การประเมินกระบวนการบริหารความเสี่ยง

The Institute of Internal Auditors | Global

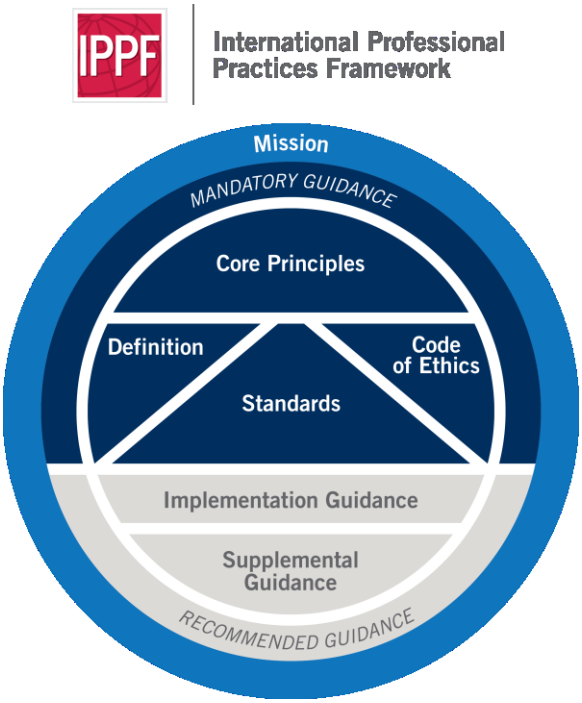
เกี่ยวกับ IPPF

กรอบโครงสร้างการปฏิบัติงานวิชาชีพสากล (IPPF®) คือ กรอบโครงสร้างการทำงานตามแนวคิดที่ IIA ได้ประกาศใช้เพื่อเป็นแนวทางปฏิบัติสำหรับวิชาชีพตรวจสอบภายในทั่วโลก

แนวทางภาคบังคับ (Mandatory Guidance) ถูกพัฒนาขึ้นตามกระบวนการการศึกษาอย่างละเอียดลึกซึ้ง ซึ่งได้มีการเปิดเผยต่อสาธารณะเพื่อที่ผู้มีส่วนได้เสียจะได้ให้ข้อมูลความคิดเห็นได้ องค์ประกอบภาคบังคับของ IPPF ประกอบไปด้วย

- หลักการพื้นฐานที่สำคัญสำหรับการปฏิบัติงานวิชาชีพตรวจสอบภายใน
- คำจำกัดความความของการตรวจสอบภายใน
- ประมวลจรรยาบรรณ
- *มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน*

ประยุกต์ใช้และปฏิบัติให้สอดคล้องกับข้อกำหนดเหล่านั้นได้อย่างไร



ในส่วนที่เป็นแนวทางที่แนะนำจะประกอบไปด้วย แนวทางการนำมาตรฐานไปใช้ปฏิบัติ (Implementation Guidance) และ แนวทางเสริม (Supplemental Guidance) แนวทางการนำมาตรฐานไปใช้ปฏิบัติ ได้รับการออกแบบมาเพื่อช่วยให้ผู้ตรวจสอบภายในเข้าใจว่าจะนำเอาข้อกำหนดต่างๆ ในแนวทางภาคบังคับไป

เกี่ยวกับแนวทางเสริม (Supplemental Guidance)

แนวทางเสริมจะให้ข้อมูลเพิ่มเติม คำแนะนำ และ วิธีปฏิบัติที่เป็นเลิศสำหรับการปฏิบัติงานให้บริการตรวจสอบภายใน เอกสารนี้จะช่วยสนับสนุน*มาตรฐาน* โดยได้ระบุประเด็นต่างๆ ตามหัวข้อ และประเด็นของแต่ละธุรกิจเฉพาะอย่าง โดยให้รายละเอียดมากกว่าแนวทางการนำมาตรฐานไปใช้ปฏิบัติ และ ได้รับการรับรองโดย IIA โดยผ่านการการทบทวนและกระบวนการอนุมัติอย่างเป็นทางการมาแล้ว

แนวปฏิบัติ (Practice Guides)

แนวปฏิบัติ เป็นรูปแบบหนึ่งของแนวทางเสริม ซึ่งจะให้วิถีทางโดยละเอียด กระบวนการแต่ละขั้นตอน พร้อมทั้งตัวอย่างที่จะช่วยสนับสนุนผู้ตรวจสอบภายในทุกคน บางแนวปฏิบัติจะเน้นไปที่:

- การให้บริการทางการเงิน
- ภาครัฐ
- เทคโนโลยีสารสนเทศ (GTAG®)

สำหรับข้อมูลภาพกว้างเกี่ยวกับเอกสารของแนวปฏิบัติที่จัดทำโดย IIA กรุณาไปที่ www.globaliia.org/standards-guidance

สารบัญ

บทสรุปสำหรับผู้บริหาร

ในทั่วโลก กิจกรรมการบริหารความเสี่ยงและความคิดริเริ่มเกี่ยวกับบริหารความเสี่ยงกำลังเป็นสิ่งจำเป็นและอยู่ในความคาดหวังของหน่วยงานกำกับดูแล หน่วยงานที่จัดอันดับ และ ผู้มีส่วนได้ส่วนเสียในภาคอุตสาหกรรมหลักๆ ซึ่งได้แก่ ภาคการให้บริการทางการเงิน ภาครัฐ ภาคการผลิต พลังงาน บริการด้านสุขภาพ และอื่นๆ อย่างไรก็ตาม การบริหารความเสี่ยงได้รับแรงผลักดันมากกว่าแค่จากหน่วยงานกำกับดูแลและแรงผลักจากภายนอกองค์กร การจัดให้มีการบริหารความเสี่ยงที่มีประสิทธิภาพและประสิทธิผล จะก่อให้เกิดประโยชน์กับองค์กรทุกๆ ประเภทและทุกขนาด โดยจะช่วยให้สามารถบรรลุวัตถุประสงค์ทั้งทางด้านการปฏิบัติงานและทางกลยุทธ์ อีกทั้งช่วยเพิ่มมูลค่าและความยั่งยืน และท้ายที่สุดจะช่วยปกป้องผู้มีส่วนได้ส่วนเสียให้มีความปลอดภัยที่ดีขึ้นได้

ผู้ตรวจสอบภายในต้องประเมินประสิทธิผล และมีส่วนช่วยในการปรับปรุงกระบวนการบริหารความเสี่ยง (มาตรฐาน 2120 – การบริหารความเสี่ยง) การเปรียบเทียบสถานะปัจจุบันของการบริหารความเสี่ยงขององค์กรกับแบบจำลองวุฒิภาวะของการบริหารความเสี่ยง จะเป็นจุดเริ่มต้นที่ดีสำหรับการประเมินในประเภทนี้ การวัดโดยการเทียบเคียงอาจช่วยให้หน่วยงานตรวจภายในสื่อสารกับผู้บริหารระดับสูงและคณะกรรมการเกี่ยวกับระดับการเจริญเติบโตของกระบวนการบริหารความเสี่ยงขององค์กรและความต้องการปรับปรุงประบวนการให้ดีขึ้นและมีความเจริญเติบโตล้ำหน้ายิ่งๆ ขึ้น ข้อมูลนี้จะทำให้ผู้ตรวจสอบภายในปรับแก้งานตรวจสอบแต่ละงานได้อย่างเหมาะสม โดยคำนึงถึงวุฒิภาวะของการบริหารความเสี่ยงของส่วนงานหรือของกระบวนการที่จะสอบทาน

แนวปฏิบัตินี้ได้ให้ตัวอย่างของแบบจำลองวุฒิภาวะของการบริหารความเสี่ยงและกระบวนวิธีพื้นฐานที่ผู้ตรวจสอบภายอาจใช้เพื่อให้ความเชื่อมั่นอย่างเป็นอิสระได้ว่า กระบวนการบริหารความเสี่ยงขององค์กรมีประสิทธิผล การนำเอาแนวปฏิบัตินี้ไปปรับใช้จะช่วยให้ผู้ตรวจสอบภายในสามารถปกป้องและเพิ่มคุณค่าขององค์กร และยังช่วยทำให้คณะกรรมการและผู้บริหารระดับสูงสมประสงค์ได้

บทนำ

ความพยายามในการบริหารความเสี่ยงขององค์กร มักถูกเรียกโดยรวมว่า โครงการบริหารความเสี่ยง อย่างไรก็ตาม การใช้คำว่า “โครงการ” มักจะถูกแปลความว่า ถูกจำกัด หรือมีขอบเขต แนวปฏิบัติฉบับนี้มองการบริหารความเสี่ยงว่าเป็นกระบวนการมากกว่า

หมายเหตุ: คำที่แสดงเป็นตัวอักษรหนาจะมีความหมายอธิบายไว้ที่ภาคอภิธานศัพท์ ในภาคผนวก ข.

จะเป็นโครงการ ซึ่งโดยนัยแล้วจะสื่อถึงความพยายามอย่างต่อเนื่องและหน้าที่งานที่ต้องมีการกระทำต่อเนื่องไปเรื่อยๆ

ในหลายๆ ประเทศ คณะกรรมการมีหน้าที่ดูแลว่า องค์กรมีกระบวนการบริหารความเสี่ยงนั้นอยู่แล้ว และสามารถรับมือกับความเสี่ยงที่กำลังเปลี่ยนแปลงไปได้อย่างมีประสิทธิผล ในขณะที่หัวหน้าหน่วยงานตรวจสอบภายในและหน่วยงานตรวจสอบภายในได้ถูกคาดหวังให้ทำการให้ความเชื่อมั่นอย่างเป็นอิสระว่ากระบวนการบริหารความเสี่ยงขององค์กรนั้นมีประสิทธิผล ซึ่งเป็นไปตามมาตรฐาน 2120 – เรื่อง การบริหารความเสี่ยง ที่ได้มีการแจกแจงเกณฑ์หลายๆ อย่างสำหรับใช้ในการประเมินความเสี่ยง

การประเมินกระบวนการบริหารความเสี่ยงขององค์กรมีความท้ายทายที่ยิ่งใหญ่ขึ้นเรื่อยๆ เนื่องจากมักจะมีการแนะนำมาตรฐานการบริหารความเสี่ยง กรอบโครงสร้าง และ รูปแบบโมเดลต่างๆ ทั้งที่มีอยู่และที่เกิดใหม่อยู่เรื่อยๆ การบริหารความเสี่ยงอาจครอบคลุมถึง นโยบาย วิธีปฏิบัติ และวิธีการควบคุมต่างๆ เพื่อให้มั่นใจได้ถึงความพอเพียง เหมาะสมแก่เวลา รวมทั้ง มีการระบุความเสี่ยง การประเมินความเสี่ยง การตอบโต้ความเสี่ยง การเฝ้าระวัง และการรายงานเกี่ยวกับความเสี่ยงขององค์กร อย่างต่อเนื่อง

ในขณะที่แนวปฏิบัติฉบับนี้ไม่สนับสนุนให้องค์กรใช้โปรแกรมการบริหารความเสี่ยง กรอบโครงสร้าง หรือแบบจำลองแบบใดแบบหนึ่งเป็นการเฉพาะ แต่ได้กล่าวถึงคุณลักษณะพื้นฐานทั่วไปของการบริหารความเสี่ยงที่มีวุฒิภาวะพัฒนาเต็มที่แล้วดังต่อไปนี้:

- วัฒนธรรมความเสี่ยง: การบูรณาการความเสี่ยงเข้ากับกระบวนการตัดสินใจ การกำหนดค่าตอบแทน โครงสร้างการให้รางวัล และ การตั้งเป้าหมาย
- การกำกับดูแลความเสี่ยง: การมีส่วนร่วมในกระบวนการบริหารความเสี่ยงตลอดทั่วทั้งองค์กร โดยบุคลากรที่มีความรู้ ทักษะ และ ความสามารถในการบริหารความเสี่ยง
- กระบวนการบริหารความเสี่ยง: การระบุความเสี่ยงที่ได้รวบรวมมา การประเมินเพื่อจัดลำดับความเร่งด่วน การจัดการ การเฝ้าระวัง และการรายงานความเสี่ยงตลอดทั่วทั้งองค์กร

นอกจากนี้แล้ว ระดับวุฒิภาวะ แนวทาง กลยุทธ์ และ การให้ความสำคัญกับหน้าที่งานที่เกี่ยวข้องกับการบริหารความเสี่ยงมักจะขึ้นอยู่กับขนาดและความซับซ้อนขององค์กรและอุตสาหกรรม และพื้นที่ที่องค์กรนั้นดำเนินงานอยู่ แนวปฏิบัตินี้จะให้ข้อมูลความเป็นมา กระบวนวิธี และเครื่องมือต่างๆ เพื่อช่วยให้ผู้ตรวจสอบ

ภายในสามารถให้ความเชื่อมั่นได้ว่า กระบวนการบริหารความเสี่ยงขององค์กรมีประสิทธิผล และเพื่อมีส่วนสนับสนุนให้เกิดการปรับปรุงกระบวนการเหล่านั้นให้ดีขึ้นได้

แนวปฏิบัตินี้จะช่วยให้ผู้ตรวจสอบภายใน:

- นำเอาหลักการในประมวลจรรยาบรรณ (Code of Ethics principles) และ*มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพตรวจสอบภายใน* (*International Standards for the Professional Practice of Internal Auditing*) ของสมาคมผู้ตรวจสอบภายใน (IIA) ไปประยุกต์ใช้เพื่อเพิ่มพูนและปกป้องคุณค่าขององค์กร โดยการให้ความเชื่อมั่น ให้คำปรึกษา และให้มุมมองที่ลึกซึ้ง อย่างเที่ยงธรรม โดยอาศัยความเสี่ยงเป็นพื้นฐาน
- ทำความเข้าใจถึงความจำเป็นที่จะต้องประเมินกิจกรรมบริหารความเสี่ยงต่างๆ
- ทำความเข้าใจถึงองค์ประกอบหลัก ของกระบวนการบริหารความเสี่ยงที่มีประสิทธิผล
- พัฒนาแนวทางการประเมินความเสี่ยงโดยคำนึงถึงสภาพแวดล้อมในทางธุรกิจและกฎระเบียบข้อบังคับของทางการ และระดับวุฒิภาวะขององค์กร
- เก็บรวมรวมข้อมูลที่จำเป็นเพื่อที่จะกำหนดขอบเขตของงานที่ได้รับมอบหมายในการประเมินกิจกรรมการบริหารความเสี่ยงต่างๆ
- ประเมินความมีประสิทธิผลของกระบวนการบริหารความเสี่ยง
- มีส่วนช่วยปรับปรุงกระบวนการบริหารความเสี่ยง

นัยสำคัญทางธุรกิจ: ความเสี่ยงและโอกาส

การบริหารความเสี่ยงเป็นแขนงวิชาหนึ่งที่มีบทบาทสำคัญยิ่งภายในองค์กรต่างๆ มานานแล้ว มันได้มีการผันแปรเปลี่ยนไปเป็นหลายรูปแบบและมีหลายชื่อ โดยมีตั้งแต่ "การบริหารความเสี่ยงโครงการ" ไปจนถึง "การบริหารความเสี่ยงทั่วทั้งองค์กร" หรือ ERM การบริหารความเสี่ยงได้รับความสนใจมาอย่างต่อเนื่อง เมื่อโลกมีการเชื่อมต่อกันและมีการเปลี่ยนแปลงทางเทคโนโลยีที่กระจายไปยังทุกธุรกิจ อย่างไรก็ตาม การรับเอาการบริหารความเสี่ยงที่ได้จัดทำไว้เป็นเอกสาร มาเป็นภารกิจระดับทั่วทั้งองค์กรก็ยังไม่ได้เป็นบรรทัดฐานเดียวกันทั้งหมด

มาตรฐาน 2120 – การบริหารความเสี่ยง

หน่วยงานตรวจสอบภายในต้องประเมินความมีประสิทธิผลและมีส่วนช่วยในการปรับปรุงกระบวนการบริหารความเสี่ยง

บทตีความ:

การที่จะตัดสินว่ากระบวนการบริหารความเสี่ยงมีประสิทธิผลหรือไม่นั้นเป็นดุลพินิจที่เป็นผลมาจากการประเมินของผู้ตรวจสอบภายในว่า:

ความล้มเหลวของการกำกับดูแล ระบบ และกระบวนการบริหารความเสี่ยง อาจจะทำให้เกิดภาระหนี้สิ้น ค่าปรับ การคว่ำบาตรทางธุรกิจ และความเสี่ยงอื่นๆ อีกได้ การสอบทานและประเมินการบริหารความเสี่ยงอย่างต่อเนื่องจะช่วยให้องค์กรสามารถหลีกเลี่ยงความสูญเสียสินทรัพย์ ทรัพย์สินทางปัญญา ส่วนแบ่งทางการตลาด โอกาสหารายได้ ความภักดีของลูกค้า ชื่อเสียงของตราสินค้า และ อื่นๆ สืบเนื่องมาจากการเกิดขึ้นของเหตุการณ์ความเสี่ยงที่น่าจะได้รับการปกป้อง หลีกเลี่ยงได้ หรือบรรเทาลงได้ (โดยการหาผู้ร่วมรับความเสี่ยงหรือโอนความเสี่ยง) ภาคผนวก ค. อธิบายถึงสถานการณ์ความเสี่ยงต่างๆ ที่เกี่ยวข้องกับกระบวนการบริหารความเสี่ยง

