คู่มือตรวจสอบ
การวางแผนรองรับ
การดำเนินธุรกิจอย่างต่อเนื่อง
(Business Continuity Planning)

คำนำ

คู่มือฉบับนี้เป็นส่วนหนึ่งของการปรับปรุงคู่มือการตรวจสอบระบบสารสนเทศ ฉบับเดือนพฤศจิกายน 2543 ของส่วนตรวจสอบเทคโนโลยีสารสนเทศ ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ ซึ่งเป็นการยกเลิก บทที่ 8 การเตรียมแผนสำรองฉุกเฉิน และใช้คู่มือฉบับนี้แทน ตามแนวทางของ Federal Financial Institutions Examination Council (FFIEC)[1] ประเทศสหรัฐอเมริกา

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศหวังว่าแนวทางการตรวจสอบในคู่มือฉบับนี้จะเป็นประโยชน์และช่วยพัฒนางานตรวจสอบด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพต่อไปในอนาคต

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ
ธันวาคม 2551

---

[1] FFIEC คือองค์กรร่วมระหว่างหน่วยงานกำกับดูแลสถาบันการเงินของประเทศสหรัฐอเมริกา ซึ่งได้แก่ The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision โดยจัดตั้งขึ้นเพื่อกำหนดหลักเกณฑ์ มาตรฐานการตรวจสอบและรูปแบบรายงานตรวจสอบสถาบันการเงิน รวมทั้งคอยให้คำแนะนำในการพัฒนาแนวทางการตรวจสอบสถาบันการเงินขององค์กรเหล่านั้นให้เป็นมาตรฐานเดียวกัน

สารบัญ

หน้าที่

<u>ส่วนที่ 1</u> บทนำ

คู่มือเรื่องการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning) ฉบับนี้กล่าวถึงแนวทางและวิธีการตรวจสอบสำหรับให้ผู้ตรวจสอบใช้ประเมินกระบวนการบริหารความเสี่ยงของสถาบันการเงินและผู้ให้บริการ เพื่อให้มั่นใจถึงความพร้อมของบริการที่สำคัญทางด้านการเงิน

ความเสียหายจากการดำเนินงาน (Operating disruptions) อาจเกิดขึ้นโดยมีสัญญาณเตือนมาก่อนหรือไม่ก็ได้ และผลที่เกิดขึ้นก็อาจจะสามารถคาดการณ์ได้หรืออาจไม่ทราบเลยก็ได้ เนื่องด้วยสถาบันการเงินมีบทบาทที่สำคัญต่อเศรษฐกิจของประเทศ จึงเป็นเรื่องสำคัญที่ธุรกิจของสถาบันการเงินจะต้องดำเนินการได้อย่างต่อเนื่องและสามารถลดผลกระทบที่เกิดจากเหตุการณ์ความเสียหายต่อการให้บริการทางการเงิน ทั้งนี้เพื่อให้สถาบันการเงินจะสามารถรักษาภาพลักษณ์ ความน่าเชื่อถือ และประชาชนมีความมั่นใจต่อระบบการเงิน แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องที่มีประสิทธิภาพจึงถือเป็นหลักสำคัญที่สถาบันการเงินใช้ในการรักษากระบวนการทางธุรกิจให้ดำเนินการต่อไปได้ในช่วงที่เกิดเหตุการณ์ความเสียหายซึ่งอาจเกิดขึ้นโดยไม่คาดคิด และการทำให้กระบวนการทางธุรกิจกลับคืนสู่ภาวะปกติ

การวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง เป็นกระบวนการที่จะทำให้สถาบันการเงินมั่นใจได้ว่าจะสามารถนำมาใช้งานเพื่อให้ธุรกิจดำเนินการต่อไปได้ในช่วงที่เกิดเหตุการณ์ความเสียหายและกอบกู้การดำเนินงานทางธุรกิจและการให้บริการแก่ลูกค้ากลับคืนสู่ภาวะปกติ ทั้งนี้เหตุการณ์ความเสียหาย ได้แก่ ภัยพิบัติ ปัญหาจากการใช้เทคโนโลยี ข้อผิดพลาดที่เกิดจากบุคคล หรือภัยจากการก่อการร้าย แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan - BCP) มี วัตถุประสงค์เพื่อที่จะลดความสูญเสียทางการเงินที่อาจเกิดขึ้นกับสถาบันการเงินให้เหลือน้อยที่สุด และช่วยให้สถาบันการเงินสามารถให้บริการลูกค้ารวมถึงผู้ที่เกี่ยวข้องในตลาดการเงินได้อย่างต่อเนื่อง อีกทั้งลดผลกระทบของความเสียหายที่อาจเกิดขึ้นกับแผนกลยุทธ์ ชื่อเสียง การปฏิบัติงาน สภาพคล่องคุณภาพของสินเชื่อ สถานะทางการตลาดของสถาบันการเงิน ตลอดจนความสามารถที่จะรักษาการดำเนินงานให้อยู่ภายใต้กฎหมาย ระเบียบและข้อบังคับของทางการ BCP ควรได้รับการปรับให้เป็นปัจจุบันอยู่เสมอเพื่อให้สอดคล้องกับการเปลี่ยนแปลงกระบวนการทางธุรกิจของสถาบันการเงินและของผู้ให้บริการทางการเงินอื่นที่เกี่ยวข้อง รวมทั้งรองรับภัยคุกคามรูปแบบใหม่ ๆ ที่อาจเกิดขึ้นด้วย

การสอบทาน BCP ของสถาบันการเงินเป็นส่วนหนึ่งของงานตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอยู่ในความรับผิดชอบของสายกำกับสถาบันการเงิน ความจำเป็นของการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและการเปลี่ยนแปลงเกณฑ์ในการวัด (Benchmark) ความมีประสิทธิผลของแผนงาน เกิดจากรูปแบบการดำเนินธุรกิจแบบใหม่ ๆ การเปลี่ยนแปลงทางด้านเทคโนโลยี และการเพิ่มขึ้นของการก่อการร้าย ตัวอย่างเช่น BCP ควรครอบคลุมถึงเหตุการณ์ความเสียหายในวงกว้างที่ส่งผลกระทบต่อพื้นที่ทั่วทั้งอาณาเขต และความเสียหายจากการสูญเสียพนักงานหรือไม่สามารถติดต่อพนักงานได้ นอกจากนั้นควรคำนึงถึงการพึ่งพาอาศัยกันระหว่างผู้มีส่วนเกี่ยวข้องในระบบการเงินรวมทั้งผู้ให้บริการทางการเงิน ทั้งในแง่ของตลาดการเงินและสถานที่ตั้งของสำนักงาน โดยส่วนมากสถาบันการเงินจะกำหนดระยะเวลา เป้าหมายที่จะใช้ในการกู้ระบบน้อยกว่าในอดีตที่ผ่านมา และสถาบันการเงินบางแห่งอาจกำหนดเป้าหมายเป็นจำนวนชั่วโมงหรือนาที

สถาบันการเงินส่วนใหญ่รวมประเด็นเรื่องการเตรียมความพร้อมให้ธุรกิจดำเนินงานได้อย่างต่อเนื่องเข้าไว้เป็นส่วนหนึ่งของการพัฒนากระบวนการทางธุรกิจเพื่อให้สถาบันการเงินสามารถลดความเสี่ยงที่อาจเกิดความเสียหายต่อการให้บริการ โดยในการจัดทำ BCP ให้มีประสิทธิผลนั้น สถาบันการเงินไม่ควรตั้งสมมติฐานว่าความต้องการใช้บริการของลูกค้าในช่วงที่ประสบปัญหาจะลดลง ตรงกันข้ามอาจจะมีปริมาณการใช้บริการเพิ่มมากขึ้นกว่าในภาวะปกติ เช่น ความต้องการในการใช้บริการ ATM ของลูกค้าอาจเพิ่มขึ้น เป็นต้น

การจัดทำคู่มือฉบับนี้ได้รวมแนวคิดจากบทเรียนที่ได้รับจากปัญหา Y2K ที่ได้ตระหนักถึงบทบาทสำคัญของเทคโนโลยี ดังนั้นรูปแบบการบริหารจัดการธุรกิจที่เป็นลักษณะภาพรวมทั้งองค์กรและเน้นกระบวนการเป็นสำคัญ ซึ่งคำนึงถึงเรื่องเทคโนโลยี กระบวนการดำเนินธุรกิจ การทดสอบ และ กลยุทธ์ในการสื่อสาร จึงมีความสำคัญยิ่งยวดต่อการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

เนื้อหาแต่ละส่วนต่อไปนี้ จะเริ่มต้นด้วยสรุปแนวทางการปฏิบัติ (Action Summary) ที่เป็นการสรุปประเด็นสำคัญของเนื้อหาในส่วนนั้น

<u>ส่วนที่ 2</u> แนวทางการจัดการที่พึงปฏิบัติ

2.1 ความรับผิดชอบของคณะกรรมการและผู้บริหารระดับสูง

สรุปแนวทางการปฏิบัติ

คณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงินมีภาระความรับผิดชอบ ดังนี้

- กำหนดนโยบายสำหรับการบริหารและควบคุมความเสี่ยง
- จัดสรรให้มีทรัพยากรและบุคลากรที่เพียงพอในการพัฒนา BCP
- อนุมัติ BCP เป็นประจำทุกปี
- กำกับดูแลให้มีการปรับ BCP ให้เป็นปัจจุบัน รวมทั้งจัดให้มีการฝึกอบรมพนักงานให้มีความเข้าใจและตระหนักถึงบทบาทและหน้าที่ของตนในการปฏิบัติตามแผน
- สอบทานผลการทดสอบ BCP

คณะกรรมการและผู้บริหารระดับสูงมีภาระความรับผิดชอบในการระบุ ประเมิน จัดลำดับความสำคัญ จัดการ และควบคุมความเสี่ยง โดยควรให้ความมั่นใจได้ว่ามีการจัดสรรทรัพยากรอย่างเหมาะสมต่อการพัฒนา บำรุงรักษา และการทดสอบแผน นอกจากนั้น คณะกรรมการมีความรับผิดชอบในการกำหนดนโยบาย จัดลำดับความสำคัญของธุรกิจ จัดสรรทรัพยากรและบุคลากรที่เพียงพอ ควบคุมดูแล อนุมัติ BCP สอบทานผลการทดสอบ และการจัดให้มีการบำรุงรักษาแผนที่ใช้อยู่ในปัจจุบัน ความมีประสิทธิผลของการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องขึ้นอยู่กับความร่วมมือของผู้บริหารและความสามารถในการระบุชี้ชัดถึงปัจจัยที่เป็นตัวผลักดันให้กระบวนการทางธุรกิจในปัจจุบันดำเนินต่อไปได้ สถาบันการเงินแต่ละแห่งจำเป็นต้องประเมินสถานะและสภาพแวดล้อมของตนเพื่อให้สามารถจัดทำ BCP ที่มีความครอบคลุม

คณะกรรมการและผู้บริหารระดับสูงควรแต่งตั้งเจ้าหน้าที่ที่จะเข้าร่วมในการพัฒนา BCP การจัดสรรทรัพยากรที่เหมาะสมเป็นสิ่งท้าทายต่อการพัฒนาและการบำรุงรักษา BCP ของสถาบันการเงิน สถาบันการเงินขนาดใหญ่ที่มีความซับซ้อนในการดำเนินธุรกิจอาจต้องกำหนดฝ่ายงานที่ทำหน้าที่ในการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง พร้อมกับกำหนดทีมงานที่ประกอบด้วยเจ้าหน้าที่ประสานงานของฝ่ายงานต่าง ๆ สำหรับสถาบันขนาดเล็กซึ่งมีการ

ดำเนินงานไม่ซับซ้อน อาจแต่งตั้งพนักงานที่เหมาะสมเป็นผู้ประสานงานในการจัดทำแผนรองรับดำเนินธุรกิจอย่างต่อเนื่อง อย่างไรก็ตามคณะกรรมการและผู้บริหารระดับสูงจะต้องมีความเข้าใจในกระบวนการทางธุรกิจหลักและรับผิดชอบ ในการจัดทำแผนให้เป็นไปตามข้อกำหนดเกี่ยวกับกระบวนการทางธุรกิจในลักษณะที่มีความมั่นคงปลอดภัยและมีเสถียรภาพ

2.2 กระบวนการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

สรุปแนวทางการปฏิบัติ

กระบวนการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของสถาบันการเงิน ควรสะท้อนถึงเป้าหมาย ดังต่อไปนี้

- การวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องเป็นเรื่องเกี่ยวกับการรักษาธุรกิจให้ดำเนินการต่อไปได้ในช่วงที่เกิดเหตุการณ์ความเสียหาย และการทำให้การดำเนินธุรกิจกลับคืนสู่ภาวะปกติ

ดังนั้นการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องจึงไม่ใช่เป็นเพียงแค่การกู้ระบบการดำเนินงานทางเทคโนโลยีสารสนเทศเท่านั้น

- กระบวนการวางแผนควรดำเนินการในลักษณะครอบคลุมทั้งองค์กร
- การวิเคราะห์ผลกระทบต่อธุรกิจและการประเมินความเสี่ยงอย่างครอบคลุมครบถ้วนเป็นพื้นฐานสำคัญของการมี BCP ที่มีประสิทธิภาพ
- BCP ที่มีประสิทธิภาพสามารถประเมินได้ด้วยการทดสอบหรือทดลองปฏิบัติงานจริงกับระบบงาน
- ควรดำเนินการให้มีการตรวจสอบ BCP และผลการทดสอบ BCP อย่างเป็นอิสระและสอบทานโดยคณะกรรมการ
- BCP ควรได้รับการปรับให้ทันสมัยอยู่เสมอเพื่อที่จะสอดคล้องและสามารถรองรับการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นในสถาบันการเงินหรือผู้ให้บริการได้

สถาบันการเงินควรวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องในลักษณะครอบคลุมทั้งองค์กร โดยพิจารณาให้ครอบคลุมเรื่องสำคัญต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจ ซึ่งไม่ใช่จำกัดอยู่เพียงการกู้ระบบเทคโนโลยีสารสนเทศและการให้บริการให้กลับมาใช้งานได้หรือ

การดำเนินการให้มีข้อมูลอยู่ในรูปอิเล็กทรอนิกส์เท่านั้น เนื่องจากการดำเนินการเพียงเท่านี้ยังไม่เพียงพอที่จะทำให้องค์กร กลับมาดำเนินธุรกิจตามปกติได้ หาก BCP ไม่ครอบคลุมถึงเรื่องสำคัญ ๆ ที่ใช้ในการดำเนินธุรกิจ เช่นบุคลากร สถานที่ทำงานได้ครบถ้วนแล้ว สถาบันการเงินก็อาจจะไม่สามารถดำเนินธุรกิจในการให้บริการลูกค้าได้ถึงระดับที่น่าพอใจ สำหรับสถาบันการเงินที่ใช้บริการจากภายนอก เช่น การประมวลผล หรือบริการเทคโนโลยีสารสนเทศอื่น ก็ยังคงต้องมี BCP สำหรับอุปกรณ์และกระบวนการปฏิบัติงาน ที่อยู่ภายใต้การควบคุมดูแลของผู้ให้บริการจากภายนอกด้วย

สถาบันการเงินควรตระหนักถึงบทบาทของตนในการดำเนินธุรกิจที่เกี่ยวข้องกับตลาดการเงิน เช่น ระบบการชำระเงินระหว่างธนาคาร ระบบการชำระรายการและการหักบัญชี ซึ่งหากการให้บริการขององค์กรเหล่านั้นประสบปัญหา ก็อาจส่งผลกระทบอย่างมีนัยสำคัญต่อความน่าเชื่อถือต่อตลาดการเงินหลัก ๆ องค์กรสมาชิกของ FFIEC สนับสนุนให้สถาบันการเงินทุกแห่งดำเนินงานร่วมกับองค์กรที่พึ่งพาอาศัยกันในการประสานงานพัฒนาและทดสอบ BCP โดยเฉพาะอย่างยิ่งสถาบันการเงินที่มีบทบาทสำคัญในตลาดการเงินจะต้องมีการวางแผนและการทดสอบร่วมกับผู้ที่เกี่ยวข้องในระบบ ทั้งนี้ ตลาดการเงินหลัก ๆ ได้แก่ ตลาดเงิน ตลาดอัตราแลกเปลี่ยนเงินตราต่างประเทศ ตลาดตราสารหนี้ภาครัฐและเอกชน

องค์กรที่จะถือได้ว่ามีบทบาทสำคัญต่อตลาดการเงินหลัก คือองค์กรที่มีขนาดและปริมาณการซื้อขายมากเพียงพอในระดับที่หากองค์กรเหล่านั้นประสบปัญหาไม่สามารถทำธุรกรรมเสร็จสิ้นภายในสิ้นวัน ก็อาจทำให้เกิดความเสี่ยงต่อระบบได้ ซึ่งองค์กรสมาชิกของ FFIEC เชื่อว่าสถาบันการเงินหลายแห่งจะมีบทบาทที่สำคัญอย่างน้อย 1 อย่างในตลาดการเงินที่สำคัญตลาดใดตลาดหนึ่ง และองค์กรสมาชิกบางแห่งของ FFIEC กำลังพิจารณาถึงประโยชน์ของการมีแนวทางเพิ่มเติมสำหรับกำหนดบทบาทในตลาดการเงินขององค์กร

ถึงแม้ว่าสถาบันการเงินไม่ได้เกี่ยวข้องกับตลาดการเงินหลัก ๆ โดยตรง แต่เป็นผู้ให้บริการทางการเงิน หรือให้บริการสนับสนุนการทำธุรกรรมในตลาดการเงินที่สำคัญต่อภาคการเงินของประเทศหรือภูมิภาค ก็ยังควรที่จะมี BCP และมีความสามารถในการกู้ธุรกิจกลับคืนสู่ภาวะปกติ โดยให้มีความเหมาะสมกับบทบาทของตน สถาบันการเงินขนาดเล็กที่การดำเนินงานไม่มีความซับซ้อนอาจไม่ จำเป็นต้องพัฒนาแผนเต็มรูปแบบ แต่ก็ต้องจัดให้มีการทดสอบที่เหมาะสมและเพียงพอเป็นประจำ

ผู้บริหารควรปรับแผน BCP ให้ทันสมัยเป็นปัจจุบันสอดคล้องกับการเปลี่ยนแปลงของกระบวนการทางธุรกิจ ตัวอย่างเช่น สถาบันการเงินไม่ว่าจะขนาดใหญ่หรือขนาดเล็ก ที่ใช้ระบบเครือข่ายแบบกระจายศูนย์ในการดำเนินธุรกิจจำเป็นต้องมีการนำโปรแกรมระบบงานที่สำคัญลงในเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (Desktop Computer) ซึ่งระบบเครือข่ายลักษณะนี้ช่วยให้การปฏิบัติงานที่สาขามีความคล่องตัวมากยิ่งขึ้น แต่นั่นก็หมายความว่า ผู้ใช้ระบบ (end-users) ควรดูแลปรับปรุง BCP ให้สอดคล้องกับกระบวนการทางธุรกิจปัจจุบันและการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นอย่างมีนัยสำคัญ ความก้าวหน้าทางเทคโนโลยีที่ทำให้การประมวลผลทำได้รวดเร็วและมีประสิทธิภาพมากขึ้น เป็นผลให้ช่วยลดเวลาในการกู้ระบบด้วย เพื่อที่สถาบันการเงินจะสามารถตอบสนองความต้องการของลูกค้าและมีความได้เปรียบในการแข่งขัน จึงได้มีความพยายามหาแนวทางลดระยะเวลาในการกู้ระบบให้สั้นลง รวมทั้งออกแบบกระบวนการทางธุรกิจให้ครอบคลุมแนวทางการกู้เทคโนโลยีกลับคืนสู่ภาวะปกติด้วย ความก้าวหน้าทางเทคโนโลยีดังกล่าว ทำให้การวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องในระดับภาพรวมทั้งองค์กรมีความสำคัญเพิ่มขึ้น

องค์กรสมาชิกของ FFIEC สนับสนุนให้สถาบันการเงินจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องที่มุ่งเน้นกระบวนการปฏิบัติงานเป็นหลัก ซึ่งเกี่ยวข้องกับสิ่งต่อไปนี้

1. การวิเคราะห์ผลกระทบต่อธุรกิจ
2. การประเมินความเสี่ยง
3. การบริหารความเสี่ยง
4. การติดตามดูแลความเสี่ยง

กรอบงานนี้สามารถนำไปใช้กับสถาบันการเงินได้ทุกขนาด การวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องควรมุ่งเน้นที่ธุรกิจหลักทั้งหมดที่จำเป็นต้องทำให้กลับคืนสู่ภาวะปกติ แผนฉุกเฉินทางด้านเทคโนโลยีสารสนเทศจะไม่ใช่ หัวใจของ BCP อีกต่อไป แต่จะเป็นเพียงส่วนสำคัญส่วนหนึ่งของกระบวนการจัดทำแผนในลักษณะภาพรวมทั้งองค์กร ดังนั้นการสอบทานกระบวนการของแต่ละธุรกิจหลักควรครอบคลุมเรื่องเทคโนโลยีที่ใช้สนับสนุนการดำเนินงานของส่วนธุรกิจนั้นด้วย

2.2.1 การวิเคราะห์ผลกระทบต่อธุรกิจ

สรุปแนวทางการปฏิบัติ

การวิเคราะห์ผลกระทบต่อธุรกิจเป็นขั้นตอนแรกของการพัฒนา BCP ซึ่งประกอบด้วย

- การระบุถึงผลกระทบของเหตุการณ์ที่ไม่สามารถควบคุมได้และไม่มีลักษณะเฉพาะอย่างใดอย่างหนึ่ง ที่ส่งผลกระทบต่อกระบวนการทางธุรกิจและลูกค้าของสถาบันการเงิน
- การพิจารณาผลกระทบที่มีถึงทุกฝ่ายงานและหน้าที่งาน มิใช่เพียงแค่งานประมวลผลข้อมูลเท่านั้น
- การกำหนดระดับการยอมรับได้ของระยะเวลาสูงสุดที่ระบบเทคโนโลยีสารสนเทศหยุดทำงาน ระดับความเสียหายของข้อมูล ระบบปฏิบัติการ และผลขาดทุนที่ยอมรับได้

ขั้นตอนแรกของการพัฒนา BCP คือการวิเคราะห์ผลกระทบต่อธุรกิจ จำนวนเวลาและทรัพยากรที่จำเป็นในการวิเคราะห์ผลกระทบต่อธุรกิจ ขึ้นอยู่กับขนาดและความซับซ้อนของสถาบันการเงิน ซึ่งการวิเคราะห์ผลกระทบต่อธุรกิจควรดำเนินการให้ครอบคลุมทุกหน้าที่งาน และทุกฝ่ายงาน มิใช่เพียงแค่งานประมวลผลข้อมูลเท่านั้น

ขั้นตอนของการวิเคราะห์ผลกระทบต่อธุรกิจ จะระบุถึงผลกระทบของเหตุการณ์ที่ไม่สามารถควบคุมได้และมีลักษณะไม่เฉพาะเจาะจงต่อกระบวนการทางธุรกิจของสถาบันการเงิน และควรมีการจัดทำประมาณการระยะเวลาสูงสุดที่เครื่องหรือระบบหยุดทำงาน เป้าหมายของการกู้ธุรกิจกลับคืนสู่ภาวะปกติ รายการค้างในระบบ และต้นทุนที่เกิดในช่วงที่เครื่องหรือระบบหยุดทำงาน ผู้บริหารควรมีการจัดลำดับของการกู้กระบวนการทางธุรกิจ ที่กำหนดเจ้าหน้าที่ เทคโนโลยีอุปกรณ์ระบบเครือข่าย สื่อสาร และข้อมูลที่ใช้ในการกู้ระบบ นอกจากนี้กระบวนการวิเคราะห์ผลกระทบต่อธุรกิจควรพิจารณาถึงผลกระทบด้านกฎหมาย และกฎระเบียบข้อบังคับของทางการ ได้แก่ การรักษาความลับและความพร้อมใช้งานของข้อมูลลูกค้า และการแจ้งหน่วยงานกำกับของทางการและลูกค้าให้ทราบเกี่ยวกับการโยกย้ายการดำเนินงาน

ผู้ที่รับผิดชอบในขั้นตอนนี้ควรพัฒนาแบบฟอร์มมาตรฐานพร้อมคำถามสำหรับการสัมภาษณ์ ที่สามารถใช้ได้กับทั้งองค์กร ซึ่งการใช้แบบสอบถามที่เป็นมาตรฐานเดียวกันนี้จะช่วยให้สามารถเปรียบเทียบผลที่ได้และทำการประเมินความต้องการเกี่ยวกับกระบวนการทางธุรกิจ

ของทั้งองค์กร นอกจากนั้นอาจมีการจัดลำดับกระบวนการทางธุรกิจเบื้องต้น ตามความสำคัญต่อการทำให้องค์กรบรรลุเป้าหมายกลยุทธ์และการรักษาความมั่นคงปลอดภัยและมีเสถียรภาพในการปฏิบัติงาน อย่างไรก็ตาม ควรมีการทบทวนการจัดลำดับทันทีที่มีการสร้างกระบวนการทางธุรกิจเพื่อตอบโต้เหตุการณ์จำลองของภัยคุกคามต่าง ๆ ในการพัฒนา BCP ด้วย

เมื่อได้มีการกำหนดถึงความต้องการที่สำคัญของสถาบันการเงินแล้ว ก็ควรทำการสอบทานหน้าที่งาน กระบวนการปฏิบัติงาน และบุคลากรของแต่ละฝ่าย ซึ่งแต่ละฝ่ายควรมีการจัดทำเอกสารระบุถึงหน้าที่ที่จะต้องปฏิบัติงานไว้อย่างชัดเจน ซึ่งควรพิจารณาตามคำถามต่อไปนี้

- อุปกรณ์พิเศษอะไรบ้างที่จำเป็นต้องใช้ และใช้อย่างไร
- ฝ่ายงานจะทำอย่างไรถ้าระบบคอมพิวเตอร์หลักขนาดใหญ่ ระบบเครือข่ายสื่อสาร หรือระบบอินเตอร์เน็ตไม่สามารถใช้งานได้
- มีจุดเสี่ยงที่อาจจะทำให้เกิดปัญหาหรือไม่ ส่งผลกระทบอย่างมีนัยสำคัญหรือไม่ อย่างไร
- มีความสัมพันธ์และการพึ่งพาหลัก ๆ อะไรบ้างจากการใช้บริการภายนอก
- จำนวนพนักงาน และขนาดพื้นที่ของสถานที่กู้ระบบที่สามารถประหยัดได้มากที่สุด
- แบบฟอร์มเฉพาะหรือวัสดุอุปกรณ์อะไรที่จำเป็นที่จะต้องมีอยู่ที่สถานที่กู้ระบบ
- อุปกรณ์เครือข่ายสื่อสารอะไรที่จำเป็นต้องมีติดตั้งที่สถานที่กู้ระบบ
- มีการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยที่สำคัญด้านใดบ้างที่ต้องจัดเตรียมไว้ล่วงหน้าก่อนดำเนินการกู้ระบบ
- ผลกระทบอะไรที่คาดว่าจะเกิดจากสถานที่กู้ระบบ ในกรณีที่ต้องรองรับหลายสายงานธุรกิจหรือหลายฝ่ายงาน
- มีการฝึกอบรมโดยสลับหน้าที่ต่าง ๆ ให้แก่พนักงาน และฝ่ายงานได้กำหนดหน้าที่หรือบทบาทแก่พนักงานเพื่อปฏิบัติงานทดแทนในกรณีที่พนักงานที่ได้รับมอบหมายให้รับผิดชอบโดยตรงไม่สามารถปฏิบัติหน้าที่ได้ หรือไม่
- มีการคำนึงถึงความรู้สึกและความจำเป็นในการใส่ใจต่อครอบครัวของพนักงานอย่างเพียงพอหรือไม่

