บทที่ 2

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

การศึกษาแนวทางการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ กรณีศึกษา บริษัท ตรีเพชรอิซูซุเซลส์ จำกัด ซึ่งประกอบกิจการขายรถยนต์เชิงพาณิชย์ ในบทนี้ผู้วิจัยได้ศึกษาค้นคว้า เอกสาร แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง นำเสนอเป็นลำดับดังนี้

2.1 การวางแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

2.2 มาตรฐานเกี่ยวกับแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

2.3 ปัจจัยความสำเร็จในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

2.4 แนวคิดเกี่ยวกับปัจจัยความสำเร็จ

2.5 การวิเคราะห์องค์ประกอบ (Factor Analysis)

2.6 งานวิจัยที่เกี่ยวข้อง

2.7 กรอบแนวคิดในการวิจัย

2.1 การวางแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

ปัจจุบันคงปฏิเสธไม่ได้ว่าระบบคอมพิวเตอร์ได้เป็นส่วนประกอบหลักในการดำเนินธุรกิจ มีคอมพิวเตอร์เซิร์ฟเวอร์ (Server)จำนวนมากในสำนักงานซึ่งแต่ละเครื่องก็มีหน้าที่หลักของตัวเอง ถ้าเกิดปัญหากับหนึ่งในเซิร์ฟเวอร์เหล่านั้นจนทำให้เซิร์ฟเวอร์นั้นไม่สามารถใช้งานได้ ผลกระทบที่เกิดขึ้นไม่ได้เพียงกระทบต่อพนักงานที่ใช้งานเซิร์ฟเวอร์เครื่องนั้นเท่านั้นแต่เกิดกับองค์กรหรือบริษัทด้วย ยกตัวอย่างเช่น ถ้าเซิร์ฟเวอร์ที่กล่าวถึงให้บริการรับส่งอีเมล์ภายในและภายนอกองค์กร สิ่งที่เกิดขึ้นคือ พนักงานไม่สามารถส่งอีเมล์เพื่อขออนุมัติงบประมาณจากผู้บริหารได้ ฝ่ายจัดซื้อไม่สามารถยืนยันการสั่งซื้อผ่านอีเมล์ได้ ผู้บริหารพลาดไม่ได้รับอีเมล์ในการประมูลโครงการใหม่ ผลเสียอีกมากมายที่เกิดขึ้นล่วนมีผลกระทบต่อการดำเนินธุรกิจทั้งสิ้น ไม่โดยทางตรง ก็โดยทางอ้อม นี่เป็นแค่ตัวอย่างที่อาจจะเกิดขึ้นในกรณีอีเมล์เซิร์ฟเวอร์ของบริษัทล่มสลาย (Crash) แต่ถ้าเซิร์ฟเวอร์ทุกเครื่อง ข้อมูลทุกประเภทที่ในปัจจุบันเก็บอยู่ในรูปของอิเล็คทรอนิคบนระบบสารสนเทศขององค์กรเกิดการล่มสลายและไม่สามารถกู้คืนได้ จะเกิดอะไรขึ้นกับบริษัทนี้

จากเหตุการณ์ก่อการร้ายเมื่อวันที่ 11 กันยายน ค.ศ. 2001 มีบริษัทจำนวนมากต้องปิดตัวไปพร้อมกับตึกเวิร์ลเทรด โดยบริษัทจำนวนหนึ่งที่ปิดตัวไปเพราะสาเหตุมาจากไม่มีระบบฟื้นฟูจากการเกิดภัยพิบัติ ที่ดีพอ ทำให้ข้อมูลต่างๆที่มีความสำคัญต่อธุรกิจต้องสูญสลายไปกับเหตุการณ์ในครั้งนั้น แต่หนึ่งในบริษัทที่สามารถรอดพ้นภัยพิบัติในครั้งนั้นได้ บริษัท Morgan Stanley เป็นบริษัททางการเงินและหลักทรัพย์รายใหญ่แห่งหนึ่งของโลกและเป็นผู้เช่าพื้นที่ในตึกเวิร์ลเทรดรายใหญ่ที่สุด จากเหตุการในวันนั้นบริษัทสูญเสียพนักงานไปจำนวน 6 คน จากพนักงานทั้งสิน 3,700 คนที่ทำงานอยู่บนตึกในขณะนั้น แต่สิ่งที่น่าสนใจก็คือ เวลา 9:20 ในเช้าวันรุ่งขึ้น ระบบสำรองได้ถูกเปิดใช้งานที่ไซต์สำรอง (Backup site) ของ Morgan Stanley และพร้อมที่เปิดทำการซื้อขายแลกเปลี่ยนหุ้นในตลาด NASDAQ ได้ทันที แต่ในครั้งนั้นกระทรวงการคลังของสหรัฐอเมริกาได้สั่งให้ชะลอการเปิดตลาดออกไปก่อน จึงทำให้ผู้บริหารของ Morgan Stanley ตัดสินใจใช้ไซต์สำรองนั้นเป็นศูนย์ติดต่อประสานงานค้นหาผู้สูญหายแห่งชาติแทน ความพร้อมของ Morgan Stanley ในครั้งนั้นจะเกิดขึ้นไม่ได้เลยถ้าขาดการวางแผน การเตรียมการ และที่สำคัญคือการซักซ้อมอย่างสม่ำเสมอ จากเหตุการณ์นี้ทำให้ทั่วโลกรวมถึงประเทศไทย ตื่นตัวในเรื่องของการวางแผนฟื้นฟูระบบสารสนเทศจากการเกิดภัยพิบัติกันอย่างมาก (ไชยกร อภิวัฒโนกุล, 2008)

แผนฟื้นฟูจากการเกิดภัยพิบัติ หรืออาจเรียกว่า แผนการรองรับการเกิดภัยพิบัติ (Disaster Recovery Plan) เป็นแผนเพื่อรองรับการเกิดภัยพิบัติต่างๆ โดยผลศึกษาจากวรรณกรรมที่เกี่ยวข้อง ได้มีผู้ให้ความหมายไว้อย่างหลากหลาย ดังนี้

Hutt et al. (1988) ได้กล่าวไว้ว่าเป็นแผนทางด้านความปลอดภัยที่ได้เตรียมวิธีที่จะทำให้ระบบคอมพิวเตอร์ขององค์การสามารถใช้งานได้ต่อไปเมื่อองค์กรประสบกับเหตุการณ์ภัยพิบัติ

Rosenthal and Sheinink (1993) การทำแผนในการกู้คืนระบบคอมพิวเตอร์ในศูนย์คอมพิวเตอร์ (Data Center) เพื่อให้การทำงานขององค์กรดำเนินต่อไปได้

Paradine (1995) กล่าวว่า มันคือแผนการที่ถูกกำหนดไว้ก่อนเกิดภัยพิบัติ

Yiu and Tse (1995) ได้อธิบายว่าแผนการฟื้นฟูภัยพิบัติคือ กระบวนการที่จะทำให้แน่ใจได้ว่า จะสามารถกู้คืนระบบสารสนเทศในระยะเวลาที่ยอมรับได้เมื่อประสบกับภัยพิบัติ

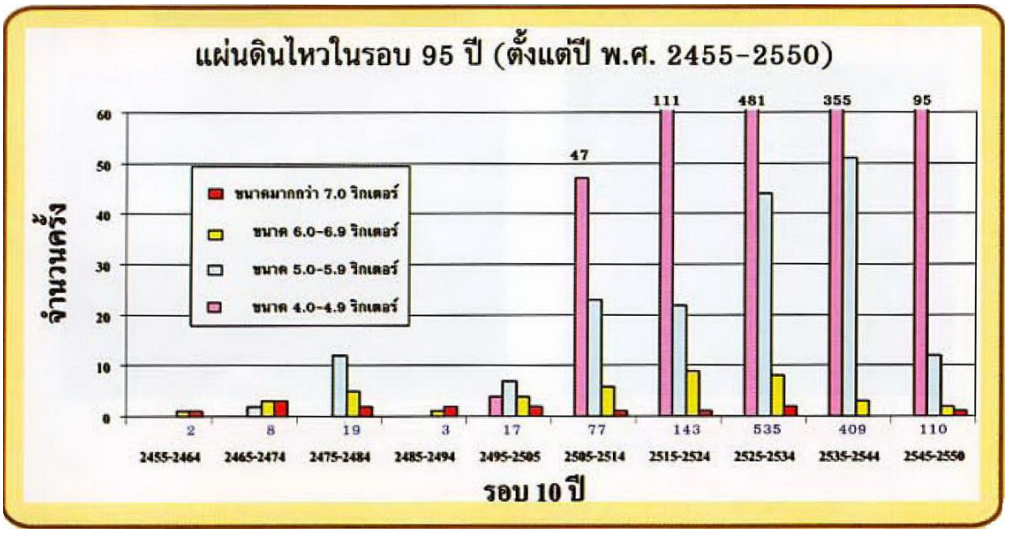
Semer (1998) กล่าวว่าสาเหตุของภัยพิบัติที่มีผลต่อระบบสารสนเทศมีดังนี้

1. ภัยธรรมชาติ (Natural Disaster) ได้แก่ อัคคีภัย อุทกภัย วาตภัย แผ่นดินไหว แผ่นดินถล่ม ฟ้าผ่า ไฟฟ้าสถิต สำหรับภัยทางธรรมชาติที่สำคัญในประเทศไทยและมีแนวโน้ม

ความรุ่นแรงเพิ่มขึ้นอย่างต่อเนื่องนั่นก็คือ แผ่นดินไหว ถึงแม้ว่าความสูญเสียจากแผ่นดินไหวในประเทศไทยมีปริมาณน้อยเมื่อเทียบกับต่างประเทศ แต่ตามข้อมูลจากกรมทรัพยากรธรณีแสดงให้เห็นว่าปริมาณการเกิดแผ่นดินไหวในประเทศไทยมีความถี่ในการเกิดเพิ่มสูงขึ้นในทุกๆปีและมีแนวโน้นความรุ่นแรงเพิ่มขึ้นด้วย

ภาพที่ 2.1

แสดงสถิติการเกิดแผ่นดินไหวในประเทศไทยในรอบ 95 ปี



ที่มา: เอกสารเผยแพร่กรมทรัพยากรธรณี “แผ่นดินไหว 6.3 ริกเตอร์ 16 พ.ค. 2550” หน้า 5

2. ความผิดปกติของซอฟท์แวร์ (Software Malfunction)

3. ความผิดปกติของฮาร์ทแวร์หรือระบบ (Hardware or System Malfunction)

4. ไฟฟ้าขัดข้อง (Power Outage)

5. คอมพิวเตอร์ไวรัส (Computer Viruses)

6. อุบัติเหตุ (Accident) ได้แก่ รถชน เครื่องบินตก ระเบิด

7. จากการกระทำของมนุษย์ (Man-Made) ได้แก่ นักเจาะระบบ (Hackers) การก่อวินาศกรรมหรือการลอบทำลายระบบ (Sabotage) และสงคราม (War)

8. จากความผิดพลาดของมนุษย์ (Human Error) เช่น การปิดคอมพิวเตอร์อย่างไม่ถูกต้อง การทำของเหลวหกใส่อุปกรณ์คอมพิวเตอร์ สะเก็ดไปจากก้นบุหรี่ เป็นต้น

ประโยชน์จากการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

การพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติเป็นการกำหนดขั้นตอนและกระบวนการต่างๆเพื่อช่วยฟื้นฟูองค์กรองค์กรจากการกู้คืนข้อมูลที่สูญเสียไปให้กลับคืนมา โดยประโยชน์จาก ขั้นตอนต่างๆในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ แบ่งได้เป็น 7 ข้อ ดังนี้ (Hawkins et al., 2000)

1. ขจัดความผิดพลาดและความสับสน (Eliminating Possible Confusion and Error) มีการกำหนดทีมงาน เพื่อรับผิดชอบกระบวนการต่างๆในการฟื้นฟูหรือกู้คืนระบบอย่างชัดเจน

2. ทำให้กระบวนการธุรกิจกลับมาดำเนินงานได้เร็วขึ้น (Reducing Disruptions to Corporate Operations) จากแผนการฟื้นฟูระบบสารสนเทศจากภัยพิบัติจะทำให้กระบวนการทางธุรกิจสามารถกลับมาให้งานได้ในระยะเวลาอันรวดเร็วหลังประสบกับภัยพิบัติ โดยเปลี่ยนการใช้งานไปยังไซต์สำรองแทน

3. มีหลายทางเลือกให้เลือกใช้ (Providing Alternatives during a Disastrous Event) ในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ มีด้วยกันหลากหลายวิธี ดังนั้นผู้บริหาระดับสูงสามารถที่จะเลือกวิธีการที่เหมาะสมกับองค์กรของตนให้มากที่สุด

4. มีผู้รับผิดชอบหลักและรอง (Reducing The Reliance on Certain Key Individuals) ในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัตินั้นจะมีการกำหนดผู้รับผิดชอบหลักและรอง หรือมากกว่าในแต่ละงาน โดยผู้รับผิดชอบทุกคนจะต้องมีความสามารถในการปฏิบัติงานนั้นๆอย่างเท่าเทียมกัน เพื่อให้งานนั้นสามารถสำเร็จไปได้ด้วยดีไม่ว่าจะเป็นใครทำ ดังนั้นงานแต่ละงานไม่ได้ขึ้นอยู่กับคนเพียงแค่คนเดียว

5. ป้องกันข้อมูลขององค์กร (Protecting The Data of The Organization) ข้อมูลถือเป็นทรัพสินประเภทหนึ่งขององค์กร ถูกจัดเก็บอยู่ในหลายรูปแบบ อาธิเช่น ฐานข้อมูล ตารางจัดการข้อมูล รูปภาพ และไฟล์เอกสาร ข้อมูลที่มีความสำคัญต่อองค์กร ยกตัวอย่างเช่น ข้อมูลลูกค้า ข้อมูลทางการเงินของบริษัท แบบฟอร์มต่างๆ ซึ่งข้อมูลเหล่านี้ถูกทำการสำรองข้อมูลแล้วเก็บอยู่ในรูปแบบต่างๆ เช่น เทปแบคอัพ (Tape Backup) หรืออยู่ในรูปของดิสค์

6. เพิ่มความมั่นใจในความปลอดภัยแก่บุคลลากร (Ensuring The Safety of Company Personnel) ในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติมีการกำหนดขั้นตอนให้พนักงานปฏิบัติ ขณะที่ระบบสารสนเทศก็ต้องทำการย้ายสถานที่ในเพื่อให้ระบบสามารถให้บริการได้อย่างต่อเนื่องหลังจากประสบภัยพิบัติ

7. ช่วยให้การฟื้นฟูมีระบบระเบียบ (Helping An Orderly Recovery) โดยแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติจะครอบคลุมปัญหาที่สามารถเกิดขึ้นระหว่างประสบภัยพิบัติ และยังเตรียมพอในด้านอุปกรณ์และทรัพยากรที่จำเป็นในการแก้ปัญหา โดยผู้บริหารจะมีการกำหนดความสำคัญของแต่ละระบบในการฟื้นฟูหรือกู้คืน เพื่อให้เกิดลำดับความสำคัญก่อนหลัง สิ่งไหนควรทำก่อน ควรทำหลัง ทำให้ไม่เกิดความสับสน

ค่าใช้จ่ายในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

การประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติให้เกิดประสิทธิภาพนั้นไม่ใช้เรื่องง่าย เนื่องจากการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติต้องอาศัยทรัพยากรขององค์กรอย่างน้อย 2 ประเภท ดังนี้

1. ต้นทุนในการเตรียมการเพื่อประยุกใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Cost of DRP Preparation) ในการเตรียมการนั้นองค์กรต้องใช้ระยะเวลาในการพิจารณาให้ได้ว่าระบบให้ที่มีความสำคัญต่อองค์กร (Mission-Critical System) ซึ่งจะเป็นระบบที่นำเข้าไปอยู่ในกระบวนการในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติต่อไป ในการเตรียมการต่างๆเหล่านี้องค์กรต้องจัดทีมงานหรือพนักงานจำนวนหนึ่งเพื่อดูแลรับผิดชอบโดยอาจใช้ระยะเวลาในขั้นตอนนี้อย่างมาก (Tremendous Amount of Man-Hours) และถ้าองค์กรตัดสินใจที่จะเลือกใช้ผู้เชียวชาญภายนอกก็จะมีค่าใช้จ่ายที่ไม่น้อยเช่นกัน ด้วยเหตุนี้ความยากหรือความท่าทายในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัตินั้นก็คือการอธิบายและโน้มน้าวให้ผู้บริการระดับสูงเข้าใจถึงความสำคัญและความจำเป็นในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ เนื่องจากผู้บริหารระดับสูงเป็นผู้พิจารณางบประมาณในการลงทุนนั่นเอง ในกรณที่องค์กรขาดความเชียวชาญในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ ทางเลือกที่ดีที่สุดคือการจ้างที่ปรึกษาภายนอก

2. ต้นทุนจากทรัพยากรขององค์กร (Cost of Corporate Resources) การประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัตินั้นจะต้องได้รับความรวมมือจากทุกๆฝ่ายภานในองค์กร ไม่ว่าจะเป็นผู้บริหารระดับสูงซึ่งต้องมีความตระหนักและให้ความสำคัญกับแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ รวมถึงการร่วมมือกันของพนักงานทุกคนในบริษัท ตลอดจนความพร้อมของเครื่องมือและสิ่งอำนวยความสะดวกที่เกี่ยวข้องกับแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

การเตรียมความพร้อมในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัตินั้น จะต้องอาศัยความร่วมมือระหว่างพนักงานภายในองค์กรและการตัดสินใจของผู้บริหารระดับสูง และเพื่อให้ได้ข้อมูลที่ครบถ้วนและสมบูรณ์มากที่สุด อาธิเช่น การประชาสัมพันธ์ในพนักงานทุกคนในองค์กรได้ตระหนักถึงความสำคัญของการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Employee Awareness) และรวมไปถึงข้อมูลทางด้านความปลอดภัยทางเทคโนโลยีและความปลอดภัยทางด้านข้อมูล (Safety of Computer Technology and Data Security) เป็นต้น โดยจะต้องอาศัยการประสานงานกันของ 3 สายงานหลักนั้นก็คือ ผู้บริหารระดับสูง (Management) สายงานสนเทศ (Information Technology) และ ทรัพยากรบุคคล (Human Resources)

ความเกี่ยวโยงของผู้บริหารระดับสูง (Management Involvement and Activities) มีดังนี้

1. ต้องมีความรู้ทางเทคโนโลยี เพื่อประโยชน์ในการสื่อสารและทำความเข้าใจกับฝ่ายสารสนเทศให้เป็นไปในทิศทางเดียวกัน

2. การเลือกบุคคลากรที่มีความเชียวชาญด้านสารสนเทศมาร่วมในการพัฒนาและดูแลแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Employing Qualified Professionals to Develop and Maintain The Company's DRP) พนักงานที่มีการทดสอบและได้ประกาศนียบัตรทางด้านสารสนเทศ (IT Certification) เช่น MCSE CCNA CCIE เป็นต้น จะเป็นการรับรองได้ว่ามีความรู้ความเข้าในระบบสารสนเทศ ซึ่งทำให้สามารถร่วมงานในการพัฒนาและดูแลแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติได้ โดยไม่ต้องเสียงบประมาณในการอบรมด้านสารสนเทศ

