คู่มือตรวจสอบ
การปฏิบัติการ
(Operations)

คำนำ

คู่มือตรวจสอบการตรวจการปฏิบัติการ เป็นส่วนหนึ่งของการปรับปรุงคู่มือการตรวจสอบระบบเทคโนโลยีสารสนเทศ ฉบับเดือนพฤศจิกายน 2543 ของส่วนตรวจสอบเทคโนโลยีสารสนเทศ ซึ่งเป็นการยกเลิกบทที่ 13 “Operations” และบทที่ 17 “Document Imaging” ของคู่มือ FFIEC Information Systems Examination Handbook ปี 1*996* อนึ่งแนวทางในคู่มือฉบับนี้จะครอบคลุมไปถึงความเสี่ยงและระบบการควบคุมภายในด้าน Operations นอกจากนี้ยังครอบคลุมไปถึงกระบวนการปฏิบัติงานและการพัฒนาบุคคลากรที่ดี อนึ่ง Operations ที่มีประสิทธิภาพเป็นตัวจักรที่สำคัญของความสำเร็จของทุกสายงานธุรกิจหลัก ดังนั้น ผู้บริหาร IT ผู้บริหารสายงานธุรกิจ และผู้ใช้งาน ควรดำเนินการเพื่อร่วมมือกันในการกำหนดระดับการให้บริการที่เหมาะสมร่วมกัน

แนวทางปฏิบัติในคู่มือฉบับนี้ สามารถนำไปปรับใช้เพื่อให้เกิดการควบคุมภายในที่เหมาะสมกับสภาพแวดล้อมทางด้าน IT และความเสี่ยงขององค์กรที่แตกต่างกันไป เช่น การปฏิบัติงานในองค์กรที่มีความสลับซับซ้อนภายในศูนย์คอมพิวเตอร์ การปฏิบัติงานแบบกระจายศูนย์ไปตามสายงานธุรกิจต่างๆ การใช้เครื่องไมโครคอมพิวเตอร์ประมวลผลแบบอิสระไม่เชื่อมโยงกับระบบงานอื่นๆ (stand alone) และระบบงานสนับสนุนอื่นๆ ของทั้งองค์กร รวมทั้งสามารถนำไปประยุกต์ใช้ได้กับองค์กรขนาดเล็กที่มีการปฏิบัติงานไม่ซับซ้อนได้ด้วย

ส่วนตรวจสอบเทคโนโลยีสารสนเทศ หวังว่าแนวทางการตรวจสอบในคู่มือฉบับนี้จะเป็นประโยชน์และช่วยพัฒนาการตรวจสอบให้มีประสิทธิภาพต่อไปในอนาคต

ส่วนตรวจสอบเทคโนโลยีสารสนเทศ

ธันวาคม 2551

สารบัญ

หน้าที่

<u>ส่วนที่ 1</u> บทนำ

การปฏิบัติการ (Operations) เกี่ยวข้องโดยตรงกับกลยุทธ์ในทางการบริหารงานและการจัดการงานประจำวันด้าน IT ซึ่งครอบคลุมถึงเรื่องการรับ การส่ง การประมวลผล การเก็บรักษาข้อมูลสารสนเทศ และการสนับสนุนกระบวนการปฏิบัติงานทางธุรกิจ

บทบาทของ IT ในการสนับสนุนการดำเนินธุรกิจได้พัฒนามากขึ้นและมีความสลับซับซ้อนมากยิ่งขึ้น แต่เดิมการปฏิบัติงานด้าน IT จะจำกัดอยู่ภายในศูนย์คอมพิวเตอร์ แต่ปัจจุบันสภาพแวดล้อมด้าน IT ได้กระจายไปอยู่ในที่ต่างๆทั่วทั้งองค์กร จึงมีความจำเป็นมากยิ่งขึ้นในการเชื่อมโยงระบบ IT ผ่านระบบการสื่อสาร เครือข่ายอินเทอร์เน็ต และการปฏิบัติงานกับคอมพิวเตอร์ในรูปแบบต่างๆกันไป และเนื่องจากความสลับซับซ้อนด้าน IT นี้เองที่ทำให้สถาบันการเงินต่าง ๆ จำเป็นที่จะต้องพึ่งพาอาศัยผู้จัดจำหน่าย หรือหุ้นส่วน และผู้ให้บริการด้าน IT อื่นๆมากขึ้นในการใช้บริการด้าน IT

<u>ส่วนที่ 2</u> แนวทางที่พึงปฏิบัติ

2.1 บทบาทและความรับผิดชอบในการตรวจสอบการปฏิบัติการ

<u>สรุปแนวทางปฏิบัติ</u>

คณะกรรมการสถาบันการเงินและผู้บริหารระดับสูง มีหน้าที่ความรับผิดชอบในการกำกับดูแลให้เกิดความมั่นคงและปลอดภัยในการปฏิบัติงานประจำวันด้าน IT ซึ่งจะช่วยสนับสนุนเป้าหมายหลักขององค์กร ซึ่งครอบคลุมถึงการปฏิบัติงานในศูนย์คอมพิวเตอร์ทั้งแบบรวมศูนย์ (Centralized) และแบบกระจายศูนย์ (Decentralized) การบริหารปฏิบัติงานภายในสายงานธุรกิจ การปฏิบัติงานสนับสนุนและงานที่เกี่ยวข้องอื่นๆ และการจัดการผู้ให้บริการภายนอก (Outsourcing arrangements) ซึ่งครอบคลุมถึงปัจจัยสำคัญต่างๆ ที่ต้องรับผิดชอบ คือ

- โครงสร้างขององค์กรด้านการปฏิบัติงานประจำวันที่เหมาะสมที่จะทำให้บรรลุผลในการช่วยสนับสนุนกิจกรรมทางธุรกิจขององค์กร
- การจัดให้มีเอกสารเกี่ยวข้องกับระบบงานต่างๆ และความเข้าใจเกี่ยวกับความสัมพันธ์ของระบบงานต่างๆ ในการสนับสนุนการดำเนินธุรกิจ
- การสร้างและสนับสนุนให้เกิดสภาพแวดล้อมในการควบคุมที่เหมาะสมผ่านกระบวนการระบุความเสี่ยง การประเมินความเสี่ยง การบริหารและการจัดการ และการเฝ้าติดตามดูแลความเสี่ยง
- การสร้างระบบรักษาความปลอดภัยทั้งด้านกายภาพและทางตรรกะให้เหมาะสมกับสภาพแวดล้อมด้านการปฏิบัติงานประจำวัน
- การจัดให้มีแผนการปฏิบัติงานประจำวันที่สามารถทำงานได้อย่างต่อเนื่อง และมีความสามารถกู้ระบบคืนกลับมาได้เมื่อเกิดปัญหาขึ้น
- การจัดหาบุคลากรที่เพียงพอ และมีกระบวนการสรรหา การสืบทอดตำแหน่ง และการฝึกอบรมที่เพียงพอ
- การจัดหาบริการจากบริษัทที่ปรึกษาหรือผู้ตรวจสอบภายนอกตามความจำเป็น

2.1.1 คณะกรรมการสถาบันการเงินและผู้บริหารระดับสูง

คณะกรรมการสถาบันการเงินและผู้บริหารระดับสูง มีหน้าที่รับผิดชอบในการที่จะทำให้เกิดความปลอดภัย มั่นคง และมีประสิทธิผลในการปฏิบัติงานด้าน IT ทั่วทั้งสถาบันการเงิน เนื่องจากระบบสารสนเทศ ไม่ว่าจะเป็นแบบรวมศูนย์ (Centralized) หรือ แบบกระจายศูนย์ (Distributed) ต่างก็มีการเชื่อมโยงถึงกันและการพึ่งพาอาศัยซึ่งกันและกันเป็นอย่างสูง ดังนั้น หากการดูแลจัดการในส่วนหนึ่งส่วนใดของสภาพแวดล้อมด้าน IT ที่มีไม่เพียงพอ อาจทำให้เกิดความเสี่ยงที่เพิ่มขึ้นต่อองค์ประกอบทั้งหมดของการปฏิบัติงานด้าน IT หรือต่อทั้งองค์กรธุรกิจได้ ด้วยเหตุผลข้างต้น คณะกรรมการและผู้บริหารระดับสูงจึงควรดูแลให้เกิดการควบคุมด้าน IT ในการปฏิบัติงานที่ประสานและสอดคล้องกันตลอดทั้งองค์กรและรวมทั้งการปฏิบัติงานของผู้ให้บริการด้านเทคโนโลยีอื่น ๆ ทั้งหมดด้วย

ถึงแม้ว่าคณะกรรมการสถาบันการเงินและผู้บริหารระดับสูงจะสามารถมอบหมายหน้าที่ในการจัดการและการกำกับดูแล Operations ให้แก่ผู้บริหารด้าน IT ได้ แต่หน้าที่ความรับผิดชอบสำหรับความปลอดภัย ความมั่นคง การควบคุม และประสิทธิผลของการปฏิบัติงานในที่สุดแล้ว ก็ยังอยู่ในความรับผิดชอบของคณะกรรมการสถาบันการเงินและผู้บริหารระดับสูง ดังนั้น **คณะกรรมการสถาบันการเงินและผู้บริหารระดับสูงจะต้องเข้าใจถึงความเสี่ยงที่เกี่ยวข้องกับ Operations ที่มีอยู่ในปัจจุบันและที่วางแผนไว้ว่าจะปฏิบัติในอนาคต ต้องกำหนดระดับความเสี่ยงที่สามารถยอมรับได้ขององค์กร จัดให้มีนโยบายการบริหารความเสี่ยงและการติดตามบริหารความเสี่ยง นอกจากนี้ ต้องวางแผนกลยุทธ์ด้าน IT ซึ่งเป็นสิ่งที่สำคัญต่อประสิทธิผลของธรรมาภิบาลด้าน IT**

2.1.2 ผู้บริหารด้านการปฏิบัติการ

หนึ่งในหน้าที่ความรับผิดชอบหลักของผู้บริหารด้านการปฏิบัติการ (Operations) คือการดูแลให้โครงสร้างด้าน IT ที่ได้วางแผนเอาไว้แล้วในปัจจุบันมีความเพียงพอที่จะช่วยให้องค์กรสามารถบรรลุวัตถุประสงค์เชิงกลยุทธ์ได้ตามเป้าหมาย โดยการจัดให้มีบุคลากรที่เพียงพอ (ทั้งด้านความรู้ ประสบการณ์ และจำนวนพนักงาน) และจัดให้มีกำลังความสามารถของระบบที่เพียงพอสามารถให้บริการได้อย่างต่อเนื่อง อนึ่ง **ผู้บริหาร Operations ควรจะให้คำแนะนำและเลือกใช้ IT ที่จะช่วยให้บรรลุเป้าหมายตามแผนกลยุทธ์พร้อมกับช่วยประหยัดทรัพยากรทั้งในแง่การควบคุมค่าใช้จ่ายในการลงทุนและค่าใช้จ่ายในการปฏิบัติงาน**

ผู้บริหาร Operations ควรจัดทำผังโครงสร้างองค์กรที่แสดงให้เห็นถึงเรื่องการจัดสรรบุคลากรที่เหมาะสมเพียงพอต่อกิจกรรมทางธุรกิจ รวมทั้งการแบ่งแยกระบบศูนย์การปฏิบัติงานหลาย

แห่ง ก็ต้องจัดทำให้ครบถ้วนด้วย การปฏิบัติงานด้าน IT ไม่ว่าจะเป็นแบบรวมศูนย์ (Centralized) หรือแบบกระจายศูนย์ (Distributed) จะต้องสามารถรองรับทั้งการปฏิบัติงานของสายงานธุรกิจและงานสนับสนุน และเอื้ออำนวยให้เกิดความสะดวกแก่ระบบสารสนเทศเพื่อการจัดการ (MIS) เพื่อผู้ใช้งานภายใน การพัฒนาสินค้าและบริการต่าง ๆ รวมทั้งการประมวลผลรายการธุรกรรม

ผู้บริหาร Operations ที่ดีควรมีความรู้ความเข้าใจในโครงสร้างด้าน IT ของทั้งองค์กร ควรมีการจัดทำเอกสารที่แสดงให้เห็นโครงสร้างว่าระบบงานเหล่านี้รองรับกระบวนการทางธุรกิจใดในองค์กรและทะเบียนทรัพย์สินด้าน IT ทั้งหมด ผู้บริหารควรทราบความสัมพันธ์เชื่อมโยงกันของระบบทั้งหลายเหล่านี้และควรทราบว่าระบบเหล่านี้มีความเกี่ยวเนื่องเชื่อมโยงในการรองรับสายงานธุรกิจอย่างไร รวมทั้งเข้าใจการไหลของข้อมูลที่ผ่านไปตามระบบต่าง ๆ โดยต้องจัดให้มีเอกสารที่แสดงถึงโครงสร้างและภาพการเชื่อมต่อกันของระบบงานต่าง ๆ โดยควร**ระบุความเสี่ยง จุดควบคุมที่ติดตั้งไว้ในระบบงาน และวิธีการดูแลรักษาระบบงานที่ควรทำอย่างต่อเนื่อง**

ผู้บริหาร Operations ควรสร้างความมั่นใจว่าสภาพแวดล้อมของการปฏิบัติงานประจำวันมีความปลอดภัยทั้งด้านกายภาพและตรรกะ เพื่อปกป้องข้อมูลที่สำคัญของลูกค้าและข้อมูลที่สำคัญขององค์กร ซึ่งทำให้ฝ่ายจัดการจะต้องจัดให้และควบคุมให้มีระบบการควบคุมการเข้าถึงเครื่องมืออุปกรณ์ โปรแกรมระบบงาน ระบบปฏิบัติงาน และข้อมูลของการทำธุรกรรมและข้อมูลของลูกค้า

ผู้บริหาร Operations ที่ดี ควรดูแลให้เกิดสภาพแวดล้อมในการควบคุมการปฏิบัติงานที่ปลอดภัยทั้งในแง่กายภาพและตรรกภาพต่อทรัพย์สินสำคัญทางธุรกิจโดยเฉพาะ ข้อมูลที่มีความสำคัญต่อการประกอบธุรกิจและข้อมูลสำคัญของลูกค้า ให้เกิดความเหมาะสมและสมดุลกันระหว่างความเสี่ยงและต้นทุนในการควบคุม และจะต้องจัดให้มีแนวทางในการปฏิบัติงาน การมอบหมายหน้าที่ความรับผิดชอบ และกฎเกณฑ์ที่ต้องปฏิบัติตามเพื่อที่จะลดความเสี่ยง นอกจากนี้ผู้บริหารควรมีการประเมินประสิทธิภาพของระบบการควบคุมเป็นระยะ ๆ โดยอาจใช้วิธีการประเมินตนเอง (self-assessments) หรือวิธีอื่นก็ได้ และควรมอบหมายให้ผู้ตรวจสอบหรือผู้สอบทานอิสระทำหน้าที่สอบทานผลการประเมินดังกล่าวร่วมด้วย

นอกจากนี้เพื่อจะให้มั่นใจว่าการปฏิบัติงานด้านธุรกรรมต่าง ๆ จะไม่สะดุดหยุดชะงัก ฝ่ายจัดการจึงควรพัฒนาแผนการดำเนินธุรกิจอย่างต่อเนื่อง (BCP) ขึ้นมาใช้งาน (รายละเอียดดังปรากฏในคู่มือตรวจสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง) และควรดำเนินการจัดให้มีระบบงานด้าน IT ที่ดีควรมีความแข็งแกร่ง ยืดหยุ่น มีประสิทธิภาพเพียงพอที่จะรองรับการสะดุดหยุดชะงักแบบ

ปกติธรรมดาได้ และสามารถฟื้นฟูระบบคืนมาได้อย่างรวดเร็วและต้องไม่ก่อให้เกิดปัญหาที่รุนแรงและค่าใช้จ่ายในกระบวนการฟื้นฟูระบบที่เพิ่มขึ้นอย่างมาก

ผู้บริหาร Operations ที่ดี ยังมีหน้าที่ในการสรรหาพนักงาน วางแผนเรื่องการสืบทอดตำแหน่งงาน รวมทั้ง วางแผนเรื่องการอบรมพัฒนาพนักงานอย่างต่อเนื่องซึ่งเป็นสิ่งสำคัญที่จะทำให้พนักงานมีความคิดสร้างสรรค์ กระตือรือร้น และมีความรู้เพิ่มมากขึ้น นอกจากนี้ผู้บริหารยังต้องรู้ว่าจุดใดเป็นข้อจำกัดของการปฏิบัติงานด้าน IT ที่มีอยู่และควรเตรียมการในการหาความช่วยเหลือจากผู้เชี่ยวชาญภายนอก ซึ่งการจ้างผู้เชี่ยวชาญจากภายนอกนั้นมักจะใช้กับงานที่ไม่ต้องการพนักงานมาปฏิบัติหน้าที่ประจำและควรจะต้องก่อให้เกิดประสิทธิภาพมากกว่าและมีค่าใช้จ่ายที่ถูกกว่าการว่าจ้างและอบรมพนักงานใหม่

2.2 การบริหารความเสี่ยง

เนื่องจาก IT ได้เข้าไปเกี่ยวข้องกับกิจกรรมทุกประเภทภายในองค์กร ในส่วนที่เกี่ยวข้องกับการพัฒนา ส่งมอบ และการจัดการกับสินค้าและบริการไม่สามารถแบ่งแยกออกได้ว่าเป็นการดำเนินงานของฝ่ายใดบ้าง จึงมีความจำเป็นที่จะต้องมีกระบวนการบริหารความเสี่ยงด้าน IT ที่มีประสิทธิภาพ ซึ่งจะต้องสามารถ ระบุ วัด ควบคุม และติดตามความเสี่ยงด้านปฏิบัติการได้ กระบวนการบริหารจัดการความเสี่ยงเริ่มต้นด้วยการระบุความเสี่ยงที่ทั้งองค์กรเผชิญอยู่ในการประกอบธุรกิจตามกลยุทธ์ที่วางไว้ โดยวางข้อตกลงร่วมกันในบทบาทของ IT ที่จะเข้าไปช่วยสนับสนุนการปฏิบัติงานทางธุรกิจ จัดทำขอบเขตของข้อตกลงร่วมกันและกรอบการประเมินความเสี่ยง **การระบุความเสี่ยงควรเริ่มด้วยการสำรวจทรัพย์สินและสภาพแวดล้อมต่าง ๆ ด้าน IT ให้ทั่วทั้งองค์กร** การสำรวจควรประกอบด้วยการระบุระบบปฏิบัติการ ฐานข้อมูล และระบบงานว่าระบบต่าง ๆ ดังกล่าวใช้ปฏิบัติงานใด ข้อมูลสำคัญที่ได้จากระบบดังกล่าว และประเมินความสำคัญของระบบงานต่อการประกอบธุรกิจ ควรมีโครงสร้างทรัพยากรด้าน IT ทั้งหมดขององค์กรที่แสดงถึงความสัมพันธ์ระหว่างระบบงานต่าง ๆ ภายในองค์กร ระบบเครือข่ายสื่อสารที่เชื่อมต่อ และระบบงานภายนอกที่เชื่อมต่อทั้งหมด

2.2.1 การกำหนด /ระบุความเสี่ยง

สรุปแนวทางปฏิบัติ

ผู้บริหารควรมีความเข้าใจอย่างละเอียดถี่ถ้วนเกี่ยวกับสภาพแวดล้อมด้าน Operations ขององค์กร และควรดูแลให้มีเอกสารสนับสนุนการปฏิบัติงานที่เหมาะสมเพียงพอกับขนาดความซับซ้อนของการปฏิบัติงานด้าน IT ที่ดำเนินอยู่ การสำรวจสภาพแวดล้อมและทรัพย์สินจะช่วยให้ผู้บริหารสามารถจัดทำผังการไหลของข้อมูลที่ผ่านไปตามระบบต่าง ๆ การเชื่อมต่อกันของระบบต่าง ๆ การพึ่งพาอาศัยกันของระบบต่าง ๆ กระบวนการทำงานด้าน IT ของธุรกิจต่าง ๆ ทะเบียนทรัพย์สินเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ (hardware) และโปรแกรมระบบงาน (software) การสำรวจสภาพแวดล้อมด้าน IT อย่างต่อเนื่องของผู้บริหาร เป็นพื้นฐานในการระบุ ประเมิน จัดการ และการเฝ้าติดตามความเสี่ยง

ปัจจัยสำคัญในการระบุความเสี่ยง รวมทั้งการพัฒนาและดูแลรักษาอย่างต่อเนื่อง ได้แก่

- ทะเบียนทรัพย์สินด้าน hardware ทั้งหมด
- ทะเบียนทรัพย์สิน software ทั้งหมด (ทั้งระบบปฏิบัติการ ระบบงาน applications ทั้งทางธุรกิจและระบบงานสนับสนุนอื่น ๆ)
- ผังโครงสร้างระบบเครือข่ายสื่อสาร หรือผังที่แสดงรายละเอียดการเชื่อมต่อทั้งภายในและภายนอกองค์กรของระบบเครือข่ายสื่อสารทั้งที่อยู่ในรูปแบบ voice และ data
- แผนภาพการไหลของข้อมูลและแผนภาพกระบวนการทำงานของธุรกิจที่จะแสดงให้เห็นการปฏิบัติงานที่ต้องสัมพันธ์และพึ่งพาอาศัยกัน
- ภาพรวมการปฏิบัติงานด้าน IT ที่รองรับเป้าหมายทางกลยุทธ์ของธุรกิจของทั้งองค์กร

ก. การสำรวจสภาพแวดล้อมด้าน IT

ปัจจุบันได้มีการนำเอา IT ฝังตัวอยู่ตามสายงานธุรกิจ หรือสายงานสนับสนุนต่าง ๆ มากขึ้นเป็นอย่างมาก การสำรวจสภาพแวดล้อมจะช่วยให้ได้รับเอกสารภาพรวมในระดับองค์กรของทรัพย์สินด้าน IT ที่มีอยู่ทั้งหมดว่าตั้งอยู่ที่ใด มีการกำหนดค่าตัวแปร (configurations) ทางด้าน hardware และ software มีการเชื่อมโยงระบบกัน (interface) อย่างไรบ้าง การสำรวจดังกล่าวควรจะต้องจัดทำให้ได้รับข้อมูลที่จะแสดงถึงภาพของกระบวนการทำงานตั้งแต่จุดเริ่มต้นของการรับข้อมูล

เข้ามาในระบบ การไหลผ่านของข้อมูลไปในระบบต่าง ๆ จนกระทั่งถึงการจัดเก็บข้อมูลในฐานข้อมูล การ**สำรวจนี้เป็นส่วนหนึ่งที่ทำให้เกิดการจัดทำทะเบียนทรัพย์สินให้เป็นปัจจุบันและทำให้มีการดูแลทรัพย์สินเหล่านั้น นอกจากนั้นยังช่วยให้ผู้บริหารเข้าใจสภาพแวดล้อมทางด้าน IT ได้อย่างครอบคลุมทั้งองค์รวมซึ่งจะทำให้สามารถจัดสรรทรัพยากรและงบประมาณเพื่อรองรับการดำเนินธุรกิจได้อย่างเหมาะสม** อีกทั้งความเข้าใจนี้ยังช่วยควบคุมต้นทุน บริหารและจัดการ configuration วิเคราะห์ถึงสาเหตุของปัญหา และจัดการในเรื่องลิขสิทธิ์ต่างๆ (license) การสำรวจสภาพแวดล้อมที่ละเอียดจะสามารถใช้เป็นพื้นฐานในการบริหารจัดการและติดตามการปฏิบัติงานประจำวัน และข้อมูลที่ได้จากการสำรวจยังมีความสำคัญต่อการประเมินกระบวนการควบคุมในเรื่องอื่น ๆ เช่น ความปลอดภัยของการใช้สารสนเทศ การวางแผนการดำเนินธุรกิจอย่างต่อเนื่อง และการบริหารจัดการความเสี่ยงในการใช้บริการจากผู้ให้บริการภายนอก ผู้บริหารควรควบคุมดูแลการจัดทำเอกสารสภาพแวดล้อมด้าน IT มีความทันสมัยเป็นปัจจุบัน โดยให้มีกระบวนการสำรวจเป็นระยะ ๆ อยู่เสมอ ซึ่งเอกสารที่ต้องมี ได้แก่ ทะเบียนทรัพย์สิน และผังแสดงโครงสร้างระบบเครือข่ายสื่อสาร(a topology or network map) สำหรับเอกสารอื่นที่ควรมีก็เป็นไปตามความเหมาะสมกับขนาดและความซับซ้อนของ IT ที่องค์กรมีอยู่ กล่าวคือ องค์กรขนาดใหญ่ที่มีการใช้ IT ที่ซับซ้อนควรมีเอกสารทั้งในระดับภาพรวมและระดับที่ลงรายละเอียดถึงกระบวนการหรือระบบงานย่อย ๆ ภายใต้ภาพรวมนั้นด้วย โดยอาจใช้ เครื่องมือในการบริหารเครือข่าย (network management tools) ในการสร้างระบบฐานข้อมูลของโครงสร้างต่าง ๆ เหล่านั้นก็ได้ และองค์กรขนาดใหญ่ที่มีความซับซ้อนทางด้าน IT ควรจัดทำเอกสารที่รวมไปถึงภาพกระบวนการทางธุรกิจและแผนผังการไหลของข้อมูล นอกจากนี้ ควรมีการจัดลำดับความสำคัญของงานที่จะต้องปฏิบัติเพื่อรองรับธุรกิจด้วย