2.2.2 การประเมินความเสี่ยง

สรุปแนวทางการปฏิบัติ

การประเมินความเสี่ยง เป็นขั้นตอนที่สองของการพัฒนา BCP ซึ่งครอบคลุมเรื่องดังต่อไปนี้

- การวิเคราะห์ภัยคุกคามจะต้องพิจารณาถึงผลกระทบต่อสถาบันการเงิน ลูกค้า และตลาดการเงินด้วย ไม่ใช่เพียงแค่พิจารณาลักษณะหรือรูปแบบของภัยคุกคามเท่านั้น
- การจัดลำดับเหตุการณ์ความเสียหายตามความรุนแรงและโอกาสที่จะเกิดขึ้น
- การวิเคราะห์เปรียบเทียบระหว่าง BCP ที่สถาบันการเงินใช้อยู่ในปัจจุบัน กับสิ่งที่ควรจะต้องดำเนินการเพื่อให้สามารถกู้ธุรกิจกลับคืนสู่ภาวะปกติ ภายในเวลาและเป็นไปตามเป้าหมายที่กำหนด

ขั้นตอนในการประเมินความเสี่ยงเป็นขั้นตอนที่สำคัญที่จะผลักดันให้การจัดทำ BCP ประสบผลสำเร็จ ถ้าเหตุการณ์จำลองของภัยคุกคามไม่สมเหตุสมผล ก็จะทำให้ BCP ไม่เพียงพอที่จะใช้งานได้ในระหว่างการประเมินความเสี่ยงนั้น ควรมีการทดสอบกระบวนการทางธุรกิจและสมมติฐานที่ใช้ในการวิเคราะห์ผลกระทบต่อธุรกิจในลักษณะการทดสอบภาวะวิกฤต ภายใต้เหตุการณ์จำลองรูปแบบต่าง ๆ ของภัยคุกคาม ซึ่งผลที่ได้จากการทดสอบจะทำให้สถาบันการเงินทราบว่ามีความจำเป็นต้องพัฒนา BCP โดยอาศัยการสนับสนุนด้านการเงินและบุคลากรหรือไม่

สถาบันการเงินควรกำหนดเหตุการณ์จำลองของภัยคุกคาม ที่มีความเป็นไปได้ที่จะเกิดขึ้นและอาจสร้างความเสียหายต่อกระบวนการทางธุรกิจตลอดจนถึงความสามารถในการตอบสนองความคาดหวังของบุคลากรภายในองค์กร หุ้นส่วนทางธุรกิจ และลูกค้า ภัยคุกคามอาจเกิดขึ้นได้ในหลายรูปแบบ เช่น การประสงค์ร้ายหรือกิจกรรมที่ก่อให้เกิดผลเสียหาย ภัยธรรมชาติ และภัยพิบัติทางเทคนิค สถาบันการเงินควรวิเคราะห์ภัยคุกคามโดยเน้นการพิจารณาไปที่ผลกระทบต่อสถาบันการเงินด้วย ไม่ใช่เพียงแต่พิจารณาลักษณะหรือรูปแบบของภัยคุกคามเท่านั้น ตัวอย่างเช่น เหตุการณ์จำลองของภัยคุกคาม อาจส่งผลกระทบต่อธุรกิจเฉพาะด้าน ระบบงานบางอย่าง สิ่งอำนวยความสะดวก สถานที่ หรือพื้นที่ตั้งบางส่วน นอกเหนือจากนั้นขนาดและความสำคัญของความเสียหายต่อธุรกิจ จะต้องพิจารณาเหตุการณ์จำลองของภัยคุกคามหลาย ๆ รูปแบบจากประสบการณ์ในอดีต และสภาพแวดล้อมและเหตุการณ์ที่เป็นไปได้ ถ้าเหตุการณ์จำลอง

ของภัยคุกคามไม่ครอบคลุมเพียงพอ ก็จะทำให้ BCP มีลักษณะพื้นฐานมากเกินไป และขาดขั้นตอนที่สมเหตุสมผลบางอย่างที่อาจจะเพิ่มความสามารถในการดำเนินการให้กระบวนการทางธุรกิจกลับคืนสู่ภาวะปกติจากเหตุการณ์ความเสียหายได้

เหตุการณ์จำลองของภัยคุกคาม จำเป็นต้องพิจารณาเรื่องผลกระทบของความเสียหายและโอกาสที่จะเกิดขึ้น ตั้งแต่ภัยที่มีโอกาสเกิดสูงแต่ส่งผลกระทบต่อธุรกิจต่ำ (เช่น ไฟตก) ไปจนถึงภัยที่มีโอกาสเกิดน้อยแต่ส่งผลกระทบต่อธุรกิจรุนแรง (เช่น พายุ การก่อการร้าย) อย่างไรก็ตามเป็นการยากที่สุดที่จะระบุภัยคุกคามที่ส่งผลกระทบต่อธุรกิจรุนแรงแต่มีโอกาสเกิดน้อย ซึ่งการประเมินความเสี่ยงจะช่วยให้ BCP มีความยืดหยุ่นและสามารถนำไปปรับใช้กับความเสียหายชนิดต่าง ๆ ที่อาจจะไม่ได้มีการพิจารณาไว้ตั้งแต่แรก

ในขั้นตอนนี้ สถาบันการเงินควรทำ Gap analysis คือวิธีการเปรียบเทียบชนิดของ BCP ที่จะทำให้การดำเนินธุรกิจกลับสู่ภาวะปกติ กับ BCP ที่สถาบันการเงินใช้อยู่ในปัจจุบัน ทั้งนี้ คณะกรรมการและผู้บริหารจะต้องให้ความสนใจในความเสี่ยงที่อาจเกิดจากความแตกต่างที่พบและควรนำมาพิจารณารวมในการพัฒนา BCP ด้วย

ในการประเมินความเสี่ยง ควรพิจารณาถึง

- ผลกระทบของความเสียหาย ต่อสถาบันการเงินและลูกค้า
- โอกาสการเกิดเหตุการณ์ โดยกำหนดเกณฑ์ในการพิจารณาขึ้นมา (จัดกลุ่มเป็น สูง กลาง ต่ำ)
- ความเสียหายที่อาจเกิดขึ้นจากแหล่งภายในและภายนอก ต่อการให้บริการเทคโนโลยีสารสนเทศ บุคลากร สิ่งอำนวยความสะดวกและผู้ให้บริการภายนอก
- ความปลอดภัยของเอกสารประมวลผลและข้อมูลสำคัญ
- ความเสียหายต่อธุรกิจในรูปแบบต่าง ๆ เช่น ภัยธรรมชาติ ภัยเกี่ยวกับเทคนิค หรือจากการกระทำของมนุษย์

ในการประเมินโอกาสของการเกิดเหตุการณ์ความเสียหาย สถาบันการเงินและผู้ให้บริการทางเทคโนโลยี ควรพิจารณาสถานที่ตั้งของสิ่งอำนวยความสะดวกและความเสี่ยงต่อภัยธรรมชาติ (เช่น สถานที่ตั้งอยู่ใกล้พื้นที่น้ำท่วม) การอยู่ใกล้สาธารณูปโภคสำคัญ (เช่น โรงงานไฟฟ้า โรงงานนิวเคลียร์ สนามบิน ถนนทางหลวง ทางรถไฟ เป็นต้น)

การประเมินความเสี่ยงควรครอบคลุมทั้งสถานที่ตั้งของสำนักงานและสิ่งอำนวยความสะดวกทั้งหมดของสถาบันการเงินและผู้ให้บริการ ควรมีการพิจารณาเหตุการณ์จำลองของภัยคุกคามที่ เลวร้ายที่สุด เช่น อุปกรณ์ถูกทำลาย และการสูญเสียพนักงาน กล่าวโดยสรุปคือ ขั้นตอนนี้สถาบันการเงินต้องจัดลำดับกระบวนการทางธุรกิจและคาดการณ์ถึงความเสียหายต่อธุรกิจที่อาจเกิดขึ้นภายใต้เหตุการณ์จำลองของภัยคุกคามต่าง ๆ

2.2.3 การบริหารความเสี่ยง

การจัดทำแผนรองรับการดำเนินงานธุรกิจอย่างต่อเนื่อง

สรุปแนวทางการปฏิบัติ

การบริหารความเสี่ยง คือการพัฒนา BCP ในภาพรวมทั้งองค์กร โดยการจัดทำเป็นลายลักษณ์อักษร ซึ่งสถาบันการเงินควรจะมั่นใจว่า BCP ครอบคลุมประเด็นต่อไปนี้

- จัดทำเป็นลายลักษณ์อักษรและเผยแพร่เพื่อให้กลุ่มบุคคลต่าง ๆ นำไปปฏิบัติได้ในเวลาที่เหมาะสม
- ระบุเงื่อนไขที่ต้องนำแผนไปปฏิบัติโดยเร็ว
- ระบุชัดเจนเกี่ยวกับขั้นตอนที่ต้องดำเนินการในระหว่างที่เกิดความเสียหาย
- มีความยืดหยุ่นที่จะรับมือหรือตอบโต้กับภัยคุกคามที่อาจเกิดขึ้นโดยไม่คาดคิดและการเปลี่ยนแปลงเงื่อนไขภายในบางอย่าง
- มุ่งเน้นถึงการทำอย่างไรให้ธุรกิจดำเนินการต่อไปได้ในช่วงที่อุปกรณ์หรืองานได้รับความเสียหายมากกว่าที่จะมุ่งเน้นไปที่การวิเคราะห์ลักษณะหรือรูปแบบของความเสียหาย
- มีประสิทธิผลต่อการลดปัญหาการให้บริการและความสูญเสียทางการเงิน

หลังจากการวิเคราะห์ผลกระทบต่อธุรกิจและการประเมินความเสี่ยงแล้ว ผู้บริหารหรือตัวแทนที่ได้รับมอบหมาย ควรเริ่มร่าง BCP ซึ่งประกอบด้วยกลยุทธ์และขั้นตอนการปฏิบัติงานในการทำให้ธุรกิจสามารถดำเนินต่อไปได้ในช่วงที่ธุรกิจได้รับความเสียหายและกลับคืนสู่ภาวะปกติภายหลังจากนั้น รวมทั้งวิธีปฏิบัติในการจัดลำดับของงาน บริการ และกระบวนการทางธุรกิจตามความสำคัญ ลักษณะของ BCP ที่ดี ควรอธิบายในรายละเอียดถึงประเภทของเหตุการณ์ที่จะนำไปสู่การประกาศเกี่ยวกับความเสียหายและกระบวนการขอใช้ BCP นอกจากนั้น ควรอธิบาย

ถึงหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงานของทีมฉุกเฉิน ควรมีหมายเลขโทรศัพท์ใช้ติดต่อเจ้าหน้าที่หลัก BCP ควรอธิบายในรายละเอียดเกี่ยวกับขั้นตอนการปฏิบัติงานในการทำให้การดำเนินธุรกิจแต่ละส่วนกลับคืนสู่ภาวะปกติและควรร่างแผนในลักษณะที่เจ้าหน้าที่ของแต่ละส่วนงานสามารถนำไปปฏิบัติได้ในเวลาที่เหมาะสม

จากที่กล่าวมาข้างต้น BCP เป็นแผนงานที่กว้างกว่าการกู้ระบบเทคโนโลยีสารสนเทศ โดยรวมถึงการทำให้การปฏิบัติงานทั้งหมดของธุรกิจกลับสู่ภาวะปกติ จึงควรมีความยืดหยุ่นที่จะตอบสนองต่อการเปลี่ยนแปลงของปัจจัยภายในและสภาวะแวดล้อมภายนอก รวมทั้งภัยคุกคามรูปแบบใหม่ที่อาจจะเกิดขึ้น แทนที่จะพัฒนาแผนตามเหตุการณ์เฉพาะเรื่อง (เช่น ไฟไหม้ พายุ) และจะมีประสิทธิผลมากขึ้น ถ้าจัดทำขึ้นให้รองรับเหตุการณ์จำลองรูปแบบต่าง ๆ และผลลัพธ์ที่ต้องการ BCP ควรอธิบายขั้นตอนที่ต้องดำเนินการเมื่อเกิดเหตุฉุกเฉินเพื่อลดความเสียหายต่อธุรกิจ รวมทั้งกิจกรรมที่จำเป็นต่อการทำให้ระบบกลับคืนสู่ภาวะปกติ ด้วยเหตุนี้ การจัดทำ BCP ควรมุ่งเน้นเรื่องการรักษาธุรกิจให้ดำเนินต่อไปในช่วงที่เกิดความเสียหายและการทำให้ธุรกิจกลับคืนสู่ภาวะปกติเหตุการณ์จำลองควรครอบคลุมเหตุการณ์ดังต่อไปนี้

- บุคลากรหลักไม่อยู่
- ไม่สามารถเข้าถึงอาคาร สิ่งอำนวยความสะดวกในเขตพื้นที่ได้
- อุปกรณ์ทำงานไม่ถูกต้อง (Hardware ระบบการสื่อสาร อุปกรณ์ที่ใช้ในการดำเนินงาน)
- ไม่สามารถใช้ Software และข้อมูลได้
- ไม่สามารถได้รับการให้บริการจากผู้ให้บริการได้
- สิ่งอำนวยความสะดวกใช้การไม่ได้ (เช่น ไฟฟ้า ระบบสื่อสาร)
- ไม่มีเอกสารและข้อมูลสำคัญ

สถาบันการเงินควรระมัดระวังในการพิจารณาสมมติฐานของ BCP โดยไม่ควรตั้งสมมติฐานว่าความเสียหายจะเกิดขึ้นเฉพาะภายในอาคารหรือพื้นที่จำกัด หรือจะสามารถเข้าใช้อุปกรณ์ สิ่งอำนวยความสะดวกต่าง ๆ ได้ หรือสามารถติดต่อเจ้าหน้าที่หลักได้ทันที รวมทั้งไม่ควรตั้งสมมติฐานว่าระบบการขนส่งต่าง ๆ จะมีความสะดวกเหมือนในภาวะปกติ

BCP ประกอบด้วยองค์ประกอบมากมาย ทั้งภายในและภายนอกสถาบันการเงิน การใช้ BCP และการรักษาให้ธุรกิจยังคงดำเนินต่อไปในช่วงที่เกิดความเสียหาย จะขึ้นกับความสำเร็จของหลายองค์ประกอบด้วยกัน BCP ในภาพรวมทั้งองค์กรอาจด้อยประสิทธิผลลงได้ถ้า

มีจุดอ่อนในองค์ประกอบใดองค์ประกอบหนึ่ง BCP ที่มีประสิทธิผลจะเป็นการประสานองค์ประกอบย่อย ๆ เข้าด้วยกัน การระบุกระบวนการที่สำคัญ หรือการพึ่งพาต่าง ๆ ของระบบและการลดความเสี่ยงที่เกิดจากการพึ่งพาอาศัยกัน (มีรายละเอียดในภาคผนวก ค)

โดยปกติแล้ว หน่วยงานหรือผู้ประสานงานในการจัดทำ BCP จะทำหน้าที่ระบุความเสี่ยงและพัฒนากลยุทธ์ในการลดความเสี่ยงของส่วนธุรกิจต่าง ๆ การพึ่งพาอาศัยกันภายในองค์กร เกิดจากสายงานธุรกิจที่ต้องพึ่งพากัน การเชื่อมโยงของระบบสื่อสาร และ/หรือการใช้ทรัพยากรร่วมกัน (เช่น งานพิมพ์ ระบบของ E-Mail) การพึ่งพาอาศัยกันภายนอกองค์กร ที่อาจส่งผลกระทบทางลบต่อ BCP ประกอบด้วย ผู้ให้บริการด้านการสื่อสาร ผู้ให้บริการต่าง ๆ ลูกค้า หุ้นส่วนทางธุรกิจ และผู้จัดหาสินค้าหรือบริการ (รายละเอียดเกี่ยวกับส่วนประกอบของ BCP อยู่ในภาคผนวก ง)

2.2.4 นโยบาย มาตรฐานและกระบวนการปฏิบัติงานอื่น

สรุปแนวทางการปฏิบัติ

นอกเหนือจากการจัดทำ BCP แล้ว นโยบายอื่น ๆ ของสถาบันการเงินควรคำนึงถึงการวางแผนเพื่อให้ธุรกิจสามารถดำเนินงานได้อย่างต่อเนื่องด้วย นโยบายเหล่านี้ได้แก่

- การพัฒนาระบบงานและโปรแกรม และการบริหารโครงการ
- การควบคุมการเปลี่ยนแปลง
- ความสอดคล้องกันของข้อมูล
- แผนการฝึกอบรมพนักงานและการสื่อสาร
- การประกันภัย
- การประชาสัมพันธ์ภายนอก (รัฐบาล สื่อ และประชาชน)
- การรักษาความปลอดภัย

นอกเหนือจากการจัดทำ BCP นโยบาย มาตรฐาน และการปฏิบัติงานต่าง ๆ เช่น การพัฒนาระบบงานและโปรแกรม การควบคุมการเปลี่ยนแปลง และความสอดคล้องกันของข้อมูล ควรพิจารณาถึงความต่อเนื่องและความพร้อมใช้งาน

การพัฒนาระบบงานและโปรแกรม และการบริหารโครงการ

ในการพัฒนาระบบงานและโปรแกรม ผู้บริหารควรรวมประเด็นเรื่องการดำเนินธุรกิจอย่างต่อเนื่องเข้าไว้เป็นส่วนหนึ่งในแผนงานของโครงการด้วย การประเมินความต้องการของการดำเนินธุรกิจอย่างต่อเนื่องในกระบวนการพัฒนาระบบงานและโปรแกรมนั้น เป็นการเตรียมการล่วงหน้า เมื่อสถาบันการเงินอยู่ระหว่างการจัดหาหรือพัฒนาระบบงานใหม่ และจะช่วยให้ระบบงานใหม่มีความแข็งแกร่งมากขึ้นซึ่งหากเกิดเหตุการณ์ความเสียหาย ก็จะทำให้ธุรกิจสามารถดำเนินการต่อได้โดยง่าย

ในการพัฒนาและจัดหาระบบงานใหม่ มาตรฐานการพัฒนาระบบงานและโปรแกรม และแผนงานของโครงการ อย่างน้อยควรครอบคลุมเรื่องดังต่อไปนี้

- สิ่งจำเป็นของหน่วยงานธุรกิจสำหรับทางเลือกต่าง ๆ เพื่อให้ธุรกิจกลับคืนสู่ภาวะปกติ
- ข้อมูลสำรองและการจัดเก็บข้อมูลในระบบเทคโนโลยีสารสนเทศ
- ข้อกำหนดเกี่ยวกับ Hardware และ Software ที่ศูนย์คอมพิวเตอร์สำรอง
- BCP และการดูแลรักษาเอกสารให้เป็นปัจจุบัน
- การทดสอบการกู้ธุรกิจกลับคืนสู่ภาวะปกติ
- การจัดการด้านบุคลากรและอุปกรณ์ต่าง ๆ

การควบคุมการเปลี่ยนแปลง

นโยบายและขั้นตอนปฏิบัติในการบริหารและควบคุมการเปลี่ยนแปลงควรครอบคลุมการเปลี่ยนแปลงสภาพแวดล้อมการปฏิบัติงาน ดังเช่นการเปลี่ยนแปลงโปรแกรมจะต้องผ่านการอนุมัติและจัดทำเอกสารประกอบ ประเด็นการดำเนินธุรกิจอย่างต่อเนื่องควรรวมอยู่ในกระบวนการควบคุมการเปลี่ยนแปลงและในขั้นตอนการนำไปปฏิบัติ เมื่อใดที่มีการเปลี่ยนแปลงในโปรแกรมระบบงาน หรือระบบปฏิบัติการ หรือโปรแกรมอรรถประโยชน์ที่ใช้งานจริง สถาบันการเงินควรมีวิธีการที่มั่นใจได้ว่าชุดสำรองต่าง ๆ ได้ปรับให้เป็นปัจจุบัน ภายใต้สภาพแวดล้อมใหม่ที่เปลี่ยนแปลงไปด้วย นอกจากนั้น ระบบงานใหม่หรือระบบงานที่มีการเปลี่ยนแปลงและมีผลกระทบต่อเครื่อง Hardware ศักยภาพของเครื่องหรือเทคโนโลยีอื่น ๆ ผู้บริหารควรให้ความ

มั่นใจได้ว่า BCP จะได้รับการปรับปรุงและศูนย์คอมพิวเตอร์สำรองจะสามารถรองรับสภาพแวดล้อมใหม่ที่ใช้งานจริงได้

ความสอดคล้องกันของข้อมูล

ความสอดคล้องกันของข้อมูลเป็นสิ่งท้าทายต่อสภาพแวดล้อมที่มีลักษณะ Active/Backup สถาบันการเงินที่มีขนาดใหญ่และมีความซับซ้อน (เช่น มีช่วงเวลาของการดำเนินงานหยุดชะงักที่ยอมรับได้ในระดับต่ำ ปริมาณรายการธุรกรรมมาก สถานที่ตั้งศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองอยู่ไกลกัน) ก็ยิ่งยากต่อการดำเนินการให้ข้อมูลมีความสอดคล้องตรงกัน ถ้าข้อมูลชุดสำรองจัดทำขึ้น ณ เวลาใกล้สิ้นวันและมีเหตุการณ์ความเสียหายเกิดขึ้นในช่วงสายของวันถัดมา รายการทุกรายการที่เกิดขึ้นหลังจากที่ได้สำรองข้อมูลจะต้องถูกสร้างขึ้นมาใหม่ (อาจด้วยวิธี Manual) เพื่อที่จะทำให้ข้อมูลที่ศูนย์คอมพิวเตอร์สำรองและที่ศูนย์คอมพิวเตอร์หลักสอดคล้องและตรงกัน

การจัดการและการทดสอบเพื่อรองรับกับเหตุการณ์ที่ไม่แน่นอน เป็นสิ่งสำคัญต่อการสร้างความมั่นใจว่า สภาพแวดล้อมของการกู้ระบบมีความสอดคล้องและตรงกันกับสภาพแวดล้อมของการทำงานหลัก เช่น Software ที่ใช้เป็นรุ่นปัจจุบัน มีการเชื่อมต่อและมีการทดสอบการเชื่อมต่อเหล่านั้น ใช้อุปกรณ์สื่อสารที่สามารถใช้ด้วยกันได้ เป็นต้น ถ้าสถานที่ตั้งระบบงาน ส่วนธุรกิจที่พึ่งพาอาศัยกัน ไม่สอดคล้องกัน ก็จะมีความเป็นไปได้ที่การกู้ระบบที่ศูนย์คอมพิวเตอร์สำรองอาจประสบปัญหาอย่างมี นัยสำคัญ อย่างไรก็ตามการควบคุมการเปลี่ยนแปลงการสำรองข้อมูล และการทดสอบที่เพียงพอ เหมาะสม จะช่วยแก้ไขปัญหาดังกล่าวได้ นอกจากนั้นผู้บริหารควรให้ความมั่นใจว่าอุปกรณ์ต่าง ๆ ที่ใช้ในการสำรองจะสามารถรองรับการประมวลผลรายการได้ในเวลาที่เหมาะสมเมื่อเกิดเหตุการณ์ความเสียหายขึ้นที่ศูนย์คอมพิวเตอร์หลัก

การวางแผนฝึกอบรมพนักงานและการสื่อสาร

สถาบันการเงินควรจัดให้มีการฝึกอบรมเกี่ยวกับการดำเนินธุรกิจอย่างต่อเนื่องให้แก่พนักงาน เพื่อมั่นใจว่าพนักงานทุกคนทราบถึงความรับผิดชอบของตนหากเกิดเหตุการณ์ความเสียหายขึ้น พนักงานหลักควรจะเข้าร่วมในกระบวนการพัฒนางานการดำเนินธุรกิจอย่าง

ต่อเนื่องและได้รับการฝึกปฏิบัติเป็นประจำ แผนการฝึกอบรมควรครอบคลุมแผนการฝึกอบรมทั้งองค์กรและแผนการฝึกอบรมของแต่ละส่วนธุรกิจ พนักงานควรทราบเงื่อนไขในการใช้ BCP ไม่ว่าจะเป็นการใช้แผนบางส่วนหรือทั้งหมด นอกจากนั้นควรทราบว่าใครเป็นผู้รับผิดชอบในการใช้ BCP ของส่วนธุรกิจและขององค์กร และสิ่งที่ต้องดำเนินการหากพนักงานหลักไม่สามารถปฏิบัติงานได้ในช่วงที่เกิดเหตุการณ์ความเสียหาย อีกทั้งควรจัดให้มีการฝึกอบรมในลักษณะไขว้กันเพื่อเตรียมความพร้อมในกรณีที่พนักงานหลักไม่สามารถอยู่ปฏิบัติงานได้ สถาบันการเงินควรจัดทำแผนตารางเวลาการฝึกอบรมและปรับปรุงแผนดังกล่าวตามการเปลี่ยนแปลงที่เกิดขึ้น

การวางแผนการสื่อสารควรระบุช่องทางการสื่อสารต่าง ๆ ในช่วงที่เกิดเหตุการณ์ความเสียหายเช่น วิทยุติดตามตัว โทรศัพท์มือถือ E-Mail วิทยุสื่อสาร เป็นต้น ควรแจกรายชื่อพร้อมหมายเลขโทรศัพท์ E-Mail Address และที่อยู่ที่ติดต่อได้ให้แก่พนักงานเพื่อใช้ติดต่อในภาวะฉุกเฉิน ซึ่งรายชื่อควรแสดงหมายเลขโทรศัพท์มากกว่า 1 หมายเลข สำหรับเผื่อไว้ในกรณีที่ระบบโทรศัพท์บางระบบใช้งานไม่ได้ นอกจากนั้น ควรจัดทำรายชื่อพร้อมหมายเลขโทรศัพท์ติดต่อผู้ให้บริการหน่วยบริการฉุกเฉิน การขนส่ง และหน่วยงานราชการ วิธีการแจกจ่ายข้อมูลไปให้พนักงานอาจทำได้ในลักษณะทำเป็นบัตรเล็ก ๆ สำหรับพกติดกระเป๋าเงิน ประกาศใน Internet หรือจัดทำผังเชื่อมโยงรายชื่อ (Call Tree) นอกจากนั้นสถาบันการเงินควรจัดสถานที่สำหรับการรายงานหรือรับโทรศัพท์ในช่วงที่เกิดเหตุการณ์ความเสียหายด้วย

สถาบันการเงินควรพัฒนาแผนการแจ้งลูกค้า ผู้ให้บริการ และหน่วยงานราชการให้ทราบถึงวิธีที่จะติดต่อสถาบันการเงินหากช่องทางการติดต่อปกติไม่สามารถใช้งานได้ แผนงานควรระบุรายชื่อเจ้าหน้าที่ที่ได้รับมอบหมายให้ติดต่อกับสื่อมวลชน หน่วยงานราชการ ผู้ให้บริการและบริษัทอื่น ๆ รวมทั้งประเภทของข้อมูลที่จะเปิดเผยได้