3. รับรองถึงความครอบคลุมของประกันอุบัติภัยของบริษัท (Ensuring Insurance coverage for LAN) โดยผู้บริหารจะสามารถรับรองได้ว่าบริษัทมีการทำประกันเพื่อคลุมครองในส่วนไหนบ้าง โดยมีส่วนที่ควรได้รับความคลุมครองจากการประกัน ได้แก่ ค่าใช้จ่ายในการกู้คืนข้อมูล ค่าชดเชยควาเสียหายของคอมพิวเตอร์เซิร์ฟเวอร์และอุปกรณ์สารสนเทศจากภัยธรรมชาติ เป็นต้น

4. จัดตั้งทีมงานเพื่อรับผิดชอบและปฏิบัติตามแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติขณะที่ประสบกับภัยพิบัติ (Organizing Specialized Respond Teams to Execute The DRP During Emergency) ในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัตินั้นจะมีทีมงานที่รับผิดชอบโดยเป็นทีมงานที่ถูกแต่งตั้งขึ้น มีดังนี้ (Semer,1998)

- ทีมผู้รับผิดชอบขั้นต้น (Initial Respond Team) เป็นทีมแรกที่มีหน้าที่ประเมินความเสียหายที่เกิดขึ้น โดยจะพิจารณาว่าระบบจะสามารถทำงานต่อไปในไซต์งานหลักหรือไม่ หรือควรจะย้ายระบบไปทำงานในสถานที่อื่น ในกรณีที่ความเสียหายรุ่นแรงมาก ทีมผู้รับผิดชอบขั้นต้นนี้จะทำการติดต่อขอความช่วยเหลือจากทีมอื่นต่อไป

- ทีมฟื้นฟูโครงสร้างหลักของระบบสารสนเทศ (Restoration Team) เป็นทีมที่มีหน้าที่ดูแลความเสียหาย และทำให้โครงสร้างหลักของระบบสารสนเทศกลับมาใช้งานได้อีกครั้ง โดยรวมถึง อุปกรณ์เน็ตเวิร์ค โครงสร้างหลักทางเน็ตเวิร์ค ไฟล์ข้อมูล ซอท์ฟแวร์ และเส้นทางการสื่อสารต่างๆ

- ทีมฟื้นฟูระบบการทำงาน (Recovery Operation Team) ในกรณีที่ทีมผู้รับผิดชอบขั้นต้นพิจารณาย้ายสถานที่การทำงานไปที่สถานที่อื่นหรือแบคอัพไซต์ ทีมฟื้นฟูระบบการทำงานจะมีหน้าที่เข้าติดตั้งและทดสอบระบบการทำงาน ณ แบคบัพไซต์ โดยรวมถึงการเชื่อมต่อโครงข่ายเน็ทเวิร์ค การเรียกข้อมูลคืนมาจากข้อมูลที่ทำการสำรองไว้ ติดตั้งฮาร์ทแวร์ เชื่อมต่อเส้นทางการสื่อสารและงานอื่นๆที่เกี่ยวข้อง

- ทีมสนับสนุนการขนย้าย (Logistics Support Team) จะเป็นทีมงานที่รับผิดชอบด้านการขนย้าย โดยในระหว่างช่วงเวลาสลับการทำงานจากไซต์งานหลักไปยังแบคอัพไซต์นั้น ทีมนี้จะช่วยในเรื่องการขนย้ายพนักงานและอาจรวมถึงครอบครัวของพนักงานด้วย

ความเกี่ยวโยงของฝ่ายเทคโนโลยีสารสนเทศ (Information Technology Involvement and Activities) มีดังนี้

1. พัฒนารูปแบบโครงข่ายเน็ทเวิร์ค (Developing a Network Blueprint) ในกรณีจำเป็นต้องมีการย้ายระบบสารสนเทศไปทำงานยังแบคอัพไซต์ โครงข่ายเน็ทเวิร์คขององค์กรต้องสามารถถูกกู้คืนกลับมาใช้งานได้อย่างรวดเร็วที่สุดเช่นกัน

2. ผลักดันให้ผู้บริการสนับสนุนการทำแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Gaining Management's Support to DRP) ผู้บริหารระดับสูงตระหนักดีถึงความเสียหายที่จะเกิดขึ้นถ้าข้อมูลที่สำคัญขององค์กรต้องหายไป ดังนั้นผู้ที่มีความเข้าใจดีทั้งในด้านเทคโนโลยีสารสนเทศและความต้องการของผู้บริหาร นั้นก็คือ ประธานฝ่ายสารสนเทศ (CIO : Chief Information Officer) ดังนั้นจึงเป็นหน้าที่ของประธานฝ่ายสารสนเทศในการแปลความหมายทางเทคโนโลยีให้อยู่ในรูปแบบภาษาในการบริหารจัดการ

3. การตรวจตราการใช้งานอินเตอร์เน็ทของพนักงาน (Monitoring Employee's Internet Access) การใช้งานอินเตอร์เน็ทเป็นอีกช่องทางที่ก่อให้เกิดภัยพิบัติต่อระบบสารสนเทศ

ขององค์กรได้ ไม่ว่าจะเป็นผู้ไม่หวังดี นักเจาะระบบ และไวรัส เป็นต้น จากโครงสร้างของอินเตอร์เน็ทที่มีความยืดหยุ่นสูงบ้างครั้งทำให้ยากในการตรวจสอบว่าข้อมูลหรือผู้บุกรุกเหล่านั้นมาจากไหน (Garfield & McKeown, 1997) ด้วยเหตุนี้ทางที่ดีที่สุดในการป้องกันผู้บุกรุกจากภายนอกระบบสารสนเทศขององค์กรคือการตรวจตราการใช้งานอินเตอร์เน็ทของพนักงานภายในอย่างรอบครอบ

4. มาตรฐานทางด้านฮาร์ทแวร์และซอฟท์แวร์ (Standardize Hardware and Software) ในบ้างองค์กรมีการใช้ฮาร์ทแวร์และซอฟท์แวร์ที่หลากหลาย ยกตัวอย่างเช่น บางแผนกใช้คอมพิวเตอร์แมคอินทอช (Macintosh) แต่ขณะเดียวกันอีกแผนกใช้คอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งเป็นการยากหรือต้องใช้เวลานานเพื่อจะกู้คืนระบบให้กับรูปแบบฮาร์ทแวร์และซอฟท์แวร์ที่หลากหลาย เพราะฉะนั้น การมีรูปแบบฮาร์ทแวร์และซอฟท์แวร์เพียงแบบเดียวจะช่วยลดเวลาและความซับซ้อนในการฟื้นฟูระบบเมื่อประสบภัยพิบัติ

5. มีการช่วยเหลือจากไอทีเวนเดอร์ที่เชื่อถือและมั่นใจได้ (Securing Support from IT Vendor) ในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติจำเป็นอย่างยิ่งที่จะต้องมีและได้นับการช่วยเหลือจากเวนเดอร์ทั้ง 2 คือ ความช่วยเหลือในด้านสารสนเทศทั่วไป เช่น การบริการหลังการขายในด้านฮาร์ทแวร์และซอฟท์เวร์ การช่วยเหลือทางด้านการติดต่อสื่อสาร และความช่วยเหลือทางด้านแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติโดยเฉพาะ โดยมีบริการต่างๆ อาธิ เช่น การกู้ข้อมูล บริการให้เช่าแบคอัพไซต์ บริการให้เช่าพื้นที่สำนักงานชั่วคราว และบริการให้เช่าฮาร์ทแวร์และอุปกรณ์ที่จำเป็นต่างๆ

6. ทำการสำรองข้อมูลอย่างสม่ำเสมอ (Performing Routine Backup) โดยข้อมูลสำคัญที่ถูกสำรองต้องถูกเก็บไว้บนเซิร์ฟเวอร์ที่อยู่ในเครื่อข่าย การสำรองข้อมูลและเก็บไว้บนเครื่องคอมพิวเตอร์ของผู้ใช้ หรือการเก็บไว้ในแผ่นดิสเก็ตนั้นถือว่าไม่มีประโยคในการแบคอัพระบบ ดังนั้นข้อมูลที่ถูกสำรองนั้นควรถูกเก็บไว้แบบรวมศูนย์ (Centralize) เพื่อให้ระบวนการแบคอัพและรีสโตร์สามารถทำได้โดยสะดวกที่สุด

7. มีการใช้เทคโนโลยีเรดบนฮาร์ทดิส (Using RAID Technology) การใช้ RAID เทคโนโลยีกับฮาร์ทดิสนั้นเป็นการเพิ่มความเสถียรภาพให้กับฮาร์ทดิส

8. ป้องกันระบบเน็ทเวิร์คจากการโจมตีของไวรัส (Preventing LAN from virus attack) โดยเลือกโปรแกรมแอนตี้ไวรัสที่เหมาะสม

9. เชื่อมต่อคอมพิวเตอร์เซิร์ฟเวอร์และอุปกรณ์ที่สำคัญผ่านเครื่องสำรองไฟ (Connecting Uninterruptable Power Supplies to Key Servers and Equipment) ไฟฟ้าเป็น

สาเหตุที่สำคัญสาเหตุหนึ่งที่ทำให้เกิดการผิดพลาดหรือสูญหายของข้อมูล ดังนั้นควรมีการติดตั้งเครื่องสำรองไฟฟ้าและเชื่อมต่อคอมพิวเตอร์เซิร์ฟเวอร์และอุปกรณ์ที่สำคัญผ่านเครื่องสำรองไปนี้

ความเกี่ยวโยงของฝ่ายทรัพยากรมนุษย์ (Human Resources)

1. จัดการอบรมการใช้งานและจรรยาบรรณในการใช้งานคอมพิวเตอร์ (Providing Employee Training Program on Computer Uses and Computer Ethics) ควรมีการอบรมการใช้งานคอมพิวเตอร์ให้กับพนักงาน โดยให้ตระหนักถึงความปลอดภัยในการใช้งานเป็นหลัก เนื่องจากการโจมตีของไวรัสในองค์กรนั้น ส่วนใหญ่แล้วมาจากพนักงานมีความรู้เท่าไม่ถึงการนำเอาไวรัสจากคอมพิวเตอร์ที่บ้านมาแพร่กระจายที่ทำงาน เป็นผลให้เกิดความเสียหายแก่องค์กรไม่ทางใดก็ทางหนึ่ง ซึ่งการอบรบจะช่วยการใช้งานและจรรยาบรรณในการใช้คอมพิวเตอร์จะช่วยลดการโจมตีของไวรัสให้อยู่ในระดับต่ำลงได้ ในบ้างองค์กรมีการระบุเรื่องจรรยาบรรณของพนักงานไว้ในสัญญาจ้างงานด้วย

2. จัดทำข้อควรปฏิบัติเพื่อความปลอดภัยขณะเกิดภัยพิบัติ (Promoting Employee Safety Awareness Programs) ผู้บริหารควรจัดทำข้อควรปฏิบัติเพื่อความปลอดภัยขณะเกิดภัยพิบัติให้อยู่ในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ เพื่อที่จะอบรมพนักงานให้ทราบถึงข้อควรปฏิบัติขณะประสบกับสถานการณ์ภัยพิบัติ การใช้งานเครื่องมือดับเพลิงในอาคาร สถานที่ที่ควรอยู่ในขณะเกิดภัยพิบัติ เพื่อให้สามารถดูแลตนเอง และอาจมีการอบรมการปฐมพยาบาลเบื้องต้นเพื่อให้พนักงานสามารถช่วยเหลือผู้อื่นได้ด้วย ในบางองค์กรมองแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติเป็นเหมือนการประกันทรัพสินขององค์กรจากภัยพิบัติ แต่น่าจะเป็นความคิดที่ดีถ้าหากจะรวมทรัพสินที่สำคัญอีกประการหนึ่งขององค์กรเข้าไปในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ นั่นก็คือ บุคคลากรขององค์กร

กลยุทธ์ในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Development Strategies for DRP) ขั้นตอนดังนี้

1. การประเมินความเสี่ยง (Performing a Risk Assessment)

กระบวนการนี้จะเริ่มจากการตรวจสอบระบบและทรัพยากรต่างๆภายในบริษัท และระบุให้ได้ว่าอะไรเป็นสิ่งที่สำคัญและจำเป็นต่อกระบวนการทางธุรกิจ โดยอาจใช้ 2 วิธีดังนี้ (Semer, 1998)

1.1 การวิเคราะห์ผลกระทบต่อธุรกิจ (Business Impact Analysis) เป็นการระบุถึงทรัพยากรที่มีความสำคัญและจำเป็น (Mission-Critical Resources) ต่อองค์กร โดยทรัพยากรเหล่านั้นจะต้องมีควาทสำคัญอย่างมากต่อการทำงานในทุกๆวันขององค์กร และเมื่อสามารถระบุได้ว่าอะไรเป็นทรัพยากรที่มีความสำคัญและจำเป็นแล้ว ในลำดับถัดไปจะต้องหาระยะเวลาสูงสุดที่องค์กรยอมให้ทรัพยากรเหล่านั้นหยุดทำงาน (Maximum Allowable Downtime) หรือกล่าวในอีกมุมหนึ่งได้ว่าองค์กรจะต้องดำเนินกิจกรรมทางธุรกิจภายในระยะเวลาเท่าไหร่หลังจากประสบกับภัยพิบัติจนมีผลทำให้ระบบล้มเหลว

1.2 การประเมินความเสี่ยง (Risk Assessment Analysis) เมื่อสามารถระบุได้แล้วว่าอะไรคือทรัพยากรที่สำคัญและจำเป็นต่อการดำเนินธุรกิจ หลังจากนั้นต้องทำการประเมินความเสี่ยงที่อาจจะเกิดขึ้นกับทรัพยากรที่สำคัญและจำเป็นเหล่านั้นซึ่งจะรวมไปถึงโครงสร้างทางด้านเน็ทเวิร์คด้วย โดยปกติผู้จัดการแผนกจะเป็นคนที่คุ้นเคยกับขั้นตอนการปฏิบัติงานในแต่ละวัน (Day-to-Day Operation) ของแผนกตนเองดีเพราะฉะนั้นผู้จักการแผนกก็อยู่ในตำแหน่งที่เหมาะสมที่จะตัดสินใจได้ว่าอะไรคือทรัพยากรที่สำคัญและจำเป็นต่อการปฏิบัติงานของแผนกนั้นๆ และควรถูกกู้คืนหรือไม่

2. การค้นหาจุดอ่อนของระบบ (Identifying Possible Vulnerabilities)

การคอยตรวจตราจุดอ่อนของระบบนั้นจะเป็นสิ่งที่ช่วยป้องกันปัญหาที่จะเกิดก่อนได้เป็นอย่างดี โดยส่วนมากแล้วจะมีการดูแลในส่วนต่างๆดังนี้ (Rothstein, 1998)

2.1 สถานที่ในการเก็บรักษาข้อมูลที่ถูกสำรองไว้ (Backup Storage Location for Data)

2.2 มาตรการความปลอดภัย (Security)

2.3 มาตรการความปลอดภัยในการเข้าถึงตัวอุปกรณ์ (Physical Security)

2.4 สถานที่อยู่ของอุปกรณ์ (The Room and Building that Housing The Computer)

2.5 ไฟฟ้า (Electrical Power)

2.6 อุปกรณ์ตรวจจับเพลิงไหมและเครื่องมือดับเพลิง (Fire Detection and Suppression)

2.7 ข้อมูลที่ขึ้นกับบุคคลเพียงคนเดียว (Depending on One Person Information)

2.8 การควบคุมการจัดการ (Management Control)

2.9 ความน่าเชื่อถือในการเชื่อมต่อสัญญาณการสื่อสารไปยังภายนอก (Reliability of Telecommunication Services)

สำหรับในประเด็นอื่นๆอาจจะรวมถึง การลาออกของพนักงาน (Employee Resignation) คอมพิวเตอร์ติดไวรัส เป็นต้น

3. พัฒนาแผนการปฏิบัติงาน (Developing a Plan of Action)

วิธีการหนึ่งในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ คือ การให้แต่ละแผนกจัดทำแผนการฟื้นฟูของตัวเอง ว่าจะทำอย่างไรที่จะสามารถแก้ปัญหาที่เกิดขึ้นในช่วงวิกฤตได้ โดยในแผนควรมีการระบุหมายเลขติดต่อของผู้ที่ได้รับมอบหมายให้ตอบสนองในทันทีเมื่อเกิดเหตุการณ์ หมายเลขติดต่อเวนเดอร์ที่เกี่ยวข้อง ที่อยู่ของไซต์สำรอง ควรหลีกเลี่ยงการระบุข้อห้ามหรือข้อปฏิบัติที่อาจทำให้เกิดความสับสน (Jackson, 1997)

4. การเลือกไซต์สำรอง (Choosing An Alternate Recovery Site)

การย้ายที่ปฏิบัติงานไปยังไซต์งานสำรอง อาจมีความจำเป็น ถ้าสาเหตุของภัยพิบัติเกิดจาก น้ำท่วม พายุ หรือไฟไหม้ ด้วยเหตุนี้ควรพิจารณาให้ทรัพยากรที่มีความสำคัญและจำเป็นต่อการดำเนินงานขององค์กร ถูกย้ายไปปฏิบัติงานในไซต์งานสำรอง (Rothstein, 1998) ไซต์งานสำรองมีหลากลักษณะ ดังนี้

4.1 การทำสัญญาในการดูแลรักษากับผู้จำหน่าย (Vendor Maintenance Agreement) เป็นสิ่งที่จำเป็นมาก เนื่องจากภายใต้ความคลุมครองของสัญญาที่ทำกับเวนเดอร์นั้นมักจะรวมถึง ความรับผิดชอบในอุปกรณ์ต่างๆ โดยจะทำการซ้อมหรือเปลี่ยน เมื่อเกิดความเสียหายขึ้นจากตัวอุปกรณ์ ซึ่งอาจจะเรียกอีกแบบหนึ่งว่า การรับรองสินค้าและบริการ (Product and Services Warranty) แต่โดยปกติจะไม่คลุมครองความเสียหายที่เกิดจากสาเหตุภายนอก อาธเช่น ไฟไหม้ น้ำท่วม แต่สามารถทำสัญญาเพิ่มเติมได้ถ้ามีความจำเป็น วิธีนี้เหมาะสมกับธุรกิจหรือองค์กรขนาดเล็กและสามารถยอมรับการหยุดทำงานของระบบหรืออุปกรณ์ชิ้นนั้นได้อย่างน้อยตามระยะเวลาที่ระบุในสัญญา (Services Level Agreement) โดยค่าบำรุงรักษาเมื่อคิดต่อเดือนแล้วควรไม่เกิน 300 ดอร์ลล่าสหรัฐ (Rothstein, 1998)

