได้กำหนดในระหว่างขั้นตอนการเก็บรวบรวมข้อมูล)
- **ความเสี่ยงตามธรรมชาติ** - ความเสี่ยงตามธรรมชาติแต่ละตัวที่จะทำให้ไม่บรรลุวัตถุประสงค์ทางธุรกิจได้ ความเสี่ยงตามธรรมชาติเป็นความเสี่ยงที่เกิดขึ้นในกรณีที่ไม่มีการควบคุมมาใช้จัดการกับความเสี่ยงนั้นๆ การสร้างระบบอย่างง่ายเพื่อระบุความเสี่ยงแต่ละตัว เช่น ระบบการใช้ตัวอักษรและตัวเลขด้วยกัน อย่างเช่นที่ใช้ในภาพที่ 1 จะช่วยให้กระบวนการสร้างแผนผังความเสี่ยงในภายหลังกนั้นทำได้ง่ายขึ้น
- **ผลกระทบ** - ระดับที่ความเสี่ยงตามธรรมชาติแต่ละตัวที่ได้ระบุไว้อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์ทางธุรกิจ (เช่น ระดับของผลกระทบที่ความเสี่ยงนี้จะมีต่อองค์กรหรือบริเวณนั้น หากความเสี่ยงดังกล่าวได้เกิดขึ้น) ผลกระทบโดยทั่วไปมักอธิบายเป็นระดับสูง กลาง หรือต่ำ และควรพิจารณาทั้งปัจจัยทางการเงินและปัจจัยที่ไม่ใช่ทางการเงิน
- **โอกาสที่จะเกิด** - ความน่าจะเป็นและความถี่ที่ความเสี่ยงตามธรรมชาติแต่ละความเสี่ยงที่ได้ระบุไว้จะเกิดขึ้น โดยทั่วไปมักใช้คำว่าระดับสูง กลาง หรือต่ำ (เช่น ความเสี่ยงจะมีโอกาสเกิดขึ้นมากน้อยเพียงใด หากไม่มีการควบคุมมาใช้จัดการกับความเสี่ยงดังกล่าว)

IA Practice Guide / Engagement Planning: Establishing Objectives and Scope

- **การควบคุม** – วิธีการควบคุมที่มีจุดประสงค์เพื่อจัดการกับความเสี่ยงแต่ละตัวตามที่ได้ระบุไว้ในระหว่างขั้นตอนการเก็บรวบรวมข้อมูล ผู้ตรวจสอบภายในอาจเพิ่มคอลัมน์ในตารางแมทริกซ์ความเสี่ยงและการควบคุมเพื่อจัดหมวดหมู่การควบคุมในแง่มุมต่อไปนี้
 - **ความสำคัญ** – สำคัญหรือไม่สำคัญ
 - **ประเภท** – เชิงป้องกันหรือเชิงตรวจหา
 - **ความอัตโนมัติ** – ทำด้วยมือ ด้วยระบบ หรือกึ่งอัตโนมัติ (วิธีการควบคุมกึ่งอัตโนมัติคือวิธีการควบคุมด้วยมือที่พึ่งพาการทำงานของโปรแกรมคอมพิวเตอร์ เช่น รายงานข้อยกเว้น)
 - **ความถี่** – รายปี รายไตรมาส รายเดือน รายสัปดาห์ รายวันหรือต่อรายการ

ตามที่กล่าวในข้างต้น ผู้ตรวจสอบภายในอาจให้คะแนนความมีนัยสำคัญของความเสี่ยงตามธรรมชาติแต่ละความเสี่ยง โดยพิจารณาจากผลกระทบและโอกาสที่จะเกิดขึ้นของความเสี่ยง เกณฑ์วัดความมีนัยสำคัญอื่นๆ ที่ควรระบุไว้ในตารางอาจได้แก่ ความเร็ว (เช่น ความเร็วของการตอบสนองและความเร็วในการฟื้นฟู) ความอ่อนไหว ความผันผวน การพึ่งพาซึ่งกันและกัน ตลอดจนความสัมพันธ์กัน นอกจากนี้ ผู้ตรวจสอบภายในอาจใช้วิธีหรือกรอบแนวทางอื่นๆ ในการระบุ จัดระเบียบ และประเมินวัตถุประสงค์ ความเสี่ยง และการควบคุมของบริเวณหรือกระบวนการที่จะทำการสอบทานได้

การพิจารณาความมีนัยสำคัญของความเสี่ยงนั้นทำให้ผู้ตรวจสอบภายในต้องใช้ความรู้ ประสบการณ์ และการคิดอย่างมีตรรกะในการตัดสินใจที่เกี่ยวกับองค์กร บริเวณหรือกระบวนการที่จะทำการสอบทาน ตลอดจนวัตถุประสงค์และบริบทของงานที่ได้รับมอบหมาย เวลาที่ใช้ไปในการเก็บรวบรวมข้อมูลระหว่างขั้นตอนต่างๆ ที่ผ่านมาจะให้ผลลัพธ์ที่มีประโยชน์อย่างมากในขั้นตอนนี้ แม้ว่า ทำายที่สุดแล้วผู้ตรวจสอบภายในจะเป็นผู้มีอำนาจสูงสุดที่จะพิจารณารายละเอียดครั้งสุดท้ายในการประเมินความเสี่ยง ณ ระดับของงานที่ได้รับมอบหมาย แต่การหารือกับฝ่ายบริหารของบริเวณหรือกระบวนการที่จะทำการตรวจสอบมักจะทำให้มุมมองอื่นๆ รวมถึงข้อมูลในเชิงลึกเพิ่มเติมเกี่ยวกับวัตถุประสงค์ทางธุรกิจ ความเสี่ยงตามธรรมชาติ การควบคุมต่างๆ ตลอดจนการจัดระดับความเสี่ยงต่างๆ ที่เกี่ยวข้อง

การจัดลำดับความเสี่ยง: แผนผังความเสี่ยง

แผนผังความเสี่ยง (Heat Map) เป็นกราฟพื้นฐานที่ผู้ตรวจสอบภายในสามารถจัดทำขึ้นเพื่อแสดงภาพที่รวมความมีนัยสำคัญของการจัดอันดับความเสี่ยงต่างๆ ที่ได้มาจากตารางความเสี่ยงและการควบคุม การรวมความมีนัยสำคัญอาจแสดงได้ด้วยการระบุผลกระทบของความเสี่ยงไว้ตามแกนหนึ่ง และโอกาสที่จะเกิดขึ้นไว้อีกแกนหนึ่ง

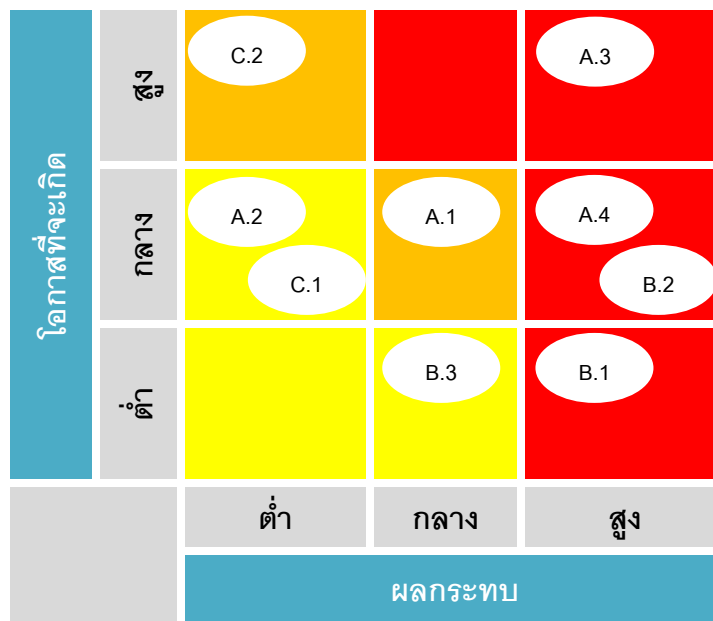
ตัวอักษรและตัวเลขที่แสดงถึงแต่ละความเสี่ยงจะถูกจัดวางไว้บนแผนผังความเสี่ยงที่ได้ระบุจุดตัดระหว่างผลกระทบและโอกาสที่จะเกิดตัวอย่างเช่น ความเสี่ยงที่มีผลกระทบสูงและ