การประกันภัย

การประกันภัย มักใช้ในการชดเชยความสูญเสียในส่วนที่ไม่สามารถป้องกันได้ โดยทั่วไปการประกันภัยจะให้ความคุ้มครองความเสี่ยงที่ไม่สามารถควบคุมได้ซึ่งอาจนำไปสู่ความเสียหายในระดับรุนแรงและผลขาดทุนอย่างมหาศาล การตัดสินใจทำประกันภัยควรพิจารณาจากความน่าจะเป็นและระดับความเสียหายที่ระบุในระหว่างการวิเคราะห์ผลกระทบต่อธุรกิจ สถาบันการเงินควรพิจารณากำหนดขนาดความเสี่ยงที่เกิดจากเหตุการณ์ความเสียหายรูปแบบต่าง ๆ และ

สอบทานทางเลือกของ ประกันภัยที่จะให้ความคุ้มครองอย่างเหมาะสม ผู้บริหารควรทราบวงเงินและความคุ้มครองที่กำหนดในนโยบายการทำประกันภัยเพื่อที่จะแน่ใจว่าความคุ้มครองมีความเหมาะสมกับลักษณะความเสี่ยงของสถาบันการเงิน สถาบันการเงินควรจัดให้มีการสอบทานเกี่ยวกับการประกันภัยทุกปีโดยคำนึงถึงเรื่องความสมเหตุสมผลของระดับและประเภทของความคุ้มครอง และความสอดคล้องกับข้อกำหนดทางกฎหมาย และข้อกำหนดของคณะกรรมการและผู้บริหาร นอกจากนั้นสถาบันการเงินควรสร้างและเก็บรักษาทะเบียนทรัพย์สินอุปกรณ์ Hardware และ Software ไว้ในสถานที่แยกต่างหากที่มีความปลอดภัย เพื่อสามารถนำมาใช้ในกระบวนการเรียกร้องค่าสินไหมทดแทน

สถาบันการเงินควรทราบข้อจำกัดของประกันภัย การประกันภัยสามารถชดใช้ความเสียหายให้แก่สถาบันการเงินในบางส่วนหรือทั้งหมดของความเสียหายที่เกิดจากความหายนะ หรือ เหตุการณ์ที่สำคัญ อย่างไรก็ตามการประกันภัยไม่สามารถใช้ทดแทน BCP ได้ เนื่องจากวัตถุประสงค์หลักของการประกันภัยไม่ใช่เพื่อการทำให้ธุรกิจกลับคืนสู่ภาวะปกติ ตัวอย่างเช่น การประกันภัยไม่สามารถชดใช้ชื่อเสียงของสถาบันที่เสียไปได้

หน่วยงานรัฐบาลและชุมชน

สถาบันการเงินอาจจำเป็นต้องประสานงานกับชุมชน หน่วยงานราชการและแหล่งข่าว เพื่อให้การใช้ BCP ประสบผลสำเร็จ โดยแนวทางที่ดีที่สุด ควรจัดให้มีการประสานงานในขั้นตอนวางแผนหรือขั้นตอนการทดสอบแผน โดยเฉพาะในกรณีที่เหตุการณ์ความเสียหายที่เกิดขึ้นในวงกว้างที่ส่ง ผลกระทบต่อการดำเนินงานของสถาบันการเงิน นอกจากนั้นในระหว่างการประเมินความเสี่ยง สถาบันการเงินควรติดต่อหน่วยงานราชการ เพื่อสอบถามเกี่ยวกับภัยต่าง ๆ ที่อาจเกิดขึ้นในเขตพื้นที่ ในขั้นตอนการกู้ธุรกิจกลับคืนสู่ภาวะปกติ ควรมีการประสานงานกับองค์กรที่ให้บริการสาธารณูปโภคต่าง ๆ รวมถึงการขนส่ง เพื่อให้แน่ใจว่าจะสามารถกู้ธุรกิจกลับคืนมาสู่ภาวะปกติได้ทันเวลา นอกจากนี้อาจมีการประสานงานกับเจ้าหน้าที่ตำรวจ กองดับเพลิง ทั้งนี้ขึ้นอยู่กับลักษณะเหตุการณ์ความเสียหายที่เกิดขึ้น

2.2.5 การติดตามดูแลความเสี่ยง

สรุปแนวทางการปฏิบัติ

การติดตามดูแลความเสี่ยงเป็นขั้นตอนสุดท้ายของการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง โดยเป็นการดำเนินการให้มั่นใจได้ว่า BCP ของสถาบันการเงินจะสามารถนำไปใช้งานได้โดยติดตามผ่านช่องทาง ดังนี้

- การทดสอบ BCP อย่างน้อยปีละ 1 ครั้ง
- การสอบทานและตรวจสอบ BCP อย่างเป็นอิสระ
- การปรับ BCP ให้เป็นปัจจุบันตามการเปลี่ยนแปลงของบุคลากร และสภาพแวดล้อมทั้งภายในและภายนอกสถาบันการเงิน

การติดตามความเสี่ยง เป็นการสร้างความมั่นใจว่า BCP จะสามารถนำไปใช้งานได้โดยการทดสอบ การสอบทานอย่างเป็นอิสระและการปรับปรุงแผนเป็นระยะ ๆ

กลยุทธ์การทดสอบในภาพรวม

การพัฒนากลยุทธ์ของการทดสอบ ต้องมีการตัดสินใจจากธุรกิจในเรื่องระดับและความถี่ของการทดสอบที่จะทำให้มั่นใจได้ว่าเป้าหมายของการกู้ธุรกิจกลับคืนสู่ภาวะปกติสามารถทำได้สำเร็จในระหว่างที่เกิดเหตุการณ์ความเสียหายต่อธุรกิจ ความถี่และความซับซ้อนของการทดสอบขึ้นอยู่กับความเสี่ยงของสถาบันการเงิน แม้กระทั่งสถาบันการเงินขนาดเล็กที่เป็นผู้รับบริการก็ควรมีการร่วมทดสอบกับผู้ให้บริการหลักของตนและทดสอบองค์ประกอบอื่น ๆ ที่สำคัญของ BCP ด้วย การทดสอบโดยไม่ใช้บุคลากร (Unmanned recovery testing) ด้วยการส่งเทปสำรองข้อมูลไปยังศูนย์คอมพิวเตอร์สำรองเพื่อให้ผู้ให้บริการทำการกู้คืนนั้น ไม่เพียงพอสำหรับการทดสอบ BCP ของสถาบันการเงิน ซึ่งหากเป็นไปได้ ควรจะมีการทดสอบด้านอื่น ๆ ของ BCP ด้วย

กลยุทธ์ของการทดสอบควรมีรายละเอียดของเงื่อนไขและความถี่ในการทดสอบโปรแกรมระบบงานและงานของส่วนธุรกิจ รวมถึงงานสนับสนุนการประมวลผลข้อมูล กลยุทธ์ควรครอบคลุมวัตถุประสงค์การทดสอบ รายการที่จะทดสอบ และกำหนดการทดสอบ รวมทั้งควร

จัดให้มีการทบทวนและการรายงานผลการทดสอบด้วย ผู้บริหารควรมั่นใจว่าการทดสอบการกู้ธุรกิจกลับคืนสู่ภาวะปกติดำเนินการอย่างน้อยปีละครั้งหรือมากกว่านั้นขึ้นอยู่กับสภาพแวดล้อมการปฏิบัติงานหรือความสำคัญของโปรแกรมระบบงานและงานของส่วนธุรกิจ

ผู้บริหารควรประเมินความเสี่ยง และข้อดีของการทดสอบประเภทต่าง ๆ พร้อมทั้งพัฒนากลยุทธ์โดยยึดตามความต้องการในการที่จะทำให้ธุรกิจดำเนินการได้ต่อเนื่องและกลับคืนสู่ภาวะปกติเป็นหลัก กระบวนการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องควรที่จะสามารถประเมินได้ว่าสถาบันการเงินมีความประสงค์ที่จะปฏิบัติงานเต็มกำลังความสามารถหรือไม่ สถาบันการเงินไม่ควรตั้งสมมติฐานว่าความต้องการใช้บริการจะลดลงในช่วงระหว่างที่เกิดเหตุการณ์ความเสียหาย ที่จริงแล้วความต้องการใช้บริการบางอย่าง (เช่น ATM) กลับจะเพิ่มขึ้น ถ้าสถาบันการเงินมีแผนที่จะลดความสามารถของศูนย์คอมพิวเตอร์สำรองในการปฏิบัติงาน ก็ควรจะมีการประเมินความเสี่ยงจากการใช้งานที่อาจเกินระดับกำลังความสามารถที่กำหนด พร้อมทั้งควรกำหนดลำดับความสำคัญถึงงานที่ต้องการจะประมวลผลหรืองานที่ไม่ต้องการจะประมวลผลด้วย

กระบวนการวางแผน BCP ควรประเมินถึงความจำเป็นที่จะให้มีการทดสอบในระดับภาพรวมทั่วทั้งองค์กร ซึ่งรวมถึงผู้ให้บริการและผู้ที่เกี่ยวข้องในตลาดที่สำคัญ มากกว่าการทดสอบเฉพาะหน่วยธุรกิจแยกต่างหาก การทดสอบอย่างครอบคลุมดังกล่าวต้องมีการประเมินการพึ่งพาอาศัยกันระหว่างงานของส่วนธุรกิจและระบบงานต่าง ๆ อีกทั้งควรมีการประเมินถึงความจำเป็นของการทดสอบตามลำดับของระบบงานเหล่านั้น ผู้บริหารควรทดสอบความสามารถในการกู้ข้อมูลปัจจุบันจากสื่อบันทึกข้อมูลสำรอง นอกจากนั้น สถาบันการเงินควรรวมขั้นตอนปฏิบัติงานและมาตรการรักษาความปลอดภัยเข้าเป็นส่วนหนึ่งในขอบเขตของการทดสอบ และควรมั่นใจว่ามีการจัดเก็บชุดสำเนาของสื่อสำรองไว้ในสถานที่ปลอดภัย เพื่อสำหรับนำมาใช้ในกรณีที่เกิดเหตุการณ์ความเสียหายขึ้นจริงในระหว่างที่ดำเนินการทดสอบ

ขอบเขตและวัตถุประสงค์ในการทดสอบ

ผู้บริหารควรกำหนดไว้ในแผนการทดสอบว่า งาน ระบบ หรือกระบวนการอะไรที่จะทดสอบและองค์ประกอบอะไรที่จะทำให้การทดสอบประสบผลสำเร็จ วัตถุประสงค์ของแผนการทดสอบเพื่อให้มั่นใจว่า BCP ยังคงความถูกต้อง ตรงประเด็นและสามารถทำงานได้ภายใต้สถานการณ์เลวร้าย การทดสอบควรครอบคลุมโปรแกรมระบบงานและงานของส่วนธุรกิจที่

กำหนดมาจากการวิเคราะห์ผลกระทบต่อธุรกิจ ซึ่งการวิเคราะห์ผลกระทบต่อธุรกิจดังกล่าวจะเป็นการกำหนดเป้าหมายของจุดที่จะกู้ธุรกิจกลับคืนสู่ภาวะปกติ ซึ่งจะนำมาใช้ในการกำหนดกลยุทธ์ของการกู้ธุรกิจกลับคืนสู่ภาวะปกติที่เหมาะสมต่อไป

วัตถุประสงค์ของการทดสอบควรเริ่มต้นจากจุดเล็ก ๆ แล้วจึงค่อย ๆ เพิ่มความซับซ้อนและขอบเขตของการทดสอบ ซึ่งสามารถขยายอย่างต่อเนื่องจนในที่สุดกลายเป็นการทดสอบแบบภาพรวมทั่วทั้งองค์กร ซึ่งรวมถึงผู้ให้บริการและผู้เกี่ยวข้องในตลาดที่สำคัญ การปฏิบัติได้ตามวัตถุประสงค์จะทำให้มีความเชื่อมั่นและวางใจในแผนมากขึ้น แผนการทดสอบที่กำหนดไว้อย่างชัดเจน ควรมีลักษณะโดยขั้นต่ำ ดังนี้

- ไม่สร้างความเสี่ยงให้กับการดำเนินธุรกิจปกติ
- ค่อย ๆ เพิ่มความซับซ้อน ระดับของการมีส่วนร่วม หน่วยงาน และสถานที่ที่เกี่ยวข้อง
- แสดงให้เห็นถึงการจัดการที่หลากหลายรูปแบบและความชำนาญในการตอบโต้ภายใต้สถานการณ์วิกฤตที่จำลองขึ้น โดยเพิ่มความเกี่ยวข้องกับทรัพยากรและผู้มีส่วนร่วมมากขึ้น
- ค้นหาข้อบกพร่อง เพื่อดำเนินการแก้ไขการกำหนดค่าและขั้นตอนปฏิบัติงานให้ถูกต้อง
- พิจารณาความบิดเบือนจากรายการทดสอบ เพื่อเพิ่มเหตุการณ์ที่ไม่ได้กำหนดไว้ในแผน เช่น การสูญเสียพนักงานหรือบริการที่สำคัญ

แผนการทดสอบเฉพาะด้าน

ผู้บริหารควรพัฒนาแผนการทดสอบสำหรับแต่ละวิธีที่ใช้ในการทดสอบ BCP แผนการทดสอบควรกำหนดเกณฑ์เชิงปริมาณที่ใช้วัดเป้าหมายของการทดสอบแต่ละข้อ นอกจากนั้นควรได้รับการทบทวนเพื่อให้มั่นใจว่าจะสามารถนำไปถือปฏิบัติได้ โดยไม่ก่อให้เกิดอันตรายใด ๆ ต่อสภาพแวดล้อมการใช้งานจริง

การสอบทานแผนการทดสอบ

ผู้บริหารควรตระเตรียมและทบทวนรายการสำหรับการทดสอบแต่ละครั้ง ก่อนที่จะทำการทดสอบ เพื่อค้นหาจุดอ่อนที่อาจนำไปสู่การทดสอบที่ไม่น่าพอใจหรือไม่ถูกต้อง ส่วนหนึ่งของกระบวนการทบทวนแผนการทดสอบนั้น แผนการทดสอบควรได้รับการปรับปรุงให้ครอบคลุมการเปลี่ยนแปลงต่าง ๆ เช่นการเปลี่ยนตัวบุคคลหลัก นโยบาย เครื่องอำนวยความสะดวก อุปกรณ์ การใช้บริการจากภายนอก และปัจจัยอื่นที่ส่งผลกระทบต่องานของส่วนธุรกิจที่สำคัญ

การพิสูจน์ความสมเหตุสมผลของสมมติฐาน

สมมติฐานของแผนการทดสอบควรผ่านการพิสูจน์ความสมเหตุสมผล เพื่อให้มั่นใจว่ามีความเหมาะสมต่อข้อกำหนดของการดำเนินธุรกิจอย่างต่อเนื่อง การพิสูจน์ดังกล่าวจะต้องได้รับความร่วมมือจากพนักงานของส่วนธุรกิจ ส่วนปฏิบัติการ และส่วนเทคโนโลยีสารสนเทศ ประเด็นที่ใช้ในการพิสูจน์ความสมเหตุสมผลของแผน มีดังนี้

- ความสำคัญของบริการ
- ปริมาณของรายการ
- ความสัมพันธ์ระหว่างงานของส่วนธุรกิจ
- การเลือกกลยุทธ์การวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องที่เกี่ยวกับการใช้สิ่งอำนวยความสะดวกและสิ่งอื่น ๆ ที่ขาดหายหรือหยุดชะงักไป
- ความพร้อมใช้และความเพียงพอของทรัพยากรในการให้บริการตามระดับที่กำหนดไว้ในแผน เช่น เวลาที่ต้องการใช้ในการสร้างสิ่งอำนวยความสะดวกต่าง ๆ การได้รับแฟ้มข้อมูลสำรอง หรือการสร้างเอกสารขึ้นใหม่

ความถูกต้องของข้อมูล

เอกสารข้อมูลและรายการทั้งหมดใน BCP ควรได้รับการตรวจสอบความถูกต้องเป็นระยะ ๆ รวมถึงเฟอร์นิเจอร์ อุปกรณ์ การเชื่อมโยงการติดต่อสื่อสาร โปรแกรมระบบงาน และ

ระบบปฏิบัติการที่ติดตั้งอยู่ที่ศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง นอกจากนี้ควรระบุรุ่นของโปรแกรมระบบงานและระบบปฏิบัติการไว้ในรายการด้วย

ความสมบูรณ์ครบถ้วนของวิธีปฏิบัติ

กระบวนการทดสอบควรได้รับการตรวจสอบเป็นระยะ ๆ เพื่อให้เกิดความมั่นใจว่ากระบวนการดังกล่าวครอบคลุมในเรื่องต่อไปนี้

- กระบวนการตอบโต้เหตุการณ์ฉุกเฉิน รวมถึงกระบวนการอพยพและการประกาศแจ้งให้ทราบ
- กระบวนการประมวลผลสำรอง รวมถึงขั้นตอนการรักษาความปลอดภัยที่ศูนย์คอมพิวเตอร์สำรอง
- กระบวนการกู้ธุรกิจกลับคืนสู่ภาวะปกติอย่างเต็มรูปแบบ รวมถึงการกลับคืนสู่การประมวลผลปกติ

วิธีการทดสอบ

วิธีการทดสอบมีได้ตั้งแต่วิธีที่มีการเตรียมการและใช้ทรัพยากรน้อยที่สุดไปจนถึงวิธีที่มีความซับซ้อนมากที่สุด การทดสอบแต่ละวิธีมีลักษณะ วัตถุประสงค์ และประโยชน์แตกต่างกันออกไป ประเภทของการทดสอบที่สถาบันการเงินจะนำมาใช้ควรกำหนดจาก ช่วงอายุการใช้งานและประสบการณ์ของสถาบันการเงินนั้นในการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ขนาด ความซับซ้อน และลักษณะของธุรกิจ ตัวอย่างของวิธีการทดสอบโดยเรียงลำดับจากที่มีความซับซ้อนน้อยไปหามาก มีดังนี้

1. การทำความเข้าใจและศึกษาการปฏิบัติงาน (Orientation /Walk-through)

เป็นประเภทการทดสอบที่พื้นฐานมากที่สุด มีวัตถุประสงค์หลักเพื่อให้มั่นใจว่าบุคคลสำคัญจากทุกส่วนงาน มีความคุ้นเคยกับ BCP โดยสามารถปฏิบัติได้ดังนี้

- การหารือเกี่ยวกับเรื่อง BCP ในที่ประชุมสัมมนาหรือในกลุ่มเล็กที่จัดขึ้น
- การฝึกอบรมรายบุคคลและทั้งทีมงาน
- การอธิบายและเน้นองค์ประกอบที่สำคัญของ BCP

2. การซักซ้อมและจำลองเหตุการณ์ (Tabletop / Mini-drill)

เป็นวิธีการทดสอบที่ต้องอาศัยการมีส่วนร่วมของผู้ทดสอบมากกว่าวิธีการทำความเข้าใจและศึกษาการปฏิบัติงาน เนื่องจากผู้เข้าร่วมทดสอบจะต้องเลือกเหตุการณ์จำลองขึ้นมาแล้วนำ BCP ไปใช้กับเหตุการณ์นั้น การทดสอบปฏิบัติได้ดังนี้

- การฝึกปฏิบัติและการพิสูจน์ความสามารถในการตอบโต้เหตุการณ์ฉุกเฉินอย่างใดอย่างหนึ่งโดยเฉพาะ
- การมุ่งเน้นการสาธิตให้ความรู้และความชำนาญ และปฏิกิริยาตอบสนองภายในทีมรวมทั้งความสามารถในการตัดสินใจ
- การสวมบทบาทกับการตอบโต้ที่จำลองขึ้นมา ณ สถานที่และสิ่งอำนวยความสะดวกที่ใช้เป็นศูนย์คอมพิวเตอร์สำรอง เพื่อปฏิบัติตามขั้นตอนฉุกเฉิน เพื่อจะได้ทราบถึงอุปสรรคและสามารถแก้ไขปัญหาในลักษณะที่ไม่เป็นอันตรายต่อสภาพแวดล้อมการดำเนินธุรกิจ
- การเคลื่อนย้ายทีมผู้บริหารหรือทีมตอบโต้เหตุการณ์ฉุกเฉินทั้งหมดหรือบางส่วน เพื่อฝึกปฏิบัติการประสานงานที่ถูกต้องเหมาะสม
- การปรับเปลี่ยนระดับความเหมือนจริงในการแจ้งและการเคลื่อนย้ายทรัพยากร ซึ่งจะแตกต่างจากเหตุการณ์จำลอง เพื่อนำผลที่ได้ไปเสริมเนื้อหาและปรับความสมเหตุสมผลของแผน

3. การทดสอบเฉพาะบางส่วน

เป็นการทดสอบประเภทแรกที่เกี่ยวข้องกับการเคลื่อนย้ายพนักงานจริง ๆ ที่สถานที่อื่น เพื่อสร้างช่องทางการสื่อสารและการประสานงานตามที่กำหนดไว้ใน BCP การทดสอบครอบคลุมดังนี้

- การสาธิตความสามารถของการบริหารภาวะฉุกเฉินของพนักงานกลุ่มต่าง ๆ โดยการฝึกปฏิบัติงานที่ต้องมีการติดต่อประสานงานกัน เช่น การควบคุมสั่งการ การประเมินการปฏิบัติงานและการวางแผน
- การติดต่อประสานงานจริงหรือจำลองสถานการณ์ขึ้นมากับศูนย์คอมพิวเตอร์สำรองด้วยการใช้ศักยภาพการสื่อสารจริง
- การเคลื่อนย้ายพนักงานและทรัพยากรตามสถานที่ต่าง ๆ ที่อยู่ในเขตพื้นที่ต่างกัน

- การปรับเปลี่ยนระดับความเหมือนจริงในการแจ้งและการเคลื่อนย้ายทรัพยากร ซึ่งจะแตกต่างกับการสมมติ

4. การทดสอบเต็มรูปแบบ

เป็นประเภทการทดสอบที่มีความครอบคลุมมากที่สุด เป็นการใช้งานทุกส่วนหรือบางส่วนของ BCP โดยการประมวลผลข้อมูลและรายการด้วยการใช้สื่อบันทึกข้อมูลสำรองที่เก็บอยู่ที่สถานที่ที่ใช้กู้ธุรกิจกลับสู่ภาวะปกติ การทดสอบครอบคลุมดังนี้

- การพิสูจน์ความเหมาะสมของงานตอบโต้เหตุการณ์ฉุกเฉิน
- การมุ่งเน้นการสาธิตให้ความรู้และความชำนาญ และการติดต่อประสานงานภายในทีมรวมทั้งความสามารถในการตัดสินใจ
- การสร้างฉากเพื่อการแสดงบทบาทในการตัดสินใจและการประสานงาน
- การประกาศแจ้ง การเคลื่อนย้ายทรัพยากรและการสื่อสารให้ทราบถึงการตัดสินใจ โดยการปฏิบัติจริง ซึ่งจะแตกต่างกับการสมมติ
- กิจกรรมที่ทำ ณ สถานที่จริงที่ใช้ตอบโต้เหตุการณ์ฉุกเฉิน
- การมีส่วนร่วมทั่วทั้งองค์กรและการติดต่อระหว่างทีมบริหารจัดการตอบโต้ภาวะฉุกเฉินทั้งภายในและภายนอก รวมทั้งความร่วมมือจากองค์กรภายนอกอย่างเต็มรูปแบบ
- การประมวลผลข้อมูลจริงที่บันทึกอยู่ในสื่อบันทึกข้อมูลสำรอง
- การฝึกปฏิบัติโดยขยายเวลาให้นานขึ้นเพื่อเป็นการให้เวลาแก่ประเด็นปัญหาที่ค่อย ๆ เกิดขึ้นอย่างเต็มที่ เหมือนกับลักษณะประเด็นปัญหาที่จะเกิดขึ้นในช่วงวิกฤต อีกทั้งเป็นการให้เวลาแก่กลุ่มพนักงานที่เกี่ยวข้องในการแสดงบทบาทให้เหมือนจริง

การดำเนินการทดสอบ

การทดสอบจำเป็นต้องมีศูนย์กลางในการประสานงาน โดยทั่วไปจะมอบหมายให้ทีมงานหรือผู้ประสานงาน BCP ซึ่งทีมงานหรือผู้ประสานงานดังกล่าวจะรับผิดชอบในการกำกับดูแลความสำเร็จของวัตถุประสงค์ที่กำหนดไว้และติดตามผลการทดสอบภายในขอบเขตที่เหมาะสม

สถาบันการเงินควรกำหนดให้พนักงานที่เข้าร่วมในการนำ BCP ไปใช้ปฏิบัติงานและการทดสอบแผนมีจำนวนมากที่สุด เนื่องจากเป็นการสร้างความตื่นตัว ความคุ้นเคย และความรู้สึกในการเป็น เจ้าของ ความสำเร็จจากการนำ BCP ไปปฏิบัติ อีกทั้งควรมีการหมุนเวียนเจ้าหน้าที่ที่เกี่ยวข้องในการทดสอบ เพื่อเตรียมความพร้อมต่อการสูญเสียพนักงานหลักที่อาจเกิดขึ้นจากเหตุภัย การเกษียณอายุ การเลื่อนตำแหน่ง การพ้นจากหน้าที่ การลาออก หรือการมอบหมายหน้าที่ใหม่ นอกจากนั้นการมีส่วนเกี่ยวข้องและการกำกับดูแลของพนักงานอิสระ เช่น ผู้ตรวจสอบ จะช่วยเพิ่มความมั่นใจในความสมเหตุสมผลของกระบวนการทดสอบและความถูกต้องของการรายงาน

การวิเคราะห์และการรายงานผลทดสอบ

การทดสอบจะเกิดประโยชน์ได้ ถ้ามีการนำผลการทดสอบไปวิเคราะห์และเปรียบเทียบกับเป้าหมายที่กำหนด รวมทั้งนำผลที่ได้จากการทดสอบไปดำเนินการต่อ

ผู้บริหารควรรายงานผลการทดสอบและแนวทางแก้ไขปัญหาต่าง ๆ ที่พบต่อคณะกรรมการ รายงานสำหรับผู้บริหารควรพิจารณาผลการทดสอบทั้งหมด การวิเคราะห์ผลการทดสอบควรครอบคลุมประเด็นดังนี้

- การประเมินความสำเร็จของการปฏิบัติตามวัตถุประสงค์ของการทดสอบ
- การประเมินความสมเหตุสมผลของข้อมูลที่ใช้ในการทดสอบ
- แผนดำเนินการแก้ไขปัญหาที่พบ
- รายละเอียดของผลต่างระหว่าง BCP กับผลการทดสอบที่เกิดขึ้นจริง
- ข้อเสนอสำหรับการเปลี่ยนแปลงแก้ไข BCP
- ข้อเสนอแนะสำหรับการทดสอบในอนาคต

การปรับแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องให้เป็นปัจจุบัน

BCP ถือเสมือนเป็นเอกสารที่ต้องมีการปรับปรุงเปลี่ยนแปลงให้ทันสมัยอยู่เสมอ เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของกิจกรรมทางธุรกิจที่ได้มีการจัดทำ BCP รองรับไว้ แผนควรได้รับการ สอบทานโดยผู้บริหารระดับสูง ทีมงานหรือผู้ประสานงานในการวางแผน ผู้

