



แนวทางปฏิบัติ

องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย

เรื่อง การบริหารความต่อเนื่องทางธุรกิจ
(Business Continuity Management : BCM)
และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง
(Business Continuity Plan : BCP)
ภัยคุกคามทางไซเบอร์ (Cyber Threat)

สารบัญ

หน้า

บทนำ

บทที่ 1 การบริหารจัดการความต่อเนื่องทางธุรกิจ

- 1.1 นโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) 2
- 1.2 โครงสร้างการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management BCM) 3
- 1.3 ความหมาย Business Continuity Management (BCM) 5
- 1.4 วัตถุประสงค์ (Objectives) ของการจัดทำแผนดำเนินธุรกิจอย่างต่อเนื่อง 6
- 1.5 แนวทางการบริหารความต่อเนื่อง (Business Continuity Management) 6
- 1.6 ขอบเขตของแผนดำเนินธุรกิจอย่างต่อเนื่อง (Scope of BCP) 7
- 1.7 คำจำกัดความตามแผนความต่อเนื่องทางธุรกิจ (Definition) 8
- 1.8 สมมติฐานของแผนดำเนินธุรกิจอย่างต่อเนื่อง (BCM Assumptions) 10

บทที่ 2 การศึกษาและทำความเข้าใจองค์กร (Understanding the Organization)

- 2.1 การวิเคราะห์ผลกระทบทางธุรกิจ 13
- 2.2 การประเมินความเสี่ยง 14

บทที่ 3 การกำหนดกลยุทธ์ในการสร้างความต่อเนื่อง BCM

(Determining BCM strategy)

- 3.1 ผลลัพธ์จากการวิเคราะห์ผลกระทบทางธุรกิจ BIA (Business Impact Analysis) 22
- 3.2 การวิเคราะห์ระยะเวลาผ่านผลกระทบทางธุรกิจ (BIA) 26

บทที่ 4 การพัฒนาและเตรียมการตอบสนองต่อเหตุการณ์ในภาวะฉุกเฉิน

(Developing and Implementing BCM Response)

- 4.1 เหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจมตี) 28
- 4.2 แผนบริหารความต่อเนื่องทางธุรกิจกรณีอัคคีภัย 30

สารบัญ

หน้า

| | |
|---|----|
| บทที่ 5 การทดสอบ ปรับปรุง และทบทวนแผน (Exercising Maintaining and Reviewing) | |
| 5.1 กระบวนการแจ้งเหตุฉุกเฉิน Call tree | 33 |
| 5.2 กระบวนการแจ้งเหตุ Call tree | 35 |
| 5.3 Tabletop Testing | 35 |
| 5.4 Simulation | 35 |
| 5.5 Full BCP Exercise | 36 |
| 5.6 การดูแลปรับปรุงแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Maintenance of the plan) | 36 |

บทที่ 6 การปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร (Embedding BCM in the Organization's Culture)

| | |
|--|----|
| 6.1 การปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร | 38 |
|--|----|

สารบัญภาพ

| | |
|---|----|
| รูปที่ 1 โครงสร้างการบริหารความต่อเนื่องทางธุรกิจ (BCM) | 3 |
| รูปที่ 2 วงจรการบริหารความต่อเนื่อง (BCM Life Cycle) | 6 |
| รูปที่ 3 ความสัมพันธ์ระหว่างค่า RTO และ MTPD | 13 |
| รูปที่ 4 Risk Matrix | 14 |
| รูปที่ 5 แผนผังแสดงการดำเนินการในเบื้องต้นของเหตุการณ์ภัยคุกคามทางไซเบอร์ | 28 |
| รูปที่ 6 ขั้นตอนการปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร | 39 |

สารบัญตาราง

| | หน้า |
|---|------|
| ตารางที่ 1 รายชื่อบุคลากรและบทบาทของทีมงานแผนบริหารความต่อเนื่องทางธุรกิจ (BCM) | 4 |
| ตารางที่ 2 รายชื่อบุคลากรและบทบาทของทีมงานแผนบริหารความต่อเนื่องทางธุรกิจ ด้านเทคโนโลยีสารสนเทศและการจัดการเหตุฉุกเฉิน | 5 |
| ตารางที่ 3 สรุปเหตุการณ์สภาวะวิกฤตและผลกระทบจากเหตุการณ์ | 7 |
| ตารางที่ 4 แสดงคำจำกัดความการบริหารความต่อเนื่องทางธุรกิจ (BCM) | 8 |
| ตารางที่ 5 แนวทางการบริหารความต่อเนื่องรายกิจกรรมที่มีระดับความสำคัญสูง | 11 |
| ตารางที่ 6 แสดงเกณฑ์การวิเคราะห์โอกาสเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ต่อกระบวนการทำงานหรือการให้บริการ (Business Impact Analysis) | 15 |
| ตารางที่ 7 แสดงเกณฑ์การประเมินผลกระทบต่อกระบวนการทำงาน (Business Impact Analysis) | 16 |
| ตารางที่ 8 แสดงเกณฑ์การประเมินด้านพนักงานและภาพลักษณ์ชื่อเสียง | 16 |
| ตารางที่ 9 แสดงเกณฑ์ระยะเวลาหยุดดำเนินการสูงสุดที่ยอมรับได้ | 17 |
| ตารางที่ 10 แสดงระยะเวลาเป้าหมายในการฟื้นคืนสภาพ | 17 |
| ตารางที่ 11 แสดงผลการประเมินความเสี่ยง กรณีเหตุการณ์ภัยคุกคามทางไซเบอร์ | 19 |
| ตารางที่ 12 แสดงผลกระทบด้านความเสี่ยง กรณีเหตุการณ์ภัยคุกคามทางไซเบอร์ | 20 |
| ตารางที่ 13 ตารางแสดงการวิเคราะห์ผลกระทบ | 23 |
| ตารางที่ 14 ผลลัพธ์จากการวิเคราะห์ผลกระทบทางธุรกิจ | 23 |
| ตารางที่ 15 ตารางแสดงกรณีระบบ AD ใช้งานไม่ได้ 3 ชั่วโมง | 24 |
| ตารางที่ 16 ตารางแสดงกรณีระบบ AD ใช้งานไม่ได้ 8 ชั่วโมง | 24 |
| ตารางที่ 17 ตารางแสดงกรณีระบบ AD ใช้งานไม่ได้ 24 ชั่วโมง | 25 |
| ตารางที่ 18 ตารางแสดงกรณีระบบ AD ใช้งานไม่ได้มากกว่า 1 วัน | 25 |
| ตารางที่ 19 ผลลัพธ์จากการวิเคราะห์ผลกระทบทางธุรกิจ | 26 |
| ตารางที่ 20 ตารางแสดงแผนบริหารความต่อเนื่องทางธุรกิจกรณีภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจมตี) | 30 |

ภาคผนวก

- นโยบายการบริหารความต่อเนื่องทางธุรกิจ อ.ส.ค.
 - คำสั่งแต่งตั้งคณะกรรมการบริหารความต่อเนื่องทางธุรกิจของ อ.ส.ค.
 - คำสั่งแต่งตั้งคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ ด้านเทคโนโลยีสารสนเทศและแผนจัดการเหตุฉุกเฉิน (Business Continuity plan : BCP)
 - ภาพกิจกรรมการฝึกซ้อมเหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจมตี)
- ประจำปี 2566

บทนำ

องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย (อ.ส.ค.) ได้จัดทำแผน BCM เรื่อง “ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม)” ขึ้น เพื่อเป็นการเตรียมความพร้อมองค์กร และสามารถนำไปใช้ในการตอบสนองการปฏิบัติงานในเหตุการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม) โดยไม่ให้เหตุการณ์ฉุกเฉินดังกล่าวส่งผลให้หน่วยงานต้องหยุดการดำเนินงาน หรือไม่สามารถให้บริการได้อย่างต่อเนื่อง

การที่ อ.ส.ค. ไม่มีกระบวนการรองรับให้การดำเนินงานเป็นไปอย่างต่อเนื่อง อาจส่งผลกระทบต่อ อ.ส.ค. ในด้านต่าง ๆ เช่น เศรษฐกิจ การเงิน การให้บริการ สังคม ชุมชน สิ่งแวดล้อม ชีวิตและทรัพย์สินของประชาชน เป็นต้น ดังนั้น การจัดทำแผนดำเนินธุรกิจอย่างต่อเนื่องจึงเป็นสิ่งสำคัญที่จะช่วยให้ อ.ส.ค. สามารถรับมือกับเหตุการณ์ที่ไม่คาดคิด และทำให้กระบวนการที่สำคัญ Business Continuity Management กลับมาดำเนินงานได้อย่างปกติในระดับการให้บริการที่กำหนดไว้ รวมทั้งลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นต่อ อ.ส.ค. ได้

แผนบริหารความต่อเนื่องฉบับนี้จัดทำขึ้น เพื่อให้องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย (อ.ส.ค.) สามารถดำเนินงานอย่างต่อเนื่องและมีประสิทธิภาพ เพื่อสามารถจัดการและปรับปรุง แก้ไขได้ภายใต้ระยะเวลาที่เหมาะสม อีกทั้งสามารถนำไปประยุกต์ใช้หากเกิดสถานการณ์อื่นๆ

บทที่ 1

การบริหารจัดการความต่อเนื่องทางธุรกิจ
(Business Continuity Management : BCM)

1.1 นโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management BCM)

องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย (อ.ส.ค.) เป็นองค์กรรัฐวิสาหกิจที่ดำเนินกิจการด้านอุตสาหกรรมนม ซึ่งครอบคลุมกิจกรรมตั้งแต่ต้นน้ำ (ส่งเสริม) กลางน้ำ (ผลิต) และปลายน้ำ (จำหน่าย) โดยต้องดำเนินการผลิตและจำหน่ายผลิตภัณฑ์จากนมโคที่มีคุณภาพในปริมาณที่สอดคล้องกับความต้องการของตลาดในแต่ละพื้นที่ ทั้งนี้ในการดำเนินกิจการมีโอกาสเกิดอุบัติเหตุต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักของกิจกรรมสำคัญซึ่งอาจส่งผลกระทบต่อผู้มีส่วนได้ส่วนเสีย ภาพลักษณ์ชื่อเสียงและกิจกรรมสำคัญขององค์กร อ.ส.ค. ได้เล็งเห็นถึงความสำคัญของการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจเพื่อเตรียมความพร้อมในการรองรับอุบัติเหตุต่าง ๆ เพื่อป้องกันและบรรเทาผลกระทบที่อาจจะเกิดขึ้นของอุบัติเหตุจึงได้กำหนดนโยบายการบริหารความต่อเนื่องทางธุรกิจของ อ.ส.ค. ไว้ดังนี้

1. อ.ส.ค. ต้องพัฒนาระบบการบริหารความต่อเนื่องทางธุรกิจให้สอดคล้องกับมาตรฐานสากล ซึ่งต้องมีความครอบคลุมถึงการวิเคราะห์ผลกระทบทางธุรกิจ การประเมินความเสี่ยง การวางกลยุทธ์ การนำไปปฏิบัติ การฝึกซ้อม การทบทวนปรับปรุงแก้ไขแผนอย่างต่อเนื่อง ตลอดจนการปลูกฝังจิตสำนึกด้านการบริหารความต่อเนื่องทางธุรกิจสู่วัฒนธรรมองค์กร ผ่านกระบวนการฝึกอบรมและการสื่อสารภายในองค์กรให้มีประสิทธิผล

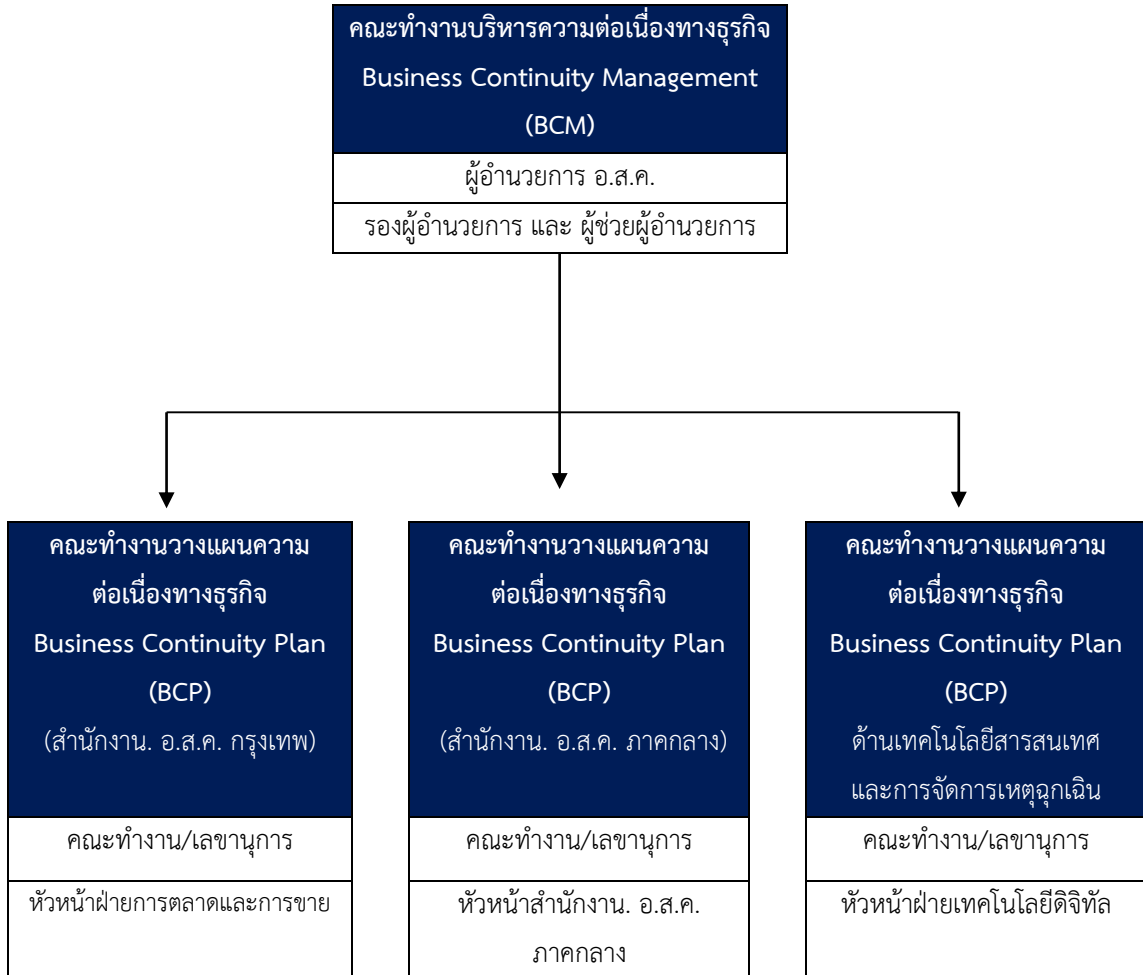
2. ให้คณะกรรมการบริหารความต่อเนื่องทางธุรกิจ (BCM Team) ของ อ.ส.ค. มีหน้าที่ในการจัดทำระบบการบริหารความต่อเนื่องทางธุรกิจ และดำเนินการต่างๆ เพื่อให้เกิดการบริหารจัดการความต่อเนื่องทางธุรกิจที่มีประสิทธิผล

3. ให้ผู้บริหารทุกระดับของ อ.ส.ค. มีหน้าที่ผลักดัน และสนับสนุนการดำเนินงานต่างๆ ในส่วนที่เกี่ยวข้องกับกระบวนการบริหารความต่อเนื่องทางธุรกิจของ อ.ส.ค.

