

ประกาศกระทรวงอุตสาหกรรม

ฉบับที่ ๔๔๒๙ (พ.ศ. ๒๕๕๕)

ออกตามความในพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม

พ.ศ. ๒๕๑๑

เรื่อง กำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรม

หลักการและแนวทางการบริหารความเสี่ยง

อาศัยอำนาจตามความในมาตรา ๑๕ แห่งพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม พ.ศ. ๒๕๑๑ รัฐมนตรีว่าการกระทรวงอุตสาหกรรมออกประกาศกำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรม หลักการและแนวทางการบริหารความเสี่ยง มาตรฐานเลขที่ มอก. 31000 - 2555 ไว้ ดังมีรายละเอียด ต่อท้ายประกาศนี้

ทั้งนี้ ให้มีผลตั้งแต่วันที่ประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๒๑ พฤษภาคม พ.ศ. ๒๕๕๕

หม่อมราชวงศ์พงษ์สวัสดิ์ สวัสดิวัตน์

รัฐมนตรีว่าการกระทรวงอุตสาหกรรม

มาตรฐานผลิตภัณฑ์อุตสาหกรรม

หลักการและแนวทางการบริหารความเสี่ยง

1. ขอบข่าย

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้กำหนดหลักการและแนวทางทั่วไปในการบริหารความเสี่ยง

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้สามารถนำไปใช้ได้กับองค์กรประเภทต่าง ๆ เช่น องค์กรภาครัฐ เอกชน วิชาชีพชุมชน สมาคม กลุ่ม หรือบุคคล ไม่เฉพาะเจาะจงว่าเป็นอุตสาหกรรมหรือภาคส่วนใด

หมายเหตุ เพื่อความสะดวกสำหรับผู้ใช้ที่แตกต่างกัน ซึ่งต่อไปในมาตรฐานนี้จะเรียกว่า “องค์กร”

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้สามารถประยุกต์ใช้ได้ตลอดช่วงการดำเนินการขององค์กร และครอบคลุมถึงกิจกรรมต่าง ๆ รวมถึงกลยุทธ์ การตัดสินใจ การดำเนินการหรือกิจการ กระบวนการทำงาน โครงการ ผลิตภัณฑ์ บริการ และสินทรัพย์

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้สามารถใช้ได้กับความเสี่ยงขององค์กรทุกประเภท ไม่ว่าความเสี่ยงขององค์กรแต่ละประเภทจะเป็นแบบใด ทั้งที่มีผลสืบเนื่องทางบวกหรือทางลบ

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้เป็นเพียงแนวทาง ไม่ได้มุ่งหวังให้เกิดการบริหารความเสี่ยงที่มีรูปแบบเหมือนกันทุกองค์กร ซึ่งการออกแบบและการนำไปใช้ของแผนและแนวทางการบริหารความเสี่ยงนั้น จะต้องนำไปใช้ให้เหมาะสมและเฉพาะเจาะจงกับองค์กรนั้น ๆ ตามวัตถุประสงค์ บริบท โครงสร้าง การดำเนินการ กระบวนการ หน้าที่งาน โครงการ ผลิตภัณฑ์ บริการ หรือสินทรัพย์ รวมถึงการปฏิบัติในเรื่องใดเรื่องหนึ่งที่ใช้

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้มีเจตนาเพื่อต้องการให้นำไปประยุกต์ใช้เพื่อให้ประสานเป็นส่วนหนึ่งของการบริหารความเสี่ยงที่ดำเนินการอยู่ในปัจจุบันหรือที่จะดำเนินการในอนาคต ไม่มีเจตนาให้นำไปทดแทนมาตรฐานเดิมที่องค์กรใช้อยู่

มาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ไม่มีจุดมุ่งหมายให้นำไปใช้เพื่อการรับรอง

2. บทนิยาม

ความหมายของคำที่ใช้ในมาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ มีดังต่อไปนี้

2.1 ความเสี่ยง (risk) หมายถึง ผลของความไม่แน่นอนต่อวัตถุประสงค์

หมายเหตุ 1 ผล หมายถึง การเบี่ยงเบนจากความคาดหวังทางบวกและ/หรือทางลบ

หมายเหตุ 2 วัตถุประสงค์สามารถมีได้หลายลักษณะ (เช่น เป้าประสงค์ด้านการเงิน สุขภาพและความปลอดภัย รวมถึงสิ่งแวดล้อม) และสามารถใช้ได้หลายระดับ (เช่น ระดับกลยุทธ์ ทั่วทั้งองค์กร โครงการ ผลิตภัณฑ์ และกระบวนการ)

หมายเหตุ 3 ความเสี่ยงโดยปกติจะเกิดจากเหตุการณ์และผลสืบเนื่องที่มีศักยภาพจะเกิดขึ้นหรือทั้งสองอย่างร่วมกัน

หมายเหตุ 4 ความเสี่ยงโดยปกติมักจะแสดงในรูปผลรวมของผลสืบเนื่องจากเหตุการณ์ (รวมถึงการเปลี่ยนแปลงของสภาพการณ์) และโอกาสเกิดของเหตุการณ์นั้น

หมายเหตุ 5 ความไม่แน่นอนเป็นสภาวะ (แม้บางส่วนของสภาวะ) ของการขาดของสารสนเทศที่เกี่ยวข้องกับความเข้าใจหรือความรู้เกี่ยวกับเหตุการณ์ ผลสืบเนื่องหรือโอกาสของการเกิดเหตุการณ์นั้น ๆ

2.2 การบริหารความเสี่ยง (risk management) หมายถึง การประสานกิจกรรมเพื่อจัดการและควบคุมองค์กรเกี่ยวกับความเสี่ยง

2.3 กรอบการบริหารความเสี่ยง (risk management framework) หมายถึง กลุ่มขององค์ประกอบที่ระบุรากฐานและการจัดการองค์กรสำหรับการออกแบบ การนำไปปฏิบัติ การติดตามตรวจสอบ การทบทวน และการปรับปรุงการบริหารความเสี่ยงอย่างต่อเนื่องทั่วทั้งองค์กร

หมายเหตุ 1 รากฐาน รวมถึงนโยบาย วัตถุประสงค์ การบังคับและความมุ่งมั่นในการบริหารความเสี่ยง

หมายเหตุ 2 การจัดการองค์กร รวมถึงแผน ความสัมพันธ์ การรับผิดชอบ ทรัพยากร การดำเนินการ และกิจกรรม

หมายเหตุ 3 กรอบการบริหารความเสี่ยงต้องสอดแทรกเข้าไปในกลยุทธ์และนโยบายการปฏิบัติการโดยรวมขององค์กร รวมถึงการปฏิบัติต่าง ๆ

2.4 นโยบายการบริหารความเสี่ยง (risk management policy) หมายถึง ประกาศที่แสดงถึงความตั้งใจและทิศทางโดยรวมขององค์กรที่เกี่ยวข้องกับการบริหารความเสี่ยง

2.5 ทักษคติเรื่องความเสี่ยง (risk attitude) หมายถึง วิธีการที่องค์กรประเมิน รวมถึงการจัดการ คงไว้ รับหรือปฏิเสธความเสี่ยง

2.6 แผนการบริหารความเสี่ยง (risk management plan) เป็นส่วนหนึ่งในกรอบการบริหารความเสี่ยงซึ่งระบุถึงวิธีการที่ใช้ องค์ประกอบในการบริหาร และทรัพยากรที่ใช้ในการบริหารความเสี่ยง

หมายเหตุ 1 องค์ประกอบในการบริหาร โดยทั่วไปรวมถึงขั้นตอนการดำเนินงาน การปฏิบัติ การมอบหมาย ความรับผิดชอบ ลำดับและระยะเวลาของกิจกรรมต่าง ๆ

หมายเหตุ 2 แผนการบริหารความเสี่ยง สามารถใช้ในส่วนของผลิตภัณฑ์ กระบวนการ และโครงการ รวมถึงเป็นส่วนหนึ่งขององค์กรทั้งหมด

- 2.7 ผู้รับผิดชอบความเสี่ยง (risk owner) หมายถึง บุคคลหรือนิติบุคคลที่มีภาระรับผิดชอบและมีอำนาจในการบริหารความเสี่ยง
- 2.8 กระบวนการบริหารความเสี่ยง (risk management process) หมายถึง การใช้นโยบายทางการบริหาร ขั้นตอนการดำเนินงาน และการปฏิบัติในกิจกรรมของการสื่อสาร การปรึกษา การจัดทำบริบท รวมถึงการชี้แจง การวิเคราะห์ การประเมินผล การแก้ไข การเฝ้าติดตามและการทบทวนความเสี่ยงอย่างเป็นระบบ
- 2.9 การจัดทำบริบท (establishing the context) หมายถึง การกำหนดปัจจัยทั้งภายในและภายนอกเพื่อนำไปสู่การบริหารความเสี่ยง รวมถึงกำหนดขอบเขตและเกณฑ์ความเสี่ยงสำหรับนโยบายการบริหารความเสี่ยง
- 2.10 บริบทภายนอก (external context) หมายถึง สภาพแวดล้อมภายนอกที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กร

หมายเหตุ บริบทภายนอก สามารถประกอบด้วย

- สังคม วัฒนธรรม การเมือง กฎหมาย ข้อบังคับ การเงิน เทคโนโลยี เศรษฐกิจ ลักษณะขององค์กรและสภาพการแข่งขันทางธุรกิจ ทั้งในระดับโลก ระดับชาติ ระดับภูมิภาค หรือระดับท้องถิ่น
- ตัวขับเคลื่อนที่สำคัญและแนวโน้มที่จะมีผลกระทบต่อวัตถุประสงค์ขององค์กร
- ความสัมพันธ์กับผู้มีส่วนได้เสียภายนอกองค์กร มุมมองของผู้มีส่วนได้เสียภายนอกองค์กร และคุณค่าขององค์กรที่มีต่อผู้มีส่วนได้เสียภายนอกองค์กร

- 2.11 บริบทภายใน (internal context) หมายถึง สภาพแวดล้อมภายในที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กร

หมายเหตุ บริบทภายใน สามารถประกอบด้วย

- การกำกับดูแล โครงสร้างองค์กร บทบาท และภาระรับผิดชอบ
- กลยุทธ์เพื่อให้บรรลุตามนโยบายและวัตถุประสงค์ที่กำหนดไว้
- ชีตความสามารถด้านทรัพยากรและความรู้ (เช่น เงินทุน เวลา คน การดำเนินการ ระบบ และเทคโนโลยี)
- ระบบสารสนเทศ การรับส่งสารสนเทศ และการดำเนินการตัดสินใจ (ทั้งเป็นทางการและไม่เป็นทางการ)
- ความสัมพันธ์กับผู้มีส่วนได้เสียภายในองค์กร มุมมองของผู้มีส่วนได้เสียภายในองค์กร และคุณค่าขององค์กรที่มีต่อผู้มีส่วนได้เสียภายในองค์กร
- วัฒนธรรมองค์กร

- มาตรฐาน แนวทาง และรูปแบบการดำเนินการต่าง ๆ ที่รับมาใช้ในองค์กร
- ระเบียบแบบแผนและความผูกพันทางพันธสัญญา

2.12 การสื่อสารและการปรึกษา (communication and consultation) หมายถึง การดำเนินการที่องค์กรดำเนินการต่อเนื่องและทำซ้ำ เพื่อให้แบ่งหรือรับสารสนเทศ รวมถึงการมีส่วนร่วมกับผู้มีส่วนได้เสียเพื่อการบริหารความเสี่ยง

หมายเหตุ 1 สารสนเทศสามารถเกี่ยวข้องกับการมีอยู่ ลักษณะขององค์กร ระเบียบแบบแผน โอกาสความมีนัยสำคัญ การเปรียบเทียบกับเกณฑ์ การยอมรับ และการแก้ไข เพื่อการบริหารความเสี่ยง