ตรวจสอบภายใน และคณะกรรมการอย่างน้อยปีละครั้ง ทีมงานหรือผู้ประสานงานควรติดต่อกับผู้จัดการของหน่วยธุรกิจต่าง ๆ ของสถาบันการเงินเป็นประจำเพื่อประเมินลักษณะและขอบเขตของการเปลี่ยนแปลงที่เกิดขึ้นกับธุรกิจ โครงสร้าง ระบบ โปรแกรมและอุปกรณ์คอมพิวเตอร์ บุคลากร หรือสิ่งอำนวยความสะดวกต่าง ๆ ของสถาบันการเงิน ซึ่งจัดเป็นส่วนหนึ่งของกระบวนการสอบทาน การเปลี่ยนแปลงมักจะเกิดขึ้นตลอดเวลา ถึงแม้ว่าได้มีการปรับปรุงแผนไปแล้วก็ตาม โดยในปัจจุบัน มี Software ระบบงานวางขายอยู่ทั่วไป ซึ่งผู้ประสานงาน BCP สามารถนำมาใช้ในการระบุและติดตามการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นในองค์กร เพื่อที่จะได้นำมาใช้ประโยชน์ต่อการปรับปรุง BCP ต่อไป

สถาบันการเงินควรวิเคราะห์การเปลี่ยนแปลงทุกอย่างที่เกิดขึ้นในองค์กร เพื่อพิจารณากำหนดผลกระทบของการเปลี่ยนแปลงดังกล่าวต่อแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องที่ใช้อยู่ในปัจจุบัน รวมทั้งพิจารณาถึงสิ่งที่จำเป็นต้องทำการปรับปรุงในแผน เพื่อให้แผนมีความครอบคลุมการ เปลี่ยนแปลงที่เกิดขึ้น ธนาคารแห่งประเทศไทยมีความคาดหวังให้สถาบันการเงินจัดทำเอกสารประกอบการปรับปรุง BCP เพื่อที่จะสามารถใช้แสดงว่าแผนสะท้อนถึงสถานะปัจจุบันของสถาบันการเงิน ประการสุดท้ายสถาบันการเงินควรมั่นใจว่าได้จัดให้มีการเผยแพร่ BCP ที่ปรับปรุงใหม่ให้กับหน่วยงานที่เกี่ยวข้อง

การตรวจสอบและการสอบทานอย่างเป็นอิสระ

ฝ่ายตรวจสอบหรือผู้มีคุณวุฒิอื่น ๆ ที่มีความเป็นอิสระควรสอบทานความเพียงพอของกระบวนการดำเนินธุรกิจอย่างต่อเนื่อง เพื่อให้แน่ใจว่าเป็นไปตามความคาดหวังของคณะกรรมการการสอบทานควรครอบคลุมถึงการประเมินความเพียงพอของการระบุกระบวนการทางธุรกิจ การพัฒนา เหตุการณ์จำลองของภัยคุกคาม การวิเคราะห์ผลกระทบต่อธุรกิจและการประเมินความเสี่ยงตลอดจนถึงแผนที่ได้จัดทำเป็นลายลักษณ์อักษร เหตุการณ์จำลองที่ใช้ทดสอบและกำหนดการทดสอบ รวมทั้งการสื่อสาร ผลการทดสอบและข้อเสนอแนะต่อคณะกรรมการ นอกจากนั้นเพื่อแสดงความรับผิดชอบ ฝ่ายตรวจสอบหรือผู้สอบทานอิสระ ควรเข้าร่วมการทดสอบ BCP ในฐานะผู้สังเกตการณ์ อีกทั้งคณะกรรมการควรสอบทานรายงานการตรวจสอบด้วยความระมัดระวังในประเด็นเรื่องความมีประสิทธิผลของกระบวนการที่ใช้ระบุจุดอ่อนของการดำเนินธุรกิจของสถาบันการเงิน

2.3 บทสรุป

โดยสรุปปัจจัย 6 ข้อดังต่อไปนี้ เป็นสิ่งสำคัญของการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องที่มีประสิทธิภาพ

1. การวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ควรดำเนินการในลักษณะภาพรวมทั่วทั้งองค์กร

2. การวิเคราะห์ผลกระทบต่อธุรกิจและการประเมินความเสี่ยงอย่างครอบคลุมเป็นพื้นฐานของ BCP ที่มีประสิทธิภาพ

3. การวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง เป็นสิ่งที่มากกว่าการกู้ระบบเทคโนโลยีสารสนเทศให้สามารถกลับมาใช้งานได้ กล่าวคือเป็นการทำให้ธุรกิจกลับคืนสู่ภาวะปกติ

4. การพิสูจน์ความมีประสิทธิผลของ BCP ทำได้โดยการทดสอบอย่างละเอียดทั่วถึง

5. BCP และผลการทดสอบควรได้รับการตรวจสอบอย่างเป็นอิสระ

6. BCP ควรได้รับการปรับปรุงเป็นระยะ เพื่อให้สะท้อนและตอบสนองต่อการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นในสถาบันการเงิน

<u>ส่วนที่ 3</u> แนวทางประเมินการตรวจสอบ

วัตถุประสงค์ของการตรวจสอบ

เพื่อให้ทราบถึงคุณภาพและความมีประสิทธิผลของกระบวนการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องขององค์กร ในแง่ความเพียงพอของกระบวนการวางแผนในการรักษาให้ธุรกิจสามารถดำเนินต่อไปได้ในช่วงที่เกิดเหตุการณ์ความเสียหายและการทำให้การดำเนินธุรกิจกลับสู่ภาวะปกติ ซึ่งอาจเป็นเหตุการณ์ความเสียหายในระดับเล็กน้อยไปจนถึงระดับรุนแรง เครื่องมือการตรวจสอบนี้สามารถนำไปใช้ในการประเมินความเพียงพอของกระบวนการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องในระดับภาพรวมทั้งองค์กรหรือในระดับส่วนธุรกิจ โดยอาจทำการสุ่มเลือกส่วนธุรกิจหนึ่ง มาตรวจสอบดูว่ากระบวนการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับส่วนธุรกิจนั้นเป็นอย่างไร

ผังงานนี้มีเจตนาให้ครอบคลุมและสามารถช่วยผู้ตรวจสอบในการกำหนดความมีประสิทธิผลของกระบวนการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของสถาบันการเงิน อย่างไรก็ตาม ผู้ตรวจสอบอาจเลือกใช้เฉพาะบางส่วน ทั้งนี้ขึ้นอยู่กับขนาด ความซับซ้อน และลักษณะของธุรกิจ

วัตถุประสงค์ที่ 1 : กำหนดขอบเขตและเป้าหมายสำหรับการสอบทานงานการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

1. สอบทานรายงานเกี่ยวกับปัญหาและประเด็นสำคัญในอดีต โดยพิจารณาในเรื่องต่อไปนี้

- รายงานตรวจสอบของทางการ
- รายงานของผู้ตรวจสอบภายในและภายนอก
- ผลการทดสอบแผนการดำเนินธุรกิจอย่างต่อเนื่อง
- ประวัติและการประเมินความเสี่ยงขององค์กร

2. สอบทานวิธีที่ผู้บริหารดำเนินการกับประเด็นการตรวจสอบครั้งล่าสุด โดยพิจารณาในเรื่องต่อไปนี้

- ความเพียงพอและระยะเวลาที่ใช้ในการดำเนินการแก้ไข

- การแก้ไขที่ต้นเหตุมากกว่าการแก้ไขที่ประเด็นแต่ละเรื่อง
- ประเด็นสำคัญที่ยังไม่ได้ดำเนินการแก้ไข

3. สัมภาษณ์ผู้บริหารและสอบทานข้อมูลที่ขอเกี่ยวกับการดำเนินธุรกิจอย่างต่อเนื่อง เพื่อระบุ เรื่องดังนี้

- กลยุทธ์ทางธุรกิจที่มีการเปลี่ยนแปลงที่มีนัยสำคัญหรือกิจกรรมที่จะส่งผลกระทบต่อกระบวนการกู้ธุรกิจกลับคืนสู่ภาวะปกติ
- การเปลี่ยนแปลงที่สำคัญในเรื่องของโปรแกรมการตรวจสอบ ขอบเขต และตารางเวลาที่เกี่ยวข้องกับกิจกรรมในการดำเนินธุรกิจอย่างต่อเนื่อง
- การเปลี่ยนแปลงกระบวนการภายในทางธุรกิจ
- การเปลี่ยนผู้บริหารหลักขององค์กร
- สภาพแวดล้อมทางเทคโนโลยีและการเปลี่ยนแปลงโครงสร้างและองค์ประกอบทางเทคโนโลยี
- การเปลี่ยนผู้ให้บริการหลัก (เช่น ผู้ให้บริการทางเทคโนโลยีการสื่อสาร การสำรอง และ/หรือการกู้งานกลับคืน) และรายชื่อของผู้จำหน่าย Software
- ปัจจัยภายในหรือภายนอกอื่น ๆ ที่อาจส่งผลกระทบต่อกระบวนการดำเนินธุรกิจอย่างต่อเนื่อง

4. กำหนดสิ่งที่ผู้บริหารใช้ในการพิจารณาเกี่ยวกับเรื่องภัยคุกคามรูปแบบใหม่และจุดอ่อนในกระบวนการดำเนินธุรกิจอย่างต่อเนื่อง โดยพิจารณาในเรื่องต่อไปนี้

- จุดอ่อนทางเทคโนโลยีและระบบรักษาความปลอดภัย
- ภัยคุกคามจากภายในองค์กร
- ภัยคุกคามจากภายนอกองค์กร (รวมถึงภัยคุกคามที่เผยแพร่ให้ทราบโดยองค์กรต่าง ๆ ที่แบ่งปันข้อมูลกัน)

5. กำหนดขอบเขตของการตรวจสอบโดยเน้นปัจจัยที่ก่อให้เกิดความเสี่ยงสูงสุดต่อสถาบันการเงินหรือผู้ให้บริการ

วัตถุประสงค์ที่ 2 กำหนดแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องในระดับภาพรวมทั้งองค์กรที่เหมาะสม

1. สอบทาน BCP ที่ได้จัดทำเป็นลายลักษณ์อักษร และตรวจสอบดูว่า แผน :

- ระบุการกอบกู้การดำเนินธุรกิจให้กลับคืนสู่สภาวะปกติของหน่วยงานธุรกิจ ฝ่ายงานและหน้าที่งาน โดย
  - อาศัยการจัดลำดับความสำคัญธุรกิจในการประเมินความเสี่ยง
  - คำนึงถึงการพึ่งพาอาศัยกันระหว่างระบบงานต่าง ๆ
- คำนึงถึงสิ่งต่อไปนี้
  - บุคลากร
  - สิ่งอำนวยความสะดวก
  - เทคโนโลยี (Hardware, Software, อุปกรณ์ที่ใช้ในการปฏิบัติงาน)
  - ระบบสื่อสารและเครือข่าย
  - ผู้จำหน่าย
  - โปรแกรมอรรถประโยชน์
  - เอกสาร (ข้อมูลและการบันทึก)
  - การมีผลบังคับใช้ตามกฎหมาย
  - การรักษาความปลอดภัย
  - สื่อที่ใช้ในการเก็บข้อมูล
  - ผู้ถือหุ้น
- ครอบคลุมการเตรียมความพร้อมรองรับเหตุการณ์ฉุกเฉิน และการบริหารจัดการวิกฤตการณ์
- มีโครงสร้างลำดับการติดต่อพนักงาน
- กำหนดความรับผิดชอบอย่างชัดเจนและมอบหมายอำนาจในการตัดสินใจให้ทีมงานหรือเจ้าหน้าที่ที่ได้รับการแต่งตั้ง รวมทั้งอำนาจ ในการประกาศภาวะฉุกเฉิน
- อธิบายขั้นตอนการปฏิบัติงานในภาวะฉุกเฉิน
- กำหนดเงื่อนไขในการเลือกใช้ศูนย์คอมพิวเตอร์สำรอง
- มีขั้นตอนการปฏิบัติงานแจ้งไปที่ศูนย์คอมพิวเตอร์สำรอง
- แต่งตั้งเจ้าหน้าที่ประชาสัมพันธ์เพื่อทำหน้าที่แจ้งให้สาธารณชนทราบ
- ระบุสถานที่ทำงาน เตรียมเครื่องมืออุปกรณ์ และรายชื่อของบริษัทผู้ให้บริการหลัก ๆ (Hardware, Software, ระบบสื่อสาร)

2. พิจารณาว่ามีขั้นตอนการปฏิบัติงานในการติดตามดูแลให้ BCP มีความทันสมัยและได้รับการปรับปรุงเป็นประจำ

วัตถุประสงค์ที่ 3 พิจารณาคุณภาพของการกำกับดูแล BCP และการให้การสนับสนุนโดยคณะกรรมการและผู้บริหารระดับสูง โดยพิจารณาในเรื่องต่อไปนี้

1. ผู้บริหารได้จัดให้มีกระบวนการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องในระดับภาพรวมทั้งองค์กร ที่มีความเหมาะสมกับขนาดและความซับซ้อนขององค์กร ซึ่งใช้กำหนดกลยุทธ์ขององค์กรในการเตรียมพร้อมรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

2. มีการมอบหมายความรับผิดชอบแก่ผู้บริหารระดับสูงในการกำกับดูแลการพัฒนา การนำไปใช้งาน การทดสอบ และการบำรุงรักษา BCP

3. คณะกรรมการมีความมั่นใจว่าได้จัดสรรทรัพยากร ซึ่งรวมถึงบุคลากรอย่างเพียงพอต่อกระบวนการเตรียมความพร้อมรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

4. คณะกรรมการสอบทานและอนุมัติ BCP ที่เป็นลายลักษณ์อักษร รวมทั้งผลการทดสอบอย่างน้อยปีละครั้ง และจดบันทึกการสอบทานดังกล่าวลงในบันทึกการประชุมคณะกรรมการ

5. ผู้บริหารระดับสูงสอบทานและจัดลำดับส่วนธุรกิจ กระบวนการทางธุรกิจ ฝ่ายงาน และบริษัทในเครือ ตามความสำคัญ และความจำเป็นในการกู้ธุรกิจกลับคืนเป็นประจำ และพิจารณาความถี่ของการสอบทานดังกล่าว

6. ผู้บริหารระดับสูงประเมินความเพียงพอของ BCP ของผู้ให้บริการ และสามารถให้ความมั่นใจได้ว่า BCP ขององค์กร สอดคล้องกับแผนของผู้ให้บริการและลำดับการกู้ธุรกิจกลับคืนมาสู่ภาวะปกติ

วัตถุประสงค์ที่ 4 พิจารณาว่าได้มีการจัดทำการวิเคราะห์ผลกระทบต่อธุรกิจ และการประเมินความเสี่ยง โดยพิจารณาในเรื่องต่อไปนี้

1. มีการวิเคราะห์ผลกระทบต่อธุรกิจของหน่วยงานและฝ่ายงานต่าง ๆ ครบถ้วน

2. สอบทานการวิเคราะห์ผลกระทบต่อธุรกิจ เพื่อพิจารณากำหนดว่า การระบุชี้และการจัดลำดับความสำคัญของธุรกิจมีความเพียงพอ

3. การวิเคราะห์ผลกระทบต่อธุรกิจ ระบุถึงระยะเวลาที่ธุรกิจได้รับความเสียหายที่ยอมรับได้ ระดับของความเสียหายของข้อมูลและรายการที่ค้างอยู่ในระบบที่ยอมรับได้ และเป้าหมายเกี่ยวกับต้นทุนและระยะเวลาที่ใช้ในการกู้ระบบกลับคืนสู่ภาวะปกติ

4. สอบทานการประเมินความเสี่ยงและพิจารณาว่าครอบคลุมถึงเหตุการณ์จำลองและโอกาสที่จะเกิดความเสียหายทั้งจากภายในและภายนอกซึ่งส่งผลกระทบต่อการให้บริการสารสนเทศ เทคโนโลยี บุคลากร อุปกรณ์อำนวยความสะดวก และผู้ให้บริการ หรือไม่ โดยครอบคลุมถึง

- ภัยธรรมชาติ เช่น ไฟไหม้ น้ำท่วม อากาศแปรปรวน
- ภัยจากเทคโนโลยี เช่น การสื่อสารขัดข้อง ไฟดับ Hardware และ Software เสียหาย
- การประทุษร้าย เช่น การบุกรุกระบบเครือข่าย การทุจริต และการก่อการร้าย

5. สอบทานเพื่อให้แน่ใจว่าการประเมินความเสี่ยง และการวิเคราะห์ผลกระทบต่อธุรกิจผ่านการสอบทานและอนุมัติโดยคณะกรรมการและผู้บริหารระดับสูง

6. สอบทานเพื่อให้แน่ใจว่า BCP ได้พิจารณาถึงความเสี่ยงด้านชื่อเสียง การดำเนินงาน การปฏิบัติตามกฎหมาย และความเสี่ยงด้านอื่น ๆ

วัตถุประสงค์ที่ 5 : พิจารณาว่าสถาบันการเงินได้จัดให้มีการบริหารความเสี่ยงที่เหมาะสมในกระบวนการดำเนินธุรกิจอย่างต่อเนื่อง โดยพิจารณาในเรื่องต่อไปนี้

1. ความเพียงพอของกลยุทธ์ในการลดความเสี่ยงมีความเพียงพอ โดยพิจารณาว่ากลยุทธ์ดังกล่าว ครอบคลุมเรื่องดังต่อไปนี้

- สถานที่ตั้งและความสามารถของ
  - ศูนย์ประมวลผลกลาง และการดำเนินงานด้านคอมพิวเตอร์
  - ห้องปฏิบัติการทางคอมพิวเตอร์ (Back-room operations)
  - สถานที่ทำงานของส่วนธุรกิจ
  - การสื่อสารทางไกล
- การสำรองสิ่งต่าง ๆ ดังนี้
  - ข้อมูล
  - ระบบปฏิบัติการ

- โปรแกรมระบบงาน
- โปรแกรมอรรถประโยชน์
- การสื่อสารทางไกล

- การจัดเก็บสิ่งดังต่อไปนี้ ไว้ที่สถานที่อื่น
  - สื่อสำรองข้อมูล
  - อุปกรณ์ที่ใช้ในการทำงาน
  - เอกสาร เช่น BCP ระเบียบวิธีปฏิบัติงานและวิธีดำเนินงานต่าง ๆ ทะเบียนทรัพย์สิน

- ระบบไฟฟ้าสำรอง
  - ระบบจ่ายไฟฟ้าสำรอง
  - เครื่องกำเนิดไฟฟ้าสำรอง

2. มีการกระจายทางภูมิศาสตร์ในเรื่องดังต่อไปนี้
   - สถานที่ประมวลผลสำรอง
   - สถานที่สำรองสำหรับกระบวนการและหน้าที่งานทางธุรกิจ
   - สถานที่เก็บข้อมูลสำรอง

3. นโยบาย มาตรฐาน และกระบวนการปฏิบัติงานครอบคลุมประเด็นเกี่ยวกับการวางแผนดำเนินธุรกิจอย่างต่อเนื่อง เช่น
   - การพัฒนาระบบงานและโปรแกรม และการบริหารโครงการ
   - กระบวนการควบคุมการเปลี่ยนแปลง
   - ความสอดคล้องกันของข้อมูล การสำรอง และการทำให้ธุรกิจกลับคืนสู่สภาพเดิม
   - การฝึกอบรมเจ้าหน้าที่และวางแผนทางด้านการสื่อสาร
   - การทำประกันภัย
   - การประสานงานกับหน่วยงานรัฐบาลและชุมชน

4. บุคลากรได้รับการฝึกอบรมอย่างเพียงพอให้สามารถปฏิบัติหน้าที่ของตนตามแผนงานที่กำหนดและมีการติดประกาศขั้นตอนปฏิบัติงานในภาวะฉุกเฉินให้เห็นอย่างชัดเจนและทราบโดยทั่วกัน

5. กลยุทธ์ในการดำเนินธุรกิจอย่างต่อเนื่อง ครอบคลุมทางเลือกสำหรับองค์ประกอบที่ต้องพึ่งพาอาศัยกันและมีผู้มีส่วนได้ส่วนเสีย ในเรื่องต่อไปนี้

- สิ่งอำนวยความสะดวก
- การสื่อสารทางไกล
- ผู้ให้บริการเทคโนโลยีจากภายนอก
- คู่ค้าหลัก/หุ้นส่วนทางธุรกิจ
- ลูกค้า/สมาชิก

6. สถาบันการเงินมีกระบวนการที่เพียงพอต่อการบำรุงรักษาแผนงานต่าง ๆ ให้มีความถูกต้องและเป็นปัจจุบัน

- แต่งตั้งบุคคลรับผิดชอบในการติดตามการเปลี่ยนแปลงกระบวนการ ตัวบุคคลและสภาพแวดล้อม
- คณะกรรมการสอบทานและอนุมัติแผนงานต่าง ๆ ทุกปีและหลังจากที่มีการปรับปรุงและเปลี่ยนแปลงที่มีนัยสำคัญ
- กระบวนการแจ้งและกระจายแผนงานต่าง ๆ ที่ได้มีการปรับปรุงแก้ไขแล้วให้แก่บุคลากรและส่งไปเก็บที่สถานที่กู้ระบบกลับคืนสู่ภาวะปกติ

7. งานตรวจสอบได้มีส่วนร่วมในงานการดำเนินธุรกิจอย่างต่อเนื่องอย่างมีประสิทธิผลและครอบคลุมถึงเรื่องต่อไปนี้

- ขอบเขตของการตรวจสอบงานการดำเนินธุรกิจอย่างต่อเนื่อง
- ผลการประเมินการเตรียมความพร้อมของการดำเนินงานอย่างต่อเนื่องในช่วงที่ทำการสอบทานสายงานต่าง ๆ ทางธุรกิจ
- การมีส่วนร่วมในการทดสอบของผู้ตรวจสอบในฐานะผู้สังเกตการณ์
- การสอบทานแผนและผลการทดสอบของผู้ตรวจสอบ

วัตถุประสงค์ที่ 6 : พิจารณาว่าสถาบันการเงินได้จัดให้มีการทดสอบ BCP อย่างเหมาะสม เพื่อให้มั่นใจว่าจะสามารถดำเนินธุรกิจต่อไปได้ในช่วงภาวะฉุกเฉิน และสามารถกู้ธุรกิจกลับคืนสู่ภาวะปกติตามที่ตั้งใจไว้ โดยพิจารณาในเรื่องต่อไปนี้

1. มีการทดสอบ BCP อย่างน้อยปีละครั้ง
2. การทดสอบครอบคลุมทุกส่วนธุรกิจหลัก ฝ่ายงาน หรือหน้าที่งาน

3. ตรวจสอบเกี่ยวกับการทดสอบแผน โดยพิจารณาเรื่องดังนี้

- การกำหนดเป้าหมายและวัตถุประสงค์ล่วงหน้า
- การกำหนดเงื่อนไขและปริมาณกิจกรรมตามสภาพความเป็นจริง
- การใช้ระบบและข้อมูลสำรองที่แท้จริงในการทดสอบ โดยจะเก็บข้อมูลสำรองชุดอื่น ๆ ไว้นอกสถานที่ เพื่อไว้ใช้ในกรณีที่เกิดเหตุฉุกเฉินในขณะที่ดำเนินการทดสอบ
- การมีส่วนร่วมและการสอบทานของผู้ตรวจสอบภายใน
- รายงานการวิเคราะห์ภายหลังการทดสอบ และกระบวนการสอบทานที่ครอบคลุมถึงการเปรียบเทียบผลการทดสอบกับเป้าหมายที่กำหนดไว้
- การพัฒนาแผนการดำเนินการแก้ไขปัญหาที่พบ
- การสอบทานโดยคณะกรรมการ

4. การทดสอบได้มีส่วนเกี่ยวข้องกับเรื่องการพึ่งพาอาศัยกันของฝ่ายงาน ผู้จำหน่ายและผู้ให้บริการหลัก ๆ เพื่อให้ทราบถึงความขัดแย้งและความไม่สอดคล้องกันที่สำคัญ

5. ระดับของการทดสอบเพียงพอกับขนาดและความซับซ้อนขององค์กร และการทดสอบครอบคลุมเรื่องดังต่อไปนี้

- การทดสอบระบบปฏิบัติการและโปรแกรมอรรถประโยชน์ (โครงสร้างพื้นฐาน)
- การทดสอบโปรแกรมระบบงานหลักทุกระบบ (ระดับของระบบงาน)
- การโอนข้อมูลระหว่างระบบงาน (การทดสอบภาพรวม)
- การทดสอบสภาพแวดล้อมอย่างครบถ้วนและการรองรับปริมาณงานมาก ๆ (การทดสอบภาวะวิกฤต)

6. การทดสอบสถานที่สำรอง ครอบคลุมเรื่องดังต่อไปนี้

- การเชื่อมต่อเครือข่ายสื่อสาร
- การประมวลผลรายการ การเชื่อมต่อและข้อมูลของการปฏิบัติงานสนับสนุน
- การเชื่อมต่อระหว่างคอมพิวเตอร์ในการดึงข้อมูลสำคัญ

7. การทดสอบโครงสร้างระบบเทคโนโลยีสารสนเทศ ครอบคลุมเรื่องดังต่อไปนี้

- การหมุนเวียนบุคลากร
- การมีส่วนร่วมของเจ้าหน้าที่จากส่วนธุรกิจ

8. ผู้บริหารควรจัดให้มีการทดสอบอย่างเหมาะสมกับ
   - ผู้ให้บริการที่สำคัญ
   - ลูกค้า
   - บริษัทในเครือ
   - สถาบันการเงินที่เกี่ยวข้อง
   - ผู้เกี่ยวข้องในระบบชำระเงินและตลาดการเงิน

วัตถุประสงค์ที่ 7 : พิจารณาว่าสถาบันการเงินจัดทำ BCP ของการดำเนินงานด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรอย่างเหมาะสมโดยเป็นส่วนหนึ่งของ BCP ขององค์กรและสอดคล้องกับ BCP ของฝ่ายงานอื่น ๆ หรือไม่ โดยพิจารณาในเรื่องต่อไปนี้

1. BCP ของส่วนเทคโนโลยีสารสนเทศสนับสนุนและสะท้อนเป้าหมายและลำดับความสำคัญตามที่ระบุไว้ใน BCP ของส่วนธุรกิจ

2. BCP ครอบคลุมทรัพยากรและเทคโนโลยีสำคัญ เช่นระบบเครือข่ายสื่อสารข้อมูลและช่องทางการให้บริการลูกค้า เป็นต้น

3. BCP ครอบคลุมโครงสร้างการเชื่อมต่อของระบบเครือข่ายและการสื่อสารของทั้งองค์กร

4. ในกรณีที่ไม่สามารถประมวลผลระบบงานได้ทุกระบบ สถาบันการเงินได้กำหนดลำดับก่อนหลังในการประมวลผลไว้ใน BCP

วัตถุประสงค์ที่ 8 : พิจารณาว่า BCP คำนึงถึงการสำรองและสามารถใช้งาน Hardware ได้เหมือนในภาวะปกติ โดยพิจารณาในเรื่องต่อไปนี้

1. การจัดให้มีความสามารถในการประมวลผลสำรองในกรณีที่ Hardware ศูนย์ข้อมูล หรือเครือข่ายบางส่วน ใช้งานไม่ได้ หรือเข้าถึงไม่ได้ และพิจารณาว่าการจัดการดังกล่าวได้ทำเป็นลายลักษณ์อักษรหรือไม่

2. ในกรณีที่องค์กรใช้ระบบสำรองที่พัฒนาขึ้นเองซึ่งติดตั้งอยู่ ณ สถานที่ต่างหากอีกแห่งหนึ่ง ให้ตรวจสอบว่า อุปกรณ์ต่าง ๆ สามารถใช้ประมวลผลทุกโปรแกรมระบบงานหลักได้อย่างเป็นอิสระ