4. ผู้บริหาร พนักงานและลูกจ้างของ อ.ส.ค. ต้องตระหนักถึงการมีส่วนร่วมเพื่อให้การดำเนินการบริหารความต่อเนื่องทางธุรกิจของ อ.ส.ค. บรรลุตามวัตถุประสงค์

1.2 โครงสร้างการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management BCM)

โครงสร้างการบริหารความต่อเนื่องทางธุรกิจ (BCM)



รูปที่ 1 โครงสร้างการบริหารความต่อเนื่องทางธุรกิจ (BCM)

รายชื่อบุคลากรและบทบาททีมงานแผนบริหารความต่อเนื่องทางธุรกิจ (BCM)

| รายชื่อ | ตำแหน่ง | ช่องทางการติดต่อ |
|---|-------------------------------|--|
| ผู้อำนวยการ อ.ส.ค. | ประธานคณะกรรมการ | |
| รองผู้อำนวยการ 1 ท่าน | คณะกรรมการ | |
| ผู้ช่วยผู้อำนวยการ 2 ท่าน | คณะกรรมการ | |
| หัวหน้าฝ่ายอำนาจการ | คณะกรรมการ | |
| หัวหน้าฝ่ายตรวจสอบภายใน | คณะกรรมการ | |
| หัวหน้าฝ่ายนโยบายและยุทธศาสตร์ | คณะกรรมการ | |
| หัวหน้าฝ่ายเทคโนโลยีดิจิทัล | คณะกรรมการ | |
| หัวหน้าฝ่ายทรัพยากรบุคคล | คณะกรรมการ | |
| หัวหน้าฝ่ายบัญชีและการเงิน | คณะกรรมการ | |
| หัวหน้าฝ่ายพัสดุและบริการ | คณะกรรมการ |  โทรศัพท์ |
| หัวหน้าฝ่ายวิจัยและพัฒนาการเลี้ยงโคนม | คณะกรรมการ |  Line |
| หัวหน้าฝ่ายส่งเสริมการเลี้ยงโคนม | คณะกรรมการ |  Video Conference |
| หัวหน้าฝ่ายท่องเที่ยวเชิงเกษตร | คณะกรรมการ |  การพบปะโดยตรง |
| หัวหน้าฝ่ายการตลาดและการขาย | คณะกรรมการ |  E-mail |
| หัวหน้าสำนักงาน อ.ส.ค. ภาคกลาง | คณะกรรมการ | |
| หัวหน้าสำนักงาน อ.ส.ค. ภาคใต้ | คณะกรรมการ | |
| หัวหน้าสำนักงาน อ.ส.ค. ภาคตะวันออกเฉียงเหนือ | คณะกรรมการ | |
| หัวหน้าสำนักงาน อ.ส.ค. ภาคเหนือตอนล่าง | คณะกรรมการ | |
| หัวหน้าสำนักงาน อ.ส.ค. ภาคเหนือตอนบน | คณะกรรมการ | |
| หัวหน้ากองเลขานุการคณะกรรมการโคนมและผลิตภัณฑ์นม | คณะกรรมการ | |
| หัวหน้ากองบริหารจัดการและพัฒนาองค์กร | คณะกรรมการและเลขานุการ | |
| หัวหน้าแผนกบริหารความเสี่ยงและควบคุมภายใน | คณะกรรมการและผู้ช่วยเลขานุการ | |

ตารางที่ 1 รายชื่อบุคลากรและบทบาทของทีมงานแผนบริหารความต่อเนื่องทางธุรกิจ (BCM)

รายชื่อบุคลากรและบทบาททีมงานคณะทำงานวางแผนความต่อเนื่องทางธุรกิจ
ด้านเทคโนโลยีสารสนเทศและแผนจัดการเหตุฉุกเฉิน

| รายชื่อ | ตำแหน่ง | ช่องทางการติดต่อ |
|---|--------------------------|------------------|
| รองผู้อำนวยการ อ.ส.ค. | ประธานคณะทำงาน | |
| หัวหน้าฝ่ายเทคโนโลยีดิจิทัล | คณะทำงาน | |
| หัวหน้าฝ่ายนโยบายและยุทธศาสตร์ | คณะทำงาน | |
| หัวหน้าฝ่ายบัญชีและการเงิน | คณะทำงาน | โทรศัพท์ |
| หัวหน้าฝ่ายการตลาดและการขาย | คณะทำงาน | Line |
| หัวหน้ากองกลยุทธ์ดิจิทัล | คณะทำงาน | Video Conference |
| หัวหน้าแผนกบริหารงานดิจิทัล | คณะทำงาน | การพบปะโดยตรง |
| หัวหน้าแผนกกำกับมาตรฐานงานดิจิทัล สารสนเทศ | คณะทำงาน | E-mail |
| หัวหน้าแผนกวิเคราะห์ข้อมูลและพัฒนา ระบบดิจิทัล | คณะทำงาน | |
| หัวหน้ากองโครงสร้างพื้นฐานและพัฒนา ระบบดิจิทัล | คณะทำงานและ เลขานุการ | |
| หัวหน้าแผนกโครงสร้างพื้นฐานดิจิทัล | ผู้ช่วยเลขานุการ | |

ตารางที่ 2 รายชื่อบุคลากรและบทบาทของทีมงานวางแผนความต่อเนื่องทางธุรกิจ
ด้านเทคโนโลยีสารสนเทศและแผนจัดการเหตุฉุกเฉิน

1.3 ความหมาย Business Continuity Management (BCM)

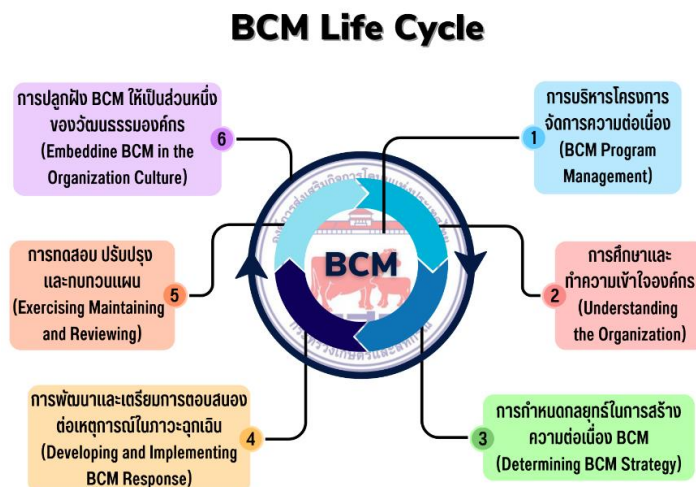
Business Continuity Management (BCM) การบริหารความต่อเนื่องทางธุรกิจ หมายถึง องค์กรรวมของกระบวนการบริหารซึ่งชี้ถึงเหตุการณ์ที่รุนแรงต่อองค์กรและผลกระทบของภัยคุกคามนั้น ต่อการดำเนินธุรกิจ และให้แนวทางในการสร้างขีดความสามารถให้องค์กรมีความยืดหยุ่น เพื่อการตอบสนองและปกป้องผลประโยชน์ของผู้มีส่วนได้ส่วนเสียชื่อเสียง ภาพลักษณ์ และกิจกรรมที่สร้างมูลค่าที่มีประสิทธิภาพ

1.4 วัตถุประสงค์ (Objectives) ของการจัดทำแผนดำเนินธุรกิจอย่างต่อเนื่อง

1. เพื่อใช้เป็นแนวทางในการบริหารความต่อเนื่อง
2. เพื่อให้ อ.ส.ค. มีการเตรียมความพร้อมในการรับมือกับ **เหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ของ อ.ส.ค. ถูกโจรกรรม)** และลดผลกระทบจากการหยุดชะงักการดำเนินงานหรือการใช้ระบบ AD อ.ส.ค. ทุกฝ่าย/สำนักงาน
3. เพื่อบรรเทาความเสียหายให้อยู่ระดับความเสี่ยงที่ยอมรับได้
4. เพื่อให้พนักงานทุกฝ่าย/สำนักงาน มีความเชื่อมั่นในศักยภาพขององค์กร แม้องค์กรต้องเผชิญกับเหตุการณ์ร้ายแรงและส่งผลกระทบจนทำให้การดำเนินงานต้องหยุดชะงัก
5. เพื่อใช้เป็นแนวทางในการบริหารจัดการในสภาวะวิกฤต/เหตุการณ์ฉุกเฉิน/สถานการณ์ภัยพิบัติ/ใช้กำหนดทรัพยากรที่จำเป็นเพื่อให้สามารถปฏิบัติการกิจได้ต่อเนื่อง
6. เพื่อลดระยะเวลา และผลกระทบจากการหยุดชะงักให้สั้นที่สุด
7. เพื่อให้ อ.ส.ค. สามารถกลับมาดำเนินงานหรือใช้งานระบบ AD ได้ตามปกติในเวลาและเป้าหมายที่กำหนด

1.5 แนวทางการบริหารความต่อเนื่อง (Business Continuity Management)

ปัจจุบันมีหลากหลายแนวทางและมาตรฐานในการการบริหารความต่อเนื่อง โดยแนวทางที่ได้รับการใช้อย่างแพร่หลาย ซึ่งกำหนดให้มี 6 องค์ประกอบหลักเป็นวงจรการบริหารความต่อเนื่อง (BCM Life Cycle) ทั้งนี้ อ.ส.ค. นำ BCM Life Cycle ไปประยุกต์ใช้สำหรับกระบวนการบริหารจัดการความต่อเนื่องทางธุรกิจ โดยขอบเขตวิธีการบริหารจัดการและทรัพยากรที่ต้องใช้ใน BCM มี 6 องค์ประกอบหลัก



รูปที่ 2 วงจรการบริหารความต่อเนื่อง (BCM Life Cycle)

1.6 ขอบเขตของแผนดำเนินธุรกิจอย่างต่อเนื่อง (Scope of BCP)

อ.ส.ค. ได้มีการวิเคราะห์ปัจจัยเสี่ยงขององค์กรประจำปี 2566 ที่มีผลโดยตรงกับหน่วยงานหลัก พิจารณาโอกาสและผลกระทบของเหตุการณ์ และใช้เกณฑ์การวิเคราะห์ตามแนวทางการบริหารความเสี่ยง ซึ่งพิจารณาจากผลกระทบของเหตุการณ์ที่อาจส่งผลกระทบต่อดำเนินงานของ อ.ส.ค. ทุกฝ่าย/สำนักงาน วางแผนความต่อเนื่องทางธุรกิจ (BCP) ฉบับนี้ใช้รองรับสถานการณ์กรณีเกิดสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินใน **อ.ส.ค. ด้วยเหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ของ อ.ส.ค. ถูกโจรกรรม)**

สรุปเหตุการณ์สภาวะวิกฤตและผลกระทบจากเหตุการณ์ (ทำเครื่องหมาย ✓ ในด้านที่ได้รับผลกระทบ)

สรุปเหตุการณ์สภาวะวิกฤตและผลกระทบจากเหตุการณ์

| เหตุการณ์ สภาวะวิกฤต | ผลกระทบ | | | | |
|---|---|---|--|-------------------------|--|
| | ด้าน อาคาร/ สถานที่ ปฏิบัติงาน หลัก | ด้านวัสดุ อุปกรณ์ที่ สำคัญ และ การจัดหา/ จัดส่ง | ด้าน เทคโนโลยี สารสนเทศ และข้อมูลที่ สำคัญ | ด้าน บุคลากร หลัก | ด้านลูกค้า/ ผู้ให้บริการ/ ผู้มีส่วนได้ส่วน เสีย |
| ภัยคุกคามทาง ไซเบอร์ (ระบบ AD ของ อ.ส.ค. ถูก โจรกรรม) | | | ✓ | ✓ | |

ตารางที่ 3 สรุปเหตุการณ์สภาวะวิกฤตและผลกระทบจากเหตุการณ์

1.7 คำจำกัดความตามแผนความต่อเนื่องทางธุรกิจ (Definition)

ตารางแสดงคำจำกัดความตามแผนความต่อเนื่องทางธุรกิจ (BCM)

| คำศัพท์ (Term) | คำจำกัดความ (Description) |
|--|--|
| การบริหารความต่อเนื่องทางธุรกิจ : Business Continuity Management (BCM) | แนวทางในการกำหนดนโยบายมาตรฐาน และกระบวนการทำงานของทั้งองค์กรเพื่อให้มั่นใจว่า ในกรณีที่มีเหตุการณ์รุนแรงที่ทำให้การปฏิบัติงานตามปกติต้องหยุดชะงัก กระบวนการทำงานที่สำคัญจะสามารถดำเนินการได้อย่างต่อเนื่อง หรือ กลับมาดำเนินการในเวลาที่เหมาะสม |
| คณะบริหารความต่อเนื่อง (Business Continuity Management Committee : BCM Committee) | ผู้บริหารระดับสูงของ อ.ส.ค. ที่มีหน้าที่กำกับดูแลให้มีการทบทวนและปรับปรุงระบบบริหารความต่อเนื่องทางธุรกิจอย่างต่อเนื่อง ประเมินสถานการณ์ และตัดสินใจพิจารณาประกาศสถานการณ์ฉุกเฉิน ภาวะวิกฤต และประกาศใช้แผน BCP รวมถึงให้คำแนะนำและพิจารณาอนุมัติการดำเนินการต่างๆ |
| แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) | แผนงานที่เป็นลายลักษณ์อักษร กำหนดขั้นตอนและกระบวนการทำงานในการเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ เพื่อช่วยให้ดำเนินการได้อย่างต่อเนื่องเมื่อเกิดเหตุที่ทำให้การดำเนินงานหยุดชะงัก |
| แผนจัดการอุบัติการณ์ (Incident Management Procedure : IMP) | แผนงานที่เป็นลายลักษณ์อักษร กำหนดขั้นตอนปฏิบัติและกระบวนการทำงาน เพื่อระงับเหตุฉุกเฉินหรือเหตุวิกฤตที่ทำให้การดำเนินงานหยุดชะงัก โดยเป็นดำเนินการระงับเหตุเบื้องต้นเพื่อมิให้นำไปสู่การประกาศใช้แผนความต่อเนื่องทางธุรกิจ (BCP) |
| ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption : MTPD) | ช่วงเวลานานที่สุดที่ธุรกิจหยุดชะงัก หากเกินกำหนดช่วงเวลานี้แล้วจะไม่สามารถทำให้ธุรกิจฟื้นคืนสู่สภาพปกติได้ |

ตารางที่ 4 แสดงคำจำกัดความการบริหารความต่อเนื่องทางธุรกิจ (BCM)