หมายเหตุ 2 การปรึกษาเป็นกระบวนการสื่อสารสองทาง ระหว่างองค์กรและผู้มีส่วนได้เสียเกี่ยวกับประเด็นก่อนตัดสินใจหรือกำหนดทิศทางของประเด็นนั้น ๆ การปรึกษา คือ

- กระบวนการซึ่งกระทบต่อการตัดสินใจ ด้วยวิธีการมุ่งใจมากกว่าการใช้อำนาจ
- การให้ข้อมูลเพื่อการตัดสินใจ ไม่ใช่การตัดสินใจร่วม

2.13 ผู้มีส่วนได้เสีย (stakeholder) หมายถึง บุคคลหรือองค์กรที่สามารถมีผลหรือได้รับผล หรือรับรู้ว่าพวกเขาได้รับผลจากการตัดสินใจหรือกิจกรรมขององค์กร

หมายเหตุ ผู้ตัดสินใจสามารถเป็นผู้มีส่วนได้เสีย

2.14 การประเมินความเสี่ยง (risk assessment) หมายถึง กระบวนการโดยรวมเกี่ยวกับการชี้บ่งความเสี่ยง การวิเคราะห์ความเสี่ยง และการประเมินผลความเสี่ยง

2.15 การชี้บ่งความเสี่ยง (risk identification) หมายถึง กระบวนการในการค้นหา การรับรู้ และการอธิบายความเสี่ยง

หมายเหตุ 1 การชี้บ่งความเสี่ยง เกี่ยวข้องกับการชี้บ่งแหล่งความเสี่ยง เหตุการณ์ สาเหตุและผลสืบเนื่องที่เป็นไปได้

หมายเหตุ 2 การชี้บ่งความเสี่ยง สามารถเกี่ยวข้องกับข้อมูลในอดีต ทฤษฎีการวิเคราะห์ ข้อมูลและความเห็นผู้เชี่ยวชาญ และความจำเป็นของผู้มีส่วนได้เสีย

2.16 แหล่งความเสี่ยง (risk source) หมายถึง องค์ประกอบโดยลำพังหรือต้องรวมกับสิ่งอื่นที่มีศักยภาพในการเป็นต้นเหตุทำให้เกิดความเสี่ยง

หมายเหตุ แหล่งความเสี่ยงสามารถเห็นได้ชัดเจนหรือเห็นไม่ชัดเจน

2.17 เหตุการณ์ (event) หมายถึง การเกิด หรือการเปลี่ยนแปลงของส่วนหนึ่งส่วนใดของสภาพการณ์

หมายเหตุ 1 เหตุการณ์สามารถเป็นหนึ่งหรือหลายสภาพการณ์ และสามารถมีได้หลายสาเหตุ

หมายเหตุ 2 เหตุการณ์สามารถประกอบด้วยบางสิ่งที่ไม่ได้เกิดขึ้น

หมายเหตุ 3 เหตุการณ์บางครั้งสามารถอ้างอิงถึงอุบัติการณ์หรืออุบัติเหตุ

หมายเหตุ 4 เหตุการณ์ที่ปราศจากผลสืบเนื่องสามารถอ้างอิงถึงเหตุการณ์เกือบเกิดอุบัติเหตุหรืออุบัติเหตุ

2.18 ผลสืบเนื่อง (consequence) หมายถึง ผลของเหตุการณ์ที่ส่งผลกระทบต่อวัตถุประสงค์

หมายเหตุ 1 เหตุการณ์ที่สามารถนำไปสู่ลำดับของผลสืบเนื่อง

หมายเหตุ 2 ผลสืบเนื่องสามารถแน่นอนหรือไม่แน่นอน และสามารถมีผลในทางบวกหรือทางลบต่อวัตถุประสงค์

หมายเหตุ 3 ผลสืบเนื่องสามารถแสดงออกในเชิงคุณภาพหรือเชิงปริมาณ

หมายเหตุ 4 จุดเริ่มต้นของผลสืบเนื่องสามารถขยายไปจนถึงจุดที่ได้รับผล

2.19 โอกาส (likelihood) หมายถึง การเปลี่ยนแปลงของบางสิ่งที่เกิดขึ้น

2.20 ลักษณะความเสี่ยง (risk profile) หมายถึง คำอธิบายกลุ่มของความเสี่ยง

หมายเหตุ กลุ่มของความเสี่ยงสามารถประกอบด้วยความเสี่ยงที่เกี่ยวกับทั้งองค์กร บางส่วนขององค์กร หรือตามที่กำหนดอื่น ๆ

2.21 การวิเคราะห์ความเสี่ยง (risk analysis) หมายถึง กระบวนการเข้าใจธรรมชาติของความเสี่ยงและกำหนดระดับความเสี่ยง

หมายเหตุ 1 การวิเคราะห์ความเสี่ยงให้พื้นฐานของการประเมินผลความเสี่ยงและการตัดสินใจเกี่ยวกับการจัดการความเสี่ยง

หมายเหตุ 2 การวิเคราะห์ความเสี่ยง รวมถึงการประมาณความเสี่ยง

2.22 เกณฑ์ความเสี่ยง (risk criteria) หมายถึง เงื่อนไขของการอ้างอิงเพื่อใช้ประเมินเทียบหาความเสี่ยงที่มีนัยสำคัญ

หมายเหตุ 1 เกณฑ์ความเสี่ยงอยู่บนพื้นฐานของวัตถุประสงค์ บริบทภายนอกและบริบทภายในขององค์กร

หมายเหตุ 2 เกณฑ์ความเสี่ยงสามารถกำหนดโดยหรือได้รับจากมาตรฐาน กฎหมาย นโยบาย และข้อกำหนดอื่น ๆ

2.23 ระดับความเสี่ยง (level of risk) หมายถึง ขนาดของความเสี่ยงหรือผลรวมของความเสี่ยง ซึ่งแสดงออกในรูปของผลรวมระหว่างผลสืบเนื่องและโอกาส

2.24 การประเมินผลความเสี่ยง (risk evaluation) หมายถึง การประเมินผลความเสี่ยงเพื่อตัดสินใจว่าขนาดของความเสี่ยงยอมรับได้หรือทนทานได้หรือไม่

หมายเหตุ การประเมินผลความเสี่ยง ช่วยในการตัดสินใจเกี่ยวกับการจัดการความเสี่ยง

2.25 การจัดการความเสี่ยง (risk treatment) หมายถึง กระบวนการในการเปลี่ยนแปลงความเสี่ยง

หมายเหตุ 1 การจัดการความเสี่ยง สามารถเกี่ยวข้องกับ

- การหลีกเลี่ยงความเสี่ยง โดยการไม่เริ่มหรือดำเนินการต่อในกิจกรรมที่ก่อให้เกิดความเสี่ยง
- การรับความเสี่ยงหรือเพิ่มความเสี่ยงเพื่อหาโอกาสทางธุรกิจ
- การจัดแหล่งความเสี่ยงออกไป
- การเปลี่ยนโอกาส
- การเปลี่ยนผลสืบเนื่อง
- การแบ่งความเสี่ยงกับหน่วยงานอื่น (รวมถึงสัญญาหรือความเสี่ยงทางการเงิน)
- การรับความเสี่ยงไว้โดยแจ้งให้ผู้ตัดสินใจทราบ

หมายเหตุ 2 การจัดการความเสี่ยงใช้ในกรณีที่มีผลสืบเนื่องเชิงลบ ซึ่งบางครั้งอ้างอิงถึง การลดความเสี่ยง การจัดการความเสี่ยง การป้องกันความเสี่ยง และการลดความเสี่ยง

หมายเหตุ 3 การจัดการความเสี่ยงสามารถสร้างความเสี่ยงใหม่หรือเปลี่ยนแปลงความเสี่ยงเดิม

2.26 การควบคุม (control) หมายถึง มาตรการที่เปลี่ยนแปลงความเสี่ยง

หมายเหตุ 1 การควบคุม รวมถึงกระบวนการ นโยบาย เครื่องมือ การปฏิบัติ หรือการกระทำใด ๆ ที่เปลี่ยนแปลงความเสี่ยง

หมายเหตุ 2 การควบคุม อาจไม่ใช่ผลการเปลี่ยนแปลงที่ได้จากเจตนาหรือการถือครอง

2.27 ความเสี่ยงที่ยังเหลืออยู่ (residual risk) หมายถึง ความเสี่ยงที่ยังคงเหลืออยู่ในองค์กรหลังจากการจัดการความเสี่ยงไปแล้ว

หมายเหตุ 1 ความเสี่ยงที่ยังเหลืออยู่สามารถรวมถึงความเสี่ยงที่ยังไม่ได้ชี้บ่ง

หมายเหตุ 2 ความเสี่ยงที่ยังเหลืออยู่สามารถเป็นความเสี่ยงที่เราคงไว้ได้

2.28 การติดตามตรวจสอบ (monitoring) หมายถึง การตรวจสอบอย่างต่อเนื่อง การควบคุมดูแล การสังเกตที่สำคัญ หรือตัดสินใจสถานะเพื่อชี้บ่งการเปลี่ยนแปลงจากระดับผลการดำเนินงานที่ต้องการหรือคาดหวัง

หมายเหตุ การติดตามตรวจสอบ สามารถใช้ได้กับกรอบการบริหารความเสี่ยง กระบวนการบริหารความเสี่ยง ความเสี่ยง หรือการควบคุม

2.29 การทบทวน (review) หมายถึง กิจกรรมที่ทำไปเพื่อตัดสินความเหมาะสม ความพอเพียง และประสิทธิผลเพื่อการบรรลุวัตถุประสงค์ที่กำหนดไว้

หมายเหตุ การทบทวนสามารถใช้ได้กับกรอบการบริหารความเสี่ยง กระบวนการบริหารความเสี่ยง ความเสี่ยง หรือการควบคุม

3. หลักการ

เพื่อให้การบริหารความเสี่ยงมีประสิทธิภาพ ทุกระดับขององค์กรควรดำเนินการให้เป็นไปตามหลักการต่าง ๆ ดังต่อไปนี้

3.1 การบริหารความเสี่ยงช่วยสร้างและปกป้องคุณค่าขององค์กร

การบริหารความเสี่ยงมีส่วนช่วยในการทำให้บรรลุวัตถุประสงค์และผลปรับปรุงการดำเนินงาน เช่น สุขภาพและความปลอดภัยของมนุษย์ การรักษาความปลอดภัย การปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ การยอมรับของสาธารณชน การปกป้องสิ่งแวดล้อม คุณภาพของผลิตภัณฑ์ การบริหารโครงการ ประสิทธิภาพในการดำเนินการ การกำกับดูแลและชื่อเสียงขององค์กร

3.2 การบริหารความเสี่ยง เป็นส่วนหนึ่งของกระบวนการดำเนินการทั้งหมดขององค์กร

การบริหารความเสี่ยงไม่ใช่กิจกรรมที่แยกออกมาทำโดยลำพังจากกิจกรรมและกระบวนการหลักขององค์กร ถือเป็นส่วนหนึ่งในความรับผิดชอบของผู้บริหารและกระบวนการดำเนินการทั้งหมดขององค์กร รวมไปถึงการวางแผนกลยุทธ์ การบริหารโครงการ และการบริหารการเปลี่ยนแปลงทั้งหมด

3.3 การบริหารความเสี่ยงเป็นส่วนหนึ่งของการตัดสินใจ

การบริหารความเสี่ยงช่วยทำให้ผู้ตัดสินใจดำเนินการสร้างทางเลือกอย่างชัดเจน (informed choices) และสามารถจัดลำดับความสำคัญในการดำเนินการ และทำให้เห็นความแตกต่างของแนวทางการดำเนินการ

3.4 การบริหารความเสี่ยงใช้ในการจัดการกับความไม่แน่นอน

การบริหารความเสี่ยงใช้จัดการกับความไม่แน่นอนที่อาจเกิดขึ้น ซึ่งต้องคำนึงถึงลักษณะเฉพาะเจาะจงของความไม่แน่นอน และวิธีการจัดการ