3. ในกรณีที่องค์กรใช้บริการสถานที่ เครื่องมือ อุปกรณ์ในการกู้ระบบจากภายนอก ให้พิจารณาสถานที่กู้ระบบ ในเรื่องต่อไปนี้

- ความสามารถในการรองรับงานประมวลผลในปริมาณที่ต้องการ
- การจัดหาเวลาในการประมวลผลอย่างเพียงพอที่จะรองรับรายการที่คาดว่าจะเกิดขึ้นในปริมาณมาก ๆ ตามลำดับความรุนแรงของเหตุการณ์ฉุกเฉิน
- สถาบันการเงินสามารถใช้สถานที่ เครื่องมือ อุปกรณ์ขององค์กรที่เป็นเจ้าของทรัพย์สินเหล่านี้ได้จนกว่าจะสามารถกู้สถานการณ์จากเหตุการณ์ความเสียหายและย้ายไปใช้งานสถานที่ เครื่องมือ อุปกรณ์ ของตนเองได้

4. สอบทานสัญญาที่ทำกับคู่สัญญา เช่น ผู้ให้บริการกู้ระบบ

5. วิธีการบริหารจัดการในกรณีที่ลูกค้าอื่น ๆ ที่ใช้บริการสถานที่ เครื่องมืออุปกรณ์ในการกู้ระบบประสบกับเหตุการณ์ความเสียหายพร้อม ๆ กัน

6. กระบวนการที่จะทำให้มั่นใจได้ว่าการเปลี่ยนแปลงใด ๆ (เช่น การปรับเปลี่ยน Hardware หรือ Software ณ สถานที่ปฏิบัติงานจริง) จะมีการปรับเปลี่ยนในลักษณะเดียวกัน ณ สถานที่ใช้ในการกู้ระบบทุกแห่ง

7. กระบวนการแจ้งให้สถาบันการเงินทราบถึงการเปลี่ยนแปลงใด ๆ ณ สถานที่ใช้ในการกู้ระบบ ซึ่งอาจทำให้ต้องปรับ Software หรือแผนการกู้ระบบ

วัตถุประสงค์ที่ 9 : พิจารณาว่ากระบวนการรองรับการดำเนินธุรกิจอย่างต่อเนื่องครอบคลุมถึง การสำรองและการกู้ข้อมูลและโปรแกรมระบบงานกลับคืนสู่ภาวะปกติ

1. พิจารณาสิ่งต่อไปนี้

- การจัดให้มีระบบปฏิบัติการไว้ทั้งสถานที่ปฏิบัติงานจริงและสถานที่อื่นภายนอก
- การจัดให้มีโปรแกรมระบบที่ใช้งานจริงไว้ทั้งสถานที่ปฏิบัติงานจริงและสถานที่อื่นภายนอก ทั้งชุด Source Program และ Object Program
- การเปลี่ยนแปลงทุกอย่างเกี่ยวกับโปรแกรมและระบบงานควรรวมอยู่ในการสำรองด้วย
- การจัดเก็บสื่อบันทึกข้อมูลสำรองไว้ในสถานที่แยกต่างหากอีกแห่งที่สามารถนำออกมาใช้ได้อย่างรวดเร็วตลอดเวลา

- ความถี่และจำนวนของรุ่นในการสำรอง มีความเพียงพอกับปริมาณรายการที่ประมวลผลและความถี่ของการปรับระบบปัจจุบัน

- การจัดเก็บแฟ้มข้อมูลธุรกรรมที่เคลื่อนไหว ไว้ทั้งสถานที่ปฏิบัติงานจริงและสถานที่อื่นภายนอก

- การส่งแฟ้มข้อมูลสำรองไปเก็บที่สถานที่แยกต่างหากอีกแห่งตามระยะเวลาที่เหมาะสม และไม่ควรนำกลับมา จนกว่าจะมีแฟ้มข้อมูลสำรองปัจจุบันส่งไปเก็บแทน

2. สอบทานแผนรองรับการดำเนินงานด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่องที่ได้จัดทำขึ้นเป็นลายลักษณ์อักษร และพิจารณากำหนดว่าแผนระบุถึงการสำรองระบบงานและการเขียนโปรแกรม (ถ้ามี) ซึ่งรวมถึง

- การสำรองเครื่องมือและ Software ที่ใช้ในการเขียนโปรแกรม

- ชุดสำเนาของเอกสารประกอบโปรแกรมและระบบงานที่แยกจัดเก็บไว้ในสถานที่ต่างหากอีกแห่ง

วัตถุประสงค์ที่ 10 : พิจารณาว่า BCP ครอบคลุมถึงการเตรียมการที่เหมาะสมเพื่อให้มั่นใจว่ากระบวนการในการกู้ศูนย์ประมวลผล กลับคืนสู่ภาวะปกติ จะสามารถใช้การได้ตามที่ต้องการ โดยพิจารณาในเรื่องต่อไปนี้

1. ศูนย์ประมวลผลมีการจัดเก็บ BCP ในรูปของเอกสารอย่างเหมาะสม ตรวจสอบว่า BCP ด้านเทคโนโลยีสารสนเทศ ให้การสนับสนุนที่เหมาะสมและสะท้อนอย่างสมเหตุสมผลถึงเป้าหมายและลำดับความสำคัญที่กำหนดใน BCP ขององค์กร

2. BCP ได้ระบุถึงวิธีการที่จะนำรายการค้างและกิจกรรมอื่น ๆ กลับคืนมาเป็นปัจจุบัน

3. สถาบันการเงินจัดให้มีแผนที่ระบุการกลับคืนสู่ภาวะการปฏิบัติงานปกติและการย้ายกลับมาสู่สถานที่ทำงานปกติ ทันทีที่แก้ไขสถานการณ์ได้ และเครื่องอำนวยความสะดวกต่าง ๆ ที่ใช้อยู่เป็นประจำสามารถใช้งานได้ใหม่อีกครั้ง

4. สถาบันการเงินจัดเก็บเอกสารอย่างเพียงพอไว้ในสถานที่ที่ใช้ในการกู้ระบบหรือ สถานที่เก็บสื่อหรือเอกสารสำคัญที่เป็น Off Site Storage โดยครอบคลุมเอกสารดังนี้

- ชุดสำเนาของ BCP แต่ละแผนย่อย

- ชุดสำเนาของเอกสารประกอบระบบงานที่จำเป็น

- ชุดสำเนาของขั้นตอนการปฏิบัติงานที่จำเป็น

วัตถุประสงค์ที่ 11 : พิจารณาว่า BCP ครอบคลุมวิธีการปฏิบัติงานด้านการรักษาความปลอดภัยอย่างเหมาะสม โดยพิจารณาในเรื่องต่อไปนี้

1. มีการรักษาความปลอดภัยทางกายภาพและการควบคุมการเข้าถึงอย่างเพียงพอในกระบวนการสำรองข้อมูลและ การจัดเก็บโปรแกรม ตลอดอายุการใช้งาน ซึ่งครอบคลุมตั้งแต่การสร้าง การโอนย้าย/ส่งไปสถานที่จัดเก็บ การจัดเก็บ การเรียกใช้และการถ่ายโอน จนถึงการทำลาย

2. มีการพิจารณาและวางแผนการควบคุมการเข้าถึงทางกายภาพและตรรกที่เหมาะสมสำหรับระบบที่ไม่ค่อยมีการใช้งาน เมื่อมีการโอนย้ายการประมวลผลไปที่ศูนย์คอมพิวเตอร์สำรองชั่วคราว

3. การตรวจจับการบุกรุกและแผนการตอบโต้เหตุฉุกเฉินโดยคำนึงถึงความพร้อมใช้ของทรัพยากรและการเปลี่ยนแปลงของสิ่งอำนวยความสะดวกและระบบต่าง ๆ ที่อาจเกิดขึ้นเมื่อมีการใช้งานศูนย์คอมพิวเตอร์สำรอง

4. ความสมเหตุสมผลของวิธีการอนุญาตให้บุคลากรได้สิทธิ์ในการเข้าถึงชั่วคราว (ทั้งทางกายภาพและตรรกะ) ในระหว่างการปฏิบัติตามแผนรองรับการดำเนินงานอย่างต่อเนื่อง

- ประเมินผลการมอบหมายงานให้เจ้าหน้าที่สำรองมีความรับผิดชอบและหน้าที่ตามสถานการณ์จำลองต่าง ๆ ของการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และการเปลี่ยนแปลงดังกล่าวทำให้ต้องมีการปรับเปลี่ยนระดับการเข้าถึงระบบงาน การปฏิบัติงาน ข้อมูลและสิ่งอำนวยความสะดวกต่าง ๆ หรือไม่

- สอบทานหลักฐานการอนุญาตและการพิสูจน์ตัวตนเพื่อพิจารณากำหนดว่าเป็นไปตามความรับผิดชอบงานหลักหรือไม่ และครอบคลุมความรับผิดชอบในการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องด้วยหรือไม่

วัตถุประสงค์ที่ 12 : พิจารณาว่า BCP ระบุกิจกรรมสำคัญที่ดำเนินการโดยผู้ให้บริการภายนอก โดยพิจารณาในเรื่องต่อไปนี้

1. BCP ระบุถึงการติดต่อสื่อสารและการเชื่อมโยงกับผู้ให้บริการภายนอกในกรณีที่เกิดเหตุการณ์ความเสียหายกับสถาบันการเงิน

2. BCP ระบุการติดต่อสื่อสารและการเชื่อมโยงกับผู้ให้บริการภายนอกในกรณีที่เกิดเหตุการณ์ความเสียหายกับเครื่องมือ อุปกรณ์ สถานที่อำนวยความสะดวกของผู้ให้บริการ

3. พิจารณาว่าสถาบันการเงินจัดให้มีเอกสารวิธีการปฏิบัติงานสำหรับการเข้าถึงการโอนถ่ายข้อมูลกับผู้ให้บริการภายนอกบริษัทคู่ค้า บริษัทในเครือ และผู้ให้บริการรายอื่น ๆ จากศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง เมื่อเกิดเหตุการณ์ความเสียหาย

4. สถาบันการเงินควรมีชุดสำเนาของ BCP ของผู้ให้บริการภายนอก และนำมารวมเข้ากับ BCP ของสถาบันการเงินตามความเหมาะสม

5. ผู้บริหารได้รับและสอบทานผลการทดสอบของผู้ให้บริการภายนอก

6. เมื่อมีการทดสอบกับผู้ให้บริการหลัก ๆ พิจารณาว่าผู้บริหารคำนึงถึงการทดสอบ ในเรื่องต่อไปนี้

- จากศูนย์คอมพิวเตอร์หลักของสถาบันการเงินไปยังศูนย์คอมพิวเตอร์สำรองของผู้ให้บริการภายนอกและ
- จากศูนย์คอมพิวเตอร์สำรองของสถาบันการเงินไปยังศูนย์คอมพิวเตอร์หลักของผู้ให้บริการภายนอกและ
- จากศูนย์คอมพิวเตอร์สำรองของสถาบันการเงินไปยังศูนย์คอมพิวเตอร์สำรองของผู้ให้บริการภายนอก

7. ผู้บริหารของสถาบันการเงินได้ประเมินความเพียงพอของแผนงานรองรับการดำเนินธุรกิจอย่างต่อเนื่องของผู้ให้บริการภายนอกผ่านทางแผนการบริหารจัดการกับผู้ให้บริการ (เช่น ข้อกำหนดในสัญญา)

บทสรุป

วัตถุประสงค์ที่ 13 : หารือแนวทางการดำเนินการแก้ไขและสื่อสารข้อเท็จจริงที่ตรวจพบ

1. จากขั้นตอนที่ใช้ปฏิบัติงาน

- จัดทำเอกสารสรุปเกี่ยวกับคุณภาพและประสิทธิผลของกระบวนการดำเนินธุรกิจอย่างต่อเนื่อง
- พิจารณากำหนดและจัดทำเอกสารเกี่ยวกับขอบเขตที่จะอาศัยวิธีปฏิบัติงาน

ของผู้ตรวจสอบภายในและภายนอกในการกำหนดขอบเขตวิธีปฏิบัติของการดำเนินธุรกิจอย่างต่อเนื่อง

2. สอบทานข้อสรุปเบื้องต้นกับหัวหน้าผู้นำสายออกตรวจ โดยคำนึงถึง

- การฝ่าฝืนกฎหมาย ระเบียบ กฎข้อบังคับ
- ประเด็นที่มีนัยสำคัญที่คณะกรรมการต้องให้ความสนใจหรือข้อเสนอแนะในรายงานการตรวจสอบ
- ผลกระทบของข้อสรุปเกี่ยวกับผลการจัดอันดับที่คาดว่าจะเกิดขึ้น

3. หารือข้อเท็จจริงที่พบกับผู้บริหารและขอทราบแนวทางแก้ไขและกำหนดระยะเวลาสำหรับการแก้ไขข้อบกพร่องที่มีนัยสำคัญ

4. จัดทำเอกสารบันทึกข้อสรุปเสนอต่อหัวหน้าผู้นำสายออกตรวจ โดยแนบรายงานพร้อมความเห็นสำหรับทุกส่วนของรายงานการตรวจสอบที่เกี่ยวข้อง

5. จัดโครงสร้างของกระดาษทำการเพื่อให้มั่นใจว่ามีหลักฐานที่ชัดเจนในการสนับสนุนข้อเท็จจริงและข้อสรุปที่สำคัญ

ภาคผนวก ก : อภิธานศัพท์ (Glossary)

Back-up Generations	วิธีการสร้างและจัดเก็บแฟ้มข้อมูลสำรอง ตามรุ่นของแฟ้มข้อมูลโดยมีศัพท์เรียกแฟ้มข้อมูลชุดล่าสุดว่า “รุ่นลูก” และแฟ้มข้อมูลชุดย้อนหลังถัดไป 1 รุ่น เรียกว่า “รุ่นพ่อ” ย้อนหลังถัดไปอีก 1 รุ่น เรียกว่า “รุ่นปู่” ซึ่งการสำรองในที่นี้จะหมายถึงการสำรองแฟ้มข้อมูลหลัก (Master Files) ของระบบงานของธุรกิจการเงิน
Business Continuity Plan (BCP)	แผนงานในการรักษาให้ธุรกิจดำเนินไปได้อย่างต่อเนื่องหรือแผนในการทำให้ธุรกิจกลับคืนสู่สภาพที่สามารถดำเนินต่อไปได้ ในกรณีที่เกิดเหตุการณ์ฉุกเฉิน โดยเขียนเป็นลายลักษณ์อักษรซึ่งมีรายละเอียดอย่างครอบคลุมและเป็นที่เข้าใจได้ง่าย
Business Impact Analysis (BIA)	กระบวนการวิเคราะห์ที่ระบุผลกระทบต่อกระบวนการทางธุรกิจของสถาบันการเงิน อันเกิดจากเหตุการณ์ทั่วไปที่ไม่อาจควบคุมได้
Critical financial markets	ตลาดการเงินซึ่งมีความสำคัญยิ่งยวดต่อเศรษฐกิจของประเทศ เช่น ตลาดเงินระยะสั้น ตลาดอัตราแลกเปลี่ยน ตลาดตราสารหนี้ และหลักทรัพย์รัฐบาล รัฐวิสาหกิจ
Data synchronization	การเปรียบเทียบและสอบยันแฟ้มข้อมูลต่าง ๆ ที่มีการพึ่งพาอาศัยกันในเวลาเดียวกัน เพื่อให้แฟ้มข้อมูลเหล่านั้นบรรจุข้อมูลที่ตรงกัน
Disaster recovery plan	แผนงานที่อธิบายถึงกระบวนการกู้ระบบเทคโนโลยีสารสนเทศกลับคืนจากภาวะความขัดข้องของการประมวลผล
Emergency plan	แผนงานที่กล่าวถึงขั้นตอนการปฏิบัติงานในทันทีทันใดเมื่อเกิดเหตุฉุกเฉิน เช่น ไฟไหม้ พายุ น้ำท่วม การขู่วางระเบิด เป็นต้น
Encryption	การแปลงข้อมูลให้อยู่ในรูปรหัสลับหรือสัญลักษณ์เครื่องหมาย
FEMA	คำย่อของ Federal Emergency Management Agency (องค์กรการจัดการเหตุฉุกเฉินของรัฐบาลกลาง สหรัฐอเมริกา)

Gap analysis	การวิเคราะห์เปรียบเทียบที่ชี้ให้เห็นถึงความแตกต่างระหว่างผลที่เกิดขึ้นจริงกับผลลัพธ์ที่ต้องการให้เป็น
GETS	คำย่อของ Government Emergency Telecommunications Service card program บัตร GETS เป็นบัตรใช้ในยามฉุกเฉิน โดยสามารถใช้ในการเข้าถึงและให้สิทธิ์พิเศษในการประมวลผลสำหรับการให้บริการสื่อสารทางเสียง (Voice Communication Service) ในภาวะฉุกเฉิน ของประเทศสหรัฐอเมริกา
HVAC	คำย่อของ Heating ,Ventilation ,Air Conditioning (เครื่องทำความร้อน เครื่องระบายอากาศ เครื่องปรับอากาศ)
Media	สื่อที่ใช้จัดเก็บข้อมูล เช่น กระดาษ เทป Hard disk แผ่นCD
Mirroring	กระบวนการสำรองข้อมูลแบบ real time หรือเกือบจะ real-time ผ่านระบบเครือข่ายสื่อสารทางคอมพิวเตอร์ไปไว้อีกพื้นที่หนึ่ง
Object program	ชุดคำสั่งที่ถูกแปลงเป็นภาษาเครื่อง และพร้อมที่จะทำงาน เช่น executed โดยคอมพิวเตอร์
PBX	คำย่อของ Private Branch Exchange (ตู้ชุมสายโทรศัพท์ภายใน)
Reciprocal agreement	ข้อตกลงระหว่างองค์กร 2 แห่ง ซึ่งใช้ระบบคอมพิวเตอร์แบบเดียวกัน โดยต่างจะจัดหาเวลาในการประมวลผลให้อีกฝ่ายหนึ่ง ในกรณีที่ระบบใดระบบหนึ่งไม่สามารถใช้งานได้ ซึ่งเวลาที่สามารถจัดหาให้ในการประมวลผลอาจอยู่บนพื้นฐานของความพยายามที่ดีที่สุด (Best Effort) หรือ เท่าที่เวลาจะอำนวย (As Time Available) ก็ได้
Recovery point objectives	จำนวนข้อมูลเสียหายที่กำหนดไว้ โดยไม่ทำให้การกู้ การดำเนินงานได้รับผลกระทบอย่างรุนแรง

Recovery site	สถานที่ปฏิบัติงานทดแทนสำหรับประมวลผลข้อมูลเมื่อเกิดเหตุฉุกเฉิน (ซึ่งอาจใช้ในการดำเนินธุรกิจด้วย) ซึ่งแบ่งได้เป็น - Hot Site คือศูนย์คอมพิวเตอร์สำรองที่มีการติดตั้งอุปกรณ์คอมพิวเตอร์ไว้อย่างสมบูรณ์พร้อมเหมือนศูนย์คอมพิวเตอร์หลัก - Cold Site คือศูนย์ปฏิบัติการคอมพิวเตอร์ที่ไม่มีอุปกรณ์คอมพิวเตอร์
Recovery time objectives	ระยะเวลาที่องค์กรยอมรับได้ในการกู้คืนระบบในกรณีที่เกิดเหตุฉุกเฉิน เช่น RTO = 1 ชั่วโมง หมายถึง ต้องกู้ระบบกลับคืนภายใน 1 ชั่วโมง
Recovery Vendors	องค์กรที่ให้บริการจัดหาสถานที่กู้ระบบ และให้บริการสนับสนุน โดยคิดค่าธรรมเนียมจากการให้บริการด้วย
Routing	กระบวนการเคลื่อนย้ายข้อมูลจากต้นทางไปยังปลายทาง
SAS 70 report	รายงานตรวจสอบขององค์กรที่ให้บริการที่ได้จัดทำตามแนวทางของ American Institute of Certified Public Accountants' Statement of Auditing Standards Number 70
Server	เครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นที่ใช้ในการบริหารจัดการเกี่ยวกับเครือข่ายสื่อสาร ตัวอย่างเช่น Print Server คืออุปกรณ์ที่ใช้บริหารงานพิมพ์ทางเครือข่าย
Source program	ชุดคำสั่งที่เขียนขึ้นด้วยภาษาทางคอมพิวเตอร์ เช่นภาษา C , Pascal, COBOL ซึ่งจะมี Complier ทำหน้าที่แปลง Source Code เป็นชุดคำสั่งที่อยู่ในรูปของภาษาเครื่อง (Object program)
System Development Life Cycle (SDLC)	กลยุทธ์หรือแผนงานที่เป็นลายลักษณ์อักษรสำหรับใช้ในการพัฒนา เปลี่ยนแปลง แก้ไขระบบงานและโปรแกรม ซึ่งหมายรวมถึงการอนุมัติขั้นต้น การจัดทำเอกสารประกอบระบบงาน แผนทดสอบและผลการทดสอบ รวมถึงการอนุมัติและการจัดทำเอกสารเกี่ยวกับการเปลี่ยนแปลงแก้ไขระบบงานและโปรแกรมที่เกิดขึ้นในภายหลัง

T-1 line	สายโทรศัพท์พิเศษที่ใช้สำหรับการติดต่อสื่อสารข้อมูลแบบ Digital
UPS	คำย่อของ Uninterruptible Power Supply เป็นชุดแบตเตอร์รี่ที่ใช้จ่ายพลังงานไฟฟ้าสำหรับช่วงเวลาใดเวลาหนึ่ง
Utility programs	ชุดคำสั่งที่ใช้ในการสร้างหรือบำรุงรักษาระบบงาน หรือใช้ในการเปลี่ยนแปลงแก้ไขข้อมูลที่จัดเก็บหรือข้อมูลที่อยู่ระหว่างการส่ง
Vaulting	กระบวนการสำรองข้อมูลเป็นระยะ ๆ ผ่านระบบเครือข่ายคอมพิวเตอร์ไปยังสถานที่กู้ระบบโดยตรง

ภาคผนวก ข : ภัยคุกคามจากภายในและภายนอก

BCP ควรจะมุ่งเน้นที่ความสามารถในการฟื้นฟูธุรกิจของสถาบันการเงินให้กลับสู่สภาวะปกติ โดยไม่คำนึงถึงลักษณะของเหตุการณ์ความเสียหาย ซึ่งอาจต้องใช้รูปแบบการโต้ตอบที่แตกต่างออกไปตามแต่ละประเภทของความเสียหาย ทั้งนี้ เหตุการณ์ความเสียหายหลายประเภทไม่ได้ส่งผลกระทบเฉพาะสถาบันการเงินเพียงอย่างเดียวแต่ยังกระทบชุมชนรอบ ๆ อีกด้วย ส่วนประกอบด้านบุคลากรเป็นสิ่งที่อาจจะไม่สามารถคาดการณ์ได้ในสถานการณ์วิกฤตจึงไม่ควรมองข้ามในการพัฒนา BCP พนักงานและครอบครัวของพนักงานอาจได้รับผลกระทบอย่างรุนแรงเท่ากับหรือมากกว่าสถาบันการเงินได้รับ ดังนั้น ผู้บริหารสถาบันการเงินควรพิจารณาผลกระทบของเหตุการณ์ความเสียหายที่มีต่อพนักงานที่สถาบันการเงินจะต้องพึ่งพาอาศัยในช่วงเกิดวิกฤต ตัวอย่างเช่น การจัดหาที่พักและบริการให้แก่ครอบครัวพนักงาน หรือการทำให้มั่นใจว่าสถานที่ทำงานสำรองอยู่ใกล้ที่อยู่ของพนักงานเพื่อให้การปฏิบัติตาม BCP ทำได้ง่ายขึ้น นอกจากนั้น การฝึกอบรมพนักงาน การสลับหน้าที่งาน และการวางแผนการสืบทอดงานมีความสำคัญเท่า ๆ กับขั้นตอนปฏิบัติในการสำรองอุปกรณ์ ข้อมูล ระบบปฏิบัติงานและโปรแกรมระบบงาน

ภาคผนวกนี้ จะกล่าวถึงภัยคุกคามภายในและภายนอก 3 ประเภทหลัก ซึ่งประกอบด้วย การกระทำที่มุ่งประสงค์ร้าย ภัยธรรมชาติ และความเสียหายที่เกิดจากเทคโนโลยี

1. การกระทำที่มุ่งประสงค์ร้าย

1.1 การทุจริต การลักขโมย หรือการขู่จะเผยความลับ

เนื่องจากบุคคลภายในองค์กรมีช่องทางที่จะทำการทุจริต การลักขโมย หรือการขู่จะเผยความลับได้ง่ายกว่าบุคคลภายนอก ดังนั้น สถาบันการเงินจึงควรมีโครงการที่กระตุ้นให้พนักงานตระหนักถึงเรื่องดังกล่าวและนโยบายรักษาความปลอดภัยของคอมพิวเตอร์ ทั้งนี้ภัยคุกคามดังกล่าวอาจเป็นสาเหตุให้ข้อมูลสูญหาย ขาดความถูกต้องเชื่อถือได้ หรือขาดความพร้อมใช้ ซึ่งอาจส่งผลเสียหายต่อการให้บริการลูกค้าได้ ดังนั้นการจำกัดการเข้าถึงข้อมูลที่อาจถูกเปลี่ยนแปลงหรืออยู่ในสภาพที่ไม่เหมาะสมต่อการใช้งานจะสามารถลดความเสี่ยงได้ สถาบันการเงินอาจมีข้อผูกพันสำหรับการเปิดเผยข้อมูลสำคัญหรือข้อมูลลับของลูกค้า ดังนั้นจึงควรจัดให้มีขั้นตอนการปฏิบัติที่เหมาะสมในการป้องกัน ข้อมูลดังกล่าว

1.2 การก่อวินาศกรรม

บุคลากรควรทราบวิธีการจัดการกับสถานการณ์ที่มีผู้บุกรุก การขู่วางระเบิดและการก่อกวนรูปแบบอื่น ๆ สถาบันการเงินไม่ควรเปิดเผยที่ตั้งของศูนย์ปฏิบัติงานสำคัญต่อสาธารณชนและไม่ควรจัดวางอุปกรณ์เครื่องอำนวยความสะดวกต่าง ๆ ให้เป็นจุดเด่นหรือไม่มีการปกปิดมิดชิด พนักงานที่ไม่พอใจอาจพยายามดำเนินการใด ๆ ที่ทำให้สถานที่ อุปกรณ์ เครื่องอำนวยความสะดวก หรือแฟ้มข้อมูลเกิดความเสียหายได้ ดังนั้นนโยบายด้านบุคลากรควรกำหนดให้มีการย้ายพนักงานที่คิดว่าจะเป็นภัยต่อ องค์กรออกจากสถานที่ทันที รวมทั้งการยกเลิกสิทธิของพนักงานคนนั้นในการเข้าถึงเครื่องคอมพิวเตอร์และอุปกรณ์เครื่องอำนวยความสะดวกทันทีด้วยการใช้ประตูล็อคได้ การติดตั้งเครื่องตรวจจับความเคลื่อนไหว การให้มีพนักงานรักษาความปลอดภัย และการใช้เครื่องมือควบคุมอื่น ๆ ที่จำกัดการเข้าถึงทางกายภาพ ล้วนเป็นมาตรการการป้องกันที่สำคัญ