โอกาสที่จะเกิดสูง (H,H) ซึ่งมีตัวอักษรและตัวเลขที่สอดคล้องกันจะถูกจัดวางไว้ที่มุมบนขวาของแผนผังความเสี่ยง (ดู A.3 ในภาพที่ 2)

ในทางกลับกัน ความเสี่ยงที่มีผลกระทบต่ำและโอกาสที่จะเกิดต่ำ (L, L) จะถูกจัดวางไว้ที่มุมล่างซ้ายของแผนผังความเสี่ยง โดยปกติแล้ว การรวมความมีนัยสำคัญของผลกระทบและโอกาสที่จะเกิดไว้ด้วยกัน จะถูกระบุด้วยระบบสี: สีแดงหมายถึงลำดับความสำคัญสูงสุด สีส้มหมายถึงความเสี่ยงที่มีนัยสำคัญเพียงพอที่จะนำมาพิจารณา และสีเหลืองหมายถึงความเสี่ยงที่ไม่เป็นภัยคุกคามที่สำคัญต่อการบรรลุวัตถุประสงค์ทางธุรกิจ

ข้อจำกัดอย่างหนึ่งของแผนผังความเสี่ยงคือ ผลกระทบและโอกาสที่จะเกิดจะดูเหมือนมีความสำคัญเท่ากัน แม้ว่าความเท่ากันนั้นอาจเป็นสิ่งที่ถูกต้องในบางครั้ง แต่ผลกระทบมักจะได้รับการพิจารณาก่อนโอกาสที่จะเกิด ตัวอย่างเช่น ในหลายๆ กรณี ความเสี่ยงที่พิจารณาแล้วพบว่ามีผลกระทบสูงและโอกาสที่จะเกิดต่ำ (H, L) จะได้รับการจัดลำดับความสำคัญไว้ก่อนความเสี่ยงที่พิจารณาแล้วพบว่ามีผลกระทบต่ำ ถึงแม้ว่ามีโอกาสที่จะเกิดสูง (L, H) นอกจากนี้ ข้อจำกัดอื่นๆ ของแผนผังความเสี่ยงคือจะแสดงเพียงแค่สองตัวแปรในเวลาเดียวกันเท่านั้น (ในที่นี้คือผลกระทบและโอกาสที่จะเกิด)

ภาพที่ 2: แผนผังความเสี่ยง



Practice Guide / Engagement Planning: Establishing Objectives and Scope

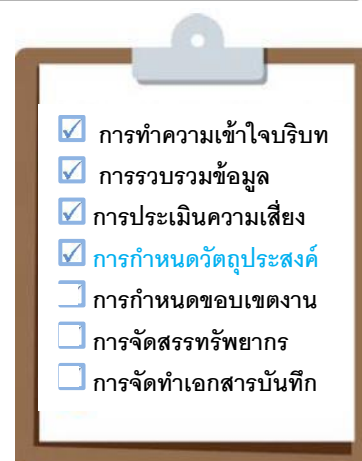
เมื่อจัดทำแผนผังความเสี่ยงแล้ว ผู้ตรวจสอบภายในจะสามารถระบุความเสี่ยงที่มีนัยสำคัญที่จำเป็นต้องรวมไว้ในขณะที่กำหนดวัตถุประสงค์ของงานที่ได้รับมอบหมายได้ง่ายขึ้น (นั่นคือ ความเสี่ยงที่ตกอยู่ในพื้นที่สีแดงและสีส้มของแผนผังความเสี่ยง) **ภาพที่ 3** ในหน้า 20 แสดงความเสี่ยงที่มีนัยสำคัญที่สุดของบัญชีเจ้าหนี้จากตัวอย่างในหน้า 12 โดยพิจารณาจากผลกระทบและโอกาสที่จะเกิดความเสี่ยงดังกล่าว

ภาพที่ 3: ความเสี่ยงที่มีนัยสำคัญ

ความเสี่ยงตามธรรมชาติ	ผลกระทบ (ต่ำ,กลาง,สูง)	โอกาสที่จะเกิด (ต่ำ,กลาง,สูง)
A.3 ไม่ได้นำเสนอ/ตรวจสอบรายงานค่าใช้จ่ายอย่างทันเวลา ส่งผลให้เกิดค่าใช้จ่ายที่ไม่เหมาะสม	สูง	สูง
A.4 รายงานค่าใช้จ่ายที่มีใบเสร็จรับเงินไม่ได้รับการตรวจสอบและอนุมัติโดยบุคคลที่เหมาะสม ส่งผลให้เกิดค่าใช้จ่ายที่ไม่เหมาะสม	สูง	กลาง
B.2 ผู้ขายนำเสนอใบแจ้งหนี้ที่ไม่ถูกต้อง ทำซ้ำหรือปลอมแปลง ซึ่งไม่ได้รับการตรวจสอบและอนุมัติโดยบุคคลที่เหมาะสม	สูง	กลาง
B.1 ผู้ขายปลอมถูกสร้างไว้ในระบบ ส่งผลให้เกิดการทุจริตค่าใช้จ่าย	สูง	ต่ำ
A.1 มีการออกบัตรเครดิตสำหรับองค์กรอย่างไม่เหมาะสม ส่งผลให้เกิดการทุจริตค่าใช้จ่าย	กลาง	กลาง
C.2 ไม่ได้รับส่วนลด เนื่องจากจ่ายชำระเงินภายหลังระยะเวลาได้รับส่วนลด	ต่ำ	สูง

การกำหนดวัตถุประสงค์ของงานที่ได้รับมอบหมาย

เมื่อผู้ตรวจสอบภายในได้ประเมินความเสี่ยงในเบื้องต้นและระบุความเสี่ยงที่มีนัยสำคัญที่จะทำการประเมินในระหว่างปฏิบัติงานที่ได้รับมอบหมายเรียบร้อยแล้ว จึงจะทำการกำหนดวัตถุประสงค์ของงานที่ได้รับมอบหมายได้ ซึ่งวัตถุประสงค์ของงานที่ได้รับมอบหมายนี้จะเป็นสิ่งที่แสดงถึงความแน่ชัดว่างานที่ได้รับมอบหมายนั้นต้องการจะบรรลุผลสำเร็จในเรื่องใด ดังนั้นวัตถุประสงค์ควรมีเป้าหมายที่ชัดเจน มีความกระชับ และมีความเชื่อมโยงกับผลการประเมินความเสี่ยงด้วย (มาตรฐาน 2210.A1)



วัตถุประสงค์ของงานการให้ความเชื่อมั่น

ผู้ตรวจสอบภายในจะต้องมีความแน่ใจว่าวัตถุประสงค์ของงานให้ความเชื่อมั่นมีความสอดคล้องกับวัตถุประสงค์ทางธุรกิจของบริเวณหรือกระบวนการที่จะทำการสอบทาน

งานให้ความเชื่อมั่นควรมุ่งเน้นไปที่การสร้างความมั่นใจว่าการควบคุมนั้นมีอยู่เพื่อจัดการกับความเสี่ยงที่ขัดขวางบริเวณหรือกระบวนการนั้นจากการบรรลุวัตถุประสงค์ทางธุรกิจได้อย่างมีประสิทธิภาพ

ผู้ตรวจสอบภายในจะต้องกำหนดหลักเกณฑ์ที่เพียงพอที่จะประเมินการกำกับดูแล การบริหารความเสี่ยง และการควบคุมของบริเวณหรือกระบวนการที่จะทำการ

สอบทาน และพิจารณาว่าได้รับบรรลุวัตถุประสงค์และเป้าหมายทางธุรกิจหรือไม่ การกำหนดหลักเกณฑ์จะช่วยให้ความมั่นใจว่าวัตถุประสงค์ของงานให้ความเชื่อมั่นนั้นสามารถวัดได้ ใช้ได้จริง และสอดคล้องกับวัตถุประสงค์ของทั้งองค์กรและบริเวณหรือกระบวนการที่จะทำการสอบทาน