4.2 ฮอตไซต์ (Hot Sites) เป็นบริการของเวนเดอร์ มีการจัดเตรียมอุปกรณ์และสิ่งอำนวยความสะดวกทุกอย่างตามที่องค์กรต้องการ ซึ่งอาจรวมถึง เครื่องคอมพิวเตอร์เซิร์ฟเวอร์

และซอฟท์แวร์ โทรคมนาคม โทรสาร เครื่องใช้ในสำนักงาน และอุปกร์ที่จำเป็นอื่นๆ ซึ่งพร้อมรองรับการโยกย้ายจากไซต์งานหลัก เพื่อให้เกิดการหยุดปฏิบัติงานของระบบน้อยที่สุด (Minimize Network Downtime) (Rothstein, 1998) โดย Patrowicz (1998) กล่าวว่า เพื่อความสะดวกในการเคลื่อนย้ายพนักงาน ฮอตไซต์ควรอยู่ห่างจากไซต์ปฏิบัติงานของพนักงานไม่เกิน 30 ไมล์ หรือ 50 กิโลเมตร แต่ Leary (1998) เสริมว่าฮอตไซต์สามารถอยู่ห่างจากไซต์ปฏิบัติงานของพนักงานได้ แต่ต้องมีการจัดเตรียมเครื่องอำนวยความสะดวกในการพักอาศัย อาธิเช่น ห้องนอน ห้องอาบน้ำ และห้องอาหาร ให้กับพนักงานด้วย นอกจากนั้นผู้บริหารควรจัดให้มีการฝึกซ้อมบุคคลากรตามแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอย่างสม่ำเสมอเพื่อรองรับกับเหตุการณ์ที่อาจเกิดขึ้นในอนาคต (Semer, 1998)

4.3 โคลไซต์ (Cold site) เป็นการเตรียมโครงสร้างพื้นฐานอันได้แก่ อาคาร ไฟฟ้า อุปกรณ์คอมพิวเตอร์ เครื่องปรับอากาศ (Patrowicz, 1998) แต่ไม่ได้มีการติดตั้งไว้ให้พร้อมใช้งานทันที ดังนั้นถ้าปัจจัยด้านเวลาในการฟื้นฟูระบบไม่ได้เป็นอุปสรรคต่อองค์ รูปแบบนี้ถือเป็นรูปแบบที่ควรพิจารณา (Semer, 1998) ค่าใช้จ่ายในการเตรียมโคลไซต์ ก็ขึ้นอยู่กับความซับซ้อนของระบบ โดยส่วนใหญ่แล้วบริษัทมักใช้โรงอาหารเป็นโคลไซต์ ในกรณีไม่ต้องย้ายสถานที่ปฏิบัติงาน (On-Site Cold Site) และเลือกใช้คลังเก็บสินค้าเป็นโคลไซต์ในกรณีต้องย้ายที่ปฏิบัติงาน (Off-Site Cold Site) สำหรับกรณีไม่ได้มีการเตรียมโคลไซต์ไว้ล่วงหน้าการเลือกใช้บริการโคลไซต์ของเวนเดอร์ก็เป็นอีกทางเลือกหนึ่ง (Leary, 1998) อย่างไรก็ตามการเลือกโคลไซต์นั้นก็มีข้อเสียบ้างประการ เช่น ความปลอดภัยในการขนย้ายอุปกรณ์คอมพิวเตอร์ ความปลอดภัยทางด้านข้อมูล ความตรงต่อเวลาในการขนย้ายของเวนเดอร์ และร่วมถึงกรณีต้องมีการเปลี่ยนชิ้นส่วนอุปกรณ์ซึ่งต้องใช้เวลาในการขนส่งเช่นกัน อาจทำให้ระบบหยุดทำงานนานกว่าที่วางแผนเอาไว้ได้ (Leary & Rothstein, 1998)

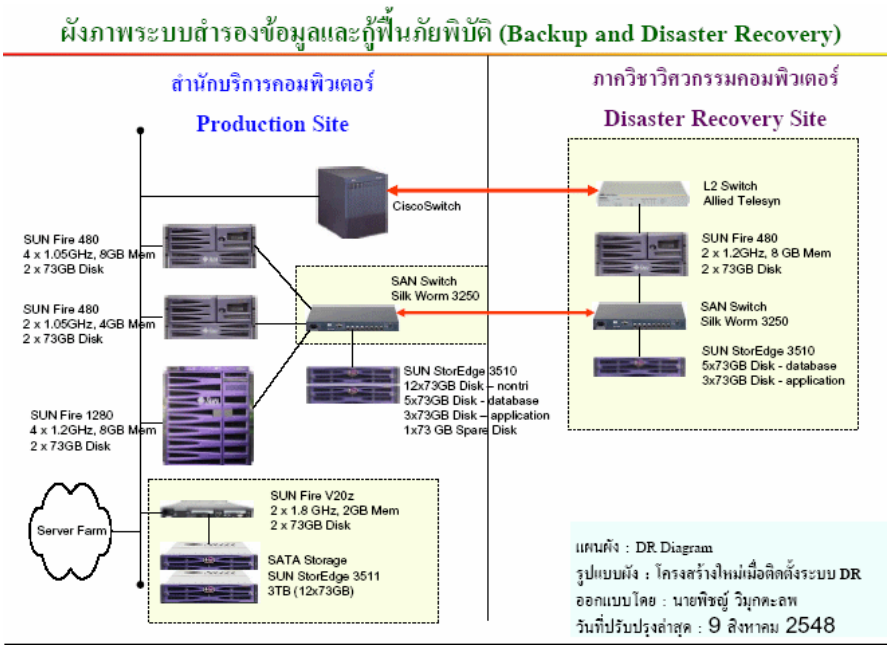
4.4 ไซต์สำรองเคลื่อนที่ (Mobile Recovery Facilities) เป็นการใช้รถพ่วง (Trailers) ที่ติดตั้งอุปกรณ์คอมพิวเตอร์ที่จำเป็น รวมถึงอาจติดตั้งเครื่องผลิตไฟฟ้าสำรอง (Backup Power Generator) ด้วย โดยข้อเสียของไซต์สำรองเคลื่อนที่นั้นก็คือ ต้องใช้เวลาในการติดตั้งและกู้คืนระบบเป็นระยะนาน อาจเป็นสัปดาห์หรือมากกว่านั้น (Rothstein, 1998)

4.5 มิลเลอร์ไซต์ (Mirrored Site) คล้ายกับฮอทไซต์ โดยมิลเลอร์ไซต์จะมีการติดตั้งอุปกรณ์ที่จำเป็นรวมถึงอุปกรณ์สัญญาณสื่อสาร ซึ่งสามารถทำงานได้ทันทีที่ต้องการ แต่มีข้อแตกต่างจากฮอตไซต์คือมิลเลอร์ไซต์จะมีกระบวนการส่งผ่านข้อมูลจากไซต์หลักไปยังมิลเลอร์ไซต์ตามตารางที่กำหนด เช่น อาจทำการส่งผ่านข้อมูลในทันทีระหว่างไซต์หลักกับมิลเลอร์ไซต์ ซึ่ง

ในกรณีนี้ ระบบสามารถสลับไปทำงานยังมิลเลอร์ไซต์ได้ทันที หรือทำการส่งผ่านข้อมูลหรือสำรองข้อมูลไปยังมิลเลอร์ไซต์ในช่วงเวลากลางคืน ผลก็คือสามารถปฏิบัติงานที่มิลเลอร์ไซต์พร้อมกับข้อมูลก่อนหน้าหนึ่งวัน แต่ไม่ว่าด้วยวิธีการส่งข้อมูลแบบไหน ระบบจะถูกฟื้นฟูกลับมาใช้งานได้ภายในวันเดียว (Rothstein, 1998) ตัวอย่างการทำมิลเลอร์ไซต์ของมหาวิทยาลัยเกษตรศาสตร์ โดยสำนักบริการคอมพิวเตอร์ได้ดำเนินการติดตั้งระบบสำรองข้อมูลและกู้ฟื้นข้อมูล สำหรับงานฐานข้อมูลระบบสารสนเทศหลักของมหาวิทยาลัย เพื่อป้องกันภัยจากภัยพิบัติต่าง ๆ ที่อาจทำให้ข้อมูลเสียหายทางด้านกายภาพ เช่น เครื่องคอมพิวเตอร์แม่ข่ายเสีย เป็นต้น ระบบจะช่วยให้ทำงานอย่างต่อเนื่อง และกู้ข้อมูลกลับคืนได้ โดยการติดตั้งชุดคอมพิวเตอร์แม่ข่ายสำรองไว้ทำงานทดแทน ในกรณีที่เครื่องคอมพิวเตอร์แม่ข่ายหลักขัดข้อง ดังภาพที่ 2.2

ภาพที่ 2.2

แสดงผังภาพระบบสำรองข้อมูลและกู้ฟื้นภัยพิบัติของมหาวิทยาลัยเกษตรศาสตร์



ที่มา: http://wiki.nectec.or.th

5. การเลือกวิธีการสำรองข้อมูล (Selecting Backup Strategy)

วิธีการสำรองข้อมูลจะมีผลต่อความเร็วในการฟื้นฟูระบบสารสนเทศ โดยในปัจจุบันมีรูปแบบการสำรองข้อมูลอยู่ 2 วิธี ดังนี้

5.1 ระบบสำรองข้อมูลแบบอินเฮาส์ (In-House Backup Systems) เป็นการสำรองข้อมูลไปยังตัวเก็บข้อมูลแล้วเก็บไว้ในสถานที่อื่นที่ไม่ใช่ห้องปฏิบัติการคอมพิวเตอร์ แต่ยังอยู่ในไซต์งานนั้นๆ เช่น การสำรองข้อมูลลงม้วนเทป แล้วนำไปเก็บไว้ในตู้นิรภัยในห้องประธาน เป็นต้น โดยวิธีนี้จะประหยัดค่าใช้จ่ายไปได้อย่างมาก แต่อย่างไรก็ตามจะต้องมีการกำหนดกระบวนการอื่นๆมารองรับในการย้ายตัวเก็บข้อมูลไปไว้ยังสถานที่อื่นที่ไม่ใช่ไซต์งานหลักลงในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติด้วย (Semer, 1998) เช่น การกำหนดตารางการส่งม้วนเทปไปเก็บไว้ยังคลังสินค้า เป็นต้น

5.2 ระบบสำรองข้อมูลแบบออฟไซต์โดยมีการเข้ารหัสข้อมูล (Offsite Backup Systems with Data Encrypted) ในวิธีนี้ข้อมูลที่จะทำการส่งไปเก็บยังออฟไซต์จะโดนเข้ารหัสเพื่อความปลอดภัย โดยปกติจะส่งผ่านวงจรเช่าสื่อสัญญาณความเร็วสูง (Lease Line) องค์กรที่มีการใช้วิธีการสำรองข้อมูลแบบนี้ ยกตัวอย่างเช่น สถาบันทางการเงิน องค์กรทางการทหาร โรงพยาบาล บริษัทขนาดใหญ่ รวมถึง สำนักงานสืบสวนของสหรัฐอเมริกา เป็นต้น (Sutton, 1998)

สิ่งที่จำเป็นอีกประการหนึ่งในการสำรองข้อมูลนั้นก็คือซอฟท์แวร์ที่ใช้ในการสำรองข้อมูลโดยคุณสมบัติของซอฟท์แวร์ในการสำรองข้อมูลที่ดี มีดังนี้

1. ทำงานอัตโนมัติ คือ หลังจากติดตั้งระบบเรียบร้อยแล้ว จะช่วยลดภาระของผู้ดูแล โดยไม่จำเป็นต้องสั่งงานหรืออยู่รอการสำรองข้อมูลเพื่อเปลี่ยนเทป ซึ่งจะช่วยลดปัญหาความผิดพลาดจากคน (Human Error) โดยควรมีความสามารถการกำหนดตารางเวลาการสำรองข้อมูล ไม่ว่าจะเป็นในแบบรายเดือน รายสัปดาห์ หรือ รายวัน เมื่อถึงเวลาที่กำหนดจะทำการสำรองข้อมูล และหาม้วนเทปที่ถูกต้องเองโดยอัตโนมัติ (Tape Library) ในทางตรงกันข้าม ขณะที่ทำการกู้คืนข้อมูลจะต้องสามารถระบุถึงม้วนเทปที่มีข้อมูลที่ต้องการอยู่ได้อย่างชัดเจนเพื่อง่ายต่อการจัดการม้วนเทป

2. สนับสนุนเทคโนโลยีที่หลากหลาย สามารถรองรับและใช้งานร่วมกับอุปกรณ์สำรองข้อมูลได้หลากหลายไม่ว่าจะเป็น เทปแบคอัพรุ่นต่างๆ เครื่อข่ายตัวจัดเจ็บข้อมูล (SAN Storage Area Network) ควรสนับสนุนเทคโนโลยีการสำรองข้อมูลในแบบต่างๆด้วย ได้แก่ LAN Free, Server Free เป็นต้น

3. ประสิทธิภาพสูง ควรทำการสำรองข้อมูล และกู้คืนได้ทีละหลายๆ หัวอ่าน ได้พร้อมกัน เพื่อความรวดเร็วในการสำรองข้อมูล การสนับสนุนเทคโนโลยีการสำรองข้อมูล อาธิเช่น

3.1 LAN Free จะทำให้ข้อมูลที่กำลังทำการสำรองไม่เข้ามารบกวนระบบเครือข่าย

3.2 Server Free เนื่องจากข้อมูลที่ทำการสำรองจะไม่ไปรบกวนเครือข่ายแล้วยังไม่รบกวนทรัพยากรของเครื่องเซิร์ฟเวอร์ด้วย เพราะข้อมูลจะส่งจากดิสก์ สู่เทปโดยตรง

3.3 ความสามารถในการบีบอัดข้อมูลก่อนส่งมาทำการสำรองข้อมูล ทำให้การสำรองข้อมูลมีความรวดเร็วขึ้นและลดปริมาณความคับคั่งในเครือข่ายให้น้อยลงด้วย

3.4 การทำ Staging Backup เป็นอีกวิธีการหนึ่งที่ช่วยเพิ่มความเร็วในการสำรองข้อมูล เพราะจะเป็นการสำรองข้อมูลลงดิสก์ ซึ่งเปรียบเสมือนบัฟเฟอร์ โดยมีความเร็วมากกว่าเทปไดรฟ์ แล้วค่อยย้ายขึ้นเทปในภายหลัง ซึ่งจะช่วยเพิ่มความเร็วในการสำรองข้อมูล

3.5 Checkpoint Restart เป็นความสามารถในการเริ่มต้นกระบวนการสำรองข้อมูลหลังจากเกิดความผิดพลาด โดยไม่ต้องเริ่มต้นใหม่ทั้งหมด จะเริ่มทำเฉพาะตั้งแต่ส่วนที่มีปัญหาเท่านั้น ซึ่งจะช่วยประหยัดเวลาในการสำรองข้อมูลมากยิ่งขึ้นในกรณีที่การสำรองข้อมูลครั้งนั้นเกิดมีปัญหาขึ้นมา

4. สนับสนุนแอพพลิเคชันหลากหลาย ควรสนับสนุนการทำออนไลน์แบคอัพแอพพลิเคชัน หรือฐานข้อมูล ที่เป็นที่นิยม ได้แก่ ออราเคิล อินฟอร์มิกซ์ ไมโครซอฟท์ เอ็กซ์เชนจ์ ดีบีทู ไซเบส โลตัสโน้ต และ SAP เป็นต้น และบางตัวอาจจะมีคุณสมบัติ อื่นอีก เช่น การทำ Block Level Incremental Backup คือการสำรองข้อมูลฐานข้อมูลเฉพาะส่วนที่มีการเปลี่ยนแปลงเท่านั้น ซึ่งจะช่วยให้การสำรองข้อมูลทำได้เร็วยิ่งขึ้น เพราะโดยปกติแล้วการสำรองข้อมูลฐานข้อมูล แม้จะมีการเปลี่ยนแปลงแค่เพียงฟิลด์เดียว ก็จะต้องทำการสำรองข้อมูลฐานข้อมูลใหม่ทั้งหมด ถ้าเป็นในด้านของแอพพลิเคชันอีเมล์ เช่น ไมโครซอฟท์เอ็กซ์เชนจ์ อาจจะมีคุณสมบัติการกู้คืนได้ถึงระดับเมล์ของแต่ละของผู้ใช้

5. รองรับการสำรองข้อมูลได้จากหลายแพลตฟอร์ม ได้แก่ ไมโครซอฟท์วินโดวส์, HP-UX, AIX, โซลารีส, IRIX ฯลฯ และถ้าผ่านการรับรองจากผู้ผลิตระบบปฏิบัติการ หรือ ฮาร์ดแวร์ต่างๆ จะช่วยทำให้มั่นใจมากยิ่งขึ้นเมื่อนำมาใช้ในระบบว่าจะไม่เกิดปัญหาตามมา

6. ควบคุมการทำงานจากศูนย์กลาง เพื่อความสะดวกในการจัดการดูแลระบบหรือ แก้ปัญหาและสามารถสำรองข้อมูลผ่านเครือข่ายได้ ข้อมูลจะวิ่งผ่านเครือข่ายมาที่แบ็กอัพเซิร์ฟเวอร์ แล้วจึงเขียนลงอุปกรณ์แบ็กอัพที่ตัวเซิร์ฟเวอร์ ไม่ว่าจะเป็นดิสก์ หรือ เทปก็ตามข้อมูลที่แบ็กอัพ ทุกอย่างจะถูกเก็บไว้ที่แบ็กอัพเซิร์ฟเวอร์ ซึ่งซอฟต์แวร์ในการแบ็กอัพ ส่วนใหญ่มีความสามารถด้านนี้อยู่แล้ว

7. ง่ายต่อการขยายระบบในอนาคต ไม่ว่าจะเพิ่มเซิร์ฟเวอร์อีกกี่ตัว หรือเพิ่มจำนวนเทปไดรฟ์ ก็ต้องไม่มีผลกระทบต่อค่าในการติดตั้งเดิมที่มีอยู่ เพียงแค่ติดตั้งส่วนที่เพิ่มหรือเปลี่ยนแปลงเข้าเท่านั้น

8. ระบบรักษาความปลอดภัย ในการติดตั้งระบบสำรองข้อมูลอาจจะต้องมีการแก้ไขระบบรักษาความปลอดภัยขององค์กรบ้าง การแก้ไขค่าบนไฟร์วอลล์ เพื่อเปิดพอร์ตบางพอร์ตสำหรับซอฟต์แวร์สำรองข้อมูลนั้น ซึ่งอาจมีความจำเป็นในการสำรองข้อมูลระหว่างเซิร์ฟเวอร์ที่อยู่คนละฝั่งกันของไฟร์วอลล์ ซอฟต์แวร์สำรองข้อมูลแต่ละตัวจะใช้หมายเลขพอร์ตต่างกัน และ จำนวนไม่เท่ากัน ซึ่งถ้าต้องใช้จำนวนพอร์ตมากเท่าไรก็ยิ่งมีผลต่อความปลอดภัยมากเท่านั้นเพราะต้องเปิดพอร์ตในพิสัยที่ค่อนข้างกว้าง หรือ อาจจะยอมรับไม่ได้เลยในนโยบายด้านระบบรักษาความปลอดภัยขององค์กร นอกจากนั้นในด้านความปลอดภัย ยังอาจจะมีการเข้ารหัสข้อมูลในขณะแบ็กอัพ เพื่อปกป้องข้อมูลหากถูกดักจับขณะที่ส่งออกไปในเครือข่าย หรือ ขณะส่งไปในสายเคเบิลเพื่อเขียนลงเทป