องค์กรที่มีการกำกับดูแลที่ดีและประสบความสำเร็จจะใช้กระบวนการบริหารความเสี่ยงเพื่อที่จะประสานทิศทางและควบคุมความเสียหายจากความเสี่ยง ไปในลักษณะที่จะช่วยส่งเสริมให้องค์กรสามารถบรรลุวัตถุประสงค์ได้ การวัดประโยชน์ที่ได้จากการที่มีกระบวนการบริหารความเสี่ยงซึ่งเติบโตเต็มที่แล้ว อาจเป็นความท้าทาย เนื่องจากมีความยากในการหาข้อมูลที่เชื่อถือได้ หากว่าข้อมูลเหล่านั้นมีอยู่แล้ว มันอาจเป็นการยากสำหรับองค์กรที่จะวิเคราะห์ ถึงวุฒิภาวะของกระบวนการบริหารความเสี่ยงขององค์กรตนเองได้อย่างเที่ยงธรรม

อย่างไรก็ตาม กระบวนการบริหารความเสี่ยงที่เติบโตเต็มที่แล้ว มักจะแสดงให้เห็นได้ถึงประโยชน์ต่างๆ เช่น

- ส่งเสริมการตัดสินใจ และ การกำหนดกลยุทธ์ โดยอาศัยความเสี่ยงเป็นพื้นฐาน
- มีการสื่อสารและการขอคำปรึกษาเพิ่มขึ้นทั่วทั้งองค์กร
- ทำให้เกิดความเชื่อมโยงและมองภาพของความเสี่ยง โอกาส และกลยุทธ์ ได้อย่างลึกซึ้ง โดยผ่านทางภาษาของความเสี่ยงที่

- *วัตถุประสงค์ขององค์กรสนับสนุนและเป็นไปในทิศทางเดียวกับพันธกิจขององค์กร*
- *มีการระบุและประเมินความเสี่ยงที่มีนัยสำคัญ*
- *มีการเลือกใช้วิธีการตอบสนองต่อความเสี่ยงที่เหมาะสม โดยเป็นไปในทิศทางเดียวกับระดับความเสี่ยงที่องค์กรยอมรับได้*
- *ข้อมูลความเสี่ยงที่เกี่ยวข้องได้ถูกระบุและสื่อสารภายในองค์กรในเวลาที่เหมาะสม ซึ่งจะช่วยให้พนักงาน ผู้บริหารและคณะกรรมการปฏิบัติภาระหน้าที่ได้*

หน่วยงานตรวจสอบภายในอาจรวบรวมข้อมูล เพื่อสนับสนุนการประเมินระหว่างการปฏิบัติงานที่ได้รับมอบหมายหลายๆ งาน เมื่อนำผลการปฏิบัติงานต่างๆ มารวมพิจารณาเข้าด้วยกันจะทำให้เกิดความเข้าใจในกระบวนการบริหารความเสี่ยงขององค์กรและประสิทธิผลของกระบวนการเหล่านั้น

มีการติดตามกระบวนการบริหารความเสี่ยงผ่านทางกิจกรรมทางการบริหารที่มีอยู่อย่างต่อเนื่อง หรือโดยการประเมินแยกต่างหาก หรือทั้ง 2 แบบร่วมกัน

เข้าใจตรงกัน (common risk language)

- ส่งเสริมให้เกิดการรายงานกิจกรรมบริหารความเสี่ยงที่เป็นเอกสารและในเวลาที่เหมาะสม เพื่อที่ผู้บริหารระดับสูงและคณะกรรมการจะได้ทราบทิศทางของผู้บริหารได้เป็นอย่างดี
- เพิ่มความน่าจะเป็นที่องค์กรจะบรรลุวัตถุประสงค์เชิงกลยุทธ์ที่ตั้งไว้ได้สร้างและปกป้องคุณค่าสำหรับผู้มีส่วนได้ส่วนเสีย

ในการนำเสนอการปรับปรุงกระบวนการบริหารความความเสี่ยง ผู้ตรวจสอบภายในอาจต้องเผชิญกับการคัดค้านไม่เห็นด้วยต่างๆ เช่น

- การประเมินความเสี่ยงทำให้เสียเวลามาก
- ข้อมูลความเสี่ยงที่รวบรวมมาได้นั้นไม่มีความเกี่ยวข้อง
- ข้อมูลความเสี่ยงไม่ได้ถูกนำมาใช้ในการตัดสินใจ

เมื่อหน่วยงานตรวจสอบภายในออกแบบการประเมินกระบวนการบริหารความเสี่ยงขององค์กร การทำความเข้าใจระดับวุฒิภาวะของการบริหารความเสี่ยงและวัฒนธรรมความเสี่ยงขององค์กรเป็นสิ่งสำคัญในอันที่จะสร้างชุดคำถามที่เหมาะสมได้ หากองค์กรยังไม่ได้พัฒนามุมมองหรือปรัชญาการบริหารความเสี่ยงของตัวเองอย่างเต็มที่แล้ว หน่วยงานตรวจสอบภายในควรทำความเข้าใจเหตุผลที่เป็นเช่นนั้นก่อนการจัดทำข้อสังเกตและข้อเสนอแนะ ความคิดเห็นเกี่ยวกับกระบวนการบริหารความเสี่ยงจะให้ข้อมูลที่ถูกต้องหรือไม่ก็เป็นสิ่งสำคัญ หากผู้บริหารเชื่อว่ากระบวนการบริหารความเสี่ยงเป็นเรื่องของกิจกรรมที่ทำตามพิธีรีตองซึ่งไม่มีประโยชน์ที่จะต้องเสียทรัพยากรเพื่อไปลงมือทำ ดังนั้น การให้ข้อเสนอแนะที่เป็นการปรับปรุงขนานใหญ่ก็อาจจะเร็วเกินไปและทำให้เกิดข้อกังขาหรือถูกปฏิเสธโดยสิ้นเชิง แทนที่จะทำเช่นนั้น ผู้ตรวจสอบภายในอาจประสบความสำเร็จมากกว่าด้วยการให้ข้อเสนอแนะในสิ่งที่เกี่ยวกับวัฒนธรรมความเสี่ยงขององค์กร

ระดับวุฒิภาวะของการบริหารความเสี่ยง

กรอบโครงสร้างการบริหารความเสี่ยงในปัจจุบันมีอยู่มากมาย แต่ละกรอบต่างก็นำเสนอหลักการที่องค์กรควรต้องพิจารณาเมื่อจะพัฒนากระบวนการบริหารความเสี่ยงอย่างครอบคลุม กรอบโครงสร้างบางกรอบมุ่งเน้นไปที่วิธีการควบคุมภายในและความสัมพันธ์ของวิธีการควบคุมภายในเหล่านั้นต่อความเสี่ยงต่างๆ ขององค์กร แต่บางกรอบก็เน้นไปที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ความเสี่ยงทางกลยุทธ์ และ ความเสี่ยงที่สามารถทำประกันได้ องค์กรหนึ่งอาจตระหนักว่าไม่มีกรอบโครงสร้างการบริหารความเสี่ยงใดเพียงกรอบเดียว ที่จะ

สามารถจัดการกับความเสี่ยงรอบด้านที่องค์กรจะต้องคำนึงถึงได้ แทนที่จะรับเอากรอบโครงสร้างเดียวมาใช้ องค์กรอาจได้ประโยชน์จากการรวมเอาองค์ประกอบต่างๆ ของกรอบโครงสร้างหลายๆ กรอบ เพื่อนำมาสร้างเป็นแบบเฉพาะตามคุณลักษณะและความจำเป็นของตน ไม่ว่าจะใช้กรอบโครงสร้างใดมาเป็นพื้นฐานของกระบวนการบริหารความเสี่ยง องค์ประกอบเฉพาะบางอย่างอาจช่วยให้องค์กรสามารถวัดระดับวุฒิภาวะได้

รูปที่ 1 แสดงตัวอย่างของ**แบบจำลองวุฒิภาวะของการบริหารความเสี่ยง** (risk management maturity model) ซึ่งแสดงห้าขั้นตอนของการพัฒนาที่อาจแสดงถึงคุณลักษณะของกระบวนการบริหารความเสี่ยงองค์ประกอบหลายๆ อย่างที่อยู่ในในองค์กรเดียวกัน อาจอยู่ในระดับวุฒิภาวะที่แตกต่างกันในเวลาหนึ่งๆ ยกตัวอย่างเช่น ระดับวุฒิภาวะของวัฒนธรรมขององค์กร อาจแตกต่างจากระดับวุฒิภาวะของการกำกับดูแลและกระบวนการ ในการวางแผนการตรวจสอบงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายอาจใช้แบบจำลองวุฒิภาวะ เพื่อปรับงานที่ได้รับมอบหมายนั้นให้เหมาะสมกับระดับวุฒิภาวะขององค์ประกอบที่กำลังสอบทานได้

รูปที่ 1 ตัวอย่างแบบจำลองวุฒิภาวะการบริหารความเสี่ยง

ระยะ	วัฒนธรรม	การกำกับดูแล	กระบวนการ
1 - เริ่มต้น	ความเสี่ยงเป็นเรื่องของหน่วยงานตรวจสอบภายใน	หัวหน้าหน่วยงานตรวจสอบภายในหรือประธานคณะกรรมการตรวจสอบ	การตรวจสอบโดยอาศัยความเสี่ยงเป็นพื้นฐาน
2 - ทำซ้ำ	ความเสี่ยงถูกถือเป็นเรื่องที่ต้องดำเนินการตามความจำเป็น	ผู้จัดการหน่วยธุรกิจ	กระบวนการประเมินความเสี่ยงตามที่จำเป็นและการประเมินการควบคุมโดยตนเอง (Control self-assessment)
ระยะ	วัฒนธรรม	การกำกับดูแล	กระบวนการ

3 - มีการกำหนด	มีการแบ่งปันข้อมูลความเสี่ยงระหว่างหน่วยงานตรวจสอบภายในและหน่วยงานที่มีหน้าที่ทางการควบคุม	ผู้บริหารระดับสูง/ คณะกรรมการ	ภาษาความเสี่ยง (Common risk language) และกระบวนการประเมินความเสี่ยงถูกใช้โดยหน่วยงานตรวจสอบภายในและหน่วยงานที่มีหน้าที่ทางการควบคุม
4 - มีการจัดการ	ความเสี่ยงถูกผนวกรวมเข้ากับการวางแผนกลยุทธ์ มีการระบุและสื่อสารระดับความเสี่ยงที่องค์กรยอมรับได้	ผู้บริหารทุกระดับและคณะกรรมการ	มีการใช้ภาษาความเสี่ยงและมีกระบวนการประเมินความเสี่ยงอย่างสม่ำเสมอทั่วทั้งองค์กร
5 - ระดับที่มีประสิทธิภาพสูงสุด	มีการผนวกรวมความเสี่ยงเข้ากับการตัดสินใจทั้งหมด การกำหนดค่าตอบแทน และ เป้าหมายขององค์กร	ทุกคนมีส่วนเกี่ยวข้อง	มีการใช้ภาษาความเสี่ยงและการรายงานความเสี่ยงแบบองค์รวมอยู่ทั่วทั้งองค์กร

เพื่อให้มั่นใจถึงตำแหน่งขององค์กรในแบบจำลองวุฒิภาวะการบริหารความเสี่ยง และเพื่อประเมินว่ากระบวนการบริหารความเสี่ยงทำหน้าที่ในองค์กรอย่างมีประสิทธิผลเพียงใดนั้น ผู้ตรวจสอบภายในควรพิจารณาองค์ประกอบหลายๆ ประการ

ทุกองค์กรมีการปฏิบัติเกี่ยวกับการบริหารความเสี่ยงในรูปแบบไม่อย่างใดก็อย่างหนึ่ง แม้ว่าพวกเขาอาจจะไม่ได้รับรู้ถึงการกระทำนั้น และอาจไม่ได้มีการจัดทำเอกสารบันทึกการทำงานของพวกเขาไว้อย่างเป็นทางการก็ตาม รูปแบบที่ง่ายที่สุดของการบันทึกการบริหารความเสี่ยงคือ การฝึกสร้างทะเบียนรายการความเสี่ยงขององค์กรโดยผู้บริหารระดับสูงปีละครั้ง

ข้อพิจารณาในทางการตรวจสอบ

องค์กรควรจะมีความพร้อมในระดับใด? หากพิจารณาระดับ 1 ถึง 5 โดยที่ 5 คือ ระดับวุฒิภาวะที่สูงสุด ไม่จำเป็นที่ทุกองค์กรต้องไปถึงระดับวุฒิภาวะที่สูงสุด การบรรลุระดับที่ 2 หรือ 3 อย่างมั่นคงอาจเป็นสิ่งที่ยอมรับได้ แต่ละองค์กรควรกำหนดระดับของวุฒิภาวะที่เหมาะสมกับสภาพแวดล้อมของตนเอง:

การกระทำเช่นนี้อาจเรียกได้ว่าเป็น “การประเมินความเสี่ยงเชิงกลยุทธ์” ซึ่งผู้บริหารระดับสูงจะพัฒนาและบันทึกรายการความเสี่ยง และจะไม่ทำการประเมินอีกจนกระทั่งปีต่อมา แต่ในทางตรงกันข้าม องค์กรที่มีกระบวนการบริหารความเสี่ยงที่เข้มแข็ง หรือ มีความเจริญเติบโตเต็มที่แล้ว กระบวนการบริหารความเสี่ยงจะพิจารณาปัจจัยความเสี่ยงต่างๆ ซึ่งรวมถึงลักษณะที่เกี่ยวกับวัฒนธรรม หรือการกำกับดูแลทั่วทั้งองค์กร ในรูปแบบที่เป็นระบบและมีโครงสร้าง

ระดับความเสี่ยงที่ยอมรับได้

กรอบโครงสร้างการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากลของสมาคมผู้ตรวจสอบภายใน ได้กำหนดความหมายของ ระดับความเสี่ยงที่องค์กรยอมรับได้ว่าเป็นระดับความเสี่ยงที่องค์กรเต็มใจจะยอมรับ สำหรับหลายๆ องค์กรระดับความเสี่ยงที่องค์กรยอมรับได้นั้น ยากที่จะพูดถึงได้อย่างชัดเจนในทางปฏิบัติเวลาที่มีการหารือกัน รูปแบบทั่วไปของระดับความเสี่ยงที่องค์กรยอมรับได้คือ ข้อความที่ว่า “ระดับของความสูญเสียที่ยอมรับได้” ซึ่งอาจได้รับอนุมัติจากผู้บริหารระดับสูงและ/หรือคณะกรรมการ โดยมีข้อแม้ว่าขอบเขตของความเสียหายอาจจะมากเกินกว่านั้นได้ แต่ต้องมีการอนุมัติโดยผู้มีอำนาจตามระดับที่เหมาะสม

การตีกรอบระดับความเสี่ยงที่ยอมรับได้ ว่าเป็น “ความเสียหายที่ยอมรับได้” นั้น อาจถูกตีความว่าเป็นแผนขององค์กรที่จะบรรลุถึงระดับของความเสียหายตามที่กำหนดไว้ (เป็นตัวเงิน) ที่จะเกิดจากความเสี่ยง ซึ่งอาจทำให้ผู้จัดการยอมรับระดับของความเสี่ยงที่สูงกว่าความจำเป็นหรือสูงกว่าที่ต้องการ ยิ่งไปกว่านั้น การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ในแง่ของกลยุทธ์อย่างกว้างๆ อาจนำไปสู่การตีความที่แตกต่างกันว่าระดับความเบี่ยงเบนที่เบี่ยงเบนออกไปจากระดับความเสี่ยงที่ยอมรับได้ (tolerances) นั้นทำงานอย่างไร เนื่องจากข้อความที่ระบุถึง 'ความเสี่ยงที่ยอมรับได้' ได้ถูกนำไปปรับใช้ในระดับล่างขององค์กร

ผู้ตรวจสอบภายในควรส่งเสริมให้องค์กรรับเอากระบวนวิธี และ รูปแบบของระดับความเสี่ยงที่ยอมรับได้ ที่ช่วยให้ผู้บริหารและคณะกรรมการสามารถเรียงลำดับความสำคัญของกลยุทธ์และการจัดสรรทรัพยากร ไปใช้ ระดับความเสี่ยงที่องค์กรยอมรับได้สามารถถูกปรับเปลี่ยนได้ง่ายและมักจะเป็นตัวถ่วงดุลในระหว่างกลยุทธ์ต่างๆ การกำหนดระดับของความเสียหายที่เปลี่ยนแปลงไม่ได้โดยผู้บริหารระดับสูงขององค์กรอาจส่งผลให้ระดับความเสี่ยงที่องค์กรยอมรับได้ถูกมองข้ามไปจากการเป็นเครื่องมือในการตัดสินใจโดยมีข้อมูลรองรับอย่างสม่ำเสมอทั่วทั้งองค์กร

โครงสร้าง: บทบาทและหน้าที่ความรับผิดชอบ

บทบาทและภาระหน้าที่สำหรับการบริหารความเสี่ยงจะถูกกระจายแตกต่างกันไปในองค์กรขึ้นอยู่กับระดับวุฒิภาวะของกระบวนการบริหารความเสี่ยงขององค์กร และทรัพยากรที่หน่วยงานตรวจสอบภายในเข้าถึงได้

ระดับวุฒิภาวะของการบริหารความเสี่ยงขององค์กรอาจแปรผันตามห้วงเวลา ซึ่งอาจอธิบายได้เป็นระยะต่างๆ ยกตัวอย่างเช่น:

1 – ระยะเริ่มต้น (Initial) ในองค์กรที่กระบวนการบริหารความเสี่ยงอยู่ในช่วงเริ่มต้นของการพัฒนา หน่วยงานตรวจสอบภายในอาจเข้าไปมีส่วนร่วมเชิงรุกมากกว่าเมื่อเทียบกับตอนที่กระบวนการมีการเจริญเติบโตมากขึ้น ที่วุฒิภาวะระยะนี้ กิจกรรมบริหารความเสี่ยงที่เฉพาะบางกิจกรรมอาจไม่ได้ดำเนินการโดยผู้บริหารของสายปฏิบัติการ หรือ หน้าที่งานที่มีบทบาทในการควบคุม การกำกับดูแล กฎหมาย การบริหารความเสี่ยง หรือ การให้ความเชื่อมั่นในคุณภาพเป็นการภายใน หน้าที่งานเหล่านั้นอาจต้องพึ่งพาการประเมินความเสี่ยงและบริการให้ความเชื่อมั่นและคำแนะนำโดยอาศัยความเสี่ยงเป็นพื้นฐานของหน่วยงานตรวจสอบภายใน