ข. ทะเบียนทรัพย์สินด้านเทคโนโลยี

ทะเบียนทรัพย์สินคอมพิวเตอร์

กระบวนการจัดทำทะเบียนทรัพย์สินด้านคอมพิวเตอร์ควรดำเนินการให้ครอบคลุมไปถึงทั้งทรัพย์สินที่องค์กรเป็นเจ้าของและไม่ได้เป็นเจ้าของ ซึ่งตั้งอยู่ในบริเวณสภาพแวดล้อมขององค์กร (รวมถึงอุปกรณ์ที่ใช้ประมวลผลในลักษณะที่ทำงานด้วยตนเองโดยไม่เชื่อมโยงไปถึงระบบงานอื่น (Stand-alone) ตามหน่วยงานต่าง ๆ ในองค์กรด้วย) ทั้งนี้ อุปกรณ์แต่ละชิ้นควรมีรหัสเฉพาะของตัวเองที่ไม่ซ้ำกันและควรติดเป็นบาร์โค้ดหรือแถบป้ายรหัสไว้ที่อุปกรณ์ตัวนั้น ๆ ตัวอย่างข้อมูลที่ควรจัดเก็บสำหรับทำทะเบียนทรัพย์สิน ได้แก่

1. เครื่องคอมพิวเตอร์ชุดใหญ่ ขนาดกลาง หรือ เครื่องคอมพิวเตอร์ server

- ชื่อผู้ขาย (Vendor) และ ชื่อรุ่น (model)
- ประสิทธิภาพของระบบประมวลผล (MIPS)
- หน่วยความจำหลัก (Core or main memory)
- อุปกรณ์จัดเก็บข้อมูล (Storage) เช่น เทป และเครื่องมืออัตโนมัติในการจัดเก็บเทป (tape silos) เป็นต้น
- บทบาทการปฏิบัติหน้าที่ (Function)
- สถานที่ตั้ง (Location)

2. คอมพิวเตอร์ตั้งโต๊ะ หรืออุปกรณ์ประมวลผลเฉพาะตัวที่ไม่เชื่อมโยงกับระบบงานอื่น

- ชื่อผู้ขาย (Vendor) และ ชื่อรุ่น (model)
- ชื่อเจ้าของเครื่องและวัตถุประสงค์ที่ใช้งาน
- การเชื่อมต่อกับระบบเครือข่ายขององค์กร
- ความสามารถในการเชื่อมต่อออกไปภายนอกองค์กร (Dial-out capability)
- สถานที่ตั้ง (Location)

3. อุปกรณ์เครือข่ายการสื่อสาร Network devices

- ชื่อผู้ขาย (Vendor) และ ชื่อรุ่น (model)
- ประเภท/ชนิด
- หน่วยความจำภายในตัวอุปกรณ์ (random access memory)
- หมายเลขแสดงตำแหน่งบนเครือข่าย Internet protocol (IP) address

4. เครื่องมือประมวลผลอื่นๆ Item processing equipment

- ชื่อผู้ขาย (Vendor) และ ชื่อรุ่น (model)
- ประเภท

การจัดทำทะเบียนคุมอุปกรณ์การสื่อสาร (telecommunication equipment) ก็ควรดำเนินการให้มีการบันทึกการใช้และการติดต่อสื่อสารไว้เป็นหลักฐาน การดำเนินการดังกล่าวมีความสำคัญมากเมื่อองค์กรมีการเลือกใช้ตู้สลับสายโทรศัพท์ private branch exchanges (PBX) หรือ

เทคโนโลยีในการสื่อสารด้วยโทรศัพท์ด้วยเครือข่ายอินเตอร์เน็ต voice over Internet protocol (VOIP) ในการเชื่อมโยงทั้งเสียงและข้อมูลอย่างต่อเนื่อง และควรจัดเก็บข้อมูลเพิ่มเติมดังต่อไปนี้

- หมายเลขและการกำหนดค่าตัวแปร (Number and configuration of trunks)
- หมายเลขของวงจร (Circuit numbers)
- ตำแหน่งที่ตั้งของจุดเชื่อมต่อเข้าอาคารสถานที่ (Entry points to the premises)
- การเชื่อมต่อเข้าสู่สำนักงานใหญ่ (Central office connectivity)
- ประเภท/ชนิดของบริการที่มีอยู่ (Types of service supplied) เช่น
  - โทรศัพท์พื้นฐานทั่วไป (POTS – plain old telephone service)
  - การสื่อสารผ่านสายสื่อสารใยแก้ว (SONET – synchronous optical network)
  - การสื่อสารผ่านสายสื่อสารทั้งเสียงและข้อมูลพร้อมๆกัน (ISDN – integrated services digital network)
  - การสื่อสารผ่านเครือข่ายที่ส่งข้อมูลแบบเป็นกลุ่มของข้อมูล (Frame relay)
  - การสื่อสารผ่านเครือข่ายไร้สาย (Wireless)

ค. ทะเบียนโปรแกรมระบบงาน

องค์กรควรจัดทำทะเบียนคุมโปรแกรมระบบงานต่างๆ ซึ่งสามารถจัดแยกออกมาได้อย่างน้อย 3 ประเภท คือ โปรแกรมระบบปฏิบัติการ (operating systems) โปรแกรมระบบงานประยุกต์ (application software) โปรแกรมสำหรับงานสนับสนุนอื่นๆ (back-office and environment applications) ทั้งนี้ application software หมายถึงโปรแกรมประมวลผลระบบงานหลัก และโปรแกรมระบบงานที่ใช้กับเครื่องคอมพิวเตอร์ตั้งโต๊ะและคอมพิวเตอร์ที่ใช้เชื่อมต่อเพื่อทำงานกับระบบงานหลักที่ใช้ประมวลผลงานหลัก ส่วน back-office and environment applications หมายถึงโปรแกรมระบบงานที่ติดตั้งทำงานอยู่บน operating system และทำหน้าที่สนับสนุนการทำงานของ application software ซึ่งมีตัวอย่างเช่น โปรแกรมจัดการระบบฐานข้อมูล (database engines) โปรแกรมเพื่อบริหารการจัดเก็บข้อมูลและการสำรองข้อมูล (back-up and storage management software) โปรแกรมระบบงานอินเตอร์เน็ตและโปรแกรมระบบงานสนับสนุนอื่นๆ (Internet servers and application

support software) โปรแกรมระบบการโอนย้ายแฟ้มข้อมูล (file transmission systems) โปรแกรมเฝ้าติดตามดูแลผลการปฏิบัติงาน (system performance monitoring applications) เป็นต้น

ตัวอย่างของข้อมูลที่ควรจัดเก็บลงทะเบียนคุมโปรแกรมระบบงานต่างๆ ได้แก่

- ประเภท หรือชื่อของระบบงาน (Type or application name) เช่น ระบบบัญชี ระบบเงินเดือน
- ผู้ผลิต หรือ ผู้จำหน่าย
- หมายเลข Serial number
- หมายเลข Version level
- หมายเลขการปรับปรุงแก้ไข Patch level
- จำนวนชุดของโปรแกรม Number of copies installed
- จำนวนของสิทธิ์ที่ได้รับอนุญาตให้ใช้งาน (Number of licenses owned)
- ประเภทของสิทธิ์ในการใช้งานซื้อมา (Types of licenses owned) เช่น รายบุคคลหรือ ทั้งองค์กร

ง. ส่วนประกอบและรูปแบบของการจัดการเครือข่ายการสื่อสาร

โครงสร้างพื้นฐานของระบบการสื่อสารขององค์มีความสำคัญมากต่อการดำเนินงานทุก ๆ ด้านทางธุรกิจ เพราะว่าเครือข่ายสื่อสารทั้งด้านเสียงและข้อมูล ถือเป็นแกนกลางหลักสำหรับการแลกเปลี่ยนข้อมูล การส่งผ่านข้อมูล และการเชื่อมต่อระบบเทคโนโลยีเข้าด้วยกัน เพราะฉะนั้นองค์กร**ควรจัดทำทะเบียนจัดเก็บค่าตัวแปรของระบบเครือข่ายเพิ่มเติมนอกเหนือจากการจัดทำทะเบียนทรัพย์สินทั้ง hardware และ software ที่เชื่อมต่อและทำงานอยู่บนระบบปฏิบัติการเครือข่ายการสื่อสาร** ทั้งนี้ผู้บริหารควรจัดทำผังแสดงโครงสร้างการสื่อสารขององค์กรตามระดับของความสลับซับซ้อนของเครือข่ายการสื่อสารขององค์กรครอบคลุมไปถึงภาพ**ของเครือข่ายการสื่อสารระดับทั่วโลก WANs (Wide Area Networks) เครือข่ายการสื่อสารระดับหัวเมืองใหญ่ MANs (Metropolitan Area Networks) และเครือข่ายการสื่อสารระยะใกล้ LANs (Local Area Networks)** โดยมีการจัดเก็บข้อมูลอย่างเพียงพอดังต่อไปนี้คือ

- การบำรุงรักษาและการแก้ไขปัญหาของเครือข่าย
- การฟื้นคืนระบบเมื่อเกิดเหตุขัดข้อง
- แผนสำหรับการขยาย, ปรับเปลี่ยนค่า configuration, หรือเพิ่มเติมเทคโนโลยีใหม่

- การระบุการเชื่อมต่อกับเครือข่ายทั้งหมดทั้งภายในและภายนอก รวมทั้งการเชื่อมต่อที่ผ่านอินเตอร์เน็ตและโมเด็มด้วย

- อธิบายประเภทของเครือข่าย เช่น DSL, dialup, cable modem, wireless

- ระบุความสามารถในการส่งผ่านข้อมูล (bandwidth) ของเครือข่ายที่เชื่อมต่อทั้งภายในเครือข่ายเดียวกันและระหว่างเครือข่าย

- ระบุและอธิบายวิธีการเข้ารหัสลับของข้อมูล (encrypted) หรือวิธีสื่อสารที่มีความปลอดภัยแบบอื่นๆ

- ระบุประเภทและกำลังความสามารถของอุปกรณ์เครือข่ายที่ใช้เชื่อมต่อ เช่น switches, routers, hubs, gateways, เป็นต้น

- ระบุประเภทของระบบรักษาความปลอดภัย เช่น firewalls, intrusion detection systems, และอุปกรณ์ดักจับแฮคเกอร์ เช่น honey pots

- ระบุผู้ให้บริการหลักของเครือข่ายสื่อสารโทรคมนาคม

- ระบุว่าสารสนเทศอะไรที่พร้อมใช้งานและเก็บอยู่ที่ใด

ผังโครงสร้างเครือข่ายสื่อสาร (network topology) จะเป็นเสมือนพิมพ์เขียวทางเทคโนโลยีของโครงสร้างระบบเครือข่ายสื่อสาร ผู้บริหารควรจัดทำเอกสารสำคัญอื่น ๆ ที่เกี่ยวกับเครือข่ายสื่อสาร เช่น เอกสารที่ระบุเกี่ยวกับประเภทของอุปกรณ์เครือข่ายสื่อสาร, ที่ตั้ง, ปริมาณข้อมูลสารสนเทศที่เก็บอยู่และส่งผ่านอยู่บนเครือข่ายสื่อสารนั้น และเอกสารที่ระบุเกี่ยวกับเครื่องมือที่ใช้ในการบริหารเครือข่ายสื่อสารทั้งหมด รวมทั้งระบุเกี่ยวกับกำลังความสามารถของอุปกรณ์ network administration console ด้วย

นอกจากนี้ผู้บริหารควรจัดทำผังการไหลของข้อมูล (data flow diagrams) ทั้งภายในเครือข่ายสื่อสารเดียวกันและที่ไหลผ่านระหว่างเครือข่ายสื่อสารหลาย ๆ เครือข่าย รวมถึงการไหลของข้อมูลไปยังเครือข่ายสื่อสารนอกองค์กรด้วย ทั้งนี้เพื่อให้เกิดความเข้าใจภาพการไหลของข้อมูลในระบบต่าง ๆ ซึ่งผังการไหลของข้อมูล ควรจะแสดงข้อมูลเหล่านี้ไว้ด้วย ได้แก่

- Data sets และ subsets ที่ใช้ร่วมกันระหว่างระบบต่าง ๆ

- ข้อมูลที่ใช้ร่วมกันของระบบงานต่าง ๆ (Applications sharing data)

- ประเภทของข้อมูล (เพื่อเผยแพร่ต่อสาธารณะ, ส่วนบุคคล, ความลับ, อื่น ๆ)

- ข้อมูลที่เป็นประโยชน์อื่น ๆ เช่น ปริมาณและประเภทของข้อมูลที่เก็บอยู่

บนสื่อต่าง ๆ ซึ่งควรแยกให้เห็นความแตกต่างระหว่างข้อมูลที่อยู่ในรูปแบบสื่ออิเล็กทรอนิกส์และข้อมูลที่เก็บอยู่ในสื่ออื่น ๆ เช่น hard copy หรือ optical images

จ. ทะเบียนสื่อชนิดต่าง ๆ

ทะเบียนทรัพย์สินด้านอุปกรณ์จัดเก็บข้อมูลควรจะเป็นส่วนที่ช่วยเสริมทะเบียนทรัพย์สินอื่น ๆ ที่ได้กล่าวมาแล้ว โดยไม่จัดทำให้เกิดความซ้ำซ้อนซึ่งรายละเอียดที่ควรระบุไว้ในทะเบียน ได้แก่ ประเภทของอุปกรณ์ ความจุของสื่อ สถานที่จัดเก็บสื่อ ประเภทของข้อมูลที่จัดเก็บอยู่ในอุปกรณ์นั้น (ข้อมูลเพื่อเผยแพร่ต่อสาธารณะ, ข้อมูลส่วนบุคคล, ข้อมูลความลับ, ข้อมูลอื่น ๆ) รวมทั้ง การจัดการควรครอบคลุมถึงโปรแกรมต้นฉบับ ผู้ที่เป็นเจ้าของข้อมูล ความถี่ในการสำรองข้อมูล วิธีการในการจัดเก็บข้อมูล (เช่น เทป, แผ่นซีดี, remote disk เป็นต้น) และที่ตั้งของระบบจัดเก็บข้อมูลสำรองถ้ามีระบบจัดเก็บข้อมูลสำรองที่อยู่ภายนอกศูนย์จัดเก็บหลักด้วย

2.2.2 การประเมินความเสี่ยง

สรุปแนวทางปฏิบัติ

ผู้บริหารควร**นำผลการสำรวจสภาพแวดล้อมด้านการปฏิบัติงาน IT และทะเบียนทรัพย์สินด้านเทคโนโลยีที่มีอยู่มาวิเคราะห์เพื่อหาสิ่งที่เป็นจุดบกพร่องและสิ่งที่เป็นภัยคุกคามต่อการปฏิบัติงานด้าน IT** กระบวนการในการประเมินความเสี่ยงนี้ควรจะทำให้ระบุได้ว่า

- ความเสี่ยงนั้นเป็นความเสี่ยงที่มาจากภายในหรือจากภายนอกองค์กร
- ความเสี่ยงนั้นเกี่ยวข้องกับบุคคล ระบบ หรือกระบวนการ
- คุณภาพและปริมาณของการควบคุม

นอกจากนั้นการประเมินความเสี่ยงควรสามารถประเมินได้ถึงปริมาณของโอกาสความน่าจะเป็นที่จะเกิดขึ้นของจุดบกพร่องและภัยคุกคามนั้น ๆ และควรสามารถประเมินผลกระทบที่ต่อเนื่องไปถึงมูลค่าความเสียหายเมื่อเกิดเหตุการณ์ดังกล่าวด้วย

การปฏิบัติงานด้าน IT ประกอบด้วยขอบเขตของการให้บริการที่ให้ทั้งแก่ผู้ใช้งานภายในองค์กรและลูกค้าภายนอกซึ่ง สง. ต้องมีการบริหารจัดการความเสี่ยงเป็นอย่างมาก ด้วยเหตุนี้จึงไม่ควรจำกัดขอบเขตการประเมินความเสี่ยงไว้กับตัวแปรต่าง ๆ เหล่านี้เท่านั้น ได้แก่ platforms ที่ใช้ระบบปฏิบัติการ(OS) ระบบงานและโปรแกรมยูทิลิตี้ต่าง ๆ เครือข่ายสื่อสารที่เชื่อมโยงอยู่ ขั้นตอนที่

ต้องมีคนเข้ามาเกี่ยวข้อง และสภาพแวดล้อมการควบคุม แต่ควรจะพิจารณาความเสี่ยงที่จะเกิดขึ้นเนื่องจากความเกี่ยวโยงกันระหว่างตัวแปรเหล่านั้นด้วย เนื่องจากจุดบกพร่องและภัยคุกคามมักจะมีศักยภาพที่จะลุกลามไปสู่ระบบและกระบวนการที่เกี่ยวข้องเชื่อมโยงกันได้อย่างรวดเร็ว

ผลของการสำรวจสภาพแวดล้อมและทะเบียนทรัพย์สินด้านเทคโนโลยี จะเป็นข้อมูลพื้นฐานที่จะช่วยในขั้นตอนการระบุและประเมินความเสี่ยง โดยผู้บริหารสามารถใช้วิธีการได้หลากหลายในการระบุและประเมินความเสี่ยง เช่น ใช้วิธีการประเมินตนเอง ข้อสังเกตจากรายงานการตรวจสอบของผู้ตรวจสอบภายในและภายนอก การสอบทานผลการวิเคราะห์ business impact analyses ที่จัดทำขึ้นสำหรับแผนฉุกเฉิน การสอบทานข้อตรวจพบในรายงานการประเมินจุดบกพร่องที่จัดทำขึ้นเพื่อวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศ และข้อสังเกตของบริษัทประกันภัยในการกำหนดเบี้ยประกัน การระบุและประเมินความเสี่ยงควรจะเน้นที่เหตุการณ์ที่สามารถทำให้เกิดการหยุดชะงักของการปฏิบัติงาน เหตุการณ์ที่กระทบต่อรายได้หรือชื่อเสียงของกิจการ รวมทั้งประเภทของเหตุการณ์อื่น ๆ ทั่วไป เช่น

- การลงทุนด้านเทคโนโลยีที่ผิดพลาด เช่น การ implement ด้านเทคโนโลยีที่ไม่เหมาะสม ความล้มเหลวของผู้ให้บริการ การกำหนดความต้องการทางธุรกิจที่ไม่ดีพอ การไม่สามารถใช้งานระบบงานใหม่ร่วมกับระบบงานที่มีอยู่แล้วได้ หรือการล้าสมัยของซอฟแวร์รวมทั้งการที่ผู้ให้บริการไม่ให้บริการสนับสนุนแล้ว

- ปัญหาที่เกี่ยวข้องกับการพัฒนาระบบหรือการนำมาใช้งาน เช่น การบริหารโครงการที่ไม่ดีพอ การใช้งบประมาณค่าใช้จ่ายหรือเวลาในการพัฒนาเกินที่กำหนดไว้ ความผิดพลาดของการเขียนโปรแกรม ความล้มเหลวของการเชื่อมต่อกับระบบงานเดิมหรือการย้ายจากระบบงานเดิม ความล้มเหลวของระบบที่ไม่เป็นไปตามความต้องการทางธุรกิจ

- ประสิทธิภาพของระบบ เช่น ขาดการวางแผนด้านประสิทธิภาพ ประสิทธิภาพของระบบในเรื่องของความยืดหยุ่นไม่เพียงพอ ซอฟแวร์มีประสิทธิภาพไม่เพียงพอต่อความเติบโตของธุรกิจ

- ความขัดข้องของระบบ เช่น ความเสี่ยงของระบบที่เชื่อมโยงกัน ความขัดข้อง/ล้มเหลวของระบบเครือข่ายสื่อสาร เครือข่ายโทรคมนาคม ฮาร์ดแวร์ หรือซอฟแวร์ เป็นต้น

- การบุกรุกระบบรักษาความปลอดภัย เช่น การบุกรุกด้านความปลอดภัยทั้งจากภายในหรือภายนอก ไวรัสคอมพิวเตอร์ การทุจริตโดยเขียนโปรแกรมฝังไว้ ตัวแปรที่ใช้ประเมินความเสี่ยงแบบรายตัว สามารถพิจารณาได้หลากหลายแง่มุม ได้แก่

- ความสำคัญและความจำเป็นของธุรกิจนั้น
- ขนาดของระบบ หรือกระบวนการที่จะปรับเปลี่ยน
- ช่องทางการเข้าถึงระบบ เช่น จากภายในหรือภายนอกองค์กร ผ่านอินเตอร์เน็ต dial-up หรือ WAN
- ลักษณะการพัฒนาระบบงาน เช่น ซื้อโปรแกรมสำเร็จรูป พัฒนาเอง หรือแบบผสมทั้งสองอย่าง
- ขอบเขตและความสำคัญของระบบ หรือจำนวนหน่วยธุรกิจที่เกี่ยวข้องกับระบบดังกล่าวที่จะได้รับผลกระทบทำให้ไม่สามารถทำงานได้
- ประเภทของการประมวลผล เช่น batch, real-time, client/server, parallel distributed
- ปริมาณและมูลค่าของรายการ
- การแบ่งประเภทหรือแบ่งชั้นความลับของข้อมูล
- การแบ่งประเภทของสิ่งที่ส่งผลกระทบต่อข้อมูล เช่น read, update, download, upload
- ประสบการณ์และความสามารถของผู้บริหารระดับปฏิบัติงาน
- จำนวนพนักงาน และเสถียรภาพของอัตรากำลัง
- จำนวนของผู้ใช้ระบบหรือลูกค้า
- การเปลี่ยนแปลงของสภาพแวดล้อมด้านกฎหมาย ข้อบังคับ ระเบียบของทางการ
- ความเสี่ยงใหม่ ๆ ที่เกิดขึ้นจากการเปลี่ยนแปลงพัฒนาการทางเทคโนโลยีหรือความล้าสมัยของเทคโนโลยี
- จุดอ่อนของการตรวจสอบหรือการประเมินตนเอง

การนำตัวแปรหลาย ๆ ตัวมาใช้ประเมินความเสี่ยงร่วมกันควรจะคำนึงถึงความเหมาะสมต่อขนาด ปริมาณ ความซับซ้อน และสภาพการณ์โดยปกติของสถาบันการเงินและสภาพการณ์โดยปกติของกิจกรรมนั้น ๆ

เมื่อสถาบันการเงินสามารถระบุและวิเคราะห์ความเสี่ยงทั้งหมดที่เกี่ยวข้องกับองค์กรได้แล้ว **ควรจะจัดลำดับผลของความเสี่ยงที่ประเมินได้นั้นตามความสำคัญของระบบนั้น ๆ ต่อธุรกิจโดยใช้น้ำหนักของโอกาสที่จะเกิดขึ้นของเหตุการณ์นั้น ๆ และน้ำหนักของผลกระทบจากเหตุการณ์นั้น**

ต่อองค์กร เช่น ในด้านการเงิน ชื่อเสียง หรือผลกระทบทางกฎหมาย **เพื่อเป็นพื้นฐานในการสร้างระบบการควบคุมการปฏิบัติงานที่มีความมั่นคง ปลอดภัย และมีประสิทธิภาพ รวมทั้งอยู่ในระดับความเสี่ยงที่กิจการยอมรับได้**

2.2.3 การลด/บรรเทาความเสี่ยง

สรุปแนวทางปฏิบัติ

ผู้บริหารควรสร้างสภาพแวดล้อมการควบคุมที่สอดคล้องเหมาะสมกับผลการประเมินความเสี่ยง **การควบคุมการปฏิบัติงานด้าน IT ที่เข้มแข็งจะเกิดจากการวางพื้นฐานในเรื่องของนโยบาย มาตรฐาน และแนวทางปฏิบัติในเรื่องต่าง ๆ ดังนี้**