9. ความสามารถในการทำสำเนา หรือสามารถก๊อบปี้เทปได้ ไม่ว่าขณะที่แบ็กอัพหรือหลังจากแบ็กอัพเรียบร้อยแล้ว เพื่อป้องกันปัญหาที่เกิดความเสียหายของม้วนเทป ดังนั้นเราอาจจะจำเป็นต้องมีการทำก๊อบปี้เทปแบคอัพมากกว่า 1 ชุด แล้วเก็บไว้ในสถานที่อื่นเพื่อใช้ในขั้นตอนของแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติขององค์กร

10. ความสามารถอื่นๆ สามารถเขียนสคริปต์เพื่อช่วยเพิ่มประสิทธิภาพหรือลดขั้นตอนในการแบ็กอัพได้ เช่น ในบางโปรแกรมคอมพิวเตอร์อาจมีความจำเป็นต้องใช้สคริปต์ก่อนการสำรองข้อมูล (Pre-Script) ในการสั่งหยุดการให้บริการของโปรแกรมคอมพิวเตอร์ก่อน หลังจากนั้นจึงทำการสำรองข้อมูลจนเสร็จ สุดท้ายก็ใช้สคริปต์หลังการสำรองข้อมูลสั่งให้เปิดใช้บริการโปรแกรมคอมพิวเตอร์นั้นๆ โดยทั้งหมดนี้จะทำงานโดยอัตโนมัติ

ในปัจจุบันซอฟท์แวร์ในการสำรองข้อมูลมีอยู่มากมาย ล่วนก็มีความสามารถที่หลากหลายไม่แพ้กัน การเลือกซอฟท์แวร์ที่มีความสามารถมากที่สุดไม่ได้หมายความว่าจะมีประสิทธิภาพมากที่สุด แต่การเลือกซอฟท์แวร์ที่ตรงกับความต้องการเหมาะกับสภาพแวดล้อมของระบบมากที่สุดนั้น จะทำให้องค์กรลงทุนไปอย่างคุ้มค่าและเกิดประโยชน์มากที่สุด

6. การจัดให้มีการบททวนและพูดคุยกันถึงขั้นตอนการปฏิบัติในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Conducting a Verbal Walk-Through)

7. การทดสอบและปรับปรุงแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอย่างสม่ำเสมอ (Testing and Update The Plan on a Regular Basis to Ensure Integrity)

เนื่องจากการเปลี่ยนแปลงที่รวดเร็วของธุรกิจ องค์กรต้องมีความสามารถในการปรับตัวให้รับกับสถานการณ์ รวมถึงในด้านเทคโนโลยีด้วย การเปลี่ยนแปลงเหล่านี้อาจส่งผลกระทบไม่มากก็น้อยต่อแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติขององค์กร สิ่งที่เกิดขึ้นก็คือ แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติไม่สามารถถูกนำไปใช้ได้จริง เพื่อไม่ให้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติที่องค์กรได้ลงทุนลงแรงในการประยุกต์ใช้เสียเปล่า องค์กรควรมีการปรับปรุงแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติและทดสอบอย่างต่อเนื่อง เพื่อให้แผนสามารถใช้ได้จริงตลอดเวลา พร้อมรับมือกับสถานการณ์ที่อาจจะเกิดขึ้นในอนาคต

2.2 มาตรฐานเกี่ยวกับแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

1. มาตรฐานการบริหารการดำเนินธุรกิจอย่างต่อเนื่องภายใต้ภาวะวิกฤติ (BS25999: Business Continuity Management (BCM) Standard)

การบริหารจัดการดำเนินธุรกิจอย่างต่อเนื่องภายใต้ภาวะวิกฤติ (Business Continuity Management BCM) เป็นกระบวนการบริหารจัดการแบบองค์รวม (Holistic Management Process) ซึ่งเป็นระบบทำให้องค์กรสามารถกำหนดปัจจัยเสี่ยง และ ผลกระทบที่อาจเกิดขึ้นได้จากปัจจัยเสี่ยงดังกล่าวว่ามีผลเสียหายต่อองค์กรมากน้อยเพียงใด ในทางทฤษฎีเราเรียกว่า การวิเคราะห์ผลกระทบของปัจจัยเสี่ยงและเหตุการณ์ไม่พึงประสงค์ต่อธุรกิจ หรือ Business Impact Analysis (BIA) และ ดำเนินการกำหนดยุทธศาสตร์ในการทำให้องค์กรสามารถดำเนินธุรกิจต่อไปได้ในภาวะฉุกเฉิน ตลอดจนลดผลกระทบจากการที่ระบบไม่สามารถให้บริการได้อย่างมีประสิทธิภาพถูกต้องตามหลักวิชาการ การทำการวิเคราะห์ผลกระทบของปัจจัยเสี่ยงและเหตุการณ์ไม่พึงประสงค์ต่อธุรกิจ เป็นส่วนหนึ่งของแผนการดำเนินธุรกิจอย่างต่อเนื่อง หรือ Business Continuity Planning (BCP)

องค์ประกอบหลักของ BCM ตามมาตรฐาน BS25999:2006 แสดงดังภาพที่ 2.3 ประกอบไปด้วย

1. BCM Program Management ถือได้ว่าเป็นหัวใจของกระบวนการทั้งหมด ที่ผู้บริหารระดับสูงต้องเข้ามามีส่วนร่วมเพื่อให้แน่ใจได้ว่า มีการจัดทำ BCM อย่างเหมาะสม และได้รับการสนับสนุนอย่างเพียงพอ

2. Understand the Organization การประเมินความเสี่ยง (Risk Assessment) และการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) เป็นกิจกรรมสำคัญหลักในข้อ

นี้ที่จะทำให้สามารถจัดระดับความสำคัญของ product หรือ service และเป็นการวิเคราะห์เพื่อระบุความเร่งด่วนของกิจกรรมต่างๆ และระดับความสามารถที่ต้องการ เพื่อนำไปเป็นข้อมูลสำคัญในการกำหนดกลยุทธ์ในข้อต่อไป

3. Determine Business Continuity Strategy การกำหนดกลยุทธ์ในภาพรวมจะทำให้การเลือกกิจกรรมหรือระบบสนับสนุนสำหรับแต่ละผลิตภัณฑ์และบริการสอดคล้องและไปในทิศทางเดียวกัน เช่นการกำหนดระดับของการดำเนินการที่ยอมรับได้ หรือการกำหนดขอบเขตของช่วงเวลาที่ยอมรับได้ เป็นต้น

4. Develop and Implement a BCM Response หลักจากที่ได้มีการกำหนดกลยุทธ์เป็นที่เรียบร้อยแล้ว ก็จะใช้กรอบดังกล่าวมาจัดทำแผนงาน เพื่อให้เป็นไปตามกรอบยุทศาสตร์ที่กำหนดไว้ โดยจัดทำแผน IMP: Incident Management Plan, BCP: Business Continuity Plan, DRP: Disaster Recovery Plan

5. BCM Exercising, Maintaining and Reviewing BCM Arrangements กิจกรรมในข้อนี้เป็นกิจกรรมที่ทำให้แน่ใจได้ว่า BCM ที่ได้จัดทำขึ้นนั้น สามารถใช้ได้จริง และมีข้อมูลที่เป็นปัจจุบันไม่ล้าหลัง หรือมีข้อมูลอ้างอิงที่ไม่สามารถนำมาใช้ได้

6. Embedding BCM in The Organization's Culture การทำให้ BCM ผสมกลมกลืนเข้าจนเป็นวัฒนธรรมองค์กรนั้นไม่ใช่เรื่องง่ายและต้องใช้เวลา ที่จะทำให้พนักงานทุกคนได้ซึมซาบและเข้าใจถึงความสำคัญของ BCM ตลอดจนบทบาทหน้าที่ที่ทุกคนพึงมีเพื่อให้ธุรกิจสามารถดำเนินต่อไปได้ในยามที่เกิดเหตุวิกฤต

มาตรฐาน BS25999 แบ่งออกได้เป็น 2 ส่วน

- ส่วนที่หนึ่งเรียกว่า "BS 25999-1:2006 -- Business Continuity Management. Code of Practice" เป็นแนวปฏิบัติที่ทางบริษัท BSI ซึ่งเป็นบริษัทผู้ตรวจประเมินชั้นนำของโลกแนะนำให้ปฏิบัติแต่ไม่บังคับ (โดยจะใช้คำว่า "Should" ในข้อกำหนดมาตรฐาน)

ภาพที่ 2.3

แสดงองค์ประกอบหลักของ BCM

ที่มา: http://www.wikipedia.org

- ส่วนที่สองเรียกว่า “BS 25999-2:2007 -- Specification for Business Continuity Management” เป็นข้อกำหนดภาคบังคับที่ต้องปฏิบัติ (ใช้คำว่า “Shall” ในมาตรฐาน) เรียกว่า ระบบบริหารจัดการธุรกิจอย่างต่อเนื่อง “Business Continuity Management System หรือ BCMS” ซึ่งสามารถต่อยอดไปยังการรับรองมาตรฐานโดยผู้ให้การรับรอง ซึ่งในขณะนี้มาตรฐาน BS 25999 นั้นให้การรับรองโดย โดย LRQA และ BSI

ซึ่งในอนาคตอันใกล้คาดว่ามาตรฐาน BS 25999 จะกลายเป็นมาตรฐานนานาชาติ ISO/IEC ดังเช่น มาตรฐาน BS7799 กลายเป็นมาตรฐาน ISO/IEC 17799 และ ISO/IEC 270001 มาแล้ว เป็นต้น

การจัดทำ BCP มีขั้นตอนหลักทั้งหมด 5 ขั้นตอนโดยสังเขป ประกอบด้วย

ขั้นตอนที่ 1 การศึกษาและวิเคราะห์ (Analysis Phase) เป็นขั้นตอนการวิเคราะห์ปัจจัยเสี่ยงและผลกระทบที่เรียกว่าการทำ “Business Impact Analysis” (BIA) ดังที่กล่าวมาแล้วในตอนต้น โดยมีหลักการในการวิเคราะห์ความแตกต่างของ Critical Function และ Non – Critical Function ขององค์กรเสียก่อน โดยดูจาก ค่า RTO และ RPO เป็นหลักโดยค่า Recovery Time Objective (RTO) หมายถึงระยะเวลาที่องค์กรยอมรับได้ในการกู้คืนระบบในกรณีที่เกิดเหตุ

ฉุกเฉินขึ้น ซึ่งเป็นค่าที่ถูกกำหนดโดยเจ้าของระบบ ต้องให้ผู้บริหารระดับสูงรับรู้ และยอมรับในค่า RTO ที่ถูกกำหนดขึ้น เช่น RTO = 1 ชั่วโมง หมายถึง ต้องกู้ระบบคืนภายในหนึ่งชั่วโมง เป็นต้น สำหรับค่า Recovery Point Objective (RPO) หมายถึง ปริมาณข้อมูลสูญหายที่องค์กรยอมรับได้ในช่วงเวลาหนึ่ง (Acceptable Loss) เช่น ถ้าค่า RPO = 2 ชั่วโมง หากเรา Backup ระบบไว้เวลา 13.00 น. และ ระบบล่มเวลา 14.50 น. เราสามารถกู้คืนข้อมูลได้ถึงเวลา 13.00 น. ก็ยังถือว่าอยู่ในเวลาที่กำหนดไว้ตาม RPO คือ ข้อมูลสูญหายไม่เกิน 2 ชั่วโมง เป็นต้น

ขั้นตอนที่ 2 การออกแบบและพัฒนา (Solution Design Phase) เป็นขั้นตอนในออกแบบยุทธศาสตร์ในการกู้ข้อมูล (Disaster Recovery) ที่เหมาะสมกับความต้องการขององค์กร

ขั้นตอนที่ 3 การประยุกต์ใช้ (Implementation Phase) เป็นขั้นตอนในการนำยุทธศาสตร์ที่ออกแบบไว้ในขั้นตอนที่ 2 มาทำเป็นแผนปฏิบัติการ โดยการเขียนแผน Business Continuity (BC) ที่สามารถนำไปใช้ปฏิบัติจริงได้

ขั้นตอนที่ 4 การทดสอบ (Testing and Organization Acceptance Phase) เป็นขั้นตอนในการทดสอบแผน Business Continuity ที่ได้เขียนไว้ในขั้นตอนที่ 3 ว่าสามารถนำมาใช้งานได้จริงเมื่อเกิดปัญหาหรือไม่ ส่วนใหญ่นิยมเรียกขั้นตอนนี้ว่า ขั้นตอน “การซ้อมแผน BCP” ซึ่งปกติจะทดสอบปีละหนึ่งครั้งเป็นอย่างน้อย

ขั้นตอนที่ 5 การบำรุงรักษา (Maintenance Phase) เป็นขั้นตอนในการปรับปรุงแผน BCP ในคู่มือ BCP ให้เป็นปัจจุบัน และรองรับขั้นตอนการกู้คือข้อมูลตามค่า RTO, RPO ที่ได้กำหนดไว้ในการทำ BIA ตลอดจนการฝึกอบรมพนักงาน (Staff Awareness) ให้มีความรู้ความเข้าใจในการนำแผน Business Continuity (BC) มาใช้ในยามฉุกเฉิน ปกติจะจัดทำและฝึกอบรมอย่างน้อยปีละหนึ่งครั้งเช่นกัน

การจัดทำ BCP นั้นคลอบคลุมทั้งระบบ IT และระบบ Non – IT แต่ถ้ากล่าวถึงการจัดทำแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติจะเป็นส่วนหนึ่งของ BCP จะเน้นไปที่การกู้คืนระบบสารสนเทศเป็นหลัก

ภาพที่ 2.4

แสดงวงจรในการจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่อง

ที่มา: http://www.wikipedia.org

2. แนวทางการเตรียมความพร้อมให้กับเทคโนโลยีสารสนเทศเพื่อการสื่อสารภายใต้ภาวะวิกฤติ (ISO/IEC 24762:2008 Information Technology -- Security Techniques -- Guidelines for Information and Communications Technology Disaster Recovery Services)

เป็นมาตรฐานใหม่ที่มุ่งเน้นเสนอแนวทางในการเตรียมความพร้อมให้กับเทคโนโลยีสารสนเทศเพื่อการสื่อสาร ซึ่งเป็นส่วนหนึ่งในการบริหารจัดการดำเนินธุรกิจอย่างต่อเนื่องภายใต้ภาวะวิกฤติ (Business Continuity Management) และเป็นขั้นเริ่มต้นในการจัดการด้านความปลอดภัยของระบบสารสนเทศ (Information Security Management) ด้วยมาตรฐานใหม่นี้จะทำให้องค์กรสามารถสร้างความยืดหยุ่นให้กับระบบสารสนเทศซึ่งสำคัญและจำเป็นในการดำเนินกิจกรรมทางธุรกิจขององค์กร

Sy (2008) บรรณาธิการของมาตราฐานชุดนี้ได้แสดงความคิดเห็นว่า “มาตรฐานนี้เป็นมาตรฐานที่พัฒนาขึ้นมาเพื่อลดความเสียหายจากภัยพิบัติหรือภาวะวิกฤตของระบบสารสนเทศและการสื่อสาร” โดยเขายังย้ำว่า “ได้มีการอธิบายถึงวิธีการเตรียมทางเลือกที่จะช่วยให้

พ้นจากสถานการณ์วิกฤต และแนววิธีปฏิบัติที่จะทำให้ระบบสารสนเทศสามารถให้งานได้ทั้งช่วงเวลาที่ประสบภัยพิบัติและการฟื้นฟูอย่างสมบูรณ์ในระยะยาว”

โดยมาตรฐานฉบับนี้จะพูดถึงแนวทางในการประยุกต์ใช้ การทดสอบ และการปฏิบัติการในการฟื้นฟูจากภัยพิบัติ ซึ่งสามารถนำไปปรับใช้ได้ทั้งกับภายในองค์กรเอง และกับผู้ให้บริการฟื้นฟูระบบสารสนเทศจากภัยพิบัติ โดยกรอบการทำงานของแนวทางการเตรียมความพร้อมให้กับเทคโนโลยีสารสนเทศเพื่อการสื่อสารภายใต้ภาวะวิกฤติแสดงดังภาพที่ 2.5

ภาพที่ 2.5
แสดงกรอบการทำงานของแนวทางการเตรียมความพร้อมให้กับเทคโนโลยีสารสนเทศเพื่อการสื่อสารภายใต้ภาวะวิกฤติ

ที่มา: International Standard ISO/IEC 24762 First Edition (2008)

2.3 ปัจจัยความสำเร็จในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

จากการศึกษาวรรณกรรมที่เกี่ยวข้อง พบว่ามีกระบวนการมากมายในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ แต่มิได้เป็นจุดมุ่งหมายหลักในการทำการวิจัยในครั้งนี้ สิ่งที่เป็นจุดมุ่งหมายหลักของงานวิจัยนี้ คือ เพื่อจะทราบถึงปัจจัยความสำเร็จในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ ซึ่งนำมาเป็นแนวทางในการประยุกต์ใช้แผนฟื้นฟูระบบ

สารสนเทศจากภัยพิบัติกับองค์กรได้ต่อไป โดยสามารถสรุปผลการศึกษาปัจจัยความสำเร็จในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติได้ ดังนี้