ตารางแสดงคำจำกัดความตามแผนความต่อเนื่องทางธุรกิจ (BCM)

| คำศัพท์ (Term) | คำจำกัดความ (Description) |
|--|--|
| ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective : RTO) | ระยะเวลาเป้าหมายในการฟื้นคืนสภาพของแต่ละผลิตภัณฑ์และบริการ โดยต้องพิจารณาถึงประสิทธิภาพของการฟื้นคืนหรือกู้คืนระบบเทคโนโลยีสารสนเทศขององค์กรและความสามารถในการเรียกคืน การดำเนินงานขององค์กร เช่น การสื่อสาร การเดินทาง การติดตั้งอุปกรณ์ การรวบรวมบุคลากร และการจัดเตรียมข้อมูลที่เกี่ยวข้อง เป็นต้น โดยค่า RTO ของแต่ละผลิตภัณฑ์และบริการต้องไม่เกินค่า MTPD ของแต่ละผลิตภัณฑ์และบริการนั้นๆ |
| แผนงานสำหรับการฟื้นฟูสู่สภาวะปกติ (Business Recovery Plan : BRP) | แผนงานที่เป็นลายลักษณ์อักษร กำหนดขั้นตอนและกระบวนการทำงานในการฟื้นฟูกระบวนการหรือกิจกรรมหลักที่สำคัญให้สามารถดำเนินการตามปกติ |
| การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA) | กระบวนการในการวิเคราะห์กิจกรรมต่างๆ และผลกระทบต่อกิจกรรมดังกล่าวหากธุรกิจเกิดการหยุดชะงักขึ้น |
| จุดเป้าหมายในการฟื้นคืนสภาพ (Recovery Point Objective : RPO) | จุดระยะเวลาเป้าหมายที่ยอมรับได้ในการกู้คืนข้อมูล หมายถึง ระยะเวลาที่ยอมรับได้ที่ข้อมูลต้องถูกสำรองโดยหน่วยจัดเก็บสำรองข้อมูล โดยระบุเป็น วินาที นาที ชั่วโมง วัน สัปดาห์ เดือน เช่น ถ้าระบุ RPO = 1 ชั่วโมง ระบบจะต้องสำรองข้อมูลทุกๆ 1 ชั่วโมง เป็นต้น |
| การประเมินความเสี่ยง (Risk Assessment : RA) | เป็นกระบวนการระบุปัจจัยเสี่ยงและนำมาจัดลำดับความเสี่ยงเพื่อพิจารณาระดับความเสี่ยงที่ยอมรับไม่ได้ขององค์กรและพิจารณาแนวทางรองรับต่อความเสี่ยง เพื่อให้การดำเนินธุรกิจมีความต่อเนื่อง |
| บุคลากร (Personnel) | เจ้าหน้าที่และพนักงานทั้งหมดของ อ.ส.ค. |

ตารางที่ 4 แสดงคำจำกัดความการบริหารความต่อเนื่องทางธุรกิจ (BCM) ต่อ

ตารางแสดงคำจำกัดความตามแผนความต่อเนื่องทางธุรกิจ (BCM)

| คำศัพท์ (Term) | คำจำกัดความ (Description) |
|---|---|
| บุคลากรหลัก (Key Personnel) | เจ้าหน้าที่และพนักงานของ อ.ส.ค. ที่ต้องดำเนินงานสำคัญในภาวะวิกฤต โดยถูกระบุชื่อไว้ในแผนบริหารความต่อเนื่องระดับหน่วยงาน |
| บุคลากรทดแทน (Replacement Personnel) | เจ้าหน้าที่และพนักงานของ อ.ส.ค. ที่ต้องดำเนินกระบวนการดำเนินงานสำคัญในภาวะวิกฤต ในกรณีที่บุคคลหลักไม่สามารถดำเนินการได้ |
| ภาวะฉุกเฉิน (Emergency) | สถานะที่เป็นอันตรายหรือสถานะที่มีอันตรายแฝงสูง ซึ่งอาจก่อให้เกิดอันตรายต่อบุคคล ทรัพย์สิน และสิ่งแวดล้อมได้ หรืออีกนัยหนึ่ง คือ สถานะที่ไม่อาจควบคุมได้ในทันทีทันใด ซึ่งอาจทำให้เกิดการเสียชีวิต บาดเจ็บ หรือเกิดความเสียหายต่อทรัพย์สิน หรือสิ่งแวดล้อมได้ |
| ภาวะวิกฤต (Crisis) | สถานการณ์รุนแรงซึ่งหากไม่ได้มีการจัดการที่เหมาะสมอาจส่งผลกระทบต่อภาพลักษณ์ชื่อเสียง และความสามารถในการปฏิบัติงานหรือการให้บริการขององค์กรได้ |

ตารางที่ 4 แสดงคำจำกัดความการบริหารความต่อเนื่องทางธุรกิจ (BCM) ต่อ

1.8 สมมติฐานของแผนความต่อเนื่องทางธุรกิจ BCM Assumptions)

เอกสารฉบับนี้จัดทำขึ้นภายใต้สมมติฐาน ดังต่อไปนี้

- เหตุการณ์ฉุกเฉินที่เกิดขึ้น คือ **ภัยคุกคามทางไซเบอร์ (ระบบ AD ของ อ.ส.ค. ถูกโจมตี)** ในช่วงเวลาสำคัญต่างๆ ณ อ.ส.ค. ทุกฝ่าย/สำนักงาน แต่ไม่ได้ส่งผลกระทบต่อสถานที่ปฏิบัติงานสำรองที่ได้มีการจัดเตรียมไว้
- ฝ่ายเทคโนโลยีดิจิทัลรับผิดชอบในการสำรองระบบสารสนเทศต่างๆ โดยระบบสารสนเทศสำรองมิได้รับผลกระทบจากเหตุการณ์ฉุกเฉินเหมือนกับระบบสารสนเทศหลัก
- “บุคลากร” ที่ถูกระบุในเอกสารฉบับนี้ หมายถึง เจ้าหน้าที่และพนักงานทั้งหมดที่ปฏิบัติงานอยู่ที่ อ.ส.ค. ทุกฝ่าย/สำนักงาน

4. สถานที่ปฏิบัติงาน คือ **อ.ส.ค. ทุกฝ่าย/สำนักงาน**

โดยได้ตั้งเหตุการณ์สมมติฐานของแผนความต่อเนื่องทางธุรกิจไว้ 2 เหตุการณ์

1.8.1 เหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม) ที่สามารถควบคุมได้ คือ การเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ โดย Hacker โจรกรรมข้อมูล User และ Password ของพนักงานทุกคนใน อ.ส.ค. โดยฝ่ายเทคโนโลยีดิจิทัลสามารถควบคุมสถานการณ์ได้ไว้ โดยรีบดำเนินการ Restore ระบบและ Reset User และ Password ได้ทันกาล ประกอบกับ Hacker ไม่ได้นำข้อมูลไปเรียกค่าไถ่ ซึ่งส่งผลกระทบต่อเล็กน้อย โดยเหตุการณ์การถูกโจรกรรมข้อมูลอยู่ในขอบเขตที่จำกัด องค์กรสามารถควบคุมสถานการณ์ได้

1.8.2 เหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม) ที่ไม่สามารถควบคุมได้ คือ การเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีผลต่อการสูญเสียกระบวนการทำงาน หรือมีผลกระทบต่อข้อมูลส่วนบุคคลขั้นร้ายแรง เนื่องจาก Hacker ดำเนินการเรียกค่าไถ่และนำข้อมูลส่วนบุคคลของพนักงานใน อ.ส.ค. เผยแพร่ต่อสาธารณะ อ.ส.ค. ไม่สามารถควบคุมสถานการณ์การถูกโจรกรรมได้ โดยทีมปฏิบัติการฉุกเฉินจำเป็นต้องเร่งดำเนินการ Restore ระบบ และ Reset User และ Password และแจ้งต่อกองกฎหมายที่มีความเชี่ยวชาญด้านกฎหมายเพื่อดำเนินการตามกระบวนการด้านกฎหมายต่อไป

แนวทางการบริหารความต่อเนื่องรายกิจกรรมที่มีระดับความสำคัญสูง

| ผลกระทบด้าน | กิจกรรมที่มีระดับความสำคัญสูง |
|-------------|--|
| ระบบ AD | <ol style="list-style-type: none"> ประสานงานกับฝ่ายเทคโนโลยีดิจิทัล เพื่อเร่งดำเนินการ Restore ระบบ และ Reset User และ Password หรือระบบสารสนเทศสำรอง ปฏิบัติงานโดยใช้ระบบงานเทคโนโลยี (Manual) ไปก่อนและจึงป้อนข้อมูลเข้าในระบบเมื่อกลับคืนสู่สภาวะปกติ |
| บุคลากรหลัก | <ol style="list-style-type: none"> กำหนดให้บุคลากรหลักมีดำเนินงานที่สำคัญมีแผนรองรับในสภาวะวิกฤติ กำหนดแนวทางกลุ่มบุคลากรที่สามารถขอให้ช่วยปฏิบัติงานชั่วคราว |
| กฎหมาย | ประสานกับกองกฎหมายเพื่อเร่งดำเนินการขั้นตอนทางกฎหมาย |

ตารางที่ 5 แนวทางการบริหารความต่อเนื่องรายกิจกรรมที่มีระดับความสำคัญสูง

บทที่ 2

การศึกษาและทำความเข้าใจองค์กร
(Understanding the Organization)

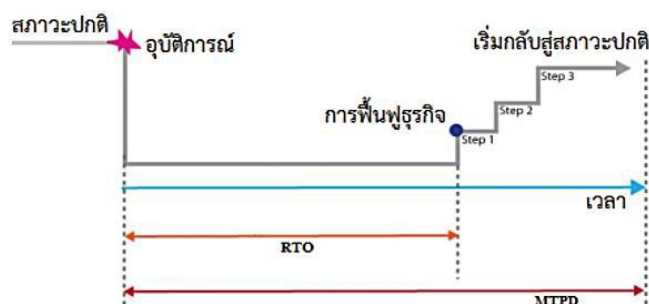
2.1 การวิเคราะห์ผลกระทบทางธุรกิจ

การวิเคราะห์ผลกระทบทางธุรกิจ คือ กระบวนการ การวิเคราะห์เพื่อหาผลกระทบจากการหยุดชะงักของกระบวนการหลัก ทำให้องค์กรสามารถเลือกที่จะฟื้นคืนสภาพกระบวนการภายหลังจากเกิดอุบัติการณ์ตามลำดับได้อย่างเหมาะสม ซึ่งถือเป็นขั้นตอนที่สำคัญของการพัฒนาการบริหารความต่อเนื่องทางธุรกิจ เนื่องจากผลลัพธ์ที่ได้จะทำให้ทราบถึงกระบวนการหลักที่มีความสำคัญต่อการดำเนินธุรกิจ ซึ่งกระบวนการดังกล่าวถ้าได้รับผลกระทบจากเหตุการณ์อัคคีภัยอาจส่งผลทำให้องค์กร ได้รับความเสียหายในด้านต่างๆ เช่น ความสูญเสียหรือเสียชีวิต ทรัพย์สิน กระบวนการทำงาน สภาพแวดล้อมเสียหาย การสูญเสียรายได้ การสูญเสียโอกาสในการลงทุนแต่ละด้าน ตลอดจนการไม่สามารถปฏิบัติตามภาระผูกพันที่มีต่อผู้มีส่วนได้ส่วนเสีย ที่อาจนำไปสู่การสูญเสียชื่อเสียงและการฟ้องร้อง เป็นต้น ซึ่งข้อมูลต่างๆ เหล่านี้จะถูกนำมาเป็นปัจจัยในการประเมินผล กระทบทางธุรกิจ เพื่อให้ทราบว่าในปัจจุบัน องค์กร มีกระบวนการหลักใดที่มีความสำคัญที่ควรพิจารณาดำเนินการปกป้องซึ่งต้องดำเนินการได้ภายใต้ค่าวิกฤตต่างๆ ที่สำคัญ ซึ่งได้แก่

1. **ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด** (Maximum Tolerable Period of Disruption, MTPD) หมายถึง ช่วงเวลาที่ส่งผลกระทบที่ไม่สามารถยอมรับได้

2. **ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ** (Recovery Time Objective, RTO) หมายถึง ระยะเวลาเป้าหมายที่ใช้ในการดำเนินการให้กลับสู่ระดับที่ยอมรับได้

3. **ระดับที่ยอมรับขั้นต่ำ** (Minimum Acceptable Level, MAL) หมายถึง ระดับต่ำสุดของการบริการที่ลูกค้ายอมรับได้ที่จะกลับคืนมาในระหว่างเกิดการหยุดชะงักซึ่งระยะเวลาเป้าหมายในการฟื้นคืนสภาพกับช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุดสามารถแสดงความสัมพันธ์กันได้ดังรูปที่.....



รูปที่ 3 ความสัมพันธ์ระหว่างค่า RTO และ MTPD

จากรูปที่ 3 พบว่า ค่า RTO จะต้องถูกกำหนดขึ้นภายใต้กรอบของค่า MTPD ซึ่งหากเลยจากช่วงเวลานี้ไปและยังไม่สามารถเริ่มฟื้นฟูธุรกิจได้จะส่งผลกระทบต่อองค์กร ทั้งนี้การฟื้นฟูดังกล่าวไม่จำเป็นต้องครบสมบูรณ์ในทันที เพียงแต่ต้องระบุให้ได้ว่าค่า RTO ที่กำหนด ณ จุดฟื้นฟูธุรกิจมีระดับ MAL เท่าใด

2.2 การประเมินความเสี่ยง

2.2.1 เกณฑ์การประเมินความเสี่ยง

การระบุประเด็นและวิเคราะห์ความเสี่ยงจากอุบัติการณ์ที่เกิดขึ้น โดยพิจารณาโอกาสที่จะเกิดอุบัติการณ์แต่ละประเภท และระดับผลกระทบที่เกิดขึ้น ตลอดจนมาตรการควบคุมที่มีอยู่ ซึ่งทำให้ทราบถึงภัยคุกคามที่มีโอกาสเกิดขึ้น และส่งผลกระทบต่อการดำเนินธุรกิจขององค์กรในด้านต่างๆ รวมถึงขนาดความรุนแรงของผลกระทบจากเหตุการณ์ที่เกิดขึ้น และจุดที่สามารถทำให้เกิดผลกระทบในปัจจุบัน จุดอ่อนของมาตรการควบคุมที่มีอยู่ในปัจจุบัน และการจัดการเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ การประเมินความเสี่ยงช่วยให้องค์กรสามารถพิจารณาถึงเหตุการณ์ที่อาจจะเกิดขึ้นและมีผลกระทบต่อการบริหารลู่วัตถุประสงค์ขององค์กร หรือกลายเป็นเหตุให้ การดำเนินธุรกิจขององค์กรหยุดชะงัก ในการประเมินจะพิจารณาจาก 2 มุมมอง ได้แก่ โอกาสที่จะเกิด (Likelihood, L) และผลกระทบ (Impact, I)