- การควบคุมสภาพแวดล้อม
- การดูแลบำรุงรักษาระบบด้วยมาตรการป้องกัน
- การรักษาความปลอดภัยทางกายภาพ
- การรักษาความปลอดภัยทางตรรกภาพ
- การควบคุมด้านบุคคลากร
- การบริหารการเปลี่ยนแปลงแก้ไขระบบ
- การควบคุมสารสนเทศ
- การให้บริการสนับสนุน/ช่วยเหลือ/แก้ไขปัญหาของผู้ใช้งาน
- การควบคุมการจัดตารางการปฏิบัติงาน รายงานและเอกสารสำคัญ
- การบริหารจัดการต่อเหตุการณ์ต่าง ๆ

การลดความเสี่ยงเกี่ยวข้องกับการสร้างสภาพแวดล้อมในการควบคุมที่ดีให้เกิดขึ้น ซึ่งจะช่วยลดภัยคุกคามทั้งจากภายในและภายนอกองค์กรให้อยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ และยังช่วยให้การปฏิบัติงานด้าน IT มีการจัดการที่เป็นระบบมากขึ้นด้วย ตัวอย่างของการควบคุม เช่น นโยบายและแนวทางปฏิบัติที่เกี่ยวข้องกับบุคลากรและการปฏิบัติงาน การแบ่งแยกหน้าที่งาน และการควบคุมโดยสองฝ่าย (dual controls) การควบคุมการนำเข้าข้อมูล โปรแกรมตรวจสอบควบคุมคุณภาพ เป็นต้น และ**ในจุดที่ไม่สามารถสร้างการควบคุมได้ก็อาจจะใช้การประกันภัยเป็นเครื่องมือในการปรับ**

ลดความเสี่ยงได้ ผู้บริหารควรจัดการให้เกิดความสมดุลกันระหว่างการสร้างการควบคุมและต้นทุนค่าใช้จ่ายรวมถึงประสิทธิภาพและประสิทธิผลด้วย

ก. นโยบาย มาตรฐานและแนวทางการปฏิบัติงาน

(1) <u>นโยบาย</u>

นโยบายที่ผ่านการอนุมัติจากคณะกรรมการจะเป็นแนวทางในภาพกว้างที่จะแสดงให้เห็นการบริหารจัดการและระดับความเสี่ยงที่กิจการนั้นยอมรับได้ ซึ่งในนโยบายควรแสดงให้เห็นแง่มุมที่สำคัญต่อกิจการ เช่น บุคลากร เงินกองทุน การรักษาความปลอดภัยทางกายภาพและตรรกภาพ การบริหารการเปลี่ยนแปลงแก้ไขระบบ การวางแผนกลยุทธ์ และแผนรองรับธุรกิจอย่างต่อเนื่อง ระดับของความลึกและความครอบคลุมของนโยบายการปฏิบัติงานด้าน IT จะขึ้นอยู่กับขนาดและความซับซ้อนของกิจการ องค์กรขนาดเล็กที่มีธุรกิจไม่ซับซ้อนอาจจะมีนโยบายด้าน IT แฝงไว้ในนโยบายด้านอื่น ๆ หรือเขียนนโยบายในลักษณะภาพรวม ขณะที่องค์กรขนาดใหญ่ที่มีความซับซ้อนทางธุรกิจอาจจะแบ่งแยกนโยบายออกตามสายธุรกิจหรือตามฝ่ายงานที่ปฏิบัติงานเลยก็ได้ **คณะกรรมการและผู้บริหารควรออกและบังคับใช้นโยบายและแนวทางปฏิบัติให้มีความเพียงพอต่อความเสี่ยงที่มีอยู่และการปรับลดความเสี่ยงขององค์กร**

(2) <u>มาตรฐาน</u>

มาตรฐานด้านเทคโนโลยีภายในองค์กรจะช่วยสร้างการควบคุมที่สามารถวัดได้และช่วยให้องค์กรบรรลุวัตถุประสงค์ที่ตั้งไว้ เนื่องจากมาตรฐานด้านเทคโนโลยีช่วยในการกำหนดจำกัดขอบเขตและช่วยให้มีความชัดเจนมากขึ้นต่อทรัพยากรที่ให้การสนับสนุนด้าน IT มาตรฐานของฮาร์ดแวร์ ซอฟแวร์ และระบบปฏิบัติการต่าง ๆ นั้นมีประโยชน์ต่อการสร้างและดูแลรักษาโครงสร้างพื้นฐานในระดับองค์กรและยังช่วยส่งเสริมการบรรลุผลสำเร็จในการปฏิบัติงานด้าน IT ลดต้นทุนค่าใช้จ่ายด้าน IT (โดยเฉพาะอย่างยิ่งในเรื่องของการจัดหา พัฒนา อบรม และบำรุงรักษา) **เพิ่มระดับความน่าเชื่อถือและระดับการประเมินสถานการณ์ล่วงหน้าได้ เป็นต้น**

ระดับของการสร้างมาตรฐานของฮาร์ดแวร์และซอฟแวร์นั้น เป็นไปตามการพิจารณาหรือการตัดสินใจทางธุรกิจ ซึ่งผู้บริหารควรจะนำมาตรฐานด้านเทคโนโลยีมาใช้กับทั้งฮาร์ดแวร์ ซอฟแวร์ ระบบปฏิบัติการ และระบบงานต่าง ๆ ทุก platform ตั้งแต่ระดับ host คอมพิวเตอร์(เมนเฟรม)จนถึงระดับผู้ใช้งาน (เครื่อง desktop) รวมทั้งการปรับปรุงมาตรฐานขั้นต่ำด้านโครงสร้างเทคโนโลยีสารสนเทศ ให้ระบบต่าง ๆ สามารถใช้งานร่วมกันได้ (interoperability) เพื่อให้มีความเหมาะสมกับขนาดขององค์กร ไม่เป็นภาระในการบำรุงรักษา และเพื่อให้ระบบสารสนเทศมีความ

ปลอดภัย นอกจากนี้ มาตรฐานด้านเทคโนโลยียังต้องสามารถบังคับใช้ได้ผ่านกระบวนการบริหารการเปลี่ยนแปลงแก้ไขระบบและการตรวจสอบภายในได้ด้วย

(3) <u>แนวทางการปฏิบัติงาน</u>

แนวทางการปฏิบัติงานเป็นสิ่งที่อธิบายกระบวนการในการปฏิบัติงานเพื่อที่จะให้บรรลุวัตถุประสงค์ตามนโยบายและมาตรฐานที่กำหนดไว้ ผู้บริหารควรจัดให้มีแนวทางการปฏิบัติสำหรับการปฏิบัติงานในระบบงานที่สำคัญ ๆ ขององค์กร ซึ่งแนวทางการปฏิบัตินี้จะต้องก่อให้เกิดการระบุอำนาจ หน้าที่ ความรับผิดชอบ ที่สามารถติดตามสืบค้นร่องรอยในการปฏิบัติงานของผู้ปฏิบัติได้ด้วย นอกจากนี้แนวทางการปฏิบัติยังช่วยในการนำแนวนโยบายการบริหารความเสี่ยงมาทำให้เกิดการควบคุมในระดับที่ลงไปในรายละเอียด ซึ่งผู้บริหารควรจะทำการสอบทานและปรับปรุงแนวทางการปฏิบัติงานให้สอดคล้องกับการปฏิบัติงานในปัจจุบันอยู่เสมอ โดยเฉพาะอย่างยิ่งเมื่อมีการเปลี่ยนแปลงการประมวลผล เปลี่ยนแปลงฮาร์ดแวร์/ซอฟแวร์ หรือการเปลี่ยนแปลงค่าคอนฟิกกูเรชั่น ของระบบต่าง ๆ

ขอบเขตของแนวทางการปฏิบัติที่ควรจัดทำนั้นขึ้นอยู่กับขนาดและความซับซ้อนของการปฏิบัติงานด้าน IT ขององค์กรและแตกต่างกันไปตามหน้าที่การปฏิบัติงานที่ปฏิบัติโดยหน่วยงาน IT Operations ซึ่งหน้าที่การปฏิบัติงานที่ควรเขียนอยู่ในแนวทางการปฏิบัติงานด้าน IT เช่น

- คู่มือปฏิบัติงานกับระบบเมนเฟรม และ midrange system
- การบริหารจัดการเครือข่ายสื่อสาร
- การบริหารจัดการโทรคมนาคม
- การบริหารจัดการอุปกรณ์เก็บข้อมูล
- การบริหารจัดการ library ของข้อมูล
- การบำรุงรักษาอุปกรณ์
- การบริหารจัดการปัญหา และการรับมือกับเหตุการณ์ฉุกเฉิน
- แผนการดำเนินธุรกิจอย่างต่อเนื่อง และแผนฉุกเฉิน
- การรักษาความปลอดภัยทั้งทางกายภาพและตรรกภาพ
- การบริหารและควบคุมการเปลี่ยนแปลงแก้ไขระบบงาน
- ข้อมูลและระบบงานสำรอง และอุปกรณ์เก็บข้อมูลที่อยู่ภายนอกศูนย์ประมวลผลหลัก
- การทำสำเนาภาพเอกสาร (Imaging)

- การประมวลผลรายการ
- การกระทบยอดและการสอบทานยอดคงเหลือ
- การควบคุมผลลัพธ์ เช่น รายงาน
- การจัดตารางการปฏิบัติงาน
- เอกสารสัญญาต่าง ๆ (Negotiable instruments)

ข. การนำระบบการควบคุมมาใช้งาน (CONTROLS IMPLEMENTATION)

(1) การควบคุมสภาพแวดล้อม (Environmental Controls)

การปฏิบัติงานด้าน IT เป็นสิ่งสำคัญจำเป็นอย่างยิ่งที่สถาบันการเงินส่วนใหญ่ต้องพึ่งพาในการดำเนินธุรกิจในแต่ละวัน ซึ่งหากเกิดการหยุดชะงักของการปฏิบัติงานด้าน IT ดังกล่าวแล้วอาจนำไปสู่ความเสี่ยงที่สำคัญทางด้านการปฏิบัติงานหรือเกิดความเสี่ยงต่อธุรกรรมหรือชื่อเสียงของกิจการได้ ผู้บริหารควรควบคุมและติดตามสภาพแวดล้อมการปฏิบัติงานทั้งที่อยู่ตามหน่วยงานธุรกิจต่าง ๆ และที่ศูนย์คอมพิวเตอร์อย่างต่อเนื่อง โดยต้องประเมินสภาพแวดล้อมการปฏิบัติงานด้าน IT อย่างรอบคอบรวมถึงดูแลให้มีการควบคุมที่เข้มแข็งด้วย

ผู้บริหารต้องพิจารณาอย่างรอบคอบในการหาแหล่งพลังงานสำรองสำหรับศูนย์ประมวลผลและศูนย์การปฏิบัติงานด้าน IT โดยต้องพิจารณาความคุ้มค่าในเรื่องต้นทุนด้วย เช่น ควรมีระบบไฟฟ้าสำรอง (UPS) หรือเครื่องผลิตกระแสไฟฟ้าสำรองโดยใช้แก๊สหรือน้ำมันเชื้อเพลิง ทั้งนี้ต้องมีการสลับไปใช้แหล่งพลังงานสำรองได้อย่างอัตโนมัติเมื่อมีเหตุการณ์ขัดข้องที่แหล่งพลังงานหลัก การเพิ่มขึ้น-ลดลงของกระแสไฟฟ้าอย่างฉับพลันอาจทำให้อุปกรณ์คอมพิวเตอร์เสียหายได้ ดังนั้นผู้บริหารต้องติดตามดูแลให้มีการรักษาระดับของกระแสไฟฟ้าที่มีเสถียรภาพ และดูแลให้มีพลังงานที่เพียงพอ(อย่างน้อยควรรองรับสำหรับการปฏิบัติงาน 2 หรือ 3 วัน) เพื่อรองรับระบบงานสำคัญจำเป็นตามที่กำหนดไว้ในงานที่ได้รับมอบหมาย ผู้บริหารควรเตรียมการในการหาแหล่งพลังงานมาเสริมทดแทนเพื่อรองรับเหตุการณ์ที่กระแสไฟฟ้าหยุดชะงักเป็นเวลานาน แก๊สที่เก็บไว้ในถังควรใช้หมดและเติมใหม่อย่างน้อยทุก ๆ หนึ่งปี อีกทางเลือกหนึ่งเพื่อลดต้นทุนอาจไม่ต้องมีแหล่งผลิตพลังงานสำรองแต่ใช้การติดตั้งกล่องที่เกี่ยวกับกระแสไฟฟ้าภายนอก(exterior electrical box)ไว้ในศูนย์การปฏิบัติงานเพื่อเชื่อมต่อกับแหล่งพลังงานชั่วคราวซึ่งภายใต้แผนการนี้ผู้บริหารควรจะเตรียมการให้เกิดความน่าเชื่อถือในการรองรับความพร้อมใช้งาน

ศูนย์การปฏิบัติงานด้าน IT ควรมีระบบโทรคมนาคมที่รองรับการปฏิบัติงานซึ่งมาจากหลายผู้ให้บริการ การติดตั้งสายของระบบโทรคมนาคมควรกำหนดให้มีการสลับสายได้อย่าง

รวดเร็วจากผู้ให้บริการหนึ่งไปยังผู้ให้บริการอีกรายโดยปราศจากภาระในการที่จะต้องมาจัดระบบการต่อสายใหม่หรือจัดระบบเส้นทางใหม่ด้วย และต้องระวังกรณีที่ผู้ให้บริการต่าง ๆ อาจร่วมกันใช้สายเคเบิ้ลหลักเส้นเดียวกันหรือมีเส้นทางของสายเคเบิ้ลผ่านสำนักงานกลาง จึงต้องดูแลว่าจะไม่เกิดจุดที่เป็น single point of failure หรือความซ้ำซ้อนของเส้นทาง

ผู้บริหารต้องดูแลบริเวณที่ตั้งของสายสื่อสารต่าง ๆ ให้มีความปลอดภัยจากการถูกทำให้สายสื่อสารไม่สามารถใช้การได้จากการมุ่งร้าย หรือจากอุบัติเหตุ และควรจัดทำเอกสารแผนกลยุทธ์เกี่ยวกับเรื่องสายสื่อสารและดูแลจัดการสายสื่อสารต่าง ๆ ด้วยการติดป้ายหรือใช้รหัสสีติดไว้ที่สายเคเบิ้ลเพื่ออำนวยความสะดวกในเวลาที่จะแก้ไขปัญหาหรือปรับปรุงระบบสายสื่อสาร

สถาบันการเงินควรวางแผนเกี่ยวกับระบบปรับอากาศ อุณหภูมิ และ ให้เหมาะสมกับความต้องการของอุปกรณ์คอมพิวเตอร์ที่มีอยู่ โดยอุปกรณ์คอมพิวเตอร์รุ่นเก่าจะผลิตความร้อนสูงกว่าเครื่องรุ่นใหม่ ๆ จึงต้องการระบบปรับอากาศที่มากกว่า แหล่งพลังงานสำรองที่เตรียมไว้ควรจะรองรับระบบปรับอากาศ อุณหภูมิ และความชื้นด้วยเพราะหากความเย็นไม่เพียงพออาจจะทำให้อุปกรณ์คอมพิวเตอร์ไม่สามารถทำงานได้ และผู้ปฏิบัติงานควรสามารถปฏิบัติตามขั้นตอนที่เขียนไว้ในแผนฉุกเฉินได้ในกรณีที่ระบบปรับอากาศ อุณหภูมิ และความชื้นหยุดชะงักหรือขัดข้องในด้านบุคลากร ควรจัดให้มีสิ่งจำเป็นต้องใช้ เพื่อรองรับเมื่อเกิดเหตุขัดข้องได้ 1 ถึง 2 วันทำการ เช่น ขวดน้ำดื่มและอาหารที่สามารถเก็บรักษาได้นาน

ศูนย์การปฏิบัติงานด้าน IT ทุกศูนย์ควรติดตั้งเครื่องตรวจจับความร้อนและควันไฟไว้บนเพดาน ในท่อปล่อยควันเสีย และใต้พื้นห้อง แต่เครื่องตรวจจับความร้อนและควันไฟไม่ควรติดตั้งใกล้ช่องลมระบายอากาศของเครื่องปรับอากาศ หรือช่องที่สามารถจ่ายควัน บางศูนย์การปฏิบัติงานที่ใหญ่ ๆ เริ่มที่จะใช้ระบบเตือนและตรวจจับควันที่มีประสิทธิภาพมากขึ้นสามารถเตือนได้อย่างรวดเร็ว (very early smoke detection alert, VESDA) เพื่อแทนที่เครื่องตรวจจับแบบเดิม ระบบ VESDA จะสุ่มตรวจระบบปรับอากาศอย่างต่อเนื่องและว่องไวในการตรวจจับมากขึ้นโดยสามารถตรวจเพลิงไหม้ได้ตั้งแต่ที่ขั้นตอนก่อนการเผาไหม้ ตั้งแต่เริ่มเกิดมีควันแต่ยังไม่มีเปลวไฟจึงสามารถที่จะเตือนได้ก่อนที่จะเกิดเพลิงไหม้แต่ว่ามีราคาแพงกว่าระบบตรวจจับแบบเดิม ซึ่งการเตือนได้อย่างรวดเร็วจะช่วยป้องกันการหยุดชะงักของอุปกรณ์จากการปล่อยน้ำหรือโฟมซึ่งอาจทำความเสียหายต่ออุปกรณ์คอมพิวเตอร์ได้

ระบบระงับอัคคีภัยนั้นมีหลากหลาย หนึ่งในหลาย ๆ ระบบที่ใช้กันอยู่ทั่วไปได้แก่ ระบบแก๊สฮาลอนแต่ระบบนี้จะทำให้โอโซนลดลงจึงมีผลต่อสิ่งแวดล้อม รัฐบาลสหรัฐจึงให้

ยกเลิกการใช้ระบบแก๊สฮาลอนโดยมีกำหนดตั้งแต่ 31 ธันวาคม 2546 เป็นต้นไป **สถาบันการเงินที่ยังใช้ระบบแก๊สฮาลอนจึงควรเตรียมการในการเปลี่ยนระบบระงับอัคคีภัยใหม่** ระบบดับเพลิงที่ใหม่กว่า ได้แก่ ระบบ FM-200, FE-13 และคาร์บอนไดออกไซด์ หรือบางแห่งอาจจะใช้น้ำในการระงับอัคคีภัย ซึ่งมีให้เลือกทั้งแบบที่มีน้ำอยู่ในท่อพร้อมแล้ว(wet-pipe) หรือท่อที่ไม่มีน้ำ(dry-pipe) ซึ่งระบบแบบที่มีน้ำอยู่ในท่อพร้อมแล้ว(wet-pipe) อาจมีความเสี่ยงจากท่อรั่วได้ **ตามหลักการที่สมบูรณ์แบบระบบระงับอัคคีภัยควรมีเวลาพอให้เจ้าหน้าที่โอเปอร์เรเตอร์ทำการปิดระบบของอุปกรณ์คอมพิวเตอร์และทำการคลุมอุปกรณ์คอมพิวเตอร์ต่าง ๆ ด้วยวัสดุป้องกันน้ำให้เรียบร้อยได้ก่อนที่ระบบระงับอัคคีภัยจะปล่อยน้ำออกมา** น้ำที่รั่วไหลออกมาอาจทำความเสียหายต่ออุปกรณ์คอมพิวเตอร์และสายไฟที่อยู่ใต้พื้นห้องคอมพิวเตอร์ได้ ดังนั้นที่ใต้พื้นห้องคอมพิวเตอร์จึงควรมีอุปกรณ์ตรวจจับน้ำเพื่อจะได้แจ้งเตือนผู้บริหารในกรณีที่อาจมีน้ำรั่วโดยที่มองไม่เห็น และอาจจะพิจารณาติดตั้งตัวระบบการระบายน้ำที่ใต้พื้นห้องคอมพิวเตอร์หรือใต้เครื่องคอมพิวเตอร์ที่มีราคาสูง

(2) <u>การดูแลบำรุงรักษาด้วยมาตรการป้องกัน (Preventive Maintenance)</u>

การดูแลบำรุงรักษาอุปกรณ์ด้วยมาตรการป้องกันจะช่วยลดความเสี่ยงต่อความขัดข้องของอุปกรณ์และสามารถตรวจหาปัญหาได้แต่เนิ่น ๆ ซึ่งครอบคลุมตั้งแต่การบำรุงรักษาเล็ก ๆ น้อย เช่น การทำความสะอาดอุปกรณ์ไปจนถึงการบำรุงรักษาที่ทำโดยบริษัทผู้ผลิต หรือผู้จำหน่าย รวมทั้งการทำความสะอาดโดยทั่วไปเพื่อให้ศูนย์ปฏิบัติการมีความสะอาดเรียบร้อย

เจ้าหน้าที่โอเปอเรเตอร์ไม่ควรทำงานที่นอกเหนือจากภาระหน้าที่ตามที่ได้รับมอบหมาย เช่น ไม่ควรซ่อมอุปกรณ์คอมพิวเตอร์เองแม้ว่าจะมีความรู้ความสามารถทำได้ก็ตาม ยกเว้นว่าได้รับการอนุมัติจากผู้บริหาร เนื่องจากสัญญาประกันเครื่องฮาร์ดแวร์และซอฟแวร์ส่วนใหญ่จะปฏิเสธความรับผิดชอบหากมีการเปลี่ยนแปลงแก้ไขใด ๆ **การดูแลบำรุงรักษาอุปกรณ์โดยโอเปอร์เรเตอร์ควรทำตามคู่มือที่บริษัทผู้ผลิตแนะนำให้ทำ ซึ่งโดยทั่ว ๆ ไป ได้แก่หน้าที่เหล่านี้**

- การทำความสะอาดหัวอ่านเทป
- การทำความสะอาดเครื่องเป็นประจำทุกวัน
- การตรวจสอบและทำความสะอาดเครื่อง MICR (the magnetic ink character recognition) reader/sorter ทุกครั้งในเวลาที่จะเปลี่ยนผลัดของโอเปอเรเตอร์
- การตรวจสอบและทำความสะอาดใต้พื้นห้องคอมพิวเตอร์ตามระยะเวลาที่กำหนด

ตารางปฏิบัติงานการดูแลบำรุงรักษาจะแตกต่างกันไปตามจำนวนและความแตกต่างของระบบเทคโนโลยี และปริมาณงานที่ต้องประมวลผล การบำรุงรักษาควรปฏิบัติตามตารางเวลาที่กำหนดทุกครั้ง **และผู้ปฏิบัติงานควรบันทึกรายการการบำรุงรักษาไว้เป็นเอกสารเพื่อให้ผู้บริหารทำการสอบทานการปฏิบัติงานของพนักงานและบริษัทผู้ให้บริการ**

บริษัทผู้ผลิตหรือบริษัทที่เป็นตัวแทนจำหน่ายจะดูแลบำรุงรักษาให้ตามที่ระบุในสัญญา สำหรับอุปกรณ์ที่สถาบันการเงินเช่าใช้บริการอาจจะระบุเรื่องของการบำรุงรักษาไว้เป็นส่วนหนึ่งของสัญญาเช่า สำหรับการใช้บริการศูนย์การปฏิบัติงานจากบุคคลภานอก ผู้บริหารควรจะดูแลให้มีการแยกระหว่างสัญญาบำรุงรักษาอุปกรณ์คอมพิวเตอร์โดยบริษัทผู้ผลิตและสัญญาให้บริการโดยศูนย์การปฏิบัติงาน สัญญาการดูแลบำรุงรักษาควรจะครอบคลุมบริการซ่อมอุปกรณ์ บริการบำรุงรักษาในลักษณะที่เป็นการป้องกันปัญหาและมีตารางกำหนดเวลาการบำรุงรักษา ศูนย์การปฏิบัติงานอาจใช้ฮาร์ดแวร์จากหลาย ๆ บริษัทผู้ผลิตแต่อาจจะใช้บริการดูแลบำรุงรักษาจากบริษัทผู้ให้บริการรายใดรายหนึ่งเพียงรายเดียวก็ได้ นอกจากนี้ในสัญญาการบำรุงรักษาควรมีกำหนดเกี่ยวกับการรับประกันเวลาในการซ่อม/การปฏิบัติงานของผู้ให้บริการ ผู้บริหารควรแจ้งกำหนดการในการบำรุงรักษาให้กับเจ้าหน้าที่โอเปอเรเตอร์ทราบ เพื่อที่เมื่อถึงกำหนดเวลานั้นโอเปอเรเตอร์จะได้ทำการ dismount โปรแกรมและข้อมูลทุกอย่างที่ไม่เกี่ยวข้องแล้วเหลือแต่เพียงซอฟแวร์ที่ต้องการใช้สำหรับการบำรุงรักษาเท่านั้น **แต่หากไม่สามารถปฏิบัติดังที่กล่าวนี้ได้ผู้บริหารควรทำการสอบทานกิจกรรมที่บันทึกอยู่ใน system logs เพื่อติดตามดูว่ามีการเข้าถึงโปรแกรมหรือข้อมูลในระหว่างที่ทำการดูแลบำรุงรักษาหรือไม่** และควรมีเจ้าหน้าที่โอเปอเรเตอร์อย่างน้อย 1 คนอยู่กับเจ้าหน้าที่จากบริษัทผู้ให้บริการตลอดเวลาที่ปฏิบัติงานอยู่ในศูนย์คอมพิวเตอร์ **บริษัทผู้ให้บริการบางรายอาจจะปฏิบัติงานบำรุงรักษาผ่านการ online ซึ่งโอเปอเรเตอร์ควรระมัดระวังไม่ให้การ online นั้นมารบกวนการให้บริการงานประมวลตามปกติของ สง. และโอเปอเรเตอร์และเจ้าหน้าที่ด้านความปลอดภัยของ สง. ควรกำหนดขั้นตอนการรักษาความปลอดภัยเพื่อให้มั่นใจว่ามีการอนุญาตให้ remote access เข้ามาบำรุงรักษาโดยผู้ให้บริการที่ได้รับการอนุมัติสิทธิและการปฏิบัติงานนั้นอยู่ภายในเวลาและขอบเขตงานที่กำหนดเท่านั้น** โอเปอเรเตอร์ควรบันทึกปัญหาต่าง ๆ และ downtime ของระบบระหว่างช่วงเวลาที่ผู้ให้บริการทำการบำรุงรักษา ซึ่งผู้บริหารสามารถใช้บันทึกดังกล่าวเป็นเครื่องมือในการบริหาร เช่น ใช้ในการคัดเลือกผู้ให้บริการ ใช้เพื่อเปรียบเทียบมาตรฐานของอุปกรณ์ต่าง ๆ ใช้ในการตัดสินใจเปลี่ยนหรือเพิ่มเติมอุปกรณ์