1. ความมุ่งมั่นจากผู้บริหารระดับสูง (Top Management Commitment) แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัตินั้น เป็นเสมือนการลงทุนระยะยาวซึ่งต้องใช้เงินทุนเป็นจำนวนมาก อาจกล่าวได้ว่าเงินทุนเป็นอีกอุปสรรคหนึ่งที่ทำให้การประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติไม่ประสบความสำเร็จ เนื่องจากต้นทุนหรือค่าใช้จ่ายต่างๆที่เกี่ยวข้องในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัตินั้นมีจำนวนที่สูงมาก ซึ่งผลตอบแทนจากการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัตินั้นจะไม่ให้ผลตอบแทนในทันทีทันใด หรือแทบกล่าวได้ว่าไม่มีผลตอบแทนเลยในสถานะการณ์ปกติ เพราะฉะนั้นเงินทุน จึงเป็นสิ่งที่สำคัญอย่างมากในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Lee & Ross, 1995) นอกจากนั้น Rosenthal and Sheiniuk (1993) ให้ความเหตุที่สอดคล้องว่าในขั้นเริ่มต้นในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ ไม่ว่าจะเป็นแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติรูปแบบไหนก็ตามสิ่งที่ต้องมีก็คือเงินทุนจำนวนมาก และการทำให้ผู้บริหารระดับสูงเข้าใจและเห็นว่าการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัตินั้นคุมค่าแก่การลงทุน ซึ่งนั่นถือเป็นสิ่งที่ท่าทายอย่างหนึ่งในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Hawkins, et al., 2000) นอกจากเงินทุนแล้ว ข้อมูลต่างๆที่มีนัยสำคัญกับการดำเนินธุรกิจก็มีความสำคัญต่อการนำมาใช้ในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติซึ่งจะได้จากผู้บริหาระดับสูง (Blake, 1994) เพราะฉะนั้นผู้บริหารระดับสูงขององค์กรจึงเป็นส่วนประกอบที่สำคัญที่จะทำให้การพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติประสบความสำเร็จ (Effgen, 1992)) และทำให้มั่นใจได้ว่ากระบวนการทั้งหมด เริ่มตั้งแต่การพัฒนา การประยุกต์ใช้ การทดสอบ และการดูแลรักษา จะสามารถบรรลุความสำเร็จได้ (Rothstein, 1988) โดย Rohde and Haskett (1990) ให้ความเห็นว่า ความมุ่งมั่นและความตั้งใจที่จะประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติของผู้บริหารนั้นจะส่งผลให้พนักงานให้ความใส่ใจและให้ความสำคัญกับแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติขององค์กร ซึ่งทำให้การประยุกค์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติประสบผลสำเร็จ นอกจากนั้น Ginn (1989) ให้เหตุผลสนับสนุนปัจจับความสำเร็จข้อนี้ไว้ 3 เหตุผลข้อแรก ผู้บริหารระดับสูงเป็นผู้ตัดสินใจให้งบประมาณในการพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ เหตุผลที่สองผู้บริหารระดับสูงเป็นผู้ตัดสินว่าเมื่อไหร่จึงควรพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ และเหตุผลสุดท้ายนั่นคือ ผู้บริหารระดับสูงเป็นผู้ตัดสินใจว่า

ใครจะมีส่วนร่วมในการพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ โดยตัวชี้วัดสำหรับปัจจัยนี้มีดังนี้

- ต้องมีการเตรียมเงินทุนสนับสนุนที่เพียงพอในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Zolkos, 2000; Pember, 1996; Ferraro & Hayes, 1993)
- ต้องมีความมุ่งมั่นและตั้งใจในการพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Gluckman, 2000; Ginn, 1989; Rohde & Haskett, 1990)
- ให้การสนับสนุนการพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Bodnar, 1993; Coleman, 1993)
- ผู้บริหารสูงสุดเป็นผู้รับผิดชอบในผลของการพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Kull, 1982; Warigon, 1999; Carlson & Parker, 1998)

สำหรับงานวิจัยที่เกี่ยวข้องกับปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านความมุ่งมั่นจากผู้บริหารระดับสูง แสดงดังตารางที่ 2.1

ตารางที่ 2.1

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านความมุ่งมั่นจากผู้บริหารระดับสูง

Success Factor Measurement	Rothstein (1988)	Rohde and Haskett (1990)	Lee and Ross (1995)	Rosenthal and Sheiniuk (1993)	Blake (1994)	Cerullo et al. (1994)	Effgen (1992)	Hawkins et al. (2000)	Chow (2000)	Pember (1996)	Ferraro (1998)	Hayes (1998)	Ginn (1989)	Bodnar (1993)	Zolkos (2000)	Coleman (1993)	Carlson and Parker (1998)	Kull (1982)	Warigon (1999)	Chow and Ha (2008)
F1 **ความมุ่งมั่นของผู้บริหารระดับสูงต่อการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ** (Top management commitment to DRP)	X	X			X	X	X		X											X
M1 มีการเตรียมเงินทุนสนับสนุนที่เพียงพอในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Top management provides an adequate financial support for DRP)			X	X				X	X	X	X	X	X		X					
M2 มีความมุ่งมั่นในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Top management commits to DRP)		X											X							

ตารางที่ 2.1 (ต่อ)

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านความมุ่งมั่นจากผู้บริหารระดับสูง

Success Factor Measurement	Rothstein (1988)	Rohde and Haskett (1990)	Lee and Ross (1995)	Rosenthal and Sheiniuk (1993)	Blake (1994)	Cerullo et al. (1994)	Effgen (1992)	Hawkins et al. (2000)	Chow (2000)	Pember (1996)	Ferraro (1998)	Hayes (1998)	Ginn (1989)	Bodnar (1993)	Zolkos (2000)	Coleman (1993)	Carlson and Parker (1998)	Kull (1982)	Warigon (1999)	Chow and Ha (2008)
M3 ให้การสนับสนุนการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Top management supports DRP)														X		X				
M4 เป็นผู้รับผิดชอบในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Top management assumes ultimate responsibility for DRP)																	X	X	X	

2. กำหนดนโยบายและเป้าหมายในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Policy and Goal) ต้องมีความชัดเจน โดยถูกบันทึกไว้เป็นลายลักษณ์อักษร และถูกเผยเพร่ให้ทราบอย่างทั่วถึงภายในองค์กร โดยมีวัตถุประสงค์เพื่อเป็นแบบแผนในการปฏิบัติ รวมถึงการระบุผู้รับผิดชอบในแต่ละกระบวนการของแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (McNurlin, 1988; Turner, 1994) การกำหนดเป้าหมายและวัตถุประสงค์ต้องชัดเจน สามารถนำไปปฏิบัติได้จริง (Salzman, 1998) จะส่งผลให้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติมีประสิทธิภาพมากยิ่งขึ้น (Rothstein, 1998) โดยตัวชี้วัดสำหรับปัจจัยนี้มีดังนี้

- มีการกำหนดขอบเขตของการพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Iyer & Sarkis, 1998)
- มีการกำหนดวัตถุประสงค์และเป้าหมายของแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติที่สามารถปฏิบัติได้จริง (Hiatt & Motz, 1990)
- มีการกำหนดแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติเป็นนโยบายขององค์กร (Petroni, 1999; Turner, 1994)
- ผู้บริหารมีวิสัยทัศน์ที่ชัดเจนในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Zolkos, 2000)

สำหรับงานวิจัยที่เกี่ยวข้องกับปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการกำหนดนโยบายและเป้าหมายในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติแสดงดังตารางที่ 2.2

ตารางที่ 2.2

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านกำหนดนโยบายและเป้าหมาย

Success Factor Measurement	Hutt et al. (1988)	Snoyer and Fischer (1993)	Hawkins et al. (2000)	Chow (2000)	Zolkos (2000)	Chow and Ha (2008)	McNurlin (1988)	Turner (1994)	Salzman (1998)	Iyer and Sarkis (1998)	Hiatt และ Motz (1990)	Meade (1993)	Kovacich (1996)	Petroni (1999)
F2 **นโยบายและเป้าหมายในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ** (DRP policy and goals)	X	X	X			X	X	X	X					
M5 มีการกำหนดขอบเขตของแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติให้ชัดเจน (Top management defines the scope of DRP)										X				
M6 มีการกำหนดวัตถุประสงค์และเป้าหมายที่สามารถปฏิบัติได้จริงของแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติให้ชัดเจน (Top management defines realistic goals and objectives of DRP)				X							X	X	X	
M7 มีการกำหนดแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติให้อยู่ในนโยบายขององค์กร (Top management establishes the policy of DRP)								X						X

ตารางที่ 2.2 (ต่อ)

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านกำหนดนโยบายและเป้าหมาย

Success Factor Measurement	Hutt et al. (1988)	Snoyer and Fischer (1993)	Hawkins et al. (2000)	Chow (2000)	Zolkos (2000)	Chow and Ha (2008)	McNurlin (1988)	Turner (1994)	Salzman (1998)	Iyer and Sarkis (1998)	Hiatt และ Motz (1990)	Meade (1993)	Kovacich (1996)	Petroni (1999)
M8 ผู้บริหารต้องมีวิสัยทัศน์ที่ชัดเจนในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Top management has a clear vision of DRP)					X									

3. การจัดตั้งคณะกรรมการเพื่อดูแลรับผิดชอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอย่างเป็นทางการ (Steering Committee) ผู้บริหารระดับสูงต้องมีการจัดตั้งคณะกรรมการเพื่อดูแลรับผิดชอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ เนื่องจากในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอาจมีกระบวนการหรือข้อกำหนดที่มีผลกระทบต่อหน่วยธุรกิจในองค์กร ดังนั้นการประสานงานกันระหว่างหน่วยธุรกิจจึงเป็นสิ่งที่สำคัญและจำเป็นมาก (Rohde & Haskett,1990) โดยตัวแทนของแต่ละแผนกย่อมมีความเข้าใจถึงระบบงานของแผนกตัวเองเป็นอย่างดี ดังนั้นควรให้ตัวแทนของแต่ละแผนกเข้ามามีส่วนร่วมในการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ เพื่อได้ทราบถึงปัญหาหรือข้อเสนอแนะต่างๆ ที่เป็นประโยชน์ต่อการพัฒนาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติขององค์กร (Wong et al., 1994) ยิ่งไปกว่านั้น Hutt et al. (1988) สรุปว่าการจัดตั้งผู้มีอำนาจหรือคณะกรรมการมาเพื่อรับผิดชอบการพัฒนาและประยุกต์ใชแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ และดูแลการประสานงานกันระหว่างหน่วยธุรกิจในองค์กรเป็นสิ่งที่สำคัญมาก โดยตัวชี้วัดสำหรับปัจจัยนี้มีดังนี้

- มีการจัดดั้งคณะกรรมการในการพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอย่างเป็นทางการ (Hawkins et al., 2000; Wong et al., 1994)
- มีตัวแทนแต่ละแผนกเป็นหนึ่งในคณะกรรมการในการพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Cerullo, 1998; Wong et al., 1994)

สำหรับงานวิจัยที่เกี่ยวข้องกับปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการจัดตั้งคณะกรรมการเพื่อดูแลรับผิดชอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอย่างเป็นทางการแสดงดังตารางที่ 2.3

4. การกำหนดลำดับความสำคัญของโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศ (Prioritization of IS Function) โดยปกติแล้วโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศที่ใช้ในองค์กรมีความสำคัญที่แตกต่างกัน เช่น สำหรับองค์กรที่ประกอบธุรกิจหลักในการขายสินค้านั้น ระบบหรือแอปพลิชั่นที่เกี่ยวข้องกับการขาย การซื้อ การจัดการคลังสินค้าจะมีความสำคัญและสามารถทำให้เกิดกระทบต่อธุรกิจได้มากกว่าระบบเทรนนิ่งพนักงานเข้าใหม่ เป็นต้น เนื่องจากต้องใช้งบประมาณจำนวนมากในการดูแลอุปกรณ์ต่างๆที่เกียวกับแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ จึงเป็นสิ่งจำเป็นที่ต้องมีการจัดลำดับความสำคัญของโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศต่างๆที่มีใช้ภายในองค์การ (Lee & Ross, 1995) การจัดลำดับความสำคัญของโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศนั้นควรพิจารณาจากผลกระทบที่จะเกิดขึ้นกับ

ความสามารถในการดำเนินธุรกิจขององค์กรหากโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศนั้นหยุดทำงาน โดยโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศที่ส่งผลกระทบต่อความสามารถในการดำเนินธุรกิจขององค์กรมากที่สุด (Mission-Critical Application) ควรอยู่ในลำดับความสำคัญสูงสุดเช่นกัน Kull (1982) ได้กล่าวไว้ว่าการจัดลำดับความสำคัญของโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศเป็นองค์ประกอบที่สำคัญที่จะทำให้การพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติประสบความสำเร็จ โดยตัวชี้วัดสำหรับปัจจัยนี้มีดังนี้

- มีการกำหนดระดับความสำคัญของกิจกรรมหลักในการดำเนินธุรกิจ (Wong et al., 1994; Murphy, 1991)
- มีการกำหนดระดับความสำคัญของกระบวนการการฟื้นฟู/กู้คืน (Wong et al., 1994; Kull, 1982)
- มีการกำหนดระดับความสำคัญของช่วงเวลาของการฟื้นฟู/กู้คืน (Cerullo, 1998; Frost 1994)

สำหรับงานวิจัยที่เกี่ยวข้องกับปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการกำหนดลำดับความสำคัญของโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศ แสดงดังตารางที่ 2.3

ตารางที่ 2.3

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านคณะกรรมการเพื่อดูแลรับผิดชอบและลำดับความสำคัญของโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศ

Success Factor Measurement	Rohde and Haskett(1990)	Lee and Ross(1995)	Hutt et al. (1988)	Wong et al. (1994)	Hawkins et al. (2000)	Chow (2000)	Kull (1982)	Chow and Ha (2008)	Bodnar (1993)	Cerullo (1998)	Murphy (1991)	Frost (1994)
F3 **คณะกรรมการในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ** (DRP steering committee)	X		X					X	X			
M9 มีการจัดตั้งคณะกรรมการในการพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอย่างเป็นทางการ (A formal steering committee has been formed for disaster recovery plan)				X	X	X						
M10 มีตัวแทนแต่ละแผนกเป็นหนึ่งในคณะกรรมการในการพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Representatives from different department participate in the steering committee)				X						X		
F4 **ลำดับความสำคัญของโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศ** (Prioritization IS functions/services)		X				X	X	X				
M11 มีการกำหนดระดับความสำคัญของกิจกรรมหลักในการดำเนินธุรกิจ (Prioritization has been established for critical functions)				X								

ตารางที่ 2.3 (ต่อ)

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านคณะกรรมการเพื่อดูแลรับผิดชอบและลำดับความสำคัญของโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศ

Success Factor Measurement	Rohde and Haskett(1990)	Lee and Ross(1995)	Hutt et al. (1988)	Wong et al. (1994)	Hawkins et al. (2000)	Chow (2000)	Kull (1982)	Chow and Ha (2008)	Bodnar (1993)	Cerullo (1998)	Murphy (1991)	Frost (1994)
M12 มีการกำหนดระดับความสำคัญของกระบวนการการฟื้นฟู/กู้คืน (Prioritization has been established for recovery activities)		X										X
M13 มีการกำหนดระดับความสำคัญของช่วงเวลาของการฟื้นฟู/กู้คืน (Prioritization has been established for recovery schedules)										X		

5. การหาจำนวนโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศที่จำเป็นต้องถูกกู้คืน (Minimum IS Processing Requirement) เนื่องจากในสถานะการณ์ที่ประสบกับภัยพิบัติ องค์กรไม่มีเวลาหรือทรัพยากรที่เพียงพอในการกู้คืนระบบการทำงานทั้งหมดภายในระยะเวลาอันสั้น ดังนั้นแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติที่มีประสิทธิภาพจะต้องระบุถึงจำนวนโปรแกรมคอมพิวเตอร์ที่สำคัญและจำเป็นต้องถูกกู้คืนโดยทันที ซึ่งโปรแกรมคอมพิวเตอร์ที่ถูกกู้คืนเหล่านี้จะต้องทำให้องค์กรสามารถดำเนินธุรกิจต่อไปในระดับที่ยอมรับได้ (Coleman, 1993) โดยต้องอาศัยความร่วมมือจากตัวแทนในแต่ละแผนกเพื่อกำหนดจำนวนระบบงานอย่างน้อยที่จะต้องถูกกู้คืน (Doughty, 1991) ซึ่งการทราบถึงจำนวนระบบงานอย่างน้อยหรืออีกนัยหนึ่งคือระบบงานที่จำเป็นต่อการดำเนินธุรกิจ จะทำให้องค์กรสามารถเตรียมทรัพยากรเพื่อใช้ตามแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติในปริมาณที่เหมาะสมไม่มากไม่น้อยจนเกินไป เช่น จะทำให้ทราบว่าจะใช้รูปแบบของ ฮอตไซด์ (Hot Sites) หรือ โคลไซด์ (Cold site) ในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติถึงจะผลคุ้มค่ากว่ากัน (Wong et al., 1994) โดยตัวชี้วัดสำหรับปัจจัยนี้มีดังนี้

- หาระยะเวลาที่ยอมให้ระบบสารสนเทศส่วนที่มีความสำคัญหยุดทำงาน (Myers, 1999; Wong et al., 1994)
- หาระยะเวลาที่ยอมรับได้ในการฟื้นฟู/กู้คืนระบบสารสนเทศส่วนที่มีความสำคัญ (Gluckman, 2000; Douglas, 1998; Tilley, 1995)
- กำหนดจุดย้อนหลังของข้อมูล (เวอร์ชัน) ที่ถูกสำรองไว้เพื่อใช้ในการกู้คืน (Myatt, 1999; Douglas, 1998; Tilley, 1995)

สำหรับงานวิจัยที่เกี่ยวข้องกับปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการหาจำนวนโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศที่จำเป็นต้องถูกกู้คืน แสดงดังตารางที่ 2.4

ตารางที่ 2.4

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการหาจำนวนโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศที่จำเป็นต้องถูกกู้คืน

Success Factor Measurement	Wong et al. (1994)	Chow (2000)	Coleman (1993)	Chow and Ha (2008)	Myers (1999)	Gluckman (2000)	Douglas (1998)	Tilley (1995)	Myatt (1999)
F5 **ขีดจำกัดของโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศที่ยอมรับได้** (DRP minimum IS processing requirements)	X		X	X					
M14 หาระยะเวลาสูงสุดที่ยอมให้ระบบสารสนเทศส่วนที่มีความสำคัญหยุดทำงาน (An maximum allowable downtime of business functions has been determined)	X	X			X				
M15 หาระยะเวลาที่ยอมรับได้ในการฟื้นฟู/กู้คืนระบบสารสนเทศส่วนที่มีความสำคัญ (Acceptable recovery time of business functions has been determined)						X	X	X	
M16 กำหนดจุดย้อนหลังของข้อมูล(เวอร์ชัน) ที่ถูกสำรองไว้เพื่อใช้ในการกู้คืน (The point in time to which data must be restored of business functions has been determined)							X	X	X

6. ระบบการสำรองข้อมูลในไซต์งานหลัก (Internal, On-site Backup System) เนื่องจากระบบสารสนเทศมีความสำคัญต่อการดำเนินกิจการขององค์กรเป็นอย่างมากดังได้กล่าวมาแล้วข้างต้น ดังนั้นการสำรองข้อมูลจึงเป็นสิ่งที่หลีกเลียงไม่ได้ใน ซึ่งจำเป็นต้องมีกำหนดไว้ในการพัฒนาและประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ โดยข้อมูลจะต้องถูกทำการสำรองและเก็บไว้ในสถานที่ที่ปลอดภัย และเมื่อจำเป็นต้องใช้เพื่อกู้ข้อมูล ก็สามารถนำออกมาใช้ได้อย่างรวดเร็ว โดยระบบการสำรองข้อมูลในไซต์งานหลักจะเป็นการสำรองข้อมูลเก็บไว้ในอุปกรณ์บันทึกข้อมูล (Backup Storage) แล้วนำไปจัดเก็บไว้ในสถานที่ที่ปลอดภัยภายในไซต์งานนั้นๆ (Hawkins et al., 2000) ยกตัวอย่างเช่น การสำรองข้อมูลเก็บในเทปบันทึกข้อมูลแล้วนำไปจัดเก็บไว้ในตู้นิรภัยนอกห้องคอมพิวเตอร์หลักขององค์กร โดยตัวชี้วัดสำหรับปัจจัยนี้มีดังนี้