โดยพิจารณาผลกระทบเชิงลบจากเหตุการณ์ที่อาจจะเกิดขึ้น ทั้งนี้จะต้องมีการประเมินความเสี่ยงบนพื้นฐานของความเสี่ยงที่มีอยู่ (Inherent Risk) และความเสี่ยงที่เหลืออยู่ (Residual Risk) จากความเสี่ยงที่มีการดำเนินการอยู่แล้ว ในการวิเคราะห์ความเสี่ยงว่าความเสี่ยงใดมีความสำคัญ ที่ต้องนำมาดำเนินการก่อน-หลังจะวิเคราะห์จากระดับความเสี่ยง (Degree of Risk) ซึ่งคำนวณโดย นำค่า L x I และพิจารณาร่วมกับเมตริกความเสี่ยง ดังรูปภาพที่ 4

| | | | | | | | |
|---------------------|-------------|--|----------|-------------|----------|------------|--|
| | | ตารางแนบมุมระดับความเสี่ยง (Degree of Risks) | | | | | |
| ผลกระทบ (Impact: I) | สูงสุด (5) | 1x5 = 5 | 2x5 = 10 | 3x5 = 15 | 4x5 = 20 | 5x5 = 25 | E = สูงสุด (สีแดง) H = สูง (สีส้ม) M = ปานกลาง (สีเหลือง) L = ต่ำ (สีเขียว) |
| | สูง (4) | 1x4 = 4 | 2x4 = 8 | 3x4 = 12 | 4x4 = 16 | 5x4 = 20 | |
| | ปานกลาง (3) | 1x3 = 3 | 2x3 = 6 | 3x3 = 9 | 4x3 = 12 | 5x3 = 15 | |
| | น้อย (2) | 1x2 = 2 | 2x2 = 4 | 3x2 = 6 | 4x2 = 8 | 5x2 = 10 | |
| | น้อยมาก (1) | 1x1 = 1 | 2x1 = 2 | 3x1 = 3 | 4x1 = 4 | 5x1 = 5 | |
| | | น้อยมาก (1) | น้อย (2) | ปานกลาง (3) | สูง (4) | สูงสุด (5) | |
| | | โอกาสเกิด (Likelihood: L) | | | | | |

รูปที่ 4 Risk Matrix

2.2.2.1 เกณฑ์การประเมินโอกาสเกิดของความเสียหาย พบว่าในการหาข้อมูลเชิงปริมาณมาสนับสนุนการประเมินความเสี่ยงเป็นไปได้ยาก จึงทำการประเมินในเชิงคุณภาพ ซึ่งต้องอาศัยการวิเคราะห์ตามหลักการอย่างระมัดระวัง ส่วนในกรณีที่สามารถหาข้อมูลเชิงปริมาณที่เกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม) หรือความถี่ที่เกิดขึ้นในอดีตได้ สามารถนำมาบ่งชี้ได้อย่างแม่นยำมากขึ้น ทั้งนี้ในการประเมินโอกาสเกิดของความเสียหาย มีเกณฑ์การประเมินโอกาสเกิดความเสียหายดังตารางที่ 6

**ตารางแสดงเกณฑ์การวิเคราะห์โอกาสเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์
ต่อกระบวนการทำงาน (Business Impact Analysis)**

| โอกาสเกิด (L) | วิเคราะห์โอกาสเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ (L) | | ระดับ | |
|---------------|---|-------------|--------------------------|---|
| | เชิงปริมาณ | เชิงคุณภาพ | | |
| น้อยมาก | มีโอกาสเกิดภัยคุกคามทางไซเบอร์ 1% | 30 ปี/ครั้ง | โอกาสเกิดน้อยมาก | 1 |
| น้อย | มีโอกาสเกิดภัยคุกคามทางไซเบอร์ มากกว่า 1% แต่ไม่เกิน 10% | 20 ปี/ครั้ง | มีโอกาสเกิดแต่นานๆครั้ง | 2 |
| ปานกลาง | มีโอกาสเกิดภัยคุกคามทางไซเบอร์ มากกว่า 10% แต่ไม่เกิน 20% | 10 ปี/ครั้ง | มีโอกาสเกิดบางครั้ง | 3 |
| สูง | มีโอกาสเกิดภัยคุกคามทางไซเบอร์ มากกว่า 20% แต่ไม่เกิน 30% | 5 ปี/ครั้ง | มีโอกาสเกิดค่อนข้างสูง | 4 |
| สูงสุด | มีโอกาสเกิดภัยคุกคามทางไซเบอร์ มากกว่า 30% | 1 ปี/ครั้ง | มีโอกาสเกิดเกือบทุกครั้ง | 5 |

**ตารางที่ 6 แสดงเกณฑ์การวิเคราะห์โอกาสเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์
ต่อกระบวนการทำงาน (Business Impact Analysis)**

2.2.2.2 เกณฑ์การประเมินผลกระทบของความเสียหาย สำหรับการประเมินผลกระทบของความเสียหายจะพิจารณาใช้เกณฑ์ในด้านของผลกระทบที่มีระดับความรุนแรงมากที่สุด โดยเลือกจากเกณฑ์ประเมินผลกระทบด้านการเงิน ทั้งนี้ค่าต่างๆ ที่นำมาใช้งานได้ถูกกำหนดขึ้นเพื่อใช้ในองค์กรอยู่ก่อนแล้ว ดังตารางที่ 7

ตารางแสดงเกณฑ์การประเมินผลกระทบด้านการเงิน
(Business Impact Analysis)

| ผลกระทบ (I) | วิเคราะห์ผลกระทบเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ (I) | | ระดับ |
|-------------|---|--|-------|
| | เชิงปริมาณ | เชิงคุณภาพ | |
| น้อยมาก | มูลค่าความเสียหายน้อยกว่า 10,000 บาท | ไม่มีผลกระทบต่อการดำเนินธุรกิจ | 1 |
| น้อย | มูลค่าความเสียหาย 10,000 – 50,000 บาท | กระทบ แต่ไม่สร้างความเสียหาย | 2 |
| ปานกลาง | มูลค่าความเสียหาย 50,000 – 250,000 บาท | กระทบ และสร้างความเสียหายบาง กิจกรรม | 3 |
| สูง | มูลค่าความเสียหาย 250,000 – 10,000,000 บาท | กระทบ และสร้างความเสียหายต่อผล การดำเนินงานธุรกิจ | 4 |
| สูงสุด | มูลค่าความเสียหายมากกว่า 10,000,000 บาทขึ้นไป | กระทบ และสร้างความเสียหาย จนไม่สามารถดำเนินธุรกิจต่อได้ | 5 |

ตารางที่ 7 แสดงเกณฑ์การประเมินผลกระทบต่อกระบวนการทำงาน
(Business Impact Analysis)

ตารางแสดงเกณฑ์การประเมินด้านพนักงานและภาพลักษณ์ชื่อเสียง

| เกณฑ์ | ด้านพนักงาน | ด้านภาพลักษณ์ | ระดับ |
|---------|---|---|-------|
| น้อยมาก | จำนวนพนักงานที่ไม่สามารถใช้ระบบ AD ได้ 10% | ไม่มีการเผยแพร่ข่าวสารที่เป็น ด้านลบ | 1 |
| น้อย | จำนวนพนักงานที่ไม่สามารถใช้ระบบ AD ได้ 20% | ปรากฏเป็นข่าวเสียหายเล็กน้อย ซึ่งไม่ใช่ ข่าวตามสื่อโทรทัศน์ หน้าเว็บไซต์ที่มี ชื่อเสียง หรือช่องทางอินเทอร์เน็ต | 2 |
| ปานกลาง | จำนวนพนักงานที่ไม่สามารถใช้ระบบ AD ได้ 30% | ลูกค้าแจ้งข้อร้องเรียนต่อ อ.ส.ค. และ อ.ส.ค. ไม่สามารถจัดการเหตุการณ์นั้นได้ | 3 |
| สูง | จำนวนพนักงานที่ไม่สามารถใช้ระบบ AD ได้ 40% | เป็นข่าวเสียหายจากสื่อโทรทัศน์ Website Page Fackbook TikTok Instagram และ สื่อสิ่งพิมพ์ เป็นเวลา 1 วัน | 4 |
| สูงสุด | จำนวนพนักงานที่ไม่สามารถใช้ระบบ AD ได้ 50% | สื่อโทรทัศน์ Website Page Fackbook TikTok Instagram และสื่อสิ่งพิมพ์ นำเสนอข่าว และเกิดการวิพากษ์วิจารณ์ ในทางลบ เป็นเวลามากกว่า 1 วันขึ้นไป | 5 |

ตารางที่ 8 แสดงเกณฑ์การประเมินด้านพนักงานและภาพลักษณ์ชื่อเสียง

2.2.2.3 การกำหนดช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (MTPD)

การกำหนดค่า MTPD ของกระบวนการหลักโดยพิจารณาเลือกจากค่าระยะเวลาที่น้อยที่สุดที่เริ่มมีระดับของผลกระทบสูงมาก และระบุค่าดังกล่าวลงในช่อง MTPD ตัวอย่างดังตารางที่ 9

ตารางแสดงเกณฑ์ระยะเวลาหยุดดำเนินการสูงสุดที่ยอมรับได้

| เกณฑ์ | ระยะเวลาหยุดดำเนินการสูงสุดที่ยอมรับได้ | ระดับ |
|---------|---|-------|
| น้อยมาก | ไม่เกิน 2 ชั่วโมง | 1 |
| น้อย | ไม่เกิน 3 ชั่วโมง | 2 |
| ปานกลาง | ไม่เกิน 4 ชั่วโมง | 3 |
| สูง | ไม่เกิน 5 ชั่วโมง | 4 |
| สูงสุด | ไม่เกิน 6 ชั่วโมง | 5 |

ตารางที่ 9 แสดงเกณฑ์ระยะเวลาหยุดดำเนินการสูงสุดที่ยอมรับได้

ตารางแสดงระยะเวลาเป้าหมายในการฟื้นคืนสภาพ

| กระบวนการหลัก | ระดับผลกระทบ/ ความเร่งด่วน (สูงสุด/สูง/ปานกลาง/ น้อย/น้อยมาก) | ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ | | | | |
|---------------|--|----------------------------------|-------------------------|-------------------------|-------------------------|-------------------------|
| | | ไม่เกิน 2 ชั่วโมง | ไม่เกิน 3 ชั่วโมง | ไม่เกิน 4 ชั่วโมง | ไม่เกิน 5 ชั่วโมง | ไม่เกิน 6 ชั่วโมง |
| ระบบ AD | น้อย | | ✓ | | | |

ตารางที่ 10 แสดงระยะเวลาเป้าหมายในการฟื้นคืนสภาพ

2.2.2 ขั้นตอนการประเมินความเสี่ยง

1) พิจารณาหาหัวข้อความเสี่ยงข้อมูล จากเอกสารการบริหารความเสี่ยงองค์กร สำหรับเล่มแผนฉบับนี้จะพิจารณาหัวข้อความเสี่ยงจากการบริหารความเสี่ยงองค์กร ในหัวข้อความเสี่ยงด้านกฎระเบียบ (Compliance Risk) โดยเป็นความเสี่ยงที่ส่งผลกระทบต่อกระบวนการหลัก อาจทำให้ระบบการปฏิบัติงาน (ระบบ AD) หยุดชะงัก

2) ระบุความเสี่ยงที่จะส่งผลกระทบต่อการทำงานขององค์กรหยุดชะงัก ส่งผลกระทบต่อระบบงานหลัก ระบบสารสนเทศ พนักงาน ทรัพย์สิน และทรัพยากรอื่นๆ ที่สนับสนุน

3) ดำเนินการประเมินความเสี่ยงโดยพิจารณาให้คะแนนตามเกณฑ์การประเมินความเสี่ยง ตามที่ระบุในข้อ 2.2.1 เกณฑ์การประเมินความเสี่ยง

4) ระบุระดับคะแนนลงในเมตริกซ์ความเสี่ยง

5) พิจารณานำความเสี่ยงที่มีระดับความรุนแรงสูง และสูงสุด หรือเห็นควรให้มีการจัดการมาดำเนินการจัดทำหรือทบทวนแผน หรือมาตรการเพื่อตอบโต้ภาวะฉุกเฉินสำหรับอุบัติการณ์หรือภัยคุกคามนั้นๆ รวมถึงวางแผนบริหารความเสี่ยงเพื่อควบคุมและลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยต้องพิจารณาถึงมาตรการเชิงรุก เพื่อลดโอกาสของการหยุดชะงัก ทำให้ช่วงเวลาของการหยุดชะงักสั้นลง และจำกัดผลกระทบของการหยุดชะงัก

2.2.3 ผลการประเมินความเสี่ยง

จากการสมมติฐานเหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม) ที่ส่งผลกระทบต่อองค์กร และทำให้พนักงานในองค์กรไม่สามารถปฏิบัติงานต่อได้ ได้ดำเนินการวิเคราะห์ความเสี่ยงอย่างเป็นระบบ ในการประเมินความเสี่ยงจะพิจารณาจากข้อมูล ได้แก่ แผนวิสาหกิจองค์กร ซึ่งมีการวิเคราะห์ประเด็นภายนอกและภายใน (SWOT) ขององค์กร การบริหารความเสี่ยงทั่วทั้งองค์กร และผลการดำเนินงานขององค์กร (Organization Performance Report : OPR) โดยมีการสร้างคู่มือในการดำเนินการชื่อว่า “การประเมินความเสี่ยง” ความเสี่ยงที่จะถูกนำมาพิจารณาตามแนวทางการบริหารความต่อเนื่องทางธุรกิจจะต้องเป็นความเสี่ยงด้านกฎระเบียบ (Compliance Risk) ซึ่งเป็นอุบัติการณ์ที่จะส่งผลกระทบต่อระบบ (Disruptive Incident) ต่อกระบวนการทำงานหลัก (ระบบ AD) จากนั้นได้มีการประเมินความเสี่ยง โดยมีรายละเอียดการพิจารณาให้คะแนนระดับโอกาสเกิดความเสี่ยงและระดับความรุนแรงของผลกระทบ

2.2.4 การประเมินสถานการณ์และกำหนดระดับความรุนแรง

เมื่อ อ.ส.ค. มีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้วจะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ โดยนำมาสรุปเป็นข้อมูล ดังนี้

**ตารางแสดงผลการประเมินความเสี่ยง กรณีเหตุการณ์ภัยคุกคามทางไซเบอร์
(ระบบ AD ถูกโจรกรรม)**

| ระบบงาน | ด้านการเงิน | | | ด้านพนักงาน | | | ด้านภาพลักษณ์ | | |
|---------|-------------|---------|-------------------------|-------------|---------|-------------------------|---------------|---------|-------------------------|
| | โอกาส | ผลกระทบ | ระดับ ความ เสี่ยง | โอกาส | ผลกระทบ | ระดับ ความ เสี่ยง | โอกาส | ผลกระทบ | ระดับ ความ เสี่ยง |
| ระบบ AD | 1 | 4 | 4 | 1 | 5 | 5 | 1 | 5 | 5 |

**ตารางที่ 11 แสดงผลการประเมินความเสี่ยง กรณีเหตุการณ์ภัยคุกคามทางไซเบอร์
(ระบบ AD ถูกโจรกรรม)**

ด้านการเงิน ระดับความเสี่ยง เท่ากับ ระดับ 4 (ความเสี่ยงต่ำ)

- โอกาสเกิดอยู่ระดับ 1 เหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม) มีโอกาสที่จะเกิด 30 ปีต่อครั้ง (มีโอกาสเกิดแต่น้อยมาก)
- ผลกระทบอยู่ระดับ 4 หากเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม) จะส่งผลกระทบและสร้างความเสียหายต่อผลการดำเนินงานธุรกิจของ อ.ส.ค. ประกอบกับจะสร้างความเสียหายให้กับ อ.ส.ค. โดยมูลค่าความเสียหายเท่ากับ 250,000 – 10,000,000 บาท

