ประกาศกระทรวงอุตสาหกรรม

ฉบับที่ ๓๘๘๔ (พ.ศ. ๒๕๕๑)

ออกตามความในพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม

พ.ศ. ๒๕๑๑

เรื่อง กำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรม

ระบบการจัดการด้านการรักษาความปลอดภัย - ข้อกำหนดสำหรับการจัดประชุม สัมมนา และนิทรรศการ

อาศัยอำนาจตามความในมาตรา ๑๕ แห่งพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม พ.ศ. ๒๕๑๑ รัฐมนตรีว่าการกระทรวงอุตสาหกรรมออกประกาศกำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรมระบบการจัดการด้านการรักษาความปลอดภัย - ข้อกำหนดสำหรับการจัดประชุม สัมมนา และนิทรรศการ มาตรฐานเลขที่ มอก. 22300 - 2551 ไว้ ดังมีรายการละเอียดต่อท้ายประกาศนี้

ประกาศ ณ วันที่ ๑๗ มิถุนายน พ.ศ. ๒๕๕๑

สุวิทย์ คุณกิตติ

รัฐมนตรีว่าการกระทรวงอุตสาหกรรม

มาตรฐานผลิตภัณฑ์อุตสาหกรรม
ระบบการจัดการด้านการรักษาความปลอดภัย - ข้อกำหนดสำหรับการจัดประชุม สัมมนา และนิทรรศการ

1. บทนำ

ศักยภาพของประเทศไทยในการเป็นศูนย์กลางของการจัดประชุม สัมมนา และนิทรรศการของโลกมีอยู่สูงมาก ไม่ว่าจะเป็นสภาพทางภูมิศาสตร์ ทรัพยากรธรรมชาติ ประวัติศาสตร์ วัฒนธรรมทางสังคม และลักษณะเฉพาะอื่น ๆ การจัดประชุม สัมมนา และนิทรรศการไม่ว่าจะเป็นระดับประเทศ หรือระดับนานาชาติจึงเป็นกิจกรรมที่สำคัญของประเทศไทยที่สามารถนำเงินตราจากต่างประเทศเข้ามาได้เป็นจำนวนมาก และมีส่วนส่งเสริมให้เศรษฐกิจของประเทศเกิดการเจริญเติบโต และมีความแข็งแกร่ง อย่างไรก็ตาม ในการจัดการประชุม สัมมนาในทุก ๆ ระดับเรื่องที่มักมีการหยิบยกขึ้นมาพิจารณามักเป็นเรื่องของการรักษาความปลอดภัย ดังนั้น องค์กร หรือหน่วยงานที่เกี่ยวข้องกับกิจกรรมการจัดประชุม สัมมนา และนิทรรศการ จึงจำเป็นต้องเตรียมความพร้อมในการรับมือกับอุบัติการณ์จากภัยคุกคาม ทั้งที่เกิดขึ้นจากธรรมชาติ เช่น คลื่นยักษ์สึนามิ แผ่นดินไหว หรือเกิดขึ้นโดยน้ำมือของมนุษย์ เช่น การก่อการร้าย การก่อวินาศกรรม ทั้งนี้เพื่อทำให้สามารถแก้ไขสถานการณ์ในยามวิกฤตต่าง ๆ ได้

การนำมาตรฐานฉบับนี้ไปใช้ในองค์กรที่เกี่ยวข้องกับกิจกรรมการจัดประชุม สัมมนา และนิทรรศการ จะทำให้องค์กรเหล่านั้นสามารถเตรียมความพร้อม สามารถรับมือต่ออุบัติการณ์ การประสานงาน การตอบสนองต่อสถานการณ์ และการฟื้นฟูภายหลังจากอุบัติการณ์นั้นได้อย่างมีประสิทธิผล ซึ่งจะทำให้การดำเนินธุรกิจสามารถดำเนินการต่อไปได้อย่างต่อเนื่อง อันจะเป็นการสร้างความเชื่อมั่นแก่ผู้มาเยือนประเทศไทย หรือผู้มารับการบริการได้อย่างสูง

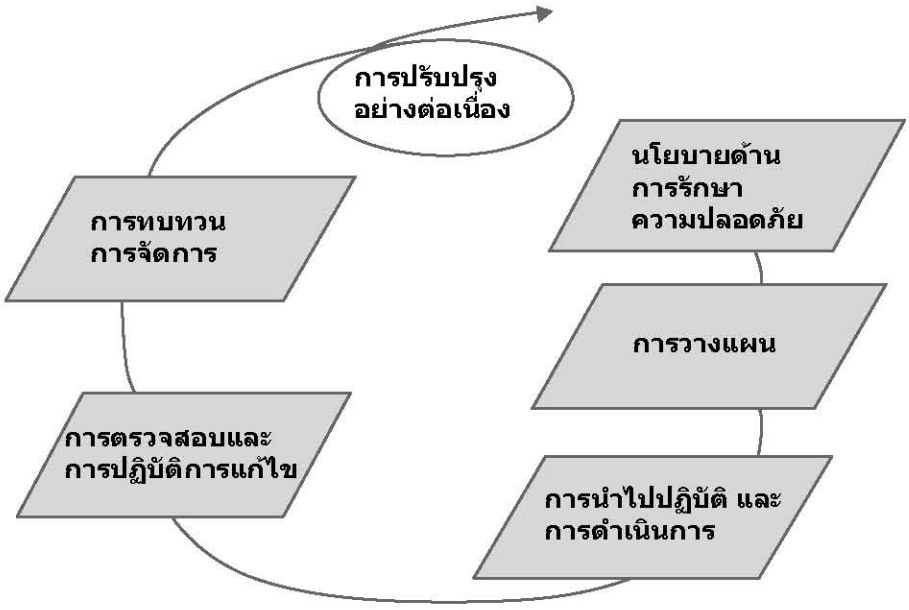
นอกจากองค์กรที่เกี่ยวข้องกับการจัดประชุม สัมมนา และนิทรรศการแล้ว มาตรฐานนี้ยังสามารถนำไปประยุกต์ใช้ได้กับองค์กรทุกประเภท ขนาด สภาพพื้นที่ วัฒนธรรม และสังคมที่มีความแตกต่างกัน อันจะช่วยให้องค์กรสามารถจัดการและการปรับปรุงผลการดำเนินงานด้านการรักษาความปลอดภัย และมีการดำเนินงานได้อย่างต่อเนื่อง รวมทั้งมีการปฏิบัติที่เป็นไปตามกฎหมายและข้อกำหนดอื่น ๆ ที่องค์กรเกี่ยวข้อง โดยให้รายละเอียดเกี่ยวกับองค์ประกอบและโครงสร้างระบบการจัดการด้านการรักษาความปลอดภัยซึ่งสามารถจะนำไปบูรณาการกับระบบการจัดการด้านอื่น ๆ ที่องค์กรมีการดำเนินการอยู่แล้ว เช่น ระบบการบริหารงานคุณภาพ ระบบการจัดการสิ่งแวดล้อม และระบบการจัดการอาชีวอนามัยและความปลอดภัย เป็นต้น ทั้งนี้ ความสำเร็จของระบบการจัดการในองค์กรย่อมขึ้นอยู่กับความมุ่งมั่นของผู้ที่เกี่ยวข้องทุกฝ่ายและทุกระดับ โดยเฉพาะผู้บริหารระดับสูงสุด ที่ต้องกำหนดนโยบายการจัดการด้านการรักษาความปลอดภัย วัตถุประสงค์ ขั้นตอนการดำเนินงาน (procedure) รวมทั้งกระบวนการต่าง ๆ ที่จะสามารถทำให้บรรลุต่อนโยบายที่กำหนดไว้

มาตรฐานนี้ไม่ได้มีจุดมุ่งหมายให้นำไปใช้เพื่อเป็นเครื่องมือการกีดกันด้านการค้า หรือ การที่สามารถดำเนินการให้สอดคล้องกับมาตรฐานนี้แล้วจะถือว่าองค์กรมีการดำเนินการตามกฎหมายที่เกี่ยวข้องแล้ว

2. ขอบข่าย

มาตรฐานฉบับนี้ ระบุข้อกำหนดสำหรับระบบการจัดการด้านการรักษาความปลอดภัย เพื่อให้องค์กรที่เกี่ยวข้องกับกิจกรรมการจัดประชุม สัมมนา และนิทรรศการ สามารถประเมิน และจัดการต่อการรักษาความปลอดภัย และสามารถดำเนินการได้อย่างต่อเนื่อง โดยการใช้นโยบาย วัตถุประสงค์ เป้าหมาย ภัยคุกคาม ความเสี่ยง การประเมินจุดอ่อนและภาวะวิกฤต (vulnerability and criticality assessment) รวมทั้ง กิจกรรมและการดำเนินการที่เกี่ยวข้องกับภัยคุกคาม ความเสี่ยง และอันตรายต่าง ๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัย และผลกระทบต่อเป้าหมายในการปรับปรุงสมรรถนะของการรักษาความปลอดภัย

องค์ประกอบของระบบการจัดการด้านการรักษาความปลอดภัยสำหรับการจัดประชุม สัมมนา และนิทรรศการ ในรูปที่ 1 มีความสำคัญ ซึ่งหากองค์กรมีการปฏิบัติตามขั้นตอนการดำเนินงานต่าง ๆ ตามรูปที่ 1 จะสามารถกำหนดนโยบายและวัตถุประสงค์ด้านการรักษาความปลอดภัย และกำหนดขั้นตอนในการนำไปปฏิบัติ พร้อมทั้งเฝ้าติดตามความสำเร็จตามเกณฑ์ที่กำหนดไว้ เพื่อทำให้เกิดวงจรการปรับปรุงระบบการจัดการด้านการรักษาความปลอดภัยอย่างต่อเนื่อง



รูปที่ 1 องค์ประกอบของระบบการจัดการด้านการรักษาความปลอดภัย
สำหรับการจัดประชุม สัมมนา และนิทรรศการ

มาตรฐานนี้ สามารถประยุกต์ใช้ได้กับองค์กรที่เกี่ยวข้องกับกิจกรรมการจัดประชุม สัมมนา และนิทรรศการทุกขนาดที่ต้องการ