- มีการกำหนดสถานที่จัดเก็บอุปกรณ์บันทึกข้อมูลภายในไซต์งานหลัก (Leary, 1998; Peach, 1991)
- มีการกำหนดกระบวนการในการสำรองข้อมูลในไซต์งานหลัก (Hawkins et al., 2000; Rohde & Haskett, 1990)

สำหรับงานวิจัยที่เกี่ยวข้องกับปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านระบบการสำรองข้อมูลในไซต์งานหลัก แสดงดังตารางที่ 2.5

7. ระบบการสำรองข้อมูลในไซต์งานสำรอง (External, Off-site Backup System) เป็นการสำรองข้อมูลเก็บไว้ในอุปกรณ์บันทึกข้อมูล แล้วนำไปจัดเก็บไว้ในสถานที่ที่ปลอดภัยภายในไซต์งานสำรอง โดย Arnell (1990) แนะนำว่าไซต์งานสำรองจะต้องตั้งอยู่ห่างจากไซต์หลักเป็นระยะทางที่ไกลเพียงพอ โดยอย่างน้อยต้องไม่ได้รับผลกระทบจากภัยพิบัติที่ไซต์หลักประสบอยู่ และอีกประเด็นหนึ่งในการสำรองข้อมูลโดยใช้การแรพพลิเคท (Data Replication) หรือการสำรองข้อมูลผ่านช่องทางการเชื่อมต่อระหว่างไซต์งานหลักและไซต์งานสำรอง อาธิเช่น ผ่านโครงข่ายสื่อสารส่วนบุคคลหรือลีสไลด์ (Leased Line) เป็นต้น การทำเช่นนี้ต้องอาศัยความระมัดระวัง เนื่องจากเป็นการโอนย้ายข้อมูลซึ่งอาจมีความสำคัญหรือเป็นความลับของบริษัทนั่นเอง โดยตัวชี้วัดสำหรับปัจจัยนี้มีดังนี้

- มีการกำหนดสถานที่จัดเก็บอุปกรณ์บันทึกข้อมูลในไซต์งานสำรอง (Hawkins et al., 2000; Rohde & Haskett, 1990)
- มีการกำหนดกระบวนการในการสำรองข้อมูลในไซต์งานสำรอง (Hawkins et al., 2000; Rohde & Haskett, 1990)

สำหรับงานวิจัยที่เกี่ยวข้องกับปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านระบบการสำรองข้อมูลในไซต์งานสำรอง แสดงดังตารางที่ 2.5

ตารางที่ 2.5

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านระบบการสำรองข้อมูลในไซต์งานหลักและไซต์งานสำรอง

Success Factor Measurement	Rothstein (1988)	Rohde and Haskett (1990)	Arnell (1990)	Wong et al. (1994)	Yiu and Tse (1995)	Hawkins et al. (2000)	Chow and Ha (2008)	Leary (1998)	Peach (1991)
F6 **ระบบการสำรองข้อมูลในไซต์งานหลัก** (Internal, on-site back-up system)							X		
M17 มีการกำหนดกระบวนการที่เป็นทางเลือกในการสำรองข้อมูลในไซต์งานหลัก (An in-house alternative processing site has been established)								X	X
M18 มีการกำหนดกระบวนการในการสำรองข้อมูลในไซต์งานหลัก (On-site backup storage has been established for recovering business functions)		X				X			
F7 **ระบบการสำรองข้อมูลในไซต์งานสำรอง** (External, off-site back-up system)			X	X	X		X		
M19 มีการกำหนดกระบวนการที่เป็นทางเลือกในการสำรองข้อมูลในไซต์งานสำรอง (An external alternative processing site has been established)	X			X		X			

ตารางที่ 2.5 (ต่อ)

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านระบบการสำรองข้อมูลในไซต์งานหลักและไซต์งานสำรอง

Success Factor Measurement	Rothstein (1988)	Rohde and Haskett (1990)	Arnell (1990)	Wong et al. (1994)	Yiu and Tse (1995)	Hawkins et al. (2000)	Chow and Ha (2008)	Leary (1998)	Peach (1991)
M20 มีการกำหนดกระบวนการในการสำรองข้อมูลในไซต์งานสำรอง (Off–site backup storage has been established for recovering business functions)		X				X			

8. มีการทดสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Testing) ถ้าขาดการทดสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอย่างสม่ำเสมออาจทำให้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติไม่สามารถใช้งานได้จริง เพราะฉะนั้นแผนการทดสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติจะต้องถูกปฏิบัติอย่างสม่ำเสมอเพื่อให้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติพร้อมที่จะใช้งานได้จริงตลอดเวลา (Rittinghouse & Ransome, 2005) โดย Snoyer and Fischer (1993) ชี้ให้เห็นว่า การเปลี่ยนแปลงของบุคคลากร ลักษณะงาน เทคโนโลยี โครงสร้างของไซต์งานที่เปลี่ยนแปลงไป และสภาพแวดล้อมทางเศรษฐกิจอาจส่งผลกระบทต่อกระบวนการการปฏิบัติ และนโยบายต่างๆ ในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ ฉะนั้นการประเมินและตรวจสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอย่างต่อเนื่องมีความสำคัญและส่งผลต่อแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติให้พร้อมที่จะใช้งานอย่างประสิทธิภาพตลอดเวลา และยิ่งไปกว่านั้นการทำการทดสอบและทำการฝึกหัดแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอย่างสม่ำเสมอนั้นอาจทำให้เราได้พบข้อผิดผลาดหรือช่องโหว่ในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ ซึ่งก็จะนำไปสู่การปรับปรุงและแก้ไขต่อไป (Callaway, 2002) โดยตัวชี้วัดสำหรับปัจจัยนี้มีดังนี้

- ทดสอบโดยการจำลองสถานการณ์การเกิดภัยพิบัติจริง (Edwards & Cooper, 1994; Wong et al., 1994)
- ทดสอบโดยทำคู่ไปกับกิจกรรมปกติ (Wong et al., 1994)
- ทดสอบกระบวนการในแผนฟื้นฟู/กู้คืน (Wong et al., 1994)
- โดยทดสอบความปกติของระบบฟื้นฟู/กู้คืน (Edwards & Cooper, 1994; Wong et al., 1994)

สำหรับงานวิจัยที่เกี่ยวข้องกับปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการทดสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ แสดงดังตารางที่ 2.6

ตารางที่ 2.6

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการทดสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

Success Factor Measurement	Lee and Ross (1995)	Snoyer and Fischer (1993)	Wong et al. (1994)	Chow (2000)	Callaway (2002)	Rittinghouse and Ransome (2005)	Chow and Ha (2008)	Edwards and Cooper (1994)
F8 **มีการทดสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ** (DRP Testing)	X	X		X	X	X	X	
M21 ทดสอบโดยการจำลองสถานการณ์การเกิดภัยพิบัติจริง (Disaster recovery plan is tested as though a real disaster occurred)			X					X
M22 ทดสอบโดยทำคู่ไปกับกิจกรรมปกติ (Disaster recovery plan is tested by duplications of regular processing)			X			X		
M23 โดยทดสอบกระบวนการฟื้นฟู/กู้คืนแต่ละกระบวนการ (Disaster recovery plan is tested by testing individual recovery procedures)			X		X			

ตารางที่ 2.6 (ต่อ)

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการทดสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

Success Factor Measurement	Lee and Ross (1995)	Snoyer and Fischer (1993)	Wong et al. (1994)	Chow (2000)	Callaway (2002)	Rittinghouse and Ransome (2005)	Chow and Ha (2008)	Edwards and Cooper (1994)
M24 โดยทดสอบความปกติของระบบฟื้นฟู/กู้คืน (Disaster recovery plan is tested by testing recovery functions)			X					X

9. มีการอบรมบุคคลากรที่เกี่ยวข้อง (Training) โดยทีมงานทุกคนต้องมีความเข้าใจในบทบาทหน้าที่ความรับผิดชอบของตนเองอย่างชัดเจนและต้องได้รับการอบรมอย่างเพียงพอเพื่อให้เกิดความราบรื่นและรวดเร็วในการปฏิบัติการณ์เมื่อประสบกับสถานการณ์ภัยพิบัติ นอกจากทีมงานที่เกี่ยวข้องจะต้องได้รับการอบรมอย่างเพียงพอแล้ว ในกรณีมีการเปลี่ยนแปลงขั้นตอนหรือเนื้อหาในข้อปฏิบัติ ทีมงานมีหน้าที่ต้องรับรู้และปรับปรุงข้อมูลของตนเองด้วย (Hutt et al., 1988) Lee and Ross (1995) ยังกล่าวไว้ว่า ผู้ที่มีหน้าที่รับผิดชอบในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัตินั้นต้องมีความรู้ความเข้าใจเป็นอย่างดีในส่วนรับผิดชอบของตนเองและต้องได้รับการอบรมเพื่อให้สามารถแก้ไขปัญหาที่อาจจะเกิดขึ้น ได้ด้วยตนเองขณะประสบกับภัยพิบัติ โดยเนื้อหาการฝึกอบรมจะครอบคลุมถึงระบบความปลอดภัยของระบบสารสนเทศต่างๆที่เกี่ยวข้อง ขั้นตอนและกระบวนการที่กำหนดในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ เพื่อให้รู้และสามารถใช้งานระบบสารสนเทศต่างๆ ได้อย่างมีประสิทธิภาพ ตามแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Al-Zahrani, 2006; Jennex, 2007) โดยตัวชี้วัดสำหรับปัจจัยนี้มีดังนี้

- มีการอบรมบุคคลากรที่เกี่ยวข้องในด้านวิธีการปฏิบัติเมื่อเกิดภัยพิบัติ (Salzman, 1998)
- มีการอบรมบุคคลากรที่เกี่ยวข้องในด้านการจัดการในสถานการณ์ฉุกเฉิน (Paton & Flin, 1999; Turner, 1994)
- มีการอบรมบุคคลากรที่เกี่ยวข้องในด้านทักษะการทำงานเป็นทีม (Solomon, 1994; Paton & Flin, 1999)
- มีการอบรมบุคคลากรที่เกี่ยวข้องในด้านการประเมินความเสียหายเมื่อเกิดภัยพิบัติ (Turner, 1994)
- มีการอบรมบุคคลากรที่เกี่ยวข้องในด้านวิธีการเตือนภัยเมื่อเกิดภัยพิบัติ (Turner, 1994)
- มีการอบรมบุคคลากรที่เกี่ยวข้องในด้านหน้าที่และความรับผิดชอบเมื่อเกิดภัยพิบัติ (Smith & Sherwood, 1995)

สำหรับงานวิจัยที่เกี่ยวข้องกับปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการอบรมบุคคลากรที่เกี่ยวข้อง แสดงดังตารางที่ 2.7

ตารางที่ 2.7

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการอบรมบุคคลากรที่เกี่ยวข้อง

Success Factor Measurement	Lee and Ross (1995)	Hutt et al. (1988)	Al-Zahrani (2006)	Jennex (2007)	Chow (2000)	Chow and Ha (2008)	Turner (1994)	Salzman (1998)	Paton and Flin (1999)	Solomon (1994)	Smith and Sherwood (1995)
F9 **มีการอบรมบุคคลากรที่เกี่ยวข้อง** (DRP Training)	X	X	X	X	X	X	X				
M25 มีการอบรมบุคคลากรที่เกี่ยวข้องในด้านวิธีการปฏิบัติเมื่อเกิดภัยพิบัติ (Training in disaster response is given to recovery personnel)								X			
M26 มีการอบรมบุคคลากรที่เกี่ยวข้องในด้านการจัดการในสถานการณ์ฉุกเฉิน (Training stress management is given to recovery personnel)							X		X		
M27 มีการอบรมบุคคลากรที่เกี่ยวข้องในด้านทักษะการทำงานเป็นทีม (Training team skill is given to recovery personnel)									X	X	
M28 มีการอบรมบุคคลากรที่เกี่ยวข้องในด้านการประเมินความเสียหายเมื่อเกิดภัยพิบัติ (Training damage assessment is given to recovery personnel)				X			X				

ตารางที่ 2.7 (ต่อ)

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการอบรมบุคคลากรที่เกี่ยวข้อง

Success Factor Measurement	Lee and Ross (1995)	Hutt et al. (1988)	Al-Zahrani (2006)	Jennex (2007)	Chow (2000)	Chow and Ha (2008)	Turner (1994)	Salzman (1998)	Paton and Flin (1999)	Solomon (1994)	Smith and Sherwood (1995)
M29 มีการอบรมบุคคลากรที่เกี่ยวข้องในด้านวิธีการเตือนภัยเมื่อเกิดภัยพิบัติ (Training notification when an disaster strikes is given to recovery personnel)	X						X				

10. การบำรุงรักษาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Maintenance) การดูแลบำรุงรักษาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ (Maintenance of DRP) แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติจะมีประสิทธิภาพได้ก็ต้องมีการบำรุงรักษาตลอดเวลา เมื่อมีการเปลี่ยนแปลงโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศ หรือการเปลี่ยนแปลงในรูปแบบธุรกิจขององค์กรจะส่งผลกระทบต่อแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติไม่ทางใดก็ทางหนึ่ง เพราะฉะนั้นควรต้องมีการปรับปรุงแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติในทันสมัยเหมาะสมกับภาวะที่เปลี่ยนแปลงไป โดยต้องทำการปรับปรุงและแก้ไขให้บ่อยที่สุดเท่าที่ทำได้ เพราะสิ่งที่จะเกิดขึ้นถ้าแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติไม่มีการปรับปรุงให้เข้ากับสถานการณ์ก็คือ องค์กรจะไม่สามารถฟื้นฟูระบบสารสนเทศให้กลับมาใช้งานได้ตามแผนที่กำหนดไว้หรืออาจจะไม่สามารถกลับมาใช้ได้อีกเลย (Lee & Rose, 1995) โดยตัวชี้วัดสำหรับปัจจัยนี้มีดังนี้

- แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติต้องได้รับการประเมินและปรับปรุงอย่างต่อเนื่อง (Mitome et al., 2001; Miller, 1997)
- แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติต้องได้รับการตรวจสอบอย่างสม่ำเสมอ (Ebling, 1996; Matthews, 1994)
- แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติต้องได้รับการแก้ไขเพื่อรองรับกับสภาพแวดล้อมที่เปลี่ยนไป (Norman, 1993; Korzeniowski, 1990)

สำหรับงานวิจัยที่เกี่ยวข้องกับปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการบำรุงรักษาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ แสดงดังตารางที่ 2.8

ตารางที่ 2.8

แสดงปัจจัยความสำเร็จและตัวชี้วัดปัจจัยความสำเร็จด้านการบำรุงรักษาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ

Success Factor Measurement	Rothstein (1988)	Lee and Ross (1995)	Chow (2000)	Chow and Ha (2008)	Frost (1994)	Peterson and Perry (1999)	Mitome et al. and2001)	Miller (1997)	Ebling (1996)	Matthews (1994)	Norman (1993)	Korzeniowski (1990)
F10 **การบำรุงรักษาแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ** (DRP maintenance)	X	X	X	X	X	X						
M31 แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติต้องได้รับการประเมินและปรับปรุงอย่างต่อเนื่อง (Disaster recovery plan is evaluated continually)							X	X				
M32 แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติต้องได้รับการตรวจสอบอย่างสม่ำเสมอ (Disaster recovery plan is reviewed regularly)									X	X		
M33 แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติต้องได้รับการแก้ไขเพื่อรองรับกับสภาพแวดล้อมที่เปลี่ยนไป (Disaster recovery plan is updated with changes)											X	X

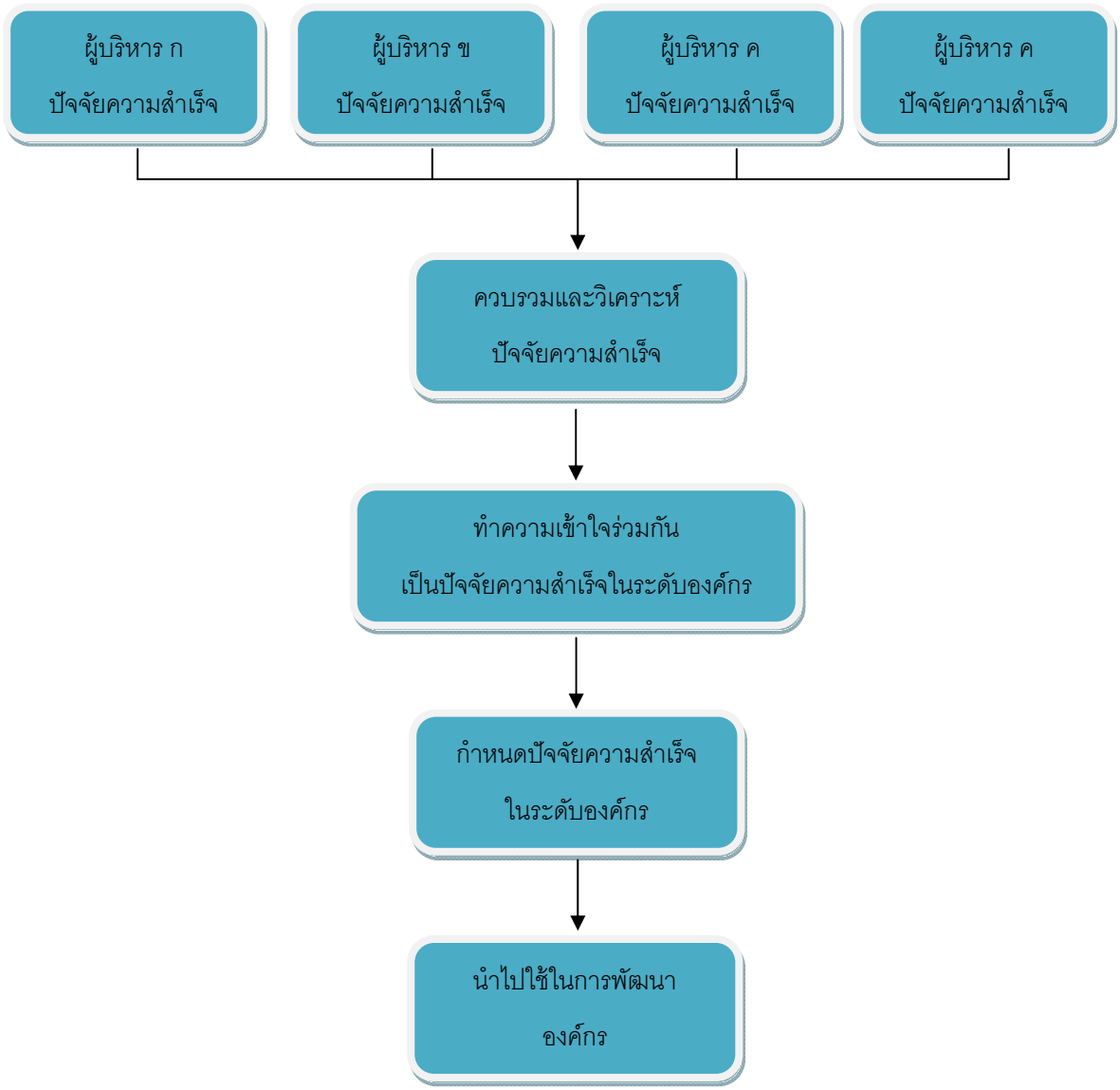
2.4 แนวคิดเกี่ยวกับปัจจัยความสำเร็จ

Kenneth C.Laudon and Jane P.Laudon (2000) กล่าวว่าปัจจัยความสำเร็จ คือ กลุ่มเป้าหมายในการดำเนินงานที่เป็นตัวรับประกันความสำเร็จขององค์กร ซึ่งแต่ละอุตสาหกรรม บริษัท ผู้บริหาร และสภาพแวดล้อมที่จะมีลักษณะของปัจจัยความสำเร็จที่แตกต่างกันออกไป วิธีการโดยส่วนมากที่ใช้ในการวิเคราะห์ปัจจัยความสำเร็จคือการสัมภาษณ์ผู้บริหารจำนวนหนึ่ง เพื่อที่จะให้ได้มาซึ่งเป้าหมายและปัจจัยความสำเร็จของพวกเขา ปัจจัยความสำเร็จเหล่านี้จะถูกนำมารวมกันเพื่อพัฒนาเป็นภาพใหญ่ของปัจจัยความสำเร็จขององค์กร ดังภาพที่ 2.6