ด้านพนักงาน ระดับความเสี่ยง เท่ากับ ระดับ 5 (ความเสี่ยงปานกลาง)

- โอกาสเกิดอยู่ระดับ 1 เหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม) มีโอกาสที่จะเกิด 30 ปีต่อครั้ง (มีโอกาสเกิดแต่น้อยมาก)
- ผลกระทบอยู่ระดับ 5 หากเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม) ทำให้พนักงานไม่สามารถใช้ระบบ AD ได้ 50%

ด้านภาพลักษณ์ ระดับความเสี่ยง เท่ากับ ระดับ 5 (ความเสี่ยงปานกลาง)

- โอกาสเกิดอยู่ระดับ 1 เหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม) มีโอกาสที่จะเกิด 30 ปีต่อครั้ง (มีโอกาสเกิดแต่น้อยมาก)
- ผลกระทบอยู่ระดับ 5 หากเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม) สื่อโทรทัศน์ Website Page Facebook Tik Tok Instagram และสื่อสิ่งพิมพ์ นำเสนอข่าว และเกิดการวิพากษ์วิจารณ์ในทางลบ เป็นเวลามากกว่า 1 วันขึ้นไป

ตารางแสดงผลกระทบด้านความเสี่ยง กรณีเหตุการณ์ภัยคุกคามทางไซเบอร์
(ระบบ AD ถูกโจมตี)

| สถานการณ์หรือ ภาวะฉุกเฉิน | ระดับความรุนแรงผลกระทบ (5 คะแนน) | | | คะแนนรวม |
|---|----------------------------------|-------------|---------------|----------|
| | ด้านการเงิน | ด้านพนักงาน | ด้านภาพลักษณ์ | |
| เหตุการณ์ภัยคุกคาม ทางไซเบอร์ (ระบบ AD ถูกโจมตี) | 4 | 5 | 5 | 14 |

ตารางที่ 12 แสดงผลกระทบด้านความเสี่ยง กรณีเหตุการณ์ภัยคุกคามทางไซเบอร์
(ระบบ AD ถูกโจมตี)

บทที่ 3

การกำหนดกลยุทธ์ในการสร้างความต่อเนื่อง BCM
(Determining BCM Strategy)

3.1. ผลลัพธ์จากการวิเคราะห์ผลกระทบทางธุรกิจ BIA (Business Impact Analysis)

อ.ส.ค. ได้ดำเนินการวิเคราะห์ BIA จากการประชุมเชิงปฏิบัติการ Workshop เมื่อวันที่ **8 มิถุนายน 2566 ณ สำนักงาน อ.ส.ค. ทุกฝ่าย/สำนักงาน** โดยมีผู้เข้าร่วมวิเคราะห์ BIA ประกอบด้วยคณะทำงานบริหารความต่อเนื่องทางธุรกิจของ อ.ส.ค. ผู้บริหาร อ.ส.ค. และผู้ปฏิบัติงานที่เกี่ยวข้องกับกระบวนการที่มีการหยุดชะงักของการดำเนินงาน ซึ่งมีกระบวนการวิเคราะห์และวัดผลกระทบหรือความสูญเสียทางธุรกิจที่เกิดจากการหยุดชะงักการดำเนินงาน ในระบบ AD (Active Directory) ที่นำมาใช้เป็นเครื่องมือในการปฏิบัติงานในกระบวนการหลักของ อ.ส.ค. อย่างต่อเนื่อง

ระบบ Active Directory (AD) คือ ระบบในการจัดเก็บชื่อ User (ผู้ใช้งานในระบบ) โดยระบบที่ต้องใช้ User และ Password ในการ Login เข้าเชื่อมต่อกับระบบ Active Directory (AD)

ระบบ E-HR

ระบบ Dportal

ระบบ E-Budget

ระบบ KM

ระบบ E-Learning

ระบบตรวจจ่ายงบประมาณ

ระบบจัดการข้อมูลผู้ใช้งาน ERP

ระบบ MIS

ระบบ EIS

ระบบ E-Mail

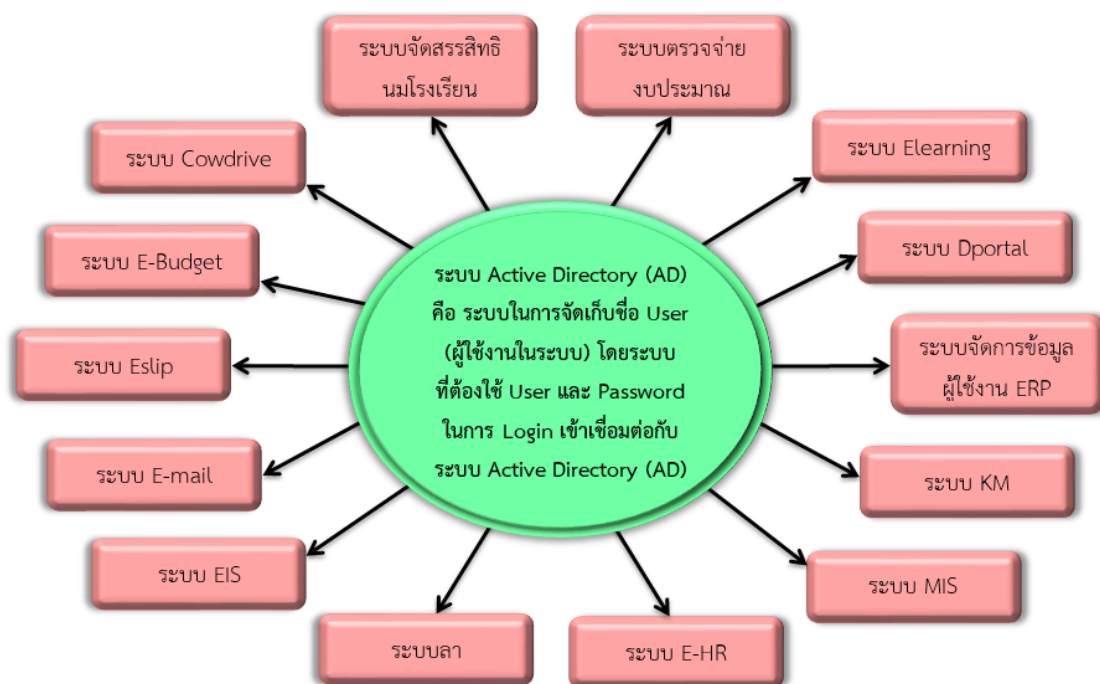
ระบบ Eslip

ระบบ Cowdrive

ระบบจัดสรรสิทธิคนโรงเรียน

ระบบลา

รูปภาพแสดงระบบที่ Log In เข้าเชื่อมต่อกับระบบ AD



รูปที่ 5 ระบบที่ Log In เข้าเชื่อมต่อกับระบบ AD

การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA) พิจารณามิติผลกระทบตามแนวทางการวิเคราะห์ความเสี่ยงของ อ.ส.ค. ที่ได้กำหนดมิติของผลกระทบไว้ 4 ด้าน คือ

- S : Strategic ด้านกลยุทธ์
- O : Operation ด้านการดำเนินงาน
- F : Finance ด้านการเงิน
- C : Compliance ด้านกฎระเบียบ

เกี่ยวข้องโดยใช้เกณฑ์ประเมิน 5 ระดับ ดังนี้

- ระดับ 1 = น้อยมาก
- ระดับ 2 = น้อย
- ระดับ 3 = ปานกลาง
- ระดับ 4 = สูง
- ระดับ 5 = สูงมาก

ตารางแสดงการวิเคราะห์ผลกระทบ

| ระดับ | ความหมาย : เชิงปริมาณ (บาท) | ความหมาย : เชิงคุณภาพ |
|---------|----------------------------------|---|
| ระดับ 1 | ไม่เกิน 10,000 บาท | น้อยมาก : ไม่มีผลกระทบ |
| ระดับ 2 | มากกว่า 10,000 – 50,000 บาท | น้อย : มีผลกระทบ แต่ไม่สร้างความเสียหาย |
| ระดับ 3 | มากกว่า 50,000 – 250,000 บาท | ปานกลาง : มีผลกระทบ สร้างความเสียหาย บางกิจกรรม/ขั้นตอน |
| ระดับ 4 | มากกว่า 250,000 – 10,000,000 บาท | สูง : มีผลกระทบและสร้างความเสียหายต่อผลการดำเนินงานธุรกิจ |
| ระดับ 5 | มากกว่า 10,000,000 บาทขึ้นไป | สูงมาก : มีผลกระทบและสร้างความเสียหายจนไม่สามารถดำเนินงานธุรกิจต่อไปได้ |

ตารางที่ 13 ตารางแสดงการวิเคราะห์ผลกระทบ

ซึ่งผลจากการประชุมเชิงปฏิบัติการ Workshop เพื่อวิเคราะห์ BIA พบว่าระบบ AD ที่นำมาใช้เป็นเครื่องมือในการปฏิบัติงานในกระบวนการหลักของ อ.ส.ค. อย่างต่อเนื่อง เพราะการใช้ระบบต่างๆที่เกี่ยวข้องกับกระบวนการทำงานที่มีความสำคัญอย่างยิ่ง ในการดำเนินธุรกิจหลักของ อ.ส.ค. จึงได้พิจารณาจัดทำแผนบริหารความต่อเนื่อง Business Continuity Plan : BCP และแผนการกู้ระบบ Disaster Recovery Plan : DRP ในปี 2566 เพื่อนำใช้ในปี 2566-2567 โดยมีผลการวิเคราะห์ดังตารางข้างล่างนี้

ผลลัพธ์จากการวิเคราะห์ผลกระทบทางธุรกิจ ของ อ.ส.ค.

| Key Service/ process | 3 Hrs. | | | | | 8 Hrs. | | | | | 24 Hrs. | | | | | >1 Day | | | | | MTPD | RTO | |
|----------------------|--------|---|---|---|-----|--------|---|---|---|-----|---------|---|---|---|-----|--------|---|---|---|-----|--------|-----------------|--------------------|
| | S | O | F | C | Max | S | O | F | C | Max | S | O | F | C | Max | S | O | F | C | Max | | ระยะเวลาเดินทาง | ระยะเวลาที่ระบบคืน |
| ระบบ AD | 1 | 2 | 2 | 1 | 2 | 2 | 3 | 3 | 1 | 3 | 2 | 4 | 4 | 1 | 4 | 2 | 5 | 5 | 1 | 5 | 4 hrs. | 30 min | 3 hrs. |

ตารางที่ 14 ผลลัพธ์จากการวิเคราะห์ผลกระทบทางธุรกิจ ของ อ.ส.ค.

3.1.1 คำอธิบายการวิเคราะห์ Key Process AD

กรณีระบบ AD ใช้งานไม่ได้ 3 ชั่วโมง

| ด้าน | ระดับ | มิติผลกระทบ 4 ด้าน |
|--------------------------------|-------|---|
| S : Strategic ด้านกลยุทธ์ | 1 | ไม่มีผลกระทบกับการกำหนดเป้าหมายการดำเนินงาน ไม่มีการหยุดชะงักของกระบวนการและการดำเนินงานทางธุรกิจ |
| O : Operation ด้านการดำเนินงาน | 2 | มีผลกระทบต่อกระบวนการทำงานน้อย แต่ไม่สร้างความเสียหาย |
| F : Finance ด้านการเงิน | 2 | มีการสูญเสียทางการเงินมากกว่า 10,000 – 50,000 บาท |
| C : Compliance ด้านกฎระเบียบ | 1 | ไม่มีผลกระทบต่อการไม่ปฏิบัติตามระเบียบข้อบังคับ และกฎหมาย |

ตารางที่ 15 ตารางแสดงกรณีระบบ AD ใช้งานไม่ได้ 3 ชั่วโมง

กรณีระบบ AD ใช้งานไม่ได้ 8 ชั่วโมง

| ด้าน | ระดับ | มิติผลกระทบ 4 ด้าน |
|--------------------------------|-------|---|
| S : Strategic ด้านกลยุทธ์ | 2 | มีผลกระทบกับการกำหนดเป้าหมายการดำเนินงานน้อย แต่ไม่สร้างความเสียหายต่อการดำเนินงานทางธุรกิจ |
| O : Operation ด้านการดำเนินงาน | 3 | มีผลกระทบต่อกระบวนการทำงานปานกลาง สร้างความเสียหายบางกิจกรรม/ขั้นตอน |
| F : Finance ด้านการเงิน | 3 | มีการสูญเสียทางการเงินมากกว่า 50,000 – 250,000 บาท |
| C : Compliance ด้านกฎระเบียบ | 1 | ไม่มีผลกระทบต่อการไม่ปฏิบัติตามระเบียบข้อบังคับ และกฎหมาย |

ตารางที่ 16 ตารางแสดงกรณีระบบ AD ใช้งานไม่ได้ 8 ชั่วโมง

กรณีระบบ AD ใช้งานไม่ได้ 24 ชั่วโมง

| ด้าน | ระดับ | มิติผลกระทบ 4 ด้าน |
|--------------------------------|-------|---|
| S : Strategic ด้านกลยุทธ์ | 2 | มีผลกระทบกับการกำหนดเป้าหมายการดำเนินงานน้อย แต่ไม่สร้างความเสียหายต่อการดำเนินงานทางธุรกิจ |
| O : Operation ด้านการดำเนินงาน | 4 | มีผลกระทบต่อกระบวนการทำงานสูง และสร้างความเสียหายต่อผลการดำเนินงานธุรกิจ |
| F : Finance ด้านการเงิน | 4 | มีการสูญเสียทางการเงินมากกว่า 250,000 – 10,000,000 บาท |
| C : Compliance ด้านกฎระเบียบ | 1 | ไม่มีผลกระทบต่อการไม่ปฏิบัติตามระเบียบ ข้อบังคับ และกฎหมาย |

ตารางที่ 17 ตารางแสดงกรณีระบบ AD ใช้งานไม่ได้ 24 ชั่วโมง

กรณีระบบ AD ใช้งานไม่ได้มากกว่า 1 วัน

| ด้าน | ระดับ | มิติผลกระทบ 4 ด้าน |
|--------------------------------|-------|---|
| S : Strategic ด้านกลยุทธ์ | 2 | มีผลกระทบกับการกำหนดเป้าหมายการดำเนินงาน แต่ไม่สร้างความเสียหายต่อการดำเนินงานทางธุรกิจ |
| O : Operation ด้านการดำเนินงาน | 5 | มีผลกระทบต่อกระบวนการทำงานสูงมาก และสร้างความเสียหายจนไม่สามารถดำเนินธุรกิจต่อไปได้ |
| F : Finance ด้านการเงิน | 5 | มีการสูญเสียทางการเงินมากกว่า 10,000,000 บาทขึ้นไป |
| C : Compliance ด้านกฎระเบียบ | 1 | ไม่มีผลกระทบต่อการไม่ปฏิบัติตามระเบียบ ข้อบังคับ และกฎหมาย |