3.5 การบริหารความเสี่ยงเป็นระบบ มีรูปแบบที่ชัดเจน และทันต่อสถานการณ์

แนวทางการบริหารความเสี่ยงอย่างเป็นระบบ ทันต่อสถานการณ์ และมีรูปแบบ มีส่วนสนับสนุนให้เกิดผลลัพธ์ที่มีประสิทธิภาพ มีความสม่ำเสมอ สามารถเปรียบเทียบ และเชื่อถือได้

3.6 การบริหารความเสี่ยงควรอยู่บนพื้นฐานสารสนเทศที่ดีที่สุดที่สามารถหาได้

ปัจจัยนำเข้า (inputs) สำหรับกระบวนการบริหารความเสี่ยงอยู่บนพื้นฐานของแหล่งสารสนเทศ เช่น ข้อมูลในอดีต ประสบการณ์ ข้อมูลป้อนกลับจากผู้มีส่วนได้เสีย การสังเกต การพยากรณ์และการวินิจฉัยของผู้เชี่ยวชาญ อย่างไรก็ตามผู้ตัดสินใจจะต้องรับทราบและคำนึงถึงข้อจำกัดของข้อมูลหรือแบบจำลองที่ใช้ หรือโอกาสที่ผู้เชี่ยวชาญจะมีความเห็นที่แตกต่างกันได้

3.7 การบริหารความเสี่ยงควรทำให้เหมาะสมกับองค์กร

การบริหารความเสี่ยง ควรทำให้เหมาะสมกับองค์กร โดยสอดคล้องกับบริบทภายในและบริบทภายนอกขององค์กรและลักษณะความเสี่ยง

3.8 การบริหารความเสี่ยงควรคำนึงถึงปัจจัยด้านบุคคลและวัฒนธรรม

การบริหารความเสี่ยงตระหนักถึงขีดความสามารถ การรับรู้ และความตั้งใจของคนทั้งภายในและภายนอกองค์กรซึ่งสามารถช่วยหรือเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ขององค์กร

3.9 การบริหารความเสี่ยงควรมีความโปร่งใสและมีส่วนร่วม

การมีส่วนร่วมอย่างเหมาะสมและทันต่อสถานการณ์ของผู้มีส่วนได้เสียและผู้ตัดสินใจในระดับต่าง ๆ ขององค์กร จะช่วยสร้างความมั่นใจว่าการบริหารความเสี่ยงยังมีความสอดคล้องและทันสมัย รวมถึงการให้ผู้มีส่วนได้เสียเป็นตัวแทนในการให้ความเห็นในการกำหนดเกณฑ์ความเสี่ยง

3.10 การบริหารความเสี่ยงควรมีการดำเนินการอย่างต่อเนื่อง ทำซ้ำและตอบสนองต่อการเปลี่ยนแปลง

การบริหารความเสี่ยงควรรับรู้และตอบสนองต่อการเปลี่ยนแปลงอย่างต่อเนื่อง การเปลี่ยนแปลงของบริบทภายในและบริบทภายนอกรวมถึงองค์ความรู้ใหม่ ควรมีการเฝ้าติดตามและการทบทวนความเสี่ยงที่เกิดขึ้นเพื่อค้นหาความเสี่ยงที่ปรากฏขึ้นใหม่ ความเสี่ยงที่เปลี่ยนแปลงไป และความเสี่ยงที่ไม่ปรากฏ

3.11 การบริหารความเสี่ยงช่วยให้องค์กรเกิดการปรับปรุงอย่างต่อเนื่อง

องค์กรควรพัฒนาและนำกลยุทธ์ไปปฏิบัติในการปรับปรุงการบริหารความเสี่ยงให้สมบูรณ์ควบคู่ไปกับประเด็นปัญหาอื่น ๆ ขององค์กร

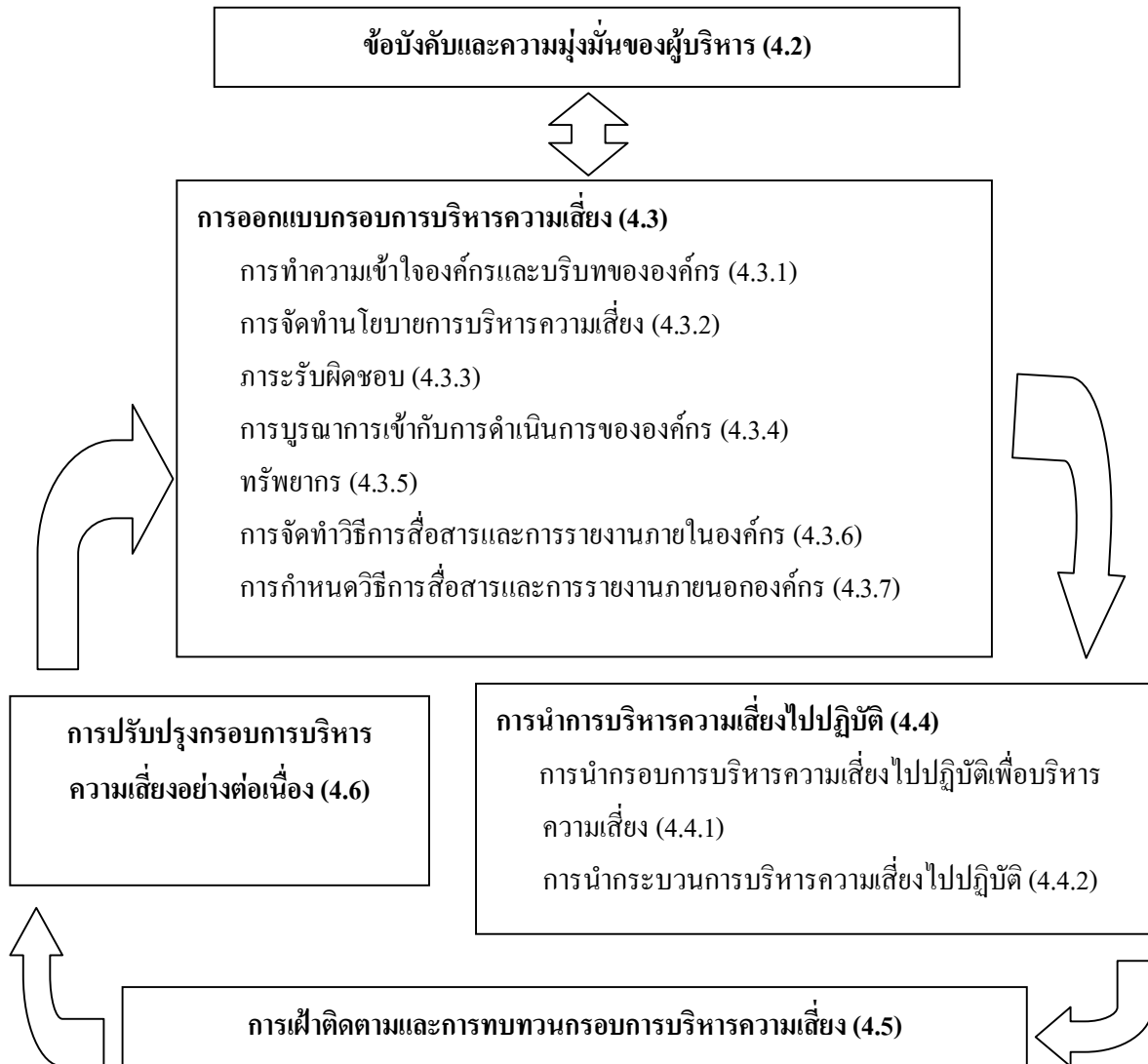
ภาคผนวก ได้ให้คำแนะนำเพิ่มเติมเพื่อให้องค์กรบริหารความเสี่ยงได้อย่างมีประสิทธิภาพมากขึ้น

4. กรอบงาน

4.1 ทั่วไป

การบริหารความเสี่ยงที่ประสบความสำเร็จจะขึ้นอยู่กับการกำหนดกรอบการบริหารความเสี่ยงที่มีประสิทธิภาพซึ่งช่วยก่อให้เกิดรากฐานและการจัดการที่จะปลูกฝังเรื่องการบริหารความเสี่ยงเข้าไปในทุกระดับขององค์กร กรอบการบริหารความเสี่ยงจะช่วยบริหารความเสี่ยงอย่างมีประสิทธิภาพโดยการใช้กระบวนการบริหารความเสี่ยงในระดับต่าง ๆ และภายในบริบทเฉพาะขององค์กร กรอบการบริหารความเสี่ยงทำให้มั่นใจว่า ข้อมูลเกี่ยวกับความเสี่ยงที่ได้จากกระบวนการเหล่านี้ มีการรายงานอย่างครบถ้วน และใช้เป็นพื้นฐานในการตัดสินใจและแสดงการรับผิดชอบในทุกระดับที่เกี่ยวข้องขององค์กร

หลักการและแนวทางนี้อธิบายถึงองค์ประกอบที่จำเป็นของกรอบการบริหารความเสี่ยง และรูปแบบของความสัมพันธ์เป็นวงจร ดังรูปที่ 2



รูปที่ 2 ความสัมพันธ์ระหว่างองค์ประกอบต่างๆ ของกรอบการบริหารความเสี่ยง
เพื่อการบริหารความเสี่ยง

กรอบการบริหารความเสี่ยงนี้มีเจตนาต้องการให้นำไปประยุกต์ใช้เพื่อให้ประสานเป็นส่วนหนึ่งของกระบวนการจัดการโดยรวมขององค์กร ดังนั้น องค์กรควรปรับองค์ประกอบของกรอบการบริหารความเสี่ยงให้มีความเหมาะสมกับความเสี่ยงขององค์กร

หากองค์กรมีระบบการบริหารความเสี่ยงซึ่งได้มีกระบวนการบริหารความเสี่ยงและการปฏิบัติ โดยได้รวมองค์ประกอบของการบริหารความเสี่ยงไว้แล้วหรือองค์กรได้มีการนำกระบวนการบริหารความเสี่ยงไปปฏิบัติ

ในบางความเสี่ยงหรือบางสถานะอยู่แล้วควรมีการทบทวนและประเมิน โดยเปรียบเทียบกับมาตรฐานนี้อย่างจริงจังเพื่อพิจารณาความครบถ้วนและประสิทธิผลของระบบดังกล่าว

4.2 ข้อบังคับและความมุ่งมั่นของผู้บริหาร

ในการนำระบบการบริหารความเสี่ยงไปใช้ในองค์กรอย่างมีประสิทธิภาพ ต้องมีความมุ่งมั่นอย่างแรงกล้าและยั่งยืนจากผู้บริหาร รวมทั้งมีกลยุทธ์และการวางแผนอย่างรอบคอบและรัดกุม เพื่อให้พนักงานทุกระดับเกิดความมุ่งมั่นร่วมกัน

ข้อบังคับที่ผู้บริหารพึงปฏิบัติ

- กำหนดและประกาศนโยบายการบริหารความเสี่ยง
- มั่นใจว่าวัฒนธรรมองค์กรสอดคล้องกับนโยบายการบริหารความเสี่ยง
- กำหนดตัวชี้วัดผลการบริหารความเสี่ยงที่สอดคล้องกับตัวชี้วัดผลการดำเนินการขององค์กร
- กำหนดวัตถุประสงค์การบริหารความเสี่ยงให้สอดคล้องกับวัตถุประสงค์และกลยุทธ์ขององค์กร
- มั่นใจว่าการดำเนินการขององค์กรสอดคล้องกับกฎหมายและข้อบังคับ
- มอบหมายการรับผิดชอบและความรับผิดชอบในระดับที่เหมาะสมภายในองค์กร
- มั่นใจว่ามีการสนับสนุนทรัพยากรที่จำเป็นในการบริหารความเสี่ยง
- สื่อสารถึงประโยชน์ที่ได้จากการบริหารความเสี่ยงไปยังผู้มีส่วนได้เสียทั้งหมดทราบ
- มั่นใจว่ากรอบการบริหารความเสี่ยงมีความเหมาะสมอย่างต่อเนื่อง