ข้อดีของวิธีการนี้คือ การใช้ข้อมูลจำนวนไม่มากในการวิเคราะห์องค์กร เป็นการสัมภาษณ์ผู้บริหารเท่านั้นและคำถามที่ใช้จะมุ่นเน้นไปที่ปัจจัยความสำเร็จจำนวนไม่มาก แทนที่จะเป็นคำถามอย่างกว้าง วิธีนี้ยังสามารถปรับให้เหมาะสมกับโครงสร้างของแต่ละอุตสาหกรรมที่แตกต่างกัน จุดอ่อนของวิธีนี้ได้แก่ กระบวนการควบรวมและการวิเคราะห์ข้อมูลที่ไม่มีรูปแบบตายตัวเพื่อที่จะควบรวมปัจจัยย่อยต่างๆให้เป็นภาพใหญ่ของบริษัทที่ชัดเจน ปัญหาที่พบบ่อยคือความขัดแย้งระหว่างปัจจัยย่อยๆ และปัจจัยระดับองค์กรที่ไม่จำเป็นต้องตรงกันเสมอ นอกจากนั้นวิธีการนี้ยังโน้มเอียงไปตามผู้บริหารเพราะเป็นผู้ให้สัมภาษณ์ ท้ายที่สุดวิธีการนี้ไม่ครอบคลุมผลกระทบจากสภาพแวดล้อมหรือผู้หริหารที่เปลี่ยนแปลงไป (Kenneth C.Laudon & Jane P.Laudon, 2000)

ภาพที่ 2.6

แสดงวิธีการกำหนดปัจจัยความสำเร็จขององค์กร



ที่มา: “ปัจจัยความสำเร็จของระบบการบริหารคุณภาพแบบควอลิตี้คอนโทรล เซอร์เคิล และแบบซิกซ์ ซิกม่า” โดย วิบูลย์ ฉัตรจิตกรกุล, 2547

พักตร์ผจง วัฒนสินธุ์ (2542) กล่าวว่า นักวิชาการมีการพิจารณาถึงปัจจัยที่ก่อให้เกิดความสำเร็จของธุรกิจที่แตกต่างกันออกไป โดยส่วนใหญ่แล้วจะพิจารณาจากการวิเคราะห์ปัจจัยภายนอก และปัจจัยภายในองค์กร การวิเคราะห์ปัจจัยภายนอกประกอบด้วย 2 ส่วนคือ

1. ปัจจัยภายนอกที่เกี่ยวข้องกับองค์กรโดยตรง ได้แก่ การวิเคราะห์อุตสาหกรรม คู่แข่งขัน ลูกค้า ผู้จัดส่งวัตถุดิบ

2. ปัจจัยภายนอกที่ไม่เกี่ยวข้องกับองค์กรโดยตรง ได้แก่ การวิเคราะห์ปัจจัยด้านเศรษฐกิจ สังคม การเมือง กฎหมาย การค้า เทคโนโลยี วัฒนธรรม

โดยการเปลี่ยนแปลงของปัจจัยภายนอกทั้งสองย่อมส่งผลให้เกิดโอกาสหรือข้อจำกัดต่อองค์กรธุรกิจ รวมทั้งส่งผลต่อความสามารถในการแข่งขันขององค์กร ส่วนปัจจัยภายในองค์กรนั้นสามารถใช้วิธีการวิเคราะห์ได้หลายวิธีด้วยกัน อาธิเช่น การวิเคราะห์ตามสายงาน (Function Analysis), การวิเคราะห์ตามตัวแบบ Value Chain, หรือการวิเคราห์ทรัพยากรและความสามารถภายใน (Resources and Capabilities Analysis) โดยการวิเคราห์แต่ละวิธีช่วยให้ทราบถึงจุดแข็งและจุดอ่อนขององค์กร ที่จะนำมาพิจารณากำหนดความสามารถในการแข่งขันขององค์กรต่อไป

2.5 **การวิเคราะห์องค์ประกอบ** (Factor Analysis)

กระบวนการวิเคราะห์องค์ประกอบถือกำเนิดขึ้นมาในช่วงต้นศตวรรษที่ 20 โดย Spearman (1904) แต่การวิเคราะห์องค์ประกอบสมัยนั้นยังเป็นวิธีการที่ยุ่งยาก ซับซ้อนและเสียเวลามาก ดังนั้น การวิเคราะห์องค์ประกอบจึงยังไม่เป็นที่แพร่หลายในหมู่นักวิจัยสมัยนั้น จนกระทั่งคอมพิวเตอร์ได้ถือกำเนิดขึ้น และตามมาด้วยโปรแกรมคอมพิวเตอร์ที่จะช่วยเหลือในการวิเคราะห์องค์ประกอบ ดังนั้นการวิเคราะห์องค์ประกอบจึงได้แพร่หลายออกไปในหมู่นักวิจัยอย่างกว้างขวาง

Kerlinger (1986) ได้กล่าวถึงการวิเคราะห์องค์ประกอบไว้ว่า การวิเคราะห์องค์ประกอบเป็นเครื่องมืออย่างหนึ่งที่มีประโยชน์มาก ถูกสร้างขึ้นมาเพื่อใช้ศึกษาปัญหาที่ซับซ้อนในศาสตร์ทางพฤติกรรม

Deniel (1988) ได้พูดถึงการวิเคราะห์องค์ประกอบไว้ว่า การวิเคราะห์องค์ประกอบถูกออกแบบมาเพื่อใช้ตรวจสอบโครงสร้างของชุดตัวแปรและเพื่อใช้อธิบายความสัมพันธ์ของตัวแปรในรูปของจำนวนที่น้อยที่สุดของตัวแปรแฝงที่สังเกตไม่ได้ ซึ่งตัวแปรแฝงที่สังเกตไม่ได้เหล่านี้ถูกเรียกว่า “องค์ประกอบ”

Joreskog and Sorbom (1989) ได้อธิบายว่า แนวคิดที่สำคัญภายใต้รูปแบบของการวิเคราะห์องค์ประกอบ คือ มีตัวแปรบางตัวที่ไม่สามารถสังเกตหรือวัดได้โดยตรง หรืออาจเรียก

ได้ว่าเป็นตัวแปรแฝงหรือองค์ประกอบ ตัวแปรที่ไม่สามารถสังเกตหรือวัดได้โดยตรงนั้น สามารถอ้างอิงได้ทางอ้อมจากข้อมูลของตัวแปรที่สังเกตได้ การวิเคราะห์องค์ประกอบเป็นกระบวนการทางสถิติสำหรับเปิดเผย (Uncooerion) ตัวแปรแฝงที่มีอยู่ โดยศึกษาผ่านความแปรปรวนระหว่างชุดของตัวแปรที่สังเกตได้

จากนิยามอาจกล่าวได้ว่า การวิเคราะห์องค์ประกอบ เป็นเทคนิคที่ใช้ในการจับกลุ่มหรือรวมตัวแปรที่มีความสัมพันธ์ไว้ในกลุ่มหรือองค์ประกอบ (Factors) เดียวกัน ซึ่งจะมีความสัมพันธ์กันมาก โดยความสัมพันธ์นั้นอาจจะเป็นทิศทางบวก (ไปในทิศทางเดียวกัน) หรืออาจจะเป็นทิศทางลบ (ไปในทางตรงกันข้ามกัน) ก็ได้ ส่วนตัวแปรที่อยู่คนละองค์ประกอบกัน จะไม่มีความสัมพันธ์กัน หรือมีความสัมพันธ์กันน้อยมาก

จุดมุ่งหมายในการวิเคราะห์องค์ประกอบมี 2 ประการคือ

1. เพื่อสำรวจหรือค้นหาตัวแปรแฝงที่ซ่อนอยู่ภายใต้ตัวแปรที่สังเกตหรือวัดได้ เรียกว่า การวิเคราะห์องค์ประกอบเชิงสำรวจ (Exploratory Factor Analysis) โดยกำหนดว่าจำนวนองค์ประกอบจะอธิบายความแปรปรวนร่วมระหว่างตัวแปร ซึ่งผู้วิจัยไม่มีหลักฐานอ้างอิงเพียงพอสำหรับเป็นกรอบของสมมติฐานเกี่ยวกับจำนวนขององค์ประกอบภายใต้ข้อมูลที่ทำการสอบวัด

2. เพื่อพิสูจน์ ตรวจสอบหรือยืนยันทฤษฎีที่ผู้อื่นค้นพบ เรียกว่า การวิเคราะห์องค์ประกอบเชิงยืนยัน (Confirmation Factor Analysis) มีขั้นตอนการดำเนินการที่ค่อนข้างสลับซับซ้อนและจำเป็นต้องอาศัยเทคนิคการวิเคราะห์ทางสถิติขั้นสูง

โดยในงานวิจัยนี้ได้ประยุกต์ใช้การวิเคราะห์องค์ประกอบเชิงสำรวจในการหาปัจจัยความสำเร็จในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติที่มีความสำคัญและสอดคล้องกับองค์กร โดยใช้ข้อมูลที่ได้จากการสำรวจระดับความคิดเห็นของบุคคลากรภายในองค์กรที่มีต่อปัจจัยความสำเร็จในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ ซึ่งการวิเคราะห์องค์ประกอบเชิงสำรวจแบ่งเป็น 6 ขั้นตอนดังนี้

ขั้นที่ 1 การสร้างเมตริกความสัมพันธ์ระหว่างคู่ของตัวแปร เป็นการตรวจสอบว่าตัวแปรต่างๆ มีความสัมพันธ์กันหรือไม่ ถ้าตัวแปรมีความสัมพันธ์กันมาก หรือมีความสัมพันธ์กันอย่างมีนัยสำคัญ จะสามารถใช้ในการวิเคราะห์องค์ประกอบได้ แต่ถ้าตัวแปรไม่มีความสัมพันธ์

หรือมีความสัมพันธ์กันน้อย ไม่ควรใช้เทคนิควิเคราะห์องค์ประกอบนี้ โดยสามารถตรวจสอบได้ 2 วิธีคือ

วิธีที่ 1 การตรวจสอบโดยใช้ค่าสัมประสิทธิ์สหสัมพันธ์ โดยการสร้างเมทริกซ์แสดงสัมประสิทธิ์สหสัมพันธ์ของตัวแปรทุกคู่

- ถ้าสัมประสิทธิ์สหสัมพันธ์ของตัวแปรคู่ใดมีค่าใกล้ +1 หรือ -1 แสดงว่าตัวแปรคู่นั้นมีความสัมพันธ์กันมาก ควรอยู่ในองค์ประกอบเดียวกัน
- ถ้าค่าสัมประสิทธิ์สหสัมพันธ์ของตัวแปรคู่ใดมีค่าใกล้ศูนย์ แสดงว่าตัวแปรคู่นั้นไม่มีความสัมพันธ์กันหรือสัมพันธ์กันน้อย ควรอยู่คนละองค์ประกอบ
- ถ้ามีตัวแปรที่ไม่มีความสัมพันธ์กับตัวแปรอื่นๆ หรือมีความสัมพันธ์กับตัวแปรอื่นๆที่เหลือน้อยมาก ควรตัดตัวแปรนั้นออกจากการวิเคราะห์

วิธีที่ 2 ผู้วิเคราะห์สามารถตรวจสอบโดยใช้สถิติ KMO (Kaiser-Meyer-Olkin) โดยค่า KMO เป็นการทดสอบว่าข้อมูลมีความเหมาะสมในการใช้วิเคราะองค์ประกอบหรือไม่ โดยค่าที่ได้ควรจะมากกว่า 0.6 (Foster et al., 2006) จึงจะถือว่าข้อมูลนั้นเหมาะสมที่จะนำมาวิเคราะห์องค์ประกอบ

ขั้นที่ 2 การสกัดองค์ประกอบหรือการสกัดปัจจัย (Factor Extraction) เป็นการค้นหาจำนวนองค์ประกอบที่มีความสามารถเพียงพอในการอธิบายความสัมพันธ์ระหว่างตัวแปรที่สังเกตได้ ทำให้ได้เมตริกซ์น้ำหนักองค์ประกอบ (Factor Loading Matrix) โดยผลลัพธ์ของการสกัดองค์ประกอบจะช่วยในการตัดสินใจเกี่ยวกับจำนวนองค์ประกอบเพื่อเก็บไว้สำหรับใช้ในการวิเคราะห์ต่อไป กฎที่ดีที่สุดสำหรับการกำหนดจำนวนองค์ประกอบคือ “Eigenvalue > 1” ค่า Eigenvalue เป็นค่าที่บ่งบอกถึงความสามารถขององค์ประกอบว่าจะอธิบายความแปรปรวนของกลุ่มตัวแปรได้มากน้อยเพียงใด โดยปกติถ้าองค์ประกอบนั้นมีค่า Eigenvalue น้อยกว่า 1 ก็ไม่มีประโยชน์ที่จะนำเอาองค์ประกอบนั้นมาใช้ในการวิเคราะห์ กล่าวโดยสรุปว่าการสกัดองค์ประกอบเป็นการหาจำนวนองค์ประกอบใหม่ที่สามารถใช้แทนตัวแปรทั้งหมดทุกตัวได้ ซึ่งจะได้เป็นเมตริกซ์น้ำหนักองค์ประกอบ โดยวิธีการสกัดองค์ประกอบแบ่งออกเป็น 2 วิธีใหญ่ดังนี้

1. วิธีวิเคราะห์องค์ประกอบหลัก (Principal Component Analysis: PCA)
2. วิธีวิเคราะห์องค์ประกอบร่วม (Common Factor Analysis: CFA)

ขั้นที่ 3 การจัดตัวแปรให้อยู่ในองค์ประกอบต่างๆ หลังจากสามารถหาค่าน้ำหนักองค์ประกอบ (Factor Loading) ได้แล้ว จะนำมาใช้พิจารณาว่าตัวแปรใดบ้างที่ควรอยู่ใน

องค์ประกอบเดียวกัน โดยพิจารณาค่าน้ำหนักองค์ประกอบของแต่ละตัวแปร ถ้าตัวแปรใดมีค่าน้ำหนักองค์ประกอบมาก (เข้าสู่ +1 หรือ -1) ควรจัดตัวแปรนั้นให้อยู่ในองค์ประกอบ ดังกล่าว แต่ในกรณีที่ไม่แน่ใจว่าควรจะจัดตัวแปรไว้ในองค์ประกอบใดให้ทำการหมุนแกนปัจจัยดังอธิบายในขั้นที่ 4

ขั้นที่ 4 การหมุนแกนปัจจัย (Factor Rotation) เป็นขั้นตอนที่จะแยกตัวแปรแต่ละตัวว่าควรจะอยู่ในองค์ประกอบใด เพราะเนื่องจากขั้นตอนการสกัดปัจจัยนั้น ตัวแปรหนึ่งๆ อาจจะอยู่หรือเป็นสมาชิกขององค์ประกอบหลายตัว ซึ่งทำให้ยากต่อการให้ความหมายและการกำหนดชื่อขององค์ประกอบ ดังนั้นการหมุนแกนจะเป็นวิธีที่จะทำให้ทราบได้ชัดเจนมากยิ่งขึ้นว่าตัวแปรใดความอยู่หรือเป็นสมาชิกขององค์ประกอบใด วิธีการหมุนแกนสามารถแบ่งได้เป็น 2 วิธีใหญ่คือ

1. การหมุนแกนแบบมุมฉาก (Orthogonal) เป็นการหมุนแกนปัจจัยจากตำแหน่งเดิมในลักษณะตั้งฉากทำให้แต่ละปัจจัยเป็นอิสระต่อกัน แต่ให้ค่าน้ำหนักเฟกเตอร์ (Factor Loading) เพิ่มขึ้นหรือลดลง โดยมีวิธีย่อยหลายวิธี คือ 1) Varimax 2) Equamax และ 3) Quartimax

2. การหมุนแกนแบบมุมแหลม (Oblique Rotation) เป็นการหมุนแกนปัจจัยจากตำแหน่งเดิมในลักษณะไม่ตั้งฉากกันทำให้แต่ละปัจจัยไม่เป็นอิสระต่อกัน แต่ให้ค่าน้ำหนักเฟกเตอร์ (Factor Loading) เพิ่มขึ้นหรือลดลง โดยมีวิธีย่อยหลายวิธี คือ 1) Direct Oblimin และ 2) Promax

ขั้นที่ 5 การให้ความหมายแก่องค์ประกอบ (Factor Meaning) เมื่อพิจารณาได้แล้วว่าแต่ละองค์ประกอบ ประกอบด้วยตัวแปรใดบ้าง ต้องทำการกำหนดชื่อหรือให้ความหมายแก่องค์ประกอบหรือตัวแปรที่ได้โดยพิจารณาว่าในปัจจัยหรือองค์ประกอบนั้นๆ ประกอบด้วยตัวแปรอะไรบ้างที่เป็นสมาชิกอยู่ แต่เนื่องจากองค์ประกอบหนึ่งๆ ประกอบไปด้วยตัวแปรทุกตัวที่เป็นสมาชิก โดยมีน้ำหนักของการเป็นสามาชิกแตกต่างกัน ดังนั้นก่อนการให้ความหมายแก่องค์ประกอบใดๆ ควรจะต้องพิจารณาเลือกตัวแปรที่น่าจะเป็นสมาชิกขององค์ประกอบนั้นๆ มากที่สุด หลังจากนั้นจึงให้ความหมายแก่องค์ประกอบที่ได้แต่ละองค์ประกอบ ซึ่งขั้นตอนในการพิจารณา (ศิริชัย พงษ์วิชัย, 2544) มีดังนี้