1.3 การก่อการร้าย

ความเสี่ยงจากการก่อการร้ายเป็นสิ่งที่เกิดขึ้นจริงและการวางแผนอย่างเพียงพอเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับช่วงที่เกิดเหตุการณ์การก่อการร้าย เป็นสิ่งสำคัญสำหรับสถาบันการเงิน ถึงแม้ว่าการก่อการร้ายบางรูปแบบ (เช่น การระบาดของเชื้อโรค การแพร่กระจายของสารเคมี) ไม่ทำอันตรายกับอุปกรณ์ก็ตาม แต่อาจทำให้ไม่สามารถเข้าถึงอุปกรณ์นั้นเป็นเวลานาน หากสถาบันการเงินสามารถตรวจจับการโจมตีได้เร็วเท่าไร ก็ยิ่งเพิ่มโอกาสที่การแก้ไขหรือทำให้กลับสู่สภาวะปกติประสบผลสำเร็จมากขึ้นเท่านั้น นอกจากนั้นควรมีการเฝ้าติดตามระบบเตือนภัยฉุกเฉินของทางการด้วย

การก่อการร้ายไม่ใช่สิ่งใหม่แต่ขนาดของความเสียหายและการทำลายล้างทวีความรุนแรงมากขึ้น การสูญเสียของชีวิตรวมทั้งการทำลายสิ่งอำนวยความสะดวก อุปกรณ์ ความสะเทือนใจและหวาดกลัวของนักงานจัดเป็นความเสียหายที่รุนแรงอย่างหนึ่ง ความเสียหายจากการสู้รบอาจก่อให้เกิดการสูญเสียช่องทางการสื่อสาร ไฟฟ้า และช่องทางการเข้าถึงเขตพื้นที่ที่ไม่ได้รับผลกระทบโดยตรง

การโจมตีของผู้ก่อการร้ายอาจเป็นได้ตั้งแต่การระเบิดเครื่องอำนวยความสะดวก การโจมตีทางคอมพิวเตอร์ ทางระบบการสื่อสาร ไฟฟ้า หรือโครงสร้างพื้นฐานของสถาบันการเงิน เป้าหมายของ การก่อการร้ายทางคอมพิวเตอร์ คือการทำลายการทำงานของระบบสารสนเทศและการสื่อสาร การโจมตีสมัยใหม่อาจใช้สารเคมี ชีวภาพ หรือวัตถุนิวเคลียร์ การก่อการร้ายด้วยอาวุธ

ชีวภาพ อาจใช้สารที่มีเชื้อแบคทีเรียหรือไวรัส ซึ่งผลกระทบยังไม่เกิดขึ้นในทันที จึงทำให้การป้องกัน การตอบโต้และการแก้ไขสถานการณ์ประสบปัญหา ถึงแม้ว่าการโจมตีด้วยนิวเคลียร์อย่างเต็มรูปแบบยังมีความเป็นไปได้น้อยที่จะเกิดขึ้น แต่สถาบันการเงินก็ควรหามาตราการเตรียมความพร้อมเพื่อรับมือต่อเหตุการณ์ที่โรงงานพลังงานนิวเคลียร์และอุตสาหกรรมที่ใช้วัตถุนิวเคลียร์ถูกโจมตี รวมทั้งสำหรับการโจมตีที่เกิดจากการใช้ Dirty Nuclear Device คืออาวุธที่รวมสารระเบิดทั่วไปกับสารกัมมันตภาพรังสีเข้าด้วยกัน

2. ความเสียหายจากภัยธรรมชาติ

2.1 อัคคีภัย

อัคคีภัยอาจนำไปสู่การสูญเสียชีวิต อุปกรณ์ และข้อมูล บุคคลในศูนย์ข้อมูลต้องทราบสิ่งที่ต้องปฏิบัติหากเกิดเพลิงไหม้ขึ้นเพื่อลดความเสี่ยงของการสูญเสียดังกล่าวให้เหลือน้อยที่สุด ควรมีการติดประกาศแนวทางการปฏิบัติและแผนการอพยพตามสถานที่ที่มองเห็นได้ชัดเจน และควรระบุถึงสถานที่นัดหมายนอกอาคารเพื่อที่บุคลากรจะไปรวมตัวกันในกรณีฉุกเฉินและแนวทางสำหรับการรักษาความปลอดภัยหรือการโยกย้ายสื่อบันทึกข้อมูล ในกรณีที่มีเวลาพอจะดำเนินการ นอกจากนั้นควรจัดให้มีการซ้อมหนีไฟเป็นประจำเพื่อให้มั่นใจว่าบุคลากรเข้าใจหน้าที่รับผิดชอบของตน ตู้สัญญานเตือนภัยและสวิทซ์ไฟฉุกเฉินควรติดตั้งอยู่ในจุดที่มองเห็นได้ชัดและไม่ถูกบัง

นอกจากนั้น ควรมีการติดตั้งเครื่องตรวจจับความร้อนและควันที่อุปกรณ์หลักและสำรองทั้งหมด แท้จริงแล้ว เครื่องตรวจดังกล่าวควรติดตั้งไว้บนเพดาน ช่องทางระบายอากาศ ใต้พื้นที่ยกระดับ เครื่องตรวจจับที่ติดตั้งไว้ใกล้เครื่องปรับอากาศหรือช่องดูดอากาศที่ขวางการก่อควันอาจไม่ส่งสัญญาณเตือนภัย การปิดไฟฟ้าฉุกเฉินควรหยุดการทำงานของระบบเครื่องปรับอากาศด้วย กำแพง ประตู ฉากกั้นและพื้นควรใช้วัสดุทนไฟ นอกจากนั้นอาคารและอุปกรณ์ควรจะต่อสายดินเพื่อป้องกันไฟฟ้ารั่ว ฟ้าผ่าสามารถเป็นเหตุให้เกิดเพลิงไหม้อาคารได้ ดังนั้นจึงควรติดตั้งสายล่อฟ้าให้เหมาะสมและการตรวจตราเพื่อป้องกันเพลิงไหม้ในสถานที่เป็นครั้งคราว สามารถนำมาใช้ในการเตรียมการและอบรมได้ด้วย

ตามกฎระเบียบของรัฐบาลในเรื่องการควบคุมการทำลายโอโซน ทำให้ระบบดับไฟด้วยสารฮาลอนถูกทดแทนด้วยระบบดับไฟแบบอื่น ระบบปัจจุบันใช้สารที่ไม่ก่อให้เกิดอันตราย

และรวมถึงการใช้สาร Intergen FM-200 , FE-13 และคาร์บอนไดออกไซด์ นอกจากนั้นควรใช้ระบบการฉีดพ่นตามท่อด้วยระบบ (Dry pipe sprinkler) ที่จะทำงานเมื่อตรวจจับได้ว่ามีเพลิงไหม้และจะเติมน้ำในท่อเมื่อต้องการ ดังนั้นจึงลดความเสี่ยงของการเกิดท่อน้ำระเบิด ระบบดังกล่าวควรมีลักษณะการทำงานที่เป็นลำดับขั้นตอน กล่าวคือหลังจากที่เครื่องตรวจจับได้ว่ามีเพลิงไหม้ จะให้เวลาเจ้าหน้าที่ดูแลระบบดำเนินการก่อนที่จะดับไฟฟ้า หรือปล่อยน้ำยาดับไฟ บุคลากรควรทราบวิธีที่จะรับมือกับระบบดับไฟอัตโนมัติและสถานที่และการทำงานของระบบไฟฟ้าและวาล์วปิดอื่น ๆ สิ่งปกคลุมกันน้ำได้ควรจัดวางไว้ใกล้อุปกรณ์ที่จะเสียหายง่ายในกรณีที่หัวฉีดน้ำทำงาน อุปกรณ์ดับเพลิงและอุปกรณ์ที่ใช้ดึงยกแผ่นพื้นควรจัดวางอยู่ในจุดที่เข้าถึงได้ง่ายและในตำแหน่งที่ชัดเจน ขอบเขตของการป้องกันอัคคีภัยขึ้นอยู่กับระดับความเสี่ยงที่สถาบันการเงินยอมรับได้และหลักปฏิบัติหรือกฎระเบียบของส่วนราชการท้องถิ่นนั้น

2.2 น้ำท่วมและความเสียหายจากน้ำรูปแบบอื่น

สถาบันการเงินที่มีสถานที่ปฏิบัติงานตั้งอยู่ในหรือใกล้พื้นที่น้ำท่วมถึง จะมีความเสี่ยงเพิ่มขึ้นและควรดำเนินการใด ๆ ที่จำเป็นเพื่อบริหารจัดการกับระดับความเสี่ยงดังกล่าว ในขณะที่น้ำท่วมมาถึงระดับชั้นล่างสุด ข้อมูลและอุปกรณ์สำคัญควรจะเก็บไว้ในชั้นที่สูงขึ้น อาจเป็นการช่วยลดความเสี่ยงได้ การยกระดับของพื้นหรือยกสายและอุปกรณ์ Server เหนือพื้นหลาย ๆ นิ้วฟุต สามารถช่วยป้องกันหรือจำกัดความเสียหายจากน้ำได้ นอกจากนั้นสถาบันการเงินควรตระหนักถึงความเสียหายจากน้ำที่อาจเกิดจากสาเหตุอื่น เช่น ท่อน้ำหลัก หน้าต่าง หรือระบบสปริงเกอร์แตก เป็นต้น และถ้ามีชั้นบนเหนือห้องคอมพิวเตอร์หรือห้องเก็บอุปกรณ์ เพดานของห้องก็ควรจะฉาบปิด เพื่อป้องกันความเสียหายจากน้ำ สถาบันการเงินอาจใช้เครื่องตรวจจับระดับน้ำเพื่อใช้ในการแจ้งปัญหาด้วยก็ได้

2.3 สภาพอากาศที่รุนแรง

สภาพภูมิประเทศจะเป็นตัวกำหนดถึงความเป็นไปได้ของการเกิดความเสียหายจากแผ่นดินไหว พายุเฮอริเคน ทอร์นาโด หรือสภาพอากาศที่รุนแรง เนื่องจากการเกิดภัยธรรมชาติมีลักษณะเชิงสุ่ม ดังนั้นสถาบันการเงินที่ตั้งอยู่ในพื้นที่ที่เคยประสบเหตุการณ์ดังกล่าวควรพิจารณากระบวนการวางแผนการดำเนินงานธุรกิจอย่างต่อเนื่องให้ครอบคลุมเหตุการณ์จำลองเหล่านี้อย่าง

เหมาะสม ในกรณีที่มีการใช้ระบบสัญญาณเตือนภัยล่วงหน้าผู้บริหารควรจัดให้มีขั้นตอนการปฏิบัติงานก่อนเกิดเหตุการณ์ความเสียหายเพื่อให้เกิดความเสียหายน้อยที่สุด

2.4 มลพิษในอากาศ

ภัยธรรมชาติบางอย่างก่อให้เกิดปัญหาที่สองตามมาคือปัญหามลพิษทางอากาศในเขตพื้นที่นั้นเช่น ปัญหาน้ำท่วมยังจะส่งผลให้เกิดเชื้อราหรือโรคติดต่ออื่น ๆ หลังจากที่ระดับลดลง ความรุนแรงของมลพิษอาจส่งผลกระทบต่อคุณภาพของอากาศในพื้นที่ของสถาบันการเงิน ซึ่งอาจถึงกับต้องมีการอพยพออกไปจากสถานที่เป็นระยะเวลานาน ดังนั้นการวางแผนการดำเนินธุรกิจอย่างต่อเนื่องควรพิจารณาความเป็นไปได้ของมลภาวะเป็นพิษในอากาศและจัดทำแผนการอพยพและการปิดระบบ ทำความร้อนระบายอากาศและปิดอากาศ เพื่อให้เกิดความเสี่ยงจากมลภาวะเป็นพิษน้อยที่สุด นอกจากนั้นควรพิจารณาปัจจัยในเรื่องระยะเวลาที่อุปกรณ์เครื่องอำนวยความสะดวกที่ได้รับผลกระทบ อาจไม่ทำงานหรือเข้าถึงไม่ได้

2.5 อันตรายจากสารเคมีรั่วไหล

สถาบันการเงินบางแห่ง มีสถานที่ปฏิบัติตั้งอยู่ใกล้กับโรงงานเคมี ทางรถไฟ ทางหลวงที่ใช้ขนส่งสารเคมีอันตราย การรั่วไหลของสารเคมีอาจทำให้เกิดมลพิษทางอากาศ ดังที่กล่าวมาแล้วข้างต้น รวมถึงไฟไหม้จากสารเคมี และความเสี่ยงต่อสุขภาพ สถาบันการเงินควรดำเนินการอย่างสมเหตุ สมผลเพื่อให้ทราบถึงประเภทของสารเคมีที่กำลังมีการผลิตหรือขนส่งใกล้กับสถาบันการเงิน และรับทราบข้อมูลเกี่ยวกับความเสี่ยงที่อาจเกิดขึ้น รวมทั้งดำเนินการเพื่อลดความเสี่ยงเหล่านั้น

3. ความเสียหายทางด้านเทคนิค

3.1 ระบบการสื่อสารล้มเหลว

ลักษณะการประมวลผลแบบกระจายศูนย์ทำให้ต้องอาศัยระบบเครือข่ายสื่อสารมากยิ่งขึ้น เพื่อใช้ในการสื่อสารเสียงและข้อมูลกับลูกค้า องค์กรภายนอกและศูนย์คอมพิวเตอร์สำรอง สถาบันการเงินที่ไม่ได้กระจายโครงสร้างระบบสื่อสารอาจมีความเสี่ยงต่อการเกิดจุดรวม

ความล้มเหลว หากเหตุการณ์ความเสียหายที่เกิดขึ้นส่งผลกระทบต่อระบบงานสำคัญหนึ่งระบบหรือมากกว่านั้น

สถาบันการเงินควรระบุและจัดทำเอกสารเกี่ยวกับจุดรวมความล้มเหลวที่อาจเกิดขึ้นกับระบบสื่อสารภายในและภายนอก ถ้ามีการใช้ระบบการสื่อสารของผู้ให้บริการหลายรายเพื่อกระจายเส้นทางการสื่อสาร ทำให้เกิดการสำรองซึ่งกันและกันเป็นการลดความเสี่ยง ผู้บริหารก็ควรดำเนินการระบุจุดที่อาจทำให้เกิดความล้มเหลวภายในระบบเหล่านั้น เทคนิคหนึ่งที่ใช้ก็คือการไล่จากจุดหนึ่งไปจุดหนึ่งในวงจรที่สำคัญหรือล่อแหลมเพื่อค้นหาจุดรวมความล้มเหลว เช่น Common Switch Router , PBX หรือชุมสายโทรศัพท์ของสำนักงาน

นอกจากการเชื่อมต่อสายสื่อสารข้อมูลกลับคืนกับบริษัทในเครือและผู้ให้บริการแล้ว การเชื่อมต่อระบบการสื่อสารกลับคืนกับพนักงานให้อยู่ในสภาพที่ใช้การได้เป็นปกติ เป็นสิ่งที่จะต้องมีการระบุไว้ใน BCP ทางเลือกหนึ่งของการใช้สายส่งสัญญาณเสียงภาคพื้นดิน คือการใช้โทรศัพท์ไร้สาย วิทยุสื่อสาร เพจเจอร์ E-mail สาธารณะ และการสื่อสารข้อความทางอินเตอร์เน็ต อีกทางเลือกหนึ่งคือการจดทะเบียนและสร้างหน้าข่าวสารบนเครือข่ายอินเตอร์เน็ต ที่สามารถใช้ในระหว่างเกิดเหตุการณ์ความเสียหายได้ ซึ่งสถาบันการเงินสามารถใช้เป็นช่องทางการสื่อสารข้อมูลและสั่งการพนักงาน ลูกค้าและ/หรือบริษัทในเครือ การใช้โทรศัพท์ผ่านดาวเทียมอาจเป็นประโยชน์ต่อการใช้เป็นช่องทางการสื่อสารกับบุคคลสำคัญ แต่ทั้งนี้ขึ้นอยู่กับความต้องการของแต่ละองค์กร

3.2 ระบบไฟฟ้าล้มเหลว

การสูญเสียไฟฟ้าเกิดขึ้นได้จากหลายสาเหตุอันประกอบด้วย พายุ ไฟไหม้ การกระทำของผู้ประสงค์ร้าย ไฟตกและไฟดับจากการที่ระบบจ่ายไฟล้มเหลว ระบบไฟฟ้าล้มเหลวอาจทำให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ ระบบทำความร้อน ความเย็นและแสงสว่าง รวมทั้งระบบการป้องกัน และการรักษาความปลอดภัย นอกจากนี้ระดับกระแสไฟฟ้าที่เพิ่มขึ้นทันทีซึ่งอาจเกิดขึ้นตอนช่วงไฟมา โดยหากไม่มีการวางแผนที่เหมาะสมแล้ว ก็จะทำให้อุปกรณ์ได้รับความเสียหายได้ การควบคุมความเสี่ยงดังกล่าว สามารถทำได้โดยการติดตั้งเครื่องวัดแรงดันไฟฟ้าและควบคุมแรงดันไฟฟ้า ที่ใช้เลี้ยงห้องคอมพิวเตอร์เพื่อป้องกันกระแสไฟฟ้าผันผวน ในเหตุการณ์ที่ระบบไฟฟ้าล้มเหลว สถาบันการเงินควรใช้แหล่งพลังงานสำรอง เช่น เครื่องจ่ายไฟฟ้าฉุกเฉิน (UPS) แก๊สโซลีน น้ำมันก๊าด ก๊าซธรรมชาติ หรือเครื่องกำเนิดไฟฟ้าดีเซล เป็นต้น UPS เป็นชุดแบตเตอรี่สำรองที่ให้พลังงานสำหรับช่วงระยะเวลาสั้น ๆ ในการเลือก UPS สถาบันการเงินควร

พิจารณาที่กำลังความสามารถของ UPS ในการรองรับการปิดระบบได้นานพอที่จะมั่นใจได้ว่าข้อมูลจะไม่สูญหายหรือเสียหาย อุปกรณ์ UPS บางอย่างสามารถปิดระบบโดยอัตโนมัติได้โดยไม่ต้องอาศัยคน

ถ้าระยะเวลาที่ใช้การประมวลผลมีความสำคัญมาก องค์กรอาจจัดเตรียมเครื่องกำเนิดไฟฟ้าที่จะจ่ายไฟฟ้าได้อย่างน้อยที่สุดให้กับอุปกรณ์สำคัญให้ทำงานต่อไปได้ในช่วงที่ไม่มีไฟฟ้า ผู้บริหารควรจัดให้มีการเก็บเชื้อเพลิงในปริมาณที่มากเพียงพอประจำ ณ สถานที่ที่สถาบันการเงินจัดเตรียมไว้ และดำเนินการจัดการเติมเชื้อเพลิงให้เต็ม ข้อดีประการหนึ่งของก๊าซธรรมชาติคือการใช้ท่อส่งก๊าซ ทำให้ไม่ต้องมีการบรรทุกขนส่งและเก็บถังก๊าซไว้ประจำที่สถาบันการเงิน เหตุการณ์ความเสียหายบางอย่างมีความรุนแรงมาก จนอาจส่งผลให้สถาบันการเงินไม่สามารถได้รับเชื้อเพลิงเพิ่มเติมได้และระบบผลิตและจัดส่งเชื้อเพลิงอาจไม่ทำงาน

สถาบันการเงินจำเป็นที่จะต้องมั่นใจว่าได้จัดให้มีการบำรุงรักษาและทดสอบแหล่งพลังงานสำรองเป็นประจำ นอกจากนั้นผู้บริหารควรหารือกับหน่วยงานราชการท้องถิ่นถึงกฎระเบียบเกี่ยวกับที่ตั้งของเครื่องกำเนิดพลังงานรวมทั้งการจัดเก็บและจัดส่งเชื้อเพลิง

3.3 อุปกรณ์และชุดโปรแกรมระบบงาน (Software) เสียหาย

อุปกรณ์และชุดโปรแกรมระบบงาน (Software) เสียหาย อาจส่งผลให้เกิดความล่าช้าในการประมวลผลและ/หรือ การนำ BCP ของส่วนธุรกิจต่าง ๆ ไปปฏิบัติขึ้นอยู่กับความรุนแรงของความเสียหาย การป้องกันโดยการบำรุงรักษาเป็นการเพิ่มความน่าเชื่อถือของระบบทางหนึ่ง ซึ่งควรนำไปใช้กับอุปกรณ์สนับสนุนอื่น ๆ เช่น ระบบควบคุมอุณหภูมิและความชื้น อุปกรณ์ตรวจจับหรือเตือนภัย เป็นต้น

3.4 ระบบการขนส่งเสียหาย

สถาบันการเงินจะไม่ควรตั้งสมมติว่าระบบการขนส่งระดับภูมิภาคหรือประเทศจะยังคงใช้ได้ตามปกติในช่วงที่เกิดเหตุการณ์ความเสียหายภัยธรรมชาติหรือความเสียหายทางเทคนิค การกระทำมุ่งประสงค์ร้าย การหยุดทำงานของพนักงาน หรืออุบัติเหตุ อาจทำให้การจราจรทางอากาศและ/หรือทางรถไฟหยุดหยุดชะงักลงได้ สิ่งเหล่านี้ อาจส่งผลกระทบต่อการชำระเงิน การหักบัญชีเช็คและการโยกย้ายพนักงานไปปฏิบัติที่ศูนย์คอมพิวเตอร์สำรองสถาบันการเงินควรสำรวจหาทางเลือกของการใช้บริการขนส่งภาคพื้นดินของบริษัทเอกชน (เช่น บริการเดินเอกสาร บริษัทบรรทุกขนส่ง (Trucking Companies) บริษัทรถประจำทาง) เพื่อให้มั่นใจว่าจะสามารถปฏิบัติงานสำคัญเหล่านี้ได้อย่างต่อเนื่อง

ภาคผนวก ค : การพึ่งพาอาศัยกัน

1. โครงสร้างพื้นฐานของระบบสื่อสารโทรคมนาคม

การสื่อสารในรูปของข้อมูลและเสียงมีความจำเป็นต่อการดำเนินธุรกิจและการเชื่อมโยงองค์ประกอบที่สำคัญต่าง ๆ ของสถาบันการเงินเข้าด้วยกัน ซึ่งได้แก่ ส่วนธุรกิจ ลูกค้า ผู้จำหน่ายและ/หรือให้บริการ ความก้าวหน้าทางเทคโนโลยีด้านเครือข่ายสื่อสารทำให้บุคคลและทรัพยากรระบบและ/หรือศูนย์ประมวลผลหลักและสำรอง สามารถอยู่แยกกันคนละสถานที่ที่มีความห่างไกลกันมากขึ้นได้ เทคโนโลยีเครือข่ายสื่อสารมีบทบาทสำคัญในการทำให้เกิดสภาพแวดล้อมการประมวลผลแบบกระจาย ที่ต้องอาศัยระบบเครือข่ายสื่อสาร โทรคมนาคมข้อมูลและเสียงมากยิ่งขึ้น เนื่องจากความสำคัญดังกล่าว สถาบันการเงินจึงจำเป็นที่จะต้องออกแบบโครงสร้างพื้นฐานของระบบการสื่อสารข้อมูลและเสียงให้สามารถปฏิบัติงาน ทดแทนกันได้และมีความสามารถในการกลับสู่สภาพการทำงานปกติสูง นอกจากนั้น การดำเนินการให้มีการสำรองการเชื่อมโยงของระบบสื่อสาร โทรคมนาคมข้อมูลและเสียงที่มีประสิทธิผล มีความสำคัญต่อสถาบันการเงินมากเท่า ๆ กับการจัดให้มีการดำเนินธุรกิจอย่างต่อเนื่องสำหรับศูนย์ประมวลผล และเนื่องจากโครงสร้างพื้นฐานของข้อมูลและเสียงมักเป็นทรัพยากรที่มีการใช้งานร่วมกันระหว่างส่วนธุรกิจต่าง ๆ ของสถาบันการเงิน ดังนั้นประเด็นเรื่องการพึ่งพาและความสำคัญของทรัพยากรเหล่านั้นจะได้นำมากล่าวในรายละเอียดต่อไป

โครงสร้างพื้นฐานของระบบสื่อสาร โทรคมนาคมมีจุดรวมมักมีจุดรวมที่สร้างความเสียหายให้กับระบบสื่อสาร โทรคมนาคม (single points of failure) ซึ่งถือเป็นจุดอ่อนและความเสี่ยงต่อสถาบันการเงิน องค์ประกอบของความเสี่ยงฝังอยู่ภายในโครงสร้างพื้นฐานเครือข่ายสื่อสาร โทรคมนาคมสาธารณะและอยู่นอกเหนือการควบคุมของสถาบันการเงินแต่ละแห่ง ด้วยเหตุนี้ สถาบันการเงินจึงจำเป็นต้องมีความกระตือรือร้นในการสร้างกระบวนการที่แข็งแกร่งเพื่อให้มั่นใจถึงความหลากหลายและความสามารถในการกลับสู่สภาพการทำงานปกติ สถาบันการเงินจำเป็นต้องพัฒนาวิธีปฏิบัติในการบริหารความเสี่ยงเพื่อระบุและกำจัดจุดรวมความเสียหาย ที่มีอยู่ในโครงสร้างพื้นฐานของระบบเครือข่ายของตน นอกจากนั้น กลยุทธ์ในการบริหารความเสี่ยงจำเป็นต้องถูกรวมเข้าไว้ในกระบวนการตั้งแต่ขั้นตอนการออกแบบ การจัดหา การปฏิบัติและการ

บำรุงรักษาระบบเครือข่ายสื่อสาร โดยควรระบุถึงจุดรวมความเสียหาย หรือจุดร่วมที่เกี่ยวข้องกับสิ่งต่อไปนี้

- โครงสร้างพื้นฐานของระบบเครือข่ายสื่อสารหลักและสำรอง
- สื่อที่ใช้ในการสื่อสารโทรคมนาคม
- ทางเข้าถึงสิ่งอำนวยความสะดวกต่าง ๆ
- เส้นทางการสื่อสารโทรคมนาคมระหว่างสำนักงานส่วนกลาง
- ตู้ชุมสายโทรศัพท์ภายในสถาบันการเงิน

สถาบันการเงินควรมีสัมพันธภาพกับผู้ให้บริการระบบสื่อสารโทรคมนาคมอย่างใกล้ชิด เพื่อให้การบริหารความเสี่ยงมีประสิทธิผลมากยิ่งขึ้น ในการประสานงานกับผู้จำหน่าย ผู้บริหารควรมีความมั่นใจว่ากลยุทธ์ในการบริหารความเสี่ยง มีลักษณะดังต่อไปนี้ เป็นอย่างน้อย

- จัดทำข้อตกลงเกี่ยวกับระดับการให้บริการที่ครอบคลุมมาตรการฉุกเฉินและการบริหารการเปลี่ยนแปลงสำหรับบริการที่ให้แก่สถาบันการเงิน
- สร้างกระบวนการจัดเก็บและตรวจสอบความถูกต้องของวงจรในระบบสื่อสารโทรคมนาคมและเส้นทางการสื่อสาร
- ครอบคลุมกรอบแนวทางในการตรวจสอบเส้นทางที่ใช้ในการสื่อสารโทรคมนาคมเป็นประจำ