2 – มีการทำซ้ำ (Repeatable) ที่ระยะนี้ หน่วยงานตรวจสอบภายในมีการจัดการที่ดีและมีทรัพยากรพอ และมีบทบาทเป็นเครื่องมือโดยทำการประเมินโดยอาศัยความเสี่ยงเป็นพื้นฐาน แต่อาจทำในขอบเขตที่กว้างขึ้น หน่วยงานตรวจสอบภายในอาจทำงานร่วมกันกับหน่วยงานที่ทำหน้าที่ควบคุม กำกับดูแล หน่วยงานกฎหมาย การบริหารความเสี่ยง และ การให้ความเชื่อมั่นในคุณภาพเป็นการภายใน โดยเพิ่มความเชี่ยวชาญด้านการตรวจสอบภายในไปช่วยเหลือหน่วยงานที่เป็นเจ้าของความเสี่ยงซึ่งอยู่ภายใต้ผู้บริหารสายงานปฏิบัติการเพื่อที่จะสร้างและติดตามวิธีการควบคุมในทางการปฏิบัติงาน วุฒิภาวะในระยะนี้เพียงพอสำหรับหลายๆ องค์กร หากว่ากระบวนการมีการปฏิบัติที่สม่ำเสมอ มีประสิทธิภาพ และสามารถทำให้เกิดผลที่ใช้การได้ ซึ่งจะช่วยในการบรรลุเป้าหมายและวัตถุประสงค์ขององค์กรได้

3 - มีการกำหนด (Defined) องค์กรที่อยู่ในระดับกลางของโมเดล อาจเป็นการผสมผสานของบางหน่วยธุรกิจที่มีระดับวุฒิภาวะที่สูงกว่าบางหน่วยธุรกิจ ในโครงสร้างนี้ หน้าที่งานการควบคุม การกำกับดูแล หน่วยงานกฎหมาย การบริหารความเสี่ยง และการให้ความเชื่อมั่นในคุณภาพเป็นการภายใน อาจเป็นเจ้าของกระบวนการบริหารความเสี่ยงและมีหน้าที่อยู่ในระดับวุฒิภาวะที่สูงขึ้นคือ ระดับที่มีการจัดการและระดับที่มีประสิทธิภาพสูงสุดอย่างสม่ำเสมอ หน่วยงานที่ทำหน้าที่ควบคุมและให้ความเชื่อมั่นอาจมีบทบาทในการช่วย

ผู้บริหารสายงานปฏิบัติการประเมินความเสี่ยงและกระทำกิจกรรมเกี่ยวกับความเสี่ยงอื่นๆ หน่วยงานตรวจสอบภายในอาจปฏิบัติงานในหน้าที่เหมือนกับในระดับที่ 2 คือระดับที่มีการทำซ้ำ

4 – มีการจัดการ *(Managed)* แบบจำลองวุฒิภาวะที่ไต่ระดับขึ้น ในองค์กรที่มีวุฒิภาวะที่เติบโตขึ้นอย่างมีนัยสำคัญ ผู้บริหารสายงานปฏิบัติการจะเป็นเจ้าของและบริหารความเสี่ยงทั่วทั้งองค์กร และมีหน้าที่ในการดำเนินการแก้ไขเพื่อที่จะจัดการกระบวนการและกิจกรรมการควบคุม หน่วยงานตรวจสอบภายในจะทำหน้าที่หลักในฐานะที่เป็นหน่วยงานให้ความเชื่อมั่นอย่างอิสระ ประเมินความมีประสิทธิผลของกระบวนการบริหารความเสี่ยงของฝ่ายบริหารและหน้าที่งานการให้ความเชื่อมั่นอื่นๆ

5 –มีประสิทธิภาพสูงสุด *(Optimized)* ในองค์กรที่สามารถบรรลุถึงขั้นมีการบริหารความเสี่ยงแบบองค์รวม มีความซับซ้อน และมีวุฒิภาวะ ผู้บริหารสายงานปฏิบัติการจะเป็นเจ้าของกระบวนการบริหารความเสี่ยง หน่วยงานที่มีหน้าที่ในการกำกับดูแลและ/หรือบริหารความเสี่ยงขององค์กรจะทำการประเมินความเสี่ยงเพื่อใช้ในงานของตนเอง พวกเขาอาจเฝ้าติดตามการประเมินความเสี่ยง และการรายงานที่จัดทำโดย ผู้บริหารสายงานปฏิบัติการ และอาจทดสอบข้อมูลความเสี่ยงตามความจำเป็น ความเสี่ยงจะถูกเฝ้าระวังและจัดการในหลายๆ กระบวนการทางธุรกิจ

หน่วยงานตรวจสอบภายใน ในฐานะที่เป็นหน่วยงานซึ่งทำหน้าที่ให้ความเชื่อมั่นอย่างเป็นอิสระ จะทำงานที่ได้รับมอบหมายเพื่อประเมินว่ากระบวนการบริหารความเสี่ยงมีประสิทธิผลในแต่ละส่วน และโดยรวมทั่วทั้งองค์กร นอกจากนั้น หน่วยงานตรวจสอบภายในอาจเปรียบเทียบการประเมินความเสี่ยงที่ตนได้จัดทำขึ้น กับ ข้อมูลความเสี่ยงที่ทำโดยผู้บริหารซึ่งได้รับการสอบทานจากหน่วยงานที่ทำหน้าที่ให้ความเชื่อมั่นเป็นการภายใน (หน่วยงานกำกับดูแล/บริหารความเสี่ยง) เพื่อวัดความแม่นยำถูกต้อง และครบถ้วนสมบูรณ์ของการประเมินโดยผู้บริหาร ในทางกลับกัน หน่วยงานตรวจสอบภายในอาจใช้ข้อมูลความเสี่ยงของผู้บริหาร เพื่อใช้แจ้งผลการประเมินความเสี่ยงของการตรวจสอบภายใน หรือ อาจใช้ทั้งสองอย่างตามความเหมาะสม หัวหน้าหน่วยงานตรวจสอบภายในควรประสานงานกับหน่วยงานอื่นที่ทำ

แหล่งที่มา
สำหรับข้อมูลเพิ่มเติมเพื่อการตัดสินบทบาทและความรับผิดชอบสำหรับการบริหารความเสี่ยง อ่านได้ที่ แนวปฏิบัติของ IIA เรื่อง “การประสานงานและการพึ่งพาผลงานของผู้อื่น: การจัดทำแผนที่การให้ความเชื่อมั่น (Coordination and Reliance: Developing an Assurance Map)"

หน้าที่ให้ความเชื่อมั่นหรือให้คำปรึกษา และ อาจพิจารณาที่จะพึ่งพาข้อมูลของเขาเหล่านั้น (มาตรฐาน 2050 – การประสานงานและการพึ่งพาผลงานของผู้อื่น)

วัฒนธรรม

ความมีประสิทธิผล และความครอบคลุมของกระบวนการบริหารความเสี่ยงขึ้นอยู่กับวัฒนธรรมความเสี่ยงขององค์กร ถ้าหากวัฒนธรรมไม่เอื้อที่จะให้มีการหารืออย่างเปิดเผย และพิจารณาความเสี่ยงทั้งในมุมที่เป็นด้านลบและด้านบวกแล้วกระบวนการบริหารความเสี่ยงก็จะล้มเหลว ผู้ตรวจสอบภายในควรตั้งคำถามว่า “ถ้าไม่มีนโยบาย ผู้บริหารจะทำงานอย่างไร” องค์กรอาจมีนโยบายและวิธีปฏิบัติที่ระบุว่า จะต้องพิจารณาถึงการบริหารความเสี่ยง แต่วัฒนธรรมอาจเป็นตัวที่บดบังเจตนารมณ์และขัดขวางการพูดคุยหารือหรือการกระทำที่จริงจังได้

หลายองค์กรอาจมีกระบวนการที่ซับซ้อนที่จะวัดและประเมินความเสี่ยง แต่วัฒนธรรมกลับไม่เอื้อต่อการบริหารความเสี่ยง ในอุตสาหกรรมที่มีกฎระเบียบกำกับ การมีกระบวนการบริหารความเสี่ยงในระดับปฏิบัติการอาจเป็นสิ่งที่จำเป็น แต่หากผู้บริหารมุ่งเน้นไปเพียงที่การทำเครื่องหมายรายการหัวข้อสิ่งที่ต้องทำ (Checklist) กระบวนการบริหารความเสี่ยงก็มีแนวโน้มว่าจะไม่สามารถไปถึงระดับวุฒิภาวะที่ข้อมูลความเสี่ยงจะถูกนำมาผนวกรวมกับการตัดสินใจ (และจะเชื่อมโยงไปที่ค่าตอบแทนและสิ่งจูงใจ) และการรวบรวม และรายงานได้ทั่วทั้งองค์กร

หากผู้ตรวจสอบภายในได้มีส่วนเกี่ยวข้องในการออกแบบกระบวนการบริหารความเสี่ยง และเห็นว่าวัฒนธรรมองค์กรไม่ส่งเสริมความพยายามดังกล่าว ผู้ตรวจสอบภายในควรนำประเด็นนี้แจ้งต่อหัวหน้าหน่วยงานตรวจสอบภายใน ผู้ซึ่งจะสามารถนำเรื่องเข้าหารือเกี่ยวกับการมีอยู่ของกระบวนการนั้นกับผู้บริหารระดับสูงและคณะกรรมการได้ ถึงแม้ว่าผู้บริหารระดับสูงมีทีท่าที่สนับสนุนการบริหารความเสี่ยงอยู่แล้ว การกดดันผู้บริหารในองค์กรที่ต่อต้านให้มาเข้าร่วมโครงการการบริหารความเสี่ยงก็แทบจะไม่คุ้มค่า ผู้บริหารต้องเข้าใจคุณค่าของการบริหารความเสี่ยงก่อนจึงจะหันมาสนับสนุนกระบวนการได้

การกำกับดูแล

เพื่อให้กระบวนการบริหารความเสี่ยงประสบผลสำเร็จ จำเป็นต้องได้รับการสนับสนุนจากผู้บริหารระดับสูงตั้งแต่เริ่มต้น เพื่อให้ได้รับการยอมรับและการจัดสรรทรัพยากรอย่างเหมาะสม จะต้องมีการใช้ข้อมูลความเสี่ยงในการตัดสินใจของผู้บริหารระดับสูงสุดขององค์กร ความสนใจของผู้ที่อยู่ในระดับสูงขององค์กรดังเช่น

คณะกรรมการตรวจสอบ เป็นสิ่งสำคัญที่จะก่อให้เกิดความต้องการในการรวบรวม ประเมิน และ จัดหาข้อมูลความเสี่ยง ถ้าคณะกรรมการตรวจสอบมีการร้องขอข้อมูลความเสี่ยงอยู่เป็นประจำในบทบาทการทำหน้าที่กำกับดูแลแล้ว ผู้บริหารก็จะต้องหาทางในการจัดหาข้อมูลเหล่านั้นจนได้

โดยทั่วไปแล้ว กระบวนการบริหารความเสี่ยงจะถูกพัฒนาจากบนลงล่าง โดยเริ่มจากผู้บริหารระดับสูง โดยที่คณะกรรมการจะถามหาการประเมินและรายงานความเสี่ยงก่อน โดยผู้บริหารในองค์กรธุรกิจชั้นนำมักจะรับเอาวิธีปฏิบัติแบบเดียวกันในภายหลังเมื่อพวกเค้าต้องจัดหาข้อมูลความเสี่ยงเพื่อให้ผู้บริหารระดับสูงใช้ เมื่อผู้จัดการธุรกิจคนสำคัญ ผู้บริหารระดับสูง และ คณะกรรมการ เข้ามาเกี่ยวข้องกับกระบวนการบริหารความเสี่ยงแล้ว โครงสร้างก็จะมีความชัดเจน และสามารถนำเอานโยบาย วิธีปฏิบัติ การรายงาน และ ระเบียบการในการยกระดับการรายงาน ไปใช้ปฏิบัติได้จริง

กระบวนการ

ระดับที่กิจกรรมการบริหารความเสี่ยงได้บูรณาการเข้ากับกระบวนการทางธุรกิจอื่นๆ ใช้เป็นมาตรวัดระดับวุฒิภาวะขององค์กรที่ดีได้ หากการประเมินความเสี่ยงเป็นเรื่องธรรมดาทั่วทั้งองค์กร ระดับการยอมรับความเสี่ยงได้มีการสื่อสารอย่างมีประสิทธิผลไปยังทุกระดับ และข้อมูลความเสี่ยงถูกใช้ในการตัดสินใจที่สำคัญ ย่อมถือได้ว่าองค์กรนั้นมีระดับวุฒิภาวะสูงกว่าองค์กรที่ทำการประเมินความเสี่ยงปีละหน หรือเท่าที่ถูกบังคับตามกฎระเบียบเท่านั้น **รูปที่** 2 แสดงให้เห็นถึงความแตกต่าง ซึ่งเป็นเพียงแค่ตัวอย่างเท่านั้น แต่ไม่ใช่ทั้งหมด

รูปที่ 2 : ตัวอย่างคำอธิบายระดับต่างๆ ของแบบจำลองวุฒิภาวะ

1 - เริ่มต้น (Initial)	
ระดับความเสี่ยงที่ยอมรับได้	ระดับการยอมรับความเสี่ยงขององค์กรนั้นรู้กันเป็นนัยๆ แต่ไม่มีการระบุหรือจัดทำเอกสารอย่างชัดเจน ผู้บริหารระดับสูงอาจจะมีความคิดใกล้เคียงกันเกี่ยวกับระดับความเสี่ยงที่องค์กรเต็มใจที่จะยอมรับ
การประเมินความเสี่ยง	ผู้ตรวจสอบภายในอาจทำการประเมินความเสี่ยง เพื่อรวบรวมข้อมูลสำหรับการปฏิบัติงานที่ได้รับมอบหมาย เพื่อให้หน่วยงานการควบคุม หน่วยงานกำกับดูแล หรือหน่วยงานที่ให้ความเชื่อมั่นเป็นการภายใน ใช้ข้อมูล และ/หรือเพื่อให้ผู้บริหารใช้ข้อมูล ผู้บริหารมิได้ลงทุนในการว่าจ้างหรืออบรมบุคลากรให้มีทักษะด้านการอำนวยความสะดวกหรือการประเมินความเสี่ยง และผู้ตรวจสอบภายในอาจเป็นบุคลากรเพียงคนเดียวที่มีความรู้รอบด้านในเรื่องการประเมินความเสี่ยง ความเสี่ยงจะถูกประเมินเมื่อจำเป็นต้องการเท่านั้น ตัวอย่างเช่น ผู้บริหารระดับสูงอาจประเมินความเสี่ยงที่เกี่ยวข้องกับกลยุทธ์ที่เขาเสนอปีละหน โครงการใหญ่ๆ และมีราคาสูงอาจต้องมีการประเมินความเสี่ยงเพราะความจำเป็น
ภาษาความเสี่ยง	ผู้บริหารจะใช้ข้อมูลความเสี่ยงเมื่อพวกเขามีข้อมูลความเสี่ยง แต่การใช้ศัพท์แสงอาจไม่สม่ำเสมอหรืออาจมีการแปลผิดความหมายไปทั่วองค์กร ทะเบียนความเสี่ยงและหลักเกณฑ์การวัดความเสี่ยงอาจจะไม่เหมือนกัน ขึ้นอยู่กับว่าจุดสนใจของการประเมินความเสี่ยงอยู่ที่ใด เกณฑ์การวัดความเสี่ยงก็ง่ายๆ เช่น ประเมินว่า สูง กลาง หรือต่ำ
การใช้ข้อมูลความเสี่ยง	ข้อมูลความเสี่ยงจะไม่ถูกรวบรวม หรือสื่อสารออกไปนอกกลุ่มที่ทำการประเมินความเสี่ยง
2 - มีการทำซ้ำ (Repeatable)	
ระดับความเสี่ยงที่ยอมรับได้	มีการระบุระดับความเสี่ยงที่องค์กรยอมรับได้โดยผู้บริหารระดับสูงและคณะกรรมการบริษัทรวมทั้งมีการจัดทำเอกสารไว้ แต่ไม่ได้กระจายไปทั่วทั้งองค์กร เรื่องนี้ไม่ได้มีการแวะเวียนเข้ามาดูอย่างสม่ำเสมอเพื่อทำให้เป็นปัจจุบัน

รูปที่ 2 : ตัวอย่างคำอธิบายระดับต่างๆ ของแบบจำลองวุฒิภาวะ (ต่อ)