วัตถุประสงค์ของงานการให้ความเชื่อมั่นจะต้อง

- สะท้อนถึงความเสี่ยงต่อวัตถุประสงค์ทางธุรกิจของบริเวณหรือกระบวนการที่ได้ประเมินแล้วว่ามีนัยสำคัญจากการประเมินความเสี่ยงในเบื้องต้น (มาตรฐาน 2210.A1)
- พิจารณาถึงความเป็นไปได้ที่จะเกิดข้อผิดพลาด การทุจริต การไม่ปฏิบัติตามกฎระเบียบ และความเสี่ยงอื่นๆ (มาตรฐาน 2210.A2)
- คำนึงถึงเกณฑ์ที่ใช้ในการประเมิน (มาตรฐาน 2210.A3)

IA Practice Guide / Engagement Planning: Establishing Objectives and Scope

ตามมาตรฐาน 2210.A3 กำหนดให้ผู้ตรวจสอบภายในจะต้องใช้เกณฑ์วัดที่กำหนดโดยฝ่ายบริหารและ/หรือ คณะกรรมการหากเกณฑ์ดังกล่าวนั้นมีอยู่ ในกรณีที่ไม่มีเกณฑ์ดังกล่าว ผู้ตรวจสอบภายในจะต้องระบุ หลักเกณฑ์ที่เหมาะสม โดยการหารือร่วมกับฝ่ายบริหารและคณะกรรมการ ทั้งนี้ ผู้ตรวจสอบภายในควร พิจารณาหาข้อมูลจากผู้เชี่ยวชาญแต่ละเรื่องเพื่อช่วยให้สามารถกำหนดตัวเกณฑ์ที่เกี่ยวข้องได้

ตัวอย่างของเกณฑ์วัด ได้แก่

- ดัชนีชี้วัดผลการดำเนินงานที่สำคัญที่มีอยู่
- เป้าหมายที่กำหนดในระหว่างการวางแผนเชิงกลยุทธ์
- ระดับของการปฏิบัติตามนโยบายและขั้นตอนการปฏิบัติงานของบริเวณหรือกระบวนการนั้นๆ กฎหมายและข้อบังคับภายนอก และ/หรือสัญญาต่างๆ
- มาตรฐานหรือเกณฑ์เปรียบเทียบในอุตสาหกรรม

เพื่อหลีกเลี่ยงการตีความผิดพลาดหรือการคัดค้านจากบุคคลใดๆ ที่ทำหน้าที่ในบริเวณหรือกระบวนการที่จะทำการสอบทาน เกณฑ์ในการประเมินควรมีความเกี่ยวข้อง เชื่อถือได้ และมีการบันทึกไว้เป็นลายลักษณ์อักษร เกณฑ์ที่เพียงพอและเหมาะสมจะทำให้ผู้ตรวจสอบภายในสามารถใช้อ้างอิงได้ในการประเมินหลักฐาน มีความเข้าใจในสิ่งที่ตรวจพบ และประเมินความเพียงพอของวิธีการควบคุมในบริเวณหรือกระบวนการที่จะทำการสอบทาน ทั้งนี้ เกณฑ์ที่มีหรือที่ไม่มี ควรนำไปเปรียบเทียบกับเกณฑ์มาตรฐาน แนวโน้มและการคาดการณ์ในอุตสาหกรรม รวมถึงนโยบายและวิธีการปฏิบัติงานขององค์กร

ต่อไปนี้เป็นตัวอย่างวิธีการกำหนดวัตถุประสงค์ของงานให้ความเชื่อมั่นสำหรับบัญชีเจ้าหนี้ที่กล่าวไว้ข้างต้น

หน่วยงานตรวจสอบภายในจะให้ความเชื่อมั่นว่า

- ค่าใช้จ่ายที่เกิดขึ้นมีความเหมาะสมตามนโยบายค่าใช้จ่ายขององค์กร
- การนำส่งรายงานค่าใช้จ่าย การอนุมัติ และการควบคุมในกระบวนการจ่ายเงินมีประสิทธิผลและประสิทธิภาพ
- ค่าใช้จ่ายด้านบุคลากรและค่าใช้จ่ายในการดำเนินงานมีความเหมาะสมและได้รับการอนุมัติ
- การจ่ายชำระค่าใช้จ่ายมีความถูกต้องและทันเวลา

วัตถุประสงค์ของงานให้คำปรึกษา

เนื่องจากงานบริการให้คำปรึกษามีลักษณะของการเป็นที่ปรึกษา ความคาดหวังและวัตถุประสงค์จะถูกพิจารณากำหนดทั้งโดยผู้รับบริการงานนั้นหรือกำหนดร่วมกัน ดังนั้น การวางแผนสำหรับงานให้คำปรึกษามักจะเกิดขึ้นภายหลังจากที่ได้กำหนดวัตถุประสงค์และขอบเขตของงานเรียบร้อยแล้ว ผู้ตรวจสอบภายในอาจไม่จำเป็นต้องทำการประเมินความเสี่ยงในเบื้องต้นอย่างที่ทำในการวางแผนสำหรับงานให้ความเชื่อมั่น อย่างไรก็ตาม มาตรฐาน 2201.C1 กำหนดให้ผู้ตรวจสอบภายในต้องทำความเข้าใจกับผู้รับบริการงานให้คำปรึกษาเกี่ยวกับวัตถุประสงค์ ขอบเขต ความรับผิดชอบของแต่ละฝ่าย และความคาดหวังอื่นๆ ในกรณีที่เป็นงานที่สำคัญ ต้องบันทึกความเข้าใจนี้ไว้เป็นลายลักษณ์อักษรด้วย

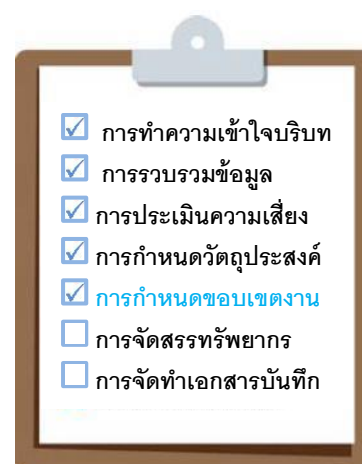
นอกจากนี้ ผู้ตรวจสอบภายในจะต้องระบุถึงกระบวนการกำกับดูแล การบริหารความเสี่ยงและการควบคุม โดยอยู่ในขอบเขตที่ได้ตกลงไว้กับผู้รับบริการงานให้คำปรึกษา (มาตรฐาน 2210.C1) ถึงแม้ว่าวัตถุประสงค์และความคาดหวังของงานให้คำปรึกษาจะถูกกำหนดโดยผู้รับบริการ ผู้ตรวจสอบภายในจะต้องมั่นใจว่าวัตถุประสงค์ของงานให้คำปรึกษามีความสอดคล้องกับคุณค่า กลยุทธ์ และวัตถุประสงค์ทางธุรกิจขององค์กร (มาตรฐาน 2210.C2)

วัตถุประสงค์ของงานให้คำปรึกษาสำหรับบัญชีเจ้าหนี้จะเป็นดังนี้

หน่วยงานตรวจสอบภายในจะให้คำปรึกษาเกี่ยวกับความเสี่ยงต่างๆ จากการว่าจ้างบุคคลภายนอกในกระบวนการที่เกี่ยวข้องกับบัญชีเจ้าหนี้