1. จัดตัวแปรให้เป็นสมาชิกในองค์ประกอบเดียว เป็นขั้นตอนที่จะดำเนินการแยกตัวแปรให้เห็นเด่นชัดว่า ตัวแปรหนึ่งๆ ควรจะถูกจัดอยู่ในกลุ่มหรือองค์ประกอบใด โดยนำค่าน้ำหนักองค์ประกอบหรือสัมประสิทธิ์ของแต่ละองค์ประกอบ ที่ได้ล่าสุดจากการหมุนแกนและเลือก

เฉพาะปัจจัย ที่มีค่า Eigenvalues หรือค่า Percent of Variance สูงตามขั้นตอนการคัดเลือกปัจจัยแล้ว จึงพิจารณาค่าน้ำหนักหรือสัมประสิทธิ์ของแต่ละปัจจัยของปัจจัยทั้งหมดที่เลือกมาว่าน้ำหนักปัจจัยหรือค่าสัมประสิทธิ์ของปัจจัยใดมีค่ามากที่สุด ก็จะหมายความว่าปัจจัยนั้นมีความสัมพันธ์กับตัวแปรนั้นมากที่สุด แสดงว่าตัวแปรนั้นๆ ควรเป็นสมาชิกของปัจจัยนั้นมากกว่าที่จะเป็นสมาชิกของปัจจัยอื่น

2. เลือกตัวแปรที่มีผลสูงต่อปัจจัย จากขั้นตอนที่ผ่านมาถึงแม้ว่าจะได้ตัวแปรที่เป็นสมาชิกในปัจจัยเดียวแล้ว แต่ตัวแปรบ้างตัวที่เข้ามาเป็นสมาชิกในปัจจัย อาจจะมีน้ำหนักการเข้ารวมตัวหรือมีความสามารถในการอธิบายปัจจัยนั้นๆต่ำ ซึ่งอาจจะกล่าวได้ว่า ถึงแม้จะไม่มีตัวแปรดังกล่าวก็สามารถให้ความหมายแก่ปัจจัยได้เพียงพออยู่แล้ว การพิจารณาจะพิจารณาจากค่าน้ำหนักหรือสัมประสิทธิ์สหสัมพันธ์ของตัวแปรจากตัวแบบการรวมตัวแบบเส้นตรง โดยจะเลือกค่าตัวแปรที่มีค่าสัมประสิทธิ์สูงซึ่งอาจจะใช้วิธีทดสอบความสัมพันธ์ทางสถิติ

3. การให้ความหมายแก่ปัจจัย เป็นขั้นตอนที่ต้องให้ความหมายหรือกำหนดชื่อแก่แต่ละปัจจัย ซึ่งในขั้นตอนนี้จะต้องอาศัยประสบการณ์ในการกำหนด หรือใช้ชื่อที่สื่อความหมายแก่แต่ละปัจจัย ทำได้โดยพิจารณาลักษณะของตัวแปรที่อยู่ในปัจจัยนั้นๆ

กล่าวโดยสรุปคือ การวิเคราะห์องค์ประกอบเป็นเทคนิคการจับกลุ่มหรือรวมตัวแปรที่มีความสัมพันธ์กัน ไว้ในกลุ่มหรือปัจจัยเดียวกัน มีขั้นตอนการวิเคราะห์ คือ

1. การสร้างเมตริกสหสัมพันธ์ระหว่างคู่ของตัวแปร
2. การสกัดองค์ประกอบหรือการสกัดปัจจัย
3. การจัดตัวแปรให้อยู่ในองค์ประกอบต่างๆ
4. การหมุนแกนปัจจัย
5. การให้ความหมายแก่องค์ประกอบให้

โดยในงานวิจัยนี้จะเลือกใช้วิธีวิเคราะห์องค์ประกอบหลัก (Principal Component Analysis: PCA) เป็นวิธีสกัดองค์ประกอบ ซึ่งวิธีวิเคราะห์องค์ประกอบหลักนี้อาศัยความสัมพันธ์เชิงเส้นของตัวแปรที่ใช้เป็นข้อมูล องค์ประกอบหลักอันดับแรกเป็นการผสมเชิงเส้น (Linear Combination) ของตัวแปรที่อธิบายการผันแปรของข้อมูลได้มากที่สุด และองค์ประกอบหลักอันดับที่สองเป็นการผสมเชิงเส้นของตัวแปรที่สามารถอธิบายการผันแปรของข้อมูลได้มากเป็นอันดับที่สอง โดยที่ไม่สัมพันธ์กับการผสมแรก ทำเช่นนี้ไปเรื่อยๆ จนได้องค์ประกอบหลักที่สามารถ

อธิบายการผันแปรของทุกตัวแปรได้ครบถ้วน ซึ่งองค์ประกอบหลักจะอธิบายการผันแปรได้น้อยลงตามลำดับและทุกองค์ประกอบจะไม่สัมพันธ์กัน และเลือกใช้วิธีการหมุนแกนแบบมุมฉากแวรี่แมกซ์ (Verimax) ซึ่งวิธีนี้จะลดจำนวนตัวแปรที่มีน้ำหนักปัจจัยมากบนแต่ละปัจจัยให้เหลือน้อยที่สุด ซึ่งจะทำให้ได้เฉพาะตัวแปรที่มีค่าสัมประสิทธิ์ในการรวมตัวแบบเชิงเส้นสูง หรืออีกนัยหนึ่งคือ มุ่งไปที่ความแตกต่างหรือความแปรปรวนของแต่ละองค์ประกอบโดยพยายามทำให้องค์ประกอบแต่ละคอลัมแตกต่างกันให้มากที่สุดซึ่งจะช่วยให้ตีความหมายของปัจจัยได้ง่าย

ซึ่งวิธีวิเคราะห์องค์ประกอบหลัก (PCA) และวิธีการหมุนแกนแบบมุมฉากแวรี่แมกซ์ (Verimax) ถูกใช้ในงานวิจัยของ Chow et al. (2009) เรื่อง “Determinant of the critical success factor of disaster recovery planning of information systems” ตีพิมพ์ใน Emerald, Information Management & Computer Security Vol.17 No. 3, 2009

2.6 งานวิจัยที่เกี่ยวข้อง

วัชรีวรรณ วัดบัว (2004) ทำการศึกษาเรื่อง การสำรองข้อมูลด้วยนวตกรรมใหม่ : Backup Media ถูกตีพิมพ์ใน อินฟอร์เมชั่น ปีที่ 11 ฉบับ 2 (กรกฎาคม-ธันวาคม 2547) ได้สรุปไว้ว่า ข้อมูลเป็นสิ่งที่มีคุณค่า ซึ่งคุณค่าของข้อมูลมีทั้งในด้านมูลค่าในตัวเองและมูลค่าจากวัตถุประสงค์ที่จะนำไปใช้ การที่ข้อมูลถูกทำลายนับเป็นปัญหาสำคัญประการหนึ่ง หากไม่ได้มีการสำรองข้อมูลไว้ จะทำให้เกิดความเสียหายที่ไม่อาจประมาณค่าได้ ถึงแม่ว่าในบ้างครั้งอาจสร้างข้อมูลขึ้นใหม่ได้ แต่อาจไม่เหมือนเดิน ดังนั้น จึงจำเป็นที่ต้องมีแนวปฏิบัติอย่างเคร่งครัดในการปกป้องข้อมูล นั่นคือ การทำการสำรองข้อมูล ซึ่งต้องมีการพิจารณาความจำเป็นและความต้องการ เพื่อนำมาจัดลำดับความสำคัญก่อนหลัง และเพื่อเป็นปัจจัยในการเลือกใช้ระบบสำรองข้อมูลและอุปกรณ์บันทึกข้อมูลได้อย่างมีประสิทธิภาพ และเพื่อหลีกเลี่ยงปัญหาและผลกระทบจากเหตุการณ์ที่ไม่อาจคาดเดาได้ในอนาคต ควรมีการเตรียมพร้อมรับมือตลอดเวลา

Karakasidis (1997) ได้เสนอกระบวนการในการวางแผนเพื่อความต่อเนื่องของธุรกิจ โดยเริ่มจากต้องได้รับการสนับสนุนและการอนุมัติจากผู้บริหารระดับสูงก่อนซึ่งเป็นสิ่งที่สำคัญอย่างมาก จากนั้นต้องมีการจัดตั้งทีมงานเพื่อพัฒนาและรับผิดชอบ โดยทีมงานจะเริ่มทำการวิเคราะห์ผลกระทบที่อาจเกิดกับธุรกิจในทุกๆ ด้าน ผลที่ได้คือจะทำให้ทราบว่าอะไรคือสิ่งที่มีความสำคัญและจำเป็นต่อองค์กรหรือต่อธุรกิจ เมื่อทราบแล้วก็ทำการจัดลำดับความสำคัญของปัจจัยเหล่านั้น เพื่อใช้ประกอบในการพิจารณากลยุทธในการสร้างความต่อเนื่องทางธุรกิจใดที่มี

ความเหมาะสมกับองค์กร และรวมถึงวางแผนการเพื่อประยุกต์ใช้กลยุทธเหล่านั้นด้วย เพื่อเสนอให้ผู้บริหารพิจารณาอนุมัติโครงการ และหลังจากนั้นทำการกำหนดข้อปฏิบัติและกระบวนการของแผนสร้างความต่อเนื่องทางธุรกิจ โดยมีพื้นฐานอยู่ข้อมูลและความเหมาะสมกับองค์กร เมื่อกระบวนการต่างๆถูกกำหนดไว้อย่างรอบครอบแล้ว จากนั้นทำการทดสอบกระบวนการที่พัฒนาขึ้นมาเพื่อประเมินผลว่าเหมาะสมและมีประสิทธิภาพต่อองค์กรหรือไม่ เพื่อจะได้กำหนดระดับการให้บริการ (SLAs) เพื่อเป็นตัวชี้วัดความสำเร็จของแผนการเพื่อความต่อเนื่องทางธุรกิจนี้ และเมื่อทุกขั้นตอนเสร็จสมบูรณ์แล้ว สิ่งที่สำคัญและขาดไม่ได้เลย นั้นก็คือ การปรับปรุงและแก้ไขกระบวนการและข้อปฏิบัติต่างๆ ในแผนเพื่อความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ

Cervone (2006) ได้เสนอแนวทางในการวางแผนฟื้นฟูจากภัยพิบัติเพื่อความต่อเนื่องในการให้บริการสำหรับระบบสารสนเทศของห้องสมุด ซึ่งเขาชี้ให้เห็นปัญหาว่า 2 ใน 5 องค์กรที่ประสบกับภัยพิบัติอย่างรุ่นแรง ไม่สามารถที่จะฟื้นฟูระบบกลับมาให้ใช้งานได้อีก ดังนั้นการพัฒนาและประยุกต์ใช้แผนฟื้นฟูภัยพิบัติเพื่อความต่อเนื่องในการให้บริการของห้องสมุดอิเลคทรอนิคนั้น ในระยะยาวจะสามารถเพิ่มโอกาศในการกู้คืนทรัพยากรทางวิชาการต่างๆของสถาบันได้มากขึ้น โดยเขายังอธิบายถึงความเหมือนและแตกต่างของ DRP และ BCP ว่าทั้งสองเป็นแผนการในการฟื้นฟูเช่นเดียวกัน แต่ DRP หรือแผนฟื้นฟูจากภัยพิบัตินั้นจะเน้นไปยังการฟื้นฟูระบบสารสนเทศและแอปพลเคชั่นเป็นหลัก ในขณะที่ BCP หรือแผนเพื่อความต่อเนื่องทางธุรกิจนั้น จะเกี่ยวข้องกับการฟื้นฟูกิจกรรมที่สำคัญและมีความจำเป็นต่อธุรกิจให้กลับมาดำเนินต่อไปเป็นหลัก ดังนั้นเมื่อมองระบบสารสนเทศเป็นสิ่งสำคัญที่ทำให้เกิดกิจกรรมทางธุรกิจแล้ว สามารถที่จะประยุกต์ใช้แผนเพื่อความต่อเนื่องทางธุรกิจเพื่อครอบคลุมระบบสารสนเทศได้เช่นเดียวกัน แต่อย่างไรก็ตามในแต่ละขั้นตอนในการประยุกต์ใช้แผนเพื่อความต่อเนื่องทางธุรกิจนั้นจะต้องใช้ทรัพยากรขององค์กรเป็นจำนวนมากกว่าการประยุกต์ใช้เพียงแค่แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ นอกจากนั้นเขายังแนะนำวิธีที่ดีที่สุดในการเริ่มต้นการวางแผนนั้นก็คือ การวิเคราะห์ผลกระทบ และการประเมินความเสี่ยงขององค์กร ซึ่งข้อมูลที่ได้จากการวิเคราะห์ผลกระทบ และการประเมินความเสี่ยงขององค์กรนั้น โดยปกติและจะถูกนำไปใช้ประโยชน์ในการพัฒนาแผน การจัดการ และรวมไปถึงการทำการทดสอบด้วย

Edwards and Cooper (1995) ได้เสนอแนวทางในการทดสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ โดยเขาได้ทำการสรุปสาเหตุที่ ทำไมองค์กรไม่ทำการทดสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ ข้อแรก ความมั่นใจในบุคคลากรทางด้านเทคนิคว่าจะสามารถทำตามแผนปฏิบัติการและแก่ปัญหาต่างๆได้อย่างลุล่วง ขณะประสบภัยพิบัติ ถึงแม่ว่าพนักงานจาก

สามารถทำงานได้ตรงตามแผนปฏิบัตการณ์ที่วางไว้และทำได้ตรงต่อเวลา แต่แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติที่ไม่เคยถูกทดสอบเลยจะมีโอกาสสูงที่แต่ละขั้นตอนของการปฏิบัติจะไม่สามารถใช้งานได้จริงในขณะเกิดเหตุ เหตุผลที่สอง แบบฝึกหัดที่สร้างขึ้นเพื่อทำการทดสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัตินั้นยากต่อการนำไปใช้ทดสอบจริงๆ

จากการศึกษางานวิจัยที่เกี่ยวข้องข้างต้นสามารถสรุปเพื่อนำไปใช้เป็นแนวทางในการสรุปผลงานวิจัยต่อไป ได้ดังนี้ คือ เนื่องจากข้อมูลเป็นสิ่งที่มีความสำคัญยิ่งต่อองค์กร ดันนั้นองค์กรจำเป็นต้องเตรียมการเพื่อหลีกเลี่ยงปัญหาและผลกระทบจากเหตุการณ์ที่ไม่อาจคาดเดาได้ในอนาคต การประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติเป็นหนทางหนึ่งในการเตรียมความพร้อมแก่องค์กร โดยมีแนวทางดังนี้คือ ผู้บริหารระดับสูงต้องตระหนักถึงความสำคัญของการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ โดยต้องจัดตั้งทีมงานเพื่อทำการศึกษาวิเคราะห์ความเสี่ยงที่จะมีผลต้องการทำงานของระบบสารสนเทศ และประเมินผลกระทบที่อาจจะเกิดแก่องค์กรในกรณีระบบสารสนเทศไม่สามารถให้บริการได้ ซึ่งจะทำให้องค์กรทราบถึงลำดับความสำคัญของโปรแกรมคอมพิวเตอร์ในระบบสารสนเทศของตนเอง เพื่อนำไปใช้ในการเลือกระบบสำรองข้อมูล ข้อกำหนด และกระบวนการในการปฏิบัติในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ อย่างเหมาะสมและมีประสิทธิภาพ ซึ่งต้องมีกระบวนการทดสอบแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติที่ทำการพัฒนาขึ้น เพื่อเป็นการยืนยันว่าแผนที่พัฒนาขึ้นมานั้นสามารถใช้งานได้จริง ซึ่งในการทดสอบจะทำให้องค์กรสามารถกำหนดระดับการให้บริการเพื่อเป็นตัวชี้วัดความสำเร็จของแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติขององค์กร และเพื่อให้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติที่ทำการพัฒนาขึ้นมานั้น พร้อมที่จะนำมาใช้งานได้อย่างมีประสิทธิภาพตลอดเวลาจะต้องมีการทดสอบเพื่อปรับปรุงและแก้ไข ข้อกำหนดและกระบวนการในการปฏิบัติในแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอย่างสม่ำเสมอ

2.7 กรอบแนวคิดในการวิจัย

งานวิจัยนี้ผู้วิจัยได้ทำการศึกษาเอกสารทางวิชาการและงานวิจัยที่เกี่ยวข้องกับแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ ซึ่งทำให้ทราบถึงความสำคัญของแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ ประโยชน์ที่องค์กรจะได้จากการประยุกต์ใช้ ตลอดจนถึงแนวทางในการวางแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ รวมทั้งได้ทำการศึกษาถึงมาตรฐานที่เกี่ยวข้องกับแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติอันได้แก่ มาตราฐานการบริหารการดำเนินธุรกิจอย่างต่อเนื่องภายใต้ภาวะวิกฤติ (BS25999: Business Continuity Management (BCM) Standard) และมาตราฐาน

ISO/IEC 24762:2008 ซึ่งเป็นแนวทางการเตรียมความพร้อมให้กับเทคโนโลยีสารสนเทศเพื่อการสื่อสารภายใต้ภาวะวิกฤต (Guidelines for information and communications technology disaster recovery services)

นอกจากนั้นผู้วิจัยยังได้ทำการศึกษาถึงปัจจัยความสำเร็จในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติจากเอกสารทางวิชาการและงานวิจัยที่เกี่ยวข้องเพื่อนำมาวิเคราะห์ถึงปัจจัยความสำเร็จในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติที่มีความสำคัญและสอดคล้องกับองค์กร ซึ่งใช้กระบวนการทางสถิติในการวิเคราะห์องค์ประกอบจากข้อมูลที่ได้จากความคิดเห็นของคนในองค์กรที่มีต่อปัจจัยความสำเร็จในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติจากเอกสารทางวิชาการและงานวิจัยที่เกี่ยวข้อง ร่วมถึงการใช้การวิเคราะห์การถดถอยพหุคูณในการหาความสัมพันธ์ระหว่างปัจจัยความสำเร็จในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติจากเอกสารทางวิชาการและงานวิจัยที่เกี่ยวข้องกับปัจจัยความสำเร็จในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติที่มีความสำคัญและสอดคล้องกับองค์กรว่ามีความสัมพันธ์กันอย่างไร

โดยองค์กรที่ใช้เป็นกรณีศึกษาในงานวิจัยนี้ คือ บริษัท ตรีเพชรอิซูซุเซลส์ จำกัด ซึ่งเป็นบริษัทที่อยู่ในกลุ่มอุตสาหกรรมรถยนต์เชิงพานิชย์ที่มีขนาดใหญ่แห่งหนึ่งในประเทศไทย และทำการสรุปเป็นแนวทางในการวางแผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติ เพื่อเป็นแนวทางในการประยุกต์ใช้แผนฟื้นฟูระบบสารสนเทศจากภัยพิบัติแก่องค์กรต่อไป จากแนวความคิดนี้สามารถเขียนเป็นกรอบแนวคิดในการวิจัย ดังภาพที่ 2.7

ภาพที่ 2.7

แสดงกรอบแนวคิดในการวิจัย