4.3 การกำหนดกรอบการบริหารความเสี่ยง

4.3.1 การทำความเข้าใจองค์กรและบริบทขององค์กร

ก่อนเริ่มกำหนดและนำกรอบการบริหารความเสี่ยงไปสู่การปฏิบัติต้องมีการประเมินและทำความเข้าใจบริบทภายนอกและบริบทภายในขององค์กร เพราะสิ่งต่าง ๆ เหล่านี้มีผลอย่างมีนัยสำคัญต่อการกำหนดกรอบการบริหารความเสี่ยง

การประเมินบริบทภายนอกขององค์กร อาจรวมถึงประเด็นต่าง ๆ ดังต่อไปนี้

- (ก) สังคม วัฒนธรรม การเมือง กฎหมาย ข้อบังคับ การเงิน เทคโนโลยี เศรษฐกิจ ลักษณะขององค์กรและสภาพการแข่งขันทางธุรกิจ ทั้งในระดับโลก ระดับชาติ ระดับภูมิภาค หรือระดับท้องถิ่น
- (ข) ตัวขับเคลื่อนที่สำคัญและแนวโน้มที่จะมีผลกระทบต่อวัตถุประสงค์ขององค์กร
- (ค) ความสัมพันธ์กับผู้มีส่วนได้เสียภายนอกองค์กร มุมมองของผู้มีส่วนได้เสียภายนอกองค์กร และคุณค่าขององค์กรที่มีต่อผู้มีส่วนได้เสียภายนอกองค์กร

การประเมินบริบทภายในองค์กรอาจรวมถึงประเด็นต่าง ๆ ดังต่อไปนี้

- การกำกับดูแล โครงสร้างองค์กร บทบาท และภาระรับผิดชอบ
- กลยุทธ์เพื่อให้บรรลุตามนโยบายและวัตถุประสงค์ที่กำหนดไว้
- จิตความสามารถด้านทรัพยากรและความรู้ (เช่น เงินทุน เวลา คน การดำเนินการ ระบบ และ เทคโนโลยี)
- ระบบสารสนเทศ การรับส่งสารสนเทศ และกระบวนการตัดสินใจ (ทั้งเป็นทางการและไม่เป็นทางการ)
- ความสัมพันธ์กับผู้มีส่วนได้เสียภายในองค์กร มุมมองของผู้มีส่วนได้เสียภายในองค์กร และคุณค่าขององค์กรที่มีต่อผู้มีส่วนได้เสียภายในองค์กร
- วัฒนธรรมองค์กร
- มาตรฐาน แนวทาง และรูปแบบการดำเนินการต่าง ๆ ที่รับมาใช้ในองค์กร
- ระเบียบแบบแผนและความผูกพันทางพันธะสัญญา

4.3.2 การจัดทำนโยบายการบริหารความเสี่ยง

นโยบายการบริหารความเสี่ยงควรกล่าวถึงวัตถุประสงค์และความมุ่งมั่นขององค์กรในการบริหารความเสี่ยงอย่างชัดเจน โดยทั่วไปแล้วควรกล่าวถึงสิ่งต่อไปนี้

- เหตุผลในการบริหารความเสี่ยงขององค์กร
- ความเชื่อมโยงระหว่างวัตถุประสงค์และนโยบายขององค์กร กับนโยบายการบริหารความเสี่ยง
- ภาระรับผิดชอบและความรับผิดชอบในการบริหารความเสี่ยง
- แนวทางและการดำเนินการเมื่อเกิดการขัดแย้งผลประโยชน์
- ความมุ่งมั่นในการสนับสนุนทรัพยากรที่มีอยู่ เพื่อช่วยผู้ที่มีภาระรับผิดชอบและความรับผิดชอบในการบริหารความเสี่ยง
- แนวทางและวิธีการในการวัดผลและรายงานผลการบริหารความเสี่ยง
- ความมุ่งมั่นในการทบทวนปรับปรุงนโยบายและกรอบการบริหารความเสี่ยงตามช่วงเวลาที่กำหนด และเมื่อมีเหตุการณ์หรือสภาพการณ์ที่เปลี่ยนแปลง

นโยบายการบริหารความเสี่ยงควรสื่อสารอย่างเหมาะสม

4.3.3 ภาระรับผิดชอบ

องค์กรควรมั่นใจว่า มีการกำหนดภาระรับผิดชอบ อำนาจหน้าที่ และความสามารถที่เหมาะสมในการบริหารความเสี่ยง รวมทั้งการนำไปปฏิบัติและการคงไว้ซึ่งกระบวนการบริหารความเสี่ยง และมั่นใจใน

ความเสี่ยงพอ ความมีประสิทธิภาพและความมีประสิทธิภาพของการควบคุมต่าง ๆ ซึ่งสามารถดำเนินการโดย

- ระบุผู้รับผิดชอบความเสี่ยงที่มีการรับผิดชอบและอำนาจหน้าที่ในการบริหารความเสี่ยง
- ระบุผู้ที่มีการรับผิดชอบในการจัดทำ การพัฒนา การนำไปปฏิบัติและการคงไว้ซึ่งกรอบการบริหารความเสี่ยง
- ระบุความรับผิดชอบในกระบวนการบริหารความเสี่ยงของทุกระดับในองค์กร
- จัดทำการวัดผลการดำเนินงาน การรายงานทั้งภายในและ/หรือภายนอก และการยกระดับการดำเนินการ
- มั่นใจว่ามีการยอมรับถึงภาระรับผิดชอบในระดับที่เหมาะสม

4.3.4 การบูรณาการเข้ากับกระบวนการขององค์กร

การบริหารความเสี่ยงควรสอดแทรกเข้าไปในการปฏิบัติและกระบวนการทั่วทั้งองค์กรในช่องทางที่เกี่ยวข้องอย่างมีประสิทธิภาพและประสิทธิผลกระบวนการบริหารความเสี่ยงควรเป็นส่วนหนึ่งของกระบวนการทำงานขององค์กร โดยเฉพาะการบริหารความเสี่ยงควรนำไปใช้ในการพัฒนานโยบาย การทบทวนและการวางแผนธุรกิจและแผนกลยุทธ์ และกระบวนการบริหารการเปลี่ยนแปลง

องค์กรควรมีแผนบริหารความเสี่ยงครอบคลุมทั่วทั้งองค์กรเพื่อให้มั่นใจว่ามีการปฏิบัติตามนโยบายการบริหารความเสี่ยง แผนการบริหารความเสี่ยงสามารถบูรณาการเข้าไปในแผนอื่นขององค์กร เช่น แผนกลยุทธ์

4.3.5 ทรัพยากร

องค์กรควรจัดสรรทรัพยากรที่เหมาะสมสำหรับการบริหารความเสี่ยง ควรพิจารณาเรื่องต่าง ๆ ดังต่อไปนี้

- บุคลากร ทักษะ ประสบการณ์ และความสามารถ
- ทรัพยากรที่จำเป็นสำหรับแต่ละขั้นตอนของกระบวนการบริหารความเสี่ยงในแต่ละกระบวนการ
- กระบวนการขององค์กร วิธีการและเครื่องมือที่ใช้ในการบริหารความเสี่ยง
- กระบวนการด้านเอกสารและขั้นตอนการดำเนินงานที่เป็นลายลักษณ์อักษร
- สารสนเทศและระบบการจัดการความรู้
- โปรแกรมการฝึกอบรม

4.3.6 การจัดทำกลไกการสื่อสารและการรายงานภายในองค์กร

องค์กรควรจัดทำกลไกและการรายงานภายในองค์กร เพื่อสนับสนุนและส่งเสริมให้เกิดการรับผิดชอบ และความเป็นผู้รับผิดชอบความเสี่ยง กลไกเหล่านี้ควรมั่นใจว่า

- องค์ประกอบหลักของกรอบการบริหารความเสี่ยง และการเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นภายหลังได้มีการนำไปสื่อสารอย่างเหมาะสม
- มีการรายงานประสิทธิผลและผลลัพธ์ของกรอบการบริหารความเสี่ยงภายในองค์กรอย่างเพียงพอ
- สารสนเทศที่ได้จากการบริหารความเสี่ยงขององค์กร เข้าถึงง่ายและพร้อมใช้งานในระดับและเวลาที่เหมาะสม
- มีกระบวนการปรึกษากับผู้มีส่วนได้เสียภายในองค์กร

กลไกเหล่านี้ควรรวมถึงกระบวนการรวบรวมสารสนเทศของความเสี่ยงจากหลาย ๆ แหล่งตามความเหมาะสม และมีความจำเป็นต้องคำนึงถึงความอ่อนไหวของสารสนเทศ

4.3.7 การจัดทำกลไกการสื่อสารและการรายงานภายนอกองค์กร

องค์กรควรพัฒนาและดำเนินการตามแผนการสื่อสารกับผู้มีส่วนได้เสียภายนอกองค์กรที่เกี่ยวข้องกับ

- การมีส่วนร่วมกับผู้มีส่วนได้เสียภายนอกที่เกี่ยวข้องอย่างเหมาะสมและมั่นใจว่ามีการแลกเปลี่ยนข้อมูลอย่างมีประสิทธิภาพ
- การรายงานสู่ภายนอกที่สอดคล้องกับข้อบังคับและข้อกำหนดของทางราชการ
- การตอบกลับและการรายงานเรื่องการสื่อสารและการปรึกษา
- การใช้การสื่อสารเพื่อสร้างความเชื่อมั่นต่อองค์กร
- การสื่อสารกับผู้มีส่วนได้เสียกรณีเกิดภาวะวิกฤติหรือสถานการณ์ที่ไม่ปกติ

กลไกเหล่านี้ควรรวมถึงกระบวนการรวบรวมสารสนเทศของความเสี่ยงจากหลาย ๆ แหล่งตามความเหมาะสม และมีความจำเป็นต้องคำนึงถึงความอ่อนไหวของสารสนเทศ

4.4 การนำการบริหารความเสี่ยงไปปฏิบัติ

4.4.1 การนำกรอบการบริหารความเสี่ยงไปปฏิบัติ

ในการนำกรอบการบริหารความเสี่ยงไปปฏิบัติ องค์กรควร

- กำหนดเวลาและกลยุทธ์ที่เหมาะสมสำหรับการนำกรอบการบริหารความเสี่ยงไปปฏิบัติ
- ประยุกต์นโยบายและกระบวนการบริหารความเสี่ยงเข้ากับกระบวนการขององค์กร
- ปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้อง
- มั่นใจว่าการตัดสินใจรวมถึงการพัฒนาและการกำหนดวัตถุประสงค์มีความสอดคล้องกับผลลัพธ์จากกระบวนการบริหารความเสี่ยง
- จัดให้มีสารสนเทศและการฝึกอบรม
- สื่อสารและปรึกษากับผู้มีส่วนได้เสียเพื่อให้มั่นใจว่ากรอบการบริหารความเสี่ยงยังคงเหมาะสม

4.4.2 การนำกระบวนการบริหารความเสี่ยงไปปฏิบัติ

การบริหารความเสี่ยงควรนำไปปฏิบัติโดยให้มั่นใจว่ากระบวนการบริหารความเสี่ยงที่กำหนดไว้ในข้อ 5. ได้นำไปประยุกต์ใช้โดยผ่านแผนการบริหารความเสี่ยงไปใช้ในทุกงานและหน้าที่ที่เกี่ยวข้องในทุกระดับขององค์กรเสมือนเป็นส่วนหนึ่งของการปฏิบัติและกระบวนการขององค์กร

4.5 การเฝ้าติดตามและการทบทวนกรอบการบริหารความเสี่ยง

เพื่อให้มั่นใจว่าการบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพและสนับสนุนผลการดำเนินงานขององค์กรอย่างต่อเนื่อง องค์กรควร