การกำหนดขอบเขตของงานที่ได้รับมอบหมาย

เมื่อได้กำหนดวัตถุประสงค์ตามความเสี่ยงแล้ว จึงจะสามารถพิจารณาขอบเขตของงานตรวจสอบที่ได้รับมอบหมายได้ เนื่องจากงานที่ได้รับมอบหมายมักจะไม่สามารถครอบคลุมได้หมดทุกสิ่ง ผู้ตรวจสอบภายในจึงต้องพิจารณาว่าสิ่งใดควรและสิ่งใดไม่ควรนำมารวม ขอบเขตของงานที่ได้รับมอบหมายจะเป็นตัวกำหนดขอบข่ายของงานและกำหนดสิ่งที่จะต้องรวมไว้ใน การตรวจสอบ ผู้ตรวจสอบภายในจะต้องพิจารณาขอบข่ายของงานอย่างรอบคอบ เพื่อให้มั่นใจได้ว่าขอบเขตมีความเพียงพอที่จะทำให้บรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมายได้ (มาตรฐาน 2220 เรื่อง ขอบเขตของงานที่ได้รับมอบหมาย)



Practice Guide / Engagement Planning: Establishing Objectives and Scope

ขอบเขตอาจเป็นสิ่งที่กำหนดองค์ประกอบต่างๆ ได้แก่ กระบวนการและ/หรือกิจกรรมโดยเฉพาะ สถานที่ตามภูมิศาสตร์ และช่วงเวลา (เช่น ณ เวลาใดเวลาหนึ่ง ไตรมาส หรือปีปฏิทิน) ซึ่งจะครอบคลุมโดยงานที่ได้รับมอบหมายภายใต้ทรัพยากรที่มีอยู่ ผู้ตรวจสอบภายในจะต้องพิจารณาความกว้างของขอบเขตอย่างรอบคอบ เพื่อให้มั่นใจว่าจะสามารถระบุข้อมูลที่น่าเชื่อถือ มีความเกี่ยวข้องและมีประโยชน์ ที่จะทำให้บรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมายที่กำหนดไว้ได้อย่างทันเวลา (มาตรฐาน 2210 เรื่อง วัตถุประสงค์ของงานที่ได้รับมอบหมาย และ มาตรฐาน 2310 เรื่อง การระบุข้อมูล)

ขอบเขตของงานการให้ความเชื่อมั่น

การพิจารณากำหนดขอบเขตของงานให้ความเชื่อมั่นนั้น เป็นสิ่งที่จะช่วยผู้ตรวจสอบภายในการสอบทานวัตถุประสงค์ของงานที่ได้รับมอบหมาย เพื่อให้มั่นใจว่าแต่ละวัตถุประสงค์จะสามารถบรรลุได้ภายใต้ตัวแปรต่างๆ ที่ได้กำหนดไว้ ทั้งนี้ เพื่อให้มั่นใจได้ว่าขอบเขตมีความเพียงพอที่จะบรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมายและสอดคล้องกับแผนการตรวจสอบภายในประจำปีขององค์กร ผู้ตรวจสอบภายในต้องใช้วิจรรณญาณอย่างมืออาชีพที่ดี โดยอาศัยประสบการณ์ที่เกี่ยวข้องและ/หรือความช่วยเหลือจากผู้บังคับบัญชา ตลอดจนต้องพิจารณาถึงระบบงาน การบันทึกข้อมูล บุคลากร และทรัพย์สินที่จับต้องได้ทั้งหมด (มาตรฐาน 2220.A1)

ผู้ตรวจสอบภายในควรพิจารณาด้วยว่าปัจจัยทางกฎหมายจะมีผลกระทบต่อขอบเขตของงานที่ได้รับมอบหมายได้อย่างไร ตัวอย่างเช่น หากองค์กรหรือบริเวณที่จะทำการสอบทานมีสัญญาห้ามการเปิดเผยข้อมูลแก่บุคคลที่สาม องค์กรอาจจำเป็นต้องแจ้งหน่วยงานทางการที่มีหน้าที่กำกับดูแลก่อนเริ่มต้นปฏิบัติงาน นอกจากนี้ ยังต้องคำนึงถึงข้อพิพาทที่คงค้างหรือใกล้จะเกิดขึ้น และกรณีที่มีการไม่ปฏิบัติตามกฎระเบียบด้วย

รายการต่อไปนี้เป็นรายการที่อาจนำมารวมและไม่นำมารวมอยู่ในขอบเขตของงานให้ความเชื่อมั่นบัญชีเจ้าหนี้

- ค่าใช้จ่าย (ในการดำเนินงาน เดินทาง วัสดุสิ้นเปลือง บุคลากร และ/หรือองค์กร เป็นต้น)
- บุคลากร (ผู้บริหารระดับสูง ฝ่ายบริหาร บุคลากรทั้งหมด เป็นต้น)
- สถานที่ตั้ง (ออฟฟิศสำนักงาน สถานที่ดำเนินงาน ประเทศ เป็นต้น)
- กรอบระยะเวลา (ปัจจุบัน อดีต รายเดือน รายไตรมาส รายปี เป็นต้น)
- ความมีสาระสำคัญ (จำนวนเงินใดๆ หรือเฉพาะจำนวนที่สูงเกินกว่าระดับที่อนุมัติได้ เป็นต้น)

IA Practice Guide / Engagement Planning: Establishing Objectives and Scope

- ระบบงาน (เฉพาะระบบงานที่ใช้ประมวลผลค่าใช้จ่าย หรือระบบทรัพยากรบุคคล หรือทุกระบบงาน เป็นต้น)

ต่อไปนี้เป็นตัวอย่างของขอบเขตของงานที่ได้รับมอบหมายสำหรับงานให้ความเชื่อมั่นสำหรับบัญชีเจ้าหนี้ดังกล่าวข้างต้น

งานให้ความเชื่อมั่นจะครอบคลุมค่าใช้จ่ายพนักงานและค่าใช้จ่ายในการดำเนินงานสำหรับงวด 12 เดือนสิ้นสุดในเดือนสิงหาคม ปี 20XX และกระบวนการนำส่ง อนุมัติ และรายงานค่าใช้จ่ายที่ได้จ่ายชำระ (รวมถึงซอฟต์แวร์ของหน่วยงานภายนอกที่ใช้ในการนำส่งรายงานค่าใช้จ่าย) ขอบเขตของงานที่ได้รับมอบหมายจะรวมถึงบุคลากรทุกคนที่ใช้ซอฟต์แวร์ของหน่วยงานภายนอกในการนำส่งค่าใช้จ่ายด้านการพนักงานและค่าใช้จ่ายดำเนินงาน นอกจากนี้งานที่ได้รับมอบหมายจะครอบคลุมการสอบทานการปฏิบัติตามนโยบายค่าใช้จ่ายขององค์กร

หากขอบเขตของงานให้ความเชื่อมั่นที่ได้รับมอบหมายถูกจำกัดไม่ว่าจะในลักษณะใดก็ตาม หรือการเข้าถึงแหล่งข้อมูลที่เป็นถูกจำกัด ผู้ตรวจสอบภายในต้องเปิดเผยสถานการณ์เหล่านี้ให้ผู้บริหารระดับสูงและ/หรือคณะกรรมการได้รับทราบ สถานการณ์ดังกล่าวอาจถือได้ว่าเป็นการทำให้ความเป็นอิสระของตรวจสอบภายในเสียได้ (มาตรฐาน 1130 เรื่อง การเสื่อมเสียความเป็นอิสระหรือความเที่ยงธรรม)

ในระหว่างปฏิบัติงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในอาจได้รับข้อมูลใหม่ๆ ที่จำเป็นต้องปรับปรุงขอบเขตของงานที่ได้รับมอบหมาย ตัวอย่างเช่น หากบริษัทย่อยกำลังจะปิดตัวและชำระบัญชีอยู่ ขอบเขตของงานที่ได้รับมอบหมายอาจเปลี่ยนแปลงโดยนำบริษัทที่ได้รับผลกระทบออกและนำบริษัทย่อยอื่นเข้ามารวมแทน เช่นเดียวกันกับกรณีที่กระบวนการหนึ่งเพียงมีการเปลี่ยนแปลงไปไม่นาน ผู้ตรวจสอบภายในควรพิจารณาว่ากระบวนการดังกล่าวยังคงอยู่ในขอบเขตหรือไม่ (เช่น ยังคงควรรวมอยู่ในงานที่รับมอบหมายในปัจจุบันหรือไม่) หรือการเปลี่ยนแปลงดังกล่าวควรได้รับการสอบทานแยกออกไปต่างหาก ในกรณีเช่นนี้ ผู้ตรวจสอบภายในอาจเลือกที่จะเปลี่ยนจุดมุ่งเน้นของงานที่ได้รับมอบหมายเป็นเพื่อให้ความเชื่อมั่นต่อกระบวนการใหม่ นำกระบวนการใหม่รวมเข้าไปในแผนการตรวจสอบภายในประจำปี หรือทำการปฏิบัติงานให้คำปรึกษาแยกต่างหาก