การประเมินความเสี่ยง	ผู้ตรวจสอบภายในทำการประเมินความเสี่ยง เพื่อรวบรวมข้อมูลสำหรับการปฏิบัติงานที่ได้รับมอบหมาย เพื่อให้หน่วยงานการควบคุม หน่วยงานกำกับดูแล หรือหน่วยงานที่ให้ความเชื่อมั่นเป็นการภายในใช้ข้อมูล และ/หรือเพื่อให้ผู้บริหารใช้ข้อมูล ผู้บริหารมิได้ลงทุนในการว่าจ้างหรืออบรมบุคลากรให้มีทักษะด้านการอำนวยความสะดวกหรือการประเมินความเสี่ยง มีการประเมินความเสี่ยงอย่างสม่ำเสมอ แต่ไม่มีการวางแผนกลยุทธ์ หรือวางแผนให้ครอบคลุมครบทุกด้านโครงการใหญ่ๆ และราคาสูงอาจได้รับการประเมินความเสี่ยงแค่เพียงครั้งเดียว
ภาษาความเสี่ยง	ผู้บริหารจะใช้ข้อมูลความเสี่ยงเมื่อพวกเขามีข้อมูลอยู่ แต่การใช้ศัพท์แสงอาจไม่สม่ำเสมอไปทั่วองค์กร ทะเบียนความเสี่ยงและ หลักเกณฑ์การวัดความเสี่ยงอาจจะไม่เหมือนกัน ขึ้นอยู่กับว่าจุดสนใจของการประเมินความเสี่ยงคือที่ใด เกณฑ์การวัดความเสี่ยงอาจมีการคำนึงเรื่องความน่าจะเป็น และผลกระทบ และเกณฑ์การวัดความเสี่ยงก็ง่ายๆ เช่น ประเมินว่า สูง กลาง หรือต่ำ
การใช้ข้อมูลความเสี่ยง	ข้อมูลความเสี่ยงบางครั้งถูกรวบรวมหรือสื่อสารนอกกลุ่มที่ทำการประเมินความเสี่ยง
3 - มีการกำหนด (Defined)	
ระดับการยอมรับความเสี่ยง	ผู้บริหารระดับสูงและคณะกรรมการบริษัทมีการกำหนดระดับความเสี่ยงที่ยอมรับได้อย่างคร่าวๆ และทั่วทั้งองค์กรอาจเข้าใจกันดีหรืออาจไม่เข้าใจก็ได้
การประเมินความเสี่ยง	หน่วยงานการควบคุม การกำกับดูแล การบริหารความเสี่ยง หรือหน่วยงานที่ให้ความเชื่อมั่นเป็นภายในอาจทำการประเมินความเสี่ยงสำหรับงานของเขา หรือสำหรับให้ผู้บริหารใช้ ผู้บริหารมิได้ลงทุนในการว่าจ้างหรืออบรมบุคลากรให้มีทักษะด้านการอำนวยความสะดวกและการประเมินความเสี่ยง จะทำการประเมินความเสี่ยงเมื่อมีความจำเป็น ตัวอย่างเช่น ผู้บริหารระดับสูงอาจร้องร้องขอให้มีการประเมินความเสี่ยงสำหรับโครงการที่ใช้เงินลงทุนขนาดใหญ่ที่มีโอกาสเสี่ยงสูงสำหรับองค์กร

รูปที่ 2 : ตัวอย่างคำอธิบายระดับต่างๆ ของแบบจำลองวุฒิภาวะ (ต่อ)

ภาษาความเสี่ยง	ผู้บริหารจะใช้ข้อมูลความเสี่ยงเมื่อเมื่อพวกเขามีข้อมูลอยู่ และการใช้ศัพท์แสงส่วนมากแล้วจะสม่ำเสมอไปทั่วทั้งองค์กร มีการใช้ทะเบียนความเสี่ยงและเกณฑ์การวัดความเสี่ยงในหลายรูปแบบ
การใช้ข้อมูลความเสี่ยง	ความเสี่ยงอาจถูกผูกกับวัตถุประสงค์ของฝ่ายหรือทีมของโครงการ แต่มักจะไม่ได้รับการพิจารณากันอย่างเปิดเผยโดยผู้บริหารระดับสูงขององค์กร
4-มีการจัดการ - Managed	
ระดับการยอมรับความเสี่ยง	ผู้บริหารระดับสูงและคณะกรรมการได้กำหนดระดับความความเสี่ยงที่ยอมรับได้และเป็นที่เข้าใจกันดีทั่วทั้งองค์กร
การประเมินความเสี่ยง	หน่วยงานการควบคุม การกำกับดูแล หรือหน่วยงานให้ความเชื่อมั่นเป็นการภายใน ทำการประเมินความเสี่ยงอย่างสม่ำเสมอสำหรับงานของเขา หรือสำหรับให้ผู้บริหารใช้ ผู้บริหารมีการลงทุนในการว่าจ้างและอบรมบุคลากรให้มีทักษะด้านการอำนวยความสะดวกและการประเมินความเสี่ยง ทำการประเมินความเสี่ยงเมื่อมีความจำเป็น และจัดการความเสี่ยงที่มีนัยสำคัญเมื่อเริ่มเกิด มากกว่าที่จะยึดติดกับแผนการตรวจที่อาศัยตามความเสี่ยงเป็นพื้นฐาน
ภาษาความเสี่ยง	ผู้บริหารระดับสูงมีการขอและใช้ข้อมูลความเสี่ยงอย่างสม่ำเสมอ และมีการใช้ศัพท์แสงซึ่งเป็นที่รู้จักกันทั่วทั้งองค์กร เกณฑ์การบริหารความเสี่ยงเป็นที่เข้าใจและนำมาใช้ปฏิบัติทั่วทั้งองค์กร
การใช้ข้อมูลความเสี่ยง	ความเสี่ยงที่มีนัยสำคัญถูกผูกกับวัตถุประสงค์ขององค์กร มีการสื่อสารข้อมูลความเสี่ยงให้กับผู้บริหารระดับสูงอย่างสม่ำเสมอ และค่าตอบแทนหรือรางวัลจูงใจของผู้บริหารอาจถูกผูกกับ KPI ที่ถูกขับเคลื่อนโดยความเสี่ยงที่ได้ถูกระบุและประเมินมาแล้ว ข้อมูลจะถูกใช้เพื่อมีส่วนช่วยในการปรับปรุงกระบวนการบริหารความเสี่ยงให้ดีขึ้นทั่วทั้งองค์กร
5.- มีประสิทธิภาพสูงสุด (Optimized)	
ระดับการยอมรับความเสี่ยง	เมื่อคณะกรรมการได้อนุมัติระดับการยอมรับความเสี่ยง ผู้บริหารและบุคลากรหลักได้นำไปใช้ปฏิบัติทั่วองค์กรในรูปแบบและระดับรายละเอียดที่เหมาะสมสำหรับการตัดสินใจ

รูปที่ 2 : ตัวอย่างคำอธิบายระดับต่างๆ ของแบบจำลองวุฒิภาวะ (ต่อ)

การประเมินความเสี่ยง	ผู้บริหารใช้กระบวนการเหมือนๆ กันในการประเมินความเสี่ยง จัดทำเอกสารข้อมูลความเสี่ยง และเฝ้าติดตามการปฏิบัติงานโดยเทียบกับ KPI ที่ได้ถูกปรับตามค่าความเสี่ยงแล้ว ผู้บริหารมีการกำหนดระเบียบพิธีการไว้แล้วที่จะทำให้มั่นใจว่าความเสี่ยงที่มีนัยสำคัญจะได้รับการจัดการเมื่อมันเกิดขึ้น แทนที่จะคอยจนกว่าจะถึงการประเมินความเสี่ยงครั้งถัดไป
ภาษาความเสี่ยง	ทั้งองค์กร ตั้งแต่คณะกรรมการบริษัท จนถึงผู้บริหารและพนักงานระดับปฏิบัติการมีความเข้าใจตรงกันถึงศัพท์แสงที่ใช้ในกระบวนการบริหารความเสี่ยง (เช่น ความเสี่ยง ปัจจัยที่ส่งผล การควบคุม ผลกระทบ ความน่าจะเป็น) และใช้ภาษาที่เข้าใจตรงกันเพื่อหารือกันเรื่องความเสี่ยง
การใช้ข้อมูลความเสี่ยง	ความเสี่ยงได้ถูกผูกเข้ากับวัตถุประสงค์ขององค์กรในทุกระดับ นอกจากนั้น ข้อมูลความเสี่ยงถูกสื่อสารไปทั่วทั้งองค์กรอย่างต่อเนื่อง และการกำหนดค่าตอบแทนและรางวัลจูงใจของผู้บริหารจะเชื่อมโยงกับ KPI ที่ถูกขับเคลื่อนโดยความเสี่ยงซึ่งได้ระบุและประเมินไว้แล้ว

บทบาทของตรวจสอบภายในในการบริหารความเสี่ยง

มาตรฐาน 2120 – การบริหารความเสี่ยง ระบุว่า “หน่วยงานตรวจสอบภายในต้องประเมินความมีประสิทธิผลและมีส่วนช่วยในการปรับปรุงกระบวนการบริหารความเสี่ยง” โดยเฉพาะอย่างยิ่ง มาตรฐานได้กำหนดให้หน่วยงานตรวจสอบภายในประเมินว่า:

- วัตถุประสงค์ขององค์กรเป็นไปในทิศทางเดียวกันกับพันธกิจขององค์กร
- ผู้บริหารได้ประเมินความเสี่ยงที่มีนัยสำคัญ
- การตอบสนองต่อความเสี่ยงของผู้บริหาร เป็นไปในทิศทางเดียวกันกับระดับความเสี่ยงที่องค์กรยอมรับได้
- ข้อมูลความเสี่ยงที่เกี่ยวข้องได้ถูกระบุและสื่อสารภายในองค์กรซึ่งรวมถึงคณะกรรมการในเวลาที่เหมาะสม

เพื่อให้การประเมินนี้สำเร็จลุล่วงได้ หน่วยงานตรวจสอบภายในอาจรวบรวมข้อมูลจากการปฏิบัติงานที่ได้รับมอบหมายหลายๆ งาน และอาจนำผลจากการปฏิบัติงานต่างๆ มารวมพิจารณาเข้าด้วยกัน เพื่อให้เกิดความ

เข้าใจอย่างครบถ้วนในกระบวนการบริหารความเสี่ยงขององค์กร และลงความเห็นเกี่ยวกับประสิทธิผลของกระบวนการเหล่านั้นได้ หน่วยงานตรวจสอบภายในจะต้องให้ความเชื่อมั่นว่า ผู้บริหารได้มีกิจกรรมเพื่อที่จะเฝ้าติดตามกระบวนการบริหารความเสี่ยงอย่างต่อเนื่องอยู่แล้ว

หน่วยงานตรวจสอบภายในอาจถูกเรียกให้ไปมีบทบาทเพิ่มเติมในการบริหารความเสี่ยง หากหน่วยงานตรวจสอบภายในถูกร้องขอให้ช่วยพัฒนากระบวนการบริหารความเสี่ยง (เช่น ทำการประเมินและจัดทำเอกสารเกี่ยวกับการประเมินความเสี่ยง) อาจจะก่อให้เกิดคำถามด้านความเป็นอิสระขึ้นได้ เพื่อให้เข้าใจถ่องแท้ถึงบทบาทที่เหมาะสม ผู้ตรวจสอบภายในควรทบทวนชุดของมาตรฐานที่เริ่มจาก 1100 – ความเป็นอิสระและความเที่ยงธรรม โดยควรให้ความสนใจในมาตรฐาน 1130 – การเสื่อมเสียความเป็นอิสระหรือความเที่ยงธรรม เป็นพิเศษ รวมทั้งมาตรฐานด้านการให้ความเชื่อมั่นและให้คำปรึกษาที่เกี่ยวเนื่องกัน มาตรฐานเหล่านี้ได้แสดงให้เห็นความแตกต่างระหว่างกิจกรรมที่เหมาะจะเป็นงานให้ความเชื่อมั่น และงานที่ให้คำปรึกษา ตัวอย่างเช่น ถือได้ว่าความเที่ยงธรรมจะเสื่อมลงหากผู้ตรวจสอบภายในได้ให้บริการด้านการให้ความเชื่อมั่นในกิจกรรมใดๆ ที่ผู้ตรวจสอบภายในได้รับผิดชอบในปีที่ผ่านมา (มาตรฐาน 1130.A1)

มาตรฐาน 1112 – บทบาทของหัวหน้าหน่วยงานตรวจสอบภายในที่นอกเหนือจากการตรวจสอบภายใน มาตรฐานนี้ยอมรับว่าหัวหน้าหน่วยงานตรวจสอบภายในอาจถูกร้องขอให้รับบทบาทและหน้าที่อื่นที่นอกเหนือจากการตรวจสอบภายใน เช่น กิจกรรมการควบคุมการปฏิบัติตามกฎระเบียบ หรือการบริหารความเสี่ยง เป็นต้น มาตรฐานได้ระบุว่า “เมื่อหัวหน้าหน่วยงานตรวจสอบภายในมีหรือคาดว่าจะมีบทบาท หรือภาระหน้าที่อื่นที่นอกเหนือจากการตรวจสอบภายใน จะต้องมีมาตรการป้องกันเพื่อจำกัดการสูญเสียความเป็นอิสระหรือความเที่ยงธรรม” มาตรการป้องกันดังกล่าวก็คือกิจกรรมการควบคุมดูแลซึ่งมักจะทำโดยคณะกรรมการ เพื่อที่จะระบุการเสื่อมเสียที่อาจเกิดขึ้นได้ หากหัวหน้าหน่วยงานตรวจสอบภายในมีภาระหน้าที่เกี่ยวกับการบริหารความเสี่ยงหรือหน้าที่งานอื่นที่เกี่ยวข้องกันแล้ว การให้บริการความเชื่อมั่นในด้านนั้นจะต้องถูกดูแลควบคุมโดยกลุ่มบุคคลที่อยู่นอกหน่วยงานตรวจสอบภายใน (มาตรฐาน 1130.A2)
บางองค์กรอาจมองว่าบทบาทของผู้ตรวจสอบภายในในการพัฒนากระบวนการบริหารความเสี่ยงเป็นการให้บริการให้คำปรึกษา ซึ่งไม่น่าจะมีผลกระทบต่อความเป็นอิสระ อย่างไรก็ตาม ควรคำนึงถึงมาตรฐาน

1130.C1 และมาตรฐาน 1130.C2 และผู้ตรวจสอบภายในควรเปิดเผยความเสื่อมเสียอันอาจเกิดขึ้นได้ (หากมี) ทางเลือกทางหนึ่งคือการแยกกลุ่มตรวจสอบ โดยมี 1 กลุ่มทำงานด้านกระบวนการบริหารความเสี่ยง และอีกกลุ่มหนึ่งประเมินความมีประสิทธิผลของกระบวนการนั้นๆ ส่วนอีกทางเลือกหนึ่ง ยอมให้ผู้ตรวจสอบภายในเป็นผู้พัฒนากระบวนการบริหารความเสี่ยง โดยมีแผนที่จะส่งมอบการปฏิบัติและการดูแลควบคุมกระบวนการนั้นๆ ไปยังบุคลากรที่อยู่ในหน่วยงานที่ทำหน้าที่ควบคุมการปฏิบัติตามกฎระเบียบ/การบริหารความเสี่ยง/การให้ความเชื่อมั่นเป็นภายใน หรือผู้บริหารระดับปฏิบัติการ ที่ผ่านการอบรมมาแล้ว

การประเมินการบริหารความเสี่ยงขององค์กร

ตามมาตรฐาน 2200 – การวางแผนสำหรับงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในต้องจัดทำและจดบันทึกแผนสำหรับแต่ละงานที่ได้รับมอบหมาย ซึ่งรวมถึง วัตถุประสงค์ ขอบเขต ช่วงเวลาที่จะปฏิบัติงาน และการจัดสรรทรัพยากรสำหรับงานนั้นๆ แผนนี้จะต้องคำนึงถึง กลยุทธ์ วัตถุประสงค์ ขององค์กร และความเสี่ยงที่เกี่ยวข้องกับงานที่ได้รับมอบหมาย

เนื้อหาในส่วนนี้ มุ่งจะให้แนวทางแก่ผู้ตรวจสอบภายในสำหรับกระบวนการวางแผนและการลงมือประเมินการบริหารความเสี่ยงขององค์กร ตัวอย่างที่ให้ไว้ซึ่งเป็นเพียงบางส่วน น่าจะช่วยผู้ตรวจสอบภายในตัดสินว่าจะรวมถึงเรื่อง/ประเด็นสำคัญใดบ้าง ประเภทเอกสารที่ต้องร้องขอ และหลักฐานที่ควรได้รับมา

อาจเป็นการยากที่จะประเมินกระบวนการบริหารความเสี่ยงทั้งหมดขององค์กรได้ ดังนั้น ควรมีการกำหนดขอบเขตของงานที่ได้รับมอบหมายโดยใช้เกณฑ์ที่จะทำให้สำเร็จผลตามวัตถุประสงค์เฉพาะอย่างได้ ตัวอย่างเช่น ขอบเขตอาจถูกกำหนดตามหน่วยงานขององค์กร สถานที่ตั้ง วัตถุประสงค์ทางกลยุทธ์ หรือโดยเกณฑ์อื่นที่มีประโยชน์ต่อองค์กร

ทำความเข้าใจบริบทและเป้าประสงค์ของงานที่ได้รับมอบหมาย

ตามที่ได้อธิบายเรื่องแบบจำลองวุฒิภาวะของการบริหารความเสี่ยง (**รูปที่** 1) โครงสร้างและกระบวนการควบคุมดูแลที่กำหนดแน่นอนแล้วมักจะส่งเสริมกระบวนการบริหารความเสี่ยงในองค์กรที่มีวัฒนธรรมที่มุ่งเน้นเรื่องความเสี่ยง แต่ในทางกลับกัน องค์กรหนึ่งอาจไม่มีโครงสร้างหรือกระบวนการที่รับผิดชอบเรื่องการบริหารความเสี่ยงโดยเฉพาะเลย

ในการประเมินการบริหารความเสี่ยงขององค์กร งานที่ได้รับมอบหมายของผู้ตรวจสอบภายในงานหนึ่งจะประกอบไปด้วย 2 ส่วน ส่วนแรกคือการระบุหลักการที่ใช้ในกระบวนการบริหารความเสี่ยงขององค์กร และอีกส่วนคือการประเมินว่าหลักการเหล่านั้นยังคงเหมาะสมและมีประสิทธิผล