- การรักษาความปลอดภัย (SECURITY)

1 <u>การรักษาความปลอดภัยทางกายภาพ (Physical Security)</u>

บุคลากร อุปกรณ์คอมพิวเตอร์ และข้อมูล ต่างเป็นทรัพย์สินที่สำคัญด้านการปฏิบัติงาน IT ผู้บริหารควรจะจัดให้มีการควบคุมรักษาความปลอดภัยทางกายภาพโดยจัดแบ่งบริเวณของศูนย์ปฏิบัติงาน IT โดยอาจ**แบ่งตามความสำคัญของมูลค่าชั้นความลับ และความจำเป็นของข้อมูลที่เก็บอยู่/ที่สามารถเข้าถึงได้ และหรือแบ่งตามความเสี่ยงที่ระบุไว้** หัวข้อนี้จะเป็นการสรุปมาตรการควบคุมและตรวจจับเพื่อการรักษาความปลอดภัยทางกายภาพเพียงบางมาตรการ และกล่าวถึงมาตรการขั้นต่ำด้านการรักษาความปลอดภัยทางกายภาพบางมาตรการเท่านั้น ซึ่งรายละเอียดเพิ่มเติมสามารถดูได้จากคู่มือตรวจสอบการรักษาความปลอดภัยข้อมูล

ศูนย์ปฏิบัติงานด้าน IT ควรจะจำกัดจำนวนของหน้าต่าง-ประตู หรือจุดที่จะเข้าถึงได้และมีแสงสว่างที่เพียงพอ อุปกรณ์ด้านการรักษาความปลอดภัยต่าง ๆ เช่น ประตูหรือรั้ว กล้องวีดีโอ และสัญญาณเตือนภัย เป็นต้น ผู้บริหารควรประเมินการปฏิบัติหน้าที่ของเจ้าหน้าที่รักษาความปลอดภัยว่าปฏิบัติการได้เหมาะสมหรือไม่ และได้รับการฝึกอบรม ได้ถูกตรวจสอบประวัติ และมีใบอนุญาตหรือปฏิบัติตามมาตรฐานของแนวทางการรักษาความปลอดภัยหรือไม่ **ผู้บริหารควรให้มีการติดตามพฤติกรรมที่ผิดปกติจากกล้องวีดีโอ และอุปกรณ์บันทึกภาพต่าง ๆ รวมทั้งควบคุมเกี่ยวกับการติดสลากทะเบียนบัญชีทรัพย์สิน บาร์โค้ด เพื่อควบคุมทรัพย์สินและอุปกรณ์ที่สำคัญและมีมูลค่า** สถาบันการเงินควรนำนโยบายและแนวทางการปฏิบัติที่จะช่วยป้องกันการลบล้างข้อมูลสารสนเทศที่สำคัญมาใช้งาน ซึ่งนโยบายนี้ควรที่จะนำมาใช้กับเครื่องคอมพิวเตอร์พกพา(laptop computers) เครื่องพีดีเอ(personal digital assistants) และอุปกรณ์เก็บข้อมูลแบบพกพาต่าง ๆ ด้วย ยิ่งไปกว่านั้นอาจขยายไปถึงเอกสารที่เป็นความลับต่าง ๆ และการลบสื่ออิเล็กทรอนิกส์

2 <u>การรักษาความปลอดภัยทางตรรกภาพ (Logical Security)</u>

การรักษาความปลอดภัยสารสนเทศมีความเกี่ยวข้องกับการปฏิบัติงานด้านเทคโนโลยี ศูนย์ประมวลผลข้อมูลควรที่จะสนับสนุนให้เกิดโครงสร้างและกระบวนการทางด้านการรักษาความปลอดภัยสารสนเทศต่อองค์กร โดยรายละเอียดเพิ่มเติมสามารถดูได้จากคู่มือตรวจสอบการรักษาความปลอดภัยข้อมูล ผู้บริหารควรที่จะทำการแบ่งประเภทของข้อมูลสารสนเทศให้เหมาะสมกับความซับซ้อนของระบบในองค์กรซึ่งโดยทั่วไปจะแบ่งตามความอ่อนไหวของสารสนเทศและจัดให้มีการควบคุมที่เหมาะสมกับประเภทของสารสนเทศที่จัดแบ่งไว้ ซึ่งเจ้าหน้าที่ด้านการปฏิบัติงาน IT ควรจะเข้าใจถึงนโยบายในการแบ่งประเภทและสามารถดูแลจัดการกับสารสนเทศประเภทต่าง ๆ ได้

อย่างถูกต้อง ต้องตระหนักและเข้าใจเกี่ยวกับมาตรการด้านการรักษาความปลอดภัยขององค์กร รวมทั้งเข้าใจบทบาทหน้าที่ของตนเองในฐานะผู้ดูแลรักษาข้อมูลสารสนเทศที่จะต้องดูแลรักษาความปลอดภัยต่อข้อมูลสารสนเทศที่ประมวลผลหรือเก็บอยู่

การบริหารจัดการด้านการปฏิบัติงาน IT สำหรับ**การรักษาความปลอดภัยทางตรรกภาพนั้น สามารถจะนำมาใช้ได้ทั้งมาตรการแบบป้องกัน เช่น การใช้ระบบ access control** มาตรการ**แบบตรวจจับพฤติกรรมที่เกิดขึ้นแล้ว เช่น การใช้ log ในการบันทึกกิจกรรมต่าง ๆ และ มาตรการการแก้ไขปัญหา เช่น แผนในการรับมือเหตุการณ์บุกรุก และการควบคุมเหล่านี้สามารถนำมาใช้ผ่านทางการบริหาร เช่น การกำหนดนโยบาย** ทางตรรกภาพ เช่น การใช้ access control หรือทางกายภาพ เช่นการล็อคประตูห้อง

ผู้บริหารควรจะนำหลักการ “การให้สิทธิน้อยที่สุดตามความจำเป็นในการปฏิบัติงาน” (least possible privilege) มาใช้กับการปฏิบัติงานด้าน IT สิทธิการเข้าถึงอาจแบ่งได้เป็น read-only, read-write หรือ create/modify ซึ่งแม้แต่สิทธิ read-only ก็มีความเสี่ยงต่อการที่จะถูกพิมพ์หรือทำสำเนาข้อมูลสารสนเทศของลูกค้าไปใช้ในทางที่ไม่เหมาะสมได้ โดยสิทธิการเข้าถึงของเจ้าหน้าที่ System และ Security administrator จะได้สิทธิพิเศษในการแก้ไขสิทธิการเข้าถึงระบบหรือข้อมูลได้ จึงควรกำหนดสิทธิที่เกี่ยวกับรายการธุรกรรมต่อ System และ Security administrator ให้น้อยที่สุด และควรให้มีเจ้าหน้าที่ที่มีความเป็นอิสระมาสอบทานกิจกรรมต่าง ๆ ของ System และ Security administrator ในกรณีขององค์กรขนาดเล็กการแบ่งแยกหน้าที่และหลักการให้สิทธิน้อยที่สุดตามความจำเป็นในการปฏิบัติงานอาจปฏิบัติได้ยากเพราะมีทรัพยากรไม่เพียงพอซึ่งก็อาจนำการควบคุมอื่นมาใช้เพื่อชดเชยได้

เครื่องมือที่เกี่ยวกับการติดตามและดูแลรักษาระบบและเครือข่ายสื่อสาร ซึ่งใช้การตรวจสภาพปัญหาความผิดพลาดต่าง ๆ นั้น ทำให้เจ้าหน้าที่ด้านปฏิบัติงาน IT สามารถเข้าถึงข้อมูลสำคัญหรืออุปกรณ์ในศูนย์การปฏิบัติงาน IT อย่างไม่เหมาะสมได้เพราะเครื่องมือ เช่น network sniffers , network diagnostics tools และ network management utilities สามารถทำการควบคุมแบบเดิม ๆ ได้ ดังนั้นผู้บริหารควรควบคุมการเข้าถึงเครื่องมือเหล่านี้ ไม่ทำให้เจ้าหน้าที่ผู้ปฏิบัติงานสามารถเข้าถึงหรือควบคุมเครื่องมือหลาย ๆ อย่างในเวลาเดียวกัน เช่น รายงานในการควบคุมตรวจสอบ Toolsที่ใช้ การกำหนดนโยบายการใช้ สิทธิพิเศษขั้นต่ำ การใช้ Logs

เครื่องมือ remote monitoring and administration tools จะนำไปสู่ความเสี่ยงที่พิเศษต่อการรักษาความปลอดภัยสารสนเทศ เพราะเครื่องมือนี้ช่วยให้โอเปอเรเตอร์เชื่อมต่อจาก

สถานที่อื่นผ่านทาง remote function เข้ามาปฏิบัติงานที่ต้องทำตามหน้าที่ได้ ซึ่งบางองค์กรได้เปิดฟังก์ชั่นนี้เป็นการทั่วไปให้พนักงานทุกคนใช้ได้ เจ้าหน้าที่ด้านการรักษาความปลอดภัยสารสนเทศควรจะติดตามการใช้งานฟังก์ชัน remote access นี้อย่างสม่ำเสมอ เพราะการเปิดให้ใช้ฟังก์ชัน remote access นี้ตลอดเวลาจะมีความเสี่ยงอย่างมากที่สุดต่อสถาบันการเงิน เพราะฟังก์ชัน remote access นี้มีศักยภาพที่จะก้าวข้ามระบบการรักษาความปลอดภัยไปได้ ผู้บริหารจึงควรประเมินและนำฟังก์ชันนี้มาใช้อย่างเหมาะสมทั้งการกำหนดสิทธิการใช้งาน การบันทึก log กิจกรรมที่ทำการควบคุมเวลาที่สามารถใช้งานฟังก์ชันนี้ได้เพื่อจะลดความเสี่ยงต่อการเข้าถึงโดยผู้ไม่ได้รับอนุมัติ

ประเภทของการ remote access อื่น เช่น โมเด็มที่ต่อเข้ากับระบบหรือต่อเข้ากับ port พิเศษที่ใช้ในการบำรุงรักษาอาจจะทำให้เกิดสภาพที่เป็น remote access ได้ เจ้าหน้าที่รักษาความปลอดภัยสารสนเทศจึงควรดูแลจุดที่เป็น remote access เหล่านี้เพราะอาจเป็นช่องทางให้เกิดการเข้าถึงอุปกรณ์สำคัญโดยบุคคลที่ไม่ได้รับอนุญาต โดย**ผู้บริหารควรกำหนดระยะเวลาในการสอบทานแผนผังโครงสร้างเครือข่ายสื่อสารและทะเบียนทรัพย์สินด้านฮาร์ดแวร์เพื่อที่จะระบุและควบคุมจุดที่เป็น remote access เหล่านี้** และจัดทำนโยบายที่เข้มงวดเกี่ยวกับการใช้โมเด็มหรือการเข้าถึงอุปกรณ์ใด ๆ โดยไม่ได้รับอนุญาต

- การบริหารจัดการฐานข้อมูล (DATABASE MANAGEMENT)

ฐานข้อมูลเป็นศูนย์กลางการเก็บรวบรวมข้อมูลเพื่อการใช้ประโยชน์สำหรับระบบงานธุรกิจต่าง ๆ ซึ่งจะเก็บข้อมูลสำคัญ เช่น ข้อมูลบัญชีลูกค้า ดังนั้นฐานข้อมูลจึงนำไปสู่ความเสี่ยงที่สำคัญ **การบริหารจัดการฐานข้อมูลที่ไม่ปลอดภัยเพียงพออาจนำไปสู่ความไม่ตั้งใจหรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต หรือข้อมูลความลับอาจถูกนำไปเปิดเผยได้ซึ่งก่อให้เกิดความเสี่ยงในด้านชื่อเสียง กฎหมาย และความเสี่ยงด้านปฏิบัติการต่าง ๆ ที่อาจนำไปสู่การสูญเสียด้านการเงินได้**

การแบ่งประเภทของสารสนเทศที่เก็บอยู่ในฐานข้อมูลเป็นพื้นฐานการควบคุมในเบื้องต้น ฐานข้อมูลที่เก็บสารสนเทศที่เป็นความลับนั้นต้องการการควบคุมที่มากกว่า ซึ่งระบบการบริหารจัดการฐานข้อมูลยุคใหม่ ๆ จะสามารถควบคุมติดตามและบันทึกการเข้าถึงข้อมูลได้ถึงระดับรายการ(record) แต่ก็เป็นการเพิ่มต้นทุนค่าใช้จ่าย

Database Administrators จะใช้ระบบบริหารจัดการฐานข้อมูล(database management system, DBMS) ในการติดตั้งค่าต่าง ๆ และในการปฏิบัติงานด้านฐานข้อมูล เนื่องจากซอฟแวร์ DBMS นั้นมีระดับของสิทธิในการเข้าถึงฐานข้อมูลอยู่ในระดับสูง/พิเศษ ผู้บริหารจึงควรดูแล

อย่างเข้มงวดต่อการใช้ซอฟแวร์นี้ **หน้าที่ของ Database Administrators คือการจัดการสิทธิการเข้าถึงสารสนเทศระดับต่าง ๆ ต่อผู้ใช้งานให้เหมาะสม** ดังนั้นความเสี่ยงหลัก ๆ ที่เกี่ยวข้องกับ Database Administrators คือ Database Administrators สามารถแก้ไขข้อมูลได้โดยปราศจากการตรวจจับของระบบได้ และความเสี่ยงที่สอง คือ Database Administrators สามารถเปลี่ยนสิทธิในการเข้าถึงฐานข้อมูลได้ ดังนั้นจึงต้องมีการป้องกันความเสี่ยงเหล่านั้นโดยการติดตามอย่างใกล้ชิดและสอบทานอย่างเข้มงวดต่อการปฏิบัติงานของ Database Administrators ในการเข้าถึงและการแก้ไขข้อมูล

การสร้างสภาพแวดล้อมการทดสอบระบบแยกต่างหาก (independent testing environment) นั้นมีความสำคัญซึ่งช่วยให้ไม่กระทบต่อความถูกต้องเชื่อถือได้ของข้อมูลในระบบงานจริงและช่วยให้การทำงานในระบบงานจริงไม่ถูกขัดจังหวะ แต่ก็**มีความเสี่ยงต่อการรักษาความปลอดภัยสารสนเทศในฐานข้อมูลทดสอบนั้น เพราะผู้ใช้งานจะทำสำเนาข้อมูลจากฐานข้อมูลจริงมาใช้ทดสอบดังนั้นจึงต้องมีการควบคุมรักษาความปลอดภัยต่อการเข้าถึงข้อมูลที่อยู่ในฐานข้อมูลทดสอบนี้เท่า ๆ กับในระบบงานจริง** การเปลี่ยนแปลงแก้ไขฐานข้อมูลจะต้องปฏิบัติตามระเบียบปฏิบัติด้านการเปลี่ยนแปลงแก้ไขโปรแกรมของ สง. ทันทีที่การทดสอบเสร็จสิ้น

เนื่องจากฐานข้อมูลเป็นที่เก็บรวบรวมข้อมูลสำคัญมันจึงตกเป็นเป้าหมายของการบุกรุกทั้งจากภายในและภายนอก ดังนั้น Database Administrators จึงควรได้รับการอบรมและสร้างความตระหนักต่อการปฏิบัติงานเพื่อจะช่วยให้การรักษาความปลอดภัยสารสนเทศมีความสมบูรณ์มากขึ้น ในระหว่างที่ Administrators ทำหน้าที่ติดตามดูแลฐานข้อมูลนั้นควรให้ความสนใจต่อกิจกรรมที่เปลี่ยนแปลงไปจากปกติซึ่งอาจจะบ่งบอกถึงสภาพของกิจกรรมที่ไม่เหมาะสมและอาจก่อให้เกิดปัญหาได้ เช่น ไวรัสอาจมีผลกระทบต่อฐานข้อมูล ดังนั้นหาก Administrators ให้ความสนใจต่อกิจกรรมที่ผิดปกติเหล่านี้ก็จะช่วยปกป้องข้อมูลสำคัญหรือช่วยให้การฟื้นคืนระบบกลับสู่สภาพปกติหรือแจ้งต่อเจ้าหน้าที่ด้านการรักษาความปลอดภัยได้ทันเวลา

ระบบงานที่เชื่อมต่อกับฐานข้อมูลจะต้องมีการรักษาความปลอดภัยสารสนเทศโดยใช้ User/Password และการให้ระดับสิทธิในการเข้าถึงฐานข้อมูลซึ่งควรให้อนุญาตเฉพาะฟังก์ชันหน้าที่ที่ระบบงานนั้นจำเป็นต้องใช้เท่านั้น

- การควบคุมด้านบุคลากร (PERSONNEL CONTROLS)

ความมั่นคงและปลอดภัยของการปฏิบัติงานด้าน IT นอกจากต้องมีเทคโนโลยีที่เหมาะสมแล้วยังต้องอาศัยพนักงานที่มีทักษะที่เหมาะสม **ผู้บริหารฝ่ายปฏิบัติการจะต้องเป็นผู้ประสานงานกับด้านทรัพยากรบุคคลในการคัดเลือกบุคลากร** โดยต้องมีการคัดเลือกจากใบสมัคร

งานและตรวจสอบประวัติของบุคคลนั้น โดยหากมีการจ้างงานควรตรวจสอบประวัติเป็นระยะ ๆ ให้มีข้อมูลประวัติที่เป็นปัจจุบันอยู่เสมอ

ความมีเสถียรภาพของอัตรากำลังมีความสำคัญต่อประสิทธิภาพของการปฏิบัติงาน เพราะถ้ามีอัตราการลาออกของพนักงานสูงอาจทำให้เกิดการหยุดชะงักในกระบวนการปฏิบัติงานหรือขาดคุณภาพงานและทำให้ต้องสิ้นเปลืองค่าใช้จ่ายในการอบรม ดังนั้นหากเป็นไปได้ผู้บริหารควรดูแลให้มีอัตราการลาออกของพนักงานต่ำ ๆ ซึ่งการกำหนดหน้าที่ความรับผิดชอบและเป้าหมายหรือความคาดหวังที่ชัดเจนอาจจะช่วยลดอัตราดังกล่าวได้

การจัดโครงสร้างอัตรากำลังในการทำงานควรก่อให้เกิดการควบคุมทั้งแบบการควบคุมโดยสองฝ่าย การแบ่งแยกหน้าที่ การหมุนเวียนหน้าที่ที่มีความเหมาะสมและปฏิบัติได้จริง กระบวนการควบคุมภายใน การควบคุมโดยสองฝ่าย และการหมุนเวียนหน้าที่จะก่อให้เกิดการพัฒนาทักษะแก่พนักงานในลักษณะ cross-training ทำให้พนักงานมีทักษะมากขึ้น นอกจากนี้เพื่อเสริมให้กระบวนการควบคุมมีคุณภาพจึงควรมีการแบ่งแยกหน้าที่ที่ดีโดยไม่ให้ใครคนใดคนหนึ่งปฏิบัติงานในกระบวนการทำงานได้ตั้งแต่ต้นจนจบ หรือไม่ให้เป็นทั้งผู้ปฏิบัติและผู้สอบทานความถูกต้องของงานที่ตนเองทำได้ เพื่อป้องกันการทุจริตหรือการตั้งใจทำให้อุปกรณ์ ระบบงานและข้อมูลเสียหายได้ สำหรับสถาบันการเงินขนาดเล็ก การแบ่งแยกหน้าที่อาจทำได้ยาก กรณีนี้อาจใช้วิธีการควบคุมโดยการหมุนเวียนหน้าที่ ซึ่งผู้บริหารก็ควรติดตามดูแลสอบทานการปฏิบัติงานอย่างใกล้ชิดเพื่อที่จะคอยเป็นพี่เลี้ยงในการอบรมและดูแลงานให้เกิดการควบคุมที่มีประสิทธิภาพ

- การบริหารการเปลี่ยนแปลงแก้ไขโปรแกรม (CHANGE MANAGEMENT)

การบริหารการเปลี่ยนแปลงแก้ไขโปรแกรมมีขอบเขตกว้างขวางครอบคลุมในเรื่องการควบคุมการเปลี่ยนแปลงแก้ไขโปรแกรม (change control) การบริหารการติดตั้งเสริมเพิ่มเติมค่าต่าง ๆ (patch management) และการเปลี่ยนแปลงสภาพ (conversions) และยังรวมถึงนโยบาย แนวทางปฏิบัติและกระบวนการในการทำการเปลี่ยนแปลงแก้ไขด้วยซึ่งจะมีกล่าวโดยละเอียดในคู่มือตรวจสอบการจัดการ และคู่มือตรวจสอบการพัฒนาและการจัดหาระบบงานและโปรแกรม

สถาบันการเงินใหญ่ ๆ ที่มีธุรกิจซับซ้อนอาจมีการเขียนนโยบายการเปลี่ยนแปลงแก้ไขระบบงานและโปรแกรม รวมทั้งสร้างมาตรฐานขั้นต่ำในกระบวนการเปลี่ยนแปลงแก้ไข โดยอาจทำในลักษณะที่สามารถใช้ได้กับทั้งองค์กรหรือใช้เฉพาะกับแต่ละประเภทธุรกิจก็ได้

สง.ขนาดเล็กที่มีธุรกิจไม่ซับซ้อนอาจไม่ต้องมีแบบแผนมากนักแต่ยังคงต้องมีการเขียนนโยบายและแนวทางเกี่ยวกับการเปลี่ยนแปลงแก้ไขไว้ด้วย

เนื่องจากเครื่องเมนเฟรม ระบบเครือข่ายสื่อสาร เครื่อง client/server และโปรแกรม มีการเปลี่ยนแปลงแก้ไขที่แตกต่างกัน ดังนั้น สง. จึงอาจต้องเขียนแนวทางปฏิบัติในแต่ละเรื่องที่อาจทำให้เกิดความไม่สอดคล้องกันของกระบวนการเปลี่ยนแปลงแก้ไขได้ ซึ่งการจะทำให้สอดคล้องกันนั้นต้องอาศัยหลักการ ดังนี้ defined, managed, repeatable และ optimized

1 <u>การควบคุมการเปลี่ยนแปลงแก้ไข (CHANGE CONTROL)</u>

การเปลี่ยนแปลงแก้ไขควรจะมีขั้นตอนที่ต้องผ่านการกำกับดูแลโดยคณะกรรมการ ซึ่งควรประกอบด้วยตัวแทนที่เหมาะสมจากสายงานธุรกิจ สายงานสนับสนุน สายงานเทคโนโลยีสารสนเทศ ฝ่ายความปลอดภัยเทคโนโลยีสารสนเทศ และฝ่ายตรวจสอบภายใน โดยที่ **สง. ขนาดใหญ่อาจมีคณะกรรมการที่เกี่ยวกับการเปลี่ยนแปลงแก้ไขโปรแกรมโดยเฉพาะ** ขณะที่ สง. ขนาดเล็กอาจใช้คณะกรรมการเทคโนโลยี (Technology Steering Committee) และควรมีนโยบายเกี่ยวกับเรื่องดังกล่าวโดยควรจะแสดงถึงมาตรฐานขั้นต่ำและปัจจัยที่กำหนดไว้ การกำกับดูแลและการควบคุมเพื่อใช้เป็นกรอบในการบริหารการเปลี่ยนแปลงแก้ไขโปรแกรม มาตรฐานของการควบคุมควรจะกล่าวถึงความเสี่ยง การทดสอบ การอนุมัติ เวลาที่จะนำออกใช้งาน การสอบทานภายหลังการนำออกใช้งาน และการฟื้นคืนระบบ