- วัดผลการดำเนินการบริหารความเสี่ยงเทียบกับตัวชี้วัด ซึ่งมีการทบทวนตามช่วงเวลาที่กำหนดอย่างเหมาะสม
- วัดความก้าวหน้าและความเบี่ยงเบนในการดำเนินการเทียบกับแผนการบริหารความเสี่ยงตามช่วงเวลาที่กำหนด
- ทบทวนตามช่วงเวลาที่กำหนดว่ากรอบการบริหารความเสี่ยง นโยบาย และแผนการบริหารความเสี่ยงยังคงมีความเหมาะสมและสอดคล้องกับบริบททั้งภายในและภายนอกขององค์กร
- รายงานความเสี่ยง ความก้าวหน้าของแผนการบริหารความเสี่ยง และการปฏิบัติตามนโยบายการบริหารความเสี่ยงยังดำเนินการได้ดีด้วยดี
- ทบทวนประสิทธิผลของกรอบการบริหารความเสี่ยง

4.6 การปรับปรุงกรอบการบริหารความเสี่ยงอย่างต่อเนื่อง

สืบเนื่องจากผลของการเฝ้าติดตามและการทบทวน ควรมีการตัดสินใจในการปรับปรุงกรอบการบริหารความเสี่ยง นโยบาย และแผนการบริหารความเสี่ยง ซึ่งการตัดสินใจนี้ควรนำไปสู่การปรับปรุงการบริหารความเสี่ยง และวัฒนธรรมการบริหารความเสี่ยงขององค์กร

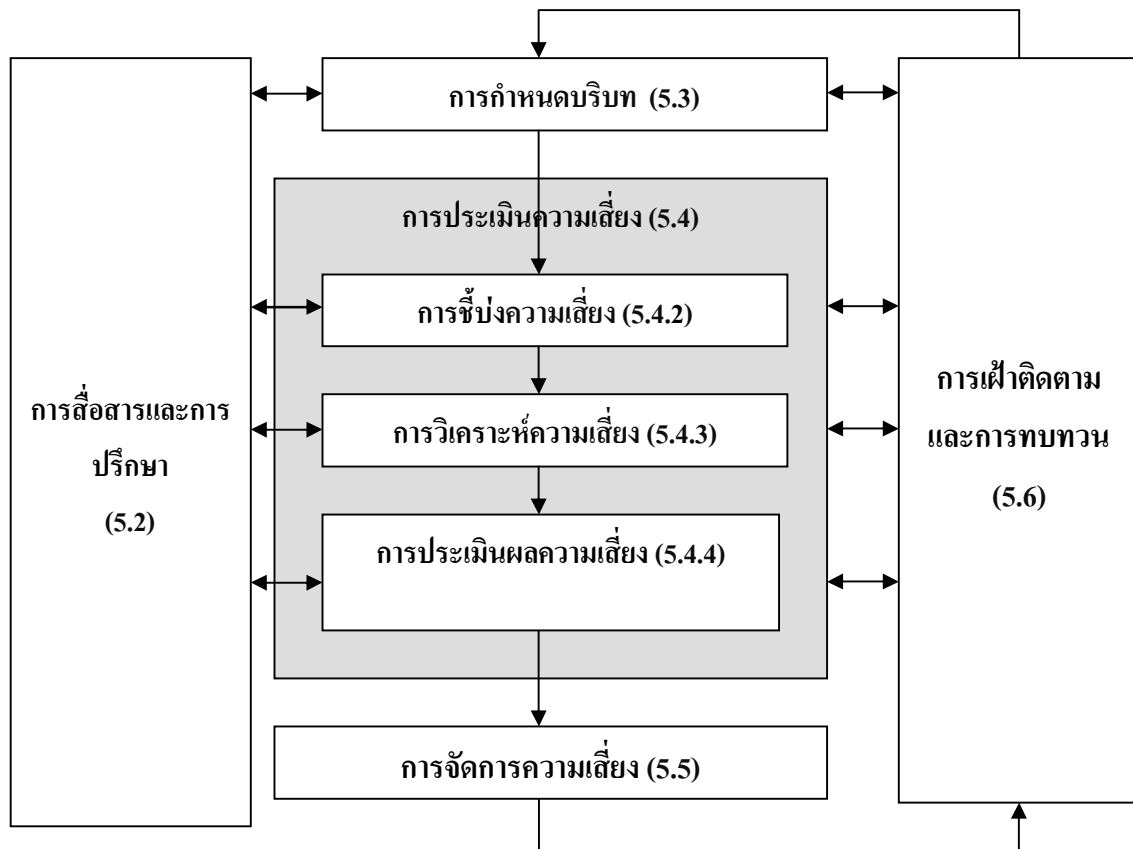
5. กระบวนการ

5.1 ทั่วไป

กระบวนการบริหารความเสี่ยงควร

- เป็นส่วนหนึ่งของการบริหาร
- ปลูกฝังอยู่ในวัฒนธรรมและการปฏิบัติ
- ปรับให้เหมาะสมกับการดำเนินการทางธุรกิจขององค์กร

ซึ่งประกอบด้วยกิจกรรมต่าง ๆ ที่อธิบายในข้อ 5.2 ถึงข้อ 5.6 โดยกระบวนการบริหารความเสี่ยงได้แสดงไว้ดังรูปที่ 3



รูปที่ 3 กระบวนการบริหารความเสี่ยง

5.2 การสื่อสารและการปรึกษา

การสื่อสารและการปรึกษากับผู้มีส่วนได้เสียทั้งภายในและภายนอก ควรดำเนินการในทุกขั้นตอนของกระบวนการบริหารความเสี่ยง

ดังนั้น แผนการสื่อสารและการปรึกษาควรจัดทำขึ้นและดำเนินการในขั้นตอนแรก ๆ แผนเหล่านี้ควรระบุถึงประเด็นต่าง ๆ ที่เกี่ยวข้องกับสาเหตุและผลที่ตามมา (ถ้าทราบ) รวมถึงมาตรการในการจัดการความเสี่ยงต่าง ๆ การสื่อสารและการปรึกษาทั้งภายนอกและภายในอย่างมีประสิทธิภาพ ควรมีการดำเนินการเพื่อให้มั่นใจว่าผู้รับผิดชอบและผู้มีส่วนได้เสียกับกระบวนการบริหารความเสี่ยงมีความเข้าใจถึงพื้นฐานของการตัดสินใจและเหตุผลของสิ่งจำเป็นที่ต้องดำเนินการ

ทีมที่ปรึกษาอาจดำเนินการ ดังนี้

- ช่วยจัดทำบริบทที่เหมาะสม
- มั่นใจว่าได้มีการทำความเข้าใจและพิจารณาผลประโยชน์ของผู้มีส่วนได้เสีย

ISO 31000 : 2009

- ช่วยให้นั่นใจว่ามีการชี้แจงความเสี่ยงอย่างเพียงพอ
- นำผู้เชี่ยวชาญในแต่ละด้านมาร่วมกันวิเคราะห์ความเสี่ยง
- มั่นใจว่ามีการพิจารณามุมมองที่แตกต่างในการกำหนดเกณฑ์ความเสี่ยงและการประเมินผลความเสี่ยง
- การเห็นชอบและสนับสนุนแผนจัดการความเสี่ยงต่าง ๆ
- ส่งเสริมการบริหารความเปลี่ยนแปลงอย่างเหมาะสมในกระบวนการบริหารความเสี่ยง
- พัฒนาแผนการสื่อสารและการปรึกษาทั้งภายในและภายนอกอย่างเหมาะสม

การสื่อสารและการปรึกษากับผู้มีส่วนได้เสียเป็นสิ่งสำคัญ เพราะการตัดสินใจเกี่ยวกับความเสี่ยงจะขึ้นอยู่กับ การรับรู้เกี่ยวกับความเสี่ยง ซึ่งการรับรู้เหล่านี้สามารถแปรผันตามความแตกต่างของคุณค่า ความจำเป็น สมมุติฐาน แนวคิดและความสนใจของผู้มีส่วนได้เสีย เนื่องจากมุมมองของผู้มีส่วนได้เสียสามารถมีผลกระทบ อย่างมีนัยสำคัญต่อการตัดสินใจ ดังนั้น จึงควรมีการชี้แจงและบันทึกการรับรู้ของผู้มีส่วนได้เสียไว้ และนำไป พิจารณาในกระบวนการตัดสินใจ

การสื่อสารและการปรึกษาควรดำเนินการไปตามข้อเท็จจริง สอดคล้อง ถูกต้อง และมีความเข้าใจในการ แลกเปลี่ยนสารสนเทศ รักษาความลับและอยู่บนพื้นฐานของความซื่อสัตย์

5.3 การกำหนดบริบท

5.3.1 ทั่วไป

การกำหนดบริบทขององค์กรควรเชื่อมโยงกับวัตถุประสงค์ที่ชัดเจนและปัจจัยทั้งภายในและภายนอก เพื่อนำไปสู่การบริหารความเสี่ยง รวมถึงกำหนดขอบเขตและเกณฑ์ความเสี่ยงให้กับกระบวนการที่เหลือ สำหรับปัจจัยต่าง ๆ เหล่านี้จะคล้ายกับการพิจารณาในการออกแบบกรอบการบริหารความเสี่ยง (ดูข้อ 4.3.1) โดยการกำหนดบริบทสำหรับกระบวนการบริหารความเสี่ยง ผู้เกี่ยวข้องจำเป็นต้องพิจารณาลึกลงไป ในรายละเอียดที่จำเพาะเจาะจงตามขอบเขตของกระบวนการบริหารความเสี่ยงที่เกี่ยวข้อง

5.3.2 การจัดทำบริบทภายนอก

บริบทภายนอก หมายถึง สภาพแวดล้อมภายนอกที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กร

การเข้าใจบริบทภายนอกเป็นสิ่งสำคัญเพื่อให้นั่นใจว่าวัตถุประสงค์และข้อห่วงใยของผู้มีส่วนได้เสีย ภายนอกได้รับการพิจารณาเมื่อมีการจัดทำเกณฑ์ความเสี่ยง บริบทภายนอกขึ้นอยู่กับบริบทองค์กรใน ภาพกว้าง (organization-wide) แต่มีรายละเอียดของข้อกำหนดกฎหมาย ข้อบังคับอย่างเฉพาะเจาะจง มุมมองการรับรู้ (perception) ของผู้มีส่วนได้เสีย และประเด็นปัญหาความเสี่ยงอื่น ๆ ที่เฉพาะเจาะจงจนถึง ขอบเขตของกระบวนการบริหารความเสี่ยง

การประเมินบริบทภายนอกขององค์กร อาจรวมถึงประเด็นต่าง ๆ ดังต่อไปนี้

- สังคม วัฒนธรรม การเมือง กฎหมาย ข้อบังคับ การเงิน เทคโนโลยี เศรษฐกิจ ลักษณะขององค์กรและสภาพการแข่งขันทางธุรกิจ ทั้งในระดับโลก ระดับชาติ ระดับภูมิภาค หรือระดับท้องถิ่น
- ตัวขับเคลื่อนที่สำคัญและแนวโน้มที่จะมีผลกระทบต่อวัตถุประสงค์ขององค์กร
- ความสัมพันธ์กับผู้มีส่วนได้เสียภายนอกองค์กร มุมมองของผู้มีส่วนได้เสียภายนอกองค์กร และคุณค่าขององค์กรที่มีต่อผู้มีส่วนได้เสียภายนอกองค์กร

5.3.3 การจัดทำบริบทภายในองค์กร

บริบทภายใน หมายถึง สภาพแวดล้อมภายในที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กร

กระบวนการบริหารความเสี่ยงควรไปในทิศทางเดียวกับวัฒนธรรมองค์กร การดำเนินการ โครงสร้าง และกลยุทธ์ บริบทภายในองค์กรหมายถึงสิ่งต่าง ๆ ภายในองค์กรที่สามารถมีอิทธิพลต่อวิถีทางที่องค์กรจะบริหารความเสี่ยง บริบทภายในองค์กรควรมีการจัดทำเพราะ