ในการวางแผนการประเมิน ผู้ตรวจสอบภายในควรศึกษาแนวทางในการนำมาตรฐานไปใช้ปฏิบัติสำหรับมาตรฐาน 2120 – การบริหารความเสี่ยง และคำนึงถึงองค์ประกอบดังต่อไปนี้:

- กลยุทธ์และแผนธุรกิจ พันธกิจ และวัตถุประสงค์ขององค์กร
- กรอบการบริหารความเสี่ยงที่ใช้ในองค์กร
- วิธีการและระดับของการระบุ การประเมิน และการดูแลความเสี่ยงที่ใช้ในปัจจุบัน
- กระบวนการที่สามารถใช้ในการเฝ้าติดตาม ประเมิน และตอบโต้ต่อความเสี่ยงและโอกาส
- ความซับซ้อนขององค์กรและกระบวนการบริหารความเสี่ยงขององค์กร โดยคำนึงถึงขนาด ความซับซ้อน วงจรชีวิต วุฒิภาวะ โครงสร้างผู้มีส่วนได้เสีย และสภาพแวดล้อมทางกฎหมายและสภาพแวดล้อมทางการแข่งขัน

รูปแบบมาตรฐานของขั้นตอนการวางแผนงาน

- ทำความเข้าใจในบริบทและจุดมุ่งหมายของงานที่ได้รับมอบหมาย
- รวบรวมข้อมูลเพื่อทำความเข้าใจงานหรือกระบวนการที่ทำการสอบทาน
- ทำการประเมินความเสี่ยงเบื้องต้นสำหรับงานหรือกระบวนการที่ทำการสอบทาน
- กำหนดวัตถุประสงค์ของงานที่ได้รับมอบหมาย
- กำหนดขอบเขตของงานที่ได้รับมอบหมาย
- จัดสรรทรัพยากร
- จดบันทึกแนวการปฏิบัติงานตรวจสอบ

แนวปฏิบัติของ IIA เรื่อง "การวางแผนงานที่ได้รับมอบหมาย: การกำหนดวัตถุประสงค์และขอบเขต" ได้ให้รายละเอียดเป็นแนวทางว่าจะวางแผนและกำหนดขอบเขตของงานตรวจสอบที่ได้รับมอบหมายอย่างไรไว้แล้ว

- ความเข้มแข็งของบทบาทการบริหารความเสี่ยง ภาระหน้าที่ และกิจกรรมการบริหารความเสี่ยงต่างๆ ทั่วทั้งองค์กร
- ผลจากกิจกรรมที่ใช้ติดตามความเสี่ยงในปัจจุบัน และการระบุและการหารือเรื่องความเสี่ยง และการตอบโต้ที่ได้ถูกเลือกมาใช้กับความเสี่ยงแต่ละตัว
- ความเสี่ยงที่เคยประสบมาในอดีต
- การเปลี่ยนแปลงใดๆ (กฎระเบียบ บุคลากร กระบวนการ หรือผลิตภัณฑ์และบริการ) ที่อาจนำมาซึ่งความเสี่ยงใหม่ๆ
- ความเสี่ยงและโอกาสที่อาจเกิดขึ้นได้ รวมถึง พัฒนาการใหม่ๆ แนวโน้ม ความเสี่ยงที่กำลังเกิดขึ้น และการหยุดชะงักที่อาจเกิดขึ้นได้กับองค์กร (และเขตแดนและอุตสาหกรรมที่องค์กรดำเนินงานอยู่)
- กฎข้อบังคับหรือข้อกำหนด/ความคาดหวังจากภายนอกที่เกี่ยวข้องกับองค์กรและขอบเขตการกำหับดูแลตามกฎหมายที่องค์กรนั้นปฏิบัติงานอยู่
- ความคาดหวังของผู้ที่ส่วนได้เสียต่อหน่วยงานตรวจสอบภายในในการให้ความเชื่อมั่นว่ากระบวนการบริหารความเสี่ยงขององค์กรมีประสิทธิผล

ประเด็นสำคัญประเด็นหนึ่งที่หน่วยงานตรวจสอบภายในควรสำรวจดู คือ ผู้บริหารได้ประกาศชัดถึงวัตถุประสงค์สำหรับการบริหารความเสี่ยงแล้วหรือไม่ ผู้ตรวจสอบภายในควรหาหลักฐานมายืนยันว่า ผู้บริหารกำลังดำเนินกิจกรรมต่างๆ เพื่อที่จะบรรลุวัตถุประสงค์เหล่านั้นได้ นอกจากนี้ ผู้ตรวจสอบภายในควรทำความเข้าใจหลายๆ เรื่องให้ชัดเจนโดยเฉพาะเข้าใจวิสัยทัศน์ของผู้บริหารสำหรับกระบวนการบริหารความเสี่ยง แผนงานของผู้บริหารเหล่านั้น และกระบวนวิธีวัดผลที่พวกเขาใช้

ในขณะที่กำลังสร้างแผนการปฏิบัติงานของแต่ละงาน ผู้ตรวจสอบภายในควรรวบรวมข้อมูลโดยผ่านทางวิธีการต่างๆ เช่น การสอบทานการประเมินครั้งที่ผ่านมา (เช่น การประเมินความเสี่ยง รายงานจากผู้ให้บริการด้านความเชื่อมั่นและให้คำปรึกษา) การทำความเข้าใจและทำแผนผังทางเดินของงานกระบวนการบริหารความเสี่ยงและวิธีการควบคุม และสัมภาษณ์ผู้มีส่วนได้เสียที่เกี่ยวข้อง ข้อมูลที่ได้รับตลอดช่วงการวางแผนนี้ควรได้รับการจดบันทึกไว้เป็นอย่างดี ทำให้เป็นปัจจุบัน และคำนึงถึงข้อมูลเหล่านี้ตลอดช่วงการทำงานที่ได้รับ

มอบหมาย ข้อมูลนี้ยังอาจเป็นประโยชน์ต่อหัวหน้าหน่วยงานตรวจสอบภายในในการวางแผนระยะยาวสำหรับงานต่างๆ ในอนาคตอีกด้วย

การรวบรวมข้อมูลเพื่อทำความเข้าใจกระบวนการบริหารความเสี่ยง

เมื่อผู้ตรวจสอบภายในได้ระบุฝ่ายงาน หน้าที่งาน และบทบาทต่างๆ ในองค์กรที่มีส่วนเกี่ยวข้องกับงานที่ได้รับมอบหมายแล้ว พวกเขาควรรวบรวมข้อมูลเพื่อสนับสนุนการประเมินความเสี่ยงเบื้องต้น และการวางแผนงานที่ได้รับมอบหมาย ตามที่ได้ระบุไว้ในมาตรฐาน 2201 – ข้อพิจารณาในการวางแผน

องค์ประกอบต่อไปนี้จะช่วยให้ผู้ตรวจสอบภายในสามารถระบุความเสี่ยงและกลยุทธ์ที่ใช้ในการจัดการความเสี่ยงเหล่านั้นได้:

- กฎบัตร นโยบาย และคำสั่งอื่นๆ ที่ออกโดยหน่วยงานกำกับดูแลซึ่งมีหน้าที่จัดให้มีกลยุทธ์ในการบริหารความเสี่ยง
- การจัดทำเอกสารเกี่ยวกับกระบวนการบริหารความเสี่ยง ได้แก่ นโยบาย แนวทาง และมาตรฐาน
- คำแถลงเกี่ยวกับความเสี่ยงที่ยอมรับได้
- เอกสารเกี่ยวกับกลยุทธ์
- รายงานที่เกี่ยวกับการควบคุมและรายงานทางการบริหารอื่นๆ ที่มีข้อมูลเกี่ยวกับผลการปฏิบัติงาน
- รายงานการประชุมคณะกรรมการ/คณะกรรมการตรวจสอบ และคณะกรรมการอื่นๆ ที่เกี่ยวข้อง (เช่น คณะกรรมการความเสี่ยง)
- กรณีศึกษาทางธุรกิจสำหรับโครงการเงินลงทุนที่สำคัญ
- รายงานประจำงวดจากบุคคลภายนอก (ได้แก่ รายงานประจำปีของบริษัทมหาชนที่กำหนดโดย กลต.)
- การประเมินความเสี่ยงของผู้บริหาร
- รายการความเสี่ยงขององค์กร เช่น ความเสี่ยงด้านกลยุทธ์ ด้านการปฏิบัติงาน ด้านทรัพยากรมนุษย์ ด้านการเงิน ด้านการปฏิบัติตามกฎข้อบังคับของทางการ และทางด้านเทคโนโลยีสารสนเทศ

- เอกสารต่างๆ เกี่ยวกับระยะต่างๆ ของกระบวนการบริหารความเสี่ยงซึ่งได้แก่ การระบุความเสี่ยง การประเมิน การจัดการความเสี่ยง และการเฝ้าระวัง
- ผลจากกิจกรรมที่ทำหน้าที่เฝ้าระวังความเสี่ยง

ตามที่ได้เขียนไว้ในแนวปฏิบัติของ IIA เรื่อง "การประสานงานและการพึ่งพาผลงานของผู้อื่น: การจัดทำแผนที่การให้ความเชื่อมั่น (Coordination and Reliance: Developing an Assurance Map) ไว้แล้วว่า การบริหารความเสี่ยงในองค์กรเป็นภาระหน้าที่ของทุกๆ คน ดังนั้น จึงควรมีข้อมูลให้พร้อมใช้ในทุกหน่วยธุรกิจ ถึงแม้ว่าจะไม่ได้มีการจัดทำเอกสารอย่างเป็นทางการหรือมีอยู่ชัดเจน แต่บางครั้ง ความเสี่ยงก็สามารถมีการประเมินโดยเปิดเผยได้ เช่น ในระหว่างการวางแผนกลยุทธ์ อย่างไรก็ตาม อาจมีการระบุความเสี่ยงไว้ไม่ชัดเจนนัก เช่น ถูกกล่าวถึงในกรณีศึกษาทางธุรกิจ (เช่น "โครงการนี้อาจก่อให้เกิดรายได้น้อยกว่าที่คาด เนื่องจากปัจจัยเหล่านี้.....") ในการระบุความเสี่ยงให้มากที่สุดเท่าที่จะทำได้ ผู้ตรวจสอบภายในควรใช้ข้อมูลที่มากกว่ารายงานที่ได้จากงานที่ได้รับมอบหมายครั้งที่ผ่านมา หรือ จากการประเมินความเสี่ยงที่จำกัดแค่ความเสี่ยงบางตัวที่เห็นได้ชัดเท่านั้น

การประเมินความเสี่ยงเบื้องต้น

มาตรฐาน 2210.A1 ระบุว่า "ผู้ตรวจสอบภายในต้องทำการประเมินเบื้องต้นถึงความเสี่ยงที่เกี่ยวข้องกับกิจกรรมที่ตรวจสอบ" แนวทางที่ใช้ในการประเมินความเสี่ยงที่มีอยู่ในกระบวนการบริหารความเสี่ยงขององค์กร มักจะแตกต่างจากแนวทางที่ใช้ในการประเมินความเสี่ยงเบื้องต้นในช่วงของการวางแผนงานที่ได้รับมอบหมายประเภทอื่น

วิธีที่มีประสิทธิผลวิธีหนึ่งในการปฏิบัติและจดบันทึกการประเมินความเสี่ยง ณ ระดับงานที่ได้รับมอบหมาย คือ การสร้างตารางแมทริกซ์ความเสี่ยงโดยระบุความเสี่ยงต่างๆ ที่เกี่ยวข้องในตารางแล้วจึงเพิ่มการวัดค่าความมีนัยสำคัญใส่เข้าไปในแมทริกซ์ รูปแบบของแมทริกซ์อาจแตกต่างกัน แต่โดยทั่วไปแล้วจะมีแถวแนวนอน (row) สำหรับความเสี่ยงแต่ละตัว และแถวแนวตั้ง (column) สำหรับวัดความเสี่ยงแต่ละตัวได้แก่ ผลกระทบ และความน่าจะเป็น

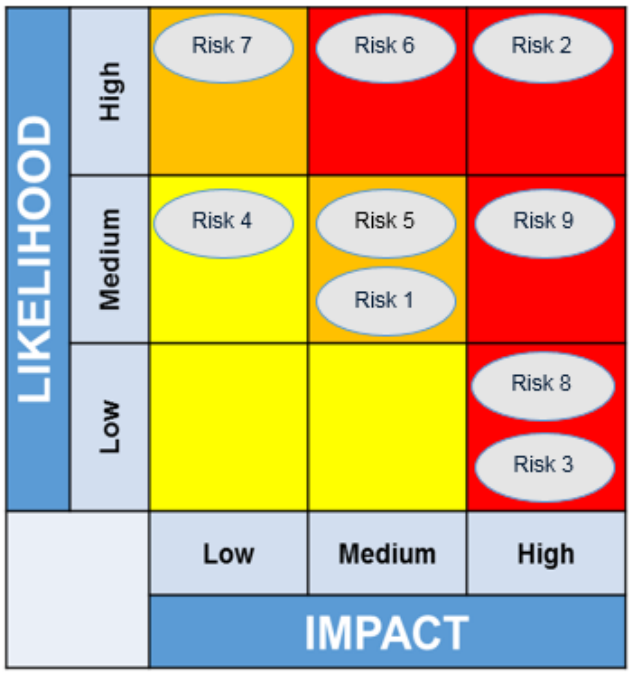
ข้อควรพิจารณาในทางการตรวจสอบ

ผู้ตรวจสอบภายในอาจเลือกที่จะประเมินกระบวนการบริหารความเสี่ยงในบริบทของงานที่ได้รับมอบหมายตามแผนงานตรวจสอบภายใน หรือ เป็นส่วนหนึ่งในการประเมินกระบวนการได้รับการระบุว่ามีความเสี่ยง ซึ่งการประเมินนี้เป็นการประเมินต่างหากก็ได้ แนวปฏิบัติของ IIA เรื่อง "การประสานงานและการพึ่งพาผลงานของผู้อื่น: การจัดทำแผนที่การให้ความเชื่อมั่น (Coordination and Reliance: Developing an Assurance Map) อาจช่วยผู้ตรวจสอบภายในในการระบุกระบวนการที่เกี่ยวข้องกับความเสี่ยงได้

ในองค์กรที่มีกระบวนการบริหารความเสี่ยงที่เจริญเติบโตเต็มที่ หน่วยงานตรวจสอบภายในอาจสามารถสอบทานและใช้การประเมินความเสี่ยงของผู้บริหารได้แทนที่จะต้องมาจัดทำเอง จากการผูกการประเมินกระบวนการบริหารความเสี่ยงเข้ากับแบบจำลองวุฒิภาวะ ผู้ตรวจสอบภายในได้แสดงให้เห็นชัดเจนว่าการประเมินความเสี่ยงเป็นองค์ประกอบหลักของการวัดระดับวุฒิภาวะของการบริหารความเสี่ยง หากผู้บริหารยังไม่เคยทำ ผู้ตรวจสอบภายในอาจจัดทำรายชื่อความเสี่ยงซึ่งเสี่ยงต่อกระบวนการบริหารความเสี่ยงที่ตกอยู่ในกลุ่มต่างๆ ในแบบจำลองวุฒิภาวะได้แก่ กลุ่มวัฒนธรรม การกำกับดูแล และกระบวนการ (ดู ภาคผนวก ง. สำหรับตัวอย่างของตารางแมทริกซ์ความเสี่ยงและการควบคุมซึ่งแสดงกลุ่มเหล่านี้อยู่แล้ว)
ความเสี่ยงเหล่านั้นจะถูกให้คะแนนในด้านผลกระทบ และความน่าจะเป็น แผนผังความเสี่ยงที่เรียกว่า Heat Map ดังตัวอย่างใน**รูปที่ 3** ก็เป็นเครื่องมือหนึ่งที่ใช้เพื่อให้เห็นภาพความมีนัยสำคัญของความเสี่ยง โดยมีการใช้มาตรวัดแบบง่ายๆ ได้แก่ สูง กลาง และต่ำ

นอกจากนั้น แผนผังความเสี่ยง อาจถูกเก็บไว้เป็นเอกสารสนับสนุนการวางแผนงานที่ได้รับมอบหมาย และแนวการปฏิบัติงาน เพื่อให้สอดคล้องกับมาตรฐาน 2240 – แนวการปฏิบัติงาน

รูปที่ 3 : แผนผังความความเสี่ยง (Heat Map)



การกำหนดวัตถุประสงค์ของงานที่ได้รับมอบหมาย

มาตรฐาน 2210 – วัตถุประสงค์ของงานที่ได้รับมอบหมาย มาตรฐานได้ระบุว่า “ต้องมีการกำหนดวัตถุประสงค์สำหรับงานแต่ละงานที่ได้รับมอบหมาย” โดยมาตรฐาน 2210.A1 และ 2210.A2 ได้เพิ่มเติมในเรื่องวัตถุประสงค์ของงานที่ได้รับมอบหมายไว้ว่า วัตถุประสงค์ของงานที่ได้รับมอบหมายต้องสะท้อนให้เห็นผลจากการประเมินความเสี่ยงเบื้องต้นนี้และต้องพิจารณาถึงความน่าจะเป็น (ซึ่งก็คือ โอกาสที่จะเกิด) ของความเสี่ยงที่มีนัยสำคัญได้แก่ ความผิดพลาด การทุจริต และการไม่ปฏิบัติตามกฎระเบียบ