ตารางที่ 18 ตารางแสดงกรณีระบบ AD ใช้งานไม่ได้มากกว่า 1 วัน

3.2 การวิเคราะห์ระยะเวลาผ่านผลกระทบทางธุรกิจ (BIA)

จากการประชุมเชิงปฏิบัติการ Workshop ผลการวิเคราะห์ผลกระทบ กำหนดระยะเวลาตั้งแต่เกิดอุบัติการณ์จนถึงมีการตัดสินใจสั่งการในการดำเนินการตามมาตรการสำรองตามแผน Business Continuity Management : BCM และ Disaster Recovery Plans : DRP ซึ่งมีระยะเวลาที่สั้นลงและงบประมาณที่เหมาะสม ดังนี้

1. ช่วงเวลาการหยุดชะงักที่ อ.ส.ค. ยอมรับได้สูงสุดเป็นระยะเวลา 4 ชั่วโมง
(Maximum Tolerable Period of Disruption : MTPD = 4 ชั่วโมง)
2. ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ ที่ อ.ส.ค. กำหนดเป็นระยะเวลา 3.30 ชั่วโมง
(Recovery Time Objective : RTO = 3.30 ชั่วโมง แก้ไข 3 ชั่วโมง เดินทาง 30 นาที)
3. ปริมาณข้อมูลสูญหายที่ อ.ส.ค. ยอมรับได้เป็นระยะเวลา 24 ชั่วโมง
(Recovery Point Objective : RPO = 24 ชั่วโมง)
4. ระยะเวลาที่ อ.ส.ค. กำหนดต้องเริ่มมาตรการสำรองเป็นระยะเวลา 30 นาที
(BCP Start Time : BCP - ST = 30 นาที ค้นหาเหตุ 10 นาที เริ่มมาตรการสำรอง 20 นาที)
5. ระยะเวลาที่ อ.ส.ค. กำหนดเวลาในการใช้แผนกู้คืนเป็นระยะเวลา 3 ชั่วโมง
(Disaster Recovery Plans : DRP = 3 ชั่วโมง)

ตารางแสดงผลลัพธ์จากการวิเคราะห์ผลกระทบทางธุรกิจ

| Key Service/ process | MTPD | RTO | | RPO | BCP-ST | | PTO- BCP/ST | Normal | BCP | DRP |
|----------------------|--------|---------|--------|---------|---------------|---------------|-------------|------------|----------------------------|--------|
| | | เดินทาง | กู้คืน | | Service Level | Service Level | | | | |
| ระบบ AD | 4 hrs. | 30 min | 3 hrs. | 24 hrs. | 10 min | 20 min | 4 hrs. | 1,083 User | 100 User (สนง. ละ 20 User) | 3 hrs. |

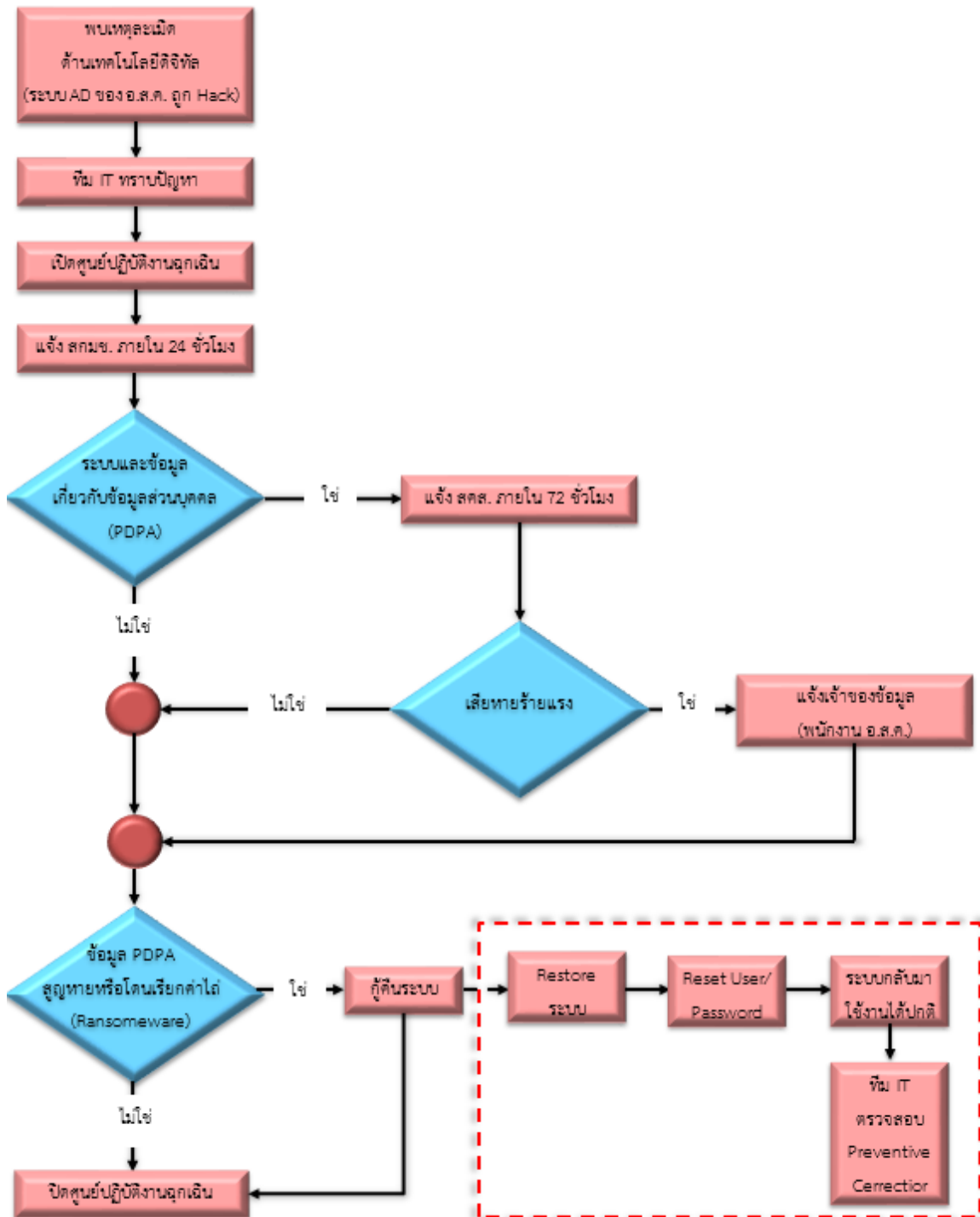
ตารางที่ 19 ผลลัพธ์จากการวิเคราะห์ผลกระทบทางธุรกิจ

บทที่ 4

การพัฒนาและเตรียมการตอบสนองต่อ
เหตุการณ์ในภาวะฉุกเฉิน
(Developing and Implementing BCM Response)

4.1 เหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจมตี)

เมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจมตี) ขึ้นกับ อ.ส.ค. ทุกฝ่าย/สำนักงาน ทีมงานที่ดูแลด้านเทคโนโลยีสารสนเทศควรประเมินเหตุการณ์ที่เกิดขึ้น โดยพิจารณาหลักเกณฑ์ดังต่อไปนี้



รูปที่ 5 แผนผังแสดงการดำเนินการในเบื้องต้นของเหตุการณ์ภัยคุกคามทางไซเบอร์

4.1.1 การประเมินสถานการณ์เมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม)

พิจารณาความรุนแรง โดยแบ่งออกเป็น 2 ระดับ ดังนี้

- **ระดับความรุนแรงขั้นต้น** : การเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ โดย Hacker โจรกรรมข้อมูล User และ Password ของพนักงานทุกคนใน อ.ส.ค. โดยฝ่ายเทคโนโลยีดิจิทัล สามารถควบคุมสถานการณ์ได้อย่างรวดเร็ว โดยรีบดำเนินการ Restore ระบบและ Reset User และ Password ได้ทันกาล ประกอบกับ Hacker ไม่ได้นำข้อมูลไปเรียกค่าไถ่ ซึ่งส่งผลกระทบต่อเล็กน้อย โดยเหตุการณ์การถูกโจรกรรมข้อมูลอยู่ในขอบเขตที่จำกัด องค์กรสามารถควบคุมสถานการณ์ได้

- **ระดับความรุนแรงสูง** : การเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีผลต่อการสูญเสียกระบวนการทำงาน หรือมีผลกระทบต่อข้อมูลส่วนบุคคลขั้นร้ายแรง เนื่องจาก Hacker ดำเนินการเรียกค่าไถ่และนำข้อมูลส่วนบุคคลของพนักงานใน อ.ส.ค. เผยแพร่ต่อสาธารณะ อ.ส.ค. ไม่สามารถควบคุมสถานการณ์การถูกโจรกรรมได้ โดยทีมปฏิบัติการฉุกเฉินจำเป็นต้องเร่งดำเนินการ Restore ระบบ และ Reset User และ Password และแจ้งต่อกองกฎหมายที่มีความเชี่ยวชาญด้านกฎหมาย เพื่อดำเนินการตามกระบวนการด้านกฎหมายต่อไป

4.2 แผนบริหารความต่อเนื่องทางธุรกิจภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม)

แผนบริหารความต่อเนื่องทางธุรกิจภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจรกรรม)

| 1. IMP : ก่อนเกิดเหตุการณ์ | 2. BCP : เกิดเหตุฯ | 3. BRP : ฟื้นฟู |
|--|---|--|
| มาตรการ | มาตรการ | มาตรการ |
| <ul style="list-style-type: none"> - พบเหตุละเมิดด้านเทคโนโลยีดิจิทัล ระบบ) AD ของ อ.ถูก .ค.ส.Hack) - ฝ่ายเทคโนโลยีสารสนเทศ รับทราบเหตุการณ์ | <ul style="list-style-type: none"> - รับทราบ/ประเมินสถานการณ์ - เปิดศูนย์ปฏิบัติการฉุกเฉิน - แจ้งผู้อำนวยการ อ.ส.ค. ทราบ (ประธานคณะกรรมการ BCM) - แจ้งรองผู้อำนวยการ อ.ส.ค. (ประธานคณะกรรมการ BCP) - แจ้งทีมเทคโนโลยีดิจิทัล 5 สำนักงานภาค | <ul style="list-style-type: none"> - แจ้ง สกมช. ภายใน 24 ชั่วโมง - ประเมินสถานการณ์ระบบและข้อมูลเกี่ยวกับข้อมูลส่วนบุคคล (PDPA) |
| <ul style="list-style-type: none"> - ประเมินสถานการณ์ - ศูนย์ปฏิบัติการฉุกเฉินเริ่มดำเนินการ - แจ้งให้รองผู้อำนวยการ อ.ส.ค. (ประธานคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ ด้านเทคโนโลยีสารสนเทศและแผนจัดการเหตุฉุกเฉิน BCP) รับทราบ | <ul style="list-style-type: none"> - แจ้งเลขานุการคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ ด้านเทคโนโลยีสารสนเทศและแผนจัดการเหตุฉุกเฉิน ให้ใช้แผน BCP กรณีภัยคุกคามทางไซเบอร์ - กำกับติดตามให้การดำเนินงานตามแผน BCP เป็นไปด้วยความเรียบร้อย | <ul style="list-style-type: none"> - แจ้ง สคส. ภายใน 72 ชั่วโมง - ดำเนินการกู้คืนระบบ (Restore ระบบ ,Reset User&Password) - ประเมินสถานการณ์สำรวจ/สรุปความเสียหาย รายงานคณะกรรมการบริหารความต่อเนื่องทางธุรกิจฯ ได้ทราบและกำกับติดตามการฟื้นฟูระบบงาน ให้สามารถให้บริการพนักงานได้ตามปกติ |

แผนบริหารความต่อเนื่องทางธุรกิจภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจมตี)

| 1. IMP : ก่อนเกิดเหตุการณ | 2. BCP : เกิดเหตุฯ | 3. BRP : ฟื้นฟู |
|---|--|--|
| มาตรการ | มาตรการ | มาตรการ |
| <ul style="list-style-type: none"> - ประเมินสถานการณ์ - แจ้งให้รองผู้อำนวยการ อ.ส.ค. (ประธานคณะทำงานบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศและแผนจัดการเหตุฉุกเฉิน BCP) | <ul style="list-style-type: none"> - แจ้งทีมไอทีทุกสำนักงานภาคได้ทราบถึงการใช้แผนเพื่อให้เตรียมห้องสำรองเป็นไปด้วยความเรียบร้อย - พนักงานที่ปฏิบัติงานหลักและระบบงานที่สำคัญ สามารถปฏิบัติงานได้บางราย | <ul style="list-style-type: none"> - รับทราบ/ประเมินสถานการณ์ - ประกาศยกเลิกใช้แผน BCP กรณี - แจ้งประธานคณะทำงานบริหารความต่อเนื่องทางธุรกิจฯ (รองผู้อำนวยการ อ.ส.ค.) รับทราบ |
| | <ul style="list-style-type: none"> - ทีมไอทีอำนวยความสะดวกในการแก้ไขสถานการณ์ภัยคุกคามทางไซเบอร์ให้ระบบ AD กลับมาใช้งานได้โดยเร็ว | <ul style="list-style-type: none"> - แจ้งเลขานุการ เพื่อประกาศยกเลิกใช้แผน BCP กรณีระบบ AD ถูกโจมตี - แจ้งทีมงาน BCP กรณีระบบ AD ถูกโจมตีให้ทราบ เพื่อให้ทีมงานกลับคืนสู่การทำงานปกติ - แจ้งพนักงานและส่วนงานที่เกี่ยวข้องทั้งหมด |

ตารางที่ 20 ตารางแสดงแผนบริหารความต่อเนื่องทางธุรกิจภัยคุกคามทางไซเบอร์ (ระบบ AD ถูกโจมตี)

บทที่ 5

การทดสอบ ปรับปรุงและทบทวนแผน
(Exercising Maintaining)

การทดสอบ ปรับปรุง และทบทวนแผนการจัดเตรียมระบบ BCM รวมถึงการตรวจประเมินจะช่วยให้องค์กรมั่นใจได้ว่า รายละเอียดที่ระบุในแผนการจัดการปฏิบัติการและแผนความต่อเนื่องทางธุรกิจครบถ้วน ถูกต้องและเป็นปัจจุบันอยู่เสมอ เพื่อให้แน่ใจได้ว่า BCM ที่ได้จัดทำขึ้นสามารถใช้ได้จริง รวมทั้งเพื่อเตรียมความพร้อมตลอดจนตรวจสอบความสามารถของบุคลากร และประสิทธิภาพของแผนในการตอบสนองต่อวิกฤติการณ์ โดยรูปแบบการทดสอบอาจมีตั้งแต่ระดับง่ายไปหายาก

5.1 กระบวนการแจ้งเหตุฉุกเฉิน (Call tree)

กระบวนการ Call tree คือกระบวนการแจ้งเหตุฉุกเฉินให้กับสมาชิกในคณะกรรมการความต่อเนื่องทางธุรกิจ โดยมีวัตถุประสงค์เพื่อบริหารจัดการขั้นตอนในการติดต่อบุคลากรภายหลัง จากมีประกาศเหตุการณ์ฉุกเฉินหรือภาวะวิกฤตของหน่วยเทคโนโลยีสารสนเทศ