2 <u>การบริหารการติดตั้งเสริมเพิ่มเติมค่าต่าง ๆ (PATCH MANAGEMENT)</u>

ผู้จำหน่ายซอฟแวร์มักจะพัฒนาหรือออก patches มาเพื่อแก้ไขปัญหา เพิ่มประสิทธิภาพ เพิ่มการรักษาความปลอดภัยให้แก่ซอฟแวร์ตัวเดิมให้ดีขึ้น ผู้บริหารควรสร้างกระบวนการในการติดตามการออก patch การทดสอบ patch ในสภาพแวดล้อมที่แยกต่างหากจากระบบงานจริง และการนำไปใช้แทนซอฟแวร์เดิมในเวลาที่เหมาะสมและการเก็บเอกสารเกี่ยวกับการติดตั้ง patch ไว้ด้วย ผู้บริหารควรสร้างกระบวนการควบคุมเกี่ยวกับเวอร์ชั่นของซอฟแวร์ระบบปฏิบัติการและระบบงาน และควรศึกษาติดตามข้อมูลเกี่ยวกับการปรับปรุงซอฟแวร์ประเด็นทางด้านการรักษาความปลอดภัย การออก patch หรือปัญหาอื่น ๆ ที่เกิดกับซอฟแวร์เวอร์ชั่นที่ใช้อยู่จากในอินเตอร์เน็ตหรือจากแหล่งข้อมูลอื่น เช่น ประกาศต่าง ๆ (bulletins)

3 <u>การเปลี่ยนแปลงสภาพ (CONVERSIONS)</u>

การ conversions จะเกี่ยวข้องกับการเปลี่ยนแปลงที่ใหญ่ ๆ ต่อระบบงานที่ใช้อยู่ การconversions เป็นสิ่งที่ซับซ้อนและมีคุณลักษณะเฉพาะตามแต่ platforms ดังนั้นจึงมีระดับความเสี่ยงที่สูงกว่าและต้องการการควบคุมที่พิเศษมากขึ้น ดังนั้นนโยบาย แนวทางปฏิบัติงาน และการควบคุมที่เข้มงวดจึงมีความสำคัญมากที่จะช่วยไม่ให้ข้อมูลเสียหาย ยิ่งไปกว่านั้นเนื่องจากการแตกสาขาของการ conversions ทำให้เกิดการขยายตัวของการปฏิบัติงานด้านเทคโนโลยี ดังนั้นผู้บริหารจึงควรประเมินกระบวนการปฏิบัติงานทั้งหมดใหม่เป็นระยะๆและพิจารณากระบวนจัดการใหม่ (re-engineering) ให้เหมาะสม การบริหารการทำ conversions จะต้องสร้างการควบคุมที่เกี่ยวกับการเปลี่ยนแปลงแก้ไขและกำหนดแผนกลยุทธ์ รวมทั้งการบริหารโครงการ การทดสอบ การจัดทำแผนฉุกเฉิน การสำรองข้อมูล การบริหารบริษัทผู้จัดจำหน่ายและการตรวจสอบภายหลังการนำระบบงานออกใช้ เพราะการ conversions ที่ไม่ถูกต้องเหมาะสมจะนำไปสู่ปัญหาที่อันตรายร้ายแรงของการปฏิบัติงานด้าน IT ความไม่พอใจของผู้ใช้งานทั้งจากภายในและภายนอกองค์กร ความเสียหายต่อชื่อเสียง และการหยุดชะงักของการปฏิบัติงานที่สำคัญ

- การแจกจ่ายและการส่งข้อมูลสารสนเทศ (INFORMATION DISTRIBUTION AND TRANSMISSION)

1 <u>ผลลัพธ์ หรือ รายงาน (Output)</u>

ผลลัพธ์จากระบบไม่ว่าจะอยู่ในรูปแบบอิเล็กทรอนิกส์หรือในรูปของกระดาษก็อาจจะเต็มไปด้วยสารสนเทศที่เป็นความลับ ดังนั้นผู้บริหารจึงควรวิเคราะห์และจัดทำรายงานแต่เฉพาะที่มีความจำเป็นเท่านั้น เพื่อลดความเสี่ยงต่อการถูกเปิดเผยข้อมูลลับและยังช่วยลดค่าใช้จ่ายรวมทั้งเพิ่มประสิทธิภาพการปฏิบัติงานด้าน IT ด้วย ซอฟแวร์ automated report management หรือซอฟแวร์ที่คล้าย ๆ กันนี้จะช่วยในการควบคุมรายงานต่าง ๆ นอกจากนี้การสร้างกระบวนการทางด้านกายภาพและตรรกภาพสำหรับการแจกจ่ายรายงานทั้งในรูปของกระดาษและในรูปอิเล็กทรอนิกส์จะช่วยให้เกิดสภาพแวดล้อมที่ปลอดภัย เช่น การใช้ตู้ใส่รายงานที่มีกุญแจล็อค รวมทั้งควรมีกระบวนการควบคุมการทำลายรายงานในทั้งสองรูปแบบอย่างเหมาะสม เช่น รายงานในรูปกระดาษควรทำการย่อยก่อนทิ้ง

2 <u>การส่งข้อมูลสารสนเทศ (Transmission)</u>

การควบคุมการส่งข้อมูลสารสนเทศควรจะให้ความสำคัญกับทั้งความเสี่ยงทางกายภาพและตรรกภาพ ซึ่ง สง. ขนาดใหญ่ควรพิจารณาแบ่งแยกวงของเครือข่าย WAN และ

LAN ออกเป็นกลุ่ม ๆ และอาจมีการป้องกันด้วยไฟร์วอลล์ (firewall) เพื่อตรวจสอบรายการที่วิ่งผ่านเข้า-ออก หรืออาจพิจารณาใช้เทคโนโลยีการเข้ารหัสข้อมูล (encryption) หรือ digital certificates หรือ public key infrastructure เพื่อป้องกันความปลอดภัยในการส่งข้อมูล ทั้งนี้รายละเอียดเกี่ยวกับเทคโนโลยีเหล่านี้จะกล่าวไว้ในคู่มือตรวจสอบการรักษาความปลอดภัยข้อมูล

การบริหารจัดการเครือข่ายสื่อสารควรจะมีการติดตามการส่งรายการข้อมูลผ่านระบบโทรคมนาคมในเรื่องของปัญหาเกี่ยวกับอัตราการสูญหายของ packets ข้อมูล การถูกรบกวน ปัญหาเกี่ยวกับประสิทธิภาพหรือความผิดปกติอื่น ๆ นอกจากนี้ Administrators ควรสอบทานเครื่องมืออุปกรณ์เครือข่ายสื่อสารเป็นระยะ ๆ เพื่อตรวจสอบกิจกรรมที่ผิดปกติที่อาจเป็นการบุกรุก ผู้บริหารควรจะสร้างการควบคุมการเข้าถึงอุปกรณ์เครือข่ายที่เข้มงวด เช่น ควรล็อคตู้ของอุปกรณ์เครือข่าย การเปลี่ยนอุปกรณ์เครือข่ายหรือการติดตั้งค่าของระบบใหม่ควรปฏิบัติตามมาตรฐานของการเปลี่ยนแปลงแก้ไขโปรแกรม และควรให้มีการตรวจสอบตัวตนและการอนุญาตตามมาตรฐานที่กำหนดไว้ของ สง. ก่อนที่จะมีการเข้าถึงอุปกรณ์เครือข่ายสื่อสารด้วยวิธีการ remote access

สถาบันการเงิน ควรหลีกเลี่ยงสภาพที่อาจจะเกิดความเสี่ยงจาก single points of failure ซึ่งการกระจายระบบเครือข่ายสื่อสารสำรองไว้ตามตึกต่าง ๆ การสร้างจุดเชื่อมต่อระบบเครือข่ายสื่อสารไปยังศูนย์การปฏิบัติงานด้าน IT หลาย ๆ จุดจะช่วยเพิ่มความยืดหยุ่นและความแข็งแกร่งต่อระบบเครือข่ายสื่อสาร

แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องควรรวมถึงระบบเครือข่ายสื่อสารโทรคมนาคมด้วย โดยต้องจัดให้มีโครงสร้างของระบบเครือข่ายสำรอง และ สง. ควรทำการทดสอบกระบวนการฟื้นคืนระบบเครือข่ายสื่อสารทั้งเครือข่ายภายในของตนเองและเครือข่ายที่ใช้บริการจากผู้ให้บริการภายนอกอย่างละเอียดถี่ถ้วน รวมทั้งผู้บริหารควรจัดทำรายงานการทดสอบไว้เป็นลายลักษณ์อักษรและใช้ผลการทดสอบทำการปรับปรุงแผนฉุกเฉินอย่างเหมาะสม นอกจากนี้ที่ศูนย์ปฏิบัติงานสำรองใด ๆ ก็จะต้องมีการควบคุมรักษาความปลอดภัยทางกายภาพที่ใกล้เคียงกัน ผู้บริหารควรสอบทานสถานะด้านการเงินของบริษัทผู้ให้บริการโทรคมนาคม เพื่อให้มั่นใจว่าจะได้รับบริการที่ต่อเนื่อง สง. ควรจะจัดหาบริษัทผู้ให้บริการสำรองไว้อย่างน้อย 1 แห่ง เพื่อกรณีที่ผู้ให้บริการหลักไม่สามารถให้บริการได้ สง.ขนาดใหญ่ หรือระบบที่เกี่ยวกับการชำระเงินควรจัดหาบริษัทผู้ให้บริการหลักและบริษัทผู้ให้บริการสำรองไว้หลาย ๆ รายเพื่อวัตถุประสงค์ในการให้บริการและการรักษาความปลอดภัย นอกจากนี้ สง. ควรรับทราบระดับความสำคัญของการฟื้นคืนบริการที่ผู้ให้บริการกำหนดไว้ในสัญญาด้วย ซึ่งการสร้างความสัมพันธ์ที่ดีกับผู้ให้บริการจะช่วยให้ผู้ให้บริการอำนวยความ

สะดวกอย่างดีในการฟื้นคืนระบบเครือข่ายสื่อสารหลังจากมีเหตุการณ์การหยุดชะงักของระบบ และ สง. ควรบริหารจัดการผู้ให้บริการภายนอกด้านเครือข่ายสื่อสารโดยควรจะติดตามรายงานที่เกี่ยวกับประสิทธิภาพความสามารถของระบบ ความพร้อมใช้งาน หรือปัจจัยหลักอื่น ๆ จากผู้ให้บริการด้วย ซึ่งรายละเอียดเพิ่มเติมเกี่ยวกับเรื่องนี้สามารถดูได้จากคู่มือตรวจสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และคู่มือตรวจสอบการให้บริการเทคโนโลยีจากบุคคลภายนอก

- การสำรองข้อมูล (STORAGE/BACK-UP)

เป้าหมายหลักของการสำรองข้อมูลที่ผู้บริหารต้องคำนึงถึง ก็คือ ความถูกต้องครบถ้วนและความพร้อมใช้งานของข้อมูล ซึ่งแนวทางในการป้องกันความเสี่ยงของผู้บริหารก็คือจะต้องมีการวางแผนอย่างเหมาะสมและควรมีการเขียนมาตรฐานในเรื่องการจัดการข้อมูลให้เหมาะสมกับระบบงาน การจะตัดสินใจเลือกใช้วิธีการสำรองข้อมูลใดผู้บริหารควรพิจารณาอย่างรอบคอบเกี่ยวกับเรื่องทางเลือกในการติดตั้งค่าต่างๆ ของระบบ (configuration options) การเปรียบเทียบผู้ให้บริการ การวิเคราะห์ต้นทุน/กำไร เป้าหมายการเติบโตขององค์กร **โดยวิธีการสำรองข้อมูลที่เลือกใช้ควรจะสามารถวัดได้อย่างเหมาะสมและรองรับการขยายตัวในอนาคต** ผู้บริหารควรดูแลคลังของชุดข้อมูล สถานที่จัดเก็บหลัก ขอบเขตและความสามารถในการรองรับของระบบจัดเก็บข้อมูล และตระหนักถึงผลกระทบของการขาดกระแสไฟฟ้าต่อสายงานธุรกิจต่าง ๆ เพื่อจะได้สร้างกระบวนการในการฟื้นคืนระบบที่เหมาะสม โดยหากเป็นไปได้ สง. ควรสร้างระบบสำรองทั้งที่เป็นแบบโครงสร้างการสำรองข้อมูลแบบคู่ หรือการทำสำเนาข้อมูลไปที่ศูนย์สำรองเพื่อให้มีข้อมูลที่เท่ากันในทั้งสองศูนย์ เพื่อลดการใช้อุปกรณ์สำรองข้อมูลที่จัดเก็บไว้ภายนอกศูนย์

สถาบันการเงินควรทำการสำรองข้อมูลและโปรแกรม และนำไปจัดเก็บไว้ในสถานที่ปลอดภัยภายนอกศูนย์หลักเพื่อใช้ในการฟื้นคืนระบบในกรณีเกิดเหตุฉุกเฉินที่ทำให้ศูนย์หลักไม่สามารถปฏิบัติงานได้ โดยผู้บริหารควรวางแผนการหมุนเวียนสื่อและกำหนดช่วงเวลาในการจัดส่งและการจัดเก็บสื่อข้อมูลในรูปแบบต่าง ๆ ไปไว้ที่สถานที่เก็บภายนอก รวมทั้งการนำสื่อข้อมูลจากสถานที่จัดเก็บภายนอกกลับมาใช้ได้ในเวลาที่เหมาะสม นอกจากนี้ควรจัดให้มีการสุ่มสอบทานสื่อที่จัดเก็บภายนอกนั้นโดยการสอบทานตารางการสำรองข้อมูลกับสื่อข้อมูลจริงที่จัดเก็บอยู่เป็นระยะ ๆ รวมทั้งควรทดสอบนำสื่อข้อมูลที่จัดเก็บอยู่นั้นมาทดลองติดตั้งโปรแกรมและข้อมูลเป็นระยะ ๆ

ในกรณีที่เกิดเหตุฉุกเฉินทำให้ระบบหยุดชะงักไปนั้น การสร้างข้อมูลขึ้นมาใหม่ไม่ควรต้องย้อนไปทำรายการเกินกว่า 1 วันทำการ ดังนั้นการวางแผนกลยุทธ์ในการสำรองข้อมูลและโปรแกรมควรเริ่มต้นจากการจัดทำทะเบียนของระบบและข้อมูลทั้งหมดในองค์กร โดยอย่างน้อย

ต้องครอบคลุมการประเมินความเสี่ยงของระบบงานและข้อมูลที่สำคัญทั้งหมดขององค์กร ซึ่งข้อมูลทะเบียนที่ได้นี้จะช่วยให้ผู้บริหารสามารถกำหนดวิธีการในการสำรองข้อมูลได้อย่างเหมาะสม ความเสี่ยงหลักของการสำรองโปรแกรมและข้อมูล ก็คือ การไม่สามารถนำระบบและข้อมูลกลับมาใช้งานได้ในกรณีที่เกิดเหตุการณ์หยุดชะงักขัดข้อง ซึ่งอาจมีสาเหตุมาจากกระบวนการในการสำรองข้อมูลที่ไม่มีประสิทธิภาพหรือสื่อที่ใช้สำรองข้อมูลไม่มีประสิทธิภาพ เป็นต้น มาตรฐานในเรื่องการจัดการข้อมูลที่เขียนขึ้นควรจะมีรายละเอียดเกี่ยวกับ วิธีการสำรองข้อมูล การอธิบายหน้าที่ความรับผิดชอบของเจ้าหน้าที่ที่เกี่ยวข้องอย่างเหมาะสม และวิธีการปฏิบัติงานที่เป็นรูปแบบเดียวกันทั้งองค์กร

รายละเอียดเพิ่มเติมเกี่ยวกับกระบวนการสำรอง สามารถดูได้จากคู่มือตรวจสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง โดยเฉพาะในหัวข้อ “off-site storage, software back-up, data file back-up, และ back-up and storage strategies”

- การกำจัดหรือทำลายสื่อที่ใช้จัดเก็บข้อมูล (DISPOSAL OF MEDIA)

กระบวนการทำลายสื่อที่เหมาะสมเป็นสิ่งที่จะช่วยป้องกันความเสี่ยงต่อความเสียหายด้านชื่อเสียงและด้านระเบียบ กฎเกณฑ์ หรือกฎหมายในเรื่องการปกป้องข้อมูลความลับของลูกค้า ผู้บริหารควรสร้างกระบวนการในการทำลายสื่อโดยกระบวนการดังกล่าวควรมีความสัมพันธ์กับความอ่อนไหวของสารสนเทศและประเภทของสื่อที่ใช้สำรองข้อมูล เช่น สื่ออิเล็กทรอนิกส์ที่เก็บข้อมูลสำคัญของลูกค้าควรจะใช้วิธีการ degauss ซึ่งเป็นวิธีปฏิบัติที่เป็นมาตรฐานสื่อข้อมูลในรูปแบบ optical ที่ล้าสมัยแล้ว เช่น “เขียนได้ครั้งเดียว,อ่านได้หลายครั้ง (write once, read many times, WORM)” ควรใช้การทำลายหรือทำรอยขีดข่วนจนกระทั่งไม่สามารถจะกู้ข้อมูลกลับมาได้ และการเก็บข้อมูลที่อยู่ในรูปอิเล็กทรอนิกส์ เช่น บนเทป บนฮาร์ดดิส นั้นจะมีปัญหาเกี่ยวกับการทำลายในรูปแบบเดียวกัน คือ จะมีข้อมูลที่เหลืออยู่และสามารถทำการกู้ข้อมูลกลับมาได้ หลังจากที่ลบข้อมูลไปแล้ว กระบวนการทำลายสื่อดังกล่าวจึงควรใช้เทคนิคในการทำลายสื่อที่จะสามารถล้างข้อมูลสารสนเทศที่สำคัญเหล่านั้นได้

- การทำสำเนาภาพเอกสาร (IMAGING)

ระบบการทำสำเนาภาพเอกสาร (IMAGING SYSTEM) เป็นระบบที่แปลงสภาพเอกสารให้เป็นไฟล์อิเล็กทรอนิกส์ ทำให้จัดเก็บและบริหารได้ดีขึ้นเนื่องจากเป็นวิธีการที่ทำให้ค้นหาและเรียกใช้เอกสารได้รวดเร็วและสามารถใช้เอกสารร่วมกันผ่านระบบเครือข่ายสื่อสารได้สะดวกมากขึ้น คุณภาพของการควบคุมเป็นสิ่งที่มีความสำคัญต่อระบบการทำสำเนาภาพเอกสาร เนื่องจากการควบคุมที่ไม่เพียงพออาจทำให้ไม่สามารถจะเรียกใช้งานสำเนาภาพเอกสารได้ หรืออาจถูก

แก้ไข/ปลอมแปลงสำเนาภาพเอกสาร หรือเกิดการสูญหายของข้อมูลความลับของลูกค้าได้ ดังนั้น ผู้บริหารจะต้องดูแลให้มีการควบคุมที่เพียงพอที่จะรักษาความปลอดภัยในกระบวนการทำสำเนาภาพเอกสารและผู้ตรวจสอบก็ควรทำหน้าที่ในการสร้างให้เกิดการควบคุมในแง่ของการตรวจสอบ (audit controls) และทางเดินรายการเพื่อการตรวจสอบ (audit trails) ที่เหมาะสม เนื่องจากกระบวนการดังกล่าวอาจทำให้การควบคุมและการตรวจสอบที่ใช้กับระบบเอกสารแบบเดิมลดน้อยลง ซึ่งประเด็นสำคัญที่ควรพิจารณาในการควบคุมและตรวจสอบระบบการทำสำเนาภาพเอกสาร ได้แก่

Capture - ผู้บริหารควรดูแลให้มีการควบคุมที่เพียงพอในจุดที่เป็นจุดเริ่มต้นของการทำสำเนาภาพเอกสาร การ Capture สามารถทำด้วย**วิธีการสแกนเอกสาร หรือแปลงสภาพเอกสารให้เป็นไฟล์ word หรือ excel แบบที่ไม่สามารถแก้ไขได้** การควบคุมที่ไม่เพียงพอในจุดนี้อาจทำให้เกิดสำเนาภาพเอกสารที่คุณภาพต่ำ อัตราความผิดพลาดสูง การทำดัชนีมีความผิดพลาด สแกนภาพเอกสารไม่ครบถ้วน หรือถูกปลอมแปลงเอกสารได้ ดังนั้นกระบวนการควบคุมควรจะสามารถป้องกันการแก้ไขเอกสารต้นฉบับเดิมก่อนที่จะสอบทานคุณภาพของสำเนาภาพเอกสารที่สร้างขึ้น

การทำดัชนี (Indexing) – ผู้บริหารควรดูแลให้มีการทำระบบดัชนีที่ถูกต้องเพื่อผู้ใช้งานจะสามารถเรียกใช้ไฟล์สำเนาภาพเอกสารได้ถูกต้องในเวลาที่รวดเร็วทันต่อความต้องการทางธุรกิจ หลักการตั้งชื่อควรที่จะบ่งบอกถึงตัวข้อมูลในเอกสารนั้นและมีการเรียงลำดับเพื่อง่ายในการค้นหา

การรักษาความปลอดภัย (Security) – การประเมินความเสี่ยงด้านการรักษาความปลอดภัยของทั้งองค์กรควรจะต้องประเมินความเสี่ยงของระบบการทำสำเนาภาพเอกสารนี้ด้วย ผู้บริหารจะต้องดูแลให้มีการรักษาความปลอดภัยที่เหมาะสมต่อระบบการทำสำเนาภาพเอกสารและข้อมูลความลับของลูกค้า เช่น โดยใช้การแบ่งแยกหน้าที่ การควบคุมการนำเข้า/รายงาน

การอบรม (Training) – ควรมีการอบรมเกี่ยวกับการใช้ระบบการทำสำเนาภาพเอกสารอย่างเหมาะสม เพื่อให้สำเนาภาพเอกสารที่ได้มีคุณภาพ

การสำรองและการฟื้นคืนระบบ (Back-Up and Recovery) - แผนการสำรองข้อมูลและการฟื้นคืนระบบควรที่จะวางแผนให้สามารถฟื้นคืนระบบได้ภายในเวลาที่กำหนดไว้ในแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง เนื่องจากระบบสำเนาภาพเอกสารทำให้สามารถเก็บข้อมูลของเอกสารได้เป็นปริมาณมาก ๆ ดังนั้นหากไฟล์สำเนาภาพเอกสารเหล่านี้สูญหายก็จะส่งผลกระทบต่อการปฏิบัติงานทางธุรกิจอย่างมีนัยสำคัญเมื่อไฟล์อิเล็กทรอนิกส์ที่สำรองไว้หรือเอกสารที่อยู่ในรูปกระดายของเดิมไม่พร้อมใช้งาน

ประเด็นด้านกฎหมาย (Legal Issues) – สง. ที่เก็บเอกสารในรูปของสำเนาภาพเอกสารควรจะศึกษาผลกระทบทางกฎหมายต่อการแปลงสภาพเอกสารต้นฉบับไปเป็นสำเนาภาพเอกสาร สง. อาจจะถูกเรียกให้ต้องแสดงทางเดินรายการเพื่อการตรวจสอบ (audit trails) และวิธีการปฏิบัติในกระบวนการทำสำเนาภาพเอกสารเพื่อแสดงให้เห็นว่าสำเนาภาพเอกสารจะไม่ถูกแก้ไข

- การบริหารจัดการต่อปัญหาหรือเหตุการณ์ต่าง ๆ (EVENT/PROBLEM MANAGEMENT)

กระบวนการบริหารจัดการปัญหาหรือเหตุการณ์ที่มีประสิทธิภาพจะช่วยป้องกันความเสี่ยงด้านการเงิน ความเสี่ยงด้านการปฏิบัติงาน และความเสี่ยงด้านชื่อเสียง ผู้บริหารควรดูแลให้มีการควบคุมที่เหมาะสมโดยจัดให้มีการระบุปัญหา การบันทึกปัญหา การติดตามปัญหา การวิเคราะห์ปัญหา และการแก้ปัญหาที่เกิดขึ้นระหว่างการปฏิบัติงานประจำวัน