นอกจากวิธีปฏิบัติในการบริหารความเสี่ยงที่แข็งแกร่งแล้ว สถาบันการเงินควรจัดให้มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับบริการทางข้อมูลและสามารถใช้ปฏิบัติได้ แผนการสื่อสารโทรคมนาคมอย่างน้อยควรครอบคลุมเรื่องทรัพยากรบุคคล การเชื่อมโยงภายในและภายนอก สื่อที่ใช้ในการสื่อสาร ระบบการบริหารเครือข่ายสื่อสารโทรคมนาคมและอุปกรณ์เครือข่าย BCP ควรกำหนดลำดับความสำคัญและระบุองค์ประกอบของเครือข่ายที่สำคัญ นอกจากนั้นควรพิจารณาองค์ประกอบพื้นฐานของแผน ซึ่งประกอบด้วย ความน่าเชื่อถือ ความยืดหยุ่น และความสอดคล้อง ในการจัดทำแผนสำรองด้วย ตัวอย่างเช่น โมเด็มสำรองอาจให้บริการได้ไม่ถึงระดับที่ต้องการ หรือสายสื่อสารอาจใช้ส่ง ข้อมูลในรูปเสียงได้ในระดับที่น่าพอใจเท่านั้น แต่ยังไม่มีคุณภาพและความเร็วเพียงพอสำหรับใช้ในการส่งข้อมูล ค่าใช้จ่ายของทางเลือกในการสำรองควรพิจารณาเทียบกับระดับของการป้องกันความเสี่ยงของทางเลือกนั้น ๆ การประเมินดังกล่าวควรครอบคลุมค่าใช้จ่ายที่เกี่ยวข้องกับการทดสอบด้วย เนื่องจากองค์ประกอบของแผนทุกองค์ประกอบ ซึ่งหมายรวมถึงสื่อที่ใช้ในการสื่อสาร ควรได้รับการทดสอบเป็นประจำ

BCP ควรระบุถึงความเป็นไปได้ในการใช้งานของแต่ละองค์ประกอบ แนวทางที่เลือกควรมีความสามารถรองรับปริมาณงานได้ตามที่มุ่งหวังไว้หรือมีความสามารถในการทำงานที่ความเร็วเพียงพอต่อการปฏิบัติงานให้ทันตามลำดับความสำคัญที่กำหนด ตัวอย่างเช่น สายโทรศัพท์แบบหมุนหมายเลขทั้งหลายอาจไม่สามารถใช้ทดแทนสาย T-1 ได้ นอกจากนั้น แผนสำรองควรตระหนักถึงเรื่องความพร้อมใช้งานและช่วงเวลารอที่แต่ละองค์ประกอบต้องใช้ในการทำงาน เช่น การติดตั้งสายสื่อสาร โมเด็มและอุปกรณ์การส่งสัญญาณเชิงซ้อน/อุปกรณ์รวมกลุ่มเพิ่มเติมที่ศูนย์คอมพิวเตอร์สำรอง

สถาบันการเงินที่มีบทบาทหลักในระบบการเงิน ควรตระหนักถึงโครงการและหน่วยงานของภาครัฐที่ทำหน้าที่ประสานงานและเร่งการทำให้ระบบกลับคืนสู่ภาวะปกติหรือการจัดหาบริการสื่อสารโทรคมนาคมในช่วงเกิดเหตุการณ์ฉุกเฉินทำได้เร็วขึ้น

BCP ควรพิจารณาเรื่องการรักษาความปลอดภัยของส่วนประกอบสำรองเพื่อให้มั่นใจในความถูกต้องเชื่อถือได้ของข้อมูล การสลับจากการใช้เส้นใยนำแสง (Fiber Optics) ไปเป็นสายเกลียวคู่ (wire pairs) หรือการสลับการใช้คู่สายเฉพาะราย (Dedicated line) ไปเป็นคู่สายสลับ (Switched line) หรือการเปลี่ยนจากระบบดิจิตัล (digital) ไปเป็นแอนะล็อก (analog) อาจทำให้ล่อแหลมต่อการถูกลอบดักจับข้อมูลหรือมีสัญญาณรบกวน ซึ่งอาจก่อให้เกิดความผิดพลาดตามมาได้ การใช้สายโทรศัพท์แบบเรียกหมายเลข (dial-up lines) อาจทำให้การเข้าถึงจากสาธารณะทำได้ง่ายขึ้น นอกจากนั้น อุปกรณ์สำรองควรได้รับการตรวจสอบถึงความสามารถในการเข้ารหัสด้วย

ความสัมพันธ์ระหว่างระบบงานที่ประมวลผลและระดับการพึ่งพาระบบสื่อสารโทรคมนาคมของสถาบันการเงินจะเป็นตัวกำหนดระดับของการสำรองที่จำเป็น ผู้บริหารควรระมัดระวังในการประเมินข้อกำหนดในการสำรองระบบสื่อสารโทรคมนาคม ตัดสินใจใช้แผนที่มีประสิทธิผล จัดทำรายละเอียดของขั้นตอนปฏิบัติ และทดสอบความมีประสิทธิผลของแผนเป็นครั้งคราว

2. ผู้ให้บริการภายนอก ผู้จัดหาหลัก และพันธมิตรทางธุรกิจ

การพึ่งพาผู้ให้บริการภายนอก ผู้จัดหาหลัก หรือพันธมิตรทางธุรกิจอาจนำสถาบันการเงินไปสู่ความล้มเหลว ซึ่งอาจเป็นผลให้ไม่สามารถกู้การดำเนินงานกลับสู่ภาวะปกติได้ทันเวลา ความเสี่ยงจากการใช้บริการภายนอกด้านข้อมูล การประมวลผลรายการ และการชำระรายการ

ประกอบด้วยภัยคุกคามต่อการรักษาความปลอดภัย ความพร้อมใช้งาน และความถูกต้องเชื่อถือได้ของระบบและทรัพยากร และภัยคุกคามต่อการรักษาความลับของข้อมูล รวมทั้งภัยคุกคามต่อการปฏิบัติตามกฎระเบียบของทางการ นอกจากนั้น การที่ผู้ให้บริการภายนอกให้บริการในนามสถาบันการเงิน เป็นการเพิ่มระดับความเสี่ยงด้านเครดิต สภาพคล่อง การปฏิบัติงาน และชื่อเสียงของสถาบันการเงิน สถาบัน การเงินควรสอบทานและทำความเข้าใจ BCP ของผู้ให้บริการ และมั่นใจว่าบริการสำคัญจะสามารถได้รับการกู้กลับคืนสู่ภาวะปกติภายในกรอบระยะเวลาที่ยอมรับได้โดย

- สัญญาควรระบุถึงความรับผิดชอบของผู้ให้บริการในการบำรุงรักษาและทดสอบแผนฉุกเฉินและแผนธุรกิจกลับคืนสู่ภาวะปกติ
- สถาบันการเงินควรได้รับผลการทดสอบและสอบทานรายงานการตรวจสอบเพื่อพิจารณาความเพียงพอของแผน และประสิทธิผลของกระบวนการทดสอบ
- หากเป็นไปได้ สถาบันการเงินควรเข้าไปมีส่วนร่วมในกระบวนการทดสอบของผู้ให้บริการด้วย
- สัญญาควรมีรายละเอียดของกรอบระยะเวลาที่ใช้ในการกู้ธุรกิจกลับคืนสู่ภาวะปกติที่เป็นไปตามความต้องการในการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของสถาบันการเงิน
- กระบวนการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของสถาบันการเงินควรครอบคลุมการจัดทำรายชื่อพร้อมหมายเลขโทรศัพท์ที่จำเป็นสำหรับการติดต่อเจ้าหน้าที่หลักที่ศูนย์ประมวลผลหลักและศูนย์คอมพิวเตอร์สำรองของผู้ให้บริการ
- นอกจากนั้น BCP ของสถาบันการเงินควรระบุวิธีที่สถาบันการเงินจะใช้ในการแลกเปลี่ยนข้อมูลกับผู้ให้บริการ หากสถาบันการเงินต้องไปปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรอง เช่นการส่งข้อมูลไปให้ผู้ให้บริการโดยใช้อุปกรณ์ของสาขา

3. สัญญาการใช้บริการ

สถาบันการเงินหลายแห่งทำสัญญากับผู้ให้บริการภายนอกและผู้ขายอื่น ๆ ที่จะให้ความช่วยเหลือในการกู้การดำเนินงานกลับคืนสู่ภาวะปกติ สำหรับสถาบันการเงินขนาดเล็ก การจัดการดังกล่าวอาจไม่คุ้มกับค่าใช้จ่ายเนื่องจากค่าใช้จ่ายในการบำรุงรักษาศูนย์คอมพิวเตอร์สำรอง

อาจมีจำนวนมากจนเป็นนัยสำคัญ หากสถาบันการเงินต้องการจัดทำสัญญากับผู้ให้บริการภายนอกสำหรับบริการกู้การดำเนินงานกลับสู่ภาวะปกติ นั้น มีข้อที่ควรพิจารณาดังนี้

- กลุ่มพนักงานผู้ให้บริการควรจัดให้มีบุคลากรที่ให้การสนับสนุนด้านเทคนิคประเภทใดอยู่ประจำที่ศูนย์คอมพิวเตอร์สำรอง เพื่อช่วยเหลือพนักงานของสถาบันการเงินในการปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรอง

- เวลาที่สามารถใช้ในการประมวลผลได้ สมมติว่ามีผู้ใช้บริการรายอื่นกำลังใช้งานศูนย์คอมพิวเตอร์สำรองในเวลาเดียวกัน สถาบันการเงินจะได้รับสิทธิในการใช้ระบบคอมพิวเตอร์ในการประมวลผลเป็นเวลานานเท่าใด และสถาบันการเงินได้รับการประกันเรื่องความเพียงพอของเวลาที่ใช้ในการประมวลผลเพื่อรองรับระดับปริมาณงานที่ต้องทำให้เสร็จที่ศูนย์คอมพิวเตอร์สำรองหรือไม่

- สิทธิในการเข้าถึงระบบและข้อมูล เนื่องจากศูนย์คอมพิวเตอร์สำรองส่วนใหญ่อาจมีการใช้งานร่วมกันกับลูกค้าจำนวนมาก สถาบันการเงินได้รับการประกันสิทธิที่จะใช้งานศูนย์เมื่อเกิดเหตุฉุกเฉินหรือไม่ หรือในอีกทางหนึ่งผู้ให้บริการให้บริการลูกค้าแบบ ใครมาก่อนได้รับบริการก่อน จนกว่าศูนย์คอมพิวเตอร์สำรองจะสามารถดำเนินการได้เต็มความสามารถหรือไม่

- มีการติดตั้งอุปกรณ์ Hardware and Software ที่สถาบันการเงินจำเป็นต้องใช้ในการปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรองหรือไม่ สถาบันการเงินจะได้รับแจ้งถึงการเปลี่ยนแปลงเกี่ยวกับอุปกรณ์ที่ศูนย์คอมพิวเตอร์สำรองหรือไม่

- การควบคุมการรักษาความปลอดภัย ศูนย์คอมพิวเตอร์สำรองมีการรักษาความปลอดภัยด้าน physical และ logical อย่างเพียงพอ ในการป้องกันสารสนเทศของสถาบันการเงินหรือไม่

- การทดสอบสัญญาของผู้ให้บริการ อนุญาตให้สถาบันการเงินทำการทดสอบศูนย์คอมพิวเตอร์สำรองในลักษณะเต็มรูปแบบอย่างน้อยปีละครั้งหรือไม่ ผู้ให้บริการดำเนินการทดสอบ BCP ของตนเอง และส่งผลการทดสอบให้สถาบันการเงินที่เป็นลูกค้าหรือไม่

- การรักษาความลับของข้อมูล ในกรณีที่มีธุรกิจอื่นใช้งานที่ศูนย์คอมพิวเตอร์สำรองด้วยนั้น ผู้ให้บริการมีขั้นตอนการดำเนินงานอย่างไรที่จะรักษาความลับของข้อมูลของสถาบันการเงิน

- การสื่อสารโทรคมนาคม ผู้ให้บริการมีขั้นตอนการปฏิบัติงานที่เหมาะสมที่จะมั่นใจได้ว่าศูนย์สำรองจัดให้มีบริการสื่อสารโทรคมนาคม (ทั้งด้านเสียงและข้อมูล) อย่างเพียง

พอที่จะรองรับจำนวนบุคลากรที่จะไปปฏิบัติงานที่ศูนย์คอมพิวเตอร์ และปริมาณการส่งข้อมูลตามที่คาดการณ์ไว้ หรือไม่

- ข้อตกลงในการแลกเปลี่ยนบริการซึ่งกันและกัน (Reciprocal Agreements) ในกรณีที่ศูนย์คอมพิวเตอร์สำรองของสถาบันการเงินเป็นสถาบันการเงินอื่นที่ได้ทำข้อตกลงในการแลกเปลี่ยนบริการซึ่งกันและกันไว้ ระบบคอมพิวเตอร์ของสถาบันการเงินที่จะไปใช้บริการนั้นมีความสามารถเพียงพอหรือไม่ ที่จะมั่นใจได้ว่างานของสถาบันการเงินที่ได้รับผลกระทบจะได้รับการดำเนินการแล้วเสร็จ อุปกรณ์ Hardware และ Software ที่ศูนย์คอมพิวเตอร์สำรองสอดคล้องกับระบบของสถาบันการเงินที่ได้รับผลกระทบหรือไม่ สถาบันการเงินจะได้รับแจ้งถึงการเปลี่ยนแปลงเกี่ยวกับอุปกรณ์ที่ศูนย์คอมพิวเตอร์สำรองหรือไม่

- พื้นที่ศูนย์คอมพิวเตอร์สำรองได้จัดหาพื้นที่และบริการที่เกี่ยวข้องอย่างเพียงพอที่สามารถรองรับบุคลากรของสถาบันการเงินที่ได้รับผลกระทบ และทำให้บุคคลเหล่านั้นสามารถดำเนินธุรกิจได้หรือไม่ ทั้งนี้อาจหมายรวมถึงการพิจารณาพื้นที่ ณ สถานที่ของผู้ให้บริการหรือในชุมชนท้องถิ่นเพื่ออำนวยความสะดวกในเรื่องอาหาร ห้องน้ำ ยารักษาโรค การดูแลครอบครัว การให้คำปรึกษาข่าวสาร การจัดหาที่พักอาศัยและสันทนาการให้แก่บุคลากร

- แฟ้มงานและแบบฟอร์มของเอกสารศูนย์คอมพิวเตอร์สำรองจัดเตรียมแฟ้มงานและแบบฟอร์มในรูปกระดาษในปริมาณที่จำเป็นต่อการดำเนินธุรกิจของสถาบันการเงินที่ได้รับผลกระทบอย่างเพียงพอหรือไม่

- สมรรถภาพและความสามารถในการให้บริการงานพิมพ์ศูนย์คอมพิวเตอร์สำรองมี สมรรถภาพในการให้บริการงานพิมพ์ที่เพียงพอต่อความต้องการของสถาบันการเงินที่ได้รับผลกระทบ หรือไม่

- การติดต่อประสานงานบุคลากรของสถาบันการเงินคนใดที่ได้รับมอบหมายให้เป็นผู้ตัดสินใจใช้ศูนย์คอมพิวเตอร์สำรอง และใครจะเป็นผู้ติดต่อกับศูนย์คอมพิวเตอร์สำรอง

ภาคผนวก ง : องค์ประกอบของแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

1. บุคลากร

เมื่อพิจารณาจากการวิเคราะห์ผลกระทบต่อธุรกิจเป็นหลัก BCP ควรกำหนดความรับผิดชอบของผู้บริหาร บุคลากรที่เกี่ยวข้อง ทีมงาน และผู้ให้บริการ โดยระบุตัวบุคลากรหลักที่จำเป็นต่อการนำแผนไปปฏิบัติให้ประสบผลสำเร็จและพัฒนาแนวทางปฏิบัติฉุกเฉินสำหรับกรณีที่บุคลากรดังกล่าวไม่สามารถปฏิบัติงานได้ นอกจากนี้ ควรระบุสิ่งที่จำเป็นต้องได้รับการสนับสนุนจากผู้ให้บริการด้วย นั้นคือ BCP ควรครอบคลุมเรื่องดังต่อไปนี้

- การกำหนดการรับช่วงหน้าที่ในการตัดสินใจ ในกรณีที่มีการสูญเสียบุคลากรระดับบริหาร
- ใครจะเป็นผู้นำทีม BCP ต่าง ๆ (เช่น วิกฤตการณ์/ ภาวะฉุกเฉิน การกู้ธุรกิจกลับคืนสู่ภาวะปกติ เทคโนโลยีการสื่อสาร สิ่งอำนวยความสะดวก ทรัพยากรบุคคล ส่วนธุรกิจและกระบวนการดำเนินงาน และบริการลูกค้า)
- ใครจะเป็นผู้ติดต่อกับผู้ให้บริการ ผู้จำหน่าย หรือ ผู้จัดหาบริการ
- ใครจะเป็นผู้รับผิดชอบต่อการรักษาความปลอดภัย (ทางด้านข้อมูลและทางกายภาพ)

การวางแผนควรพิจารณาเรื่องทรัพยากรบุคคลที่จำเป็นสำหรับการตัดสินใจและการปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรองภายใต้สถานการณ์ต่าง ๆ อีกทั้งควรมีการระบุตัวบุคคลหลักที่ทำหน้าที่ตัดสินใจเกี่ยวกับแนวทางที่จะใช้ในการปรับปรุง ซ่อมแซม หรือ สร้างสิ่งอำนวยความสะดวกหลักขึ้นมาใหม่ ซึ่งอาจต้องใช้บุคลากรมากกว่าที่จำเป็นต้องใช้สำหรับการดำเนินธุรกิจอย่างต่อเนื่อง

ผู้ประสานงานในการวางแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และ/หรือ คณะกรรมการวางแผนควรรับผิดชอบในการปรับปรุง BCP เป็นประจำอย่างน้อยปีละครั้ง และเมื่อมีการเปลี่ยนแปลงการปฏิบัติงานและสภาพแวดล้อมที่สำคัญ

2. องค์ประกอบของเทคโนโลยี (Technology Components)

BCP ที่มีประสิทธิผล ควรระบุองค์ประกอบของเทคโนโลยีที่จำเป็นดังต่อไปนี้

- Hardware เช่น Mainframe, Network และ End User
- Software เช่น โปรแกรมระบบงาน ระบบปฏิบัติการ และโปรแกรมอรรถประโยชน์
- การสื่อสาร เช่น ระบบเครือข่าย และระบบสื่อสารโทรคมนาคม
- แฟ้มข้อมูล และกลุ่มข้อมูลที่สำคัญ (Vital records)
- อุปกรณ์ที่ใช้ในการประมวลผลการปฏิบัติงาน
- อุปกรณ์สำนักงาน

การจัดทำทะเบียนทรัพย์สินที่ครอบคลุมอย่างกว้างขวางจะเป็นประโยชน์ต่อการกู้ธุรกิจกลับคืนสู่ภาวะปกติ อีกทั้งยังทำให้มั่นใจได้ว่าทุกองค์ประกอบจะได้รับการพิจารณาในช่วงระหว่างการพัฒนาแผน การวางแผนควรครอบคลุมถึงการระบุข้อมูลสำคัญของส่วนธุรกิจที่เก็บอยู่ในเครื่องคอมพิวเตอร์ (Workstation) ของเจ้าหน้าที่แต่ละคนในส่วนงานนั้น ซึ่งอาจจะไม่ได้มีการสำรองข้อมูลตามตารางเวลา การสำรองที่เหมาะสม นอกจากนี้ แผนควรระบุถึง Record ของข้อมูลที่สำคัญ วิธีการสำรองที่จำเป็น และตารางเวลาที่เหมาะสมในการสำรองข้อมูลสำคัญเหล่านั้นด้วย

สถาบันการเงินควรดำเนินการด้วยความระมัดระวังในการกำหนดทรัพย์สินประเภทที่ไม่มีนัยสำคัญ ในภาวะที่ระบบทำงานได้ตามปกติ ธนาคารทางโทรศัพท์ (Internet Banking) หรือระบบ ATM อาจจะเหมือนไม่ใช่ระบบงานสำคัญ อย่างไรก็ตามระบบงานเหล่านี้อาจจะกลายมามีบทบาทสำคัญใน BCP และอาจเป็นช่องทางหลักที่ใช้ให้บริการลูกค้าในช่วงที่เกิดเหตุการณ์ความเสียหาย ในทำนองเดียวกันระบบ Electronic Mail อาจจะไม่ใช่ระบบหลักที่ใช้ในการดำเนินธุรกิจ แต่ก็อาจเป็นเพียงระบบเดียวที่จะใช้ติดต่อสื่อสารกับพนักงานและภายนอกได้ในช่วงที่เกิดเหตุการณ์ความเสียหาย

2.1 ทางเลือกในการกู้ศูนย์ประมวลผลกลาง

สถาบันการเงินควรดำเนินการอย่างเป็นทางการในการจัดเตรียมความสามารถในการประมวลผลสำรองเพื่อรองรับในกรณีที่ศูนย์ประมวลผลกลางไม่สามารถใช้งานได้หรือเข้าถึงไม่ได้ การเลือกใช้ประเภทของแนวทางในการกู้ศูนย์ประมวลผลกลางแบบใด จะขึ้นอยู่กับ

ความสำคัญของกระบวนการดำเนินธุรกิจที่กำลังกู้กลับคืนสู่ภาวะปกติรวมทั้งเป้าหมายด้านระยะเวลาที่ใช้ในการกู้ธุรกิจ ทางเลือกของแผนการกู้กลับคืนสู่ภาวะปกติ (Recovery Plan) อาจเป็นได้ในหลายรูปแบบและอาจเกี่ยวข้องกับการใช้ศูนย์ประมวลผลอื่นหรือการให้ผู้ให้บริการภายนอกดำเนินการจัดตั้งศูนย์คอมพิวเตอร์สำรองให้ ข้อตกลงหรือสัญญาตามกฎหมายกับบริษัทผู้ให้บริการ ควรมีความชัดเจนในเรื่องการเตรียมการสำหรับการทำให้ศูนย์ประมวลผลกลางกลับคืนสู่ภาวะปกติ ในที่นี้จะขอกล่าวถึงทางเลือกในการกู้ศูนย์ประมวลผลกลางซึ่งเป็นที่ยอมรับ อย่างไรก็ตามสถาบันการเงินจะต้องสามารถอธิบายเหตุผลของการเลือกใช้ แนวทาง รวมทั้งทำไมถึงพิจารณาว่าแนวทางที่เลือกมีความเหมาะสมกับขนาดและความซับซ้อนของสถาบันการเงิน

- Hot site (Traditional “active/backup” model) ศูนย์คอมพิวเตอร์สำรองที่มีลักษณะเป็น Hot Site จะมีการติดตั้งอุปกรณ์คอมพิวเตอร์ที่สอดคล้องกับศูนย์คอมพิวเตอร์หลักและโดยมากจะสามารถใช้ปฏิบัติงานได้นานหลายชั่วโมงสถาบันการเงินหลายแห่งอาจใช้บริการศูนย์คอมพิวเตอร์สำรองจากบุคคลภายนอก การสำรองรูปแบบนี้ กำหนดให้ต้องมีการโอนย้ายพนักงานหลักไปที่ศูนย์คอมพิวเตอร์สำรองเป็นอย่างน้อย นอกจากนั้นยังกำหนดให้ต้องมีการโอนย้ายสื่อบันทึกข้อมูลสำรองไปเก็บไว้นอกสถานที่อย่างน้อยทุกวัน สถาบันการเงินขนาดใหญ่ที่มีการประมวลผลแบบ real time หรือมีรายการประมวลผลจำนวนมาก ควรจะพิจารณาใช้การสำรองในลักษณะ Mirroring หรือ Vaulting ถ้าสถาบันการเงินใช้บริการศูนย์ Hot Site ของผู้ให้บริการภายนอก อาจมีความเสี่ยงที่ความสามารถของศูนย์ของผู้ให้บริการอาจไม่เพียงพอที่จะให้การสนับสนุนการปฏิบัติงานในกรณีที่เกิดเหตุการณ์ความเสียหายขนาดใหญ่หรือในระดับภูมิภาคได้ สถาบันการเงินขนาดเล็กที่มีความซับซ้อนน้อยกว่าอาจทำสัญญาการขอใช้บริการศูนย์ Mobile Hot Site เช่น ตู้รถเคลื่อนที่ที่ติดตั้งอุปกรณ์คอมพิวเตอร์ที่จำเป็น โดยสามารถลากไปตั้งไว้ ณ สถานที่ที่กำหนดเมื่อเกิดเหตุการณ์ความเสียหายและต่อเชื่อมกับเครื่องจ่ายไฟฟ้า (Power Source)

- Duplicate Facilities/Split Operations (“active/active” model) ภายใต้สถานการณ์นี้จะมี Active Site 2 แห่งหรือมากกว่า ทำหน้าที่เป็นศูนย์คอมพิวเตอร์สำรองซึ่งกันและกัน ซึ่งแต่ละศูนย์คอมพิวเตอร์สำรอง มีความสามารถที่จะรองรับงานบางส่วนหรือทั้งหมดของศูนย์คอมพิวเตอร์ อีกแห่งสำหรับช่วงระยะเวลาหนึ่งได้ ด้วยกลยุทธ์นี้การดำเนินธุรกิจสามารถกลับคืนสู่ภาวะปกติได้ทันที แต่ก็ขึ้นอยู่กับระบบที่ใช้ในการสนับสนุนการปฏิบัติงานและความสามารถในการปฏิบัติงานของแต่ละศูนย์ด้วย การที่แต่ละศูนย์ต้องดำรงความสามารถส่วนเกินและมีความซับซ้อนในการปฏิบัติงานเพิ่มขึ้น อาจก่อให้เกิดค่าใช้จ่ายสูงอย่างมีนัยสำคัญ ข้อจำกัดของ

เทคโนโลยีปัจจุบันบางอย่าง เช่น เทคโนโลยีการสำรองแบบ Real time Synchronous data mirroring อาจเป็นอุปสรรคต่อการกระจายศูนย์คอมพิวเตอร์ให้อยู่คนละสถานที่ที่ห่างไกลกัน อย่างไรก็ตาม อาจมีทางเลือกการสำรองอื่น นอกเหนือจากการทำ Synchronous Mirroring ที่จะทำให้ศูนย์สามารถตั้งอยู่คนละสถานที่ที่ห่างไกลกันมากขึ้นได้

- Cold site เป็นสถานที่ที่เป็นส่วนหนึ่งของกลยุทธ์ในการกู้ธุรกิจกลับคืนสู่ภาวะปกติระยะยาวเป็นการจัดหาสถานที่สำรอง ซึ่งไม่มีการติดตั้งอุปกรณ์คอมพิวเตอร์ แต่มีการติดตั้งระบบ ไฟฟ้า เครื่องปรับอากาศ เครื่องทำความร้อน อุปกรณ์อิเล็กทรอนิกส์ ระบบเครือข่ายสื่อสาร สายโทรศัพท์ และพื้นยกระดับ ตัวอย่างของสถานการณ์มีการใช้งาน Cold site คือเมื่อสถาบันการเงินสามารถดำเนินธุรกิจกลับสู่ภาวะปกติที่ศูนย์คอมพิวเตอร์สำรองอีกแห่ง เช่น Hot site ได้ แต่ยังมีความจำเป็นต้องใช้สถานที่ต่อไปอีกในระหว่างที่กำลังสร้างศูนย์ประมวลผลกลางขึ้นมาใหม่ Cold site มักจะต้องใช้เวลาหลายสัปดาห์ในการทำให้อยู่ในสภาพที่ใช้ปฏิบัติงานได้ สถาบันการเงินอาจว่าจ้างผู้ให้บริการภายนอกจัดหาศูนย์ Cold Site ให้ หรืออาจใช้สถานที่อีกแห่ง เช่นสาขาหรือศูนย์ปฏิบัติการอื่น เป็นศูนย์ Cold Site