ก) ปรับปรุงการรักษาความปลอดภัย และการป้องกันสินทรัพย์ที่มีความสำคัญ

ข) จัดทำ ดำเนินการ รักษาไว้ และปรับปรุงระบบการจัดการด้านการรักษาความปลอดภัยอย่างต่อเนื่อง

ค) มั่นใจถึงการเป็นไปตามนโยบายด้านการรักษาความปลอดภัยที่กำหนดไว้

ง) แสดงถึงการเป็นไปตามข้อกำหนดที่เกี่ยวข้อง

จ) องค์กรสามารถตรวจสอบระบบการจัดการด้านการรักษาความปลอดภัยของตนเอง และประกาศแสดงตนว่ามีระบบการจัดการด้านการรักษาความปลอดภัยเป็นไปตามมาตรฐานฉบับนี้ได้เอง หรือขอรับการรับรองระบบการจัดการด้านการรักษาความปลอดภัยจากหน่วยรับรอง (Certification Body) ก็ได้

ข้อกำหนดทั้งหมดในมาตรฐานฉบับนี้ มีวัตถุประสงค์ที่จะนำไปใช้โดยการผนวกรวมกับระบบการจัดการด้านการรักษาความปลอดภัยใด ๆ ที่ใช้กันอยู่แล้วในองค์กรต่าง ๆ ขอบข่ายของการประยุกต์ใช้ขึ้นอยู่กับปัจจัยต่าง ๆ เช่น นโยบายด้านการรักษาความปลอดภัยขององค์กร ลักษณะของกิจกรรม สินค้า การบริการ สถานที่ตั้ง และข้อจำกัดต่าง ๆ ภายใต้เงื่อนไขการดำเนินการขององค์กร

3. คำศัพท์ และ คำจำกัดความ

สำหรับวัตถุประสงค์ของมาตรฐานฉบับนี้ ให้ใช้คำศัพท์ และ คำจำกัดความ ดังต่อไปนี้

หมายเหตุ *ตัวพิมพ์เข้มที่ใช้ในคำจำกัดความนี้แสดงถึงคำศัพท์ที่อ้างอิงถึงอีกคำหนึ่งในข้อกำหนดนี้ และ ได้วงเล็บหมายเลขลำดับที่ของคำศัพท์ไว้ด้วย*

3.1 การรักษาความปลอดภัย

บรรดามาตรการที่กำหนดขึ้น ตลอดจนการดำเนินการทั้งปวงเพื่อพิทักษ์รักษา และคุ้มครองป้องกันสิ่งที่เป็นความลับขององค์กร สินทรัพย์ และบุคลากร ให้พ้นจากการรั่วไหล การจารกรรม การบ่อนทำลาย หรือการกระทำอื่นใดที่มีผลกระทบกระเทือนหรือเป็นภัยต่อองค์กร ที่เกิดการกระทำด้วยความตั้งใจ ไม่ตั้งใจ หรือที่เกิดขึ้นเองโดยธรรมชาติ

3.2 การจัดการด้านการรักษาความปลอดภัย

กิจกรรม และวิธีการปฏิบัติที่เป็นระบบและมีการประสานงานกัน ในการที่องค์กร (ดูข้อ 3.34) สามารถบริหารความเสี่ยง (ดูข้อ 3.15) ผลกระทบ (ดูข้อ 3.23) และภัยคุกคาม (ดูข้อ 3.29) ที่อาจเกิดขึ้น

3.3 การประเมินความเสี่ยง

กระบวนการโดยรวมของการชี้บ่ง วิเคราะห์ และประเมินความเสี่ยง

หมายเหตุ *การประเมินความเสี่ยง เกี่ยวข้องกับกระบวนการในการชี้บ่งภัยคุกคาม และจุดอ่อน (ดูข้อ 3.16) ที่มีอยู่ทั้งภายใน และภายนอก การชี้บ่งโอกาสที่จะเกิดเหตุการณ์จากภัยคุกคามและจุดอ่อนนั้น การระบุถึงงานวิกฤตที่จำเป็นต่อองค์กรเพื่อสร้างความต่อเนื่องในการดำเนินการ การระบุถึงการควบคุมที่จำเป็นในการลดการแพร่กระจาย และประเมินต้นทุนที่เกิดขึ้นจากการควบคุมดังกล่าว*

3.4 การประเมินจุดอ่อน

กระบวนการในการชี้บ่งและการประมาณจุดอ่อน (ดูข้อ 3.16)

3.5 การประเมินผลกระทบ

กระบวนการในการวิเคราะห์ผลกระทบที่มีต่อสินทรัพย์ การทำงาน การบริการ สินค้า และความต่อเนื่องในการดำเนินการ (ดูข้อ 3.14)

3.6 การประเมินภาวะวิกฤต

กระบวนการที่ถูกออกแบบมา เพื่อใช้ในการชี้บ่งและประเมินความเสี่ยงของสินทรัพย์ บนพื้นฐานของพันธกิจหรือหน้าที่ต่อองค์กร กลุ่มของประชาชนที่ได้รับความเสี่ยง หรือ ความสำคัญจากการถูกขัดขวางต่อการดำเนินการอย่างต่อเนื่อง

3.7 การป้องกันอันตรายและภัยคุกคาม

กระบวนการ วิธีการปฏิบัติ เทคนิค วัสดุ ผลิตภัณฑ์ การบริการหรือทรัพยากร ที่ใช้ในการหลีกเลี่ยง ลด หรือควบคุมความเสี่ยง และภัยคุกคามทุกประเภท เพื่อลดผลกระทบทางด้านลบต่อการรักษาความปลอดภัย (ดูข้อ 3.24)

3.8 การตรวจประเมินภายใน

กระบวนการที่เป็นระบบ เป็นอิสระ และจัดทำไว้เป็นเอกสาร ที่ดำเนินการโดยองค์กรเอง เพื่อให้ได้หลักฐานการตรวจประเมิน และ ทวนสอบหลักฐานการตรวจประเมินอย่างเป็นธรรม เพื่อตัดสินว่าระบบการจัดการด้านการรักษาความปลอดภัยที่กำหนดขึ้น มีการปฏิบัติเป็นไปตามเกณฑ์การตรวจประเมิน

หมายเหตุ *ในหลายกรณีโดยเฉพาะองค์กรขนาดเล็ก ความเป็นอิสระสามารถแสดงโดยความเป็นอิสระจากหน้าที่ความรับผิดชอบสำหรับงานที่กำลังถูกตรวจประเมิน*

3.9 การปฏิบัติการแก้ไข

การปฏิบัติการขจัดสาเหตุของความไม่สอดคล้อง (ดูข้อ 3.13) ที่พบ

3.10 การปฏิบัติการป้องกัน

การขจัดสาเหตุของความไม่สอดคล้อง (ดูข้อ 3.13) ที่อาจเกิดขึ้น

3.11 การปรับปรุงอย่างต่อเนื่อง

กระบวนการที่เกิดขึ้นซ้ำ ๆ เพื่อทำให้ระบบการจัดการด้านการรักษาความปลอดภัย (ดูข้อ 3.30) ดีขึ้น ทำให้บรรลุถึงการปรับปรุงผลการดำเนินงานด้านการรักษาความปลอดภัยโดยรวม (ดูข้อ 3.25) และสอดคล้องกับนโยบายด้านการรักษาความปลอดภัย (ดูข้อ 3.17) ขององค์กร

3.12 ขั้นตอนการดำเนินงาน

วิธีการที่กำหนดในการดำเนินกิจกรรม หรือกระบวนการ

3.13 ความไม่สอดคล้อง

การไม่ปฏิบัติตามข้อกำหนด

3.14 ความต่อเนื่องในการดำเนินการ

ความสามารถเชิงกลยุทธ์และยุทธวิธีขององค์กร ในการวางแผนตอบโต้กับแต่ละเงื่อนไข สถานการณ์ และอุบัติการณ์ เพื่อให้ดำเนินการต่อไปได้อย่างต่อเนื่อง ซึ่งความสามารถเหล่านี้ ต้องได้รับการยอมรับจากฝ่ายบริหารก่อน

หมายเหตุ *ความต่อเนื่องในการดำเนินการ เป็นคำที่ใช้ทั่วไปมากกว่าความต่อเนื่องทางธุรกิจ ซึ่งใช้ได้ทั้งกับหน่วยงานที่ต้องการกำไร และกับองค์กรทุกลักษณะ เช่น องค์กรที่ไม่ใช่ภาครัฐ องค์กรที่อยู่ในความสนใจของสาธารณชน และองค์กรภาครัฐ*

3.15 ความเสี่ยง

โอกาสของการเกิดภัยคุกคาม (ดูข้อ 3.29) ด้านการรักษาความปลอดภัย ทำให้เกิดผลตามมาที่ไม่พึงประสงค์

3.16 จุดอ่อน

จุดที่ง่ายต่อการรั่วไหล การจารกรรม การก่อวินาศกรรม การบ่อนทำลาย หรืออื่น ๆ ทั้งทางกายภาพ การปฏิบัติงาน เศรษฐกิจ ธุรกิจ ความถูกต้องตามกฎหมาย และความเสียหายอื่น ๆ

3.17 นโยบายด้านการรักษาความปลอดภัย

ความมุ่งหมายและทิศทางโดยรวมขององค์กร ที่กำหนดอย่างเป็นทางการโดยผู้บริหารระดับสูง (ดูข้อ 3.21)

หมายเหตุ *นโยบายด้านการรักษาความปลอดภัยควรเกี่ยวข้องกับความปลอดภัยของสินทรัพย์ขององค์กรและแผนสำหรับการควบคุมความปลอดภัยของกระบวนการ และกิจกรรมที่เกี่ยวข้องซึ่งสอดคล้องกับนโยบายขององค์กร และ ข้อกำหนดกฎระเบียบ*

3.18 บันทึก

เอกสารซึ่งแสดงผลสำเร็จ หรือเป็นหลักฐานการดำเนินงานของกิจกรรม

3.19 เป้าหมายด้านการรักษาความปลอดภัย

รายละเอียดข้อกำหนดการปฏิบัติงาน ซึ่งใช้กับทั้งองค์กร หรือบางส่วน ซึ่งเกิดจากวัตถุประสงค์ด้านการรักษาความปลอดภัย (ดูข้อ 3.31) และความจำเป็นในการกำหนด และการทำให้สำเร็จ เพื่อให้สามารถบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัย

3.20 ผู้ตรวจประเมิน

บุคคลซึ่งมีความสามารถดำเนินการตรวจประเมิน

3.21 ผู้บริหารระดับสูง

บุคคลหรือกลุ่มบุคคล ที่เป็นผู้กำหนดทิศทางและควบคุมองค์กรในระดับสูงสุด

หมายเหตุ *ความรับผิดชอบของผู้บริหารระดับสูง ตลอดสายการบังคับบัญชาควรมีความชัดเจน*

3.22 ผู้มีส่วนเกี่ยวข้อง (ผู้มีส่วนได้ส่วนเสีย)

บุคคลที่ให้ความสนใจในการปฏิบัติงาน และผลสำเร็จ และ/หรือผลกระทบ (ดูข้อ 3.23) จากกิจกรรมขององค์กร

หมายเหตุ *ผู้มีส่วนเกี่ยวข้อง (ผู้มีส่วนได้ส่วนเสีย) รวมถึง ลูกค้า หุ้นส่วน ผู้ถือหุ้น เจ้าหน้าที่การเงิน ผู้รับทำประกัน ผู้ควบคุม หน่วยงานดูแลกฎระเบียบ พนักงาน ผู้รับเหมา ผู้ส่งมอบ องค์กรผู้ใช้แรงงาน อุปกรณ์/เครื่องมือช่วยอำนวยความสะดวก (ดูข้อ 3.38) ของผู้ที่อยู่รอบข้าง และสังคม*

3.23 ผลกระทบ

ผลลัพธ์ที่ได้ประเมินว่าจะเกิดขึ้น

3.24 ผลกระทบของการรักษาความปลอดภัย

การเปลี่ยนแปลง หรือผลลัพธ์ ไม่ว่าจะเป็นผลทางบวก หรือทางลบ บางส่วนหรือทั้งหมด ที่เป็นผลจาก หรือมีผลต่อความเสี่ยง และภัยคุกคามขององค์กร

3.25 ผลการดำเนินงานด้านการรักษาความปลอดภัย

ผลการบริหารความเสี่ยง และภัยคุกคามขององค์กร ซึ่งสามารถวัดได้

3.26 แผนงานการจัดการด้านการรักษาความปลอดภัย

วิธีการที่จะทำให้วัตถุประสงค์ และเป้าหมายด้านการรักษาความปลอดภัยประสบผลสำเร็จ ซึ่งรวมไปถึงความพร้อม การตอบรับ การผ่อนหนักให้เป็นเบา การฟื้นฟู และเหนือสิ่งอื่นใด การตระหนักและการป้องกันความเสี่ยง และภัยคุกคาม

3.27 ภาวะฉุกเฉิน

เหตุการณ์ที่เกิดขึ้นทันทีทันใด เร่งด่วน ไม่คาดคิดมาก่อน ซึ่งต้องได้รับการจัดการโดยทันที เพื่อไม่ให้ขยายตัวลุกลามจนเกิดความสูญเสียอย่างร้ายแรง

หมายเหตุ *ภาวะฉุกเฉิน มักจะเป็นอุบัติการณ์ หรือสถานการณ์ที่ยุ่งวุ่นวาย ซึ่งมักต้องคาดการณ์หรือมีการเตรียมพร้อม แต่มักจะไม่คาดคิดมาก่อน*

3.28 ภาวะวิกฤต

การปฏิบัติการและหน้าที่การทำงาน ซึ่งมีความสำคัญสูงสุดต่อองค์กร และมีความจำเป็นต่อการทำงาน อย่างมีประสิทธิผล และเพื่อป้องกันสินทรัพย์ของบุคลากร ธุรกิจ และสินทรัพย์ทางกายภาพ

3.29 ภัยคุกคาม

สถานการณ์ เหตุการณ์ หรือภาวะที่มีศักยภาพในการก่อให้เกิดความสูญเสีย หรือ อันตรายต่อชีวิตและสินทรัพย์ ซึ่งอาจจะเกิดจากการกระทำของมนุษย์ หรือ ภัยธรรมชาติ

3.30 ระบบการจัดการด้านการรักษาความปลอดภัย

ส่วนหนึ่งของระบบการบริหารงานขององค์กร ซึ่งใช้ในการกำหนดและนำนโยบายด้านการรักษาความปลอดภัย (ดูข้อ 3.17) ไปปฏิบัติ และบริหารความเสี่ยง และภัยคุกคาม ขององค์กร ซึ่งรวมถึง โครงสร้างองค์กร กิจกรรม การวางแผน การจัดสรรความรับผิดชอบ วิธีการปฏิบัติ ขั้นตอนการดำเนินงาน (ดูข้อ 3.12) กระบวนการ และทรัพยากร

3.31 วัตถุประสงค์ด้านการรักษาความปลอดภัย

เป้าหมายรวม ผลลัพธ์ หรือผลสำเร็จ ซึ่งประกอบด้วยนโยบายด้านการรักษาความปลอดภัย ที่องค์กรตั้งเป้าไว้ว่าจะต้องทำให้สำเร็จ

3.32 ศักยภาพของความสูญเสีย

การบาดเจ็บ เจ็บป่วย สินทรัพย์เสียหายที่เป็นไปได้ จากเหตุการณ์ ไม่ว่าจะมีการคาดการณ์ หรือไม่คาดการณ์ไว้ล่วงหน้า อันจะส่งผลกระทบต่อความสามารถขององค์กร ในการที่จะทำงานได้อย่างมีประสิทธิผล เป็นเหตุทำให้เกิดอันตรายอย่างรุนแรงต่อโครงสร้างพื้นฐาน และส่งผลอย่างมีนัยสำคัญต่อมนุษย์ หรือ สินทรัพย์ขององค์กร หรือต่อผู้มีส่วนเกี่ยวข้อง (ดูข้อ 3.22) หรือ ทำให้เกิดผลที่ไม่ดีต่อชื่อเสียง หรือความคงอยู่ต่อไปขององค์กรนั้น

3.33 ห่วงโซ่อุปทาน

ขั้นตอนที่เชื่อมโยงกันของทรัพยากรและกระบวนการ ซึ่งเริ่มตั้งแต่การจัดหาวัตถุดิบ และรวมไปถึงการนำส่งสินค้าหรือการบริการไปยังผู้บริโภค โดยผ่านขั้นตอนของการขนส่ง

หมายเหตุ *ห่วงโซ่อุปทาน อาจรวมถึงผู้ส่งมอบ ผู้จัดจำหน่าย อุปกรณ์/เครื่องมือช่วยอำนวยความสะดวกในการผลิต ผู้ให้บริการขนส่ง ศูนย์กระจายสินค้าภายใน ผู้กระจายสินค้า ผู้ค้าส่ง และ บุคคลอื่น ๆ ที่นำสินค้าไปสู่ ผู้บริโภคลำดับสุดท้าย*

3.34 องค์กร

บริษัท บรรษัท วิสาหกิจ องค์การ สถาบัน หรือ อาจเกิดจากการรวมตัวกันของหน่วยงานเหล่านี้ ไม่ว่าจะเป็นรัฐหรือเอกชน ที่ซึ่งมีหน้าที่การดำเนินงานและมีการบริหารจัดการเป็นของตัวเอง

หมายเหตุ *องค์กร ในที่นี้จะหมายถึง องค์กรที่เกี่ยวข้องกับกิจกรรมการจัดประชุม สัมมนา และนิทรรศการสำหรับองค์กรที่มีหน่วยงานปฏิบัติการมากกว่าหนึ่งหน่วย หน่วยงานปฏิบัติการหนึ่งหน่วยนั้นอาจถือว่าเป็นองค์กรได้*

3.35 อันตราย

แหล่งอันตราย หรือสภาพที่อาจก่อให้เกิดอันตราย ไม่ว่าจะเป็นทางกายภาพ หรือทางการดำเนินงาน ที่สามารถก่อให้เกิดผลกระทบบางอย่างในทางที่ไม่ดีได้

3.36 อุบัติการณ์

เหตุการณ์ที่ไม่พึงประสงค์ที่เกิดขึ้นแล้วมีผลให้เกิดอุบัติเหตุ หรือ เหตุการณ์เกือบเกิดอุบัติเหตุ

3.37 อุบัติเหตุ

เหตุการณ์ที่ไม่พึงประสงค์ที่เกิดขึ้นแล้วมีผลให้เกิดการบาดเจ็บ การเจ็บป่วย การเสียชีวิตและสินทรัพย์เสียหาย หรือ เกิดการหยุดชะงักของการดำเนินธุรกิจ

3.38 อุปกรณ์/เครื่องมือช่วยอำนวยความสะดวก

โรงงาน เครื่องจักร อุปกรณ์ ที่ดิน อาคาร ยานพาหนะ ระบบสารสนเทศ อุปกรณ์ที่ช่วยในการเคลื่อนย้าย และส่วนอื่น ๆ ของโครงสร้างพื้นฐาน หรือโรงงาน และระบบที่เกี่ยวข้อง ซึ่งสามารถมีการแยกแยะ และบอกปริมาณของการทำงานและการบริการได้

3.39 เอกสาร

ข้อมูล และสื่อที่เกี่ยวข้อง

หมายเหตุ *สื่อ อาจเป็นกระดาษ แม่เหล็ก อิเล็กทรอนิกส์หรือออปติคัลคอมพิวเตอร์ (electronic disc หรือ optical computer disc ภาพถ่าย หรือ ตัวอย่างมาตรฐาน หรือ สิ่งเหล่านี้รวมกัน*

4. ข้อกำหนดระบบการจัดการด้านการรักษาความปลอดภัยสำหรับการจัดประชุม สัมมนา และนิทรรศการ

4.1 ข้อกำหนดทั่วไป

องค์กรที่ดำเนินการจัดประชุม สัมมนาและนิทรรศการ ซึ่งต่อไปนี้จะเรียกว่า “องค์กร” ต้องจัดทำระบบการจัดการด้านการรักษาความปลอดภัยไว้เป็นลายลักษณ์อักษร นำไปปฏิบัติ รักษาไว้ ประเมิน และปรับปรุงระบบการจัดการอย่างต่อเนื่อง

องค์กรต้องกำหนดและจัดทำเอกสารแสดงถึงขอบข่ายของระบบการจัดการด้านการรักษาความปลอดภัยของตน ซึ่งองค์กรมีความอิสระในการกำหนดขอบข่ายดังกล่าว โดยอาจเลือกที่จะนำข้อกำหนดของมาตรฐานฉบับนี้ ไปใช้ในองค์กรทั้งหมด หรือจะใช้เฉพาะในหน่วยงานปฏิบัติการ หรือในบางกิจกรรมก็ได้ องค์กรต้องมั่นใจว่าขอบข่ายของระบบการจัดการด้านการรักษาความปลอดภัย มีความสอดคล้องกับความเชื่อมั่นสำหรับการคงอยู่ขององค์กร และการบริการ/การดำเนินงาน ความสัมพันธ์กับผู้มีส่วนเกี่ยวข้องซึ่งมีผลกระทบเกี่ยวเนื่องกับการรักษาความปลอดภัยขององค์กร รวมทั้งการจ้างหน่วยงานภายนอก (outsourcing) และห่วงโซ่อุปทาน

หมายเหตุ *ขอบข่ายของระบบการจัดการด้านการรักษาความปลอดภัยขององค์กรที่กำหนดไว้นี้ เป็นเพียงหลักเกณฑ์ขั้นต่ำสุด ในการนำมาตรฐานฉบับนี้ไปใช้งาน ซึ่งยังจะรวมถึง โครงสร้างพื้นฐาน การดำเนินงาน และกิจกรรมต่าง ๆ ที่จำเป็นที่จะทำให้องค์กรเกิดความคงอยู่และดำเนินงานได้อย่างต่อเนื่อง*

ระบบการจัดการด้านการรักษาความปลอดภัยได้รับการออกแบบมาเพื่อต้องการสร้างความมั่นใจ ว่ามีการจัดการด้านความเสี่ยงทั้งหมดและมีการปฏิบัติงานได้อย่างต่อเนื่อง ภายใต้รูปแบบการประสานงาน และการควบคุม ที่ได้มีการกำหนดไว้โดยองค์กร ระบบการจัดการด้านการรักษาความปลอดภัยต้องมีความเหมาะสมกับขนาด ความซับซ้อนและลักษณะขององค์กร โดยระบบดังกล่าวต้องให้กรอบงานสำหรับการจัดการ

ด้านความเสี่ยง และภัยคุกคาม ที่องค์กรเกี่ยวข้องได้อย่างชัดเจน ในขณะเดียวกันก็สามารถให้หลักประกันว่าการดำเนินงานจะเป็นไปอย่างต่อเนื่อง และยังช่วยทำให้องค์กรสามารถเน้นถึงจุดปฏิบัติงานที่ต้องการเปลี่ยนแปลง รวมทั้งเมื่อมีการเปลี่ยนแปลงของสภาพแวดล้อมต่าง ๆ

ระบบการจัดการด้านการรักษาความปลอดภัยจะเกิดประสิทธิผลได้ ต้องนำไปบูรณาการกับระบบการบริหารอื่น ๆ ขององค์กร โดยผู้บริหารระดับสูงและผู้บริหารระดับอื่น ๆ ต้องเข้าร่วมในการทบทวน ให้การสนับสนุน และผลักดัน

ก่อนที่จะมีการนำระบบการจัดการด้านการรักษาความปลอดภัยไปปฏิบัติ องค์กรต้องพิจารณาถึงวัตถุประสงค์การดำเนินงานในภาวะวิกฤต ที่ได้รับการชี้บ่งไว้ในยุทธศาสตร์ แผนธุรกิจ นโยบาย และเครื่องมือต่าง ๆ ที่ใช้ในการบริหาร

4.2 นโยบายด้านการรักษาความปลอดภัย

องค์กรต้องกำหนดและรักษาไว้ซึ่งนโยบาย ที่แสดงถึงความมุ่งมั่นต่อการรักษาความปลอดภัยโดยนำระบบการจัดการด้านการรักษาความปลอดภัยไปปฏิบัติ

ผู้บริหารระดับสูงต้องกำหนดนโยบายด้านการรักษาความปลอดภัยไว้เป็นเอกสาร และต้องมั่นใจว่าได้มีการชี้บ่งถึงกิจกรรมและภารกิจหลักขององค์กร รวมทั้งมีการป้องกันสินทรัพย์ที่มีความวิกฤต

นโยบายด้านการรักษาความปลอดภัย ต้อง

ก) ชี้บ่งภัยคุกคามด้านการรักษาความปลอดภัยและอันตรายต่าง ๆ ไว้อย่างเหมาะสม ตามลักษณะของกิจกรรม การบริการ และสินค้าขององค์กร และผลกระทบที่อาจจะเกิดขึ้นจากภัยคุกคามและอันตรายต่าง ๆ ดังกล่าวต่อองค์กรและบริเวณข้างเคียง

ข) แสดงความมุ่งมั่นที่จะปฏิบัติตามข้อกำหนดของกฎหมาย และข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

ค) แสดงความมุ่งมั่นที่จะดำเนินงานตามแนวปฏิบัติของวิชาชีพ และข้อกำหนดอื่น ๆ ที่องค์กรเป็นสมาชิก

ง) เป็นกรอบในการกำหนดและทบทวนวัตถุประสงค์และเป้าหมายระบบจัดการด้านการรักษาความปลอดภัยขององค์กร

จ) ปรับปรุงแผนงานด้านการรักษาความปลอดภัยและยกระดับขีดความสามารถอย่างต่อเนื่อง

ฉ) แสดงความมุ่งมั่นที่จะปรับปรุง การป้องกัน และ/หรือ การบรรเทาต่อความเสี่ยงและภัยคุกคามอย่างต่อเนื่อง

ช) จัดทำเป็นเอกสาร นำไปปฏิบัติ และรักษาไว้

ซ) สอดคล้องกับนโยบายด้านอื่น ๆ ขององค์กร

ฌ) สื่อสารให้บุคลากรทั้งหมดซึ่งทำงานให้ หรือ ในนามขององค์กรได้รับทราบถึงความสำคัญในเรื่องของการรักษาความปลอดภัย และเผยแพร่สู่สาธารณะ

4.3 การวางแผน

4.3.1 การประเมินภัยคุกคามต่อการรักษาความปลอดภัยและความเสี่ยง

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานสำหรับการชี้บ่งภัยคุกคามอันตราย การประเมินความเสี่ยง การประเมินจุดอ่อน การประเมินภาวะวิกฤต และการวิเคราะห์ผลกระทบ

องค์กรต้องใช้กระบวนการวิเคราะห์อย่างเป็นระบบเพื่อพิจารณาถึงโอกาสที่ภัยคุกคามจะเข้ามาสร้างความเสียหายต่อสินทรัพย์ บุคคล และการทำงาน กระบวนการประเมินความเสี่ยงต้องครอบคลุมถึงการประเมินภัยคุกคาม การประเมินจุดอ่อน และการประเมินภาวะวิกฤต กระบวนการวิเคราะห์และการประเมินความเสี่ยงต้องจัดทำเป็นเอกสาร

ภัยคุกคามต้องรวมถึงการกระทำที่ตั้งใจ ไม่ได้ตั้งใจ และ ภัยธรรมชาติ ที่เชื่อถือได้ว่าจะสร้างผลกระทบที่มีนัยสำคัญต่อองค์กร ผู้มีส่วนเกี่ยวข้อง ห่วงโซ่อุปทาน และ/หรือ แหล่งชุมชนโดยรวม

องค์กรต้องทำการวิเคราะห์ผลกระทบด้านการรักษาความปลอดภัยเพื่อกำหนดกรอบสำหรับการชี้บ่งและการประเมินภัยคุกคาม ความเสี่ยงด้านการรักษาความปลอดภัย รวมทั้ง การจัดการและการรักษาความปลอดภัยที่เกี่ยวข้องกับภัยคุกคามและความเสี่ยงดังกล่าวต่อไป นอกจากนี้ต้องมีการชี้บ่งถึงมาตรการควบคุม และมีการปฏิบัติตามมาตรการรักษาความปลอดภัยดังกล่าว

วิธีการที่ใช้ในการประเมินและการควบคุมภัยคุกคามด้านการรักษาความปลอดภัยและการชี้บ่งความเสี่ยงอย่างน้อยต้องมีความเหมาะสมกับลักษณะและขนาดของการดำเนินการขององค์กร การประเมินภัยคุกคามและความเสี่ยงด้านการรักษาความปลอดภัยต้องพิจารณาถึงโอกาสในการเกิดอุบัติการณ์และผลกระทบที่อาจจะเกิดขึ้นตามมาหลังจากนั้นทั้งหมด โดยต้องรวมถึงสิ่งต่าง ๆ ต่อไปนี้เป็นอย่างน้อย

ก) ความเสียหายทางกายภาพจากภัยคุกคามและความเสี่ยง ความเสียหายจากอุบัติการณ์ ความเสียหายจากการจงใจ หรือการก่อการร้าย หรือการก่ออาชญากรรม
ข) ภัยคุกคามและความเสี่ยงจากการดำเนินการ ซึ่งรวมถึงการควบคุมด้านการรักษาความปลอดภัยส่วนประกอบของร่างกาย และกิจกรรมอื่น ๆ ที่มีผลกระทบกับผลการดำเนินงาน สภาวะ หรือความปลอดภัยขององค์กร
ค) สุขภาพและความปลอดภัยของบุคคลในบริเวณ หรือพื้นที่ที่มีผลกระทบในขณะเกิดอุบัติการณ์ (การบาดเจ็บ และตาย)
ง) สุขภาพและความปลอดภัยของบุคคลที่เกี่ยวข้องกับการตอบสนองต่ออุบัติการณ์ที่เกิดขึ้น
จ) การดำเนินการอย่างต่อเนื่อง และการส่งมอบหรือการให้บริการ
ฉ) ความเสียหาย หรือการพังทลายของสินทรัพย์ อุปกรณ์/เครื่องมือช่วยอำนวยความสะดวกและโครงสร้างพื้นฐาน
ช) การคงอยู่ของห่วงโซ่อุปทาน
ซ) สิ่งแวดล้อม และเหตุการณ์ทางธรรมชาติ (พายุ น้ำท่วม เป็นต้น) ที่อาจมีผลทำให้มาตรการและอุปกรณ์ด้านการรักษาความปลอดภัยไม่มีประสิทธิผล
ฌ) สภาวะด้านเศรษฐกิจและการเงิน
ญ) ความรับผิดชอบต่อกฎหมายและข้อตกลง
ฎ) ข้อมูล การสื่อสาร และการคงอยู่ของเครือข่าย (cyber) และการรักษาความปลอดภัย
ฏ) การจัดการข้อมูลและการรักษาความปลอดภัยของเอกสาร
ฐ) ภัยคุกคามและความเสี่ยงต่อผู้มีส่วนเกี่ยวข้อง ได้แก่ ความล้มเหลวจากการไม่สามารถปฏิบัติได้ตามเกณฑ์ข้อกำหนดของกฎหมาย

ฑ) ความเสียหายต่อการเสียชื่อเสียง ความเชื่อมั่นของพนักงาน หลักประกันของลูกค้า ตราสินค้า หรือความเชื่อมั่นต่อองค์กร

องค์กรต้องมั่นใจว่าการประเมินจุดอ่อน และภาวะวิกฤต มีการพิจารณาอย่างละเอียดครอบคลุม และนำผลการประเมินไปกำหนดนโยบายและวัตถุประสงค์ด้านการรักษาความปลอดภัย และนำไปสู่การพัฒนาโปรแกรม (เช่น โปรแกรมการฝึกอบรม การดำเนินการ และการควบคุม) เพื่อสามารถ ป้องกัน ลด ควบคุม บรรเทาภัยคุกคาม และความเสี่ยง รวมทั้งผลกระทบที่จะเกิดขึ้น

องค์กรต้องจัดเก็บข้อมูลที่เกี่ยวข้องกับการประเมินภัยคุกคาม ความเสี่ยง และจุดวิกฤต ให้มีความทันสมัย รวมทั้งการเก็บรักษาความลับอย่างเหมาะสม การประเมินภัยคุกคาม ความเสี่ยง และจุดวิกฤต ต้องดำเนินการทบทวนเป็นระยะตามความเหมาะสม หรือ เมื่อมีการเปลี่ยนแปลงที่มีผลต่อสภาพแวดล้อมในการทำงาน ขั้นตอนการดำเนินงาน การทำงาน และการบริการ

4.3.2 กฎหมาย และข้อกำหนดอื่น ๆ

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงาน สำหรับ

ก) การชี้บ่ง และติดตามข้อกำหนดของกฎหมาย และข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับภัยคุกคามและความเสี่ยงด้านการรักษาความปลอดขององค์กร เช่น ภัยคุกคามและความเสี่ยงต่ออุปกรณ์/เครื่องมือช่วยอำนวยความสะดวก กิจกรรม สินค้า การบริการ ผู้รับเหมา และห่วงโซ่อุปทาน

ข) การกำหนดวิธีการและจัดทำเป็นเอกสารแสดงถึงการประยุกต์ใช้กฎหมายและข้อกำหนดอื่น ๆ กับภัยคุกคามและความเสี่ยงด้านการรักษาความปลอดภัย

องค์กรต้องเก็บรักษาข้อมูลนี้ให้มีความทันสมัย โดยต้องมีการสื่อสารข้อมูลที่เกี่ยวข้องกับกฎหมายและข้อกำหนดอื่น ๆ ให้ผู้ที่ทำงานในนามขององค์กร และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง รวมทั้งผู้รับเหมา

ระบบการจัดการด้านการรักษาความปลอดภัยต้องมุ่งมั่นดำเนินการให้สอดคล้องกับกฎหมาย กฎ ระเบียบที่เกี่ยวข้อง นโยบาย รวมทั้งพิจารณาถึงแนวทางการปฏิบัติที่ดีด้านการรักษาความมั่นคงที่เกี่ยวข้องกับกิจกรรม สินค้า และการบริการ

4.3.3 วัตถุประสงค์ เป้าหมาย และแผนงาน

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งเอกสารที่ระบุถึงวัตถุประสงค์ด้านการรักษาความปลอดภัยสำหรับการป้องกัน การบรรเทา และการฟื้นฟูจากภัยคุกคามด้านการรักษาความปลอดภัย ในทุก ๆ หน่วยงานและในทุก ๆ ระดับที่เกี่ยวข้องภายในองค์กร

องค์กรต้องชี้บ่งอันตราย ภัยคุกคามและความเสี่ยง และต้องดำเนินการป้องกันไม่ให้เกิดขึ้น

วัตถุประสงค์ และเป้าหมายด้านการรักษาความปลอดภัยต้องสามารถปฏิบัติได้ และสอดคล้องกับนโยบายด้านการรักษาความปลอดภัย รวมทั้งความมุ่งมั่นในการปรับปรุงอย่างต่อเนื่อง

ในการจัดทำและทบทวนวัตถุประสงค์ และเป้าหมาย องค์กรต้องคำนึงถึงข้อกำหนดของกฎหมาย และข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง นอกจากนี้ องค์กรต้องพิจารณาถึงความเสี่ยงและภัยคุกคามที่มีนัยสำคัญ หน่วยงานและการดำเนินงานที่มีความวิกฤต เทคโนโลยีและทางเลือกต่าง ๆ และข้อกำหนดด้านการเงิน การดำเนินงาน และทางธุรกิจขององค์กร

เป้าหมายที่องค์กรกำหนดขึ้นต้องสามารถวัดได้ มีการตอบสนองกับสภาพแวดล้อมด้านการรักษาความปลอดภัยที่มีการเปลี่ยนแปลง และมีการทบทวนตามช่วงระยะเวลาที่กำหนด

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งแผนงานเพื่อให้บรรลุวัตถุประสงค์ และเป้าหมายขององค์กรสำหรับทุก ๆ หน่วยงานและในทุก ๆ ระดับ โดยแผนงานมีการระบุถึง

ก) วิธีการ และระยะเวลาดำเนินการ

ข) การกำหนดความรับผิดชอบ และทรัพยากร

ในทางปฏิบัติ แผนงานด้านการรักษาความปลอดภัยต้องสามารถวัดได้ และสอดคล้องกับนโยบายด้านการรักษาความปลอดภัย รวมทั้งความมุ่งมั่นในการป้องกันการเกิดอุบัติการณ์ การดำเนินงานให้สอดคล้องกับกฎหมายและข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง และการปรับปรุงอย่างต่อเนื่อง

แผนงานด้านการรักษาความปลอดภัยประกอบด้วย 2 ส่วน คือ

1. แผนงานสำหรับการจัดการป้องกันและการบรรเทา
2. แผนงานสำหรับการจัดการตอบสนองและการฟื้นฟู

4.3.3.1 แผนงานสำหรับการจัดการป้องกันและการบรรเทา

แผนงานสำหรับการจัดการป้องกันและการบรรเทา ต้องสอดคล้องกับผลของการชี้บ่งภัยคุกคามและอันตรายด้านการรักษาความปลอดภัย การประเมินความเสี่ยง (โดยการใช้วิธีต่าง ๆ เช่น การวิเคราะห์ผลกระทบ การประเมินแผนงาน การทดลองปฏิบัติ เป็นต้น) แผนงานต้องช่วยให้องค์กรลดผลกระทบจากอุบัติการณ์ด้านการรักษาความปลอดภัยให้เหลือน้อยที่สุด ต้องมีแผนสำหรับการตอบสนองและได้รับการฟื้นฟูโดยรวดเร็ว

แผนงานต้องคำนึงถึงการเคลื่อนย้าย การกำจัด หรือการบรรเทาจากภัยคุกคามและอันตรายต่าง ๆ โดยการเลือกใช้วิธีการและเทคโนโลยีต่าง ๆ ทั้งนี้ให้ขึ้นอยู่กับประสบการณ์ของหน่วยงานอื่น ๆ และมีการพิจารณาถึงข้อกำหนดด้านการเงิน การดำเนินงาน และทางธุรกิจ รวมทั้งมุมมองของผู้ที่มีส่วนเกี่ยวข้อง

แผนงานสำหรับการจัดการป้องกันและการบรรเทา ต้องพิจารณาถึง

- ประโยชน์และค่าใช้จ่าย
- เทคโนโลยีที่เลือกใช้
- ผลกระทบของการรักษาความปลอดภัยและความพยายามในการรักษาความต่อเนื่องในการดำเนินการ
- ลักษณะและค่าใช้จ่ายสำหรับการดำเนินการอย่างต่อเนื่อง
- เปรียบเทียบให้เห็นถึงต้นทุนของกลยุทธ์ที่เลือกระหว่างความไม่ปลอดภัยกับการรักษาความต่อเนื่องในการดำเนินการ
- ผลตอบแทนจากการลงทุนขององค์กร

แผนงานต้องพิจารณาถึงการอพยพและเคลื่อนย้ายคน การปรับหรือการเคลื่อนย้ายสินทรัพย์ที่มีสภาพเสี่ยง การจัดหาระบบและเครื่องมือเพื่อการป้องกัน ข้อมูลข่าวสาร เอกสาร และสื่อสารด้านการรักษาความปลอดภัย จัดทำระบบการเตือนภัยคุกคามและอันตราย ขั้นตอนการสื่อสาร บุคลากรที่มีเกินความจำเป็น ระบบที่มีความวิกฤต วัสดุต่าง ๆ รวมทั้งสิ่งต่าง ๆ ที่จะหาได้จากหน่วยงานอื่น ๆ ซึ่งองค์กรได้มีการทำข้อตกลงร่วมกันไว้

แผนในการบรรเทา ต้องประกอบด้วยกิจกรรมที่มีในระหว่างเกิดเหตุการณ์ และกิจกรรมในระยะยาวเพื่อขจัดอันตราย ที่มีผลกระทบกับการรักษาความปลอดภัยขององค์กร หรือ การลดผลกระทบของอันตราย ความเสี่ยง และภัยคุกคามดังกล่าวที่ไม่สามารถขจัดออกไปได้

4.3.3.2 แผนงานสำหรับการจัดการตอบสนองและการฟื้นฟู

องค์กรต้องวางแผนสำหรับการตอบสนองกับอุบัติการณ์และโศกนาฏกรรมต่าง ๆ โดยพิจารณาถึงกิจกรรมหลัก ๆ ความรับผิดชอบต่อข้อตกลง ความต้องการต่าง ๆ ของลูกจ้างและชุมชนข้างเคียง ความต่อเนื่องของการดำเนินงาน การฟื้นฟูสภาพแวดล้อม

องค์กรต้องวางแผนเกี่ยวกับขั้นตอนในการตอบสนองไว้ล่วงหน้า เพื่อให้เกิดการบริหารงานร่วมกันและมีการนำไปปฏิบัติ ซึ่งต้องรวมถึง

1) การตอบสนองต่อภาวะฉุกเฉิน : การเข้าระงับเหตุเบื้องต้นเพื่อป้องกันบุคคลและสินทรัพย์จากอันตรายในขณะนั้น
2) การดำเนินการอย่างต่อเนื่อง: มีการจัดเตรียมกระบวนการ การควบคุม และทรัพยากรต่าง ๆ เพื่อให้มั่นใจว่าองค์กรสามารถตอบสนองต่อวัตถุประสงค์ของการดำเนินงานในภาวะวิกฤตได้
3) การฟื้นฟู: กระบวนการ ทรัพยากรต่าง ๆ และความสามารถขององค์กรที่จะนำมาใช้เพื่อให้องค์กรสามารถฟื้นกลับดำเนินการตามภารกิจขององค์กรได้ใหม่ หลังเหตุการณ์

การบริหารแผนงานสำหรับการตอบสนองและการฟื้นฟู ต้องมีองค์ประกอบทั่ว ๆ ไป อย่างน้อยต่อไปนี้

1) การกำหนดบทบาทหน้าที่ ความรับผิดชอบ ของกลุ่มคนภายในองค์กร ทุกหน่วยงาน และแต่ละบุคคล รวมถึงหน่วยงานภายนอกด้วย
2) การกำหนด สายการบังคับบัญชาและอำนาจในการสั่งการ สำหรับหน่วยงานต่าง ๆ และผู้มีหน้าที่ในแผน
3) การกำหนดความสามารถและทรัพยากรที่ต้องการ

ในการจัดทำแผนงานสำหรับการตอบสนองและการฟื้นฟู องค์กรต้องพิจารณาข้อกำหนดด้านทรัพยากรอย่างน้อยต่อไปนี้

1) บันทึกที่จำเป็น (ทั้งที่เป็นในรูปของเอกสารและในสื่ออิเล็กทรอนิกส์)
2) บัญชีรายชื่อสำหรับติดต่อพนักงานที่เกี่ยวข้อง/รับผิดชอบ
3) คู่มือขั้นตอนการดำเนินงาน
4) โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการใช้งาน รวมทั้งแผนและขั้นตอนในการฟื้นฟู
5) อุปกรณ์/เครื่องมือช่วยอำนวยความสะดวกที่ต้องใช้โดยองค์กร และมีการติดตั้งอยู่สถานที่อื่น ๆ

6) อุปกรณ์การติดต่อสื่อสาร
7) อุปกรณ์สำนักงาน
8) ระบบสาธารณูปโภค (น้ำ พลังงาน เป็นต้น)

องค์กรต้องพิจารณาขอบข่ายและลักษณะของการพึ่งพาซึ่งกันและกันกับหน่วยงานภายนอก โดยมีการกำหนดรายละเอียดของการติดต่อ และความคาดหวังของผู้มีส่วนเกี่ยวข้อง

4.4 การนำไปปฏิบัติและการดำเนินการ

4.4.1 ทรัพยากร บทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่สั่งการ

องค์กรต้องกำหนดและจัดสรรทรัพยากร และพันธมิตรที่จำเป็นอย่างเพียงพอสำหรับการปฏิบัติ และการควบคุมการจัดการด้านการรักษาความปลอดภัยและการดำเนินงานอย่างต่อเนื่อง และ การปรับปรุงประสิทธิผลการดำเนินงานอย่างต่อเนื่อง

ทรัพยากร รวมถึง ทรัพยากรบุคคล เช่น คนงานที่ปฏิบัติงานที่มีผลกระทบกับระบบการจัดการด้านการรักษาความปลอดภัย และบุคลากรที่มีความเชี่ยวชาญเฉพาะ โครงสร้างพื้นฐาน เทคโนโลยี และทรัพยากรด้านการเงิน สารสนเทศ และสินทรัพย์ทางปัญญา โดยบุคลากรต้องมีความสามารถบนพื้นฐานของการศึกษา ฝึกอบรม ความเชี่ยวชาญ และประสบการณ์

องค์กรต้องกำหนด จัดทำเป็นเอกสาร และสื่อสารให้ทราบถึงบทบาท หน้าที่ความรับผิดชอบ และอำนาจหน้าที่สั่งการ เพื่อเอื้ออำนวยให้เกิดการจัดการด้านการรักษาความปลอดภัยที่มีประสิทธิผล

ผู้บริหารระดับสูงขององค์กรต้องแต่งตั้งผู้แทนของฝ่ายบริหาร ซึ่งนอกเหนือจากความรับผิดชอบอื่น โดยกำหนดบทบาท ความรับผิดชอบ และอำนาจหน้าที่ เพื่อ

ก) ให้มั่นใจว่าข้อกำหนดและกระบวนการของระบบการจัดการด้านการรักษาความปลอดภัยได้มีการจัดทำ นำไปปฏิบัติ และรักษาไว้
ข) ประเมินและทบทวนผลการดำเนินงานของระบบการจัดการด้านการรักษาความปลอดภัย และรายงานให้ผู้บริหารระดับสูงทราบถึงการบรรลุเป้าหมาย และใช้เป็นพื้นฐานเพื่อการปรับปรุง
ค) มั่นใจว่ามีการส่งเสริมทั่วทั้งองค์กรให้ตระหนักถึงข้อกำหนดของการจัดการด้านการรักษาความปลอดภัย

องค์กรต้องสร้างขีดความสามารถในการสนับสนุนการรักษาความปลอดภัยให้สามารถดำเนินการได้อย่างต่อเนื่องโดยไม่ขาดแคลนในเรื่อง กำลังคน เครื่องมือ อุปกรณ์ อาหารและเครื่องดื่ม โดยจัดทำขั้นตอนการดำเนินงานสำหรับการสนับสนุนภายใต้ขอบข่ายของ

- การจัดตั้งคลังพัสดุ
- การรับสิ่งของ วัสดุ อุปกรณ์
- การจัดเก็บ
- การแจกจ่าย
- การดูแลรักษา
- การทดสอบ
- การบริการ บุคลากร ทรัพยากร วัสดุ และ อุปกรณ์/เครื่องมือช่วยอำนวยความสะดวกที่ทำขึ้นหรือได้รับการบริจาคเพื่อสนับสนุนระบบการจัดการด้านการรักษาความปลอดภัย

ในการจัดการด้านทรัพยากร อย่างน้อยต้องพิจารณาถึงหัวข้อต่อไปนี้

ก) บุคลากร เครื่องมือ การฝึกอบรม อุปกรณ์/เครื่องมือช่วยอำนวยความสะดวก เงินลงทุน ความรู้ความชำนาญ วัสดุ และกรอบเวลาที่องค์กรกำหนด

ข) ปริมาณ ระยะเวลาการตอบสนอง ขีดความสามารถ ข้อจำกัด ค่าใช้จ่าย และความรับผิดต่าง ๆ ที่เกี่ยวข้องกับการใช้ทรัพยากร

ค) ข้อตกลงร่วมกันในด้านการให้ความช่วยเหลือระหว่างหน่วยงาน และชุมชน

4.4.2 ความสามารถ การฝึกอบรม และความตระหนัก

องค์กรต้องมั่นใจว่าบุคลากรที่ปฏิบัติงานให้องค์กร หรือทำงานในนามขององค์กร ที่มีโอกาสในการป้องกันก่อให้เกิด ตอบสนอง บรรเทา หรือมีผลกระทบต่อการรักษาความปลอดภัยที่ได้มีการชี้บ่งโดยองค์กรว่ามีนัยสำคัญ มีความสามารถบนพื้นฐานอย่างเหมาะสมของการศึกษา การฝึกอบรม ทักษะ และประสบการณ์

องค์กรต้องชี้บ่งความจำเป็นของการฝึกอบรมที่เกี่ยวข้องกับภัยคุกคามและความเสี่ยงด้านการรักษาความปลอดภัย องค์กรต้องวางแผน และจัดการฝึกอบรม หรือดำเนินการอื่นใดเพื่อตอบสนองความจำเป็นที่ต้องการการฝึกอบรม และเก็บรักษาบันทึกของความสามารถและการฝึกอบรมไว้

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานเพื่อให้มั่นใจว่าบุคลากรที่ปฏิบัติงานให้องค์กร หรือในนามขององค์กรมีความตระหนักถึง

ก) ความสำคัญของการปฏิบัติตามนโยบายด้านการรักษาความปลอดภัย ขั้นตอนการดำเนินงาน และข้อกำหนดอื่น ๆ ของระบบการจัดการด้านการรักษาความปลอดภัย

ข) ภัยคุกคามและความเสี่ยงที่มีนัยสำคัญ และผลกระทบที่เกี่ยวข้องทั้งที่เกิดขึ้นจริง หรืออาจจะเกิดขึ้นที่เกี่ยวข้องกับงาน และประโยชน์ที่เกิดขึ้นต่อการรักษาความปลอดภัยเมื่อมีการปรับปรุงผลการปฏิบัติงาน

ค) บทบาท และหน้าที่ความรับผิดชอบในการบรรลุผลสำเร็จของการปฏิบัติตามข้อกำหนดของระบบการจัดการด้านการรักษาความปลอดภัย

ง) ขั้นตอนการดำเนินงานสำหรับการป้องกันตนเองและการอพยพ

จ) ขั้นตอนการดำเนินงานสำหรับการตอบสนองต่อภาวะฉุกเฉินและการฟื้นฟู

ฉ) ผลสืบเนื่องที่อาจจะเกิดขึ้นจากการไม่ปฏิบัติตามขั้นตอนการดำเนินงานที่กำหนดไว้

4.4.3 การติดต่อสื่อสาร และการเตือนภัย

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงาน ที่พิจารณาถึงข้อกำหนดสำหรับสภาวะปกติและภาวะฉุกเฉิน สำหรับ

ก) การติดต่อสื่อสารภายในระหว่างระดับ และสายงานต่าง ๆ ขององค์กร

ข) การรับเรื่อง การทำเป็นเอกสาร และการตอบสนองต่อการติดต่อสื่อสารที่เกี่ยวข้องจากผู้มีส่วนเกี่ยวข้อง

ค) การรับเอาข้อมูลการเตือนภัยจากหน่วยงานของรัฐในระดับชาติ ระดับภูมิภาค หรือระดับท้องถิ่นมาปรับใช้กับระบบการจัดการด้านการรักษาความปลอดภัยขององค์กร

ง) การเตือนภัยให้ประชาชนทั้งภายในและภายนอกที่อาจได้รับผลกระทบจากอุบัติการณ์ที่เกิดขึ้นจริงหรือที่อาจจะเกิดขึ้นให้มีการตื่นตัวและเปลี่ยนแปลงไปสู่ระบบการจัดการด้านการรักษาความปลอดภัยต่อไป

จ) จัดตั้งระบบสื่อสารเพื่อใช้ในการควบคุมภาวะฉุกเฉิน

ฉ) สร้างช่องทางสำหรับการสื่อสารให้มั่นใจว่ามีช่องทางในการสื่อสารที่สามารถใช้การได้อย่างพอเพียง โดยให้ความสำคัญกับช่องทางที่จำเป็นต้องใช้ในสภาวะวิกฤต

องค์กรต้องตัดสินใจสำหรับการสื่อสารข้อมูลเกี่ยวกับความเสี่ยงและภัยคุกคามที่มีนัยสำคัญขององค์กรสู่ภายนอก และจัดทำผลการตัดสินใจขององค์กรไว้เป็นเอกสาร องค์กรต้องกำหนดวิธีการสำหรับการติดต่อสื่อสารสู่ภายนอก อย่างไรก็ตาม กรณีข้อมูลที่มีการสื่อสารออกสู่ภายนอกหากเป็นข้อมูลที่มีความอ่อนไหวต้องมีการรักษาความลับไว้ ข้อมูลที่ไม่มีความอ่อนไหวเท่านั้นที่สามารถเผยแพร่ต่อสาธารณชน

ระบบการสื่อสารการจัดการด้านการรักษาความปลอดภัยต้องมีการทดสอบตามช่วงเวลาที่กำหนด

4.4.4 การจัดทำเอกสาร

องค์กรต้องจัดทำและรักษาไว้ซึ่งเอกสารต่าง ๆ สำหรับระบบการจัดการด้านการรักษาความปลอดภัยซึ่งต้องประกอบด้วย

ก) นโยบาย วัตถุประสงค์ และเป้าหมายด้านการรักษาความปลอดภัย

ข) การอธิบายขอบข่ายของระบบการจัดการด้านการรักษาความปลอดภัย

ค) การอธิบายหัวข้อสำคัญของระบบการจัดการด้านการรักษาความปลอดภัย และความสัมพันธ์ซึ่งกันและกัน และอ้างอิงไปถึงเอกสารที่เกี่ยวข้อง

ง) เอกสาร รวมทั้งบันทึกที่เกี่ยวกับการประเมินความเสี่ยง ภัยคุกคาม และภาวะวิกฤต ที่กำหนดโดยมาตรฐานฉบับนี้ และ

จ) เอกสาร รวมทั้งบันทึกที่ถูกกำหนดโดยองค์กรว่าจำเป็น เพื่อให้มั่นใจถึงประสิทธิผลของการวางแผน การปฏิบัติการ และการควบคุมกระบวนการที่สัมพันธ์กับประเด็นการรักษาความปลอดภัยที่มีนัยสำคัญ

4.4.5 การควบคุมเอกสาร

เอกสารที่จัดทำขึ้นสำหรับระบบการจัดการด้านการรักษาความปลอดภัย และที่กำหนดโดยมาตรฐานฉบับนี้ต้องได้รับการควบคุม บันทึกเป็นรูปแบบเฉพาะของเอกสารและต้องถูกควบคุมในข้อกำหนดที่ 4.4.6

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงาน สำหรับการควบคุมเอกสาร รวมทั้งข้อมูลและเอกสารสนับสนุนต่าง ๆ ที่ได้มีการเก็บรวบรวมไว้ในรูปแบบของสื่อต่าง ๆ เพื่อ

ก) กำหนดวิธีการในการออกเอกสาร การแก้ไข การทบทวนและการรับรองเอกสารโดยผู้มีอำนาจหน้าที่ตามที่กำหนดไว้

ข) ทบทวน และปรับปรุงให้ทันสมัยอยู่เสมอตามความจำเป็น และอนุมัติเอกสารฉบับใหม่

ค) มั่นใจว่าการเปลี่ยนแปลง และสถานะของเอกสารฉบับล่าสุด ได้รับการชี้บ่งไว้

ง) มั่นใจว่าเอกสารฉบับที่เกี่ยวข้องที่สามารถประยุกต์ใช้ได้อยู่ในจุดที่ใช้งาน

จ) มั่นใจว่าเอกสารยังคงอ่านง่าย และสามารถบ่งชี้ได้อย่างชัดเจน

ฉ) มั่นใจว่าเอกสารที่รับมาจากภายนอกที่ถูกกำหนดโดยองค์กรว่าจำเป็นสำหรับการวางแผน และการดำเนินงานของระบบการจัดการด้านการรักษาความปลอดภัยได้รับการชี้บ่ง และมีการควบคุมการแจกจ่าย

ช) ป้องกันการใช้เอกสารที่ถูกยกเลิกการใช้งานแล้วโดยไม่ตั้งใจ และมีการใช้การชี้บ่งที่เหมาะสมกับเอกสารเหล่านี้เพื่อเก็บรักษาไว้สำหรับจุดประสงค์ใด ๆ

4.4.6 การควบคุมบันทึก

องค์กรต้องจัดทำ และรักษาไว้ซึ่งบันทึกที่จำเป็นในการแสดงความสอดคล้องกับข้อกำหนดของระบบการจัดการด้านการรักษาความปลอดภัยขององค์กร และของมาตรฐานฉบับนี้ และผลสำเร็จที่ได้บรรลุผลแล้ว

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานสำหรับการบ่งชี้ การจัดเก็บ การป้องกัน การเรียกใช้ กำหนดระยะเวลาการจัดเก็บ และการทำลายบันทึก

บันทึกต้องสามารถอ่านได้อย่างชัดเจน สามารถบ่งชี้ได้ และ สามารถติดตามสอบกลับได้ และต้องมีการสำรองข้อมูลอิเล็กทรอนิกส์ และการเข้าถึงข้อมูลเฉพาะผู้ที่มีอำนาจเท่านั้น

4.4.7 การควบคุมการปฏิบัติงาน

องค์กรต้องจัดทำ และนำไปปฏิบัติซึ่งเอกสารขั้นตอนการดำเนินงาน และมีการควบคุมเพื่อให้สอดคล้องกับนโยบาย การประเมินภัยคุกคาม ความเสี่ยงและภาวะวิกฤต วัตถุประสงค์และเป้าหมาย

องค์กรต้องวางแผนสำหรับการดำเนินการเหล่านี้ รวมทั้งการสอบเทียบ และ/หรือ การทวนสอบอุปกรณ์และการซ่อมบำรุง เพื่อให้มั่นใจว่ามีการดำเนินงานภายใต้สภาวะที่กำหนด โดย

ก) จัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานเป็นเอกสารเพื่อควบคุมสถานการณ์ที่อาจจะเบี่ยงเบนไปจากนโยบาย วัตถุประสงค์ และเป้าหมายด้านการรักษาความปลอดภัย

ข) กำหนดเกณฑ์การปฏิบัติไว้ในขั้นตอนการดำเนินงาน

ค) จัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานที่เกี่ยวข้องกับความเสี่ยง ภัยคุกคาม และอันตราย ที่ได้รับการชี้บ่งว่ามีนัยสำคัญต่อองค์กร และมีการสื่อสารขั้นตอนการดำเนินงาน และข้อกำหนดที่เกี่ยวข้องให้กับผู้ที่อยู่ในห่วงโซ่อุปทาน รวมทั้งผู้รับเหมาให้ได้รับทราบ

ขั้นตอนการดำเนินงานต้องครอบคลุมถึงการควบคุมการออกแบบ การติดตั้ง การดำเนินงาน การตกแต่ง และการปรับปรุงการรักษาความปลอดภัยที่เกี่ยวข้องกับชิ้นส่วนของอุปกรณ์ เครื่องมือ และการสอบเทียบหรือทวนสอบ เป็นต้น ในกรณีที่การจัดเตรียมการที่มีการเปลี่ยนแปลง หรือมีการจัดเตรียมการขึ้นใหม่ที่มีผลกระทบต่อการรักษาความปลอดภัย องค์กรต้องพิจารณาถึงภัยคุกคาม และความเสี่ยงที่เกี่ยวข้องกับการรักษาความปลอดภัยก่อนที่จะนำไปปฏิบัติ

ขั้นตอนการดำเนินงานและการควบคุมต้องระบุถึงความน่าเชื่อถือ และการดำเนินงานได้อย่างต่อเนื่อง ความปลอดภัยและสุขภาพของประชาชน และการปกป้องสินทรัพย์ และสภาพแวดล้อมที่อาจจะมีผลกระทบจากอุบัติการณ์ด้านการรักษาความปลอดภัย

4.4.8 การเตรียมพร้อมต่ออุบัติการณ์และการตอบสนอง

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานสำหรับการเตรียมความพร้อมต่ออุบัติการณ์ที่มีการชี้บ่งไว้และสำหรับการบรรเทา การตอบสนอง และการฟื้นฟู ต่อสถานการณ์ฉุกเฉินที่มีโอกาสจะเกิดขึ้น และจากการประเมินความเสี่ยง ภัยคุกคาม จุดอ่อน และภาวะวิกฤต

องค์กรต้องทบทวน และปรับปรุงขั้นตอนการดำเนินงานสำหรับการเตรียมพร้อมต่ออุบัติการณ์ และการตอบสนองขององค์กรเป็นระยะ ๆ เมื่อจำเป็น โดยเฉพาะอย่างยิ่งภายหลังจากการเกิดอุบัติการณ์ด้านการรักษาความปลอดภัย

องค์กรต้องทดสอบขั้นตอนการดำเนินงานตามช่วงเวลาที่กำหนด รวมทั้งการสื่อสารวิธีการ และการเตรียมแผนรองรับ ทดลองปฏิบัติตามแผนหากทำได้ และให้ข้อแนะนำสำหรับการตอบสนองต่อภาวะฉุกเฉินให้ลูกจ้าง และผู้ที่ทำงานในนามขององค์กร รวมทั้งผู้มีส่วนเกี่ยวข้องด้วย

องค์กรต้องตอบโต้ต่อภัยคุกคามที่เกิดขึ้นจริง อุบัติการณ์ด้านการรักษาความปลอดภัย สถานการณ์ที่เป็นผลจากภาวะฉุกเฉิน และการป้องกัน หรือการบรรเทาผลกระทบที่เป็นความเสียหายจากการรักษาความปลอดภัย

4.5 การตรวจสอบและการปฏิบัติการแก้ไข

4.5.1 การเฝ้าติดตามและการวัดผล

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานเพื่อใช้ในการเฝ้าติดตามและการวัดผลตามช่วงระยะเวลาที่กำหนดไว้สำหรับคุณลักษณะที่สำคัญของการดำเนินงานซึ่งมีผลกระทบที่มีนัยสำคัญต่อการรักษาความปลอดภัย หรือที่มีผลกระทบต่อระบบการจัดการด้านการรักษาความปลอดภัย

ขั้นตอนการดำเนินงานต้องประกอบด้วยการจัดทำเอกสารที่เป็นข้อมูลในการเฝ้าติดตามตรวจสอบผลการปฏิบัติงาน การควบคุมการปฏิบัติงานที่เกี่ยวข้อง และความสอดคล้องกับวัตถุประสงค์ และเป้าหมายด้านการรักษาความปลอดภัยขององค์กร

องค์กรต้องมั่นใจว่ามีการนำเครื่องมือที่ได้รับการสอบเทียบ และ/หรือได้รับการทวนสอบไปใช้ในการเฝ้าติดตาม และการวัดผล และมีการรักษาเครื่องมือ รวมทั้งต้องเก็บรักษาบันทึกที่เกี่ยวข้องไว้

4.5.2 การประเมินระบบ

องค์กรต้องประเมินแผนงานการจัดการด้านการรักษาความปลอดภัย ขั้นตอนการดำเนินงาน และขีดความสามารถ โดยการทบทวนตามช่วงระยะเวลา การทดสอบ รายงานที่จัดทำขึ้นภายหลังเกิดอุบัติการณ์ การเรียนรู้จากบทเรียน การประเมินผลการดำเนินงานและการทดลองปฏิบัติ ซึ่งการเปลี่ยนแปลงที่มีนัยสำคัญจากปัจจัยต่าง ๆ เหล่านี้ ต้องนำไปสู่การจัดทำเป็นขั้นตอนการดำเนินงานอย่างทันท่วงที

ในความมุ่งมั่นให้เกิดความสอดคล้อง องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานในการประเมินความสอดคล้องกับข้อกำหนดของกฎหมาย แนวทางการปฏิบัติที่ดี และความสอดคล้องกับนโยบายและวัตถุประสงค์ขององค์กร

องค์กรต้องจัดเก็บบันทึกผลการประเมินที่มีการดำเนินการตามช่วงระยะเวลาที่กำหนดไว้ ผลที่เกิดขึ้นจากการประเมินต้องนำเสนอสู่การทบทวนของฝ่ายบริหาร

4.5.3 ความไม่สอดคล้อง การปฏิบัติการแก้ไข และการปฏิบัติการป้องกัน

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงาน สำหรับการจัดการกับความไม่สอดคล้องที่เกิดขึ้นจริง และที่มีแนวโน้มว่าจะเกิดขึ้น และเพื่อดำเนินการปฏิบัติการแก้ไข และการปฏิบัติการป้องกัน ขั้นตอนการดำเนินงานจะต้องระบุข้อกำหนดสำหรับ

ก) ระยะเวลาในการตอบสนองมีความเหมาะสมกับจุดอ่อนและภาวะวิกฤตที่พบ

ข) การชี้บ่ง และการแก้ไขสิ่งที่ไม่เป็นไปตามข้อกำหนด และดำเนินการปฏิบัติงานเพื่อลดผลกระทบต่อการรักษาความปลอดภัย

ค) การสอบสวนการไม่เป็นไปตามข้อกำหนดเพื่อพิจารณาหาสาเหตุของการไม่เป็นไปตามข้อกำหนด และดำเนินการปฏิบัติงานเพื่อหลีกเลี่ยงการไม่เป็นไปตามข้อกำหนดซ้ำอีก

ง) การประเมินความจำเป็นสำหรับการปฏิบัติงานเพื่อป้องกันการไม่เป็นไปตามข้อกำหนด และดำเนินการปฏิบัติงานอย่างเหมาะสม เพื่อหลีกเลี่ยงการไม่เป็นไปตามข้อกำหนดขึ้น

จ) การบันทึกผลของการปฏิบัติการแก้ไข และการปฏิบัติการป้องกันที่ได้ดำเนินการไป

ฉ) การทบทวนประสิทธิผลของการปฏิบัติการแก้ไข และการปฏิบัติการป้องกันที่ได้ดำเนินการไป

การปฏิบัติงานที่ได้ดำเนินการไปแล้วต้องเหมาะสมกับขนาดของปัญหา และผลกระทบต่อระบบการรักษาความปลอดภัยที่เกิดขึ้น และภายในกรอบระยะเวลาที่กำหนดไว้

องค์กรต้องมั่นใจว่าการเปลี่ยนแปลงใด ๆ ที่จำเป็นได้รับการดำเนินการในการจัดทำเอกสารของระบบการจัดการด้านการรักษาความปลอดภัย

4.5.4 การตรวจประเมินภายใน

องค์กรต้องมั่นใจว่าการตรวจประเมินภายในของระบบการจัดการด้านการรักษาความปลอดภัยได้รับการดำเนินการตามช่วงเวลาที่ได้วางแผนไว้ เพื่อ

ก) พิจารณาว่าระบบการจัดการด้านการรักษาความปลอดภัย

1) เป็นไปตามแผนสำหรับการจัดการด้านการรักษาความปลอดภัย รวมทั้งข้อกำหนดของมาตรฐานหรือไม่

2) ดำเนินการ และรักษาไว้อย่างถูกต้องหรือไม่

ข) รายงานข้อมูลที่เป็นผลของการตรวจประเมินให้ผู้บริหารทราบ

องค์กรต้องการวางแผน จัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งโปรแกรมการตรวจประเมิน โดยการพิจารณาถึงความสำคัญของการปฏิบัติงานด้านการรักษาความปลอดภัยที่เกี่ยวข้อง และผลการตรวจประเมินครั้งที่ผ่านมา

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานซึ่งระบุถึงหน้าที่ความรับผิดชอบและข้อกำหนดในการวางแผน และการดำเนินการตรวจประเมิน การรายงานผล และการเก็บรักษาบันทึกที่เกี่ยวข้องไว้ และการกำหนดเกณฑ์ ขอบข่าย ความถี่ และวิธีการตรวจประเมิน

การคัดเลือกผู้ตรวจประเมินและการตรวจประเมินต้องมั่นใจว่ากระบวนการตรวจประเมินมีความเป็นธรรม (objectivity) และ ไม่ลำเอียง (impartiality)

4.6 การทบทวนการจัดการ

ผู้บริหารระดับสูงต้องทบทวนระบบการจัดการด้านการรักษาความปลอดภัยขององค์กรตามช่วงระยะเวลาที่ได้วางแผนไว้ เพื่อให้มั่นใจว่าระบบการจัดการยังคงมีความเหมาะสม เพียงพอ และมีประสิทธิผลอย่างต่อเนื่อง

การทบทวนต้องรวมถึงการประเมินโอกาสเพื่อการปรับปรุง และความจำเป็นในการเปลี่ยนแปลงระบบการจัดการด้านการรักษาความปลอดภัย รวมทั้งนโยบาย วัตถุประสงค์ และเป้าหมายด้านการรักษาความปลอดภัย

บันทึกของการทบทวนการจัดการต้องมีการเก็บรักษาไว้

ปัจจัยนำเข้าสู่การทบทวนการจัดการอย่างน้อยต้องรวมถึง

ก) ผลการตรวจประเมินภายใน และ ความสอดคล้องกับข้อกำหนดของกฎหมาย และข้อกำหนดอื่น ๆ ที่องค์กรเกี่ยวข้อง

ข) การติดต่อสื่อสารจากหน่วยงานที่มีส่วนได้ส่วนเสีย รวมทั้งข้อร้องเรียน

ค) ประสิทธิผลการปฏิบัติงานด้านการรักษาความปลอดภัยขององค์กร

ง) การบรรลุวัตถุประสงค์และเป้าหมาย

จ) สถานะของการปฏิบัติการแก้ไข และการป้องกัน

ฉ) การติดตามผลการปฏิบัติงานจากการทบทวนการจัดการครั้งที่ผ่านมา

ช) การเปลี่ยนแปลงของภัยคุกคาม แหล่งอันตราย รวมทั้งการเปลี่ยนแปลงของกฎหมาย และข้อกำหนดอื่น ๆ ที่เกี่ยวข้องกับความเสี่ยงภัย ภัยคุกคาม และอันตรายด้านการรักษาความปลอดภัย

ซ) ข้อเสนอแนะเพื่อการปรับปรุง

ผลจากการทบทวนการจัดการต้องรวมถึงการตัดสินใจ และการดำเนินการใด ๆ ซึ่งเกี่ยวข้องกับการเปลี่ยนแปลงนโยบาย วัตถุประสงค์ เป้าหมายด้านการรักษาความปลอดภัย และองค์ประกอบอื่น ๆ ของระบบการจัดการด้านการรักษาความปลอดภัยที่อาจเป็นไปได้ ซึ่งสอดคล้องกับความมุ่งมั่นในการปรับปรุงอย่างต่อเนื่อง