พนักงานที่ปฏิบัติงานด้าน IT ควรได้รับทราบกระบวนการบริหารจัดการปัญหาหรือเหตุการณ์เพื่อเตรียมความพร้อมเมื่อต้องปฏิบัติ ซึ่งผู้ที่ควรเข้ามามีส่วนร่วมในกระบวนการบริหารจัดการปัญหาหรือเหตุการณ์ ได้แก่ หน่วยงานด้านการปฏิบัติงาน IT ผู้บริหารของสถาบันการเงินนั้น ผู้ตรวจสอบภายใน หน่วยงานด้านการป้องกันการทุจริต หน่วยงานด้านการรักษาความปลอดภัยสารสนเทศ และทีมงานที่ทำหน้าที่รับมือและโต้ตอบการบุกรุกด้านการรักษาความปลอดภัย (computer security incident response teams) การวางแผนในการบริหารจัดการปัญหาควรครอบคลุมทั้งฮาร์ดแวร์ ระบบปฏิบัติการ ระบบงาน และอุปกรณ์รักษาความปลอดภัย และควรครอบคลุมประเด็นเหล่านี้

- การระบุปัญหา/เหตุการณ์ต่าง ๆ และการจัดระดับความรุนแรงตามความเสี่ยง
- ผลกระทบจากปัญหา/เหตุการณ์ดังกล่าว และการวิเคราะห์สาเหตุของปัญหา
- การจัดทำเอกสารบันทึกปัญหาและการติดตามสถานะของปัญหา
- ลำดับขั้นของกระบวนการปฏิบัติงาน (The process for escalation)
- แนวทางการแก้ไขปัญหา
- การรายงานต่อฝ่ายบริหาร
- ข้อมูลสารสนเทศเพื่อการติดต่อและการสื่อสาร เช่น รายชื่อ ตำแหน่งในปัจจุบัน และเบอร์โทรศัพท์ของผู้ที่ต้องติดต่อ และผู้ที่ควรได้รับแจ้งให้ทราบเหตุการณ์ เช่น หน่วยงาน

ที่กำกับดูแล ตำรวจ สื่อมวลชน หรือสายงานธุรกิจที่ได้รับผลกระทบ และสภาพเหตุการณ์ที่หน่วยงานเหล่านั้นควรจะได้รับทราบ

แม้ว่าจะมีการวางแผนด้านการปฏิบัติงานเพื่อที่จะให้ได้รับผลงานที่ถูกต้องและตรงเวลาแล้ว แต่เหตุการณ์ผิดปกติก็ยังอาจจะเกิดขึ้นในระหว่างการปฏิบัติงานจริงได้ ดังนั้น ผู้บริหารควรติดตามดูแลและแก้ไขเหตุการณ์เหล่านั้น ซึ่งตัวอย่างของเหตุการณ์ต่าง ๆ ในการปฏิบัติงานบนระบบงานจริง ได้แก่

โปรแกรมขัดข้อง – เจ้าหน้าที่ด้านปฏิบัติการ IT ควรจะบันทึกข้อมูลเหตุการณ์โปรแกรมขัดข้องว่าต้องการแก้ไขทันทีทันใดหรือไม่ และควรแจ้งต่อผู้ที่มีหน้าที่เกี่ยวข้องให้เหมาะสมเพื่อจะได้ทำการปรับปรุงแก้ไขตามกระบวนการเปลี่ยนแปลงแก้ไข บางกรณีอาจต้องการการแก้ไขโดยเร่งด่วนจากเจ้าหน้าที่พัฒนาโปรแกรม ซึ่งกระบวนการเพื่อรองรับเหตุฉุกเฉินเร่งด่วนนี้บางครั้งจะเรียกว่ากระบวนการ “**fire call**” ก็คือจะมีการบอกว่าใครจะเป็นคนแจ้งต่อใคร จะต้องรายงานให้ทราบเกี่ยวกับเรื่องอะไรบ้าง

สถานะของยอดคงเหลือไม่ลงตัว – พนักงานที่มีหน้าที่รับผิดชอบอาจทำการประมวลผลข้อมูลซ้ำอีกครั้งเพื่อตรวจดูความถูกต้องของยอดรวมรายการของการประมวลผลทั้งหมด เนื่องจากอาจมีข้อผิดพลาดขณะที่โอเปอเรเตอร์ทำการประมวลผล ซึ่งควรจะบันทึกผลเป็นเอกสารไว้ด้วยและควรแจ้งให้ผู้บริหารทราบเพื่อการสืบหาสาเหตุและแก้ไขต่อไป

การปฏิบัติงานด้าน IT โดยผู้อื่นที่ไม่ใช่หน้าที่ตามปกติ – โดยปกติแล้วเจ้าหน้าที่ด้านปฏิบัติการจะต้องมีการ cross-trained และมีหน้าที่ในการปฏิบัติงานแทนกันในกรณีมีเจ้าหน้าที่ขาดงาน เช่น โอเปอเรเตอร์อาจจะทำหน้าที่แทนเจ้าหน้าที่ที่ดูแลจัดเก็บเทป ในกรณีเช่นนี้อาจมีความผิดพลาดเกิดขึ้นได้ทั้งโดยตั้งใจและไม่ตั้งใจ ซึ่งการกำหนดให้เจ้าหน้าที่ตำแหน่งใดปฏิบัติงานแทนเจ้าหน้าที่ตำแหน่งใดผู้บริหารควรคำนึงถึงการควบคุมในเรื่องการแบ่งแยกหน้าที่ด้วย

ประเด็นเกี่ยวกับ LOG – เทคนิคการแก้ไขปัญหาส่วนใหญ่ของศูนย์ปฏิบัติการด้าน IT จะขึ้นอยู่กับความสามารถในการอ่าน วิเคราะห์และแปลผลรายการกิจกรรมหลาย ๆ รายการที่เกี่ยวข้องกันใน log การจัดการเกี่ยวกับ**เหตุการณ์ที่อ่านผลได้จาก log เป็นสิ่งที่ผู้บริหารต้องมีส่วนร่วมกับทีม incident response** นอกจากนี้ผู้บริหารทางด้านปฏิบัติงาน IT ควรทำการสอบทานอย่างสม่ำเสมอถึงความครบถ้วนของ log ทุกอันเพื่อให้มั่นใจว่า log ไม่ถูกลบ แก้ไข หรือเขียนข้อมูลทับ

การปฏิบัติงานฐานข้อมูล – ถึงแม้ว่าจะมีเครื่องมือที่ช่วยป้องกันความปลอดภัยให้แก่ฐานข้อมูลแล้วก็ตาม แต่โอเปอเรเตอร์อาจใช้โปรแกรมที่เป็นยูทิลิตี้ของระบบในการเข้าถึง หรือผู้ที่ไม่ได้รับอนุญาตเข้ามาแก้ไขระบบฐานข้อมูลได้ ซึ่งกรณีเหล่านี้อาจทำให้ระบบฐานข้อมูลล่มหรือใช้การไม่ได้ ผู้บริหารทางด้านปฏิบัติงาน IT ควรทำการสอบทาน log อย่างสม่ำเสมอเกี่ยวกับรายการกิจกรรมที่เกี่ยวข้องกับระบบฐานข้อมูล และแจ้งให้ทีม incident response ทราบ

การลาออกของพนักงานด้านปฏิบัติการ – **เมื่อมีพนักงานที่ปฏิบัติงานเกี่ยวข้องกับข้อมูลความลับของลูกค้าลาออกไปด้วยเหตุผลใด ๆ ก็ตาม ผู้บริหารควรเปลี่ยนแปลงหรือเพิกถอนสิทธิของบุคคลนั้นทั้งด้านกายภาพและตรรกภาพ** เช่น กุญแจตู้ บัตรประจำตัวพนักงาน รหัสผู้ใช้งาน ซึ่งควรจะมีระเบียบปฏิบัติในการจัดการเรื่องพนักงานลาออกหรือย้ายหน่วยงานนี้โดยควรกำหนดหน้าที่ความรับผิดชอบระหว่างฝ่ายงานด้านการปฏิบัติงาน IT และฝ่ายทรัพยากรบุคคลให้ชัดเจน

ความผิดปกติในระหว่างการประมวลผล – **ผู้บริหาร หัวหน้ากะ หรือผู้ที่มีความเป็นอิสระ ควรทำหน้าที่สอบทาน log ของการประมวลผลเพื่อตรวจดูรายการที่ผิดปกติ วิเคราะห์สาเหตุและแนวทางการแก้ไข เพราะโอเปอเรเตอร์อาจทำการเรียกโปรแกรมที่อยู่นอกเหนืองานปกติซึ่งอาจเป็นสาเหตุให้เกิดปัญหา หรือตั้งใจจะทำทุจริตก็ได้** ดังนั้นใน สง. ใหญ่ ๆ จึงมักเขียนโปรแกรมในการประมวลผลแบบอัตโนมัติเพื่อลดความเสี่ยงจากเหตุการณ์นี้ ถ้าใน log มีรายการของเหตุการณ์ผิดปกติที่ไม่สามารถอธิบายสาเหตุได้ก็ควรทำการประมวลผลใหม่อีกครั้ง และส่งรายการ log ของเหตุการณ์ผิดปกติที่ไม่สามารถอธิบายได้นั้นให้แก่ทีม incident response เพื่อทำการตรวจสอบ

ผู้บริหารควรให้การอบรมแก่เจ้าหน้าที่ด้านการปฏิบัติงานเพื่อให้ตระหนักและรับทราบบทบาทหน้าที่ของตนในเรื่องของการรักษาความปลอดภัย การแจ้งต่อทีม incident response การปฏิบัติหน้าที่ตามแผนรองรับการดำเนินธุกิจอย่างต่อเนื่อง ซึ่งผู้บริหารจะต้องให้ความสำคัญต่อความปลอดภัยของพนักงานเป็นลำดับแรก (สูงสุด) หากมีเหตุการณ์ที่อาจคุกคามถึงความปลอดภัยต่อชีวิตพนักงาน

- การช่วยแก้ไขปัญหาให้ผู้ใช้งาน (USER SUPPORT/ HELP DESK)

หน้าที่ในการช่วยแก้ไขปัญหาให้ผู้ใช้งานเกี่ยวข้องทั้งผู้ให้บริการภายในองค์กรเองและผู้ให้บริการภายนอก สง. ที่ใช้บริการการปฏิบัติงานจากผู้ให้บริการภายนอก ตัว สง. เองก็จะอยู่ในฐานะของผู้ใช้งาน

กระบวนการในการแก้ไขปัญหาให้ผู้ใช้งานอาจช่วยให้ผู้ใช้งานสามารถปฏิบัติงานตามหน้าที่ได้อย่างมีประสิทธิภาพและประสิทธิผล สง.อาจจะใช้กระบวนการในการแก้ไขปัญหานี้ไปเป็นตัววัดตัวหนึ่งในการวัดระดับการให้บริการภายใน (internal service level agreement , internal SLA) ระดับการให้บริการภายในและวัตถุประสงค์ของการแก้ไขปัญหาที่ไม่สอดคล้องกับความต้องการของผู้ใช้งานจะมีส่วนทำให้รายได้ลดลง เพิ่มต้นทุนค่าใช้จ่าย และลดคุณภาพของการให้บริการแก่ลูกค้าได้

ใน สง. ขนาดใหญ่หน้าที่ของ Help desk ก็คือให้การช่วยเหลือผู้ใช้งาน ซึ่งหน่วยงาน help desk นี้มักจะประกอบด้วยพนักงานที่ได้รับการอบรมเกี่ยวกับการแก้ไขปัญหาโดยมีซอฟแวร์ที่ใช้ช่วยติดตามประเด็นปัญหา แต่ใน สง. ขนาดเล็กอาจมีพนักงานเพียงคนเดียวหรือไม่กี่คนทำหน้าที่นี้โดยอาศัยบริษัทผู้จำหน่ายผลิตภัณฑ์ภายนอกคอยช่วยเหลืออีกที

ทางเลือกของเทคโนโลยีที่มีประสิทธิภาพและเหมาะสมกับการให้บริการแก้ไขปัญหาให้ผู้ใช้งานนั้นมีหลากหลาย เช่น internet, intranet และระบบ voice response unit (VRU) นั้นจะช่วยในการรายงานปัญหาและช่วยให้สามารถลดจำนวนของเจ้าหน้าที่ help desk ที่จะมาคอยช่วยเหลือแก้ไขปัญหาของผู้ใช้งานลงได้ ซึ่งเจ้าหน้าที่ help desk จะต้องทำการบันทึกเรื่องราวปัญหาไม่ว่าโดยการเขียนหรือการบันทึกลงระบบงานคอมพิวเตอร์ ซึ่งรายละเอียดที่ควรบันทึกได้แก่ ผู้ใช้งาน การอธิบายปัญหา ระบบงานที่ได้รับผลกระทบ ระดับความสำคัญของปัญหา สถานภาพปัจจุบันจนถึงการแก้ไข ผู้ที่เกี่ยวข้องในการแก้ไขปัญหา สาเหตุของปัญหา เวลาเป้าหมายที่จะใช้ในการแก้ไขปัญหา ข้อมูลการติดต่อกับผู้ใช้งาน และข้อมูลที่เกี่ยวข้องอื่น ๆ

Help desk ควรประเมินและจัดระดับความสำคัญของปัญหาเพื่อให้ปัญหาที่สำคัญที่สุดได้รับการแก้ไขทันที ซึ่งตัวแปรที่จะใช้ในการจัดระดับปัญหา เช่น จำนวนของผู้ใช้งานหรือลูกค้าที่จะได้รับผลกระทบ การสูญเสียรายได้ ค่าใช้จ่ายที่เกิดขึ้น เป็นต้น

หน้าที่ของ Help desk ยังต้องช่วยสนับสนุนในเรื่องของระบบองค์ความรู้ (knowledge base systems) ซึ่งจะต้องมีเจ้าหน้าที่ไว้คอยตอบคำถามหรือปัญหาทั่วไปด้วย ซึ่งเจ้าหน้าที่ Help desk จะต้องได้รับทราบองค์ความรู้ใหม่ ๆ จากบริษัทผู้จำหน่ายผลิตภัณฑ์หรือจากเจ้าหน้าที่ Help desk ท่านอื่นที่มีประสบการณ์อยู่เสมอ ผู้ใช้งานทั่วไปอาจสามารถเข้าไปใช้ระบบองค์ความรู้ผ่านทางโทรศัพท์ อินเตอร์เน็ต อินทราเน็ต เพื่อจะหาทางแก้ไขปัญหาของตนเองก็ได้แต่ต้องมีระบบการพิสูจน์ตัวตนของผู้ใช้งานที่เหมาะสม ซึ่งจะทำให้ประสิทธิภาพของหน้าที่การแก้ไขปัญหาให้ผู้ใช้งานดีมากขึ้น ถ้ามีการว่าจ้างบริษัทภายนอกทำหน้าที่ในการแก้ไขปัญหาให้ผู้ใช้งาน ผู้บริหารจะต้องให้สิทธิใน

การเข้ามาแก้ไขปัญหาของผู้ให้บริการภายนอกตามหน้าที่งานที่ต้องปฏิบัติ โดยรายละเอียดสามารถดูได้จากคู่มือตรวจสอบการให้บริการเทคโนโลยีจากบุคคลภายนอก

- การควบคุมอื่น ๆ (OTHER CONTROLS)

1 <u>การจัดตารางการปฏิบัติงาน (Scheduling)</u>

การควบคุมและการปฏิบัติตามตารางการปฏิบัติงานที่เข้มงวด จะช่วยให้การปฏิบัติงานมีประสิทธิภาพมากขึ้น ผู้บริหารควรจะจัดให้มีนโยบายหรือแนวทางการปฏิบัติสำหรับการสร้างหรือแก้ไขงานที่จัดไว้ในตารางการปฏิบัติงาน โดยอาจจะใช้เครื่องมือมาช่วยในการจัดตารางการปฏิบัติงานโดยอัตโนมัติหรือไม่ก็ได้

2 <u>เอกสารสำคัญต่าง ๆ (NEGOTIABLE INSTRUMENTS)</u>

เอกสารสำคัญต่าง ๆ ต้องการการควบคุมที่เฉพาะเพื่อป้องกันความเสียหายเป็นตัวเงิน เจ้าหน้าที่ด้านปฏิบัติการควรปฏิบัติตามระเบียบปฏิบัติด้านการรักษาความปลอดภัยต่อต้นฉบับเอกสารสัญญาต่าง ๆ ทั้งที่อยู่ในรูปฟอร์มเปล่าและที่ประมวลผลไปแล้ว

2.2.4 การติดตามและรายงานความเสี่ยง (RISK MONITORING AND REPORTING)

<u>สรุปแนวทางปฏิบัติ</u>

ผู้บริหารควรติดตามดูแลความเสี่ยงจากการปฏิบัติงานด้าน IT และติดตามดูประสิทธิภาพของการควบคุมที่สร้างขึ้น โดยอาจใช้เครื่องมือ เช่น การประเมินตนเองเพื่อสอบทานความเพียงพอและประสิทธิภาพของสภาพแวดล้อมในการควบคุม และใช้การตรวจสอบภายในเพื่อเป็นเครื่องมือในการสอบทานการควบคุมด้วย ทั้งนี้ ผู้บริหารควรจะได้รับรายงานการติดตามและการประเมินตนเองที่ครบถ้วนถูกต้องภายในเวลาที่สมควรด้วย

โดยปกติแล้วการติดตามความเสี่ยงช่วยให้ผู้บริหารและคณะกรรมการมั่นใจว่าการควบคุมการปฏิบัติงานมีประสิทธิภาพ ซึ่งเครื่องมือที่สำคัญในการสอบทานการปฏิบัติงานด้าน IT ได้แก่ รายงาน MIS เช่น รายงานประสิทธิภาพของฮาร์ดแวร์และระบบเครือข่ายสื่อสาร รายงานความพร้อมใช้ของระบบ รายงานเวลาในการตอบสนองต่อการทำงานของระบบ เป็นต้น การประเมินการควบคุมด้วยตนเองอย่างสม่ำเสมอจะเป็นมาตรวัดที่ช่วยให้ผู้บริหารทราบประสิทธิภาพการปฏิบัติงาน

และความเสี่ยง ถึงแม้ว่าจะมีการประเมินการควบคุมด้วยตนเองแล้ว อย่างไรก็ตามยังต้องมีการตรวจสอบทั้งจากผู้ตรวจสอบภายในและภายนอกอยู่ ซึ่งจะทำหน้าที่เป็นผู้ประเมินอิสระในการประเมินการปฏิบัติงานด้าน IT โดยรายละเอียดเกี่ยวกับหน้าที่ของผู้ตรวจสอบ IT สามารถศึกษาเพิ่มเติมได้จากคู่มือตรวจสอบการตรวจสอบภายในและภายนอก

ผู้บริหารควรติดตามระบบเทคโนโลยีอย่างสม่ำเสมอ ไม่ว่าที่ศูนย์ประมวลผลกลางหรือที่กระจายอยู่ตามสายงานธุรกิจหรือที่บริษัทคู่ค้าเพื่อจะดูแลให้มีการปฏิบัติงานอย่างถูกต้อง มีประสิทธิภาพและบรรลุผลสำเร็จตามเป้าหมายที่กำหนดไว้ การติดตามและการรายงานที่มีประสิทธิภาพจะช่วยให้สามารถระบุความไม่เพียงพอของทรัพยากร การปฏิบัติงานที่ไม่ได้มาตรฐาน และยังเป็นการบริหารระบบในลักษณะ proactive อีกด้วยซึ่งจะช่วยให้ สง. บรรลุเป้าหมายที่ต้องการในการขยายธุรกิจได้

ผู้บริหารควรติดตามดูแลการปฏิบัติงานของผู้ให้บริการภายนอกตามแนวทางหรือกระบวนการบริหารจัดการผู้ให้บริการภายนอกที่ สง. กำหนดขึ้น ซึ่งส่วนใหญ่ผู้ให้บริการภายนอกจะต้องปฏิบัติให้ได้ตาม SLA ที่กำหนดไว้โดยผู้บริหารต้องดูแลให้มีการปฏิบัติตามที่กำหนดไว้และให้มีการจ่ายค่าชดเชยหรือค่าปรับหากมีการปฏิบัติไม่เป็นไปตามเงื่อนไขที่กำหนด และรายงานที่ได้รับจากผู้ให้บริการภายนอกควรประกอบด้วยมาตรวัดประสิทธิภาพและการระบุสาเหตุของปัญหา ผลการปฏิบัติงานของผู้ให้บริการภายนอกนั้นควรจะนำมาพิจารณาร่วมกับผลการปฏิบัติงานภายในของ สง. เองด้วยเพื่อใช้ในการวางแผนการปฏิบัติงานที่ดี

ก. การติดตามการปฏิบัติงาน (PERFORMANCE MONITORING)

การบริหารและติดตามการปฏิบัติงานเกี่ยวข้องกับการวัดประสิทธิภาพและประสิทธิผลของการปฏิบัติงานเทียบกับมาตรฐานที่ตั้งไว้ภายในองค์กรหรือมาตรฐานของอุตสาหกรรมภายนอก ตัวแปรที่ใช้วัดการปฏิบัติงาน ได้แก่ การใช้ประโยชน์ของทรัพยากร ปัญหาการปฏิบัติงาน ประสิทธิภาพหรือกำลังความสามารถของระบบ เวลาในการตอบสนองของระบบ และกิจกรรมของพนักงาน ผู้บริหารควรจะประเมินความพึงพอใจของสายงานธุรกิจและลูกค้าภายนอกด้วย ระบบงานหรือพนักงานที่ขาดประสิทธิภาพไม่เพียงส่งผลกระทบต่อความพึงพอใจของลูกค้า แต่ยังอาจทำให้ไม่สามารถปฏิบัติตามสัญญา SLA ที่กำหนดไว้ได้ซึ่งอาจมีผลทำให้ถูกปรับ โดยรายละเอียดเพิ่มเติมสามารถศึกษาได้จากคู่มือตรวจสอบการให้บริการเทคโนโลยีจากบุคคลภายนอก

การวัดการปฏิบัติงานด้าน IT จะแตกต่างกันไปตามขนาดและความซับซ้อนของธุรกิจที่ สง. นั้นดำเนินการอยู่ ผลที่ได้จากการวัดเมื่อนำมาวิเคราะห์จะช่วยสนับสนุนการบริหารงาน

ประจำวันด้านการปฏิบัติงาน ช่วยในการวิเคราะห์หาสาเหตุของปัญหาได้อย่างรวดเร็ว และยังเป็นมาตรวัดพื้นฐานและแนวโน้มของข้อมูลที่ใช้เพื่อวางแผนกำลังความสามารถได้อีกด้วย

ตัวอย่างของการวัดทางด้านเทคโนโลยี เช่น การวัดประสิทธิภาพการใช้งาน CPU ตามประเภทของระบบงาน หรือตามช่วงเวลาต่าง ๆ ของวัน การวัดความพร้อมใช้ของระบบเครือข่ายสื่อสาร การสิ้นสุดของโปรแกรมในลักษณะที่ผิดปกติ

ตัวอย่างของการวัดทางด้านประสิทธิภาพการปฏิบัติงาน : ในด้านของการให้บริการทางเทคโนโลยีหรือ IT help desk เช่น ปริมาณของปัญหาที่ได้รับจากการโทรเข้ามาสอบถาม ในด้านทรัพยากรบุคคล เช่น อัตรากำลังที่มีอยู่จริงเมื่อเทียบกับอัตรากำลังที่อนุมัติตามโครงสร้าง ร้อยละของพนักงานที่ได้รับการอบรม เป็นต้น

ข. การวางแผนเกี่ยวกับกำลังความสามารถของระบบ (CAPACITY PLANNING)

การวางแผนกำลังความสามารถของระบบเกี่ยวข้องกับการใช้ข้อมูลการปฏิบัติงานขั้นพื้นฐานไปจนถึงแบบจำลองและโครงการต่าง ๆ ที่จำเป็นในอนาคต การวางแผนกำลังความสามารถของระบบควรจะเน้นทั้งปัจจัยภายใน (เช่น การเติบโตของธุรกิจ การควบรวมกิจการ สายผลิตภัณฑ์ใหม่ เป็นต้น) และปัจจัยภายนอก เช่น ความพึงพอใจของลูกค้าที่เปลี่ยนแปลงไป กำลังความสามารถของคู่แข่ง เป็นต้น) **ผู้บริหารควรติดตามดูแลกำลังความสามารถของทรัพยากรด้านเทคโนโลยีเพื่อวางแผนในเรื่องกำลังความสามารถของระบบ** เช่น อัตราความเร็วของการประมวลผล อุปกรณ์เก็บข้อมูลหลักของแต่ละเครื่องประมวลผลกลาง เป็นต้น ทั้งนี้ การวางแผนด้านกำลังความสามารถของระบบจะเกี่ยวข้องกับเรื่องของงบประมาณและกระบวนการวางแผนกลยุทธ์ และยังเกี่ยวข้องกับด้านบุคลากร เช่น จำนวนพนักงาน การอบรมอย่างเหมาะสม และการวางแผนสืบทอดตำแหน่งงาน

ค. การประเมินตนเอง (CONTROL SELF-ASSESSMENTS)

การประเมินตนเองใช้สอบทานความเพียงพอและความมีประสิทธิผลของสภาพแวดล้อมการควบคุม เนื่องจากช่วยให้สามารถระบุความเสี่ยงที่เกิดขึ้นหรือความเสี่ยงที่เปลี่ยนแปลงไปได้ล่วงหน้า ผู้บริหารควรกำหนดความถี่บ่อยในการทำการประเมินตนเองตามผลการประเมินความเสี่ยงและใช้การประเมินตนเองนี้ในการกำหนดแผนและขอบเขตการตรวจสอบเนื้อหา และรูปแบบของการประเมินตนเองนี้ก็ขึ้นอยู่กับขนาดและความซับซ้อนของ สง. โดยส่วนใหญ่มักอยู่ในรูปแบบฟอร์มที่เป็นทั้ง narrative responses และแบบ checklist สำหรับเนื้อหาของแบบฟอร์มการประเมินตนเองควรจะเน้นที่เรื่องของการควบคุมต่าง ๆ ให้ครอบคลุมสิ่งที่กล่าวถึงในคู่มือเล่มนี้ เช่น

นโยบาย มาตรฐาน แนวทางการปฏิบัติงาน รวมทั้งการควบคุมที่เฉพาะเจาะจง และควรจะระบุ ชื่อระบบ กระบวนการ หรือหน้าที่งานที่ถูกตรวจสอบ ผู้ที่ทำการประเมิน นอกจากนี้ผู้บริหารจะต้องสอบทานและวิเคราะห์รายงานผลการประเมินด้วย การทำ forensic review ต่อผลการประเมินเป็นสิ่งที่มีค่าในแง่ที่จะทำให้เกิดสภาพแวดล้อมการควบคุมที่มีประสิทธิผล

<u>ส่วนที่ 3</u> แนวทางการตรวจสอบ

3.1 วัตถุประสงค์ของการตรวจสอบ

เพื่อประเมินคุณภาพและประสิทธิผลของการปฏิบัติงานด้านเทคโนโลยีของ สง. ซึ่ง **แนวทางการตรวจสอบนี้จะช่วยในการประเมินความเพียงพอของการบริหารความเสี่ยง และการควบคุมสภาพแวดล้อมด้านการปฏิบัติงานเทคโนโลยีของ สง.** ผู้ตรวจสอบอาจจะเลือกนำบางส่วนของแนวทางนี้ไปใช้ในการตรวจสอบตามความเหมาะสมกับ ขนาด ความซับซ้อน และสภาพทางธุรกิจของ สง. หรือตามความเหมาะสมกับความเสี่ยงที่ได้วิเคราะห์และวางแผนในการตรวจสอบไว้ วัตถุประสงค์และแนวทางการตรวจสอบนี้จะแบ่งเป็น 2 Tier ได้แก่

การตรวจสอบทั่วไป (Tier 1) : ประเมินกระบวนการระบุและบริหารความเสี่ยงของ สง.