จุดเริ่มต้นของกระบวนการ Call Tree จะเริ่มจากหัวหน้าคณะทำงานวางแผนความต่อเนื่องทางธุรกิจแจ้งผู้ประสานงานคณะทำงานวางแผนความต่อเนื่องทางธุรกิจ โดยผู้ประสานงานฯ จะแจ้งหัวหน้าทีมวางแผนความต่อเนื่องทางธุรกิจรับทราบเหตุการณ์ฉุกเฉินและประกาศใช้แผนบริหารความต่อเนื่องทางธุรกิจ

จากนั้นหัวหน้าทีมบริหารความต่อเนื่องทางธุรกิจจะดำเนินการติดต่อและแจ้งไปยังทีมงานของตนตลอดจนบุคลากรภายใต้บังคับบัญชาตามสายงานบังคับบัญชา เพื่อรับทราบเหตุการณ์ฉุกเฉินและประกาศใช้แผนบริหารความต่อเนื่องทางธุรกิจ ที่ได้รับผลกระทบตามรายชื่อและช่องทางการติดต่อสื่อสาร ประกอบด้วย ประธานคณะทำงานวางแผนความต่อเนื่องทางธุรกิจ ในการบริหารความต่อเนื่องทางธุรกิจ ผู้ประสานงานคณะทำงานวางแผนความต่อเนื่องทางธุรกิจและทีมวางแผนความต่อเนื่องทางธุรกิจ

กรณีที่ไม่สามารถติดต่อหัวหน้าทีมได้ ให้ติดต่อไปยังบุคลากรสำรอง โดยพิจารณา ดังนี้

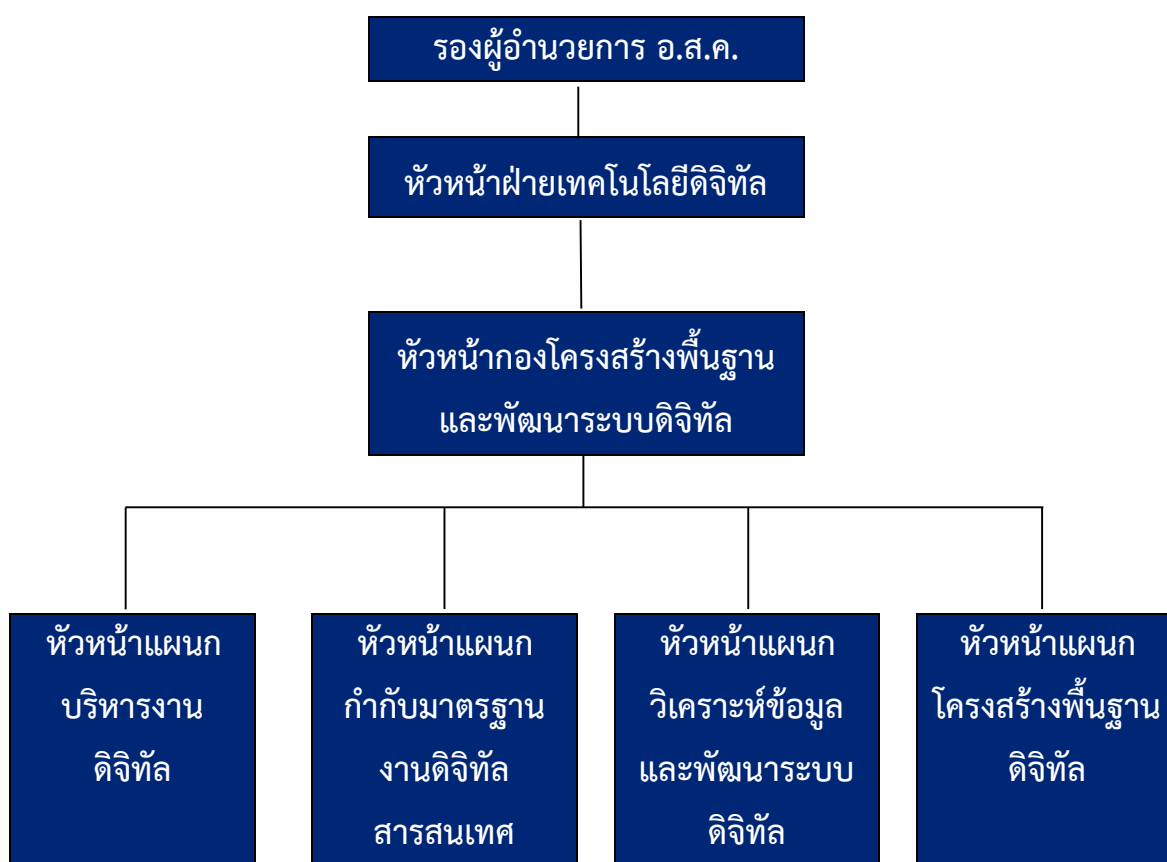
1. ถ้าเหตุการณ์เกิดขึ้นในเวลาทำการ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์ของหน่วยงานเป็นช่องทางแรก
2. ถ้าเหตุการณ์เกิดขึ้นนอกเวลาทำการหรือสถานที่ที่ปฏิบัติงานหลักได้รับผลกระทบ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์เป็นช่องทางแรก
3. ถ้าสามารถติดต่อบุคลากรหลักได้ให้แจ้งข้อมูลแก่บุคลากรหลักของหน่วยงานทราบดังต่อไปนี้

3.1 สรุปสถานการณ์ของเหตุการณ์ฉุกเฉินและประกาศใช้แผนบริหารความ
ต่อเนื่อง

3.2 เวลาและสถานที่สำหรับการนัดประชุมเร่งด่วนของหน่วยงาน สำหรับ
ผู้บริหารของหน่วยงานและคณะทำงานวางแผนความต่อเนื่องทางธุรกิจ

3.3 ขั้นตอนการปฏิบัติงาน เพื่อบริหารความต่อเนื่องทางธุรกิจต่อไป เช่น
สถานที่ที่รวมพลในกรณีที่มีการย้ายสถานที่ทำงานไปยังสถานที่สำรอง

แผนผังโครงสร้าง CallTree ด้านเทคโนโลยีสารสนเทศ



รูปที่ 9 แสดงแผนผังโครงสร้าง CallTree ของหน่วยเทคโนโลยีสารสนเทศ

5.2 กระบวนการแจ้งเหตุ Call tree

ภายหลังจากได้รับการตอบรับจากบุคลากรหลักครบถ้วนตามผังการติดต่อ (Call Tree) หัวหน้าทีมงานบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ มีหน้าที่โทรกลับไปแจ้งยังผู้ประสานงานคณะบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ เพื่อรวบรวมสรุปความพร้อมของหน่วยเทคโนโลยีสารสนเทศ ในการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ รวมทั้งความปลอดภัยในชีวิต ทรัพย์สิน และเจ้าหน้าที่ทั้งหมด

ทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ มีหน้าที่ในการปรับปรุงข้อมูลสำหรับการติดต่อให้เป็นปัจจุบันอยู่ตลอดเวลา เพื่อให้กระบวนการติดต่อพนักงานภายในองค์กรสามารถดำเนินงานได้อย่างต่อเนื่อง และสำเร็จลุล่วงในระยะเวลาที่คาดหวังในกรณีที่เกิดเหตุการณ์ฉุกเฉินและมีการประกาศใช้แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

5.3 Tabletop Testing

การประชุมแลกเปลี่ยนความคิดเห็นกับทุกหน่วยที่เกี่ยวข้องโดยจำลองโจทย์สถานการณ์ขึ้นมา และลองนำแผน BCP มาพิจารณาว่า ใช้ตอบโจทย์แต่ละขั้นตอนได้หรือไม่

5.4 Simulation

มีการทดสอบแผนบริหารความต่อเนื่องฯ บางส่วนหรือทั้งหมดเป็นประจำทุกปี เพื่อให้มั่นใจว่าหน่วยงานมีการเตรียมตัวและมีความสามารถในการกู้คืนธุรกิจสำคัญภายในระยะเวลาที่กำหนดไว้

ควรทดสอบแผนบริหารความต่อเนื่องทางธุรกิจ โดยการสร้างสถานการณ์จำลอง (Simulation WExercises) เป็นประจำทุกปี โดยต้องมีการปรับเปลี่ยนหมุนเวียนสถานการณ์จำลอง เพื่อให้แน่ใจว่าได้มีการทดสอบความสูญเสีย/เสียหายของปัจจัยหลักที่เกี่ยวข้องทุกๆ 1 ปี

ข้อบกพร่อง ใดๆ (GAP) ที่เกิดจากการทดสอบการบริหารความต่อเนื่องทางธุรกิจ จะต้องมีการติดตามให้เสร็จสิ้นภายใน 3 เดือน นับตั้งแต่วันที่ทดสอบ ถ้าไม่สามารถดำเนินการติดตามได้ตามเวลาที่กำหนดให้หัวหน้าทีมและผู้ประสานงานความต่อเนื่องทางธุรกิจได้แจ้งผู้บริหารระดับสูงเพื่อพิจารณาแนวทางแก้ไขข้อบกพร่องนั้นๆ ให้หมดไปโดยเร็ว

5.5 Full BCP Exercise

การทดสอบเต็มรูปแบบและใกล้เคียงสถานการณ์จริงมากที่สุด

5.6 การดูแลปรับปรุงแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Maintenance of the plan)

กำหนดให้ต้องมีการปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจ ให้เป็นปัจจุบันทุกปี หรือทุกครั้งหลังการทดสอบหรือภายใน 3 เดือน ในกรณีที่มีการเปลี่ยนแปลงสำคัญ เช่น รายชื่อผู้ที่จะต้องได้รับการแจ้งเหตุ (Staff Recall List) ควรมีการปรับปรุงให้เป็นปัจจุบันทุกๆ ไตรมาส การลดความซับซ้อนของขั้นตอนต่างๆ และส่งสำเนาให้กับเลขานุการคณะทำงานวางแผนความต่อเนื่องทางธุรกิจ เพื่อให้ทราบการเปลี่ยนแปลงหน้าที่ความรับผิดชอบของทีม การปฏิบัติหน้าที่และขั้นตอนปฏิบัติต่างๆ ที่สอดคล้องกับการบริหารความต่อเนื่องทางธุรกิจ ฐานข้อมูลบัญชีรายการ/รายชื่อ และคู่มือปฏิบัติงานทั้งหมด ซึ่งเป็นส่วนหนึ่งของการบริหารความต่อเนื่องทางธุรกิจ หรือต้องมีการอ้างอิงไว้ในการบริหารความต่อเนื่องทางธุรกิจ ต้องปรับปรุงให้เป็น ปัจจุบันอยู่เสมอ

บทที่ 6

การปลูกฝัง BCM ให้เป็นส่วนหนึ่ง
ของวัฒนธรรมองค์กร

(Embedding BCM in the Organization's Culture)

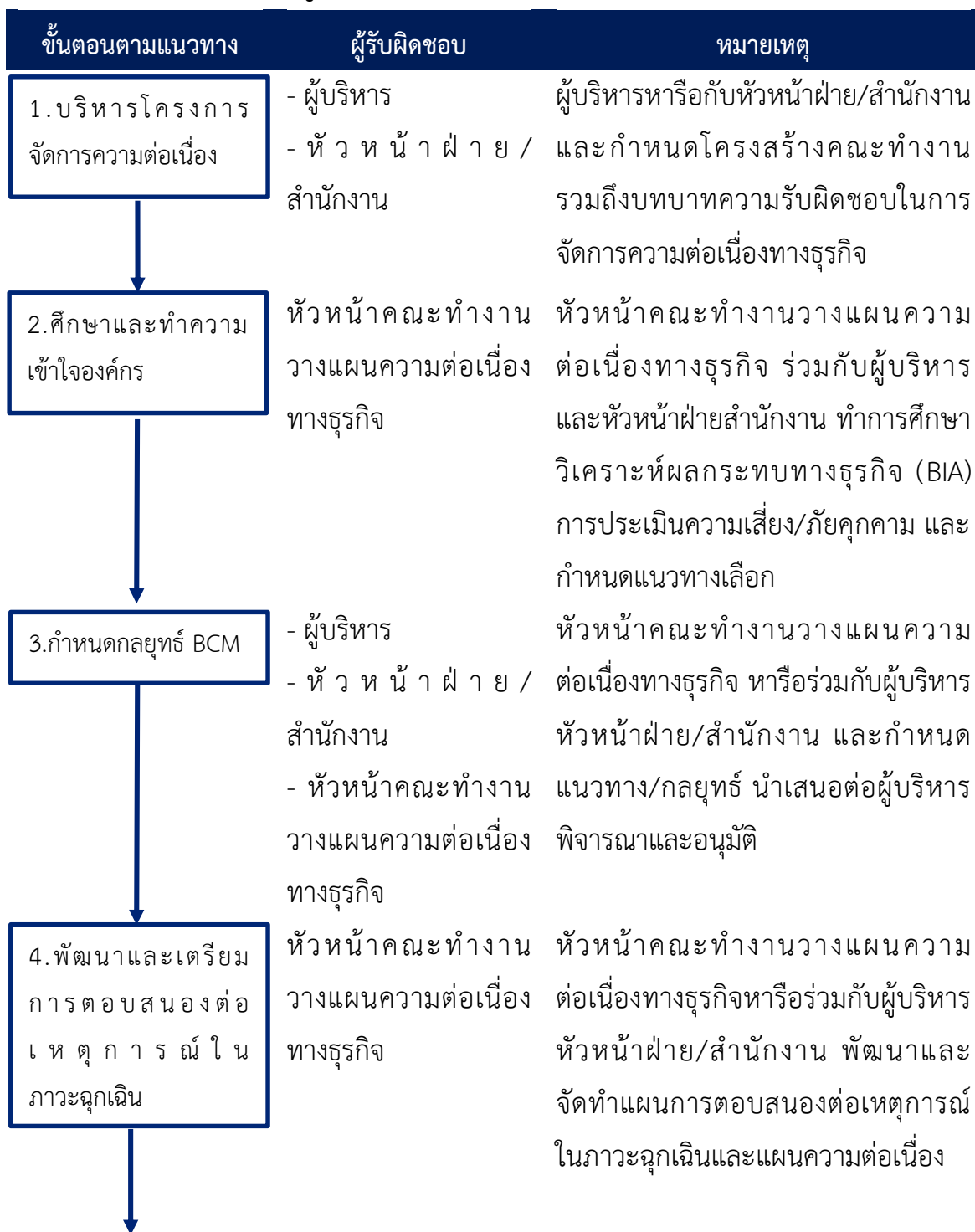
6.1 การปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร

เป็นขั้นตอนที่สำคัญประการหนึ่งในการทำให้ BCM ผสมกลมกลืนเข้าจนเป็นวัฒนธรรมองค์กรโดยเป็นเรื่องที่ต้องใช้เวลาและจิตวิทยาที่จะทำให้พนักงานทุกคนได้ซึมซาบและเข้าใจถึงความสำคัญของ BCM ตลอดจนบทบาทหน้าที่ที่ทุกคนพึงมีเพื่อให้ภารกิจสามารถดำเนินต่อไปได้ในยามที่เกิดเหตุวิกฤติ การปลูกฝังวัฒนธรรมองค์กรเกี่ยวกับการบริหารความต่อเนื่องทางธุรกิจ เพื่อให้เกิดความตระหนักถึงการบริหารความต่อเนื่องทางธุรกิจกลายเป็นส่วนหนึ่งของการปฏิบัติงานหลักขององค์กร พร้อมทั้งเพิ่มความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งหมดในด้านการบริหารจัดการอุบัติการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อ การดำเนินธุรกิจของ อ.ส.ค.