- Tertiary Location สถาบันการเงินบางแห่งกำหนดให้มีสถานที่แห่งที่สามหรือการสำรองข้อมูลสำรองอีกที Tertiary Location เป็นการเพิ่มระดับการป้องกันในกรณีที่ทั้งศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองไม่สามารถใช้ปฏิบัติงานได้ นอกจากนั้น Tertiary Location จะกลายเป็นศูนย์คอมพิวเตอร์สำรองหลักในกรณีที่สถานบันการเงินประกาศภาวะฉุกเฉินและกำลังปฏิบัติงานโดยไม่มีศูนย์คอมพิวเตอร์สำรอง

สถาบันการเงินบางแห่งทำข้อตกลงที่เรียกว่า ข้อตกลงที่จะให้บริการซึ่งกันและกัน (Reciprocal Agreement) กับสถาบันการเงินอื่นในการให้บริการสำรองอุปกรณ์ การจัดการในลักษณะนี้ จะอยู่บนพื้นฐานของการปฏิบัติงานด้วยความพยายามอย่างดีที่สุด โดย สถาบันการเงิน A สัญญาที่จะเป็นศูนย์คอมพิวเตอร์สำรองให้กับสถาบันการเงิน B ตราบเท่าที่สถาบันการเงิน A มีเวลาที่จะปฏิบัติงานให้ และในทางกลับกัน ซึ่งโดยส่วนใหญ่ Reciprocal Agreement มักจะไม่เป็นที่ยอมรับ เนื่องจากสถาบันการเงินที่ตกลงจะให้บริการสำรอง มีความสามารถส่วนเกินไม่เพียงพอที่จะรองรับการประมวลผลรายการของสถาบันการเงินที่ได้รับผลกระทบได้ภายในเวลาที่เหมาะสม ถ้าสถาบันการเงินเลือกที่จะทำ Reciprocal Agreement และสามารถสร้างวิธีจัดการสำหรับการสำรองในระดับที่ยอมรับได้ สถาบันการเงินก็ควรที่จะจัดทำข้อตกลงเป็นลายลักษณ์อักษร และกำหนดข้อบังคับให้สถาบันการเงิน A จัดหาความสามารถและเวลาในการประมวลผล

อย่างเพียงพอ นอกจากนั้น ข้อตกลงควรระบุให้ชัดเจนว่าสถาบันการเงินแต่ละแห่งจะได้รับการแจ้งถึงการเปลี่ยนแปลงใด ๆ ที่เกิดกับอุปกรณ์และ Software ของสถาบันการเงินอีกแห่งหนึ่ง

2.2 สิ่งอำนวยความสะดวกในการกู้ระบบสำรอง

ศูนย์คอมพิวเตอร์สำรองควรได้รับการทดสอบอย่างน้อยปีละครั้ง และเมื่อมีการเปลี่ยนแปลงอุปกรณ์หรือโปรแกรมระบบงาน เพื่อให้มั่นใจว่าอุปกรณ์หรือโปรแกรมระบบงานที่ศูนย์คอมพิวเตอร์สำรอง มีความสอดคล้องกับของศูนย์คอมพิวเตอร์หลัก นอกจากนั้น ศูนย์คอมพิวเตอร์สำรองควรมีระดับการรักษาความปลอดภัยทางกายภาพที่มากกว่าศูนย์คอมพิวเตอร์หลัก เนื่องจาก คนและระบบที่ใช้ในการควบคุมการเข้าถึงศูนย์คอมพิวเตอร์สำรอง อาจไม่คุ้นเคยกับบุคลากรที่ถูกโอนย้ายไปปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรองนั้น ซึ่งการรักษาความปลอดภัยดังกล่าวควรครอบคลุมการควบคุมการเข้าถึงศูนย์คอมพิวเตอร์สำรองและระบบคอมพิวเตอร์ทั้งทางกายภาพและทางตรรก นอกจากนั้น ควรมีการจัดเก็บ BCP และขั้นตอนการปฏิบัติงานไว้ที่ศูนย์คอมพิวเตอร์สำรอง หรือสถานที่จัดเก็บภายนอก

ไม่ว่าจะใช้กลยุทธ์ในการกู้ระบบแบบใด แผนการกู้ระบบควรครอบคลุมถึงวิธีการกู้ รายการค้างและ/หรือรายการสูญหายให้กลับคืนมา แผนควรระบุถึงวิธีในการดึงข้อมูลรายการธุรกรรมปัจจุบันกลับคืนมาจากช่วงเวลาที่เกิดความเสียหายและประมาณการกรอบระยะเวลาที่ใช้ในการกู้คืน

ขนาดของพื้นที่ทำงานที่ศูนย์คอมพิวเตอร์สำรอง มีความสำคัญเท่า ๆ กับสมรรถภาพในการประมวลผลข้อมูล ผู้บริหารควรจัดการเตรียมสิ่งอำนวยความสะดวก พื้นที่ทำงานและอุปกรณ์สำหรับพนักงานไว้ใช้ดำเนินธุรกิจอย่างต่อเนื่อง

2.3 การกระจายพื้นที่ทางภูมิศาสตร์ (Geographic Diversity)

ในการพิจารณากำหนดสถานที่ตั้งของศูนย์คอมพิวเตอร์สำรอง ผู้บริหารควรพิจารณาเรื่อง การกระจายพื้นที่ทางภูมิศาสตร์ สถาบันการเงินควรจะพิจารณาถึงขอบเขตของพื้นที่ที่อาจได้รับความเสียหายและสัญญาณบ่งชี้การเกิดเหตุการณ์ความเสียหายในระดับจังหวัดหรือระดับภูมิภาคการกำหนดระยะห่างระหว่างศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองควรพิจารณาถึงเป้าหมายด้านระยะเวลาที่ใช้ในการกู้ธุรกิจและความต้องการของส่วนธุรกิจ หากเกิดเหตุการณ์ความเสียหายในระดับภูมิภาคแล้ว ศูนย์คอมพิวเตอร์สำรองที่ตั้งอยู่ใกล้กับศูนย์

คอมพิวเตอร์หลักมากเกินไปก็อาจได้รับความเสียหายด้วย อย่างไรก็ตามหากจัดตั้งศูนย์คอมพิวเตอร์สำรองไกลจากศูนย์คอมพิวเตอร์หลักมากเกินไป ก็อาจเป็นอุปสรรคต่อการโอนย้ายบุคลากรที่จำเป็นไปปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรองได้เช่นกัน ถ้าการเคลื่อนย้ายบุคลากรไปศูนย์คอมพิวเตอร์สำรองมีความจำเป็นต่อการทำให้ธุรกิจดำเนินไปได้อย่างต่อเนื่องแล้ว ปัจจัยที่นำมาพิจารณาก็ควรมุ่งไปที่ความเต็มใจในการเดินทางของบุคลากรเหล่านั้นในช่วงเกิดเหตุฉุกเฉิน รูปแบบการเดินทางที่จัดให้ รวมถึงที่พักและค่าครองชีพสำหรับพนักงานที่ต้องเคลื่อนย้าย (หากเป็นไปได้) ในการประเมินสถานที่ตั้งของศูนย์คอมพิวเตอร์สำรอง ควรมีการวิเคราะห์สถานการณ์ของการเกิดภัยคุกคามที่ศูนย์คอมพิวเตอร์สำรองในรูปแบบต่าง ๆ ด้วย

2.4 กลยุทธ์ในการสำรองและการจัดเก็บ (Back-up and storage strategies)

ผู้บริหารของสถาบันการเงินควรทำการตัดสินใจเกี่ยวกับการสำรองแฟ้มข้อมูลและชุดโปรแกรมระบบงาน บนพื้นฐานของความสำคัญของแฟ้มข้อมูลและชุดโปรแกรมระบบงานเหล่านั้นที่มีต่อการดำเนินงานของสถาบันการเงิน ในการกำหนดลำดับของการสำรองผู้บริหารควรพิจารณาข้อมูลทุกประเภทและผลกระทบที่อาจเกิดจากการสูญหายของแฟ้มข้อมูล ซึ่งได้แก่ ข้อมูลทางการเงิน กฎระเบียบ ข้อมูลด้านการบริหารและปฏิบัติงาน ระบบปฏิบัติการ โปรแกรมระบบงาน และโปรแกรมระบบที่ใช้ในการรักษาความปลอดภัยในการกำหนดลำดับของการสำรอง ผู้บริหารควรประเมินความเสี่ยงให้ครอบคลุมประเด็นดังต่อไปนี้

- การสูญหายของแฟ้มข้อมูลดังกล่าวจะทำให้เกิดข้อบกพร่องในการปฏิบัติงานของสถาบันหรือไม่
- แฟ้มข้อมูลดังกล่าวใช้สำหรับการบริหารทรัพย์สินขององค์กรหรือใช้ในการตัดสินใจหรือไม่
- แฟ้มข้อมูลดังกล่าวประกอบด้วยโครงสร้างระบบการรักษาความปลอดภัยและระบบปฏิบัติการที่ได้รับการปรับปรุงให้เป็นปัจจุบัน ซึ่งจำเป็นต่อการทำให้การดำเนินงานกลับสู่ภาวะปกติได้อย่างปลอดภัยหรือไม่
- การสูญเสียแฟ้มข้อมูลดังกล่าวส่งผลต่อการสูญเสียรายได้หรือไม่
- ข้อผิดพลาดหรือการสูญหายของข้อมูล จะส่งผลกระทบอย่างมีนัยสำคัญการเงิน (ชื่อเสียง) หรือลูกค้าของสถาบันการเงินหรือไม่

ความถี่ของการสำรองแฟ้มข้อมูลขึ้นอยู่กับความสำคัญของโปรแกรมระบบงาน และ ข้อมูล ควรมีการสำรองข้อมูลสำคัญด้วยวิธีการจัดทำแฟ้มข้อมูลไว้หลายรุ่น (เช่น "รุ่นปู่-รุ่นพ่อ-รุ่นลูก" เป็นต้น) และหมุนเวียนออกไปเก็บนอกสถานที่อย่างน้อยทุกวัน ระบบที่เป็น Online real time หรือระบบที่มีปริมาณงานมากอาจจำเป็นต้องใช้วิธีสำรองที่แข็งขันมากขึ้น เช่นการทำ mirroring หรือการทำ electronic vaulting ที่ศูนย์คอมพิวเตอร์อีกแห่ง เพื่อให้มั่นใจว่ามีการสำรองการปฏิบัติงานที่เหมาะสม ซึ่งเป็นอีกทางเลือกหนึ่งแทนการจัดเก็บเทปบันทึกข้อมูลสำรอง

สถานที่เก็บเทปบันทึกข้อมูลสำรอง ยังคงเป็นวิธีการที่สถาบันการเงินหลายแห่งใช้ อย่างไรก็ตาม หากสถาบันการเงินใช้เทปเป็นสื่อในการสำรองข้อมูล ควรจัดส่งเทปบันทึกข้อมูลสำรองดังกล่าวไปเก็บนอกสถานที่โดยเร็วที่สุดเท่าที่จะทำได้ และไม่ควรเก็บไว้ข้ามคืนในสถานที่ที่จัดทำเทปสำรองดังกล่าว สื่อที่ใช้ในการสำรองโดยเฉพาะเทป ควรจะได้รับการทดสอบเป็นประจำ เพื่อให้มั่นใจว่ายังสามารถอ่านข้อมูลในเทปได้ เมื่อเวลาผ่านไป เทปที่มีการใช้ซ้ำ ๆ หรืออยู่ในอุณหภูมิหรือความชื้นที่ แปรปรวน อาจไม่สามารถใช้อ่านข้อมูลทั้งหมดหรือบางส่วนที่เก็บอยู่ในเทปได้

การบันทึกจากระยะไกล คือกระบวนการบันทึกทะเบียนทางคอมพิวเตอร์ของธุรกรรมหรือรายการประจำวันจากระยะไกล ซึ่งทะเบียนทางคอมพิวเตอร์และรายการดังกล่าวจะถูกนำไปใช้ในการกู้รายการและการเปลี่ยนแปลงใด ๆ กับฐานข้อมูลที่เกิดขึ้นตั้งแต่การสำรองครั้งล่าสุดให้กลับคืนมา

สถาบันการเงินควรสำรองชุดโปรแกรมระบบปฏิบัติการและโปรแกรมระบบงานทุกครั้งเมื่อมีการเปลี่ยนแปลงแก้ไขหรือมีการปรับปรุงให้เป็นปัจจุบัน

2.5 การสำรองแฟ้มข้อมูล (Data File Backup)

องค์ประกอบที่สำคัญที่สุดอย่างหนึ่งของกระบวนการสำรองจะเกี่ยวข้องกับแฟ้มข้อมูลของสถาบันการเงินโดยไม่คำนึงถึง Platform ที่ใช้เก็บข้อมูล สถาบันการเงินจำต้องสามารถสร้างแฟ้มข้อมูลหลักล่าสุด ที่มีรายการจนถึง ณ เวลาที่เกิดเหตุการณ์ความเสียหาย ควรมีการสำรองแฟ้มข้อมูลทั้งในและนอกสถานที่เพื่อให้มีความสามารถในการกู้ข้อมูลกลับคืน ระยะเวลาการเก็บแฟ้มข้อมูลปัจจุบันหรือแฟ้มข้อมูลหลักในอดีตและแฟ้มรายการประจำวันที่จำเป็นต้องใช้ในการเรียกข้อมูลปัจจุบันขึ้นมา มีความสำคัญต่อการทำให้การประมวลผลสามารถดำเนินต่อไปได้ในช่วงที่เกิดเหตุการณ์ความเสียหาย การสร้างหรือการหมุนเวียนแฟ้มข้อมูล

ประมวลผลหลัก ควรจะดำเนินการอย่างน้อยทุกวันหรือบ่อยขึ้นตามความเหมาะสมกับปริมาณรายการที่ประมวลผลหรือรายการทาง Online แฟ้มข้อมูลที่มีความสำคัญรองลงมาอาจจะไม่จำเป็นต้องสำรองบ่อยครั้ง และไม่ว่าจะเป็นกรณีใดก็ตามควรนำแฟ้มข้อมูลสำรอง ไปเก็บนอกสถานที่ในเวลาที่เหมาะสม และจะไม่นำกลับมาจนกว่าจะมีแฟ้มข้อมูลสำรองชุดใหม่ถูกนำไปเก็บแทน

2.6 การสำรอง Software (Software Back Up)

การสำรอง Software สำหรับทุก Platform ของ Hardware ประกอบด้วยพื้นฐาน 3 อย่างคือ 1.Software ระบบปฏิบัติการ (Operating software) 2.Software ระบบงาน (Application software) และ 3.Software อรรถประโยชน์ (Utility software) สถาบันการเงินควรจัดหาสถานที่ภายนอก เพื่อจัดเก็บ software และเอกสารที่เกี่ยวข้องทั้งหมดอย่างเพียงพอ ถึงแม้ว่าสถาบันการเงินจะใช้ชุด software ที่มาตรฐานจากผู้จำหน่ายรายหนึ่งก็ตาม software ที่ติดตั้งอยู่คนละแห่งก็อาจมีลักษณะแตกต่างกันออกไปได้ ซึ่งความแตกต่างดังกล่าว ได้แก่ การเปลี่ยนแปลงและการตั้งค่าพารามิเตอร์ รายละเอียดของการรักษาความปลอดภัย ทางเลือกในการจัดทำรายงาน ข้อมูลของบัญชีผู้ใช้ หรือการกำหนดทางเลือกอื่น ๆ ในช่วงหรือหลังจากการใช้งานระบบ ด้วยเหตุนี้การสำรองให้ครอบคลุมทุก software ที่มีความสำคัญจึงเป็นสิ่งจำเป็นที่ควรดำเนินการ

สถาบันการเงินควรสำรอง software ระบบปฏิบัติการชุดปัจจุบันอย่างน้อย 2 ชุด โดยชุดหนึ่งเก็บลงเทปและ Disk Library เพื่อให้มีความพร้อมใช้ได้ทันทีเมื่อต้นฉบับได้รับความเสียหาย ส่วนอีกชุดควรจัดเก็บไว้ที่สถานที่ภายนอกสถาบันการเงิน โดยให้มีการรักษาความปลอดภัยอย่างรัดกุม อีกทั้งควรจัดให้มีการทดสอบชุดสำรองดังกล่าวเป็นประจำและจัดทำใหม่เมื่อระบบปฏิบัติการเปลี่ยนแปลง

Softwareระบบงาน ซึ่งหมายรวมถึง Source version (ถ้ามีอยู่ในความครอบครองของสถาบันการเงิน) และ Object version ของโปรแกรมระบบงานทั้งหมด ควรมีการจัดเก็บรักษาในลักษณะเดียวกับ Software ระบบปฏิบัติการ หากมีการเปลี่ยนแปลงโปรแกรม ชุดสำรองของโปรแกรมดังกล่าวก็ควรได้รับการปรับปรุงให้เป็นปัจจุบันด้วย

การอาศัยสภาพแวดล้อมการประมวลผลแบบกระจายที่เพิ่มขึ้น เป็นเหตุให้การจัดหาทรัพยากรและขั้นตอนปฏิบัติในการสำรองสำหรับ LAN และ WAN อย่างเพียงพอ เป็นเรื่องที่

มีความสำคัญ ผู้บริหารต้องให้ความมั่นใจได้ว่าสถาบันการเงินดำเนินการสำรองทุกโปรแกรม ระบบงานและข้อมูลที่เหมาะสมไว้ครบถ้วนแล้ว

การสำรองข้อมูลจะใช้เวลาน้อยกว่าการกู้ข้อมูลกลับสู่สภาพเดิม ทั้งนี้ขึ้นอยู่กับขนาดของสถาบันการเงินรวมทั้งลักษณะและการเปิดเผยความเสี่ยงที่คาดว่าจะเกิดขึ้น การสำรองแฟ้มข้อมูลอาจใช้เวลาน้อย แต่การสร้างแฟ้มข้อมูลขึ้นมาใหม่จากเอกสารรายงาน (สมมติว่ามีข้อมูลอยู่ในรูปของเอกสารรายงาน) อาจต้องใช้เวลาเป็นวันสัปดาห์ หรือเดือนจึงจะแล้วเสร็จ ขั้นตอนปฏิบัติที่จัดทำอย่างครอบคลุมและชัดเจนเป็นสิ่งจำเป็นต่อการกู้ระบบและเครือข่ายสื่อสารสำคัญกลับคืนสู่ภาวะปกติ ซึ่งขั้นตอนปฏิบัติดังกล่าว ควรครอบคลุมเรื่องดังต่อไปนี้เป็นอย่างน้อย

- ความถี่ของรอบระยะเวลาการปรับปรุงและการจัดเก็บข้อมูลและ Software สำรอง
- การสอบทานความสอดคล้องหรือความเข้ากันได้ของ Software และ Hardware กับทรัพยากรสำรองเป็นประจำ
- การทดสอบความมีประสิทธิผลของขั้นตอนการปฏิบัติงานสำรองในการทำให้ธุรกิจกลับคืนสู่ภาวะปกติเป็นประจำ
- แนวทางในการติดป้าย จัดทำทะเบียนรายการขนส่งและจัดเก็บรักษาสื่อบันทึกข้อมูลสำรอง
- การบำรุงรักษาทะเบียน เนื้อหาและสถานที่เก็บแฟ้มข้อมูล
- การจัดทำเอกสารโครงสร้างของ Hardware, Software และระบบเครือข่ายสื่อสาร
- มาตรการควบคุมที่ใช้ในการลดความเสี่ยงที่อาจเกิดจากการโอนข้อมูลสำรอง โดยไม่ว่าจะเป็นการโอนข้อมูลทางอิเล็กทรอนิกส์หรือการส่งแผ่นดิสเก็ตและเทปไปมากับสถานที่จัดเก็บ
- มาตรการควบคุมที่ให้ความมั่นใจถึงความถูกต้องครบถ้วนเชื่อถือได้ของข้อมูล การรักษาความลับของลูกค้า และการรักษาความปลอดภัยทางกายภาพของ เอกสาร สื่อ และอุปกรณ์ Hardware

2.7 สถานที่จัดเก็บภายนอก (Off-site storage)

สถานที่จัดเก็บภายนอก ควรมีการควบคุมและการรักษาความปลอดภัยในด้านสภาพแวดล้อมด้วยการมีขั้นตอนปฏิบัติงานที่จำกัดการเข้าถึงทางกายภาพที่อนุญาตให้เฉพาะบุคคลผู้มีสิทธิเท่านั้น นอกจากนั้นสถาบันการเงินควรพิจารณาให้สถานที่ภายนอกดังกล่าวของตนอยู่ห่างไกลจากสถานที่ปฏิบัติงานคอมพิวเตอร์อย่างเพียงพอที่จะทำให้ทั้งสองแห่งจะไม่ได้รับผลกระทบจากเหตุการณ์ความเสียหายพร้อมกัน นอกจากชุดสำเนาของ BCP แล้วสถาบันการเงินควรจัดเก็บชุดสำเนาของขั้นตอนการปฏิบัติงานที่จำเป็นทั้งหมด ได้แก่ ขั้นตอนปฏิบัติงานสิ้นวัน สิ้นเดือน สิ้นไตรมาส เป็นต้น รวมทั้งขั้นตอนปฏิบัติงานที่ครอบคลุมประเด็นปัญหาที่มีโอกาสเกิดน้อยหรือมีลักษณะเฉพาะเป็นพิเศษไว้นอกสถานที่ด้วย หรืออาจพิจารณาในอีกแนวทางหนึ่ง คือ การจัดเก็บข้อมูลสำคัญไว้ใน Shared Network Drive ที่มีการรักษาความปลอดภัยอย่างรัดกุมโดยมีการสำรองข้อมูลไปพร้อมกับการสำรองระบบเครือข่ายที่ดำเนินการตามกำหนดระยะเวลาอย่างเป็นประจำ อย่างไรก็ตาม Shared Network Drive ดังกล่าว ควรอยู่คนละสถานที่เพื่อป้องกันการได้รับผลกระทบจากเหตุการณ์ความเสียหายพร้อมกัน ผู้บริหารจำเป็นที่จะต้องจัดให้มีการใช้สื่อที่ไม่ได้อาศัยระบบเครือข่าย (เช่น เอกสาร) เพื่อให้สามารถรองรับกรณีที่เกิดความเสียหายกับระบบเครือข่ายในช่วงระยะเวลาหนึ่ง

นอกจากนี้ ควรมีการจัดเก็บพัสดุสำรอง เช่น แบบฟอร์ม คู่มือ กระดาษหัวจดหมาย เป็นต้น ไว้นอกสถานที่ในปริมาณที่เหมาะสม และผู้บริหารควรดูแลการรักษาทะเบียนพัสดุให้เป็นปัจจุบันตรงกับจำนวนพัสดุสำรองที่มีอยู่จริง

3. สิ่งอำนวยความสะดวก (FACILITIES)

BCP ควรระบุถึงการโยกย้ายสถานที่ สำหรับเหตุการณ์ความเสียหายที่เกิดขึ้นในช่วงเวลาสั้น ปานกลาง และยาว ในขั้นตอนการวางแผน ควรพิจารณาเรื่องสถานที่ตั้ง ขนาด ความสามารถ (ของคอมพิวเตอร์และระบบสื่อสารโทรคมนาคม) และสิ่งอำนวยความสะดวกอื่น ๆ ที่จำเป็นต่อการทำให้ธุรกิจกลับคืนสู่ภาวะปกติได้ตามระดับของบริการที่กำหนดโดยส่วนธุรกิจสำคัญ สิ่งเหล่านี้ครอบคลุมถึงการวางแผนเรื่องพื้นที่ทำงาน โทรศัพท์ เครื่องคอมพิวเตอร์ (Workstation) การเชื่อมโยงเครือข่ายสื่อสาร เป็นต้น ในการพิจารณาศูนย์คอมพิวเตอร์สำรอง ผู้บริหารควรพิจารณาความเป็นไปได้หรือโอกาสเกิดเหตุการณ์ความเสียหายระยะยาว นอกจากนี้

ในระหว่างการดำเนินการให้ธุรกิจกลับสู่ภาวะปกติ ควรมีการประเมิน BCP อีกครั้ง เพื่อพิจารณาว่าจะต้องใช้แผนที่สามหรือไม่ ควรมีการพัฒนาขั้นตอนปฏิบัติงานเกี่ยวกับการใช้ศูนย์คอมพิวเตอร์สำรอง อีกทั้ง ควรมีการระบุแฟ้มข้อมูล งานที่ต้องนำเข้าระบบหรือแบบฟอร์มเฉพาะต่าง ๆ ไว้ในแผนที่จัดทำเป็นลายลักษณ์อักษร

นอกเหนือจากขั้นตอนในการรับพัสดุ อุปกรณ์ เช่น สื่อบันทึกข้อมูล เอกสาร พัสดุ เป็นต้น ที่จัดเก็บไว้ในสถานที่จัดเก็บภายนอกแล้ว แผนควรครอบคลุมลำดับขั้นตอนปฏิบัติ (Logistic Procedures) สำหรับการเคลื่อนย้ายบุคลากรไปที่ศูนย์คอมพิวเตอร์สำรอง รวมทั้ง อาจจำเป็นที่จะต้องมีแผนรองรับสำหรับการจัดหาที่พัก อาหาร และแนวทางการพิจารณาเรื่องครอบครัวพนักงาน

4. การสื่อสาร (COMMUNICATION)

การสื่อสารเป็นส่วนสำคัญของ BCP ซึ่งควรครอบคลุมการสื่อสารกับบุคลากรฉุกเฉิน พนักงาน ผู้อำนวยการ หน่วยงานกำกับของทางการ ผู้จำหน่ายหรือผู้ให้บริการ (ข้อมูลรายละเอียดการติดต่อ) ลูกค้า (ขั้นตอนการแจ้ง) และสื่อ (บุคคลที่ได้รับมอบหมายให้เป็นตัวแทนของสถาบันการเงินในการให้ข่าวแก่สื่อ) ช่องทางการสื่อสารสำรองที่ควรพิจารณา ได้แก่ โทรศัพท์มือถือ เพจเจอร์ โทรศัพท์ดาวเทียม และการสื่อสารโดยทางอินเตอร์เน็ต เช่น E-mail หรือการส่งข้อความเร่งด่วน

5. ข้อควรพิจารณาอื่นๆ (Other considerations)

สถาบันการเงินแต่ละแห่งมีความแตกต่างกัน และกระบวนการดำเนินธุรกิจก็แตกต่างกันออกไปด้วย อย่างไรก็ตาม ผู้บริหารควรพิจารณาวิธีการที่จะทำให้เรื่องต่อไปนี้ประสบผลสำเร็จ คือ

- การป้องกันการเกิดเหตุการณ์ฉุกเฉินและการเตรียมความพร้อมการดำเนินงานด้าน BCP
- การตรวจสอบเพื่อเปรียบเทียบเวลาที่ใช้ในการกู้ธุรกิจกลับคืนสู่ภาวะปกติกับข้อกำหนดของส่วนธุรกิจ

- การประกาศภาวะฉุกเฉิน และกระบวนการนำ BCP ออกใช้งาน
- การรายงานความคืบหน้าของการกู้ธุรกิจกลับคืนสู่ภาวะปกติ
- การทดสอบแผนงาน