การตรวจสอบเชิงลึก (Tier 2) : กล่าวถึงการตรวจสอบในส่วนที่มีความเสี่ยงเพิ่มเติม Tier 1 และ Tier 2 เป็นเหมือนชุดเครื่องมือที่ผู้ตรวจสอบจะสามารถเลือกใช้ได้ในการตรวจสอบแต่ละครั้ง ตามแต่วัตถุประสงค์ในการตรวจสอบที่ตั้งขึ้น ผู้ตรวจสอบควรประสานงานประเด็นการตรวจสอบนี้กับผู้ตรวจสอบด้านอื่น ๆ เพื่อหลีกเลี่ยงการทำงานที่ซ้ำซ้อนและควรรวมประเด็นการตรวจสอบจากแนวทางการตรวจสอบอื่น ๆ ที่เกี่ยวข้องกับการปฏิบัติงานด้าน IT ไว้ด้วย

3.2 วัตถุประสงค์และกระบวนการตรวจสอบทั่วไป (Tier 1)

<u>วัตถุประสงค์ 1</u> : พิจารณา**ขอบเขตและวัตถุประสงค์ของการตรวจสอบการปฏิบัติงานด้านเทคโนโลยี**

1. สอบทานรายงานที่ผ่านมา เพื่อพิจารณาประเด็นหรือข้อสังเกตต่าง ๆ ที่ผ่านมา โดยพิจารณาจาก

- รายงานการตรวจสอบของทางการ
- รายงานการตรวจสอบของผู้ตรวจสอบภายในและภายนอก
- รายงานการสอบทานระบบงานที่ใช้บริการจากบริษัทผู้ให้บริการแก่ สง. นั้น
- สถานะและผลการประเมินความเสี่ยงในภาพรวมของ สง.

2. สอบทานคำชี้แจงของผู้บริหาร จากรายงานการตรวจสอบครั้งก่อน และจากรายงานการตรวจสอบภายในและภายนอกของ สง. ที่ทำการตรวจสอบหลังจากการตรวจสอบครั้งก่อนของทางการ โดยพิจารณาจาก

- ความเพียงพอและระยะเวลาในการดำเนินการแก้ไข
- การแก้ไขควรเป็นการแก้ไขที่ต้นเหตุ
- ประเด็นที่ยังไม่ได้แก้ไข

3. สัมภาษณ์ ผู้บริหารและสอบทานรายการขอที่เกี่ยวกับการปฏิบัติงานสารสนเทศเพื่อดูว่ามี

- การเปลี่ยนแปลงที่สำคัญต่อกลยุทธ์หรือการดำเนินธุรกิจใด ที่อาจส่งผลกระทบต่อสภาพแวดล้อมการปฏิบัติงาน
- การเปลี่ยนแปลงที่สำคัญของโปรแกรมการตรวจสอบ ขอบเขตการตรวจสอบและแผนการตรวจสอบที่เกี่ยวข้องกับการปฏิบัติงาน
- การเปลี่ยนแปลงโครงสร้างพื้นฐาน สภาพแวดล้อม และการติดตั้งค่าหรือองค์ประกอบอื่น ๆ ที่เกี่ยวกับการปฏิบัติงานภายใน
- การเปลี่ยนแปลงทางการบริหารจัดการที่สำคัญ
- การเปลี่ยนแปลงผู้ให้บริการหลัก เช่น ระบบงาน Core Banking ระบบบริการทางอินเตอร์เน็ต เป็นต้น
- ปัจจัยภายในและภายนอกอื่น ๆ ที่อาจส่งผลกระทบกับสภาพแวดล้อมการปฏิบัติงาน

<u>วัตถุประสงค์ 2</u> : พิจารณาคุณภาพของ**การกำกับดูแลและการให้การสนับสนุนการปฏิบัติงานด้าน IT โดยคณะกรรมการและผู้บริหารระดับสูง**

1. พิจารณาโครงสร้างองค์กรของการปฏิบัติงานด้าน IT และประเมินประสิทธิผลของโครงสร้างในการไปสนับสนุนกิจกรรมทางธุรกิจของ สง.

2. สอบทานเอกสารที่แสดงถึง หรือสัมภาษณ์ผู้บริหารถึงระบบงาน และการปฏิบัติงานด้านเทคโนโลยี ในลักษณะภาพรวมทั้งองค์กรเพื่อให้เข้าใจถึงวิธีการที่ระบบเหล่านี้ให้การสนับสนุนต่อกิจกรรมทางธุรกิจ และประเมินความเพียงพอของการจัดทำเอกสารดังกล่าวหรือประเมินความสามารถของผู้บริหาร

3. สอบทานรายงาน MIS ที่เกี่ยวกับการบริหารการปฏิบัติงาน ดูว่ามีการติดตามและรายงานอย่างต่อเนื่องหรือเป็นระยะ ๆ และประเมินความเพียงพอของระบบ MIS ในเรื่องดังต่อไปนี้

- เวลาในการตอบสนองต่อการเรียกใช้งานของระบบ และปริมาณงานในช่วงเวลาหนึ่ง (throughput)
- ความพร้อมใช้ของระบบงาน และ/หรือ เวลาที่ระบบหยุดทำงาน
- จำนวน อัตราร้อยละ ประเภท และสาเหตุของการล้มเหลวของงานประมวลผล
- **อัตราการใช้งานระบบโดยเฉลี่ยและที่ระดับสูงสุด** รวมถึงแนวโน้มและกำลังความสามารถของระบบ

วัตถุประสงค์ 3 : พิจารณาว่า**ผู้บริหารระดับสูงและคณะกรรมการได้ดูแลให้เกิดการบริหารจัดการความเสี่ยงทั้งการระบุ วัด ควบคุม และติดตามความเสี่ยงด้านการปฏิบัติงาน IT** ดังนี้

1. สอบทานเอกสาร หรือสัมภาษณ์ผู้บริหารระดับสูงเกี่ยวกับโอกาสที่จะเกิดขึ้นของความเสี่ยงและผลกระทบต่อการปฏิบัติงานด้าน IT ประเมินกระบวนการประเมินความเสี่ยงของผู้บริหาร

2. สอบทานรายงาน หรือสัมภาษณ์ผู้บริหารเกี่ยวกับการติดตามดูแลการปฏิบัติงานและการควบคุมสภาพแวดล้อม ประเมินความเพียงพอของเนื้อหาในรายงานและความทันต่อเวลาที่ต้องการใช้งานของรายงาน

3. พิจารณาว่าผู้บริหารได้มีการประสานงานกระบวนการจัดการความเสี่ยงด้านการปฏิบัติงานกับกระบวนการจัดการความเสี่ยงด้านอื่น ๆ เช่น ด้านการรักษาความปลอดภัยสารสนเทศ ด้านการวางแผนการดำเนินธุรกิจอย่างต่อเนื่อง และด้านการตรวจสอบภายใน

วัตถุประสงค์ 4 : **ทำความเข้าใจสภาพแวดล้อมการปฏิบัติงาน**

1.สอบทานและพิจารณาความเพียงพอของแบบสำรวจสภาพแวดล้อม และทะเบียนทรัพย์สินหรือเอกสารอื่นที่อธิบายเกี่ยวกับฮาร์ดแวร์และซอฟแวร์ โดยพิจารณาจาก

- อุปกรณ์คอมพิวเตอร์ : ผู้จัดจำหน่าย และรุ่นของเครื่อง
- องค์ประกอบของเครือข่ายสื่อสาร
- ชื่อระบบงาน วันที่นำออกใช้งาน เวอร์ชั่น ของระบบงานทางธุรกิจ ระบบปฏิบัติการ และระบบยูทิลิตี้ต่าง
- รูปแบบของการประมวลผล : online/real time, batch และ memo post

2. สอบทานแผนภาพและผังโครงสร้างของระบบเพื่อให้ทราบถึงที่ตั้งทางกายภาพและเพื่อให้เข้าใจการเชื่อมต่อกันระหว่าง

- ฮาร์ดแวร์
- การเชื่อมต่อเครือข่ายสื่อสารทั้งภายในและภายนอก
- การเชื่อมต่อโดยใช้โมเด็ม
- การเชื่อมต่ออื่น ๆ กับบุคคลที่ 3 ภายนอกองค์กร

3. ทำความเข้าใจสภาพแวดล้อมของระบบเมนเฟรม ระบบเครือข่ายสื่อสาร ระบบโทรคมนาคม และทำความเข้าใจวิธีการและแผนภาพการไหลของสารสนเทศในกระบวนการทางธุรกิจ

4.. สอบทานและประเมิน นโยบาย แนวทางการปฏิบัติงาน และมาตรฐานที่ สง. นำมาใช้กับสภาพแวดล้อมการปฏิบัติงานด้านคอมพิวเตอร์

วัตถุประสงค์ 5 : พิจารณาว่า**มีการควบคุมที่เพียงพอต่อการจัดการด้านการปฏิบัติงานที่สัมพันธ์กับความเสี่ยง**

1. พิจารณาว่าผู้บริหารมีการนำเครื่องมือ กระบวนการ และโปรแกรมต่าง ๆ มาใช้เพื่อให้เกิดการควบคุมการปฏิบัติงานที่มีประสิทธิผลในเรื่องเหล่านี้หรือไม่

- การบริหารจัดการการปฏิบัติงาน และการวางแผนด้านกำลังความสามารถของระบบ
- กระบวนการให้บริการสนับสนุนและแก้ไขปัญหาของผู้ใช้งาน
- การบริหารโครงการ การเปลี่ยนแปลงแก้ไขโปรแกรม การติดตั้งเสริมเพิ่มเติมค่าต่าง ๆ (Project, change and patch management)
- การบริหารการเปลี่ยนแปลงสภาพ (Conversion management)
- มาตรฐานของฮาร์ดแวร์ ซอฟแวร์ และการติดตั้งค่าคอนฟิกกูเรชั่น ของทั้งฮาร์ดแวร์และซอฟแวร์
- การรักษาความปลอดภัยทางด้านตรรกภาพและกายภาพ
- การควบคุมระบบสำเนาภาพเอกสาร (Imaging system controls)
- การควบคุมและติดตามสภาพแวดล้อม
- การบริหารจัดการปัญหาหรือเหตุการณ์

2. พิจารณาว่ามีกระบวนการและมีการควบคุมในการปฏิบัติงานประจำวัน ได้แก่

- ระบบการจัดตารางการปฏิบัติงานที่มีประสิทธิผล

- เครื่องมือในการติดตามดูแลเพื่อตรวจจับปัญหา หรือกำลังความสามารถของระบบ
- การแก้ไขปัญหาที่เกิดกับการประมวลผลประจำวัน และกระบวนการแก้ไขที่เหมาะสม
- การรักษาความปลอดภัยต่อสื่อและอุปกรณ์จัดเก็บข้อมูล และรายงานต่าง ๆ
- การประเมินตนเอง

3. พิจารณาว่าผู้บริหารมีการบริหารจัดการด้านทรัพยากรบุคคลที่เหมาะสม โดยประเมินว่า

- โครงสร้างองค์กรเหมาะสมกับแนวทางการดำเนินธุรกิจของ สง.
- ผู้บริหารได้ทำการสืบประวัติของพนักงานทุกคนที่เกี่ยวข้องกับงานที่มีความเสี่ยงหรือไม่
- การแบ่งแยกหน้าที่ และการหมุนเวียนหน้าที่มีความเพียงพอ
- ผู้บริหารมีนโยบายและแนวทางที่จะป้องกันไม่ให้อัตราการลาออกของพนักงานสูงเกินไป

<u>วัตถุประสงค์ 6</u> : สอบทาน**วิธีการในการจัดเก็บและสำรองข้อมูล** และกลยุทธ์การจัดเก็บที่ศูนย์จัดเก็บข้อมูลสำรอง

1. สอบทานวิธีการเก็บข้อมูลของทั้งองค์กร ประเมินว่าผู้บริหารมีการวางแผนกระบวนการจัดเก็บข้อมูลที่เหมาะสม และมีการสร้างมาตรฐานและแนวทางการปฏิบัติงานที่เหมาะสมเพื่อเป็นแนวทางในการทำงาน

2. สอบทานกลยุทธ์การสำรองข้อมูลของ สง. ประเมินว่าผู้บริหารได้วางแผนกระบวนการสำรองข้อมูลไว้อย่างเหมาะสม และได้สร้างมาตรฐานและแนวทางการปฏิบัติงานที่เหมาะสมเพื่อเป็นแนวทางในการทำงาน

3. สอบทานรายการของทั้งไฟล์ข้อมูลและไฟล์โปรแกรมที่เก็บอยู่ทั้งในศูนย์จัดเก็บข้อมูลหลักและศูนย์จัดเก็บข้อมูลสำรอง พิจารณาว่ารายการของไฟล์ที่เก็บมีความเพียงพอ และผู้บริหารได้วางกระบวนการที่เหมาะสมสำหรับการปรับปรุงและบำรุงรักษาไฟล์ทั้งหลายนี้

4. สอบทานและพิจารณาว่าผู้บริหารได้สร้างกระบวนการสำรองข้อมูลที่เหมาะสมที่จะทำให้การสำรองไฟล์ข้อมูลและไฟล์โปรแกรมทำได้อย่างเหมาะสมกับเวลา ประเมินความเหมาะสมของช่วงเวลาของการหมุนเวียนสื่อเก็บข้อมูลสำรองที่นำไปเก็บไว้ที่ศูนย์จัดเก็บข้อมูลสำรอง

5. ระบุสถานที่ตั้งของศูนย์จัดเก็บข้อมูลสำรองและประเมินว่ามีการควบคุมทางกายภาพที่เพียงพอหรือไม่

6. พิจารณาว่าผู้บริหารได้จัดให้มีการตรวจนับสื่อสำรองข้อมูลที่จัดเก็บไว้ที่ศูนย์สำรองอย่างสม่ำเสมอเป็นระยะ ๆ

7. พิจารณาว่ามีกระบวนการในการนำสื่อที่สำรองข้อมูลและโปรแกรมมาทดสอบอ่านและ restore โปรแกรม เพื่อให้มั่นใจในความพร้อมใช้งาน

วัตถุประสงค์ 7 : พิจารณาว่ามีการดูแลติดตามและการควบคุมสภาพแวดล้อมที่เหมาะสม โดยสอบทาน**การควบคุมสภาพแวดล้อมและติดตามกำลังความสามารถของการปฏิบัติงานด้านเทคโนโลยี** ที่เกี่ยวกับ

- พลังงานไฟฟ้า
- บริการโทรคมนาคม
- ระบบปรับอากาศ และระบบความชื้น
- การเตรียมการเรื่องน้ำ
- สายเคเบิ้ลคอมพิวเตอร์
- เครื่องตรวจจับควันและอุปกรณ์ดับเพลิง
- การรั่วไหลของน้ำ
- การบำรุงรักษาในลักษณะที่เป็นการป้องกันปัญหา

วัตถุประสงค์ 8 : พิจารณาว่ามี**กลยุทธ์และการควบคุมเกี่ยวกับบริการโทรคมนาคมที่เหมาะสม**

1. ประเมินว่ามีการควบคุมที่สอดคล้องกับความเสี่ยงด้านการปฏิบัติงานโทรคมนาคม เช่น

- โครงสร้างและกระบวนการด้านโทรคมนาคมสอดคล้องกับแผนกลยุทธ์
- การดูแลติดตามการปฏิบัติงานด้านโทรคมนาคม เช่น เวลาที่ระบบหยุดทำงาน (downtime) ปริมาณงานในช่วงเวลาหนึ่ง (throughput) อัตราการใช้ประโยชน์/การใช้งานจากกำลังความสามารถของระบบ
- ประเมินความเพียงพอของความพร้อมใช้งาน อัตราความเร็วของโทรคมนาคม และความกว้างของช่องสัญญาณ (bandwidth) กำลังความสามารถของระบบ (capacity)

2. พิจารณาว่ามีการควบคุมรักษาความปลอดภัยต่อสภาพแวดล้อมด้านโทรคมนาคมอย่างเพียงพอ เช่น

- การควบคุมการเข้าถึงตู้เก็บสายสื่อสารโทรคมนาคม อุปกรณ์และสายสื่อสารให้เข้าถึงได้แต่เฉพาะผู้ได้รับอนุญาตเท่านั้น
- การรักษาความปลอดภัยต่อเอกสาร/คู่มือด้านโทรคมนาคม
- กระบวนการเปลี่ยนแปลงแก้ไขระบบโทรคมนาคมที่เหมาะสม
- การควบคุมการเข้าถึงระบบด้วยการพิสูจน์ตัวตน

3. สัมภาษณ์ผู้เกี่ยวข้องว่าระบบโทรคมนาคมมีความยืดหยุ่นและมีการเตรียมการเพื่อให้ระบบมีความต่อเนื่อง เช่น

- กำลังความสามารถของระบบโทรคมนาคม
- การมีผู้ให้บริการด้านโทรคมนาคมที่รองรับหลายราย
- การมีเส้นทางของสายสื่อสารหลายเส้นทาง และมีจุดเชื่อมต่อระบบหลาย ๆ จุด
- การมีระบบโทรคมนาคมสำรองโดยใช้บริการจากผู้ให้บริการโทรศัพท์รายอื่นนอกเหนือจากผู้ให้บริการหลัก

<u>วัตถุประสงค์ 9</u> : ประเมินว่า**ระบบการทำสำเนาภาพเอกสาร (imaging systems) มีสภาพแวดล้อมการควบคุมที่เพียงพอ**

1. ระบุและสอบทานกระบวนการใช้งานและแนวทางการทำสำเนาภาพเอกสาร และบรรยายหน้าที่การทำงานของระบบการทำสำเนาภาพเอกสาร

- ได้รับเอกสารผังโครงสร้างการไหลของข้อมูลในระบบและฟังการบรรยายเกี่ยวกับการไหลของข้อมูลในระบบ
- ประเมินความเพียงพอของการควบคุมระบบการทำสำเนาภาพเอกสาร ในประเด็นเหล่านี้
  - การรักษาความปลอดภัยทางกายภาพ
  - การรักษาความปลอดภัยต่อข้อมูล
  - กระบวนการจัดการเอกสาร
  - การแก้ไขปัญหาข้อผิดพลาด
  - กระบวนการเปลี่ยนแปลงแก้ไขโปรแกรม
  - การฟื้นคืนระบบ

- การเก็บรักษาข้อมูลรายการที่สำคัญ

2. ประเมินความเพียงพอของการควบคุมที่เกี่ยวข้องกับความถูกต้องเชื่อถือได้ของเอกสารที่สแกนเข้าระบบ ทั้งในแง่ของความถูกต้องแม่นยำ ความครบถ้วนสมบูรณ์ และประเด็นที่อาจเป็นการทุจริต

3. สอบทานและประเมินการควบคุมต่อเอกสารต้นฉบับว่าจะไม่ถูกทำลาย เช่น เอกสารต้นฉบับจะไม่ถูกย่อยหลังจากถูกสแกนเข้าไปในระบบการทำสำเนาภาพเอกสารแล้ว

4. พิจารณาว่าผู้บริหารมีการติดตามดูแลและกำกับการปฏิบัติตามกฎหมาย ระเบียบ และมาตรฐานอื่น ๆ

5. ประเมินระดับความสำคัญของระบบการทำสำเนาภาพเอกสารที่เกี่ยวข้องกับกระบวนการวางแผนการดำเนินธุรกิจอย่างต่อเนื่อง และสายงานธุรกิจที่เกี่ยวข้องกับระบบการทำสำเนาภาพเอกสารได้เข้าไปมีส่วนร่วมในกระบวนการตามแผนการดำเนินธุรกิจอย่างต่อเนื่องหรือไม่

6. พิจารณาการแบ่งแยกหน้าที่ที่เกี่ยวข้องกับระบบการทำสำเนาภาพเอกสาร

<u>วัตถุประสงค์ 10</u> : ประเมิน**ความมีประสิทธิภาพของแผนการในการบริหารจัดการปัญหาหรือเหตุการณ์ต่าง ๆ**

1. ประเมินศักยภาพของแผนการในการบริหารจัดการปัญหาหรือเหตุการณ์ต่าง ๆ ในแง่ของการระบุ วิเคราะห์ และการแก้ไข เช่น

- Escalation ของการหยุดชะงักของการปฏิบัติงาน ต่อการประกาศเหตุการณ์ภัยพิบัติ
- การให้ความร่วมมือกับหน่วยงานรักษาความปลอดภัยสารสนเทศในกรณีที่มีเหตุการณ์การบุกรุกระบบรักษาความปลอดภัยหรือเหตุการณ์อื่น ๆ ที่คล้ายคลึงกัน

2. ประเมินว่าแผนการในการบริหารจัดการปัญหาหรือเหตุการณ์ต่าง ๆ มีความเพียงพอต่อการรองรับเหตุการณ์ที่ผิดปกติหรือกิจกรรมที่ไม่ใช่การทำงานโดยปกติ เช่น

- ความล้มเหลวของโปรแกรมที่ประมวลผลบนระบบงานจริง
- รายงานของผลิตภัณฑ์ที่ไม่สมดุล (do not balance)
- การปฏิบัติงานที่ดำเนินการโดยพนักงานที่ไม่ใช่พนักงานที่ทำหน้าที่นั้นเป็นประจำ
- การลบ เปลี่ยนแปลง แก้ไข หรือ เขียนทับไฟล์ที่ถูกระบุไว้บน logs และรายงาน
- การเปลี่ยนแปลงแก้ไขหรือความเสียหายต่อระบบฐานข้อมูล

- การอบรมเกี่ยวกับการสืบสวนเหตุการณ์ และการสร้างความตระหนักต่อเหตุการณ์ต่าง ๆ ที่ผิดปกติ

3. พิจารณาว่ามี help desk ที่ช่วยสนับสนุนและแก้ไขปัญหาให้ผู้ใช้งานทางธุรกิจอย่างเพียงพอหรือไม่ เช่น