โดยการสร้างให้เกิดวัฒนธรรมที่ส่งเสริมให้การดำเนินงานของระบบ BCM เป็นส่วนหนึ่งของค่านิยมของ อ.ส.ค. และการบริหารที่มีประสิทธิผล โดยจะต้อง

1. สร้างให้เกิดจิตสำนึกทางด้าน BCM ให้เกิดกับบุคลากร อ.ส.ค. โดยให้มีความรู้ความเข้าใจ และความตระหนักถึง BCM รวมถึงมีการประเมินความมีประสิทธิผลของการดำเนินการอย่างสม่ำเสมอ
2. สื่อสารให้บุคลากรของ อ.ส.ค. ได้เห็นถึงความสำคัญของการบรรลุวัตถุประสงค์ของ BCM การปฏิบัติตามนโยบาย BCM และปรับปรุงระบบอย่างต่อเนื่อง
3. ดูแลให้มั่นใจได้ว่าบุคลากรในองค์กร มีความตระหนักถึงการมีส่วนร่วมที่จะทำให้วัตถุประสงค์ BCM ประสบความสำเร็จตามที่กำหนด

ขั้นตอนการปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร



รูปที่ 6 ขั้นตอนการปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร

ขั้นตอนการปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร (ต่อ)

| ขั้นตอนตามแนวทาง | ผู้รับผิดชอบ | หมายเหตุ |
|--|--|--|
| 5. การทดสอบปรับปรุงและทบทวนแผน | หัวหน้าคณะทำงานวางแผนความต่อเนื่องทางธุรกิจ | หัวหน้าคณะทำงานวางแผนความต่อเนื่องทางธุรกิจ ร่วมกับผู้บริหารและหัวหน้าฝ่าย/สำนักงาน ดำเนินการทดสอบแผนที่ได้มีการจัดทำขึ้น |
| 6. ปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรม | <ul style="list-style-type: none"> - ผู้บริหาร - หัวหน้าฝ่าย / สำนักงาน - หัวหน้าคณะทำงานวางแผนความต่อเนื่องทางธุรกิจ | <p>คณะทำงานวางแผนความต่อเนื่องทางธุรกิจ ร่วมกับผู้บริหารและหัวหน้าฝ่าย/สำนักงาน นำเสนอแนวทางการปลูกฝัง BCM แก่พนักงานทุกฝ่าย/สำนักงานนำไปปฏิบัติ</p> |

รูปที่ 6 ขั้นตอนการปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร

ภาคผนวก



ประกาศองค์การส่งเสริมกิจการโคนมแห่งประเทศไทย
นโยบายการบริหารความต่อเนื่องทางธุรกิจ อ.ส.ค.
(Business Continuity Management BCM)

องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย (อ.ส.ค.) เป็นองค์กรรัฐวิสาหกิจที่ดำเนินกิจการด้านอุตสาหกรรมนม ซึ่งครอบคลุมกิจกรรมตั้งแต่ต้นน้ำ (ส่งเสริม) กลางน้ำ (ผลิต) และปลายน้ำ (จำหน่าย) โดยต้องดำเนินการผลิตและจำหน่ายผลิตภัณฑ์จากนมโคที่มีคุณภาพในปริมาณที่สอดคล้องกับความต้องการของตลาดในแต่ละพื้นที่ ทั้งนี้ในการดำเนินกิจการมีโอกาสเกิดอุบัติเหตุการณ์ต่างๆ ที่อาจส่งผลให้เกิดการหยุดชะงักของกิจกรรมสำคัญซึ่งอาจส่งผลกระทบต่อผู้มีส่วนได้ส่วนเสีย ภาพลักษณ์ชื่อเสียงและกิจกรรมสำคัญขององค์กร อ.ส.ค.ได้เล็งเห็นถึงความสำคัญของการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจเพื่อเตรียมความพร้อมในการรองรับอุบัติเหตุการณ์ต่างๆ เพื่อป้องกันและบรรเทาผลกระทบที่อาจเกิดขึ้นของอุบัติเหตุการณ์จึงได้กำหนดนโยบายการบริหารความต่อเนื่องทางธุรกิจของ อ.ส.ค. ไว้ดังนี้

1. อ.ส.ค. ต้องพัฒนาระบบการบริหารความต่อเนื่องทางธุรกิจให้สอดคล้องกับมาตรฐานสากล ซึ่งต้องมีความครอบคลุมถึงการวิเคราะห์ผลกระทบทางธุรกิจ การประเมินความเสี่ยง การวางกลยุทธ์ การนำไปปฏิบัติการฝึกซ้อม การทบทวนปรับปรุงแก้ไขแผนอย่างต่อเนื่อง ตลอดจนการปลูกฝังจิตสำนึกด้านการบริหารความต่อเนื่องทางธุรกิจสู่วัฒนธรรมองค์กร ผ่านกระบวนการฝึกอบรมและการสื่อสารภายในองค์กรให้มีประสิทธิผล
2. ให้คณะกรรมการบริหารความต่อเนื่องทางธุรกิจ (BCM Team) ของ อ.ส.ค. มีหน้าที่ในการจัดทำระบบการบริหารความต่อเนื่องทางธุรกิจ และดำเนินการต่างๆ เพื่อให้เกิดการบริหารจัดการความต่อเนื่องทางธุรกิจที่มีประสิทธิผล
3. ให้ผู้บริหารทุกระดับของ อ.ส.ค. มีหน้าที่ผลักดัน และสนับสนุนการดำเนินงานต่างๆ ในส่วนที่เกี่ยวข้องกับกระบวนการบริหารความต่อเนื่องทางธุรกิจของ อ.ส.ค.
4. ผู้บริหาร พนักงานและลูกจ้างของ อ.ส.ค. ต้องตระหนักถึงการมีส่วนร่วมเพื่อให้การดำเนินการบริหารความต่อเนื่องทางธุรกิจของ อ.ส.ค. บรรลุตามวัตถุประสงค์

ประกาศ ณ วันที่ 1 ตุลาคม 2565

(นายสมพร ศรีเมือง)

ผู้อำนวยการ

องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย อ.ส.ค.



คำสั่งองค์การส่งเสริมกิจการโคนมแห่งประเทศไทย
ที่ ๑ /๒๕๖๖
เรื่อง แต่งตั้งคณะกรรมการบริหารความต่อเนื่องทางธุรกิจของ อ.ส.ค.
(Business Continuity Management : BCM)

เพื่อให้การดำเนินงานในด้านการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) เป็นไปด้วยความเรียบร้อย บรรลุวัตถุประสงค์ และสามารถบริหารความพร้อมต่อสภาวะวิกฤติขององค์กรอย่างมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๒๑ และมาตรา ๒๔ แห่งพระราชกฤษฎีกาจัดตั้ง อ.ส.ค. พ.ศ. ๒๕๑๔ และที่แก้ไขเพิ่มเติม ประกอบด้วย

| ๑. ผู้อำนวยการ | ประธานคณะกรรมการ |
|--|-------------------------------|
| ๒. รองผู้อำนวยการ ๑ ท่าน | คณะกรรมการ |
| ๓. ผู้ช่วยผู้อำนวยการ ๒ ท่าน | คณะกรรมการ |
| ๔. หัวหน้าฝ่ายผู้อำนวยการ | คณะกรรมการ |
| ๕. หัวหน้าฝ่ายนโยบายและยุทธศาสตร์ | คณะกรรมการ |
| ๖. หัวหน้าฝ่ายเทคโนโลยีดิจิทัล | คณะกรรมการ |
| ๗. หัวหน้าฝ่ายทรัพยากรบุคคล | คณะกรรมการ |
| ๘. หัวหน้าฝ่ายบัญชีและการเงิน | คณะกรรมการ |
| ๙. หัวหน้าฝ่ายพัสดุและบริการ | คณะกรรมการ |
| ๑๐. หัวหน้าฝ่ายวิจัยและพัฒนาการเลี้ยงโคนม | คณะกรรมการ |
| ๑๑. หัวหน้าฝ่ายส่งเสริมการเลี้ยงโคนม | คณะกรรมการ |
| ๑๒. หัวหน้าฝ่ายท่องเที่ยวเชิงเกษตร | คณะกรรมการ |
| ๑๓. หัวหน้าฝ่ายการตลาดและการขาย | คณะกรรมการ |
| ๑๔. หัวหน้าสำนักงาน อ.ส.ค. ภาคกลาง | คณะกรรมการ |
| ๑๕. หัวหน้าสำนักงาน อ.ส.ค. ภาคใต้ | คณะกรรมการ |
| ๑๖. หัวหน้าสำนักงาน อ.ส.ค. ภาคตะวันออกเฉียงเหนือ | คณะกรรมการ |
| ๑๗. หัวหน้าสำนักงาน อ.ส.ค. ภาคเหนือตอนล่าง | คณะกรรมการ |
| ๑๘. หัวหน้าสำนักงาน อ.ส.ค. ภาคเหนือตอนบน | คณะกรรมการ |
| ๑๙. หัวหน้ากองเลขานุการคณะกรรมการโคนมและผลิตภัณฑ์นม | คณะกรรมการ |
| ๒๐. หัวหน้ากองบริหารจัดการและพัฒนาองค์กร ฝ่ายนโยบายและยุทธศาสตร์ | คณะกรรมการและเลขานุการ |
| ๒๑. หัวหน้าแผนกบริหารความเสี่ยงและควบคุมภายใน กองบริหารจัดการและพัฒนาองค์กร ฝ่ายนโยบายและยุทธศาสตร์ | คณะกรรมการและผู้ช่วยเลขานุการ |

โดยให้คณะทำงานฯ มีอำนาจหน้าที่ดังนี้

๑. ศึกษา วิเคราะห์ และประเมินความเสี่ยงที่อาจส่งผลกระทบต่อ การปฏิบัติภารกิจหลัก หรือ งานบริการสำคัญของ อ.ส.ค. เมื่อเกิดสภาวะวิกฤติ

๒. สื่อสารทำความเข้าใจให้บุคลากรของ อ.ส.ค. มีความรู้ ความเข้าใจ เกิดความตระหนักและมีความพร้อมเมื่อเกิดสภาวะวิกฤติ

๓. ติดตาม ประเมินผล รวมทั้งให้ข้อเสนอแนะเพื่อปรับปรุง และทบทวนแผนบริหาร ความต่อเนื่องทางธุรกิจให้มีประสิทธิภาพยิ่งขึ้น

๔. จัดทำรายงานสรุปผลการปฏิบัติงานตามแผนบริหารความต่อเนื่องทางธุรกิจ ต่อคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายในของ อ.ส.ค.

๕. ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป หากคำสั่งใดซึ่งขัดแย้งหรือแย้งตามคำสั่งนี้ให้ถือปฏิบัติตามคำสั่งนี้

สั่ง ณ วันที่ ๑ ตุลาคม ๒๕๖๕

(นายสมพร ศรีเมือง)

ผู้อำนวยการ

องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย



คำสั่งองค์การส่งเสริมกิจการโคนมแห่งประเทศไทย
ที่ ๑๑๔/๒๕๖๖
เรื่อง แต่งตั้งคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ
ด้านเทคโนโลยีสารสนเทศและแผนจัดการเหตุฉุกเฉิน (Business Continuity plan : BCP)

เพื่อให้องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย ถือปฏิบัติและจัดทำขึ้นเพื่อให้เกิดความมั่นใจว่าองค์การส่งเสริมกิจการโคนมแห่งประเทศไทย จะมีการดำเนินงานในธุรกิจสำคัญอย่างต่อเนื่องไม่หยุดชะงักเมื่อมีเหตุการณ์ความเสี่ยงที่เป็นภาวะวิกฤติ มีการแต่งตั้งคณะกรรมการบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ และแผนจัดการเหตุฉุกเฉิน เพื่อดำเนินการพัฒนาเป็นไปตามกรอบและแนวทางที่มีมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๒๑ และมาตรา ๒๔ แห่งพระราชกฤษฎีกาจัดตั้ง อ.ส.ค. พ.ศ. ๒๕๑๔ และที่แก้ไขเพิ่มเติม จึงแต่งตั้งคณะกรรมการบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ และแผนจัดการเหตุฉุกเฉิน (Business Continuity plan : BCP) ประกอบด้วย

- | | |
|---|------------------------|
| ๑. รองผู้อำนวยการ อ.ส.ค. | ประธานคณะกรรมการ |
| ๒. หัวหน้าฝ่ายเทคโนโลยีดิจิทัล | คณะกรรมการ |
| ๓. หัวหน้าฝ่ายนโยบายและยุทธศาสตร์ | คณะกรรมการ |
| ๔. หัวหน้าฝ่ายบัญชีและการเงิน | คณะกรรมการ |
| ๕. หัวหน้าฝ่ายการตลาดและการขาย | คณะกรรมการ |
| ๖. หัวหน้ากองกลยุทธ์ดิจิทัล | คณะกรรมการ |
| ๗. หัวหน้าแผนกบริหารงานดิจิทัล | คณะกรรมการ |
| ๘. หัวหน้าแผนกกำกับมาตรฐานงานดิจิทัลสารสนเทศ | คณะกรรมการ |
| ๙. หัวหน้าแผนกวิเคราะห์ข้อมูลและพัฒนาระบบดิจิทัล | คณะกรรมการ |
| ๑๐. หัวหน้ากองโครงสร้างพื้นฐานและพัฒนาระบบดิจิทัล | คณะกรรมการและเลขานุการ |
| ๑๑. หัวหน้าแผนกโครงสร้างพื้นฐานดิจิทัล | ผู้ช่วยเลขานุการ |

หน้าที่และอำนาจ

๑. ดำเนินการให้ระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการได้ตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP) ด้านเทคโนโลยีสารสนเทศ และแผนการจัดการเหตุฉุกเฉิน

๒. ประเมินค่าความเสียหายเบื้องต้น เมื่อระบบงานหยุดชะงัก

๓. ดำเนินการให้ศูนย์คอมพิวเตอร์สำรอง สามารถดำเนินธุรกิจอย่างต่อเนื่อง

๔. ดำเนินการกู้คืนระบบปฏิบัติการ (System) และข้อมูลระบบของ อ.ส.ค.

๕. ดำเนินการเชื่อมต่อระบบ Network ให้สามารถปฏิบัติงานได้ทั่วทั้งองค์กร

๖. ทบทวนและทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงอยู่เสมอ

๗. จัดทำรายงานประเมินความเสียหายของชีวิต ทรัพย์สิน ข้อมูล ระบบสารสนเทศที่สำคัญ ปัญหา อุปสรรค พร้อมข้อเสนอแนะเป็นลายลักษณ์อักษร เสนอต่อคณะทำงานบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM)

๘. ดำเนินการอื่นๆ ตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑ มีนาคม ๒๕๖๖



(นายสมพร ศรีเมือง)

ผู้อำนวยการ องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย









