

## ประกาศกระทรวงอุตสาหกรรม

ฉบับที่ ๔๕๖๓ (พ.ศ. ๒๕๕๖)

ออกตามความในพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม

พ.ศ. ๒๕๑๑

เรื่อง ยกเลิกและกำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรม

ระบบการบริหารความต่อเนื่องทางธุรกิจ - ข้อกำหนด

โดยที่เป็นการสมควรแก้ไขปรับปรุงมาตรฐานผลิตภัณฑ์อุตสาหกรรม ระบบการบริหารความต่อเนื่องทางธุรกิจ - ข้อกำหนด มาตรฐานเลขที่ มอก. 22301 - 2553

อาศัยอำนาจตามความในมาตรา ๑๕ แห่งพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม พ.ศ. ๒๕๑๑ รัฐมนตรีว่าการกระทรวงอุตสาหกรรมออกประกาศยกเลิกประกาศกระทรวงอุตสาหกรรม ฉบับที่ ๔๑๖๖ (พ.ศ. ๒๕๕๓) ออกตามความในพระราชบัญญัติมาตรฐานผลิตภัณฑ์อุตสาหกรรม พ.ศ. ๒๕๑๑ เรื่อง กำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรม ระบบการบริหารความต่อเนื่องทางธุรกิจ - ข้อกำหนด ลงวันที่ ๙ กุมภาพันธ์ พ.ศ. ๒๕๕๓ และออกประกาศกำหนดมาตรฐานผลิตภัณฑ์อุตสาหกรรม ระบบการบริหารความต่อเนื่องทางธุรกิจ - ข้อกำหนด มาตรฐานเลขที่ มอก. 22301 - 2556 ขึ้นใหม่ ดังมีรายละเอียดต่อท้ายประกาศนี้

ทั้งนี้ ให้มีผลตั้งแต่วันประกาศในราชกิจจานุเบกษา เป็นต้นไป

ประกาศ ณ วันที่ ๒ สิงหาคม พ.ศ. ๒๕๕๖

ประเสริฐ บุญชัยสุข

รัฐมนตรีว่าการกระทรวงอุตสาหกรรม

# มาตรฐานผลิตภัณฑ์อุตสาหกรรม

## ระบบการบริหารความต่อเนื่องทางธุรกิจ –

### ข้อกำหนด

#### 0. บทนำ

##### 0.1 ทัวไป

มาตรฐานนี้ระบุข้อกำหนดสำหรับการจัดทำและการจัดการระบบการบริหารความต่อเนื่องทางธุรกิจ (BCMS) ได้อย่างมีประสิทธิภาพ

ระบบการบริหารความต่อเนื่องทางธุรกิจ มุ่งเน้นถึงความสำคัญเกี่ยวกับ

- ก) ความเข้าใจถึงความต้องการและความจำเป็นขององค์กรในการกำหนดนโยบายและวัตถุประสงค์สำหรับการบริหารความต่อเนื่องทางธุรกิจ
- ข) การนำไปปฏิบัติและการควบคุมการดำเนินการ และการวัดขีดความสามารถขององค์กรโดยรวมในการจัดการกับอุบัติการณ์ที่ทำให้เกิดการหยุดชะงัก
- ค) การเฝ้าระวัง และทบทวนสมรรถนะและประสิทธิผลของระบบการบริหารความต่อเนื่องทางธุรกิจ
- ง) การปรับปรุงอย่างต่อเนื่องบนพื้นฐานจากการวัดผลตามวัตถุประสงค์

เช่นเดียวกับระบบบริหารงานอื่นๆ ระบบการบริหารความต่อเนื่องทางธุรกิจมีองค์ประกอบหลักที่สำคัญดังต่อไปนี้

- ก) นโยบาย
- ข) การกำหนดหน้าที่ความรับผิดชอบของบุคลากร
- ค) กระบวนการในการจัดการที่เกี่ยวข้องกับ
  - 1) นโยบาย
  - 2) การวางแผน
  - 3) การนำไปปฏิบัติและการดำเนินการ
  - 4) การประเมินสมรรถนะ

5) การทบทวนการบริหารงาน

6) การปรับปรุง

ง) เอกสารหลักฐานที่สามารถตรวจประเมินได้

จ) กระบวนการบริหารความต่อเนื่องทางธุรกิจใดๆ ที่เกี่ยวข้องกับองค์กร

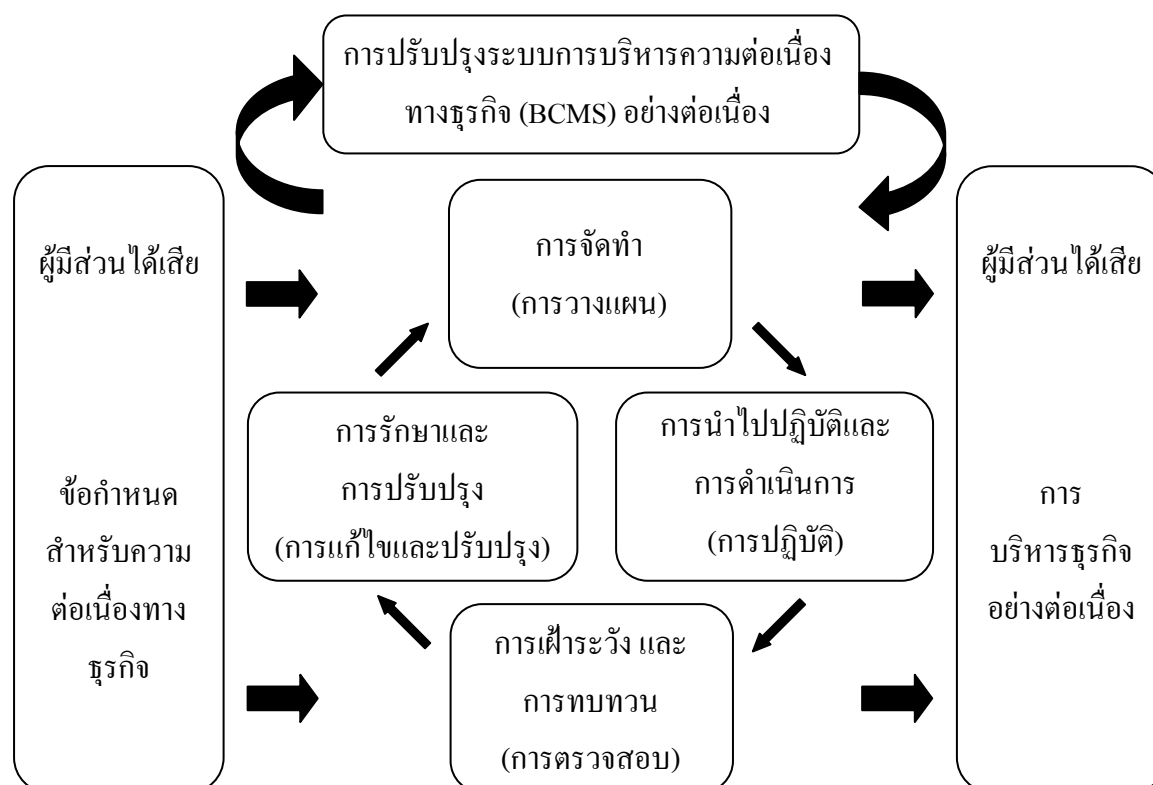
ความต่อเนื่องทางธุรกิจมีส่วนช่วยทำให้สังคมกลับคืนสู่สภาพเดิมได้เร็วยิ่งขึ้น (resilient society) กระบวนการฟื้นฟูอาจจำเป็นต้องมีส่วนเกี่ยวข้องกับชุมชนที่กว้างขวางมากขึ้น รวมถึงผลกระทบของสภาพแวดล้อมขององค์กรต่อองค์กรเองและองค์กรอื่นๆ ดังนั้นทั้งองค์กรเองและองค์กรอื่นๆ อาจมีความจำเป็นในการเข้ามามีส่วนร่วมในกระบวนการฟื้นฟูด้วย

## 0.2 รูปแบบวงจร Plan-Do-Check-Act (PDCA)

มาตรฐานนี้ประยุกต์ใช้รูปแบบ “การวางแผน (Plan) – การปฏิบัติ (Do) – การตรวจสอบ (Check) – การแก้ไขและปรับปรุง (Act)” (PDCA Model) เพื่อการวางแผน การจัดทำ การนำไปปฏิบัติ การดำเนินการ การเฝ้าระวัง การทบทวน การรักษา และการปรับปรุงประสิทธิผลของระบบการบริหารความต่อเนื่องทางธุรกิจขององค์กรอย่างต่อเนื่อง

รูปแบบวงจรนี้ทำให้มั่นใจว่ามีความสอดคล้องกับมาตรฐานระบบบริหารงานอื่นๆ เช่น มอก.9001 ระบบบริหารงานคุณภาพ มอก.14001 ระบบการจัดการสิ่งแวดล้อม ISO/IEC 27001 ระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ISO/IEC 20000-1 เทคโนโลยีสารสนเทศ – การบริหารงานบริการ และ ISO 28000 – ข้อกำหนดสำหรับระบบการจัดการความปลอดภัยสำหรับห่วงโซ่อุปทาน ดังนั้นจึงช่วยในการนำไปปฏิบัติและการดำเนินการแบบบูรณาการกับระบบบริหารงานอื่นๆ ที่เกี่ยวข้อง

รูปที่ 1 แสดงให้เห็นถึงระบบการบริหารความต่อเนื่องทางธุรกิจ ที่มีการใช้ปัจจัยนำเข้า (input) จากผู้มีส่วนได้เสีย รวมทั้งข้อกำหนดสำหรับความต่อเนื่องทางธุรกิจ โดยผ่านการดำเนินการและกระบวนการที่จำเป็นเพื่อทำให้เกิดผลลัพธ์ของความต่อเนื่องที่เป็นไปตามข้อกำหนด (เช่น การบริหารธุรกิจอย่างต่อเนื่อง)



รูปที่ 1 รูปแบบ PDCA ที่นำมาประยุกต์ใช้กับกระบวนการของระบบการบริหารความต่อเนื่องทางธุรกิจ

ตารางที่ 1 คำอธิบายของรูปแบบ PDCA

|                                                   |                                                                                                                                                                                                                                               |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| การวางแผน<br>(การจัดทำ)                           | จัดทำนโยบายความต่อเนื่องทางธุรกิจ วัตถุประสงค์ เป้าหมาย การควบคุม กระบวนการ และขั้นตอนการดำเนินงานที่เกี่ยวข้องสำหรับการปรับปรุงความต่อเนื่องทางธุรกิจ เพื่อช่วยให้ได้ผลลัพธ์ที่เป็นไปในแนวทางเดียวกันกับนโยบายและวัตถุประสงค์โดยรวมขององค์กร |
| การปฏิบัติ<br>(การนำไปปฏิบัติและ<br>การดำเนินการ) | นำไปปฏิบัติและดำเนินการตามนโยบาย การควบคุม กระบวนการ และขั้นตอนการดำเนินงานความต่อเนื่องทางธุรกิจ                                                                                                                                             |
| การตรวจสอบ<br>(การเฝ้าระวังและการทบทวน)           | เฝ้าระวังและทบทวนสมรรถนะเทียบกับนโยบายและวัตถุประสงค์ รายงานผลลัพธ์ต่อฝ่ายบริหารเพื่อทบทวน และพิจารณาและสั่งให้ดำเนินการเพื่อการฟื้นฟูและการปรับปรุง                                                                                          |
| การแก้ไขและปรับปรุง<br>(การรักษาและการปรับปรุง)   | รักษาและปรับปรุงระบบการบริหารความต่อเนื่องทางธุรกิจโดยใช้การปฏิบัติการแก้ไขบนพื้นฐานของผลการตัดสินใจจากการทบทวน การบริหารงาน และการทบทวนขอบข่ายของระบบการบริหารความต่อเนื่องทางธุรกิจ และนโยบายและวัตถุประสงค์ความต่อเนื่องทางธุรกิจ          |

0.3 องค์ประกอบของ PDCA ในมาตรฐานนี้

ในรูปแบบวงจร Plan-Do-Check-Act ดังที่แสดงในตารางที่ 1 รายละเอียดของข้อ 4 จนถึงข้อ 10 ในมาตรฐานนี้จะครอบคลุมองค์ประกอบต่างๆ ดังต่อไปนี้

- ข้อ 4 เป็นองค์ประกอบของการวางแผน ข้อนี้ได้แนะนำข้อกำหนดที่จำเป็นเพื่อกำหนดบริบทของระบบการบริหารความต่อเนื่องทางธุรกิจ เนื่องจากเป็นส่วนที่ประยุกต์ใช้กับองค์กร ตลอดจนความต้องการ ข้อกำหนด และขอบข่าย
- ข้อ 5 เป็นองค์ประกอบของการวางแผน ข้อนี้ได้รวบรวมข้อกำหนดเฉพาะสำหรับบทบาทหน้าที่ของผู้บริหารสูงสุดในระบบการบริหารความต่อเนื่องทางธุรกิจ และทำให้เห็นว่าความเป็นผู้นำทำให้ทั้งองค์กรเห็นถึงความคาดหวังโดยผ่านทางถ้อยแถลงของนโยบายได้อย่างไร
- ข้อ 6 เป็นองค์ประกอบของการวางแผน ข้อนี้ได้อธิบายข้อกำหนดที่เกี่ยวข้องกับการจัดทำวัตถุประสงค์เชิงกลยุทธ์ และได้ให้คำแนะนำสำหรับระบบการบริหารความต่อเนื่องทางธุรกิจโดยรวมทั้งหมด รายละเอียดเนื้อหาของข้อ 6 มีความแตกต่างจากการกำหนดโอกาสในการลดความเสี่ยงที่ได้มาจากการประเมินความเสี่ยง และวัตถุประสงค์ของการฟื้นฟูที่ได้จากการวิเคราะห์ผลกระทบทางธุรกิจ (BIA)   
*หมายเหตุ การวิเคราะห์ผลกระทบทางธุรกิจและกระบวนการประเมินความเสี่ยงได้ให้รายละเอียดไว้ในข้อ 8*
- ข้อ 7 เป็นองค์ประกอบของการวางแผน ข้อนี้ช่วยสนับสนุนการดำเนินการสำหรับระบบการบริหารความต่อเนื่องทางธุรกิจเนื่องจากมีความเกี่ยวข้องกับการกำหนดความสามารถและการสื่อสารที่ต้องดำเนินการต่อเนื่องเป็นระยะๆ ตามความต้องการของผู้มีส่วนได้เสีย ในขณะที่จัดทำเอกสารควบคุม รักษา และจัดเก็บรักษาเอกสารที่จำเป็น
- ข้อ 8 เป็นองค์ประกอบของการปฏิบัติ ข้อนี้ได้ระบุข้อกำหนดความต่อเนื่องทางธุรกิจ พิจารณาว่าจะดำเนินการกับข้อกำหนดดังกล่าวได้อย่างไร และการจัดทำขั้นตอนการดำเนินงานเพื่อการจัดการกับอุบัติการณ์ที่ทำให้เกิดการหยุดชะงัก
- ข้อ 9 เป็นองค์ประกอบของการตรวจสอบ ข้อนี้ได้รวบรวมข้อกำหนดที่จำเป็นเพื่อการวัดสมรรถนะของระบบการบริหารความต่อเนื่องทางธุรกิจ ตรวจสอบว่าระบบการบริหารความต่อเนื่องทางธุรกิจเป็นไปตามมาตรฐานฉบับนี้ และความคาดหวังของฝ่ายบริหาร และการแสวงหาข้อมูลย้อนกลับมายังฝ่ายบริหารที่เกี่ยวข้องกับความคาดหวัง
- ข้อ 10 เป็นองค์ประกอบของการแก้ไขและปรับปรุง ข้อนี้ได้ระบุและการดำเนินการต่อความไม่เป็นไปตามข้อกำหนดของระบบการบริหารความต่อเนื่องทางธุรกิจโดยผ่านทางปฏิบัติการแก้ไข

## 1. ขอบข่าย

มาตรฐานนี้ใช้สำหรับการบริหารความต่อเนื่องทางธุรกิจ โดยระบุข้อกำหนดเพื่อวางแผน จัดทำ นำไปปฏิบัติ ดำเนินการ เฝ้าระวัง ทบทวน รักษาไว้ และปรับปรุงระบบการจัดการที่เป็นเอกสารอย่างต่อเนื่อง เพื่อป้องกันโอกาสของการเกิด เตรียมการ ตอบสนอง และฟื้นฟูกิจการจากอุบัติการณ์ที่ทำให้เกิดการหยุดชะงักขึ้น

ข้อกำหนดในมาตรฐานนี้เป็นข้อกำหนดทั่วไปและตั้งใจให้นำไปประยุกต์ใช้ได้กับทุกองค์กร (หรือบางส่วน) โดยไม่คำนึงถึงประเภท ขนาด และลักษณะขององค์กร ขอบเขตของการประยุกต์ใช้ข้อกำหนดนี้ขึ้นอยู่กับสภาพแวดล้อมและความซับซ้อนของการดำเนินการขององค์กร

มาตรฐานนี้ไม่ได้ตั้งใจให้มีการนำไปปฏิบัติโดยมีการจัดทำโครงสร้างของระบบการบริหารความต่อเนื่องทางธุรกิจที่เหมือนกันในทุกองค์กร แต่ต้องการให้แต่ละองค์กรมีการออกแบบระบบการบริหารความต่อเนื่องทางธุรกิจที่เหมาะสมกับความต้องการและเป็นไปตามข้อกำหนดของผู้มีส่วนได้เสีย รวมทั้งต้องเป็นไปตามกฎหมาย กฎระเบียบ ข้อกำหนดขององค์กรและภาคอุตสาหกรรม ผลิตภัณฑ์และบริการ กระบวนการในการจ้างงาน ขนาด และโครงสร้างขององค์กร และข้อกำหนดของผู้มีส่วนได้เสีย

มาตรฐานนี้สามารถนำไปประยุกต์ใช้ได้กับองค์กรทุกประเภทและทุกขนาด ที่มีความต้องการ

- ก) จัดทำ นำไปปฏิบัติ รักษาไว้ และปรับปรุงระบบการบริหารความต่อเนื่องทางธุรกิจ
- ข) สร้างความมั่นใจว่าเป็นไปตามนโยบายความต่อเนื่องทางธุรกิจ
- ค) แสดงให้เห็นว่าเป็นไปตามข้อกำหนดอื่นๆ
- ง) ขอรับการรับรองระบบการบริหารความต่อเนื่องทางธุรกิจโดยหน่วยรับรองที่ได้รับการรับรองระบบงาน (accredited certification body)
- จ) ประเมินตนเอง และประกาศรับรองตนเองว่าเป็นไปตามมาตรฐานนี้

มาตรฐานนี้สามารถใช้ในการประเมินว่าองค์กรมีความสามารถในการดำเนินงานได้อย่างต่อเนื่องตามความต้องการของตนเองและตามข้อบังคับทางกฎหมาย

## 2. เอกสารอ้างอิง

ไม่มีเอกสารอ้างอิง

### 3. บทนิยาม

ความหมายของคำที่ใช้ในมาตรฐานผลิตภัณฑ์อุตสาหกรรมนี้ ให้เป็นไปตามบทนิยามต่อไปนี้

#### 3.1 กิจกรรม (activity)

กระบวนการหรือชุดของกระบวนการที่ดำเนินการโดยองค์กร (หรือในนามขององค์กร) เพื่อผลิต หรือช่วยสนับสนุนต่อผลิตภัณฑ์และบริการ

ตัวอย่าง กระบวนการรวมถึง การบัญชี ศูนย์ติดต่อ เทคโนโลยีสารสนเทศ การผลิต การกระจาย

#### 3.2 การตรวจประเมิน (audit)

กระบวนการที่เป็นระบบ เป็นอิสระ และเป็นเอกสาร เพื่อให้ได้มาซึ่งหลักฐานและการประเมินผลที่เป็นรูปธรรม เพื่อพิจารณาความเป็นไปตามข้อกำหนด

หมายเหตุ 1 การตรวจประเมินแบ่งเป็นการตรวจประเมินภายใน (โดยบุคคลที่ 1) หรือการตรวจประเมินภายนอก (โดยบุคคลที่ 2 หรือ 3) และอาจเป็นการตรวจประเมินหลายๆ ระบบพร้อมกัน

หมายเหตุ 2 บทนิยาม “หลักฐาน” และ “เกณฑ์การตรวจประเมิน (audit criteria)” ได้ระบุไว้ใน ISO 19011

#### 3.3 ความต่อเนื่องทางธุรกิจ (business continuity)

ความสามารถขององค์กรในการส่งมอบผลิตภัณฑ์หรือบริการได้ต่อไปภายหลังเกิดเหตุการณ์ที่ทำให้เกิดการหยุดชะงัก ในระดับที่ยอมรับได้ตามที่กำหนดไว้

(ที่มา ISO 22300)

#### 3.4 การบริหารความต่อเนื่องทางธุรกิจ (business continuity management - BCM)

กระบวนการบริหารแบบองค์รวมซึ่งชี้บ่งภัยคุกคามที่อาจเกิดขึ้นต่อองค์กร และผลกระทบของภัยคุกคามนั้นต่อการดำเนินธุรกิจ และให้แนวทางในการสร้างขีดความสามารถให้องค์กรมีความยืดหยุ่น (resilience) เพื่อการตอบสนองและปกป้องผลประโยชน์ของผู้มีส่วนได้เสียหลัก ชื่อเสียง ภาพลักษณ์ และกิจกรรมที่สร้างมูลค่าที่มีประสิทธิผล

#### 3.5 ระบบการบริหารความต่อเนื่องทางธุรกิจ (business continuity management system - BCMS)

ส่วนหนึ่งของระบบการบริหาร ซึ่งประกอบด้วยการจัดทำ การนำไปปฏิบัติ การดำเนินการ การเฝ้าระวัง การทบทวน การรักษา และการปรับปรุงให้เกิดความต่อเนื่องของธุรกิจ

หมายเหตุ ระบบการบริหาร ประกอบด้วยโครงสร้างองค์กร นโยบาย การวางแผนกิจกรรมต่างๆ ความรับผิดชอบ ขั้นตอนการดำเนินงาน กระบวนการ และทรัพยากรที่ต้องใช้

### 3.6 แผนความต่อเนื่องทางธุรกิจ (business continuity plan)

เอกสารขั้นตอนการดำเนินงานที่ให้แนวทางแก่องค์กรในการตอบสนอง การฟื้นฟู การกลับมาดำเนินการ และการติดตั้งเพื่อให้สามารถดำเนินงานได้ในระดับที่กำหนดไว้ภายหลังจากการหยุดชะงัก

หมายเหตุ โดยทั่วไปแผนความต่อเนื่องทางธุรกิจจะครอบคลุมถึงทรัพยากร การบริการ และกิจกรรมต่างๆ ที่ต้องการ เพื่อให้มั่นใจว่าภารกิจ/หน้าที่ที่มีความสำคัญต่อธุรกิจ ยังคงดำเนินงานได้อย่างต่อเนื่อง

### 3.7 โปรแกรมความต่อเนื่องทางธุรกิจ (business continuity programme)

กระบวนการบริหารงานและการปกครองที่ดำเนินการไปโดยได้รับการสนับสนุนจากผู้บริหารสูงสุดและทรัพยากรอย่างเหมาะสมเพื่อนำระบบการบริหารความต่อเนื่องทางธุรกิจ ไปปฏิบัติและรักษาไว้ได้

### 3.8 การวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis)

กระบวนการในการวิเคราะห์กิจกรรมต่างๆ และผลกระทบต่อกิจกรรมดังกล่าวหากธุรกิจเกิดการหยุดชะงักขึ้น

(ที่มา ISO 22300)

### 3.9 ความสามารถ (competence)

การประยุกต์ใช้ความรู้ และทักษะเพื่อให้บรรลุผลลัพธ์ที่ต้องการ

### 3.10 ความเป็นไปตามข้อกำหนด (conformity)

การสามารถทำให้เป็นไปตามข้อกำหนด

(ที่มา ISO 22300)

### 3.11 การปรับปรุงอย่างต่อเนื่อง (continual improvement)

กระบวนการที่เกิดขึ้นซ้ำๆ ซึ่งส่งผลต่อการเพิ่มสมรรถนะ

(ที่มา ISO 22300)

### 3.12 การแก้ไข (correction)

การปฏิบัติการเพื่อขจัดความไม่เป็นไปตามข้อกำหนดที่ตรวจพบ

(ที่มา ISO 22300)

3.13 การปฏิบัติการแก้ไข (corrective action)

การปฏิบัติการเพื่อขจัดสาเหตุของความไม่เป็นไปตามข้อกำหนดและป้องกันการเกิดซ้ำ

หมายเหตุ ในกรณีที่เกิดผลลัพธ์อื่นที่ไม่ต้องการ ปฏิบัติการที่จำเป็นเพื่อลดให้เหลือน้อยที่สุด หรือขจัดสาเหตุ และลดผลกระทบ หรือป้องกันการเกิดซ้ำ ปฏิบัติการดังกล่าวจะอยู่นอกแนวคิดของ “การปฏิบัติการแก้ไข” ตามคำนิยามนี้

(ที่มา ISO 22300)

3.14 เอกสาร (document)

สารสนเทศและสื่อที่ใช้

หมายเหตุ 1 สื่ออาจจะเป็น กระดาษ แม่เหล็ก จานอิเล็กทรอนิกส์ หรือออพติคอล รูปภาพ หรือตัวอย่าง หรือสิ่งต่างๆ เหล่านี้รวมกัน

หมายเหตุ 2 ชุดของเอกสาร ตัวอย่างเช่น ข้อกำหนด และบันทึก ซึ่งโดยปกติมักจะเรียกว่า “การเอกสาร”

3.15 เอกสารสารสนเทศ (documented information)

สารสนเทศที่ได้รับการควบคุมและรักษาไว้โดยองค์กร รวมทั้งสื่อที่ใช้เก็บสารสนเทศดังกล่าว

หมายเหตุ 1 เอกสารสารสนเทศอาจจะอยู่ในรูปแบบและสื่อใดๆ ก็ได้

หมายเหตุ 2 เอกสารสารสนเทศสามารถอ้างอิงถึง

- ระบบการบริหารงาน รวมทั้งกระบวนการที่เกี่ยวข้อง
- สารสนเทศที่จัดทำขึ้นเพื่อใช้สำหรับการดำเนินการขององค์กร (การเอกสาร)
- หลักฐานจากผลลัพธ์ที่เกิดขึ้น (บันทึก)

3.16 ประสิทธิภาพ (effectiveness)

การดำเนินการกิจกรรมและผลลัพธ์ที่เกิดขึ้นเป็นไปตามแผนที่ระบุไว้

(ที่มา ISO 22300)

3.17 เหตุการณ์ (event)

การเกิดขึ้นหรือการเปลี่ยนแปลงของสถานการณ์ที่เป็นการเฉพาะ

หมายเหตุ 1 เหตุการณ์สามารถเกิดขึ้นได้มากกว่าหนึ่งครั้ง และสามารถมาจากหลายสาเหตุ

หมายเหตุ 2 เหตุการณ์สามารถประกอบขึ้นจากสิ่งที่ยังไม่ได้เกิดขึ้น

หมายเหตุ 3 เหตุการณ์ในบางครั้งสามารถใช้คำว่า “อุบัติการณ์” หรือ “อุบัติเหตุ (accident)”

หมายเหตุ 4 เหตุการณ์ที่ไม่มีผลกระทบที่เกิดขึ้นตามมาอาจใช้คำว่า “เหตุการณ์เกือบเกิดอุบัติเหตุ (near miss, incident, near hit หรือ close call)”

(ที่มา ISO/IEC Guide 73)

### 3.18 การฝึกซ้อม (exercise)

กระบวนการเพื่อการฝึกอบรม การประเมิน การฝึกปฏิบัติ และการปรับปรุงสมรรถนะภายในองค์กร

หมายเหตุ 1 การฝึกซ้อมสามารถนำไปใช้เพื่อยืนยันเกี่ยวกับนโยบาย แผนงาน ขั้นตอนการดำเนินงาน การฝึกอบรม อุปกรณ์ และข้อตกลงระหว่างองค์กร เพื่อเป็นการชี้แจงและการฝึกอบรมบุคลากรเกี่ยวกับบทบาทหน้าที่และความรับผิดชอบ เพื่อปรับปรุงการประสานงานและการสื่อสารระหว่างองค์กร เพื่อชี้แจงช่องว่างเกี่ยวกับทรัพยากร เพื่อการปรับปรุงสมรรถนะของแต่ละบุคคลและชี้แจงถึงโอกาสในการปรับปรุง และสร้างโอกาสในการฝึกปฏิบัติต่อสถานการณ์เฉพาะหน้า

หมายเหตุ 2 การทดสอบเป็นการฝึกซ้อมที่มีความเฉพาะเจาะจง โดยมีความคาดหวังผลจากการฝึกซ้อมว่าผ่านหรือไม่ผ่านตามเป้าหมายหรือวัตถุประสงค์หรือวัตถุประสงค์ของการฝึกซ้อมที่ได้วางแผนไว้

(ที่มา ISO 22300)

### 3.19 อุบัติการณ์ (incident)

สถานการณ์ที่อาจทำให้หรือสามารถนำไปสู่การหยุดชะงัก ความสูญเสีย ภาวะฉุกเฉิน หรือ สภาวะวิกฤต

(ที่มา ISO 22300)

### 3.20 โครงสร้างพื้นฐาน (infrastructure)

ระบบของสิ่งอำนวยความสะดวก อุปกรณ์ และบริการที่จำเป็นสำหรับการดำเนินการขององค์กร

### 3.21 ผู้มีส่วนได้เสีย (interested party/stakeholder)

บุคคล หรือองค์กรที่สามารถทำให้เกิดผลกระทบหรือได้รับผลกระทบ หรือเชื่อว่าตนเองได้รับผลกระทบจากการตัดสินใจหรือกิจกรรม

หมายเหตุ ผู้มีส่วนได้เสียอาจจะเป็นบุคคลหรือกลุ่มของบุคคล ที่มีส่วนได้เสียในการตัดสินใจ หรือกิจกรรมใดๆ ขององค์กร

3.22 การตรวจประเมินภายใน (internal audit)

การตรวจประเมินที่ดำเนินการโดยองค์กรเองหรือโดยบุคคลภายนอกที่ทำในนามขององค์กรเพื่อนำผลที่ได้ไปทบทวนการบริหารงานและจุดประสงค์อื่นๆ และอาจใช้เป็นพื้นฐานในการประกาศความเป็นไปตามข้อกำหนดขององค์กร

หมายเหตุ ในกรณีองค์กรขนาดเล็ก ความเป็นอิสระสามารถแสดงได้โดยการมอบหมายผู้ตรวจประเมินที่ไม่มีส่วนรับผิดชอบในกิจกรรมที่รับการตรวจประเมิน

3.23 การสั่งให้ดำเนินการ (invocation)

ระบบในการประกาศให้เริ่มดำเนินการความต่อเนื่องทางธุรกิจขององค์กรตามที่ได้เตรียมการไว้เพื่อสามารถส่งมอบสินค้าและบริการหลักได้อย่างต่อเนื่อง

3.24 ระบบการบริหารงาน (management system)

องค์ประกอบขององค์กรที่สัมพันธ์กันหรือมีปฏิสัมพันธ์ต่อกันเพื่อนำไปกำหนดนโยบายและวัตถุประสงค์และกระบวนการเพื่อให้บรรลุวัตถุประสงค์ดังกล่าว

หมายเหตุ 1 ระบบการบริหารงานสามารถเป็นระบบเดียวหรือหลายระบบ

หมายเหตุ 2 องค์ประกอบของระบบการบริหารงาน รวมถึงโครงสร้างขององค์กร บทบาทหน้าที่และความรับผิดชอบ การวางแผน การดำเนินการ เป็นต้น

หมายเหตุ 3 ขอบข่ายของระบบการบริหารงานสามารถครอบคลุมทั้งองค์กร ระบุเจาะจงสำหรับบางหน่วยงานหรือแผนกโดยเฉพาะในองค์กร หรือกลุ่มของกิจกรรม

3.25 ช่วงเวลาการหยุดบริการที่ยอมรับได้สูงสุด (maximum acceptable outage - MAO)

ช่วงเวลาที่ส่งผลกระทบทำให้ไม่สามารถยอมรับได้จากการจัดส่งสินค้า หรือให้บริการ หรือดำเนินกิจกรรม

หมายเหตุ ดูช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด

3.26 ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (maximum tolerable period of disruption - MTPD)

ช่วงเวลาที่ส่งผลกระทบทำให้ไม่สามารถยอมรับได้จากการจัดส่งสินค้า หรือให้บริการ หรือดำเนินกิจกรรม

หมายเหตุ ดูช่วงเวลาการหยุดบริการที่ยอมรับได้สูงสุด

3.27 การวัด (measurement)

กระบวนการเพื่อค้นหาค่า

- 3.28 วัตถุประสงค์ความต่อเนื่องทางธุรกิจขั้นต่ำสุด (minimum business continuity objective - MBCO)  
ระดับต่ำสุดของการบริการ และ/หรือ ผลิตภัณฑ์ที่องค์กรยอมรับ โดยยังคงสามารถบรรลุวัตถุประสงค์ทางธุรกิจในระหว่างเกิดการหยุดชะงัก
- 3.29 การเฝ้าระวัง (monitoring)  
การค้นหาสถานภาพของระบบ กระบวนการ หรือกิจกรรม  
หมายเหตุ การค้นหาสถานภาพอาจจำเป็นต้องใช้การตรวจสอบ การเฝ้าดู หรือการสังเกตอย่างจริงจัง
- 3.30 ข้อตกลงว่าด้วยการให้ความช่วยเหลือซึ่งกันและกัน (mutual aid agreement)  
การเตรียมการล่วงหน้าเพื่อสร้างความเข้าใจระหว่างหน่วยงานตั้งแต่สองหน่วยงานขึ้นไปเพื่อให้ความช่วยเหลือซึ่งกันและกัน  
(ที่มา ISO 22300)
- 3.31 ความไม่เป็นไปตามข้อกำหนด (nonconformity)  
การไม่สามารถทำให้เป็นไปตามข้อกำหนด  
(ที่มา ISO 22300)
- 3.32 วัตถุประสงค์ (objective)  
ผลลัพธ์ที่ต้องการบรรลุ  
หมายเหตุ 1 วัตถุประสงค์อาจเป็นกลยุทธ์ ยุทธวิธี หรือ การดำเนินการ  
หมายเหตุ 2 วัตถุประสงค์สามารถเกี่ยวข้องกับด้านต่างๆ (เช่น การเงิน สุขภาพและความปลอดภัย และ เป้าประสงค์ด้านสิ่งแวดล้อม) และสามารถประยุกต์ใช้ได้ในระดับต่างๆ (เช่น กลยุทธ์ ทั้งทั้ง องค์กร โครงการ ผลิตภัณฑ์ และกระบวนการ)  
หมายเหตุ 3 วัตถุประสงค์อาจแสดงได้ในวิธีการอื่นๆ เช่น ผลสัมฤทธิ์ที่ต้องการ จุดประสงค์ เกณฑ์ การดำเนินการ วัตถุประสงค์การดำเนินธุรกิจอย่างต่อเนื่อง หรืออาจจะใช้คำอื่นที่มีความหมาย เช่นเดียวกัน เช่น จุดมุ่งหมาย เป้าประสงค์ หรือเป้าหมาย  
หมายเหตุ 4 ตามบริบทของมาตรฐานระบบการจัดการการรักษาความปลอดภัยของสังคม วัตถุประสงค์ ความปลอดภัยกำหนดโดยองค์กร-ซึ่งสอดคล้องกับนโยบายการรักษาความปลอดภัยของสังคม เพื่อให้บรรลุตามผลที่ได้กำหนดไว้

3.33 องค์กร (organization)

บุคคลหรือกลุ่มของบุคคลซึ่งมีหน้าที่ของตนเอง โดยการกำหนดความรับผิดชอบ อำนาจหน้าที่ และความสัมพันธ์ต่อกันเพื่อให้บรรลุวัตถุประสงค์

หมายเหตุ 1 องค์กรในที่นี้อาจรวมถึง บริษัท ห้างหุ้นส่วนจำกัด สถาบัน มูลนิธิ ความร่วมมือ สมาคมนิติบุคคล ผู้ประกอบการ หรือส่วนหนึ่ง หรือ สิ่งต่างๆ เหล่านี้รวมกัน โดยอาจจะเป็นความร่วมมือกันของภาครัฐหรือภาคเอกชน

หมายเหตุ 2 สำหรับองค์กรที่มีการแบ่งเป็นหน่วยปฏิบัติการมากกว่าหนึ่งหน่วย หน่วยปฏิบัติการหนึ่งๆ อาจถูกกำหนดให้เป็นองค์กรก็ได้

3.34 การให้หน่วยงานอื่นดำเนินการแทน (outsource)

การทำข้อตกลงกับองค์กรภายนอกเพื่อให้ดำเนินการในบางส่วนของกิจกรรมหรือกระบวนการขององค์กร

หมายเหตุ แม้องค์กรภายนอกจะอยู่ภายนอกขอบข่ายของระบบการบริหารงาน อย่างไรก็ตามกิจกรรมหรือกระบวนการที่มอบให้องค์กรภายนอกดำเนินการแทนจะยังคงอยู่ในขอบข่ายของระบบ

3.35 สมรรถนะ (performance)

ผลลัพธ์ที่สามารถวัดได้

หมายเหตุ 1 สมรรถนะสามารถวัดได้ทั้งในเชิงปริมาณหรือเชิงคุณภาพ

หมายเหตุ 2 สมรรถนะสามารถเกี่ยวข้องกับกิจกรรมการบริหารงาน กระบวนการ ผลิตภัณฑ์ (รวมทั้งบริการ) ระบบ หรือองค์กรต่างๆ

3.36 การประเมินสมรรถนะ (performance evaluation)

กระบวนการในการค้นหาผลลัพธ์ที่สามารถวัดได้

3.37 บุคลากร (personnel)

บุคคลที่ทำงานให้กับองค์กรหรือทำงานภายใต้การควบคุมขององค์กร

หมายเหตุ บุคลากร อาจหมายรวมถึง ลูกจ้าง พนักงานนอกเวลา พนักงานเจ้าหน้าที่ (agency staff)

3.38 นโยบาย (policy)

ความมุ่งมั่นและทิศทางขององค์กรที่แถลงการณ์อย่างเป็นทางการโดยผู้บริหารสูงสุด

3.39 ขั้นตอนการดำเนินงาน (procedure)

การกำหนดวิธีการในการดำเนินกิจกรรมหรือกระบวนการ

## 3.40 กระบวนการ (process)

กลุ่มของกิจกรรมที่สัมพันธ์หรือที่มีปฏิสัมพันธ์ต่อกันเพื่อเปลี่ยนปัจจัยนำเข้าไปสู่ผลลัพธ์ที่ต้องการ

## 3.41 ผลิตภัณฑ์และบริการ (product and service)

ผลลัพธ์จากการดำเนินงานขององค์กรที่สร้างประโยชน์ต่อลูกค้า ผู้รับ และผู้มีส่วนได้เสีย เช่น ชิ้นงานจากการผลิต การประกันรถยนต์ และการพยาบาลอนามัยชุมชน (community nursing)

## 3.42 กิจกรรมที่มีความสำคัญ (prioritized activities)

กิจกรรมที่ต้องให้ความสำคัญในระดับต่างๆ เพื่อบรรเทาผลกระทบ ภายหลังการเกิดอุบัติการณ์

หมายเหตุ คำศัพท์ในกลุ่มนี้ที่ใช้ทั่วไปในการอธิบายถึงกิจกรรมต่างๆ ได้แก่ วิกฤต (critical) มีความจำเป็น (essential) ความสำคัญ (vital) เร่งด่วน (urgent) และหลักสำคัญ (key)

(ที่มา ISO 22300)

## 3.43 บันทึก (record)

เอกสารที่ระบุผลลัพธ์หรือหลักฐานที่เกิดขึ้นจากกิจกรรมที่ได้ดำเนินการ

## 3.44 เป้าหมายของการฟื้นคืนสภาพ (recovery point objective - RPO)

จุดซึ่งสารสนเทศที่ใช้ในกิจกรรมต้องได้รับการฟื้นฟูเพื่อให้สามารถกลับมาดำเนินกิจกรรมต่อไปได้

หมายเหตุ สามารถใช้คำว่าระยะเวลาสูงสุดที่ข้อมูลเกิดการสูญหาย (maximum data loss)

## 3.45 ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (recovery time objective - RTO)

ระยะเวลาหลังจากเกิดอุบัติการณ์ขึ้น ที่ทำให้

- ผลิตภัณฑ์หรือบริการต้องกลับคืนสภาพเดิม
- กิจกรรมต้องกลับมาดำเนินการได้
- ทรัพยากรต้องได้รับการฟื้นฟู

หมายเหตุ สำหรับผลิตภัณฑ์ บริการ และกิจกรรม ระยะเวลาเป้าหมายในการฟื้นคืนสภาพต้องน้อยกว่าระยะเวลาของผลกระทบด้านลบที่เกิดจากการที่ไม่สามารถส่งมอบผลิตภัณฑ์/บริการอยู่ในระดับที่ไม่สามารถเป็นที่ยอมรับได้

3.46 ข้อกำหนด (requirement)

ความต้องการและความคาดหวังที่ได้ระบุไว้ หรือเป็นที่เข้าใจโดยทั่วไป หรือข้อปฏิบัติตามหลักกฎหมาย

หมายเหตุ 1 เป็นสิ่งที่รู้กัน โดยทั่วไป หมายถึง เป็นธรรมเนียมปฏิบัติหรือแนวปฏิบัติโดยทั่วไปสำหรับองค์กรและผู้มีส่วนได้เสียว่าความต้องการหรือความคาดหวังจะเป็นไปตามนั้น

หมายเหตุ 2 ข้อกำหนดที่กำหนดไว้คือ สิ่งที่ได้ระบุไว้อย่างชัดเจน เช่น การระบุไว้ในเอกสารสารสนเทศ

3.47 ทรัพยากร (resources)

สินทรัพย์ บุคลากร ทักษะ สารสนเทศ เทคโนโลยี (รวมทั้งอาคารและอุปกรณ์) สถานที่ตั้ง และเครื่องอุปโภค และสารสนเทศ (ไม่ว่าจะอยู่ในสื่ออิเล็กทรอนิกส์หรือไม่) ที่องค์กรจำเป็นต้องมีอย่างเพียงพอเพื่อใช้สำหรับการดำเนินการเมื่อจำเป็น และทำให้บรรลุวัตถุประสงค์ขององค์กร

3.48 ความเสี่ยง (risk)

ผลกระทบของความไม่แน่นอนต่อวัตถุประสงค์

หมายเหตุ 1 ผลกระทบคือการเบี่ยงเบนไปจากสิ่งที่คาดหวังไว้ ทั้งที่ดีหรือไม่ดี

หมายเหตุ 2 วัตถุประสงค์สามารถมีแง่มุมที่แตกต่างกัน (เช่น การเงิน สุขภาพและความปลอดภัย และเป้าประสงค์ด้านสิ่งแวดล้อม) และสามารถประยุกต์ใช้ได้ในระดับต่างๆ (เช่น กลยุทธ์ ทั่วทั้งองค์กร โครงการ ผลิตภัณฑ์ และกระบวนการ) วัตถุประสงค์อาจแสดงได้ในวิธีการอื่นๆ เช่น ผลสัมฤทธิ์ที่ต้องการ จุดประสงค์ เกณฑ์การดำเนินการ วัตถุประสงค์การดำเนินธุรกิจอย่างต่อเนื่อง หรืออาจจะใช้คำอื่นที่มีความหมายเช่นเดียวกัน เช่น จุดมุ่งหมาย เป้าประสงค์ หรือเป้าหมาย

หมายเหตุ 3 ความเสี่ยงมักจะแบ่งแยกโดยอ้างอิงถึงเหตุการณ์ที่อาจจะเกิดขึ้น (Guide 73 ข้อ 3.5.1.3) และผลกระทบที่เกิดขึ้นตามมา (Guide 73 ข้อ 3.6.1.3) หรือสองอย่างนี้รวมกัน

หมายเหตุ 4 ความเสี่ยงมักจะแสดงออกในรูปของผลรวมของผลสืบเนื่องจากเหตุการณ์ (รวมถึงการเปลี่ยนแปลงของสถานการณ์กับโอกาสที่จะเกิดขึ้น (Guide 73 ข้อ 3.6.1.1)

หมายเหตุ 5 ความไม่แน่นอน เป็นสถานะของการขาดข้อมูลเกี่ยวกับความเข้าใจหรือความรู้ของเหตุการณ์ ผลที่ตามมา หรือโอกาสของการเกิด

หมายเหตุ 6 ในบริบทของมาตรฐานระบบการบริหารความต่อเนื่องทางธุรกิจ วัตถุประสงค์ความต่อเนื่องทางธุรกิจถูกกำหนดขึ้นโดยองค์กรซึ่งสอดคล้องกับนโยบายความต่อเนื่องทางธุรกิจ เพื่อให้บรรลุผลลัพธ์ที่กำหนดไว้ ในการประยุกต์ใช้คำว่า “ความเสี่ยงและองค์ประกอบของการจัดการความเสี่ยง” ควรอ้างอิงถึงวัตถุประสงค์ขององค์กร แต่ไม่จำกัดเพียงวัตถุประสงค์ความต่อเนื่องทางธุรกิจที่ระบุไว้ในข้อ 6.2 ของมาตรฐานนี้เท่านั้น

### 3.49 ความเสี่ยงที่ยอมรับได้ (risk appetite)

ระดับและประเภทของความเสี่ยงที่องค์กรเต็มใจยอมรับได้

### 3.50 การประเมินความเสี่ยง (risk assessment)

กระบวนการโดยรวมเกี่ยวกับการชี้แจงความเสี่ยง (risk identification) การวิเคราะห์ความเสี่ยง (risk analysis) และการประเมินผลความเสี่ยง (risk evaluation)

### 3.51 การบริหารความเสี่ยง (risk management)

การประสานกิจกรรมเพื่อสั่งการและควบคุมองค์กรเกี่ยวกับความเสี่ยง

### 3.52 การทดสอบ (testing)

ขั้นตอนการดำเนินงานเพื่อการประเมินผล วิธีการเพื่อการกำหนด หรือการยืนยันถึงการมีอยู่ คุณภาพหรือข้อเท็จจริงของบางสิ่งบางอย่าง

หมายเหตุ 1 การทดสอบอาจจะใช้คำว่า “การทดลอง (trial)”

หมายเหตุ 2 การทดสอบมักจะนำไปประยุกต์ใช้กับแผนสนับสนุนต่างๆ

### 3.53 ผู้บริหารสูงสุด (top management)

บุคคลหรือกลุ่มบุคคลซึ่งสั่งการและควบคุมองค์กรในระดับสูงสุด

หมายเหตุ 1 ผู้บริหารสูงสุดมีอำนาจในการมอบอำนาจหน้าที่ และจัดสรรทรัพยากรภายในองค์กร

หมายเหตุ 2 ในกรณีที่ขอบข่ายของระบบบริหารงานครอบคลุมเฉพาะบางส่วนขององค์กร ดังนั้นผู้บริหารสูงสุดหมายถึงบุคคลหรือกลุ่มบุคคลที่สั่งการและควบคุมองค์กรในส่วนนั้น

### 3.54 การทวนสอบ (verification)

ข้อยืนยันโดยมีหลักฐานเพื่อแสดงว่าได้เป็นไปตามข้อกำหนดที่กำหนดไว้

3.55 สภาพแวดล้อมในการทำงาน (work environment)

กลุ่มของสภาวะต่างๆ ณ จุดดำเนินงาน

หมายเหตุ สภาวะต่างๆ รวมถึงปัจจัยทางกายภาพ สังคม จิตวิทยา และสิ่งแวดล้อม (เช่น อุณหภูมิ รูปแบบของการให้การยอมรับ (recognition schemes) การยศาสตร์ และบรรยากาศการทำงาน)

#### 4. บริบทขององค์กร

4.1 ความเข้าใจองค์กรและบริบทขององค์กร

องค์กรต้องพิจารณาประเด็นภายนอกและภายในที่เกี่ยวข้องกับจุดประสงค์ขององค์กรและที่มีผลกระทบต่อความสามารถขององค์กรในการบรรลุผลลัพธ์ตามที่คาดหวังไว้ต่อระบบการบริหารความต่อเนื่องทางธุรกิจ

ประเด็นเหล่านี้ต้องถูกนำมาพิจารณาเมื่อมีการจัดทำ นำไปปฏิบัติ และการรักษาไว้ซึ่งระบบการบริหารความต่อเนื่องทางธุรกิจขององค์กร

องค์กรต้องชี้แจงและจัดทำเป็นเอกสาร ดังนี้

- ก) กิจกรรมต่างๆ ขององค์กร หน้าที่งาน การบริการ ผลิตภัณฑ์ หุ่นส่วน ห่วงโซ่อุปทาน ความสัมพันธ์กับผู้มีส่วนได้เสีย และแนวโน้มของผลกระทบที่เกี่ยวข้องกับอุบัติการณ์ที่ทำให้เกิดการหยุดชะงัก
- ข) ความเชื่อมโยงระหว่างนโยบายความต่อเนื่องทางธุรกิจ และวัตถุประสงค์ขององค์กร และนโยบายด้านอื่นๆ รวมทั้งกลยุทธ์การบริหารความเสี่ยงขององค์กรโดยรวม
- ค) ความเสี่ยงที่ยอมรับได้ขององค์กร

ในการกำหนดบริบท องค์กรต้อง

- 1) กำหนดวัตถุประสงค์ รวมทั้งที่เกี่ยวข้องกับความต่อเนื่องทางธุรกิจอย่างชัดเจน
- 2) ระบุปัจจัยภายนอกและภายในที่ก่อให้เกิดความไม่แน่นอนที่ทำให้เกิดความเสี่ยง
- 3) กำหนดเกณฑ์ความเสี่ยงโดยการพิจารณาถึงความเสี่ยงที่ยอมรับได้
- 4) กำหนดเป้าหมายของระบบการบริหารความต่อเนื่องทางธุรกิจ

## 4.2 ความเข้าใจถึงความต้องการและความคาดหวังของผู้มีส่วนได้เสีย

### 4.2.1 ทั่วไป

ในการจัดทำระบบการบริหารความต่อเนื่องทางธุรกิจ องค์กรต้องพิจารณาถึง

- ก) ผู้มีส่วนได้เสียที่มีความเกี่ยวข้องกับระบบการบริหารความต่อเนื่องทางธุรกิจ
- ข) ข้อกำหนดของผู้มีส่วนได้เสียเหล่านี้ (เช่น ความต้องการและความคาดหวังที่ได้ระบุไว้ หรือเป็นที่เข้าใจโดยทั่วไป หรือเป็นข้อผูกพัน)

### 4.2.2 ข้อกำหนดด้านกฎหมายและระเบียบข้อบังคับ

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานเพื่อการชี้แจง การเข้าถึง และการประเมินข้อกำหนดด้านกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องกับองค์กรซึ่งสัมพันธ์กับความต่อเนื่องของการดำเนินงาน ผลิตภัณฑ์ และบริการ รวมทั้งผลประโยชน์ของผู้มีส่วนได้เสียที่เกี่ยวข้อง

องค์กรต้องมั่นใจว่าได้มีการประยุกต์ใช้กฎหมาย ระเบียบข้อบังคับ และข้อกำหนดอื่นๆ ซึ่งองค์กรเกี่ยวข้องโดยการจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งระบบการบริหารความต่อเนื่องทางธุรกิจ

องค์กรต้องจัดทำสารสนเทศเหล่านี้เป็นลายลักษณ์อักษรและทำให้ทันสมัย กฎหมายใหม่และที่เปลี่ยนแปลง ระเบียบข้อบังคับ และข้อกำหนดอื่นๆ ต้องสื่อสารให้กับลูกจ้างที่ได้รับผลกระทบและผู้มีส่วนได้เสียอื่นๆ

## 4.3 การกำหนดขอบข่ายระบบการบริหารความต่อเนื่องทางธุรกิจ

### 4.3.1 ทั่วไป

องค์กรต้องกำหนดขอบเขตและขอบข่ายในการนำระบบการบริหารความต่อเนื่องทางธุรกิจไปประยุกต์ใช้

ในการกำหนดขอบข่าย องค์กรต้องพิจารณาถึง

- ประเด็นภายนอกและภายใน ตามข้อ 4.1
- ข้อกำหนด ตามข้อ 4.2

ขอบข่ายต้องจัดทำเป็นเอกสารสารสนเทศ

#### 4.3.2 ขอบข่ายของระบบการบริหารความต่อเนื่องทางธุรกิจ

องค์กรต้อง

- ก) กำหนดหน่วยงานต่างๆ ขององค์กรที่อยู่ในระบบการบริหารความต่อเนื่องทางธุรกิจ
- ข) จัดทำข้อกำหนดของระบบการบริหารความต่อเนื่องทางธุรกิจโดยพิจารณาถึงพันธกิจ เป้าประสงค์ ข้อผูกพันภายในและภายนอกขององค์กร (รวมทั้งที่เกี่ยวข้องกับผู้มีส่วนได้เสีย) และความรับผิดชอบทางกฎหมายและระเบียบข้อบังคับ
- ค) ชี้นำผลิตภัณฑ์และบริการ รวมทั้งกิจกรรมที่เกี่ยวข้องทั้งหมดภายในขอบข่ายของระบบการบริหารความต่อเนื่องทางธุรกิจ
- ง) คำนึงถึงความต้องการและผลประโยชน์ของผู้มีส่วนได้เสีย (เช่น ลูกค้า นักลงทุน ผู้ถือหุ้น) ห่วงโซ่อุปทาน ปัจจัยนำเข้าและความต้องการ ความคาดหวัง และผลประโยชน์ของสาธารณะ และ/หรือชุมชน (ตามความเหมาะสม)
- จ) กำหนดขอบข่ายของระบบการบริหารความต่อเนื่องทางธุรกิจที่เหมาะสมกับขนาด ลักษณะ และความซับซ้อนขององค์กร

ในการกำหนดขอบข่าย องค์กรต้องจัดทำเป็นเอกสารและอธิบายถึงการละเว้น ทั้งนี้การละเว้นต้องไม่กระทบต่อความสามารถและความรับผิดชอบขององค์กรในการจัดเตรียมเพื่อความต่อเนื่องของธุรกิจ และการดำเนินการให้เป็นไปตามข้อกำหนดของระบบการบริหารความต่อเนื่องทางธุรกิจซึ่งได้พิจารณาจากการวิเคราะห์ผลกระทบทางธุรกิจ หรือการประเมินความเสี่ยง และข้อกำหนดของกฎหมายหรือระเบียบข้อบังคับที่เกี่ยวข้อง

#### 4.4 ระบบการบริหารความต่อเนื่องทางธุรกิจ

องค์กรต้องจัดทำ นำไปปฏิบัติ รักษา และปรับปรุงระบบการบริหารความต่อเนื่องทางธุรกิจตามข้อกำหนดของมาตรฐานนี้อย่างต่อเนื่อง รวมทั้งกระบวนการที่จำเป็นและปฏิสัมพันธ์ระหว่างกระบวนการเหล่านั้น

### 5. ความเป็นผู้นำ

#### 5.1 ความเป็นผู้นำและความมุ่งมั่น

ผู้บริหารสูงสุดและผู้บริหารอื่นที่มีหน้าที่เกี่ยวข้องต้องเป็นผู้นำในการแสดงออกถึงความตระหนักต่อความสำคัญของระบบการบริหารความต่อเนื่องทางธุรกิจ

*ตัวอย่าง      ความเป็นผู้นำและความมุ่งมั่นสามารถแสดงออกโดยการจูงใจและการมอบอำนาจให้บุคลากรเข้ามามีส่วนช่วยให้ระบบการบริหารความต่อเนื่องทางธุรกิจเกิดประสิทธิผล*

## 5.2 ความมุ่งมั่นของฝ่ายบริหาร

ผู้บริหารสูงสุดต้องเป็นผู้นำในการแสดงให้เห็นถึงความตระหนักต่อความสำคัญ และความมุ่งมั่นต่อระบบการบริหารความต่อเนื่องทางธุรกิจโดย

- มั่นใจว่านโยบายและวัตถุประสงค์ที่กำหนดขึ้นสำหรับระบบการบริหารความต่อเนื่องทางธุรกิจ สอดคล้อง (compatible) กันกับกลยุทธ์ขององค์กร
- มั่นใจว่ามีการบูรณาการข้อกำหนดของระบบการบริหารความต่อเนื่องทางธุรกิจกับกระบวนการทางธุรกิจขององค์กร
- มั่นใจว่ามีการจัดสรรทรัพยากรสำหรับระบบการบริหารความต่อเนื่องทางธุรกิจที่เพียงพอ
- สื่อสารให้เข้าใจถึงความสำคัญของระบบการบริหารความต่อเนื่องทางธุรกิจที่มีประสิทธิภาพและสอดคล้องตามข้อกำหนดของระบบการบริหารความต่อเนื่องทางธุรกิจ
- มั่นใจว่าระบบการบริหารความต่อเนื่องทางธุรกิจบรรลุผลสัมฤทธิ์ตามที่คาดหวังไว้
- อำนาจการและสนับสนุนบุคลากรเข้ามามีส่วนช่วยให้ระบบการบริหารความต่อเนื่องทางธุรกิจเกิดประสิทธิภาพ
- ส่งเสริมให้มีการปรับปรุงอย่างต่อเนื่อง
- สนับสนุนให้ผู้บริหารที่มีบทบาทหน้าที่ที่เกี่ยวข้อง ได้แสดงความเป็นผู้นำและความมุ่งมั่นในการประยุกต์ใช้มาตรฐานดังกล่าวในงานที่รับผิดชอบ

หมายเหตุ 1 คำว่า “ธุรกิจ” ในมาตรฐานนี้ ให้มีความหมายกว้างๆ ว่าหมายถึงกิจกรรมหลักต่างๆ ที่ทำให้องค์กรสามารถบรรลุวัตถุประสงค์

ผู้บริหารสูงสุดต้องจัดเตรียมหลักฐานที่แสดงถึงความมุ่งมั่นในการจัดทำ การนำไปปฏิบัติ การดำเนินการ การเฝ้าระวัง การทบทวน การรักษา และการปรับปรุงระบบการบริหารความต่อเนื่องทางธุรกิจ โดย

- กำหนดนโยบายความต่อเนื่องทางธุรกิจ
- มั่นใจว่าได้มีการกำหนดวัตถุประสงค์และแผนงานของระบบการบริหารความต่อเนื่องทางธุรกิจ
- กำหนดบทบาทหน้าที่ ความรับผิดชอบ และความสามารถสำหรับการบริหารความต่อเนื่องทางธุรกิจ
- แต่งตั้งบุคคล (อาจมากกว่าหนึ่งคน) ให้มีความรับผิดชอบต่อระบบการบริหารความต่อเนื่องทางธุรกิจ พร้อมทั้งกำหนดอำนาจหน้าที่และความสามารถอย่างเหมาะสมในบทบาทหน้าที่สำหรับการนำไปปฏิบัติการและรักษาไว้ซึ่งระบบการบริหารความต่อเนื่องทางธุรกิจ

หมายเหตุ 2 บุคคลเหล่านี้สามารถมีความรับผิดชอบอื่นภายในองค์กร

ผู้บริหารสูงสุดต้องมั่นใจว่ามีการมอบหมายบทบาทหน้าที่อื่นที่เกี่ยวข้องและสื่อสารเกี่ยวกับความรับผิดชอบและอำนาจหน้าที่ให้เข้าใจทั่วทั้งองค์กร โดย

- กำหนดเกณฑ์การยอมรับความเสี่ยงและระดับของความเสี่ยงที่สามารถยอมรับได้
- มีส่วนร่วมในการฝึกซ้อมและทดสอบอย่างจริงจัง
- มั่นใจว่ามีการประเมินภายในระบบการบริหารความต่อเนื่องทางธุรกิจ
- ทบทวนการบริหารงานสำหรับระบบการบริหารความต่อเนื่องทางธุรกิจ
- แสดงให้เห็นถึงความมุ่งมั่นในการปรับปรุงอย่างต่อเนื่อง

### 5.3 นโยบาย

ผู้บริหารสูงสุดต้องจัดทำและสื่อสารนโยบายความต่อเนื่องทางธุรกิจ โดยนโยบายต้อง

- ก) เหมาะสมกับเป้าหมายขององค์กร
- ข) ให้กรอบสำหรับการกำหนดวัตถุประสงค์ความต่อเนื่องทางธุรกิจ
- ค) ประกอบด้วยความมุ่งมั่นในการเป็นไปตามข้อกำหนดที่นำมาประยุกต์ใช้
- ง) รวมถึงความมุ่งมั่นในการปรับปรุงระบบการบริหารความต่อเนื่องทางธุรกิจอย่างต่อเนื่อง

นโยบายระบบการบริหารความต่อเนื่องทางธุรกิจต้อง

- เป็นเอกสารสารสนเทศ
- ได้รับการสื่อสารภายในองค์กร
- เปิดเผยต่อผู้มีส่วนได้เสียตามความเหมาะสม
- ได้รับการทบทวนความต่อเนื่องอย่างเหมาะสมตามระยะเวลาและเกิดการเปลี่ยนแปลงอย่างมีนัยสำคัญ

องค์กรต้องเก็บรักษาเอกสารสารสนเทศเกี่ยวกับนโยบายความต่อเนื่องทางธุรกิจ

### 5.4 บทบาทหน้าที่ ความรับผิดชอบ และอำนาจหน้าที่ในองค์กร

ผู้บริหารสูงสุดต้องมั่นใจว่ามีการมอบหมายและสื่อสารความรับผิดชอบและอำนาจหน้าที่สำหรับบทบาทหน้าที่ต่างๆ ที่เกี่ยวข้องภายในองค์กร

ผู้บริหารสูงสุดต้องมอบหมายความรับผิดชอบและอำนาจหน้าที่ เพื่อ

- ก) มั่นใจว่าระบบการบริหารงานเป็นไปตามข้อกำหนดของมาตรฐานนี้
- ข) รายงานสมรรถนะของระบบการบริหารความต่อเนื่องทางธุรกิจต่อผู้บริหารสูงสุด

## 6. การวางแผน

### 6.1 ปฏิบัติการเพื่อดำเนินการกับความเสี่ยงและโอกาส

ในการวางแผนสำหรับระบบการบริหารความต่อเนื่องทางธุรกิจ องค์กรต้องพิจารณาประเด็นต่างๆ ที่ได้ระบุไว้ในข้อ 4.1 และข้อกำหนดต่างๆ ที่ได้ระบุไว้ในข้อ 4.2 และพิจารณาความเสี่ยงและโอกาสที่จำเป็นต้องดำเนินการต่อไป เพื่อให้

- ก) มั่นใจว่าระบบการบริหารงานสามารถบรรลุผลลัพธ์ตามที่มุ่งหวังไว้
- ข) ป้องกันหรือลดผลกระทบที่ไม่ต้องการ
- ค) บรรลุซึ่งการปรับปรุงอย่างต่อเนื่อง

องค์กรต้องวางแผน

- ก) การปฏิบัติการเพื่อดำเนินการกับความเสี่ยงและโอกาสเหล่านี้
- ข) โดยใช่วิธีการว่าจะดำเนินการอย่างไรเพื่อ
  - 1) บูรณาการและนำการปฏิบัติการเข้าไปในกระบวนการของระบบการบริหารความต่อเนื่องทางธุรกิจขององค์กร (ดูข้อ 8.1)
  - 2) ประเมินประสิทธิผลของปฏิบัติการเหล่านี้ (ดูข้อ 9.1)

### 6.2 วัตถุประสงค์ความต่อเนื่องทางธุรกิจและแผนงานเพื่อให้บรรลุวัตถุประสงค์

ผู้บริหารสูงสุดต้องมั่นใจว่ามีการกำหนดวัตถุประสงค์ความต่อเนื่องทางธุรกิจและสื่อสารไปยังหน่วยงานในระดับต่างๆ ที่เกี่ยวข้องภายในองค์กร

วัตถุประสงค์ความต่อเนื่องทางธุรกิจต้อง

- ก) สอดคล้องกับนโยบายความต่อเนื่องทางธุรกิจ
- ข) คำนึงถึงระดับต่ำสุดของผลิตภัณฑ์และบริการที่สามารถยอมรับได้เพื่อให้บรรลุตามวัตถุประสงค์ทางธุรกิจขององค์กร
- ค) สามารถวัดได้
- ง) คำนึงถึงข้อกำหนดที่เกี่ยวข้อง
- จ) เฝ้าระวังและปรับให้ทันสมัยตามความเหมาะสม

องค์กรต้องเก็บรักษาเอกสารสารสนเทศเกี่ยวกับวัตถุประสงค์ความต่อเนื่องทางธุรกิจ

เพื่อให้บรรลุวัตถุประสงค์ความต่อเนื่องทางธุรกิจ องค์กรต้องพิจารณาถึง

- ผู้รับผิดชอบ
- สิ่งที่ต้องดำเนินการ
- ทรัพยากรที่ต้องการ
- กำหนดระยะเวลาแล้วเสร็จ
- วิธีการประเมินผล

## 7. การสนับสนุน

### 7.1 ทรัพยากร

องค์กรต้องพิจารณาและจัดเตรียมทรัพยากรที่จำเป็นสำหรับการจัดทำ การนำไปปฏิบัติ การรักษา และการปรับปรุงระบบการบริหารความต่อเนื่องทางธุรกิจอย่างต่อเนื่อง

### 7.2 ความสามารถ

องค์กรต้อง

- ก) พิจารณาความสามารถที่จำเป็นของบุคลากรที่ทำงานภายใต้การควบคุมขององค์กรที่ส่งผลกระทบต่อสมรรถนะ
- ข) มั่นใจว่าบุคลากรมีความสามารถบนพื้นฐานของการศึกษา การฝึกอบรม และประสบการณ์ที่เหมาะสม
- ค) ปฏิบัติการใดๆ เพื่อให้มั่นใจว่าบุคลากรมีความสามารถตามที่ต้องการ และมีการประเมินประสิทธิผลของปฏิบัติการที่ได้ดำเนินการเหล่านั้น หากสามารถทำได้
- ง) เก็บรักษาเอกสารสารสนเทศอย่างเหมาะสมเพื่อเป็นหลักฐานความสามารถ

หมายเหตุ ตัวอย่างปฏิบัติการที่สามารถทำได้ เช่น การจัดให้มีการฝึกอบรม การให้คำแนะนำ หรือการมอบหมายงานใหม่ให้ลูกจ้างปัจจุบัน หรือจ้างเหมาบุคลากรที่มีความสามารถ

### 7.3 ความตระหนัก

บุคลากรที่ทำงานภายใต้การควบคุมขององค์กรต้องมีความตระหนักต่อ

- ก) นโยบายความต่อเนื่องทางธุรกิจ
- ข) การมีส่วนร่วมช่วยให้ระบบการบริหารความต่อเนื่องทางธุรกิจเกิดประสิทธิผล รวมทั้งประโยชน์จากการปรับปรุงสมรรถนะของการบริหารความต่อเนื่องทางธุรกิจ

- ค) สิ่งที่ทำให้เกิดความไม่เป็นไปตามข้อกำหนดของระบบการบริหารความต่อเนื่องทางธุรกิจ
- ง) บทบาทหน้าที่ของตนเองในระหว่างที่เกิดอุบัติการณ์ที่ทำให้เกิดการหยุดชะงัก

#### 7.4 การสื่อสาร

องค์กรต้องพิจารณาสิ่งจำเป็นสำหรับการสื่อสารภายในและภายนอกที่เกี่ยวข้องกับระบบการบริหารความต่อเนื่องทางธุรกิจ ซึ่งรวมถึง

- ก) เนื้อหาสาระหรือประเด็นที่ต้องการสื่อสาร
- ข) เวลาที่เหมาะสมในการสื่อสาร
- ค) ผู้รับข้อมูล

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานสำหรับ

- การสื่อสารภายในระหว่างผู้มีส่วนได้เสียและลูกจ้างภายในองค์กร
- การสื่อสารภายนอกกับลูกค้า หน่วยงานที่เป็นหุ้นส่วน ชุมชนท้องถิ่น และผู้มีส่วนได้เสียอื่นๆ รวมทั้งสื่อมวลชนต่างๆ
- การรับ การทำเป็นเอกสาร และการตอบสนองต่อการสื่อสารต่างๆ จากผู้มีส่วนได้เสีย
- การปรับใช้ และการบูรณาการระบบให้คำปรึกษาเกี่ยวกับภัยคุกคาม (threat advisory system) ในระดับประเทศหรือระดับภูมิภาค หรือ เทียบเท่า ไปสู่การวางแผนและการดำเนินการหากมีความเหมาะสม
- มั่นใจว่ามีวิธีการสื่อสารอย่างเพียงพอในระหว่างที่เกิดอุบัติการณ์ที่ทำให้เกิดการหยุดชะงัก
- การสื่อสารตามโครงสร้างที่จัดเตรียมไว้ตามอำนาจหน้าที่อย่างเหมาะสม และมั่นใจว่ามีการดำเนินงานร่วมกันระหว่างองค์กรต่างๆ ที่ทำหน้าที่ตอบสนอง และบุคลากรตามความเหมาะสม
- การดำเนินการและการทดสอบขีดความสามารถของการสื่อสารที่ได้จัดเตรียมไว้ในระหว่างการเกิดอุบัติการณ์ที่ทำให้เกิดการหยุดชะงักจากการสื่อสารตามปกติ

หมายเหตุ ข้อกำหนดสำหรับการสื่อสารในการตอบสนองต่ออุบัติการณ์ได้กำหนดเพิ่มเติมไว้ในข้อ 8.4.2

## 7.5 เอกสารสารสนเทศ

### 7.5.1 ทั่วไป

ระบบการบริหารความต่อเนื่องทางธุรกิจขององค์กรต้องรวมถึง

- เอกสารสารสนเทศที่เป็นข้อกำหนดตามมาตรฐานนี้
- เอกสารสารสนเทศที่องค์กรพิจารณาแล้วว่าเป็นข้อกำหนดสำหรับระบบการบริหารความต่อเนื่องทางธุรกิจที่มีประสิทธิผล

หมายเหตุ ขอบเขตของเอกสารสารสนเทศสำหรับระบบการบริหารความต่อเนื่องทางธุรกิจสามารถแตกต่างกันในแต่ละองค์กร อันเนื่องมาจาก

- ขนาดขององค์กรและประเภทของกิจกรรม กระบวนการ ผลิตภัณฑ์ และบริการ
- ความซับซ้อนและปฏิสัมพันธ์ของกระบวนการ
- ความสามารถของบุคลากร

### 7.5.2 การจัดทำและการทำให้ทันสมัย

ในการจัดทำ หรือการทำให้เอกสารสารสนเทศมีความทันสมัย องค์กรต้องมั่นใจตามความเหมาะสมถึง

- ก) การชี้แจงและรายละเอียดของเอกสารสารสนเทศ เช่น หัวข้อ ชื่อ วันที่ ผู้แต่ง หมายเลข
- ข) รูปแบบ เช่น ภาษา รุ่นของซอฟต์แวร์ ภาพกราฟิก และสื่อที่ใช้ เช่น กระดาษ อิเล็กทรอนิกส์ และการทบทวนและการอนุมัติสำหรับความเพียงพอ

### 7.5.3 การควบคุมเอกสารสารสนเทศ

เอกสารสารสนเทศที่ต้องการสำหรับระบบการบริหารความต่อเนื่องทางธุรกิจ และตามข้อกำหนดของมาตรฐานนี้ต้องได้รับการควบคุมเพื่อมั่นใจว่า

- ก) มีเพียงพอและเหมาะสมเมื่อใช้งาน ตามสถานที่และเวลาที่ต้องการ
- ข) มีการปกป้องที่เพียงพอ (เช่น จากการไม่รักษาความลับ มีการใช้งานที่ไม่เหมาะสม หรือขาดซึ่งความซื่อสัตย์)

สำหรับการควบคุมเอกสารสารสนเทศ องค์กรต้องดำเนินกิจกรรมดังต่อไปนี้ ตามความเหมาะสม

- การแจกจ่าย การเข้าถึง การเรียกออกมาใช้ และการใช้
- การจัดเก็บและการดูแล รวมทั้งการดูแลเพื่อให้สามารถอ่านได้ง่าย เช่น มีความชัดเจนเพียงพอต่อการอ่าน
- การควบคุมการเปลี่ยนแปลง เช่น การควบคุมครั้งที่จัดทำ (version)
- ระยะเวลาการเก็บ และการทำลายทิ้ง
- การป้องกันการนำสารสนเทศที่ยกเลิกแล้วไปใช้โดยไม่ตั้งใจ

เอกสารสารสนเทศที่รับมาจากภายนอกองค์กรซึ่งได้พิจารณาแล้วว่ามีความจำเป็นสำหรับการวางแผน และการดำเนินการของระบบการบริหารความต่อเนื่องทางธุรกิจต้องมีการชี้แจงและควบคุมตามความเหมาะสม

ในการควบคุมเอกสารสารสนเทศ องค์กรต้องมั่นใจว่ามีการกำหนดถึงการปกป้องเอกสารสารสนเทศอย่างเพียงพอ เช่น การปกป้องจากการยินยอม การดัดแปลงแก้ไขจากผู้ที่ไม่มียานาจ หรือ การลบทิ้ง

*หมายเหตุ การเข้าถึง ให้มีความหมายว่าเป็นการตัดสินใจเกี่ยวกับการอนุญาตให้มองเห็นเอกสารสารสนเทศเท่านั้น หรือการอนุญาตและให้อำนาจในการมองเห็นและเปลี่ยนแปลงเอกสารสารสนเทศได้ด้วย ฯลฯ*

## 8. การดำเนินการ

### 8.1 การวางแผนและการควบคุมการดำเนินการ

องค์กรต้องพิจารณา วางแผน นำไปปฏิบัติ และควบคุมกระบวนการที่จำเป็นเพื่อให้เป็นไปตามข้อกำหนด และการดำเนินการตามข้อ 6.1 โดย

- ก) จัดทำเกณฑ์ควบคุมสำหรับกระบวนการเหล่านั้น
- ข) ควบคุมกระบวนการเหล่านั้นให้เป็นไปตามเกณฑ์ที่ได้กำหนดไว้
- ค) จัดเก็บเอกสารสารสนเทศเพื่อแสดงว่ามีการควบคุมกระบวนการตามแผนที่กำหนดไว้

องค์กรต้องควบคุมการเปลี่ยนแปลงจากที่ได้วางแผนไว้ และทบทวนผลที่จะเกิดตามมาจากการเปลี่ยนแปลงที่ไม่ได้ตั้งใจและดำเนินการเพื่อบรรเทาผลกระทบด้านลบตามความจำเป็น

องค์กรต้องมั่นใจว่ามีการควบคุมกระบวนการที่ให้องค์กรอื่นดำเนินการแทน

## 8.2 การวิเคราะห์ผลกระทบทางธุรกิจและการประเมินความเสี่ยง

### 8.2.1 ทั่วไป

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งกระบวนการที่กำหนดขึ้นเป็นเอกสารและเป็นทางการสำหรับการวิเคราะห์ผลกระทบทางธุรกิจและการประเมินความเสี่ยง ซึ่ง

- ก) กำหนดบริบทการประเมิน กำหนดเกณฑ์และประเมินถึงแนวโน้มของผลกระทบที่อาจเกิดขึ้นจากอุบัติการณ์ที่ทำให้เกิดการหยุดชะงัก
- ข) พิจารณาถึงกฎหมายและข้อกำหนดอื่นๆ ที่เกี่ยวข้องกับองค์กร
- ค) รวมถึงการวิเคราะห์อย่างเป็นระบบ การจัดลำดับความสำคัญของการจัดการความเสี่ยง และค่าใช้จ่ายที่เกี่ยวข้อง
- ง) กำหนดผลลัพธ์ที่ต้องการจากการวิเคราะห์ผลกระทบทางธุรกิจและการประเมินความเสี่ยง
- จ) ระบุข้อกำหนดเพื่อให้สารสนเทศนี้มีความทันสมัยและเป็นความลับ

หมายเหตุ การวิเคราะห์ผลกระทบทางธุรกิจและการประเมินความเสี่ยงมีอยู่หลายวิธี ซึ่งจะพิจารณาถึงลำดับก่อนหลังในการจัดการกับความเสี่ยงเหล่านี้

### 8.2.2 การวิเคราะห์ผลกระทบทางธุรกิจ

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งกระบวนการประเมินที่กำหนดขึ้นอย่างเป็นทางการและเป็นเอกสารสำหรับการพิจารณาถึงลำดับความสำคัญของความต่อเนื่องและการฟื้นฟู วัตถุประสงค์ และเป้าหมาย ซึ่งกระบวนการนี้ต้องรวมถึงการประเมินผลกระทบจากการหยุดชะงักของกิจกรรมที่มีส่วนสนับสนุนต่อผลิตภัณฑ์และบริการขององค์กรด้วย

การวิเคราะห์ผลกระทบทางธุรกิจต้องรวมถึงสิ่งต่างๆ ต่อไปนี้

- ก) การชี้แจงกิจกรรมที่สนับสนุนการส่งมอบผลิตภัณฑ์และบริการ
- ข) การประเมินผลกระทบตลอดช่วงระยะเวลาที่กิจกรรมเหล่านี้หยุดชะงัก
- ค) กำหนดลำดับความสำคัญของกรอบระยะเวลาเพื่อการกลับมาดำเนินการได้อีกครั้งของกิจกรรมเหล่านี้ในระดับขั้นต่ำสุดที่กำหนดซึ่งสามารถยอมรับได้ โดยคำนึงถึงระยะเวลาที่ไม่สามารถยอมรับได้หากไม่มีการแก้ไขผลกระทบนั้น
- ง) การชี้แจงถึงการพึ่งพาและทรัพยากรที่สนับสนุนกิจกรรมเหล่านี้ รวมทั้งผู้ส่งมอบ ผู้รับจ้าง (outsourcing partner) และผู้มีส่วนได้เสียอื่นๆ ที่เกี่ยวข้อง

### 8.2.3 การประเมินความเสี่ยง

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งกระบวนการประเมินความเสี่ยงที่กำหนดขึ้น  
อย่างเป็นทางการและเป็นเอกสาร สำหรับการชี้บ่ง การวิเคราะห์ และการประเมินความเสี่ยง  
จากอุบัติเหตุที่ทำให้เกิดการหยุดชะงักอย่างเป็นระบบ

หมายเหตุ กระบวนการนี้สามารถดำเนินการตามมาตรฐาน มอก.31000

องค์กรต้อง

- ก) ชี้บ่งความเสี่ยงของการหยุดชะงักต่อกิจกรรมที่มีความสำคัญขององค์กรและกระบวนการ ระบบ  
สารสนเทศ บุคลากร ลิขสิทธิ์ ผู้รับจ้าง และทรัพยากรอื่นที่สนับสนุนสิ่งเหล่านี้
- ข) วิเคราะห์ความเสี่ยงอย่างเป็นระบบ
- ค) ประเมินว่ามีความเสี่ยงที่เกี่ยวข้องกับการหยุดชะงักใดที่จำเป็นต้องมีการจัดการความเสี่ยง
- ง) ชี้บ่งการจัดการความเสี่ยงที่มีความเหมาะสมกับวัตถุประสงค์ความต่อเนื่องทางธุรกิจ และเป็นไป  
ตามระดับความเสี่ยงที่องค์กรสามารถยอมรับได้

หมายเหตุ องค์กรต้องตระหนักว่าข้อมูลพื้นฐานการเงินหรือของภาครัฐบางประการ จำเป็นต้อง  
สื่อสารรายละเอียดของความเสี่ยงเหล่านี้แตกต่างกันไปในแต่ละระดับ นอกจากนี้  
ความต้องการทางสังคมบางประการ สามารถเป็นการประกันถึงการแบ่งปันของ  
สารสนเทศในระดับของรายละเอียดที่เหมาะสม

## 8.3 กลยุทธ์ความต่อเนื่องทางธุรกิจ

### 8.3.1 การกำหนดและการเลือก

การกำหนดและการเลือกกลยุทธ์ต้องอยู่บนพื้นฐานของผลลัพธ์ที่มาจากการวิเคราะห์ผลกระทบ  
ทางธุรกิจและการประเมินความเสี่ยง

องค์กรต้องกำหนดกลยุทธ์ความต่อเนื่องทางธุรกิจอย่างเหมาะสมสำหรับ

- ก) การปกป้องกิจกรรมที่มีความสำคัญ
- ข) สร้างเสถียรภาพ ความต่อเนื่อง การกลับมาดำเนินการใหม่ และการฟื้นฟูกิจกรรมที่มีความสำคัญ  
และกิจกรรมที่เกี่ยวข้อง รวมทั้ง ทรัพยากรที่จำเป็นต่อกิจกรรมที่มีความสำคัญ
- ค) การบรรเทา การตอบสนอง และการจัดการผลกระทบ

การกำหนดกลยุทธ์ ต้องรวมถึง การอนุมัติกรอบเวลาในการกลับคืนมาดำเนินการของกิจกรรมที่มีความสำคัญ

องค์กรต้องประเมินขีดความสามารถของผู้ส่งมอบสำหรับการดำเนินธุรกิจอย่างต่อเนื่อง

#### 8.3.2 การจัดทำข้อกำหนดด้านทรัพยากร

องค์กรต้องพิจารณาข้อกำหนดด้านทรัพยากรเพื่อนำกลยุทธ์ที่ได้เลือกไว้ไปปฏิบัติ ประเภทของทรัพยากรที่นำมาพิจารณาอย่างน้อยต้องประกอบด้วย

- ก) บุคลากร
- ข) สารสนเทศและข้อมูล
- ค) อาคาร สภาพแวดล้อมในการทำงาน และสาธารณูปโภคที่เกี่ยวข้อง
- ง) สิ่งอำนวยความสะดวก อุปกรณ์ และโภคภัณฑ์
- จ) ระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- ฉ) การขนส่ง
- ช) การเงิน
- ซ) หุ้นส่วน และผู้ส่งมอบ

#### 8.3.3 การปกป้องและการบรรเทา

สำหรับความเสี่ยงที่กำหนดให้ต้องมีการลดความเสี่ยง องค์กรต้องพิจารณาถึงมาตรการเชิงรุก โดย

- ก) ลดโอกาสของการหยุดชะงัก
- ข) ทำให้ช่วงเวลาของการหยุดชะงักสั้นลง
- ค) จำกัดผลกระทบของการหยุดชะงักเฉพาะผลิตภัณฑ์และบริการที่สำคัญขององค์กร

องค์กรต้องเลือกและจัดการความเสี่ยงอย่างเหมาะสมให้สอดคล้องตามความเสี่ยงที่ยอมรับได้

### 8.4 การจัดทำและการนำขึ้นขั้นตอนการดำเนินงานการบริหารความต่อเนื่องทางธุรกิจไปปฏิบัติ

#### 8.4.1 ทั่วไป

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานการบริหารความต่อเนื่องทางธุรกิจ เพื่อจัดการกับอุบัติการณ์ที่ทำให้เกิดการหยุดชะงักและทำให้กิจกรรมสามารถดำเนินไปอย่างต่อเนื่องบนพื้นฐานของวัตถุประสงค์ของการฟื้นฟูที่ได้ระบุไว้จากการวิเคราะห์ผลกระทบทางธุรกิจ

องค์กรต้องจัดทำขั้นตอนการดำเนินงานเป็นเอกสารซึ่งรวมถึงการเตรียมการที่จำเป็น เพื่อให้มั่นใจว่ากิจกรรมสามารถดำเนินไปอย่างต่อเนื่องและมีการจัดการกับอุบัติการณ์ที่ทำให้เกิดการหยุดชะงัก

ขั้นตอนการดำเนินงานต้อง

- ก) กำหนดระเบียบวิธีการสำหรับการสื่อสารภายในและภายนอกอย่างเหมาะสม
- ข) มีความเฉพาะเจาะจงในขั้นตอนต่างๆ ที่ต้องดำเนินการทันทีในระหว่างหยุดชะงัก
- ค) มีความยืดหยุ่นต่อการตอบสนองภัยคุกคามที่ไม่ได้คาดการณ์ไว้ และต่อสถานการณ์ภายในและภายนอกที่มีการเปลี่ยนแปลง
- ง) มุ่งเน้นต่อผลกระทบจากเหตุการณ์ที่มีแนวโน้มทำให้เกิดการหยุดชะงัก
- จ) กำหนดขึ้นบนพื้นฐานของข้อสมมติฐานที่ได้ระบุไว้ และการวิเคราะห์การพึ่งพซึ่งกันและกัน
- ฉ) มีประสิทธิภาพในการลดผลกระทบให้เกิดขึ้นน้อยที่สุดโดยปฏิบัติตามกลยุทธ์สำหรับการบรรเทาที่เหมาะสม

#### 8.4.2 โครงสร้างการตอบสนองต่ออุบัติการณ์

องค์กรต้องจัดทำเอกสารขั้นตอนการดำเนินงานและนำไปปฏิบัติ และการจัดการโครงสร้างเพื่อตอบสนองต่ออุบัติการณ์ที่ทำให้เกิดการหยุดชะงัก โดยบุคลากรที่รับผิดชอบ มีอำนาจหน้าที่ และความสามารถที่จำเป็นในการจัดการกับอุบัติการณ์

โครงสร้างการตอบสนองต้อง

- ก) ระบุระดับของผลกระทบที่จะมีการตัดสินใจให้เริ่มตอบสนองอย่างเป็นทางการ
- ข) ประเมินลักษณะและขอบเขตของอุบัติการณ์ที่ทำให้เกิดการหยุดชะงัก และแนวโน้มของผลกระทบ
- ค) เริ่มต้นการตอบสนองความต่อเนื่องทางธุรกิจอย่างเหมาะสม
- ง) มีกระบวนการและขั้นตอนการดำเนินงานสำหรับการเริ่มต้น การดำเนินการ การประสานงาน และการสื่อสารในการตอบสนอง
- จ) มีทรัพยากรอย่างเพียงพอสำหรับใช้สนับสนุนกระบวนการและขั้นตอนการดำเนินงานในการจัดการกับอุบัติการณ์ที่ทำให้เกิดการหยุดชะงักเพื่อทำให้เกิดผลกระทบน้อยที่สุด
- ฉ) สื่อสารกับผู้มีส่วนได้เสียและผู้มีอำนาจตามกฎหมาย รวมทั้งสื่อต่างๆ

องค์กรต้องตัดสินใจโดยพิจารณาจากประเด็นความปลอดภัยของชีวิตว่าเป็นสิ่งสำคัญสูงสุด และได้ปรึกษาหารือกับผู้มีส่วนได้เสียแล้วว่าองค์กรจะสื่อสารไปยังภายนอกเกี่ยวกับความเสี่ยงและผลกระทบที่มีนัยสำคัญนี้หรือไม่ และให้จัดทำผลการตัดสินใจไว้เป็นเอกสาร หากการตัดสินใจให้สื่อสารไปยังภายนอก องค์กรต้องจัดทำและนำไปปฏิบัติซึ่งขั้นตอนการดำเนินงานสำหรับการสื่อสาร การเตือนภัย และการแจ้งเตือนไปยังภายนอก รวมทั้งสื่อที่ใช้ตามความเหมาะสม

#### 8.4.3 การแจ้งเตือนและการสื่อสาร

องค์กรต้องจัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งขั้นตอนการดำเนินงานสำหรับ

- ก) การตรวจหาอุบัติเหตุการณ์
- ข) การเฝ้าระวังอุบัติเหตุการณ์อย่างสม่ำเสมอ
- ค) การสื่อสารภายในองค์กรและการรับ การทำเป็นเอกสาร และการตอบสนองต่อการสื่อสารที่ได้รับจากผู้มีส่วนได้เสีย
- ง) การรับ การทำเป็นเอกสาร และการตอบสนองต่อระบบให้คำปรึกษาเกี่ยวกับความเสี่ยง (risk advisory system) ในระดับประเทศหรือระดับภูมิภาค หรือที่เทียบเท่า
- จ) การประกันว่าช่องทางที่ใช้สำหรับการสื่อสารในระหว่างเกิดอุบัติเหตุการณ์ที่ทำให้หยุดชะงักมีอยู่อย่างเพียงพอ
- ฉ) สร้างโครงข่ายในการสื่อสารกับหน่วยงานที่ทำหน้าที่ตอบสนองต่อภาวะฉุกเฉิน
- ช) บันทึกข้อมูลที่สำคัญเกี่ยวกับอุบัติเหตุการณ์ การปฏิบัติการและการตัดสินใจที่ได้ทำไปแล้ว สำหรับประเด็นต่อไปนี้ เป็นสิ่งที่ต้องพิจารณาและดำเนินการ หากสามารถทำได้
  - การเตือนภัยต่อผู้มีส่วนได้เสียที่มีแนวโน้มว่าจะได้รับผลกระทบจากอุบัติเหตุการณ์ที่ทำให้เกิดการหยุดชะงักที่เกิดขึ้นแล้ว หรือที่ใกล้จะเกิดขึ้น
  - การประกันว่าสามารถดำเนินงานร่วมกันในการตอบสนองระหว่างหลายองค์กรหรือบุคลากร
  - การใช้อุปกรณ์สื่อสาร

ขั้นตอนการดำเนินงานในการสื่อสารและการแจ้งเตือนต้องมีการฝึกซ้อมอย่างสม่ำเสมอ

#### 8.4.4 แผนความต่อเนื่องทางธุรกิจ

องค์กรต้องจัดทำเอกสารขั้นตอนการดำเนินงานสำหรับการตอบสนองต่ออุบัติเหตุการณ์ที่ทำให้เกิดการหยุดชะงัก และวิธีการที่จะดำเนินการได้อย่างต่อเนื่อง หรือการฟื้นฟูกิจกรรมภายในกรอบระยะเวลาที่ได้กำหนดไว้ ขั้นตอนการดำเนินงานดังกล่าวต้องระบุผู้รับผิดชอบในการนำขั้นตอนดังกล่าวไปปฏิบัติ

แผนความต่อเนื่องทางธุรกิจต้องประกอบด้วยหัวข้อต่อไปนี้

- ก) การกำหนดบทบาทหน้าที่และความรับผิดชอบสำหรับบุคลากรและทีมงานที่มีอำนาจหน้าที่ในระหว่างและภายหลังการเกิดอุบัติการณ์
- ข) กระบวนการสำหรับการให้เริ่มตอบสนองต่ออุบัติการณ์
- ค) รายละเอียดการจัดการจัดการกับผลกระทบที่เกิดขึ้นอย่างทันที่จากอุบัติการณ์ที่ทำให้เกิดการหยุดชะงัก โดยคำนึงถึง
  - 1) ศักยภาพของแต่ละบุคคล
  - 2) กลยุทธ์ ยุทธวิธี และทางเลือกในการดำเนินการสำหรับการตอบสนองต่อการหยุดชะงัก
  - 3) การป้องกันความเสียหายที่จะเกิดขึ้นเพิ่มเติม หรือการสูญเสียกิจกรรมที่สำคัญ
- ง) รายละเอียดของวิธีการและสถานการณ์ที่องค์กรจะสื่อสารกับพนักงานและบุคคลที่เกี่ยวข้อง ผู้มีส่วนได้เสียที่สำคัญ และหน่วยงานที่ต้องติดต่อเมื่อเกิดเหตุฉุกเฉิน
- จ) วิธีการที่องค์กรจะเริ่มดำเนินกิจกรรมหรือฟื้นฟูกิจกรรมที่มีความสำคัญภายในกรอบระยะเวลาที่ได้พิจารณากำหนดไว้ล่วงหน้า
- ฉ) รายละเอียดของการตอบสนองของสื่อขององค์กรภายหลังการเกิดอุบัติการณ์ ซึ่งรวมถึง
  - 1) กลยุทธ์การสื่อสาร
  - 2) วิธีการที่ต้องการในการประสานกับสื่อ
  - 3) แนวทางหรือรูปแบบสำหรับร่างแถลงการณ์สำหรับสื่อมวลชน
  - 4) ผู้แถลงข่าวที่มีความเหมาะสม
- ช) กระบวนการสำหรับการถอนตัวภายหลังอุบัติการณ์สิ้นสุดลง

แต่ละแผนต้องกำหนด

- เป้าหมายและขอบข่าย
- วัตถุประสงค์
- เกณฑ์สำหรับการเริ่มปฏิบัติการและขั้นตอนการดำเนินงาน
- การปฏิบัติตามขั้นตอนการดำเนินงาน
- บทบาทหน้าที่ ความรับผิดชอบ และอำนาจหน้าที่
- ข้อกำหนดและขั้นตอนการดำเนินงานสำหรับการสื่อสาร

- การพึ่งพากันและปฏิสัมพันธ์ระหว่างหน่วยงานภายในและภายนอก
- ทรัพยากรที่ต้องการ
- แผนผังของสารสนเทศ และกระบวนการด้านการเอกสาร

#### 8.4.5 การฟื้นฟู

องค์กรต้องมีเอกสารขั้นตอนการดำเนินงานในการฟื้นฟู และทำให้กิจกรรมทางด้านธุรกิจที่ดำเนินการตามมาตรการชั่วคราวกลับสู่การดำเนินการตามภาวะปกติภายหลังอุบัติการณ์

#### 8.5 การฝึกซ้อมและการทดสอบ

องค์กรต้องฝึกซ้อมและทดสอบขั้นตอนการดำเนินงานความต่อเนื่องทางธุรกิจเพื่อให้มั่นใจว่าขั้นตอนมีความสอดคล้องกับวัตถุประสงค์ความต่อเนื่องทางธุรกิจขององค์กร

องค์กรต้องดำเนินการฝึกซ้อมและทดสอบ โดยที่

- ก) สอดคล้องกับขอบข่ายและวัตถุประสงค์ของระบบการบริหารความต่อเนื่องทางธุรกิจ
- ข) อยู่บนพื้นฐานของสถานการณ์สมมติที่เหมาะสม และมีการวางแผนเป็นอย่างดี โดยมีเป้าหมายและวัตถุประสงค์ซึ่งได้กำหนดไว้อย่างชัดเจน
- ค) ทบทวนความใช้ได้ของการดำเนินการเพื่อความต่อเนื่องของธุรกิจที่เกี่ยวข้องกับผู้มีส่วนได้เสีย โดยดำเนินการร่วมกันเมื่อเวลาผ่านไป
- ง) ลดความเสี่ยงจากการหยุดชะงักของการดำเนินการให้เหลือน้อยที่สุด
- จ) จัดทำรายงานสรุปผลภายหลังการทดสอบที่รวมถึงผลลัพธ์ ข้อเสนอแนะ และสิ่งที่ต้องปรับปรุงต่อไป
- ฉ) ได้รับการทบทวนภายใต้บริบทของการส่งเสริมการปรับปรุงอย่างต่อเนื่อง
- ช) ดำเนินการตามช่วงเวลาที่ได้วางแผนไว้ และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญเกิดขึ้นภายในองค์กร หรือต่อสภาพแวดล้อมของการดำเนินงานขององค์กร

## 9. การประเมินสมรรถนะ

### 9.1 การเฝ้าระวัง การวัด การวิเคราะห์ และการประเมิน

#### 9.1.1 ทั่วไป

องค์กรต้องพิจารณาถึง

ก) สิ่งที่ต้องการวัดและเฝ้าระวัง

ข) วิธีการสำหรับการเฝ้าระวัง การวัด การวิเคราะห์ และการประเมิน เพื่อให้มั่นใจถึงความถูกต้องของผลลัพธ์ตามความเหมาะสม

ค) เวลาที่ต้องดำเนินการวัดและเฝ้าระวัง

ง) เวลาที่ต้องดำเนินการวิเคราะห์และการประเมินผลลัพธ์ที่ได้จากการวัดและเฝ้าระวัง

องค์กรต้องเก็บรักษาเอกสารสารสนเทศเพื่อเป็นหลักฐานแสดงถึงผลลัพธ์อย่างเหมาะสม

องค์กรต้องประเมินสมรรถนะและประสิทธิผลของระบบการบริหารความต่อเนื่องทางธุรกิจ

นอกจากนี้ องค์กรต้อง

- ดำเนินการกับแนวโน้มหรือผลลัพธ์ในเชิงลบกรณีที่เกิดขึ้น ก่อนที่ความไม่เป็นไปตามข้อกำหนดจะเกิดขึ้น

- เก็บรักษาเอกสารสารสนเทศเพื่อเป็นหลักฐานแสดงถึงผลลัพธ์

ขั้นตอนการดำเนินงานสำหรับการเฝ้าระวังสมรรถนะ ต้องให้ได้มาซึ่ง

- การกำหนดหน่วยวัดสมรรถนะ (performance metrics) ที่เหมาะสมกับความต้องการขององค์กร

- ขอบเขตการเฝ้าระวังครอบคลุมถึงการบรรลุนโยบาย วัตถุประสงค์ และเป้าหมายความต่อเนื่องทางธุรกิจขององค์กร

- สมรรถนะของกระบวนการ ขั้นตอนการดำเนินงาน และหน่วยงานที่ทำการปกป้องกิจกรรมที่มีความสำคัญ

- การเฝ้าระวังความเป็นไปตามข้อกำหนดของมาตรฐานนี้และวัตถุประสงค์ความต่อเนื่องทางธุรกิจ

- การเฝ้าระวังหลักฐานของความบกพร่องของการดำเนินระบบการบริหารความต่อเนื่องทางธุรกิจที่เกิดขึ้นในอดีต

- การบันทึกข้อมูลและผลลัพธ์ของการเฝ้าระวังและการวัดเพื่อนำมาช่วยในการปฏิบัติการแก้ไขในภายหลัง

หมายเหตุ ข้อบกพร่องของการดำเนินงาน สามารถรวมถึงความไม่เป็นไปตามข้อกำหนด เหตุการณ์ที่เกือบจะสูญเสีย ความล้มเหลวของการเตือนภัย และอุบัติการณ์ที่เกิดขึ้นจริง

9.1.2 ขั้นตอนการดำเนินการประเมินผลของความต่อเนื่องทางธุรกิจ

- ก) องค์กรต้องประเมินขั้นตอนการดำเนินงานด้านความต่อเนื่องทางธุรกิจและขีดความสามารถขององค์กรเพื่อให้มั่นใจว่าขั้นตอนดังกล่าวยังคงมีความเหมาะสม พอเพียง และมีประสิทธิผล
- ข) การประเมินต้องพิจารณาถึงการทบทวนตามช่วงเวลาที่กำหนดไว้ การฝึกซ้อม การทดสอบ การรายงานภายหลังการเกิดอุบัติการณ์ และการประเมินสมรรถนะ การเปลี่ยนแปลงอย่างมีนัยสำคัญที่เกิดขึ้นต้องมีการนำไปปรับปรุงขั้นตอนการดำเนินงานภายในระยะเวลาที่เหมาะสม
- ค) องค์กรต้องประเมินความสอดคล้องกับข้อกำหนดของกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง การปฏิบัติที่เป็นเลิศในภาคอุตสาหกรรมนั้นๆ และการเป็นไปตามนโยบายและวัตถุประสงค์ความต่อเนื่องทางธุรกิจขององค์กรตามช่วงเวลาที่กำหนด

ง) องค์กรต้องประเมินตามช่วงเวลาที่ได้วางแผนไว้และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

เมื่อเกิดอุบัติการณ์ที่ทำให้เกิดการหยุดชะงักและเป็นผลให้มีการดำเนินการตามขั้นตอนการดำเนินงานความต่อเนื่องทางธุรกิจ องค์กรต้องทบทวนภายหลังการเกิดอุบัติการณ์นั้นและบันทึกผลลัพธ์ไว้

9.2 การตรวจประเมินภายใน

องค์กรต้องตรวจประเมินภายในองค์กรตามช่วงเวลาที่กำหนดไว้ เพื่อให้ได้สารสนเทศมาประกอบการพิจารณาว่าระบบการบริหารความต่อเนื่องทางธุรกิจ

ก) เป็นไปตาม

- 1) ข้อกำหนดสำหรับระบบการบริหารความต่อเนื่องทางธุรกิจขององค์กร
- 2) ข้อกำหนดของมาตรฐานนี้

ข) มีการนำไปปฏิบัติและรักษาไว้ได้อย่างมีประสิทธิภาพ

องค์กรต้อง

- วางแผน จัดทำ นำไปปฏิบัติ และรักษาไว้ซึ่งโปรแกรมการตรวจประเมิน รวมทั้งความถี่ วิธีการ ความรับผิดชอบ ข้อกำหนดในการวางแผน และการรายงาน โดยโปรแกรมการตรวจประเมินต้องคำนึงถึงความสำคัญของกระบวนการที่เกี่ยวข้องและผลจากการตรวจประเมินครั้งก่อน
- ระบุเกณฑ์การตรวจประเมินและขอบข่ายสำหรับการตรวจประเมินแต่ละครั้ง

- คัดเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินเพื่อให้มั่นใจถึงความเป็นรูปธรรมและความเป็นกลางของกระบวนการตรวจประเมิน
- มั่นใจว่ามีการรายงานผลการตรวจประเมินให้ผู้บริหารที่เกี่ยวข้อง
- เก็บรักษาเอกสารสารสนเทศเพื่อเป็นหลักฐานแสดงการนำโปรแกรมการตรวจประเมินไปปฏิบัติและผลการตรวจประเมิน

โปรแกรมการตรวจประเมิน รวมทั้งกำหนดการใดๆ ต้องอยู่บนพื้นฐานจากผลการประเมินความเสี่ยงจากกิจกรรมต่างๆ ขององค์กร และผลของการตรวจประเมินที่ผ่านมา ขั้นตอนการดำเนินงานการตรวจประเมินต้องครอบคลุมถึงขอบข่าย ความถี่ วิธีการ และความสามารถ รวมทั้งความรับผิดชอบและข้อกำหนดสำหรับการตรวจประเมินและการรายงานผล

ผู้บริหารที่รับผิดชอบในพื้นที่ที่รับการตรวจประเมินต้องมั่นใจว่าได้ทำการแก้ไขและการปฏิบัติการแก้ไขที่จำเป็นโดยไม่ชักช้าเพื่อกำจัดสิ่งที่ไม่เป็นไปตามข้อกำหนดที่ตรวจพบรวมทั้งสาเหตุ กิจกรรมในการตรวจติดตามผลต้องรวมถึงการทวนสอบผลของการดำเนินการและการรายงานผลของการทวนสอบ

### 9.3 การทบทวนการบริหารงาน

ผู้บริหารสูงสุดต้องทบทวนระบบการบริหารความต่อเนื่องทางธุรกิจขององค์กรตามช่วงเวลาที่กำหนดไว้เพื่อให้มั่นใจว่ายังคงเหมาะสม เพียงพอ และมีประสิทธิผลอย่างต่อเนื่อง

การทบทวนการบริหารงานต้องพิจารณาถึง

- ก) สถานะของการปฏิบัติการจากการทบทวนการบริหารงานครั้งก่อน
- ข) การเปลี่ยนแปลงประเด็นภายนอกและภายในที่เกี่ยวข้องกับระบบการบริหารความต่อเนื่องทางธุรกิจ
- ค) สารสนเทศของสมรรถนะของความต่อเนื่องทางธุรกิจ รวมทั้งแนวโน้มเกี่ยวกับ
  - 1) ความไม่เป็นไปตามข้อกำหนดและการปฏิบัติการแก้ไข
  - 2) ผลการประเมินการเฝ้าระวังและการวัด
  - 3) ผลการตรวจประเมิน
- ง) โอกาสสำหรับการปรับปรุงอย่างต่อเนื่อง

การทบทวนการบริหารงานต้องพิจารณาถึงสมรรถนะขององค์กร ประกอบด้วย

- การติดตามผลปฏิบัติการจากการทบทวนการบริหารงานครั้งก่อน
- ความจำเป็นในการเปลี่ยนแปลงระบบการบริหารความต่อเนื่องทางธุรกิจ รวมทั้งนโยบายและวัตถุประสงค์
- โอกาสสำหรับการปรับปรุง
- ผลการตรวจประเมินและการทบทวนระบบการบริหารความต่อเนื่องทางธุรกิจ รวมทั้งผู้ส่งมอบและหุ้นส่วนที่สำคัญตามความเหมาะสม
- เทคนิค ผลิตภัณฑ์ หรือขั้นตอนการดำเนินงานที่อาจนำข้อบกพร่องเพื่อการปรับปรุงสมรรถนะและประสิทธิผลของระบบการบริหารความต่อเนื่องทางธุรกิจ
- สถานะของการปฏิบัติการแก้ไข
- ผลจากการฝึกซ้อมและการทดสอบ
- ความเสี่ยงหรือประเด็นต่างๆ ที่ไม่ได้ระบุไว้ในการประเมินความเสี่ยงที่ผ่านมา
- การเปลี่ยนแปลงใดๆ ทั้งภายในและภายนอกที่อาจส่งผลกระทบต่อขอบข่ายของระบบการบริหารความต่อเนื่องทางธุรกิจ
- ความเพียงพอของนโยบาย
- ข้อเสนอแนะสำหรับการปรับปรุง
- การเรียนรู้และการดำเนินการที่เกิดขึ้นจากอุบัติการณ์ที่ทำให้เกิดการหยุดชะงัก
- การปฏิบัติที่ดีและข้อเสนอแนะใหม่ๆ

ผลจากการทบทวนการบริหารงานต้องรวมถึงการตัดสินใจและการดำเนินการที่เกี่ยวข้องกับโอกาสในการปรับปรุงอย่างต่อเนื่องและความต้องการให้มีการเปลี่ยนแปลงที่เป็นไปได้ต่อระบบการบริหารความต่อเนื่องทางธุรกิจ และประกอบด้วยรายละเอียดดังต่อไปนี้

- ก) ความหลากหลายของขอบข่ายของระบบการบริหารความต่อเนื่องทางธุรกิจ
- ข) การปรับปรุงประสิทธิผลของระบบการบริหารความต่อเนื่องทางธุรกิจ
- ค) การปรับการประเมินความเสี่ยง การวิเคราะห์ผลกระทบทางธุรกิจ แผนความต่อเนื่องทางธุรกิจ และขั้นตอนการดำเนินงานที่เกี่ยวข้องให้ทันสมัย

ง) การปรับเปลี่ยน (modification) ขั้นตอนการดำเนินงานและการควบคุมการตอบสนองต่อเหตุการณ์ภายในหรือภายนอกที่อาจส่งผลกระทบต่อระบบการบริหารความต่อเนื่องทางธุรกิจ รวมทั้งการเปลี่ยนแปลงต่อ

- 1) ข้อกำหนดทางธุรกิจและการดำเนินการ
- 2) ข้อกำหนดในการลดความเสี่ยงและข้อกำหนดด้านความมั่นคง
- 3) สภาพและกระบวนการในการดำเนินการ
- 4) ข้อกำหนดของกฎหมายและระเบียบข้อบังคับต่างๆ
- 5) เงื่อนไขความรับผิดชอบตามข้อตกลง (contractual obligation)
- 6) ระดับของความเสี่ยง และ/หรือ เกณฑ์ในการยอมรับความเสี่ยง
- 7) ทรัพยากรที่จำเป็น
- 8) ข้อกำหนดด้านแหล่งทุนและงบประมาณ

จ) วิธีการวัดถึงประสิทธิผลของการควบคุม

องค์กรต้องเก็บรักษาไว้ซึ่งเอกสารสารสนเทศเพื่อเป็นหลักฐานของผลการทบทวนการบริหารงาน  
องค์กรต้อง

- สื่อสารผลการทบทวนการบริหารงานไปยังผู้มีส่วนได้เสียที่เกี่ยวข้อง
- ปฏิบัติการที่เกี่ยวข้องกับผลการทบทวนเหล่านั้นอย่างเหมาะสม

## 10. การปรับปรุง

10.1 ความไม่เป็นไปตามข้อกำหนดและการปฏิบัติการแก้ไข

เมื่อเกิดความไม่เป็นไปตามข้อกำหนด องค์กรต้อง

ก) ชี้บ่งความไม่เป็นไปตามข้อกำหนด

ข) ตอบสนองต่อสิ่งที่ไม่เป็นไปตามข้อกำหนด และวิธีต่อไปนี้หากทำได้

- 1) ปฏิบัติการเพื่อการควบคุม และแก้ไขความไม่เป็นไปตามข้อกำหนดเหล่านี้
- 2) ดำเนินการต่อผลที่เกิดขึ้น

- ค) องค์กรต้องประเมินความจำเป็นในการปฏิบัติการเพื่อจัดสาเหตุของความไม่ปฏิบัติตามข้อกำหนด ด้วย เพื่อไม่ให้เกิดซ้ำหรือเกิดขึ้นในที่อื่นใด โดย
- 1) ทบทวนความไม่ปฏิบัติตามข้อกำหนด
  - 2) พิจารณาสาเหตุของความไม่ปฏิบัติตามข้อกำหนด
  - 3) พิจารณาว่ามีความไม่สอดคล้องที่คล้ายคลึงกันเกิดขึ้นหรือมีแนวโน้มเกิดขึ้นหรือไม่
  - 4) ประเมินความจำเป็นสำหรับการปฏิบัติการแก้ไขเพื่อให้มั่นใจว่าความไม่ปฏิบัติตามข้อกำหนดจะไม่เกิดซ้ำหรือเกิดขึ้นในที่อื่นอีก
  - 5) พิจารณาและนำการปฏิบัติแก้ไขไปปฏิบัติตามที่จำเป็น
  - 6) ทบทวนประสิทธิผลของการปฏิบัติการแก้ไขที่ได้ดำเนินการไป
  - 7) เปลี่ยนแปลงระบบการบริหารความต่อเนื่องทางธุรกิจ หากจำเป็น
- ง) นำการปฏิบัติการใดๆ ที่จำเป็นไปปฏิบัติ
- จ) ทบทวนประสิทธิผลของการปฏิบัติการแก้ไขที่ได้ดำเนินการไป
- ฉ) เปลี่ยนแปลงระบบการบริหารความต่อเนื่องทางธุรกิจ หากจำเป็น
- การปฏิบัติการแก้ไขต้องเหมาะสมกับผลกระทบจากความไม่ปฏิบัติตามข้อกำหนดที่พบ
- องค์กรต้องเก็บรักษาเอกสารสารสนเทศเพื่อเป็นหลักฐานของ
- ลักษณะของความไม่ปฏิบัติตามข้อกำหนดและการปฏิบัติการที่ได้ดำเนินการหลังจากนั้น
  - ผลของการปฏิบัติการแก้ไข

## 10.2 การปรับปรุงอย่างต่อเนื่อง

องค์กรต้องปรับปรุงอย่างต่อเนื่องเพื่อการคงไว้ซึ่งระบบการบริหารความต่อเนื่องทางธุรกิจที่เหมาะสมเพียงพอ หรือเกิดประสิทธิผล

หมายเหตุ องค์กรสามารถใช้กระบวนการของระบบการบริหารความต่อเนื่องทางธุรกิจ เช่น ความเป็นผู้นำ การวางแผน และการประเมินสมรรถนะเพื่อบรรลุผลในการปรับปรุง