วัตถุประสงค์โดยรวมของการประเมินกระบวนการบริหารความเสี่ยงขององค์กร มักจะเป็นไปเพื่อให้ความกระจ่างแจ้งต่อผู้บริหารระดับสูงและคณะกรรมการเกี่ยวกับระดับวุฒิภาวะของการบริหารความเสี่ยงขององค์กร และมันสอดคล้องกับความคาดหวังของพวกเขาหรือไม่ การประเมินนี้อาจรวมถึงการวัดโดยการเทียบเคียงกับวิธีปฏิบัติที่เป็นเลิศซึ่งทางผู้บริหารระดับสูงและคณะกรรมการได้เลือกหรืออนุมัติให้ใช้ได้

สำหรับงานให้ความเชื่อมั่น ตามมาตรฐาน 2210.A3 ระบุว่า เกณฑ์ที่เพียงพอเป็นสิ่งจำเป็นต่อการประเมินการกำกับดูแล การบริหารความเสี่ยง และหากผู้ตรวจสอบภายในพบว่าผู้บริหารระดับสูงและคณะกรรมการได้จัดตั้งเกณฑ์ที่เหมาะสมเพียงพอแล้ว (เช่น มีการใช้กรอบโครงสร้างการบริหารความเสี่ยง) ก็ควรใช้เกณฑ์นั้นในการประเมิน หากยังไม่มีเกณฑ์ที่เหมาะสม ผู้ตรวจสอบภายในควรหารือร่วมกับผู้บริหารและ/หรือคณะกรรมการในการสร้างเกณฑ์การประเมินผล ตัวอย่างชนิดของเกณฑ์ที่ใช้ในการประเมินอาจได้แก่:

- เกณฑ์ภายใน (เช่น นโยบาย และระเบียบปฏิบัติขององค์กร)
- เกณฑ์ภายนอก (เช่น กฎหมาย และระเบียบข้อบังคับที่ใช้บังคับ)
- วิธีปฏิบัติชั้นนำ (เช่น อุตสาหกรรม และแนวทางในทางวิชาชีพ)

ผู้ตรวจสอบภายในสามารถปรับเปลี่ยนและนำแบบจำลองวุฒิภาวะที่กล่าวมาแล้วมาใช้เพื่อสะท้อนให้เห็นถึงเกณฑ์เหล่านี้ตามความเหมาะสมของแต่ละองค์กร อาจมีการนำข้อกำหนดจากภายนอกมาใช้ร่วมกับวิธีปฏิบัติที่เป็นเลิศของอุตสาหกรรม ผนวกเข้ากับแบบจำลองวุฒิภาวะ และนำมาเปรียบเทียบกับนโยบาย และวิธีปฏิบัติขององค์กร

สำหรับองค์กรที่ยังไม่เจริญเติบโตนัก งานให้คำปรึกษาอาจจะเหมาะกว่า และวัตถุประสงค์ของงานก็อาจจะต้องได้รับความเห็นชอบจากผู้บริหารระดับสูงและ/หรือคณะกรรมการ ในงานให้คำปรึกษานั้น วัตถุประสงค์จะเป็นไปในลักษณะของการให้คำแนะนำ ตัวอย่างเช่น เพื่อที่จะสร้างความตระหนักถึงคุณค่าของการนำกระบวนการบริหารความเสี่ยงที่เป็นทางการมากขึ้นมาใช้ปฏิบัติ

การกำหนดขอบเขตของงานที่ได้รับมอบหมาย

หัวหน้าหน่วยงานตรวจสอบภายใน หรือผู้ตรวจสอบภายในที่ได้รับมอบหมายจากหัวหน้าหน่วยงานตรวจสอบภายใน ควรมีส่วนร่วมในการประชุมที่เกี่ยวกับความเสี่ยงและการบริหารความเสี่ยง ในทุกครั้งทั่วทั้งองค์กร ซึ่งอาจช่วยขับเคลื่อนให้หน่วยงานตรวจสอบภายในสามารถหาแนวทางกำหนดขอบเขตของการประเมิน ดังเช่นที่

ได้กำหนดไว้ในมาตรฐาน 2220 - เรื่องขอบเขตของงานที่ได้รับมอบหมาย ที่ว่า ขอบเขตของงานที่ได้รับมอบหมาย จะต้องเพียงพอที่จะบรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมายได้

อย่างน้อยที่สุด ขอบเขตของการประเมินใดๆ ก็ตาม ที่เกี่ยวกับการบริหารความเสี่ยง ควรยืนยันได้ว่ากระบวนการที่เกี่ยวกับความเสี่ยงที่ถูกระบุนั้น ได้มีการปฏิบัติตามและเป็นไปตามเกณฑ์ภายนอก (เช่น กฎหมาย ข้อบังคับ ข้อกำหนดเกี่ยวกับอุตสาหกรรม) หรือไม่ เมื่อกำหนดขอบเขตของงานที่ได้รับมอบหมาย ผู้ตรวจสอบภายในอาจพิจารณาถึง:

1. ความเพียงพอและมีประสิทธิผลในการปฏิบัติงานของนโยบาย ระเบียบปฏิบัติ และกิจกรรมที่สนับสนุนกระบวนการบริหารความเสี่ยง รวมถึงความสอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ ความคาดหวังของผู้มีส่วนได้เสีย และมาตรฐานอุตสาหกรรม
2. ความมีประสิทธิผลของโครงสร้างการกำกับดูแลที่สนับสนุนนโยบาย วิธีปฏิบัติ และกิจกรรมที่เกี่ยวกับกระบวนการบริหารความเสี่ยง
3. ความเพียงพอของทรัพยากรที่ทุ่มเทให้กับการสนับสนุนกระบวนการบริหารความเสี่ยง
4. การรวมประเด็นต่อไปนี้ไว้ในกระบวนการบริหารความเสี่ยง:

    - การกำหนดบทบาทและหน้าที่ของการบริหารความเสี่ยงและการให้ความเชื่อมั่นให้ชัดเจน ในทั่วทั้งองค์กร
    - การคำนึงถึงความเสี่ยงไว้ชัดเจนแล้วในกลยุทธ์ขององค์กร
    - รายการ/ทะเบียนความเสี่ยง เกณฑ์การจัดระดับความเสี่ยง และกระบวนการประเมินความเสี่ยง
    - ความคาดหวังเกี่ยวกับการจัดการความเสี่ยง
    - การรายงานความเสี่ยงที่กำหนดไว้
    - กระบวนการในการจัดประเภท การยกระดับการรายงาน และการติดตามสิ่งที่พบจากกิจกรรมการเฝ้าระวังความเสี่ยง

ในขณะที่องค์ประกอบเหล่านี้ควรปรากฏให้เห็นได้ในรูปแบบใดรูปแบบหนึ่งโดยเป็นส่วนหนึ่งของกระบวนการบริหารความเสี่ยง ผู้ตรวจสอบภายในอาจดัดแปลงขอบเขตให้เข้ากับความต้องการเฉพาะอย่างขององค์กร หรืองานแต่ละงานที่ได้รับมอบหมาย

การจัดสรรทรัพยากร

เมื่อได้กำหนดวัตถุประสงค์และของเขตของงานที่ได้รับมอบหมายแล้ว หัวหน้าหน่วยงานตรวจสอบภายใน หรือผู้ตรวจสอบภายในที่ได้รับมอบหมายจะต้องพิจารณาลักษณะและความซับซ้อนของงานที่ได้รับมอบหมายนั้น ข้อจำกัดด้านเวลา และทรัพยากรที่มีอยู่ แล้วจึงตัดสินว่าจำนวนของทรัพยากร และความสามารถที่ผสมผสานกัน มีเพียงพอที่จะทำงานที่ได้รับมอบหมาย โดยใช้ความระมัดระวังในทางวิชาชีพอย่างเหมาะสม (มาตรฐาน 2230 – การจัดสรรทรัพยากรสาหรับงานที่ได้รับมอบหมาย) ได้หรือไม่

ในการประเมินกระบวนการบริหารความเสี่ยง ผู้ตรวจสอบภายในควรทราบถึงข้อกำหนดสำหรับการบริหารความเสี่ยงของอุตสาหกรรมที่องค์กรดำเนินงานอยู่ รวมทั้งต้องคุ้นเคยกับกรอบโครงสร้างความเสี่ยงและกรอบการควบคุมหลายๆ แบบ และเข้าใจวัฒนธรรมขององค์กร และการควบคุมเชิงนามธรรม (soft controls) อื่นๆ ขององค์กร

เนื่องจากการประเมินกระบวนการบริหารความเสี่ยงทั้งหมดขององค์กรเป็นงานที่ต้องใช้แรงงานและเวลาเป็นอย่างมาก หัวหน้าหน่วยงานตรวจสอบภายในควรพัฒนาแนวทางสำหรับงานที่ได้รับมอบหมายที่สมเหตุสมผลในแง่ของทรัพยากร ในการที่จะทำให้มั่นใจได้ว่ามีทรัพยากรเพียงพอนั้น งานที่ได้รับมอบหมายอาจใช้แนวทางได้หลายแบบ ตามที่แสดงใน**รูปที่** 4 ขึ้นอยู่กับโครงสร้างขององค์กร ตัวอย่างที่แสดงถึงแนวทางที่เหมาะสมต่อไปนี้ เป็นเพียงแค่บางส่วนเท่านั้น

รูปที่ 4 : **ตัวอย่างแนวทางในการปฏิบัติงานที่ได้รับมอบหมาย**

แนวทางจากบนลงล่าง	
วิธีการรวบรวมข้อมูลที่มีประสิทธิผลที่สุด	■ การสัมภาษณ์ ■ การสอบทานเอกสาร
ผู้ที่มักจะต้องเข้าร่วม	■ สมาชิกคณะกรรมการ (เช่น คณะกรรมการตรวจสอบ และ/หรือประธานคณะกรรมการความเสี่ยง) ■ ผู้บริหารระดับสูง ■ ผู้บริหารกลุ่ม/ฝ่าย
ข้อจำกัด	■ ระดับรายละเอียดที่เก็บรวบรวมได้จะอยู่ในระดับต่ำ ■ การประเมินอาจเน้นที่การกำกับดูแลโดยถือเป็นหน้าที่งานของผู้เข้าร่วม ■ มุมมองของคณะกรรมการและผู้บริหารระดับสูงอาจไม่ได้เป็นตัวแทนของบุคลากรอื่นทั้งหมดในองค์กร โดยเฉพาะเกี่ยวกับเรื่องวัฒนธรรม

แนวทางจากล่างสู่บน	
วิธีรวบรวมข้อมูลที่มีประสิทธิผลที่สุด	■ การสัมภาษณ์ ■ การทำแบบสอบถาม ■ การสอบทานเอกสาร ■ การทำความเข้าใจกระบวนการจัดทำเอกสาร หรือกระบวนการปฏิบัติงาน (Walk-throughs)
ผู้ที่มักจะต้องเข้าร่วม	■ ผู้จัดการสายการผลิต ■ ผู้ควบคุมงาน
ข้อจำกัด	■ แบบสอบถามอาจทำให้เกิดความสับสนหากไม่มีการใช้ภาษาความเสี่ยงที่เข้าใจตรงกันหรือกระบวนการที่เหมือนกัน ■ อาจไม่ได้กระจายความเห็นตอบกลับไปอย่างสม่ำเสมอให้กับผู้เข้าร่วมทุกคน ■ ผู้จัดการสายการผลิตและผู้ควบคุมงานหลายๆ คน อาจไม่สามารถเข้าร่วมได้เนื่องจากข้อจำกัดด้านเวลาและทรัพยากร (ซึ่งอาจเป็นข้อบ่งชี้ถึงการให้ความสำคัญต่อกระบวนการบริหารความเสี่ยงได้)
แนวทางผสม	
วิธีรวบรวมข้อมูลที่มีประสิทธิผลที่สุด	■ การสัมภาษณ์ (บุคลากรระดับสูง) ■ การทำแบบสอบถาม (บุคลากรระดับล่าง) ■ การสอบทานเอกสาร
ผู้ที่มักจะต้องเข้าร่วม	■ สมาชิกคณะกรรมการ (เช่น ประธานคณะกรรมการตรวจสอบ และ/หรือ ประธานคณะกรรมการความเสี่ยง) ■ ผู้บริหารระดับสูง ■ ผู้บริหารกลุ่ม/ฝ่าย ■ ผู้จัดการสายการผลิต
ข้อจำกัด	■ แม้วิธีการนี้น่าจะให้มุมมองที่ครอบคลุมมากขึ้น แต่ข้อจำกัดที่ได้เอ่ยถึงไว้ข้างบนก็ยังอาจเกิดขึ้นได้

การจัดทำเอกสารแนวการปฏิบัติงานสำหรับงานที่ได้รับมอบหมาย

ในระหว่างการวางแผนงาน ผู้ตรวจสอบภายในจะจดบันทึกข้อมูลเกี่ยวกับงานที่ได้รับมอบหมายไว้ในกระดาษทำการ ข้อมูลนี้จะกลายเป็นส่วนหนึ่งของแนวการปฏิบัติงานสำหรับงานที่ได้รับมอบหมายที่ต้องจัดทำเพื่อให้บรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมายได้ (มาตรฐาน 2240 – แนวการปฏิบัติงาน)

กระบวนการกำหนดวัตถุประสงค์และขอบเขตของงานที่ได้รับมอบหมายอาจก่อให้เกิดกระดาษทำการอย่างใดอย่างหนึ่ง หรือทั้งหมดดังต่อไปนี้:

- แผนผังกระบวนการ
- ทะเบียนความเสี่ยง
- สรุปการสัมภาษณ์ และแบบสอบถาม
- เหตุผลในการตัดสินใจเกี่ยวกับระดับวุฒิภาวะของการบริหารความเสี่ยงขององค์กร
- เกณฑ์ที่จะใช้ในการประเมินกระบวนการบริหารความเสี่ยง

การปฏิบัติงานที่ได้รับมอบหมาย และการรายงานผล

จากภาคผนวก จ. แสดงให้เห็นในระดับทั่วไปถึง กิจกรรมที่ผู้ตรวจสอบภายในจะสามารถปฏิบัติโดยเป็นส่วนหนึ่งของการประเมินกระบวนการบริหารความเสี่ยงขององค์กร มาตรฐานชุด 2300 (การปฏิบัติงานที่ได้รับมอบหมาย) ไดอธิบายถึงข้อกำหนดในการระบุ วิเคราะห์ ประเมินและบันทึกข้อมูลที่เพียงพอต่อการปฏิบัติงานเพื่อให้บรรลุวัตถุประสงค์ของงานที่ได้รับมอบหมายได้

งานที่ได้รับมอบหมายควรก่อให้เกิดข้อเสนอแนะที่เหมาะสมต่อสถานะในปัจจุบันและสถานะที่ต้องการในอนาคตของผู้บริหารในแบบจำลองวุฒิภาวะ ผู้ตรวจสอบภายในควรปฏิบัติตามวิธีการที่กำหนดไว้ของหน่วยงานตรวจสอบภายในในการสื่อสารถึงผลของงานที่ได้รับมอบหมาย ตามที่ระบุไว้ในมาตรฐานชุด 2400 (การสื่อสารผลการปฏิบัติงาน) และแนวทางการนำเอามาตรฐาน 2400 ไปใช้ปฏิบัติ ผู้ตรวจสอบภายในควรสังเกตว่า เพื่อให้เป็นไปตามมาตรฐาน 2410 – เกณฑ์สำหรับการสื่อสาร และมาตรฐาน 2410.A1 ในรายงานชุดสุดท้ายที่สื่อสารถึงผลการปฏิบัติงานนั้น จะต้องใส่ วัตถุประสงค์ ขอบเขต ผลการปฏิบัติงานของงานที่ได้รับมอบหมาย ข้อสรุปที่ใช้การได้ ข้อเสนอแนะ และ/หรือแผนดำเนินการแก้ไข ไว้ในรายงานด้วย

เพื่อให้สอดคล้องกับมาตรฐาน 2440 – การเผยแพร่ผลการปฏิบัติงาน หัวหน้าหน่วยงานตรวจสอบภายในต้องสื่อสารผลการปฏิบัติงานไปยังกลุ่มบุคคลที่เหมาะสม สำหรับการประเมินกระบวนการบริหารความเสี่ยงแล้วอาจจะเกี่ยวข้องกับการออกรายงานให้กับผู้บริหารระดับสูง คณะกรรมการ และกลุ่มบุคคลอื่น ตามความเหมาะสม การสื่อสารอาจจะต้องปรับให้เหมาะกับผู้รับรายงานเหล่านั้น

การประเมินกระบวนการบริหารความเสี่ยงของหน่วยงานตรวจสอบภายใน

เพื่อประเมินประสิทธิภาพและประสิทธิผลของหน่วยงานตรวจสอบภายในและเพื่อระบุโอกาสในการปรับปรุงงาน โดยให้สอดคล้องกับมาตรฐาน 1300 – โครงการประกันคุณภาพและปรับปรุงงาน นั้น หัวหน้าหน่วยงานตรวจสอบภายในอาจประยุกต์ใช้บทเรียนที่ได้จากการประเมินการบริหารความเสี่ยงทั่วทั้งองค์กรโดยตรวจสอบภายใน การใช้แบบจำลองวุฒิภาวะของการบริหารความเสี่ยง (ตาม**รูปที่ 1**) อาจช่วยให้หัวหน้าหน่วยงานตรวจสอบภายในปรับปรุงกระบวนการบริหารความเสี่ยงของหน่วยงานตรวจสอบภายในได้ และดำเนินการให้ไปสู่ระดับที่สูงขึ้นในทุกๆ แง่มุมของทุกกลุ่ม ระดับวุฒิภาวะที่เติบโตขึ้นจะช่วยเพิ่มความสามารถในการให้บริการความเชื่อมั่นและบริการให้คำปรึกษาของหน่วยงานตรวจสอบภายใน พร้อมทั้งทำให้สามารถปกป้องและเพิ่มคุณค่าองค์กรได้ดียิ่งขึ้น