Practice Guide / Engagement Planning: Establishing Objectives and Scope

เมื่อได้เริ่มปฏิบัติงานให้ความเชื่อมั่น การปรับปรุงใดๆ ต่อแนวทางการปฏิบัติงาน (ซึ่งรวมถึงการเปลี่ยนแปลงใดๆ ในขอบเขต) จะต้องได้รับการอนุมัติ (มาตรฐาน 2240.A1) นอกจากนี้ หากมีโอกาสในการให้บริการให้คำปรึกษาที่มีนัยสำคัญเกิดขึ้นในระหว่างการปฏิบัติงานให้ความเชื่อมั่น ผู้ตรวจสอบภายในควรพิจารณาว่าจำเป็นต้องขออนุมัติเพื่อดำเนินงานให้คำปรึกษาแยกต่างหากหรือไม่ หากจำเป็น ผู้ตรวจสอบภายในควรทำความเข้าใจกับผู้รับบริการเป็นลายลักษณ์อักษรเกี่ยวกับวัตถุประสงค์ ขอบเขต ภาระหน้าที่ของแต่ละฝ่าย และความคาดหวังอื่นๆ ของผู้รับบริการ รวมทั้งการสื่อสารผลของการปฏิบัติงานให้คำปรึกษาซึ่งต้องเป็นไปตามมาตรฐานที่เกี่ยวข้องกับงานการให้คำปรึกษา (มาตรฐาน 2220.A2)

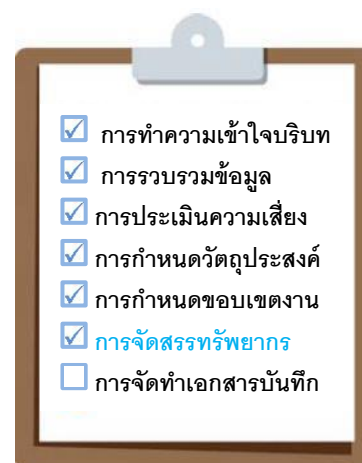
ขอบเขตของงานให้คำปรึกษา

ขอบเขตของงานให้คำปรึกษาจะถูกออกแบบมาเพื่อตอบสนองต่อความคาดหวังของผู้รับบริการ ตามที่กำหนดไว้ในมาตรฐาน 2220.C1 ขอบเขตของงานให้คำปรึกษาจะต้องเพียงพอที่จะบรรลุวัตถุประสงค์ที่ได้ตกลงไว้กับผู้รับบริการ หากผู้ตรวจสอบภายในได้กำหนดเงื่อนไขเกี่ยวกับขอบเขตขึ้นมาในระหว่างการปฏิบัติงาน จะต้องมีการพูดคุยถึงเงื่อนไขเหล่านี้กับผู้รับบริการ เพื่อตัดสินใจว่าจะยังคงต้องการให้ปฏิบัติงานต่อไปหรือไม่ ตัวอย่างเช่น ผู้ตรวจสอบภายในอาจกำหนดเงื่อนไขในสถานการณ์ที่มีข้อมูลไม่เพียงพอที่จะปฏิบัติงานให้คำปรึกษาได้ หรือเห็นว่าผลจากการปฏิบัติงานดังกล่าวอาจไม่เพิ่มคุณค่าให้แก่องค์กร

นอกจากนี้ มาตรฐาน 2220.C2 กำหนดให้ผู้ตรวจสอบภายในต้องกล่าวถึงวิธีการควบคุมให้สอดคล้องกับวัตถุประสงค์ของงานที่ได้รับมอบหมายและต้องตื่นตัวต่อประเด็นการควบคุมที่มีนัยสำคัญ ยิ่งไปกว่านี้ มาตรฐาน 2130.C1 ได้กำหนดให้ผู้ตรวจสอบภายในต้องผนวกเอาความรู้ในเรื่องของการควบคุมที่ได้มาจากการให้บริการให้คำปรึกษาไปใช้ในการประเมินกระบวนการควบคุมขององค์กรด้วย

การจัดสรรทรัพยากร

ภายหลังจากกำหนดวัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมายแล้ว ผู้ตรวจสอบภายในจะต้องพิจารณาความเหมาะสมและเพียงพอของทรัพยากรเพื่อให้บรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมาย ตามที่กำหนดไว้ในมาตรฐาน 2230 เรื่อง การจัดสรรทรัพยากรสำหรับงานที่ได้รับมอบหมาย บทตีความของมาตรฐาน 2230 ได้อธิบายคำว่า “เหมาะสม” ไว้ว่า หมายถึง ส่วนผสมของความรู้ ทักษะรวมทั้งความสามารถอื่นๆ ที่จำเป็นในการปฏิบัติงาน และคำว่า “เพียงพอ” หมายถึง ปริมาณทรัพยากรที่จำเป็นในการปฏิบัติงานให้สำเร็จโดยใช้ความระมัดระวังในทางวิชาชีพอย่างเหมาะสม



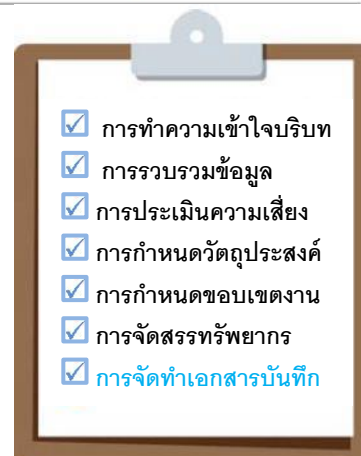
ทรัพยากรจะถูกจัดสรรให้แก่งานที่ได้รับมอบหมายโดยพิจารณาจากสิ่งต่อไปนี้

- ความรู้ของผู้ตรวจสอบภายในที่ได้มาในระหว่างการวางแผนสำหรับงานที่ได้รับมอบหมาย
- ลักษณะและความซับซ้อนของงานที่ได้รับมอบหมาย
- ข้อจำกัดทางด้านเวลาและ/หรือจำนวนชั่วโมงที่ได้ประมาณไว้สำหรับงานที่ได้รับมอบหมาย
- ความรู้ ทักษะ และประสบการณ์ของทรัพยากรที่มีอยู่

ผู้ตรวจสอบภายในควรพิจารณาด้วยว่าทรัพยากรจากภายนอก (เช่น ผู้เชี่ยวชาญ หรือทรัพยากรเพิ่มเติม) หรือเทคโนโลยีมีความจำเป็นหรือไม่ หากหน่วยงานตรวจสอบภายในไม่มีทรัพยากรที่เหมาะสมหรือเพียงพอ

การจัดทำเอกสารบันทึกแผนงาน

ในระหว่างการวางแผน ผู้ตรวจสอบภายในควรจัดทำบันทึกข้อมูลไว้ในกระดาษทำการของงานที่ได้รับมอบหมาย ข้อมูลนี้จะกลายเป็นส่วนหนึ่งของแนวทางการปฏิบัติงานซึ่งต้องจัดทำขึ้นเพื่อให้บรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมาย ตามที่กำหนดไว้ในมาตรฐาน 2240 เรื่อง แนวการปฏิบัติงาน



กระบวนการกำหนดวัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมายอาจก่อให้เกิดกระดาษทำการอันใดอันหนึ่งหรือทั้งหมดดังต่อไปนี้

- แผนผังกระบวนการ
- การทำสรุปจากช่วงการสัมภาษณ์และระดมสมอง
- การประเมินความเสี่ยงในเบื้องต้น (เช่น ตารางเมทริกซ์ความเสี่ยงและการควบคุม และแผนผังความเสี่ยง)
- เหตุผลในการตัดสินใจเกี่ยวกับว่า ความเสี่ยงตัวไหนที่จะถูกรวมไว้ในงานที่ได้รับมอบหมาย
- เกณฑ์ที่จะใช้ในการประเมินบริเวณหรือกระบวนการที่จะทำการสอบทาน (จำเป็นสำหรับงานให้ความเชื่อมั่น ตามมาตรฐาน 2210.A3)

หัวหน้าหน่วยงานตรวจสอบภายในและ/หรือผู้ที่ได้รับมอบหมายให้ควบคุมงาน ควรสอบทานกระดาษทำการทั้งหมดเพื่อยืนยันว่าข้อมูลมีความครบถ้วนและถูกต้อง การสอบทานเอกสารโดยผู้บังคับบัญชาควรสอบทานว่า วัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมายนั้นได้สะท้อนถึงผลการประเมินความเสี่ยงในเบื้องต้น และเกณฑ์ที่ใช้ในการประเมินที่ได้ถูกระบุหรือมีกำหนดไว้ สำหรับงานให้ความเชื่อมั่นนั้น แนวการปฏิบัติงานจะต้องได้รับการอนุมัติก่อนนำไปใช้ (มาตรฐาน 2240.A1) แต่ในทางกลับกัน ข้อกำหนดสำหรับแนวการปฏิบัติงานการให้คำปรึกษานั้นจะขึ้นอยู่กับลักษณะของงานที่ได้รับมอบหมาย

นอกจากนี้ ผลการประเมินความเสี่ยงในเบื้องต้น วัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมายควรนำไปหารือกับฝ่ายบริหารของบริเวณหรือกระบวนการที่จะทำการสอบทาน รวมทั้งผู้มีส่วนได้เสียที่สำคัญทั้งองค์กร (เช่น ผู้จัดการความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎระเบียบ หัวหน้าหน่วยงานบริหารความเสี่ยง และ

Practice Guide / Engagement Planning: Establishing Objectives and Scope

ผู้บริหารระดับสูง) การหรือดังกล่าวจะเป็นการเปิดโอกาสให้ทุกๆ หน่วยงานได้ทำความเข้าใจร่วมกันเกี่ยวกับผลการประเมินความเสี่ยง ระดับของงานที่ได้รับมอบหมาย เพื่อยืนยันถึงความเสี่ยงและวิธีการควบคุมที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย ตลอดจนเข้าใจสถานะของตนในการประเมินความเสี่ยงระดับทั่วทั้งองค์กร การหรือควรรวมถึงการยืนยันว่าคุณคลากรและทรัพยากรที่สำคัญจะมีเวลาให้ในระหว่างการปฏิบัติงานที่ได้รับมอบหมาย ทั้งนี้ ข้อมูลเหล่านี้อาจจะถูกสื่อสารไปยังคณะกรรมการเพื่อทราบด้วย

ผู้ตรวจสอบภายในอาจจัดทำเอกสารบันทึกการวางแผนของงานที่ได้รับมอบหมาย (บันทึกการวางแผน) เพื่อใช้สื่อสารวัตถุประสงค์ ขอบเขตและช่วงเวลาที่จะปฏิบัติงานของงานที่ได้รับมอบหมาย บันทึกการวางแผนนี้จะเปิดโอกาสให้ผู้ตรวจสอบภายในสร้างความมั่นใจว่าฝ่ายบริหารของบริเวณหรือกระบวนการที่จะทำการสอบทานมีความเข้าใจและให้การสนับสนุนแผนงานดังกล่าว หากฝ่ายบริหารไม่เห็นด้วยกับองค์ประกอบใดในแผน ผู้ตรวจสอบภายในอาจทำการปรับปรุงหรือบันทึกเหตุผลหากไม่สามารถปรับปรุงตามข้อโต้แย้งของฝ่ายบริหารได้ นอกจากนี้ บันทึกการวางแผนอาจช่วยผู้ตรวจสอบภายในในการสื่อสารงานที่ได้รับมอบหมายไปยังผู้ตรวจสอบภายในคนอื่นๆ และคณะกรรมการได้ ทั้งนี้ การจัดทำบันทึกแผนงานและความคิดเห็นของฝ่ายบริหารไว้อย่างเป็นทางการเป็นลายลักษณ์อักษรมักจะถูกรวมไว้เป็นส่วนหนึ่งของกระดาษทำการของงานที่ได้รับมอบหมาย

การวางแผนและการจัดทำเอกสารอย่างละเอียดนั้น นอกจากจะจำเป็นที่ต้องปฏิบัติเพื่อให้สอดคล้องกับมาตรฐานแล้ว ยังเป็นขั้นตอนสำคัญที่จะช่วยให้ผู้ตรวจสอบภายในสามารถเตรียมการและปฏิบัติงานที่ได้รับมอบหมายได้สำเร็จลุล่วง เนื่องจากไม่ใช่ทุกความเสี่ยงที่จะสามารถหรือควรรวมไว้ในงานที่ได้รับมอบหมายเพียงงานเดียว แต่การวางแผนอย่างเหมาะสมจะช่วยให้ผู้ตรวจสอบภายในในการให้ความสำคัญไปที่ความเสี่ยงที่มีนัยสำคัญที่สุดภายในบริเวณหรือกระบวนการที่จะทำการสอบทานได้

ภาคผนวก ก มาตรฐานของสมาคมผู้ตรวจสอบภายในที่เกี่ยวข้อง

มาตรฐานการปฏิบัติงานวิชาชีพการตรวจสอบภายในที่เป็นสากลของ IIA ได้ถูกคัดเลือกเฉพาะที่เกี่ยวข้องกับแนวปฏิบัติฉบับนี้ตามที่ระบุไว้ด้านล่าง เพื่อเป็นการช่วยเหลือในการนำมาตรฐานไปปฏิบัติใช้นั้น ทาง IIA ขอแนะนำให้ผู้ตรวจสอบภายในไปดูที่แนวทางการนำมาตรฐานไปใช้ปฏิบัติ (Implementation Guide--IG) ที่เกี่ยวข้องกับมาตรฐานแต่ละฉบับ

มาตรฐาน 2200 – การวางแผนสำหรับงานที่ได้รับมอบหมาย

ผู้ตรวจสอบภายในต้องจัดทำและจัดบันทึกแผนสำหรับแต่ละงานที่ได้รับมอบหมาย ซึ่งรวมถึง วัตถุประสงค์ ขอบเขต ช่วงเวลาที่จะปฏิบัติงาน และการจัดสรรทรัพยากรสำหรับงานนั้นๆ แผนนี้จะต้องคำนึงถึง กลยุทธ์ วัตถุประสงค์ขององค์กร และความเสี่ยงที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย

มาตรฐาน 2201 - ข้อพิจารณาในการวางแผน

ในการวางแผนสำหรับงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในต้องคำนึงถึง:

- กลยุทธ์และวัตถุประสงค์ของกิจกรรมที่กำลังจะสอบทานและวิธีการที่จะใช้ในการควบคุมผลการดำเนินงานของกิจกรรมนั้น
- ความเสี่ยงที่มีนัยสำคัญต่อ วัตถุประสงค์ ทรัพยากร และการดำเนินงานของกิจกรรมนั้น ตลอดจนหนทางที่จะใช้ในการจัดการกับผลกระทบที่อาจเกิดจากความเสี่ยงนั้น ให้อยู่ในระดับที่ยอมรับได้
- ความเพียงพอและควมมีประสิทธิภาพของกระบวนการการกำกับดูแล การบริหารความเสี่ยงและการควบคุมของกิจกรรมนั้นเมื่อเปรียบเทียบกับกรอบปฏิบัติหรือต้นแบบที่เกี่ยวข้อง
- โอกาสที่จะปรับปรุงกระบวนการการกำกับดูแล การบริหารความเสี่ยงและการควบคุมสำหรับกิจกรรมนั้นได้อย่างมีนัยสำคัญ