- (ก) การบริหารความเสี่ยงกำหนดอยู่ในบริบทวัตถุประสงค์ขององค์กร
- (ข) วัตถุประสงค์และเกณฑ์ของแต่ละโครงการ กระบวนการ หรือกิจกรรม ควรได้รับการพิจารณาถึงวัตถุประสงค์ขององค์กรโดยรวม
- (ค) บางองค์กรอาจไม่ทราบถึงโอกาสในการบรรลุกลยุทธ์ โครงการ หรือวัตถุประสงค์ทางธุรกิจ และส่งผลกระทบอย่างต่อเนื่องถึงความมุ่งมั่น ความน่าเชื่อถือ ความไว้วางใจและคุณค่าขององค์กร

องค์กรควรเข้าใจบริบทภายใน อาจรวมถึงประเด็นต่าง ๆ ดังต่อไปนี้

- การกำกับดูแล โครงสร้างองค์กร บทบาท และภาระรับผิดชอบ
- กลยุทธ์เพื่อให้บรรลุตามนโยบายและวัตถุประสงค์ที่กำหนดไว้
- จัดความสามารถด้านทรัพยากรและความรู้ (เช่น เงินทุน เวลา คน การดำเนินการ ระบบ และเทคโนโลยี)
- ระบบสารสนเทศ การรับส่งสารสนเทศ และการดำเนินการตัดสินใจ (ทั้งเป็นทางการและไม่เป็นทางการ)
- ความสัมพันธ์กับผู้มีส่วนได้เสียภายในองค์กร มุมมองของผู้มีส่วนได้เสียภายในองค์กร และคุณค่าขององค์กรที่มีต่อผู้มีส่วนได้เสียภายในองค์กร
- วัฒนธรรมองค์กร
- มาตรฐาน แนวทาง และรูปแบบการดำเนินการต่าง ๆ ที่รับมาใช้ในองค์กร
- ระเบียบแบบแผนและความผูกพันทางพันธะสัญญา

5.3.4 การจัดทำบริบทของกระบวนการบริหารความเสี่ยง

องค์กรหรือส่วนขององค์กรที่นำกระบวนการบริหารความเสี่ยงไปประยุกต์ใช้ควรกำหนดวัตถุประสงค์ กลยุทธ์ ขอบเขต และตัวแปร (parameter) ของกิจกรรม ผู้บริหารความเสี่ยงควรพิจารณาอย่างจริงจังถึงความจำเป็นของทรัพยากรที่ใช้ในการบริหารความเสี่ยง ทรัพยากรที่ต้องการ ความรับผิดชอบ และอำนาจหน้าที่ รวมทั้งบันทึกที่ต้องจัดเก็บ ควรมีการกำหนดไว้

บริบทของกระบวนการบริหารความเสี่ยงจะแปรเปลี่ยนไปตามต้องการขององค์กร ซึ่งสามารถประกอบด้วย

- กำหนดเป้าหมายและวัตถุประสงค์ของกิจกรรมการบริหารความเสี่ยง
- กำหนดความรับผิดชอบไว้ในกระบวนการบริหารความเสี่ยง
- กำหนดขอบเขต ความลึกและความกว้างของกิจกรรมบริหารความเสี่ยงที่จะดำเนินการ รวมถึงสิ่งที่ได้ดำเนินการและสิ่งที่ได้ละเว้น
- กำหนดกิจกรรม กระบวนการ หน้าที่งาน โครงการ ผลิตภัณฑ์ การบริการ หรือสินทรัพย์ตามช่วงเวลา และสถานที่
- กำหนดความสัมพันธ์ระหว่างแต่ละโครงการ กระบวนการ หรือกิจกรรม กับโครงการอื่น ๆ กระบวนการหรือกิจกรรมขององค์กร
- กำหนดวิธีการประเมินความเสี่ยง
- กำหนดวิธีประเมินผลการดำเนินงานและประสิทธิผลในการบริหารความเสี่ยง
- ชี้นำและระบุการตัดสินใจที่ต้องดำเนินการ
- การชี้แจง กำหนดขอบเขต หรือกำหนดกรอบที่จำเป็นในการศึกษา ขนาดและวัตถุประสงค์ขององค์กร และทรัพยากรที่ต้องการในการศึกษา

การคำนึงถึงปัจจัยเหล่านี้และปัจจัยอื่น ๆ ที่เกี่ยวข้อง ช่วยให้มั่นใจว่าแนวทางการบริหารความเสี่ยงที่ใช้เหมาะสมกับสภาพการณ์ต่าง ๆ ที่เกิดขึ้นกับองค์กร และความเสี่ยงที่ส่งผลต่อการบรรลุวัตถุประสงค์ขององค์กร

5.3.5 กำหนดเกณฑ์ความเสี่ยง

องค์กรควรกำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยงที่สำคัญ เกณฑ์ควรสะท้อนคุณค่า วัตถุประสงค์ และทรัพยากรขององค์กร เกณฑ์บางเกณฑ์สามารถกำหนดโดยหรือได้รับจากกฎหมายและกฎระเบียบหรือ

ข้อกำหนดอื่น ๆ ที่องค์กรเป็นสมาชิก เกณฑ์ความเสี่ยงต้องสอดคล้องกับนโยบายบริหารความเสี่ยงขององค์กร (ดูข้อ 4.3.2) ต้องกำหนดตั้งแต่เริ่มต้นกระบวนการบริหารความเสี่ยงและทบทวนอย่างต่อเนื่อง

เมื่อกำหนดเกณฑ์ความเสี่ยง ปัจจัยที่ต้องพิจารณาควรรวมถึงสิ่งต่าง ๆ ดังต่อไปนี้

- ลักษณะขององค์กร และประเภทของสาเหตุและผลสืบเนื่องที่สามารถเกิดขึ้นและวิธีการที่จะวัด
- วิธีการกำหนดโอกาส
- ช่วงเวลาของโอกาสและ/หรือผลสืบเนื่อง
- วิธีการกำหนดระดับความเสี่ยง
- มุมมองของผู้มีส่วนได้เสีย
- ระดับความเสี่ยงที่ยอมรับได้
- เมื่อใดก็ตามที่มีหลาย ๆ ความเสี่ยงเกิดขึ้นร่วมกัน ควรมีการพิจารณาจัดการความเสี่ยงที่อาจสูงขึ้น และพิจารณาว่าความเสี่ยงเหล่านั้นเกิดขึ้นร่วมกันได้อย่างไร

5.4 การประเมินความเสี่ยง

5.4.1 ทั่วไป

การประเมินความเสี่ยงเป็นกระบวนการที่รวมถึงการชี้บ่งความเสี่ยง การวิเคราะห์ความเสี่ยง และการประเมินผลความเสี่ยง

หมายเหตุ ดู ISO/IEC 31010 เทคนิคการประเมินความเสี่ยง

5.4.2 การชี้บ่งความเสี่ยง

องค์กรควรชี้บ่งแหล่งความเสี่ยง ส่วนที่ได้รับผลกระทบ เหตุการณ์ (รวมถึงการเปลี่ยนแปลงของสภาพการณ์) สาเหตุของการเกิด และศักยภาพของผลสืบเนื่องที่อาจเกิดขึ้น จุดมุ่งหมายของขั้นตอนนี้คือการจัดทำบัญชีความเสี่ยงที่ครอบคลุมเหตุการณ์ต่าง ๆ ที่อาจส่งเสริม ขัดขวาง ลด เร่ง หรือชะลอ การบรรลุวัตถุประสงค์ การชี้บ่งความเสี่ยงเป็นเรื่องสำคัญที่ต้องดำเนินการโดยไม่ต้องอ้างถึงโอกาสที่จะเกิด การชี้บ่งอย่างครอบคลุมเป็นสิ่งที่สำคัญมากเพราะความเสี่ยงที่ไม่ได้ถูกชี้บ่งในขั้นตอนนี้จะไม่ถูกนำไปวิเคราะห์ในขั้นตอนต่อไป

การชี้บ่งความเสี่ยงควรครอบคลุมทุกความเสี่ยง แม้ว่าแหล่งความเสี่ยงนั้นไม่ได้อยู่ภายใต้การควบคุมขององค์กร หรือแหล่งความเสี่ยงหรือสาเหตุยังไม่ปรากฏชัดก็ตาม การชี้บ่งความเสี่ยงควรรวมการตรวจสอบผลที่เกิดขึ้นตามมาจากเหตุการณ์นั้น ๆ รวมถึงผลที่เกิดขึ้นในแต่ละขั้นและผลรวมของผลทั้งหมดที่เกิดขึ้น การชี้บ่งความเสี่ยงควรพิจารณาผลที่เกิดขึ้นตามมาในวงกว้างที่จะเกิดแม้ว่าจะมีโอกาสในการเกิดน้อย

ก็ตาม นอกจากนี้การซึ่งความเสี่ยงจำเป็นอย่างยิ่งที่ต้องพิจารณาสาเหตุและสถานการณ์ที่เป็นไปได้ ซึ่งแสดงให้เห็นผลสืบเนื่องที่อาจเกิดขึ้น ฉะนั้นสาเหตุและผลสืบเนื่องที่สำคัญทั้งหมดควรได้รับการพิจารณาองค์กรควรประยุกต์ใช้วิธีการและเทคนิคการซึ่งความเสี่ยงให้เหมาะสมกับวัตถุประสงค์ จิตความสามารถ และความเสี่ยงที่เผชิญอยู่ สารสนเทศที่เกี่ยวข้องและเป็นปัจจุบันมีความสำคัญในการซึ่งความเสี่ยง ซึ่งรวมถึงสารสนเทศย้อนหลังที่เหมาะสมเท่าที่จะหาได้ ทั้งนี้ ผู้ที่มีส่วนร่วมในการซึ่งความเสี่ยงควรมีความรู้ที่เหมาะสม

5.4.3 การวิเคราะห์ความเสี่ยง

การวิเคราะห์ความเสี่ยงเกี่ยวข้องกับการทำความเข้าใจความเสี่ยง ซึ่งจะได้ข้อมูลสำหรับใช้ในการประเมินผลความเสี่ยงและการตัดสินใจจัดการความเสี่ยงด้วยวิธีการและกลยุทธ์ที่เหมาะสมที่สุด การวิเคราะห์ความเสี่ยงยังสามารถให้ข้อมูลนำเข้าสำหรับตัดสินใจทางเลือกในการจัดการความเสี่ยงในประเภทและระดับความเสี่ยงที่แตกต่างกันด้วย

การวิเคราะห์ความเสี่ยงเกี่ยวข้องกับการพิจารณาถึงสาเหตุและแหล่งความเสี่ยง ผลสืบเนื่องทั้งทางบวกและทางลบรวมถึงโอกาสที่ผลสืบเนื่องเหล่านั้นจะเกิดขึ้น นอกจากนี้ควรทำการซึ่งปัจจัยที่มีผลต่อโอกาสและผลสืบเนื่อง ความเสี่ยงเป็นผลจากการพิจารณาผลสืบเนื่องและโอกาสรวมถึงปัจจัยร่วมอื่น ๆ ที่มีผลต่อความเสี่ยง สำหรับเหตุการณ์ที่มีผลสืบเนื่องหลายอย่างที่สามารถส่งผลกระทบต่อหลายวัตถุประสงค์นั้น ต้องพิจารณาถึงประสิทธิผลและประสิทธิภาพของมาตรการควบคุมที่มีอยู่

แนวทางในการกำหนดเกณฑ์ผลสืบเนื่องและโอกาส รวมถึงแนวทางในการนำเกณฑ์ทั้งสองอย่างมาพิจารณาร่วมกันเพื่อกำหนดระดับความเสี่ยงนั้น ควรสะท้อนประเภทของความเสี่ยง สารสนเทศที่มีและจุดมุ่งหมายที่จะนำผลการประเมินความเสี่ยงไปใช้ แนวทางนี้ควรสอดคล้องกับเกณฑ์ความเสี่ยง ซึ่งควรพิจารณาความเกี่ยวโยงของความเสี่ยงและแหล่งความเสี่ยงที่แตกต่างกันเป็นสิ่งสำคัญ

การวิเคราะห์ความเสี่ยงควรนำความเชื่อมั่นในการกำหนดระดับความเสี่ยงและความไวในการตอบสนองต่อเงื่อนไขที่กำหนดไว้ล่วงหน้า และสมมุติฐานมาพิจารณา และควรสื่อสารอย่างมีประสิทธิภาพให้ผู้ทำหน้าที่ตัดสินใจ รวมถึงผู้มีส่วนได้เสียทราบอย่างเหมาะสม ปัจจัยที่ควรระบุและให้ความสำคัญ ได้แก่ ความเห็นที่แตกต่างของผู้เชี่ยวชาญ ความไม่แน่นอน ความพร้อม คุณภาพ ปริมาณ และสารสนเทศที่มีการเคลื่อนไหว หรือข้อจำกัดของแบบจำลอง

การวิเคราะห์ความเสี่ยงสามารถดำเนินการในเชิงรายละเอียดได้หลายระดับ ขึ้นกับความเสี่ยง จุดมุ่งหมายของการวิเคราะห์ รวมทั้งสารสนเทศ ข้อมูลและทรัพยากรที่มีอยู่ การวิเคราะห์สามารถทำได้ทั้งในเชิงคุณภาพ เชิงกึ่งปริมาณ เชิงปริมาณ หรือร่วมกันขึ้นอยู่กับสภาพการณ์

ผลสืบเนื่องและโอกาสสามารถกำหนดได้จากผลลัพธ์ของแบบจำลองของเหตุการณ์เดียวหรือหลาย ๆ เหตุการณ์ หรือการประมาณค่านอกช่วง (extrapolation) จากการศึกษาเชิงการทดลอง หรือจากข้อมูลที่มีอยู่ ผลสืบเนื่องสามารถแสดงในรูปของผลกระทบที่เป็นเห็นได้ชัดเจน (tangible) หรือเห็นไม่ชัดเจน (intangible) ในบางกรณีมีความต้องการการระบุค่าเป็นตัวเลขหรือรายละเอียด เพื่อใช้ในการระบุถึงผลสืบเนื่องและโอกาสสำหรับเวลา สถานที่ กลุ่มคน หรือสถานการณ์ที่แตกต่างกันไป

5.4.4 การประเมินผลความเสี่ยง

จุดมุ่งหมายของการประเมินผลความเสี่ยง เพื่อช่วยในการตัดสินใจว่าความเสี่ยงใดต้องมีการจัดการและจัดลำดับความสำคัญเพื่อดำเนินการจัดการความเสี่ยงบนพื้นฐานของผลลัพธ์ของการวิเคราะห์ความเสี่ยง การประเมินผลความเสี่ยง เป็นการเปรียบเทียบระดับความเสี่ยงที่พบระหว่างกระบวนการวิเคราะห์ความเสี่ยงกับเกณฑ์ความเสี่ยงที่กำหนดขึ้นเมื่อบริบทได้รับการพิจารณา โดยผลจากการเปรียบเทียบนี้ทำให้เห็นความจำเป็นในการจัดการความเสี่ยง

การตัดสินใจควรพิจารณาถึงบริบทของความเสี่ยงในภาพกว้าง รวมถึงการพิจารณาที่จะยอมรับความเสี่ยงที่เกิดจากภาคส่วนอื่น ๆ นอกเหนือจากองค์กรที่ได้ประโยชน์จากความเสี่ยงนั้น การตัดสินใจควรเป็นไปตามกฎหมาย ข้อบังคับและข้อกำหนดอื่น ๆ

ในบางสถานการณ์ การประเมินผลความเสี่ยงสามารถนำไปสู่การตัดสินใจเพื่อการวิเคราะห์ที่จะมีต่อไป การประเมินผลความเสี่ยงยังคงสามารถนำไปสู่การตัดสินใจที่จะไม่จัดการความเสี่ยงด้วยวิธีการอื่นใด นอกเหนือจากการรักษามาตรการควบคุมที่มีอยู่เดิม การตัดสินใจจะได้รับอิทธิพลจากทัศนคติเรื่องความเสี่ยงในองค์กรและเกณฑ์ความเสี่ยงที่กำหนดขึ้น

5.5 การจัดการความเสี่ยง

5.5.1 ทั่วไป

การจัดการความเสี่ยงเป็นการเลือกทางเลือกหนึ่งหรือมากกว่าทางเลือกเพื่อเปลี่ยนแปลงความเสี่ยงและการนำทางเลือกไปปฏิบัติ การจัดการความเสี่ยงทำให้เกิดหรือเปลี่ยนแปลงมาตรการควบคุมต่าง ๆ

การจัดการความเสี่ยงเกี่ยวกับกระบวนการที่เป็นวงจรต่อไปนี้

- การประเมินการจัดการความเสี่ยง
- การตัดสินใจว่า จะยอมรับระดับความเสี่ยงที่เหลืออยู่ได้หรือไม่
- ถ้ายอมรับไม่ได้ ให้กำหนดการจัดการความเสี่ยงใหม่
- การประเมินประสิทธิภาพการจัดการความเสี่ยงนั้น

ทางเลือกในการจัดการความเสี่ยงไม่จำเป็นต้องเฉพาะเจาะจงหรือเหมาะสมกับทุกสภาพการณ์ ทางเลือกอาจรวมถึง

- (ก) การหลีกเลี่ยงความเสี่ยงโดยการตัดสินใจที่จะไม่เริ่มหรือดำเนินการต่อในกิจกรรมที่ก่อให้เกิดความเสี่ยง
- (ข) การรับความเสี่ยงหรือเพิ่มความเสี่ยงเพื่อหาโอกาส (opportunity)
- (ค) การขจัดแหล่งความเสี่ยง
- (ง) การเปลี่ยนโอกาส (likelihood)
- (จ) การเปลี่ยนผลสืบเนื่อง
- (ฉ) การเปลี่ยนความเสี่ยงกับภาคส่วนอื่น (รวมถึงสัญญาและความเสี่ยงทางการเงิน)
- (ช) การคงความเสี่ยงไว้โดยแจ้งการตัดสินใจ

5.5.2 การเลือกทางเลือกในการจัดการความเสี่ยง

การเลือกทางเลือกในการจัดการความเสี่ยงที่เหมาะสมที่สุดเป็นการหาสมดุล ระหว่างต้นทุนและความพยายามของการนำไปปฏิบัติเทียบกับประโยชน์ที่ได้รับ โดยพิจารณาถึงกฎหมาย ข้อบังคับ และข้อกำหนดอื่น ๆ เช่น ความรับผิดชอบต่อสังคม และการปกป้องสิ่งแวดล้อมทางธรรมชาติ การตัดสินใจในการจัดการความเสี่ยงควรคำนึงความคุ้มค่าทางเศรษฐกิจ เช่น มีความรุนแรง (ผลสืบเนื่องเชิงลบสูง) แต่ความเสี่ยงน้อยมาก (โอกาสต่ำ)

ทางเลือกในการจัดการความเสี่ยงสามารถนำไปใช้ทีละทางเลือกหรือหลาย ๆ ทางเลือกรวมกัน โดยปกติองค์กรก็จะได้ประโยชน์จากการใช้ทางเลือกหลาย ๆ ทางเลือกรวมกัน

ในการเลือกทางเลือกการจัดการความเสี่ยง องค์กรควรพิจารณาถึงคุณค่าและการรับรู้ของผู้มีส่วนได้เสีย และวิธีการที่เหมาะสมที่สุดในการสื่อสาร ในกรณีที่ทางเลือกในการจัดการความเสี่ยงส่งผลกระทบต่อความเสี่ยงอื่นในองค์กรหรือกับผู้มีส่วนได้เสียควรนำมาพิจารณาด้วย แม้ว่าประสิทธิผลจะเท่ากัน การจัดการความเสี่ยงบางอย่าง ผู้มีส่วนได้เสียจะยอมรับได้มากกว่ากลุ่มอื่น ๆ

แผนการจัดการความเสี่ยงควรชี้บ่งลำดับความสำคัญของการนำการจัดการความเสี่ยงแต่ละเรื่องไปปฏิบัติให้ชัดเจน

การจัดการความเสี่ยงสามารถทำให้เกิดความเสี่ยงได้ ความเสี่ยงที่มีนัยสำคัญสามารถทำให้มาตรการการจัดการความเสี่ยงล้มเหลวหรือไม่มีประสิทธิผล ดังนั้น การติดตามตรวจสอบถือเป็นส่วนหนึ่งของแผนการจัดการความเสี่ยงเพื่อประกันว่ามาตรการยังคงมีประสิทธิผล

การจัดการความเสี่ยงสามารถทำให้เกิดความเสี่ยงอื่นตามมาซึ่งจำเป็นต้องประเมิน จัดการติดตาม ตรวจสอบและทบทวน ความเสี่ยงอื่นที่ตามมาควรรวมไว้ในแผนการจัดการความเสี่ยงเดียวกันกับความ

เสี่ยงเดิมโดยไม่จัดการเหมือนเป็นความเสี่ยงใหม่ การเชื่อมโยงระหว่างความเสี่ยงทั้งสองนี้ควรชี้แจงและรักษาไว้

5.5.3 การเตรียมการและการนำแผนการจัดการความเสี่ยงไปปฏิบัติ

จุดมุ่งหมายของแผนการจัดการความเสี่ยง คือ เอกสารแสดงการบันทึกการเลือกวิธีการจัดการและนำไปปฏิบัติต่อไปอย่างไร

สารสนเทศที่ใช้ในแผนการจัดการควรประกอบด้วย

- เหตุผลในการเลือกวิธีการจัดการ รวมถึงประโยชน์ที่คาดว่าจะได้รับ
- การรับผิดชอบของผู้รับผิดชอบ แผน รวมทั้งความรับผิดชอบของผู้นำแผนไปปฏิบัติ
- กิจกรรมที่จะดำเนินการ
- ทรัพยากรที่ต้องการรวมทั้งทรัพยากรสำรองฉุกเฉิน
- การวัดผลการทำงานและข้อจำกัด
- ความต้องการในการรายงานและการติดตามตรวจสอบ
- เวลาและกำหนดการ

แผนการจัดการควรบูรณาการกับกระบวนการบริหารองค์กรและหารือกับผู้มีส่วนได้เสียที่เหมาะสม

หลังจากการจัดการความเสี่ยงแล้ว ผู้ตัดสินใจและผู้มีส่วนได้เสียอื่นๆ ควรตระหนักถึงลักษณะและความเสี่ยงที่ยังเหลืออยู่ ความเสี่ยงที่ยังเหลืออยู่ควรจัดทำเป็นเอกสารและติดตามตรวจสอบ ทบทวนอย่างเหมาะสม เพื่อการจัดการต่อไป

5.6 การติดตามตรวจสอบและการทบทวน

การติดตามตรวจสอบและการทบทวนควรเป็นส่วนหนึ่งของแผนของกระบวนการบริหารความเสี่ยงและมีการตรวจสอบหรือเฝ้าระวังเป็นประจำ จะเป็นช่วงเวลาหรือครั้งคราวก็ได้

ความรับผิดชอบสำหรับการติดตามตรวจสอบและการทบทวนควรกำหนดไว้อย่างชัดเจน

กระบวนการติดตามตรวจสอบและการทบทวนขององค์กร ควรผนวกรวมประเด็นปัญหาทั้งหมดของกระบวนการบริหารความเสี่ยงเข้าไปด้วย ทั้งนี้ เพื่อจุดมุ่งหมาย ดังนี้

- การทำให้มั่นใจว่า การควบคุมเป็นไปอย่างมีประสิทธิภาพและประสิทธิผลทั้งในการออกแบบและการดำเนินการ
- การได้สารสนเทศเพิ่มเติมเพื่อปรับปรุงการประเมินความเสี่ยงต่อไป