ภาคผนวก ก. มาตรฐานและแนวปฏิบัติของสมาคมผู้ตรวจสอบภายใน (IIA) ที่เกี่ยวข้อง

แหล่งข้อมูลของสมาคมผู้ตรวจสอบภายใน (IIA) ต่อไปนี้ได้ถูกใช้อ้างอิงตลอดแนวปฏิบัตินี้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการประยุกต์ใช้*มาตรฐานสากลสำหรับการปฏิบัติงานวิชาชีพการตรวจสอบภายใน* กรุณาดู **แนวทางการนำมาตรฐานไปใช้ปฏิบัติ (Implementation Guides) ของ IIA** ด้วย

ประมวลจรรยาบรรณ
หลักการที่ 1: ความมีคุณธรรม
หลักการที่ 2: ความเที่ยงธรรม
หลักการที่ 3: การรักษาความลับ
หลักการที่ 4: ความสามารถในหน้าที่
มาตรฐาน
มาตรฐาน 1100 – ความเป็นอิสระและความเที่ยงธรรม
มาตรฐาน 1112 – บทบาทของหัวหน้าหน่วยงานตรวจสอบภายในที่นอกเหนือจากการตรวจสอบภายใน
มาตรฐาน 1130 – การเสื่อมเสียความเป็นอิสระหรือความเที่ยงธรรม
มาตรฐาน 2050 – การประสานงานและการพึ่งพาผลงานของผู้อื่น
มาตรฐาน 2120 – การบริหารความเสี่ยง
มาตรฐาน 2200 – การวางแผนสำหรับงานที่ได้รับมอบหมาย
มาตรฐาน 2201 – ข้อพิจารณาในการวางแผน
มาตรฐาน 2210 – วัตถุประสงค์ของงานที่ได้รับมอบหมาย
มาตรฐาน 2220 – ขอบเขตของงานที่ได้รับมอบหมาย
มาตรฐาน 2230 – การจัดสรรทรัพยากรสำหรับงานที่ได้รับมอบหมาย
มาตรฐาน 2240 – แนวการปฏิบัติงาน
มาตรฐาน 2300 – การปฏิบัติงานที่ได้รับมอบหมาย
มาตรฐาน 2400 – การสื่อสารผลการปฏิบัติงาน
มาตรฐาน 2410 – เกณฑ์สำหรับการสื่อสาร
มาตรฐาน 2440 – การเผยแพร่ผลการปฏิบัติงาน
แนวปฏิบัติ
แนวปฏิบัติเรื่อง “รายงานการตรวจสอบ: การสื่อสารผลการปฏิบัติงานตรวจสอบที่ได้รับมอบหมาย” ปี 2559 แนวปฏิบัติเรื่อง “การประสานงานและการพึ่งพาผลงานของผู้อื่น: การพัฒนาแผนที่การให้ความเชื่อมั่น” ปี 2561 แนวปฏิบัติเรื่อง “การวางแผนสำหรับงานที่ได้รับมอบหมาย: การกำหนดวัตถุประสงค์ และขอบเขต” ปี 2560

ภาคผนวก ข. อภิธานศัพท์

คำศัพท์ที่มีเครื่องหมายดอกจัน (*) มาจากภาคอภิธานศัพท์ของ *กรอบการปฏิบัติงานวิชาชีพสากลของ IIA* ฉบับปีพ.ศ. 2560 (*The IIA's International Professional Practices Framework®)*

คณะกรรมการ – board*: คณะบุคคลในระดับสูงสุดที่ทำหน้าที่ในการกำกับดูแลองค์กร (ตัวอย่างเช่น คณะกรรมการองค์กร คณะกรรมการกำกับดูแล หรือคณะกรรมการนโยบาย หรือ ทรัสตี) ซึ่งมีหน้าที่ในการสั่งการและ/หรือสอดส่องดูแลกิจกรรมขององค์กร และพิจารณาความรับผิดชอบในผลงานการบริหารของผู้บริหารระดับสูง ถึงแม้การจัดระบบการกำกับดูแลอาจแตกต่างกันไปตามแต่ละขอบเขตอำนาจของแต่ละรัฐ หรือในแต่ละภาคส่วน โดยมากแล้ว คณะกรรมการจะรวมถึงสมาชิกที่ไม่ได้มีส่วนในการบริหาร หากในองค์กรไม่มีคณะกรรมการแล้ว คำว่า "คณะกรรมการ" ที่ใช้ในมาตรฐานนี้จะหมายถึง กลุ่มคนหรือบุคคลที่ทำหน้าที่กำกับดูแลองค์กร นอกจากนั้น คำว่า "คณะกรรมการ" ที่ใช้ในมาตรฐานนี้ อาจหมายถึง คณะหรือองค์คณะอื่นใดที่ทางองค์คณะซึ่งมีหน้าที่กำกับดูแลได้มอบหมายหน้าที่บางอย่างให้ (เช่น คณะกรรมการตรวจสอบ)

หัวหน้าหน่วยงานตรวจสอบภายใน – chief audit executive*: คำว่า หัวหน้าหน่วยงานตรวจสอบภายใน จะหมายถึง บทบาทของบุคคลซึ่งอยู่ในตำแหน่งงานที่อยู่ในระดับสูง ซึ่งรับผิดชอบในการบริหารหน่วยงานตรวจสอบภายในให้มีประสิทธิผลโดยสอดคล้องกับกฎบัตรของหน่วยงานตรวจสอบภายใน และ องค์ประกอบส่วนที่เป็นภาคบังคับของกรอบการปฏิบัติงานวิชาชีพตรวจสอบภายในที่เป็นสากล หัวหน้าหน่วยงานตรวจสอบภายใน หรือบุคคลที่ต้องรายงานต่อหัวหน้าหน่วยงานตรวจสอบภายใน ควรมีประกาศนียบัตรทางวิชาชีพและคุณสมบัติที่เหมาะสม อย่างไรก็ตามชื่อตำแหน่ง และ/หรือหน้าที่ของหัวหน้าหน่วยงานตรวจสอบภายใน อาจแตกต่างกันในแต่ละองค์กร

สภาพแวดล้อมของการควบคุม – control environment*: ทัศนคติและการกระทำของคณะกรรมการและฝ่ายบริหารในการให้ความสำคัญกับการควบคุมภายในองค์กร สภาพแวดล้อมของการควบคุมนี้ทำให้เกิดระบบระเบียบและโครงสร้างในอันที่จะบรรลุวัตถุประสงค์เบื้องต้นของระบบควบคุมภายในสภาพแวดล้อมของการควบคุมมีองค์ประกอบดังนี้

- ความมีคุณธรรมและคุณค่าทางจริยธรรม
- ปรัชญาทางการบริหารและลักษณะของการบริหาร
- โครงสร้างขององค์กร

- การมอบหมายอำนาจและหน้าที่
- นโยบายและวิธีปฏิบัติทางด้านทรัพยากรบุคคล
- ความสามารถของบุคลากร

หน่วยงานตรวจสอบภายใน – internal audit activity*: ฝ่าย สายงาน คณะที่ปรึกษา หรือ ผู้ปฏิบัติหน้าที่อื่น ๆ ที่ให้บริการการให้ความเชื่อมั่นและการให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระ ซึ่งออกแบบมาเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานขององค์กร หน่วยงานตรวจสอบภายในช่วยให้องค์กรบรรลุเป้าหมายได้ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการกำกับดูแล การบริหารความเสี่ยง และการควบคุม อย่างเป็นระบบและเป็นระเบียบ

แบบจำลองวุฒิภาวะ – maturity model: มาตรวัดที่ใช้วัดสถานะปัจจุบันขององค์กรและความคืบหน้าไปสู่ความเชี่ยวชาญในบริเวณที่กำหนด

ระดับความเสี่ยงที่ยอมรับได้ – risk appetite*: ระดับความเสี่ยงที่องค์กรเต็มใจที่จะยอมรับ

การบริหารความเสี่ยง – risk management*: กระบวนการในการระบุ ประเมิน จัดการ และควบคุมเหตุการณ์หรือสถานการณ์ไม่พึงประสงค์ที่อาจจะเกิดขึ้น เพื่อก่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ขององค์กร

ภาคผนวก ค. สถานการณ์ความเสี่ยงที่อาจเกิดขึ้นได้

เพื่อให้มั่นใจว่าองค์กรจะประสบความสำเร็จและสร้างคุณค่าได้ ความเสี่ยงที่มีนัยสำคัญขององค์กรทั้งหมด ซึ่งรวมถึงความเสี่ยงในการสูญเสียโอกาส จะต้องมีการทำความเข้าใจให้ชัดเจน จัดลำดับความสำคัญ และจัดการอย่างเหมาะสม การประเมินและให้ความเชื่อมั่นในกระบวนการบริหารความเสี่ยงอย่างเหมาะสมจะช่วยให้องค์กรสามารถดำเนินการเพื่อป้องกันหรือจัดการกับสถานการณ์ความเสี่ยงดังเช่นรายการที่ระบุไว้ในที่นี้ได้อย่างเหมาะสม มิฉะนั้นแล้ว ความสามารถในการบรรลุเป้าหมายและวัตถุประสงค์ขององค์กรอาจถูกบั่นทอนลงได้:

- ความเชื่อมั่นอย่างเป็นอิสระที่ให้ต่อคณะกรรมการและผู้บริหารระดับสูงไม่เพียงพอและนำไปสู่ความเข้าใจผิดในระหว่างทั้งสองกลุ่มว่า ได้มีการจัดการความเสี่ยงให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ขององค์กรแล้ว และสนับสนุนองค์กรให้สามารถบรรลุวัตถุประสงค์และกลยุทธ์ได้อย่างเพียงพอแล้ว
- การกำกับดูแลการบริหารความเสี่ยง ระบบ และกระบวนการเกิดความล้มเหลว ส่งผลเสียต่อการกำกับดูแลขององค์กรและเกี่ยวพันถึงการจัดอันดับโดยหน่วยงานที่มีหน้าที่จัดอันดับ ซึ่งต่อมาได้ถูกสื่อสารต่อไปยังผู้มีส่วนได้เสียและตลาดแล้ว
- เหตุการณ์ความเสี่ยงที่สามารถป้องกันได้เกิดขึ้น ส่งผลให้เกิดหนี้สิน ค่าปรับ การลงโทษจากหน่วยราชการ และเกิดผลเสียอื่นๆ ที่เกี่ยวข้องตามมา รวมถึงการสูญเสียสินทรัพย์ ทรัพย์สินทางปัญญา ส่วนแบ่งทางการตลาด โอกาสสร้างรายได้ ความภักดีของลูกค้า และชื่อเสียงของตราผลิตภัณฑ์
- การจัดสรรทรัพยากรและการกำหนดบทบาทหน้าที่ ไม่ได้ถูกปรับใช้ให้เหมาะสม ดังนั้น จึงไม่สามารถสร้างกระบวนการบริหารความเสี่ยงด้านการปฏิบัติงานที่ยั่งยืนให้เกิดขึ้นได้
- วัฒนธรรมองค์กรขัดขวางความก้าวหน้าเพื่อก้าวไปสู่ระดับวุฒิภาวะของการบริหารความเสี่ยงที่สูงขึ้น
- ความเสี่ยงอาจถูกเพิกเฉย ไม่ได้มีการจัดลำดับความสำคัญอย่างเหมาะสม หรือไม่ได้ถูกทำให้บรรเทาลงอย่างมีประสิทธิผล นำไปสู่การเกิดเหตุการณ์ความเสี่ยงที่กีดขวางไม่ให้วัตถุประสงค์และกลยุทธ์ของธุรกิจและองค์กรประสบผลสำเร็จ
- ข้อจำกัดทางด้านช่วงจังหวะเวลาและโอกาสไม่เป็นไปตามที่กำหนดเนื่องมาจากการจัดการความเสี่ยงที่ผิดพลาด
- การจัดลำดับความสำคัญและกลยุทธ์ขององค์กรไม่ได้ถูกกำหนดขึ้นพร้อมๆ กับความตระหนักรู้ในเรื่องความเสี่ยงหรือตัวผลักดันให้เกิดความเสี่ยงที่ซ่อนอยู่เบื้องหลังความคิดริเริ่มต่างๆ

- ไม่ได้คำนึงถึงความเสี่ยงทางด้านสารสนเทศ ทรัพยากรมนุษย์ และการจัดหาเงินทุน ส่งผลให้เกิดความสูญเสียทางด้านการเงิน หรือการปฏิบัติงาน หรือความล้มเหลวของกลยุทธ์

ภาคผนวก ง. ตารางความเสี่ยง และการควบคุม

ตารางต่อไปนี้แสดงรายการประเด็นความเสี่ยงที่สำคัญและวิธีการควบคุมหลักบางส่วนที่ผู้ตรวจสอบภายในควรพิจารณาเมื่อทำการประเมินกระบวนการบริหารความเสี่ยงขององค์กร ตารางรายการนี้ยังไม่ครบถ้วนสมบูรณ์หรือตั้งใจให้นำไปใช้เป็นแนวการปฏิบัติงานสำหรับงานที่ได้รับมอบหมายหรือใช้เป็นรายการ (checklist) เพื่อการตรวจสอบได้

ความเสี่ยงทางด้านวัฒนธรรม	
ความเสี่ยง	**วิธีการควบคุม**
▪ ไม่มีการจัดสรรทรัพยากรให้กับการขยายงานบริหารความเสี่ยง ▪ ความเสี่ยงถูกมองว่ามีหน่วยงานตรวจสอบภายในและหน้าที่งานควบคุม “เป็นเจ้าของ” ▪ การกำหนดเวลาการสัมภาษณ์ และรับผลตอบกลับจากแบบสอบถามในเวลาที่เหมาะสมนั้นเป็นเรื่องยาก ▪ ข่าวร้ายไม่ขึ้นไปถึงเบื้องบนขององค์กร ▪ ความท้าทายที่จะให้ทั่วทั้งองค์กรร่วมมือกันนั้น ไม่สามารถคาดการณ์ได้ หรือมากกว่าที่ได้คาดการณ์ไว้ ▪ องค์กรไม่สามารถรับรู้ว่า มีผู้ตอบสนองต่อการเปลี่ยนแปลงอย่างไร ▪ องค์กรมองกระบวนการบริหารความเสี่ยงว่าเป็นสิ่งที่กำหนดไว้ ▪ หน่วยงานตรวจสอบภายในไม่สามารถรายงานและอธิบายสิ่งที่ตรวจพบรวมทั้งการจัดอันดับความเสี่ยงได้อย่างมีประสิทธิผล ▪ ผู้บริหารกลัวความเสี่ยง ▪ ประเพณีวัฒนธรรมขัดแย้งกับเป้าหมายและวัตถุประสงค์ของการบริหารความเสี่ยง	▪ หน่วยงานตรวจสอบภายในดำเนินการประชุมเชิงปฏิบัติการหรือทำการสัมภาษณ์เพื่อนำพาให้พนักงานเข้าใจกระบวนการบริหารความเสี่ยง ▪ คณะกรรมการให้ความมั่นใจใน การปฏิบัติให้เห็นเป็นแบบอย่างโดยผู้นำองค์กร (Tone at the top) ที่มีประสิทธิผล ▪ การประชุมแบบลับจะทำให้พนักงานสามารถแสดงความคิดเห็น/แจ้งประเด็นหรืออุปสรรคทางวัฒนธรรมเพื่อสื่อสารข้อมูลความเสี่ยง ▪ ผู้บริหารระดับสูงสนับสนุนให้มีการประชุม มีการอภิปรายและการแลกเปลี่ยนข้อมูลระหว่างผู้บริหารในทุกระดับ อย่างสม่ำเสมอ ▪ ผู้บริหารให้ความมั่นใจว่าการรายงานข้อมูลความเสี่ยงขึ้นไปยังเบื้องบนในองค์กรจะไม่เกิดการ แก้แค้น/เอาคืน

ภาคผนวก ง. ตารางความเสี่ยง และการควบคุม (ต่อ)

ความเสี่ยงทางด้านการกำกับดูแล	
ความเสี่ยง	**วิธีการควบคุม**
▪ หน่วยต่างๆ (คณะกรรมการ ผู้บริหาร ทางการ ผู้มีหน้าที่กำกับดูแล) มีข้อกำหนดสำหรับการบริหารความเสี่ยงที่แตกต่างกัน ▪ ไม่มีระบบการรายงานประเด็นเกี่ยวกับการบริหารความเสี่ยงที่เป็นมาตรฐาน (เช่น ช่วงจังหวะเวลา รูปแบบ) ▪ ผู้บริหารไม่มีการพูดถึงเรื่องความเสี่ยงในการประชุมให้สม่ำเสมอ ▪ คณะกรรมการไม่ได้เล่นบทบาทของกำกับดูแลอย่างเพียงพอ	▪ เกณฑ์สำหรับการบริหารความเสี่ยงภายในและภายนอกเป็นที่รู้จักและถูกสร้างขึ้นในกระบวนการ ▪ องค์กรลงทุนในซอฟต์แวร์เกี่ยวกับการรายงานความเสี่ยง ▪ คณะกรรมการและผู้บริหารระดับสูงร้องขอข้อมูลความเสี่ยงตลอดทั่วทั้งองค์กร