2201.A1 – ในการวางแผนการปฏิบัติงานสำหรับกลุ่มบุคคลภายนอกองค์กร ผู้ตรวจสอบภายในต้องทำความเข้าใจกับผู้รับบริการเป็นลายลักษณ์อักษรเกี่ยวกับวัตถุประสงค์ ขอบเขต ภาระหน้าที่ของแต่ละฝ่าย และความคาดหวังอื่นๆ ของผู้รับบริการ รวมทั้งข้อจำกัดในการเผยแพร่ผลงานและการเข้าถึงเอกสารข้อมูลที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย

2201.C1 – ในงานให้คำปรึกษา ผู้ตรวจสอบภายในต้องทำความเข้าใจกับผู้รับบริการเกี่ยวกับวัตถุประสงค์ ขอบเขต ความรับผิดชอบของแต่ละฝ่าย และความคาดหวังอื่นๆ ของผู้รับบริการ ในกรณีที่เป็นงานที่สำคัญ ต้องบันทึกความเข้าใจไว้เป็นลายลักษณ์อักษร

มาตรฐาน 2210 – วัตถุประสงค์ของงานที่ได้รับมอบหมาย

ต้องมีการกำหนดวัตถุประสงค์สำหรับงานแต่ละงานที่ได้รับมอบหมาย

2210.A1 – ผู้ตรวจสอบภายในต้องทำการประเมินเบื้องต้นถึงความเสี่ยงที่เกี่ยวข้องกับกิจกรรมที่ตรวจสอบวัตถุประสงค์ของงานที่ได้รับมอบหมายต้องสะท้อนให้เห็นผลจากการประเมินนี้

2210.A2 – ในการกำหนดวัตถุประสงค์ของงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในต้องคำนึงถึงความเป็นไปได้ที่จะเกิดข้อผิดพลาด การทุจริต การไม่ปฏิบัติตามกฎระเบียบ และความเสี่ยงอื่นๆ ที่มีนัยสำคัญ

2210.A3 – เกณฑ์ที่เพียงพอเป็นสิ่งจำเป็นต่อการประเมินการกำกับดูแล การบริหารความเสี่ยง และการควบคุม ผู้ตรวจสอบภายในต้องมั่นใจในขอบเขตที่ฝ่ายบริหารและ/หรือคณะกรรมการใช้ในการกำหนดเกณฑ์ที่เหมาะสมเพื่อตัดสินได้ว่าการบรรลุวัตถุประสงค์และเป้าหมายแล้ว หากเหมาะสมแล้ว ผู้ตรวจสอบภายในต้องใช้เกณฑ์นั้นในการประเมินผล หากยังไม่เหมาะสม ผู้ตรวจสอบภายในต้องระบุเกณฑ์การประเมินที่เหมาะสมด้วยการหารือกับฝ่ายบริหารและ/หรือคณะกรรมการ

บทตีความ :

ประเภทของเกณฑ์ต่างๆ ได้แก่

- เกณฑ์ภายใน (เช่น นโยบาย และคู่มือการปฏิบัติงานขององค์กร)
- เกณฑ์ภายนอก (เช่น กฎหมายและระเบียบข้อบังคับซึ่งกำหนดโดยทางการ)
- เกณฑ์ซึ่งเป็นวิธีปฏิบัติชั้นนำ (เช่น แนวทางของอุตสาหกรรมและในทางวิชาชีพ)

มาตรฐาน 2220 – ขอบเขตของงานที่ได้รับมอบหมาย

ขอบเขตของงานที่ได้รับมอบหมายที่กำหนดขึ้นนั้น จะต้องเพียงพอที่จะบรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมายได้

IA Practice Guide / Engagement Planning: Establishing Objectives and Scope

2220.A1 – ขอบเขตของงานที่ได้รับมอบหมายต้องรวมถึงการคำนึงถึงสิ่งต่าง ๆ ที่เกี่ยวข้อง ได้แก่ ระบบงาน การบันทึกข้อมูล บุคลากร และทรัพย์สินที่จับต้องได้รวมทั้งทรัพย์สินที่อยู่ในความควบคุมดูแลของกลุ่มบุคคลที่สาม

2220.A2 – หากมีโอกาสในการให้บริการให้คำปรึกษาที่มีนัยสำคัญเกิดขึ้นในระหว่างการปฏิบัติงาน ให้ความเชื่อมั่น ผู้ตรวจสอบภายในควรทำความเข้าใจกับผู้รับบริการเป็นลายลักษณ์อักษรเกี่ยวกับวัตถุประสงค์ ขอบเขต ภาระหน้าที่ของแต่ละฝ่าย และความคาดหวังอื่น ๆ ของผู้รับบริการ รวมทั้งการสื่อสารผลของการปฏิบัติงานให้คำปรึกษาซึ่งต้องเป็นไปตามมาตรฐานที่เกี่ยวกับงานการให้คำปรึกษา

2220.C1 – ในการปฏิบัติงานให้คำปรึกษา ผู้ตรวจสอบภายในต้องมั่นใจว่าได้กำหนดขอบเขตของงานที่ได้รับมอบหมายไว้เพียงพอที่จะบรรลุวัตถุประสงค์ที่ได้ตกลงไว้ หากผู้ตรวจสอบภายในได้กำหนดเงื่อนไขเกี่ยวกับขอบเขตขึ้นมาในระหว่างการปฏิบัติงาน จะต้องมีการพูดคุยถึงเงื่อนไขเหล่านี้กับผู้รับบริการว่าจะยังคงต้องการให้ปฏิบัติงานต่อไปหรือไม่

2220.C2 – ในระหว่างการปฏิบัติงานให้คำปรึกษา ผู้ตรวจสอบภายในต้องกล่าวถึงวิธีการควบคุมให้สอดคล้องกับวัตถุประสงค์ของงานที่ได้รับมอบหมายและต้องตื่นตัวต่อประเด็นการควบคุมที่มีนัยสำคัญ

มาตรฐาน 2230 – การจัดสรรทรัพยากรสำหรับงานที่ได้รับมอบหมาย

ผู้ตรวจสอบภายในต้องกำหนดทรัพยากรให้เหมาะสมและเพียงพอเพื่อให้บรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมายได้โดยอาศัยการประเมินลักษณะและความซับซ้อนของงานที่ได้รับมอบหมายแต่ละงาน ข้อจำกัดในเรื่องเวลารวมทั้งทรัพยากรที่มีอยู่

บทตีความ :

คำว่า 'เหมาะสม' หมายถึง ส่วนผสมของ ความรู้ ทักษะ รวมทั้งความสามารถอื่น ๆ ที่จำเป็นในการปฏิบัติงาน คำว่า 'เพียงพอ' หมายถึง ปริมาณทรัพยากรที่จำเป็นในการปฏิบัติงานให้สำเร็จโดยใช้ความระมัดระวังในทางวิชาชีพอย่างเหมาะสม

ภาคผนวก ข ภาคอภิธานศัพท์

คำศัพท์ที่ระบุด้วยเครื่องหมายดอกจัน (*) เป็นคำศัพท์ที่นำมาจากภาคอภิธานศัพท์ของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากลของ IIA

Assurance Services - การบริการให้ความเชื่อมั่น*: การตรวจสอบหลักฐานอย่างเที่ยงธรรมเพื่อให้ได้มาซึ่งการประเมินกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุมขององค์กร อย่างเป็นอิสระ ตัวอย่าง ได้แก่ การตรวจสอบทางการเงิน การตรวจสอบผลการปฏิบัติงาน การตรวจสอบการปฏิบัติตามกฎระเบียบ การตรวจสอบความมั่นคงปลอดภัยของระบบต่างๆ และการตรวจสอบสถานะกิจการ (Due Diligence Engagement)

Consulting Services – การบริการให้คำปรึกษา*: กิจกรรมการให้คำปรึกษา แนะนำ และบริการที่เกี่ยวข้องกับผู้รับบริการ โดยลักษณะและขอบเขตของงานจะเป็นไปตามข้อตกลงที่ทำขึ้นร่วมกันกับผู้รับบริการ โดยมีเป้าหมายที่จะเพิ่มคุณค่าและปรับปรุงกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุมขององค์กร โดยผู้ตรวจสอบภายในต้องไม่เข้าไปรับภาระหน้าที่ในทางการบริหาร ตัวอย่าง ได้แก่ การให้คำปรึกษาคำแนะนำ การอำนวยความสะดวก และการฝึกอบรม

Control – การควบคุม*: การกระทำใด ๆ โดยฝ่ายบริหาร คณะกรรมการ และกลุ่มบุคคลอื่น ๆ เพื่อจัดการกับความเสี่ยงและเพิ่มความเป็นไปได้ในอันที่จะบรรลุวัตถุประสงค์และเป้าหมายที่กำหนดไว้ ผู้บริหารจะวางแผนจัดระบบ รวมทั้งกำกับและสั่งการให้เกิดการปฏิบัติอย่างเพียงพอเพื่อก่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลว่าจะบรรลุวัตถุประสงค์และเป้าหมายได้

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

Practice Guide / Engagement Planning: Establishing Objectives and Scope

Engagement Objectives – วัตถุประสงค์ของงานที่ได้รับมอบหมาย*: คำแถลงอย่างกว้าง ๆ ที่จัดทำโดยผู้ตรวจสอบภายใน ซึ่งกำหนดสิ่งที่ต้องการจะบรรลุในงานที่ได้รับมอบหมายนั้น

Engagement scope - ขอบเขตของงานที่ได้รับมอบหมาย: สิ่งที่มีงเน้นและขอบข่ายของงานที่ได้รับมอบหมายที่กำหนดโดยผู้ตรวจสอบภายใน ซึ่งระบุถึงกิจกรรม กระบวนการ ระบบงาน ช่วงเวลาและองค์ประกอบอื่นๆ ที่ต้องนำมารวมไว้

Risk – ความเสี่ยง*: ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่จะส่งผลกระทบต่อการบรรลุเป้าหมายขององค์กร ความเสี่ยงวัดได้จากผลกระทบจากเหตุการณ์และโอกาสที่จะเกิดเหตุการณ์นั้น

Significance – ความมีนัยสำคัญ*: ความสำคัญที่เกี่ยวข้องกับประเด็นที่กำลังพิจารณา ซึ่งรวมถึงปัจจัยทั้งในเชิงคุณภาพและเชิงปริมาณ เช่น ขนาด ลักษณะ ผลกระทบ ความเกี่ยวข้อง และความร้ายแรง ดุลพินิจอย่างมีอาชีพจะช่วยให้ผู้ตรวจสอบในการประเมินความมีนัยสำคัญของประเด็นภายใต้วัตถุประสงค์ที่เกี่ยวข้อง

กิตติกรรมประกาศ

ทีมงานพัฒนาแนวปฏิบัติ

Glenn Ho, CIA, CRMA, South Africa (Chairman)

Caroline Glynn, CIA, United States (Project Lead)

Doug Hileman, CRMA, CPEA, United States

Thomas Sanglier, CIA, CRMA, United States

ผู้ให้คำแนะนำแนวปฏิบัติที่มาจากทั่วโลก

Farah Araj, CIA, QIAL, Canada

ÖzgeAscioglu, CIA, CFSA, CRMA, Turkey

Cheryl Dove, United Kingdom

Stephen Germain, CIA, United States

Lee Wyckoff, CIA, United States

มาตรฐานและแนวทางปฏิบัติระดับสากลของ IIA

Christine Hovious, CIA, CRMA, Director (Project Lead)

Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President

Debi Roth, CIA, Managing Director

Lauressa Nelson, Technical Writer

Christina Brune, Technical Writer

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 190,000 คน จากมากกว่า 170 ประเทศและดินแดน สำนักงานใหญ่ของสมาคมตั้งอยู่ที่เลคแมรี (Lake Mary) มลรัฐฟลอริดา สหรัฐอเมริกา สำหรับข้อมูลเพิ่มเติมโปรดเยี่ยมชม <https://global.theiia.org>

เกี่ยวกับแนวทางเสริม (Supplemental Guidance)

แนวทางเสริมเป็นส่วนหนึ่งของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล (IPPF) ของ IIA และให้แนวทางเพิ่มเติม (ไม่บังคับ) สำหรับการปฏิบัติกิจกรรมต่างๆ ของหน่วยงานตรวจสอบภายใน โดยที่แนวทางเสริมสนับสนุนมาตรฐาน **แนวทางเสริม**จึงไม่ได้ต้องการที่จะเชื่อมโยงโดยตรงกับความสำเร็จในการปฏิบัติให้สอดคล้องกับมาตรฐาน แต่มีวัตถุประสงค์เพื่อพูดถึงประเด็นเฉพาะ รวมทั้งประเด็นบางประเด็นของบางภาคส่วน กับมีกระบวนการและวิธีการโดยรายละเอียดใส่ไว้ให้ด้วย แนวทางนี้ได้รับการรับรองโดย IIA โดยผ่านกระบวนการสอบทานและการอนุมัติอย่างเป็นทางการมาแล้ว

แนวปฏิบัติ (Practice Guides)

แนวปฏิบัติเป็นรูปแบบหนึ่งของแนวทางเสริม (Supplemental Guidance) ที่ให้แนวทางสำหรับการดำเนินกิจกรรมตรวจสอบภายในโดยละเอียด ซึ่งรวมถึงรายละเอียดของกระบวนการและวิธีการต่างๆ เช่น เครื่องมือและเทคนิค โปรแกรม และขั้นตอนที่ละเอียด รวมถึงตัวอย่างผลงานที่ส่งมอบ ในฐานะที่แนวปฏิบัติถือเป็นส่วนหนึ่งของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล (IPPF) จึงเพียงแค่นำไปปฏิบัติสอดคล้องกับแนวปฏิบัติ (แต่ไม่บังคับ) แนวปฏิบัติได้รับการรับรองโดย IIA โดยผ่านกระบวนการสอบทานและการอนุมัติอย่างเป็นทางการมาแล้ว

แนวการตรวจสอบเทคโนโลยีสารสนเทศระดับโลก (Global Technologies Audit Guide--GTAG) เป็นรูปแบบหนึ่งของแนวปฏิบัติที่เขียนขึ้นโดยใช้ภาษาธุรกิจที่ตรงไปตรงมา เพื่อก้าวถึงประเด็นต่างๆ ที่เกี่ยวข้องกับการบริหาร การควบคุม หรือความปลอดภัยที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศภายใน ในช่วงเวลาที่เหมาะสม

สำหรับเอกสารแนะนำแนวทางอื่นๆ ที่จัดทำและรับรองโดยสมาคมผู้ตรวจสอบภายใน ท่านสามารถเยี่ยมชมเว็บไซต์ของเราได้ที่ www.globaliia.org/standards-guidance

ข้อความปฏิเสธความรับผิดชอบ

IIA ตีพิมพ์เอกสารนี้เพื่อจุดประสงค์ในการให้ข้อมูลและเพื่อการศึกษาเท่านั้น และไม่ได้มีวัตถุประสงค์เพื่อให้คำตอบที่ชัดเจนที่สุดสำหรับสถานการณ์เฉพาะแต่ละสถานการณ์ ดังนั้น จึงมีวัตถุประสงค์เพียงเพื่อใช้เป็นแนวทางในการปฏิบัติงานเท่านั้น IIA จึงใคร่แนะนำให้ท่านขอคำปรึกษาจากผู้เชี่ยวชาญอิสระซึ่งมีความรู้เกี่ยวข้องโดยตรงกับสถานการณ์เฉพาะนั้นๆ IIA จะไม่รับผิดชอบใดๆ ต่อการที่ผู้ใดก็ตามเชื่อและอาศัยคำแนะนำนี้แต่เพียงอย่างเดียว

ลิขสิทธิ์

ลิขสิทธิ์© สมาคมผู้ตรวจสอบภายใน พ.ศ. 2560

หากต้องการขออนุญาตทำซ้ำ โปรดติดต่อ guidance@theiia.org.

17 สิงหาคม