ISO 31000 : 2009

- การวิเคราะห์และเรียนรู้บทเรียนจากเหตุการณ์ต่าง ๆ (รวมถึงเหตุการณ์เกือบเกิดอุบัติเหตุ) การเปลี่ยนแปลง แนวโน้ม ความสำเร็จและความล้มเหลวต่าง ๆ
- การตรวจหาการเปลี่ยนแปลงทั้งบริบทภายนอกและบริบทภายใน รวมถึงการเปลี่ยนแปลงเกณฑ์ความเสี่ยง และตัวความเสี่ยงเองซึ่งต้องการการทบทวนการจัดการความเสี่ยงและการจัดลำดับความสำคัญ
- การชี้แจงความเสี่ยงที่อุบัติขึ้นใหม่

ความก้าวหน้าในการนำแผนการจัดการความเสี่ยงไปปฏิบัติก่อให้เกิดการวัดผลการดำเนินการ ซึ่งผลดังกล่าวสามารถนำมาผนวกเป็นภาพรวมการบริหารผลการดำเนินงาน การวัดผลและการรายงานกิจกรรมต่าง ๆ ต่อภายนอกและภายใน

การดำเนินการ รวมถึงกิจกรรมการรายงานทั้งภายในและภายนอกโดยรวมขององค์กร

ผลของการติดตามตรวจสอบและการทบทวนควรมีการบันทึกและรายงานผลทั้งภายในและภายนอกอย่างเหมาะสม และควรใช้เป็นปัจจัยนำเข้าในการทบทวนกรอบการบริหารความเสี่ยง (ดูข้อ 4.5)

5.7 การบันทึกกระบวนการบริหารความเสี่ยง

กิจกรรมการบริหารความเสี่ยงควรสอบกลับได้ ในกระบวนการบริหารความเสี่ยง การบันทึกจะเป็นพื้นฐานสำหรับการปรับปรุงวิธีการและเครื่องมือ รวมถึงในกระบวนการทั้งหมด

การสร้างบันทึกควรพิจารณาถึง

การตัดสินใจที่เกี่ยวข้องกับการจัดทำบันทึกควรพิจารณาถึง

- ความจำเป็นขององค์กรในการเรียนรู้อย่างต่อเนื่อง
- ประโยชน์จากการนำสารสนเทศไปใช้ซ้ำเพื่อจุดมุ่งหมายในการบริหาร
- ต้นทุนค่าใช้จ่ายและความพยายามในการจัดทำและรักษาไว้ของบันทึก
- ความจำเป็นในการบันทึกตามกฎหมาย ข้อบังคับ และข้อปฏิบัติ
- วิธีการเข้าถึง ความง่ายในการนำมาใช้งาน และสื่อที่ใช้ในการจัดเก็บ
- ระยะเวลาจัดเก็บ
- ความอ่อนไหวของสารสนเทศ

ภาคผนวก ก.

(เพื่อเป็นข้อมูล)

คุณลักษณะในการส่งเสริมการบริหารความเสี่ยง**ก.1 ทั่วไป**

ทุกองค์กรควรตั้งเป้าหมายสำหรับระดับของผลการดำเนินงานตามกรอบการบริหารความเสี่ยงขององค์กรอย่างเหมาะสม เพื่อให้สอดคล้องกับความสำเร็จของการตัดสินใจที่ต้องทำ รายการคุณลักษณะดังปรากฏข้างล่างจะแสดงให้เห็นถึงผลการดำเนินงานระดับสูงในการบริหารความเสี่ยง เพื่อช่วยให้องค์กรวัดผลการดำเนินงานขององค์กรเทียบกับเกณฑ์เหล่านี้ จึงได้กำหนดตัวชี้วัดที่ชัดเจนไว้ในแต่ละคุณลักษณะ

ก.2 ผลลัพธ์ที่สำคัญ

ก.2.1 องค์กรทราบความเสี่ยงที่เป็นปัจจุบัน ถูกต้องและครอบคลุมของตนเอง

องค์กรมีความเข้าใจความเสี่ยงที่เป็นปัจจุบัน ถูกต้องอย่างครบถ้วน

ก.2.2 ความเสี่ยงขององค์กรอยู่ในเกณฑ์ความเสี่ยงที่องค์กรกำหนด

ก.3 คุณลักษณะ**ก.3.1 การปรับปรุงอย่างต่อเนื่อง**

จุดมุ่งเน้นอยู่ที่องค์กรมีการปรับปรุงการบริหารความเสี่ยงอย่างต่อเนื่อง โดยกำหนดเป้าประสงค์ผลการดำเนินงานขององค์กร การวัดผล การทบทวน และนำไปสู่การเปลี่ยนแปลงกระบวนการ ระบบ ทรัพยากร ขีดความสามารถ และทักษะ

การปรับปรุงอย่างต่อเนื่องสามารถแสดงได้จากการวัดผลการดำเนินการขององค์กรและผลการดำเนินการของผู้จัดการเป็นรายบุคคลเทียบกับเป้าประสงค์ที่กำหนดไว้แล้วอย่างชัดเจน โดยผลการดำเนินการขององค์กรสามารถตีพิมพ์เผยแพร่และสื่อสารได้ ตามปกติจะมีการทบทวนผลการดำเนินงานอย่างน้อยปีละหนึ่งครั้งแล้วจึงปรับปรุงกระบวนการและกำหนดวัตถุประสงค์ของผลการดำเนินงานใหม่สำหรับช่วงเวลาถัดไป

การประเมินผลการดำเนินการการบริหารความเสี่ยงนี้ ถือเป็นส่วนหนึ่งของการประเมินผลการดำเนินงานทั้งหมดขององค์กรโดยรวม และของระบบการวัดผลสำหรับหน่วยงานและรายบุคคล

ก.3.2 ความพร้อมการรับมือในเรื่องความเสี่ยง

ในการยกระดับการบริหารความเสี่ยง จะรวมถึงการกำหนดการรับมือที่ชัดเจนและครบถ้วน การควบคุมความเสี่ยง และงานการจัดการความเสี่ยง บุคคลที่ได้รับการมอบหมายการรับมือที่ชัดเจนนั้นต้องมีทักษะที่เหมาะสมและทรัพยากรต่าง ๆ อย่างเพียงพอต่อการควบคุมตรวจสอบ ติดตามตรวจสอบ

ความเสี่ยง ปรับปรุงมาตรการควบคุมและสื่อสารเกี่ยวกับความเสี่ยงอย่างมีประสิทธิภาพ รวมถึงการบริหาร
สิ่งเหล่านั้นไปยังผู้มีส่วนได้เสียภายนอกและผู้มีส่วนได้เสียภายใน

ในเรื่องเหล่านี้สามารถชี้แจงได้โดยสมาชิกทุกคนภายในองค์กรมีความตระหนักรู้เพิ่มเติมในเรื่องความ
เสี่ยง การควบคุมและงานที่สมาชิกแต่ละคนมีภาระรับผิดชอบ ซึ่งโดยปกติสิ่งเหล่านี้จะระบุอยู่ใน
คำบรรยายลักษณะงาน (job description) ฐานข้อมูล (database) หรือระบบสารสนเทศ (information
system) สำหรับคำนิยามของบทบาท ภาระรับผิดชอบและความรับผิดชอบควรเป็นส่วนหนึ่งในโปรแกรม
การเตรียมบุคลากรก่อนเริ่มงาน (induction programme) ขององค์กร

องค์กรมั่นใจว่าผู้ที่มีภาระรับผิดชอบ พร้อมทั้งจะบรรลุถึงบทบาทที่กำหนดให้ด้วยการมอบอำนาจหน้าที่
เวลา การฝึกอบรม ทรัพยากร และทักษะที่เพียงพอต่อภาระรับผิดชอบที่ได้รับ

ก.3.3 การประยุกต์ใช้การบริหารความเสี่ยงในการตัดสินใจ

การตัดสินใจทั้งหมดภายในองค์กรในระดับที่มีความสำคัญและมีนัยสำคัญใด ๆ ก็ตามเกี่ยวข้องกับการ
พิจารณาความเสี่ยงอย่างเปิดเผยและการประยุกต์ใช้การบริหารความเสี่ยงในระดับที่เหมาะสม

ในเรื่องนี้สามารถแสดงได้ด้วยบันทึกการประชุมและการตัดสินใจที่แสดงถึงการได้หารือในเรื่องความ
เสี่ยงที่ชัดเจน นอกจากนี้ต้องให้เห็นว่าองค์ประกอบของการบริหารความเสี่ยงทั้งหมดได้มีการนำไปใช้กับ
กระบวนการที่สำคัญสำหรับการตัดสินใจภายในองค์กร เช่น การตัดสินใจจัดสรรเงินทุน ในโครงการใหญ่
และการเปลี่ยนแปลงโครงสร้างและการเปลี่ยนแปลงองค์กร ดังเหตุผลที่ว่ามานี้ การบริหารความเสี่ยงที่ดี
ในองค์กรจึงเป็นพื้นฐานของการกำกับดูแลองค์กรที่มีประสิทธิภาพ

ก.3.4 การสื่อสารอย่างต่อเนื่อง

ในการยกระดับการบริหารความเสี่ยง จะรวมถึงการสื่อสารอย่างต่อเนื่องกับผู้มีส่วนได้เสียภายนอกและ
ภายใน รวมทั้งการรายงานผลการดำเนินงานการบริหารความเสี่ยงที่ครอบคลุมและสม่ำเสมอ ซึ่งเป็น
ส่วนหนึ่งของการกำกับดูแลที่ดี

ในเรื่องนี้สามารถแสดงได้ด้วยการสื่อสารกับผู้มีส่วนได้เสีย ซึ่งเป็นองค์ประกอบส่วนหนึ่งที่จำเป็นของการ
บริหารความเสี่ยง การสื่อสารนั้นที่ถูกต้องควรเป็นกระบวนการสื่อสารแบบสองทาง การได้รับข้อมูลที่
เหมาะสมสามารถช่วยตัดสินใจเกี่ยวกับระดับความเสี่ยงและความจำเป็นในการแก้ไขความเสี่ยงเทียบกับ
เกณฑ์ที่กำหนดไว้อย่างครอบคลุม

การรายงานภายนอกและภายในอย่างครอบคลุมและสม่ำเสมอทั้งในเรื่องความเสี่ยงที่มีนัยสำคัญและ
ผลการดำเนินงานบริหารความเสี่ยงมีส่วนช่วยอย่างมากในการกำกับดูแลองค์กรอย่างมีประสิทธิภาพ

ก.3.5 การบูรณาการอย่างเต็มรูปแบบกับโครงสร้างการกำกับดูแลขององค์กร

การบริหารความเสี่ยงถือเป็นหัวใจสำคัญของกระบวนการบริหารองค์กร เนื่องจากความเสี่ยงเป็นผลของความไม่แน่นอนต่อวัตถุประสงค์ โครงสร้างและกระบวนการของการกำกับดูแลจึงอยู่บนพื้นฐานของการบริหารความเสี่ยง การบริหารความเสี่ยงที่มีประสิทธิผลเป็นสิ่งที่ผู้บริหารถือว่าเป็นเรื่องจำเป็น เพื่อให้บรรลุวัตถุประสงค์ขององค์กร

ในเรื่องนี้สามารถแสดงได้ด้วยวิธีการสื่อสารของผู้บริหาร (manager language) และจากเอกสารสำคัญในองค์กรที่ใช้คำว่า “ความไม่แน่นอน” ที่เกี่ยวข้องกับความเสี่ยง คุณลักษณะนี้ยังสะท้อนให้เห็นได้ตามปกติในถ้อยแถลงนโยบายขององค์กรโดยเฉพาะอย่างยิ่งที่เกี่ยวกับการบริหารความเสี่ยง ตามปกติคุณลักษณะนี้จะได้รับการทวนสอบโดยการสัมภาษณ์ผู้บริหารและโดยการพิจารณาจากหลักฐานการปฏิบัติและถ้อยแถลงนโยบาย