ความเสี่ยงทางด้านกระบวนการ	
ความเสี่ยง	**วิธีการควบคุม**
▪ กระบวนการประเมินความเสี่ยงไม่สม่ำเสมอกันทั่วทั้งองค์กร ▪ มีการระบุความเสี่ยงมากเกินไป ▪ ผลลัพธ์ของความเสี่ยงไม่ได้มีการเฝ้าติดตามประเมิน ▪ เกณฑ์ของผลกระทบและโอกาสที่จะเกิดเหตุการณ์ของความเสี่ยงมีความแตกต่างกัน ถึงแม้ว่าจะเป็นสายธุรกิจที่คล้ายคลึงกันก็ตาม ▪ การจัดการความเสี่ยงไม่ได้ถูกรายงานเหนือขึ้นไปกว่าระดับหัวหน้าผู้ควบคุมงาน	▪ องค์กรเห็นด้วยกับกรอบโครงสร้างการบริหารความเสี่ยงที่จะนำมาใช้ ▪ องค์กรลงทุนในทรัพยากรที่ใช้ในการรวบรวมข้อมูลความเสี่ยงและการรายงานเป็นระยะอย่างสม่ำเสมอ ▪ หน้าที่งานควบคุม (เช่น หน่วยงานกำกับดูแลการปฏิบัติตามกฎระเบียบ หน่วยงานกฎหมาย หน่วยงานที่ดูแลเรื่องสิ่งแวดล้อม สุขภาพและความปลอดภัย) ได้รับการฝึกอบรมเป็นอย่างดีในกระบวนการประเมินความเสี่ยง และผู้บริหารได้นำกรอบโครงสร้างการบริหารความเสี่ยงมาใช้

ภาคผนวก ง. ตารางความเสี่ยง และการควบคุม (ต่อ)

- หน่วยงานตรวจสอบภายในเป็นหน่วยงานเดียวที่ดำเนินการประเมินความเสี่ยงทั่วทั้งองค์กรได้เสร็จสมบูรณ์
- กระบวนการบริหารความเสี่ยงใช้ภาษาและคำบางคำที่บุคลากรไม่เข้าใจ
- ระดับจำนวนของความเสี่ยงที่ต้องการ (เป็นตัวเลข) ไม่ได้รับความเห็นชอบ
- การมุ่งเน้นไปที่ความเสี่ยงที่กำลังเกิดขึ้นใหม่ๆ ไม่เพียงพอ
- อภิธานศัพท์ ที่อธิบายคำศัพท์ที่เกี่ยวข้องกับการบริหารความเสี่ยงและคำอธิบายของกระบวนการการประเมินความเสี่ยง ได้มีการจัดเตรียมไว้ในก่อนที่จะมีการทำการประเมินความเสี่ยง
- ตารางแมทริกซ์ผลกระทบ และโอกาสที่จะเกิดเหตุการณ์ที่มีความเสี่ยง ได้ถูกนำมาใช้อย่างสม่ำเสมอทั่วทั้งองค์กร

ภาคผนวก จ. การประเมินกระบวนการบริหารความเสี่ยง

ในระดับทั่วๆ ไป ตารางเหล่านี้จะอธิบายกิจกรรมที่ผู้ตรวจสอบภายในอาจปฏิบัติโดยเป็นส่วนหนึ่งของการประเมินกระบวนการบริหารความเสี่ยงขององค์กร กิจกรรมเหล่านี้ไม่ได้เป็นแนวการปฏิบัติงานที่สมบูรณ์สำหรับการประเมินนั้นๆ ผู้ตรวจสอบภายในอาจจำเป็นต้องทำการวิเคราะห์ในเชิงลึกเพิ่มขึ้น และปรับขั้นตอนการทดสอบให้เหมาะสมกับนโยบายและวิธีการปฏิบัติงานที่เป็นเอกลักษณ์เฉพาะขององค์กร สำหรับการประเมินกระบวนการบริหารความเสี่ยงที่สมบูรณ์นั้น ผู้ตรวจสอบภายในอาจจำเป็นต้องสร้างแนวการปฏิบัติงานเฉพาะด้านของบริเวณที่เกี่ยวข้อง (เช่น ความเสี่ยงด้านกฎหมาย ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ การวางแผนเชิงกลยุทธ์) โดยเฉพาะอย่างยิ่ง หากการประเมินถูกแบ่งออกเป็นงานย่อยๆ ตามที่ได้กล่าวไว้ในแนวปฏิบัติฉบับนี้

วัฒนธรรมของการบริหารความเสี่ยง
การรายงานความเสี่ยง

- รวบรวมเอกสาร ซึ่งรวมถึง:
  - กฎบัตร นโยบาย และข้อมูลคำสั่งอื่นๆ สำหรับหน่วยงานกำกับดูแลที่มีหน้าที่ในการจัดตั้งและดูแลกระบวนการบริหารความเสี่ยง
  - การจัดทำเอกสารในทุกระยะของกระบวนการรายงานความเสี่ยง
- ทำความเข้าใจกับความเสี่ยงหลักที่ได้รับการระบุมาแล้วว่ามีความเกี่ยวข้องกับวัตถุประสงค์ขององค์กรอย่างไร
- ตัดสินว่าการรายงานความเสี่ยง มีการสื่อสารถึงสถานะของความเสี่ยงอย่างถูกต้องแม่นยำในองค์กร (เช่น มีความซับซ้อนเกินไป หรือง่ายเกินไปหรือไม่)
- ให้ค่าคะแนนความเสี่ยงให้เป็นไปตามกระบวนวิธีการประเมินความเสี่ยงตามที่องค์กรกำหนด
- สอบทานข้อมูลที่ได้รับจากการประเมินความเสี่ยงเบื้องต้น เพื่อประเมินผลกระทบและโอกาสที่จะเกิดเหตุการณ์ที่เกี่ยวข้องกับวัฒนธรรมความเสี่ยง

ภาคผนวก จ. การประเมินกระบวนการบริหารความเสี่ยง (ต่อ)

การสื่อสาร

- ติดตามการรายงานความเสี่ยงในหลายๆ จุด เพื่อให้แน่ใจว่าข้อมูลเกี่ยวกับความเสี่ยงได้มีการสื่อสารออกไปอย่างราบรื่นในทุกระดับทั่วทั้งองค์กรหรือไม่
- ตรวจสอบการสอบสวนกรณีจริยธรรมและการปฏิบัติตามกฎในเรื่องที่เกี่ยวกับความเสี่ยง เพื่อตัดสินว่ามีปัญหาการแก้แค้นหรือเอาคืนที่มาจากการสื่อสารข้อมูลความเสี่ยงหรือไม่
- ใช้แบบสำรวจ การสัมภาษณ์ หรือวิธีการอื่นเพื่อให้แน่ใจได้ว่า พนักงานได้เข้าร่วมในโครงการการสื่อสาร และระดับความเข้าใจในวัตถุประสงค์ของการบริหารความเสี่ยงขององค์กรของพวกเขามีอยู่ในระดับใด

ความรับผิดชอบในผลงานตามหน้าที่

- ยืนยันว่าเจ้าของความเสี่ยงมีหน้าที่รับผิดชอบต่อความเสี่ยงที่เกิดขึ้นในขอบเขตอำนาจของพวกเขา
- ยืนยันว่าคณะกรรมการ และผู้บริหารระดับสูงมีหน้าที่รับผิดชอบที่จะต้องร้องขอและนำข้อมูลความเสี่ยงไปใช้เพื่อการตัดสินใจ

การกำกับดูแลเรื่องการบริหารความเสี่ยง

การรายงานความเสี่ยง

- การนำข้อมูลความเสี่ยงที่รายงานไว้มาใช้ประโยชน์ในการประเมินวัฒนธรรมและตรวจสอบความเหมาะสมในแง่ของการแจกจ่ายข้อมูล การเฝ้าติดตามประเมิน และการเก็บรักษาข้อมูล
- สอบทานข้อมูลที่ได้รับจากการประเมินความเสี่ยงในเบื้องต้น เพื่อประเมินผลกระทบและโอกาสที่จะเกิดเหตุการณ์ที่เกี่ยวข้องกับการกำกับดูแลการบริหารความเสี่ยง

การรายงานคณะกรรมการ

- สอบทานรายงานที่เกี่ยวข้องกับความเสี่ยงที่ได้ถูกจัดทำขึ้นสำหรับคณะกรรมการ ทำให้แน่ใจว่ารายงานมีข้อมูลที่เกี่ยวข้องทั้งหมดซึ่งจำเป็นต่อคณะกรรมการที่จะนำไปใช้ในการตัดสินใจ
- สอบทานรายงานจากผู้บริหารระดับสูง เกี่ยวกับสถานะของความเสี่ยงที่เกี่ยวข้องกับกลยุทธ์และระดับความเสี่ยงที่ยอมรับได้

ภาคผนวก จ. การประเมินกระบวนการบริหารความเสี่ยง (ต่อ)

ระดับความเสี่ยงที่ยอมรับได้

- สอบทานข้อมูลรายละเอียดระดับความเสี่ยงที่ยอมรับได้ขององค์กร เพื่อดูความครบถ้วนและเพียงพอ ซึ่งรวมถึงองค์ประกอบต่อไปนี้:

  - ความเสี่ยงที่สามารถรับได้ (Risk capacity): ระดับความเสี่ยงสูงสุดที่องค์กรสามารถยอมรับได้ภายใต้ข้อผูกมัดและข้อจำกัดในปัจจุบัน รวมทั้งระดับของทรัพยากรที่มีอยู่

  - ขีดจำกัดความเสี่ยง (Risk limits): การจัดสรรขีดจำกัดของระดับความเสี่ยงที่ยอมรับได้โดยรวมขององค์กร ไปให้กับสายธุรกิจ หน่วยงานเกี่ยวกับกฎหมาย กลุ่มความเสี่ยงเฉพาะอย่าง และระดับย่อยอื่นๆ ที่เกี่ยวข้อง

  - การเบี่ยงเบนออกไปจากระดับความเสี่ยงที่ยอมรับได้ (Risk tolerance): จำนวนความเบี่ยงเบนที่องค์กรจะยอมรับได้ในแง่รายได้ และค่าใช้จ่าย ฯลฯ โดยกำหนดขอบเขตสำหรับความเสี่ยงที่สามารถรับได้และขีดจำกัดความเสี่ยงที่ตามมา

- สอบทานแผน และกระบวนการเพื่อสื่อสารระดับความเสี่ยงที่ยอมรับได้ไปยังพนักงานทุกคน
- ทำให้แน่ใจได้ว่า แผนนั้นครอบคลุมทั่วทั้งองค์กร และมีการดำเนินการตามแผนอย่างสม่ำเสมอ
- ใช้แบบสำรวจ การสัมภาษณ์ หรือวิธีการอื่นใด เพื่อให้มั่นใจในการเข้าร่วมโครงการการสื่อสารและระดับความเข้าใจของพนักงานเกี่ยวกับระดับความเสี่ยงที่ยอมรับได้ขององค์กร

กระบวนการบริหารความเสี่ยง

นโยบาย และวิธีปฏิบัติงาน

- พิสูจน์ว่านโยบายและวิธีปฏิบัติงานเป็นปัจจุบันและได้รับการปรับปรุงในเวลาที่เหมาะสมเมื่อมีการเปลี่ยนแปลงวิธีการปฏิบัติงานเกิดขึ้น
- ยืนยันว่าการปรับปรุงใดๆ ที่ร้องขอโดยคณะกรรมการในระหว่างการสอบทานประจำปี ได้กระทำอย่างถูกต้องเหมาะสม
- ทำให้แน่ใจว่านโยบายและวิธีปฏิบัติงานครอบคลุมกระบวนการบริหารความเสี่ยงทั้งหมดโดยละเอียด ส่วนที่มีความสำคัญเป็นพิเศษ ได้แก่:

  - ความสัมพันธ์กับกลยุทธ์ และระดับความเสี่ยงที่ยอมรับได้

  - ภาพรวมการกำกับดูแล

  - ขีดจำกัดความเสี่ยงและการเบี่ยงเบนออกไปพร้อมกับตัวกระตุ้นที่เกี่ยวเนื่องกัน และระเบียบพิธีการ

ภาคผนวก จ. การประเมินกระบวนการบริหารความเสี่ยง (ต่อ)

ในการยกระดับการรายงาน (เดินตามรอยกระบวนการปฏิบัติงานเริ่มตั้งแต่จุดที่ระบุว่ามีการฝ่าฝืน จนถึงการแก้ไขปัญหา)

- บทบาทและภาระหน้าที่
- ข้อควรคำนึงเกี่ยวกับข้อมูล

- ข้อกำหนดของทางการ

กระบวนการประเมินความเสี่ยง

- ระบุสถานที่และความถี่ในการประเมินความเสี่ยงทั่วทั้งองค์กร
- ตรวจสอบโดยละเอียดว่ากระบวนการระบุความเสี่ยง การประเมิน การจัดการ การเฝ้าติดตาม และการรายงานมีความสอดคล้องกันหรือไม่
- สอบทานข้อมูลที่ได้จากการประเมินความเสี่ยงในเบื้องต้น เพื่อประเมินผลกระทบและโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงที่เกี่ยวข้องกับกระบวนการบริหารความเสี่ยงทั่วทั้งองค์กร

ภาคผนวก ฉ. ข้อมูลอ้างอิง และอ่านเพิ่มเติม

ข้อมูลอ้างอิง

International Professional Practices Framework (IPPF), 2017 edition. Lake Mary, FL: The Institute of Internal Auditors, 2017.

อ่านเพิ่มเติม

Anderson, Richard J. and Mark L. Frigo. *Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors.* Lake Mary, FL: Internal Audit Foundation, 2017. https://bookstore.theiia.org/assessing-and-managing-strategic-risks.

Anderson, Urton and Andrew J. Dahle. *Applying the International Professional Practices Framework, 4th Edition*. Lake Mary, FL: Internal Audit Foundation, 2018. https://bookstore.theiia.org/applying-the-international-professional-practices-framework-4th-edition-2.

Baker, Larry L. *Practical Enterprise Risk Management: Getting to the Truth*. Lake Mary, FL: Internal Audit Foundation, 2018. https://bookstore.theiia.org/practical-enterprise-risk-management-getting-to-the-truth.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *COSO Enterprise Risk Management – Integrating with Strategy and Performance*. COSO, 2017. https://bookstore.theiia.org/enterprise-risk-management-integrating-with-strategy-and-performance.

Committee of Sponsoring Organizations of the Treadway Commission. *COSO Enterprise Risk Management – Integrating with Strategy and Performance: Compendium of Examples*. PwC, 2018. https://bookstore.theiia.org/coso-enterprise-risk-management-integrating-with-strategy-and-performance-compendium-of-examples.

International Organization for Standardization (ISO). ISO 31000:2018, *Risk management – Guidelines*. ISO, 2018. https://www.iso.org/standard/65694.html.

Sobel, Paul J. *Auditor's Risk Management Guide: Integrating Auditing and ERM, 2015 Edition.* Wolters Kluwer, 2015.

Sobel, Paul J. *Managing Risk in Uncertain Times: Leveraging COSO's New ERM Framework*. Lake Mary, FL: Internal Audit Foundation, 2018. https://bookstore.theiia.org/managing-risk-in-uncertain-times-2.

กิตติกรรมประกาศ

ทีมงานพัฒนาแนวปฏิบัติ

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

Hans-Peter Lerchner, CIA, Austria (Project Lead)

Susan Haseley, CIA, United States

Rune Johannessen, CIA, CCSA, CRMA, Norway

Ian Lyall, CIA, CCSA, CGAP, CRMA, Australia

Michael Lynn, CRMA, United States

Denis Neukomm, CIA, CRMA, Switzerland

ผู้ให้คำแนะนำแนวปฏิบัติที่มาจากทั่วโลก (Global Guidance Contributors)

Mohamed Ahmed Abdulla, Egypt

Lance Johnson, CIA, CRMA, United States

Cornelis Klumper, CIA, United States

Steven Nyakatuura, CFSA, South Africa

Tejinder Bob Shahi, CIA, Canada

Rita Thakkar, CIA, United States

มาตรฐานสากลและแนวปฏิบัติของ IIA (IIA Global Standards and Guidance)

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

Jim Pelletier, CIA, CGAP, Vice President

Cassian Jae, Managing Director

Jeanette York, CCSA, FS Director

Shelli Browning, Technical Editor

Lauressa Nelson, Technical Editor

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)

.

เกี่ยวกับ IIA

สมาคมผู้ตรวจสอบภายใน (IIA) เป็นหน่วยงานด้านการตรวจสอบภายในที่ได้รับการยอมรับอย่างกว้างขวางในการเป็นผู้ให้การสนับสนุน ผู้ให้ความรู้ และผู้กำหนดมาตรฐาน แนวทางปฏิบัติต่างๆ และวุฒิบัตรรับรองคุณวุฒิต่างๆ ที่เกี่ยวข้องกับวิชาชีพตรวจสอบภายใน สมาคมก่อตั้งขึ้นในปี พ.ศ. 2484 ในปัจจุบัน IIA ได้ให้บริการสมาชิกมากกว่า 190,000 คน จากมากกว่า 170 ประเทศและดินแดน สำนักงานใหญ่ของสมาคมตั้งอยู่ที่เลคแมรี่ (Lake Mary) รัฐฟลอริดา สหรัฐอเมริกา สำหรับข้อมูลเพิ่มเติมโปรดเยี่ยมชม www.globaliia.org

ข้อความปฏิเสธความรับผิดชอบ

IIA ตีพิมพ์เอกสารนี้เพื่อจุดประสงค์ในการให้ข้อมูลและเพื่อการศึกษาเท่านั้น และไม่ได้มีวัตถุประสงค์เพื่อให้คำตอบที่ชัดเจนที่สุดสำหรับสถานการณ์เฉพาะแต่ละสถานการณ์ ดังนั้น จึงมีวัตถุประสงค์เพียงเพื่อใช้เป็นแนวทางในการปฏิบัติงานเท่านั้น IIA ใคร่แนะนำให้ท่านขอคำปรึกษาจากผู้เชี่ยวชาญอิสระซึ่งมีความรู้เกี่ยวข้องโดยตรงกับสถานการณ์เฉพาะนั้นๆ IIA จะไม่รับผิดชอบใดๆ ต่อการที่ผู้ใดก็ตามเชื่อและอาศัยคำแนะนำนี้แต่เพียงอย่างเดียว

ลิขสิทธิ์

มีนาคม 2562

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