- การระบุและวิเคราะห์ปัญหาอย่างมีประสิทธิภาพ
- การแก้ไขปัญหาอย่างทันกาล
- การนำวิธีการป้องกันที่มีประสิทธิภาพมาใช้

วัตถุประสงค์ 11 : ประเมิน**การควบคุมสภาพแวดล้อมของการประมวลผล**รายการของลูกค้า เช่น

- จุดเริ่มต้น หรือจุดนำเข้าของรายการ
- ลักษณะการจัดเก็บของรายการ เช่น microfilming, optical recording หรือ imaging
- หลักฐานการปฏิบัติงาน
- การประมวลผลรายการแบบ batch
- การตรวจสอบยอดจำนวนเงินที่นำเข้าระบบ (Check in-clearing)
- การสอบทานและการกระทบยอดรายการ
- การควบคุมรายการ
- จุดสิ้นสุดของรายการ

สรุป (Conclusion)

วัตถุประสงค์ 12 : **หารือเกี่ยวกับข้อสังเกตที่ตรวจพบ และแนวทางการแก้ไข**

1. พิจารณาความจำเป็นที่จะต้องติดตามตรวจสอบต่อด้วยแนวทางการตรวจสอบใน Tier 2

2. จากการปฏิบัติงานตามแนวทางการตรวจสอบทั้ง Tier 1 และ Tier 2

- ทำบันทึกสรุปเป็นลายลักษณ์อักษรในเรื่องที่เกี่ยวกับประสิทธิผลและการควบคุมในสภาพแวดล้อมการปฏิบัติงาน
- สรุปและบันทึกเพิ่มเติมเกี่ยวกับข้อสังเกตที่คุณอ้างอิงมาจากการปฏิบัติงานตรวจสอบของผู้ตรวจสอบภายในและภายนอกในประเด็นที่เกี่ยวข้องกับประสิทธิผลของการควบคุมการปฏิบัติงาน

3. ทบทวนข้อสรุปในเบื้องต้นของคุณกับหัวหน้าผู้ควบคุมงานตรวจสอบ (EIC) ในเรื่องที่เกี่ยวกับ

- การละเมิดกกหมาย กฎระเบียบ และข้อบังคับ
- การให้เหตุผลรองรับในประเด็นสำคัญซึ่งจะมีความหมายต่อความสนใจของคณะกรรมการ หรือการให้คำแนะนำในรายงานการตรวจสอบ
- การไม่ปฏิบัติตามแนวทางการกำกับดูแล

4. หารือข้อสังเกตที่ตรวจพบกับผู้บริหารและขอทราบแนวทางการแก้ไขที่ผู้บริหารวางแผนไว้

5. ทำบันทึกสรุปความเห็นของคุณส่งให้ผู้นำสายออกตรวจหรือผู้บริหารทีม (EIC) เพื่อจัดเตรียมทำรายงานสรุปผลการตรวจสอบ

6. จัดระดับความเสี่ยงตามแนวทาง URSIT rating

7. จัดทำกระดาษทำการที่จะช่วยสนับสนุนข้อสังเกตที่ตรวจพบและสนับสนุนการสรุปผลการตรวจสอบ

3.3 วัตถุประสงค์และกระบวนการตรวจสอบเชิงลึก (Tier 2)

แนวทางการตรวจสอบใน Tier 2 จัดเตรียมไว้เพื่อการตรวจสอบเพิ่มเติมเพื่อยืนยันความถูกต้องของการประเมินประสิทธิผลของการปฏิบัติงานด้านเทคโนโลยี และยังช่วยผู้ตรวจสอบในการหาต้นเหตุของความอ่อนแอของระบบ ซึ่งแนวทางการตรวจสอบใน Tier 2 นี้จะสามารถเลือกนำไปใช้หรือนำไปใช้ทั้งหมดก็ได้ขึ้นอยู่กับขอบเขตของการตรวจสอบและความจำเป็นที่ต้องการตรวจสอบเพิ่มเติมในการยืนยันความถูกต้อง ผู้ตรวจสอบควรประสานงานประเด็นการตรวจสอบนี้กับผู้ตรวจสอบด้านอื่น ๆ เพื่อหลีกเลี่ยงการทำงานที่ซ้ำซ้อนและควรรวมประเด็นการตรวจสอบจากแนวทางการตรวจสอบอื่น ๆ ที่เกี่ยวข้องกับการปฏิบัติงานด้าน IT ไว้ด้วย

แนวทางการตรวจสอบใน Tier 2 นี้อาจไม่จำเป็นต้องลงทุนด้านการควบคุม โดยการเลือกนำการควบคุมมาใช้งานควรจะสอดคล้องกับความเสี่ยงที่สภาพแวดล้อมการปฏิบัติงานด้าน IT ของ สง. นั้นเผชิญอยู่ ขนาดและความซับซ้อนของการปฏิบัติงานด้านเทคโนโลยีของ สง.

ก. สภาพแวดล้อมการปฏิบัติงาน

1. สอบทานกระบวนการที่วางไว้เพื่อให้มั่นใจว่าระบบต่าง ๆ ยังมีความถูกต้องแม่นยำและสะท้อนให้เห็นภาพรวมทั้งหมดของ สง. โดย

1.1 เครื่องคอมพิวเตอร์ (ประเภท : mainframes, midranges, servers และ standalone)

- ชื่อผู้ขาย (Vendor) และ ชื่อรุ่น (model) และประเภทของเครื่อง
- ระบบปฏิบัติการ วันที่นำออกใช้ของระบบ เวอร์ชั่น
- ประสิทธิภาพของระบบประมวลผล เช่น หน่วยวัดที่เป็น MIPS (millions of instructions per second) เป็นต้น
- หน่วยความจำ (memory)
- ตัวเก็บข้อมูล (Storage)
- บทบาทหน้าที่ (Role)
- สถานที่ตั้ง (Location), IP address (ถ้ามี) และสถานะ (ใช้งาน/ไม่ได้ใช้งาน)
- รูปแบบการประมวลผลระบบงาน

1.2 อุปกรณ์เครือข่ายสื่อสาร (Network devices)

- ชื่อผู้ขาย (Vendor) และ ชื่อรุ่น (model) และประเภท
- IP address
- หน่วยความจำภายในตัวอุปกรณ์ (random access memory)
- รุ่นของฮาร์ดแวร์
- ระบบปฏิบัติการ
- รุ่น เวอร์ชั่นของ patch และวันที่นำ patch ออกใช้งาน

1.3 ซอฟแวร์

- ประเภท หรือชื่อของระบบงาน (Type or application name)
- ผู้ผลิต หรือ ผู้จำหน่าย
- Serial number
- Version level
- Patch level
- จำนวนของสิทธิการอนุญาตให้ใช้ซอฟแวร์ (Number of licenses owned) และ Number of copies installed

ข. นโยบาย แนวทางการปฏิบัติ และระเบียบปฏิบัติในการควบคุม

พิจารณาว่าพนักงานที่เป็นระดับหัวหน้างานได้มีการสอบทาน console log และเก็บรักษา log ไว้ในสภาพแวดล้อมที่ปลอดภัยเพื่อใช้ในเวลาที่ต้องการติดตามร่องรอยการตรวจสอบ

ค. การสำรองข้อมูล / การจัดเก็บข้อมูล

1. พิจารณาว่าผู้บริหารได้ดำเนินการให้มีกระบวนการติดตามและควบคุมการสำรองข้อมูล

2. ถ้า สง. มีการใช้เครื่องมือ/วิธีการสำรองข้อมูลที่ทันสมัย เช่น storage area network (SAN) หรือ network-attached storage (NAS) โดย

- พิจารณาว่าผู้บริหารได้จัดทำบันทึกเกี่ยวกับการวิเคราะห์ต้นทุนค่าใช้จ่ายของเครื่องมือดังกล่าวไว้อย่างเหมาะสม และแสดงให้เห็นถึงเหตุผลของการเลือกใช้เครื่องมือดังกล่าว
- สอบทานว่าได้มีการนำเครื่องมือหรืออุปกรณ์สำรองข้อมูลดังกล่าวมาใช้กับระบบงานสำคัญอย่างเหมาะสมและมีประสิทธิผล
- สอบทานว่า Administrator ด้านการสำรองข้อมูล ได้บริหารจัดการอุปกรณ์สำรองข้อมูลในลักษณะเป็นแต่ละระบบงาน เพื่อให้การดูแลติดตามและแก้ไขปัญหาที่เกี่ยวกับการสำรองข้อมูลสามารถจัดการได้เป็นแต่ละประเด็นเฉพาะตัวของแต่ละสายงานธุรกิจ

3. ถ้ามีการใช้ระบบบริหารจัดการเทป ให้สอบทานว่าผู้ที่มีสิทธิเหนือการควบคุมมีเฉพาะเจ้าหน้าที่ที่มีหน้าที่ความรับผิดชอบที่เหมาะสมหรือไม่

4. สอบทานการบริหารจัดการที่ศูนย์จัดเก็บข้อมูลสำรองว่ามีเพียงพอหรือไม่ โดยดูจาก

- คู่มือกระบวนการปฏิบัติงาน
- บันทึกการปฏิบัติงานของเจ้าหน้าที่ประจำแต่ละผลัด และ logs
- ชีทสำหรับเจ้าหน้าที่แต่ละผลัดที่ใช้เป็นคู่มือในการปฏิบัติงานประมวลผล

ง. การควบคุมและการติดตามดูแลสภาพแวดล้อม

1. ประเมินว่าความสามารถในการควบคุมและการติดตามดูแลสภาพแวดล้อมด้านเทคโนโลยีที่มี ข้อตรวจพบที่ควรติดตามนั้น มีการควบคุมที่สามารถจะป้องกันปัญหาและตรวจจับสิ่งที่จะทำให้การปฏิบัติงานหยุดชะงักได้หรือไม่

-ระบบไฟฟ้าสำรองที่เพียงพอ (เช่น UPS , เครื่องผลิตกระแสไฟฟ้า (generator))

- ระบบโทรคมนาคมสำรองที่เพียงพอ

- ระบบปรับอากาศ อุณหภูมิที่เหมาะสมและสามารถใช้กับแหล่งพลังงานสำรองได้

- การควบคุมป้องกันสายเคเบิ้ลรวมทั้งจัดระบบและทำป้ายติดสายเคเบิ้ลให้เรียบร้อย

- ระบบตรวจจับควันและระบบระงับอัคคีภัยที่เพียงพอในการป้องกันความเสียหายต่ออุปกรณ์คอมพิวเตอร์และมีการดูแลให้สามารถใช้งานได้

- จัดให้มีระบบที่เหมาะสมในการตรวจจับการรั่วไหลของน้ำก่อนที่อุปกรณ์คอมพิวเตอร์จะได้รับความเสียหาย

- การจัดการและการปฏิบัติงานในการดูแลบำรุงรักษาที่ปลอดภัยและน่าเชื่อถือว่าจะช่วยป้องกันหรือช่วยลดการหยุดชะงักของสภาพแวดล้อมการปฏิบัติงานได้

- การอบรมพนักงานให้สามารถใช้งานระบบการควบคุมและติดตามดูแลได้อย่างเหมาะสม

จ. การรักษาความปลอดภัยทางกายภาพ

1. สอบทานและประเมินว่าวิธีการรักษาความปลอดภัยที่มีข้อตรวจพบที่ควรติดตามนั้น มีการรักษาความปลอดภัยที่น่าเชื่อถือได้และเพียงพอที่จะป้องกันความเสียหายต่อทรัพยากรบุคคล ทรัพย์สินที่จับต้องได้และทรัพย์สินด้านสารสนเทศ โดยพิจารณาว่า

- ศูนย์ปฏิบัติการตั้งอยู่ในสถานที่ที่ปลอดภัยและมีการจำกัดจำนวนของหน้าต่างและจุดที่จะสามารถเข้าถึงได้จากภายนอก

- มีการแบ่งโซนและจัดแบ่งระดับของวิธีการรักษาตามความสำคัญ

- ผู้บริหารให้การอบรมพนักงานในเรื่องที่เกี่ยวกับนโยบายและแนวทางการรักษาความปลอดภัย

- การรักษาความปลอดภัยบริเวณรอบนอก เช่น การติดตั้งไฟภายนอกศูนย์ ประตูรั้ว รั้ว กล้องวีดีโอ

- ประตูหรือทางเข้าต่าง ๆ มีการรักษาความปลอดภัยด้วยกุญแจที่เป็นอิเล็กทรอนิกส์

- เจ้าหน้าที่รักษาความปลอดภัยทั้งที่มีอาวุธและไม่มีอาวุธ ควรได้รับการอบรมอย่างเหมาะสมและมีใบอนุญาตในการทำงาน รวมทั้งการสืบสวนประวัติของเจ้าหน้าที่ดังกล่าว

- มีการควบคุมการเข้าถึงทางด้านกายภาพที่ควบคุมให้พนักงานที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าไปปฏิบัติงานตามหน้าที่รับผิดชอบได้

- ผู้บริหารต้องจัดให้มีบัตรประจำตัวพนักงานที่มีรูปถ่ายเพื่อการผ่านเข้าไปบริเวณที่ต้องควบคุม ดังนั้นให้สอบทานว่ามีเครื่องมืออิเล็กทรอนิกส์ที่ควบคุมการเข้าถึงที่ทันสมัยใช้อยู่หรือไม่

- ผู้บริหารต้องควบคุมดูแล 'บุคคลภายนอก' ที่เข้ามาภายในศูนย์ปฏิบัติการโดยใช้บัตรผู้เข้าเยี่ยมชม (visitor) โดยควรติดตามดูแลบุคคลภายนอกนั้นตลอดเวลาที่อยู่ภายในศูนย์ปฏิบัติการ

- ประตู หน้าต่าง และทางผ่านเข้าออกอื่น ๆ ควรจะมีเครื่องมือที่คอยส่งเสียงเตือนเมื่อมีผู้ผ่านเข้าออก เพื่อจะได้สังเกตว่าผู้ที่ผ่านเข้าออกเป็นผู้ที่เหมาะสมหรือไม่ และอาจใช้กล้องวีดีโอบันทึกภาพผู้ผ่านเข้าออกไว้ด้วย

- แนวทางที่เป็นลายลักษณ์อักษรที่ใช้เพื่อการอนุมัติและการบันทึก log ของการรับหรือการขนย้ายออกของอุปกรณ์จากศูนย์ปฏิบัติการว่ามีความเหมาะสมหรือไม่

- เอกสารที่เป็นความลับจะต้องถูกย่อยก่อนที่จะทิ้ง

- แนวทางที่เป็นลายลักษณ์อักษรที่ใช้เพื่อป้องกันข้อมูลสารสนเทศจากการถูกลบอย่างเหมาะสม

ฉ. การบริหารจัดการต่อเหตุการณ์ต่าง ๆ

1. สอบทานว่ามีการจัดทำเอกสารที่เหมาะสมที่จะใช้ในการสนับสนุนการบริหารจัดการต่อเหตุการณ์ต่าง ๆ ให้มีความมั่นคงปลอดภัย เช่น

- มี logs ที่บันทึกการจัดการเหตุการณ์ต่าง ๆและการแก้ไขปัญหา

- มี logs ที่จะแสดงให้เห็นว่าเจ้าหน้าที่ได้ปฏิบัติตามคู่มือ/แนวทางการปฏิบัติงาน

- การแจ้ง/ประกาศการแก้ไขปัญหาให้แก่ส่วนงานอื่นทราบ

- ประวัติการอบรมที่แสดงให้เห็นว่าเจ้าหน้าที่ด้านปฏิบัติการได้รับการอบรมในเรื่องต่าง ๆเหล่านี้จนสามารถปฏิบัติงานได้อย่างคล่องแคล่ว

- แนวทางการปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

- แนวทางการปฏิบัติในเหตุการณ์ที่เกี่ยวกับการรักษาความปลอดภัย

- แนวทางการแก้ไขกิจกรรมที่ผิดปกติ

- บันทึกประวัติของ
- การปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง
- การปฏิบัติในเหตุการณ์ที่เกี่ยวกับการรักษาความปลอดภัย
- การแก้ไขปัญหา/ตอบโต้เหตุการณ์ที่ผิดปกติ

2. สอบทานว่าคู่มือแผนฉุกเฉินที่ประกาศใช้ได้กล่าวถึง

- การอพยพพนักงาน
- การปิดระบบยูทิลิตี้ต่าง ๆ
- การปิดเครื่อง / อุปกรณ์ต่าง ๆ
- การเปิด/ปิด อุปกรณ์ระบบระงับอัคคีภัย
- การรักษาความปลอดภัยทรัพย์สินมีค่า

3. สอบทานว่าคู่มือแผนฉุกเฉินได้ถูกประกาศใช้ทั่วทั้งองค์กร

4. ประเมินว่าผู้ปฏิบัติงานได้รับการอบรมเกี่ยวกับการปฏิบัติตามแผนฉุกเฉินที่ประกาศใช้อย่างเพียงพอ และผู้ปฏิบัติงานมีความคุ้นเคยในหน้าที่และความรับผิดชอบของตนเองในกรณีที่เกิดเหตุฉุกเฉิน

5. สอบทานว่า สง. มีการทดสอบแผนฉุกเฉิน

ช. การให้บริการสนับสนุน/กระบวนการแก้ไขปัญหาของผู้ใช้งาน (Help Desk/User Support Processes)

1. ประเมินว่าระบบสารสนเทศเพื่อการบริหาร (MIS) เหมาะสมกับขนาดและความซับซ้อนของสถาบันการเงิน

- พิจารณาประสิทธิภาพของระบบ MIS ในการใช้บริหารติดตามในเรื่องที่เกี่ยวกับ Help desk เช่น ปริมาณและแนวโน้มของตัววัดที่สำคัญต่าง ๆ ข้อตกลงในการให้บริการ (SLAs) ที่ไม่สามารถทำได้ตามที่ตกลงกันไว้ การวิเคราะห์ผลกระทบ การวิเคราะห์หาสาเหตุของปัญหา และแผนการดำเนินการแก้ไขสำหรับประเด็นที่ยังไม่ได้รับการแก้ไข
- พิจารณาว่าแผนการดำเนินการมีการระบุถึงผู้รับผิดชอบ กรอบระยะเวลาดำเนินการในการแก้ไขปัญหา

2. ประเมินว่าเทคโนโลยีที่ใช้ในการบริหารจัดการการปฏิบัติงานให้บริการสนับสนุน/แก้ไขปัญหาของผู้ใช้งาน (Help desk operations) เหมาะสมกับขนาดและความซับซ้อนของการปฏิบัติงาน โดยพิจารณาในประเด็นเหล่านี้

- สิทธิการเข้าถึงระบบต่าง ๆ ของ Help desk

- การบันทึกปัญหาและการติดตามปัญหา

- การบันทึกปัญหาแบบอัตโนมัติ และกระบวนการติดตามสำหรับปัญหาที่ไม่สามารถแก้ไขได้ทันที

- การแจ้งเตือนโดยอัตโนมัติเมื่อมีปัญหาที่อยู่ในระดับอันตรายที่ไม่สามารถแก้ไขได้ตามเวลาที่กำหนดใน SLA หรือประสิทธิภาพของกระบวนการติดตามปัญหาที่ทำโดย manual

3. ประเมินว่าวิธีการพิสูจน์ตัวตนของผู้ใช้งานมีความเหมาะสมกับระดับของความเสี่ยงและประเภทของการควบคุมวิธีการพิสูจน์ตัวตนที่ help desk ใช้พิสูจน์ตัวตนของผู้ใช้งานนั้นเหมาะสมกับกิจกรรมที่ถูกดำเนินการ

4. ประเมินคุณภาพของระบบ MIS ที่ใช้ในการบริหารการปฏิบัติงาน help desk ว่าเหมาะสมกับขนาดและความซับซ้อนของสถาบันการเงิน พิจารณาตัววัด
ต่าง ๆ ที่ต้องการเพื่อใช้ติดตามปริมาณและแนวโน้มของปัญหา การกำกับดูแลให้เป็นไปตาม SLA ที่กำหนดไว้ อัตราความพึงพอใจของผู้ใช้

5. ประเมินว่ามีการใช้แนวทางการประเมินความเสี่ยงในการจัดลำดับประเด็นปัญหาหรือไม่ และมีวิธีการกำหนดนิยามของปัญหาที่มีความรุนแรงอย่างไร และมีวิธีการจัดลำดับความสำคัญของปัญหาที่ได้รับจาก Call Center อย่างไร

6. ประเมินว่าผู้บริหารได้มีการนำข้อมูลสารสนเทศจากหน่วยงาน help desk ไปใช้พัฒนาการปฏิบัติงานด้านเทคโนโลยีในภาพรวมอย่างไร

- พิจารณาว่าผู้บริหารมีเครื่องมือและกระบวนการที่มีประสิทธิภาพในการะบุประเด็นที่เป็นความเสี่ยงสูงหรือประเด็นที่อาจก่อให้เกิดผลกระทบต่อเนื่องต่อระบบงานอื่น ๆ ที่เกี่ยวข้อง

- พิจารณาในประเด็นที่ถูกระบุว่าเป็นความเสี่ยงสูงหรือประเด็นที่อาจก่อให้เกิดผลกระทบต่อเนื่องต่อระบบงานอื่น ๆ ที่เกี่ยวข้องนั้นมีกระบวนการจัดการที่มีประสิทธิภาพหรือไม่ ซึ่งกระบวนการจัดการที่มีประสิทธิภาพในที่นี้หมายถึง การวิเคราะห์หาสาเหตุของปัญหา การวิเคราะห์หาผลกระทบ แผนการดำเนินการที่มีประสิทธิภาพ และกระบวนการติดตาม

ซ. การควบคุมการปฏิบัติงานที่เกี่ยวกับรายการธุรกรรม (Item Processing)

1. พิจารณาว่ามีการควบคุมที่เพียงพอโดยรอบบริเวณจุดเริ่มต้นของรายการและจุดนำเข้าข้อมูล เช่น

- มีการสอบทานบันทึกประจำวันโดยเจ้าหน้าที่ระดับหัวหน้างานและมีการลงนามว่าได้ทำการสอบทานแล้ว

- การควบคุมต่อผลลัพธ์จากคอมพิวเตอร์ เช่น รายงานที่พิมพ์ออกมา แผ่นฟิล์ม และ optical disk เป็นต้น

- การแบ่งแยกหน้าที่

- การจำกัดการทำงานของอุปกรณ์ส่วนบุคคล สำหรับผู้ที่ไม่มีหน้าที่เกี่ยวข้อง

- สอบทานการกระทบยอดรวมของรายการทางการเงิน

- วิเคราะห์รายการที่พิสูจน์ยอดแล้วไม่ลงตัวเพื่อพิจารณาว่ามีผู้ระบุความแตกต่างและปรับปรุงแก้ไขรายการ รวมทั้งจัดเก็บเอกสารการปรับปรุงแก้ไขรายการเหล่านั้นในรูปของแบบฟอร์ม proof department correction และพิจารณาว่ามีการอนุมัติแบบฟอร์มดังกล่าวโดยพนักงานระดับหัวหน้างานหรือไม่

- การสอบทานการจัดการประจำวันโดยพนักงานระดับหัวหน้าผลัดด้วยการสอบทานรายงานการปฏิบัติงาน

2. พิจารณาว่าการควบคุมโดยรอบบริเวณหน่วยงานเคลียริ่งว่ามีความเพียงพอเหมาะสม เช่น

- การอนุมัติรายการที่บันทึกในบัญชีแยกประเภทโดยหัวหน้างานหรือหัวหน้าเสมียน

- การวิเคราะห์และการแก้ไขรายการที่ถูกปฏิเสธ

- การบันทึกรายการพักชั่วคราว (suspense items) ที่ส่งไปให้ สถาบันการเงินเป็นเจ้าของรายการแก้ไข

- การอนุมัติรายการพักชั่วคราว (suspense items) โดยหัวหน้างาน

- การส่งไฟล์รายการภายในเวลาที่เหมาะสม

3. พิจารณาความเพียงพอในการควบคุมสำหรับการทำรายการพิเศษที่ได้รับการยกเว้นจากกระบวนการปกติ (exception processing) เช่น มีการสอบทานรายงานการทำรายการพิเศษที่ได้รับการยกเว้นจากกระบวนการปกติอย่างสม่ำเสมอ และมีเอกสารรองรับการทำรายการดังกล่าวอย่างเหมาะสม

4. พิจารณาความเพียงพอในการควบคุมการจัดทำ Statement เช่น การบันทึกและสอบสวนรายการที่ไม่ตรงหรือมีผู้โต้แย้ง ที่ยังไม่สามารถแก้ไขได้

ฌ. ระบบการทำสำเนาภาพเอกสาร (Imaging Systems)

1. สอบทานและประเมินระบบสำเนาภาพเอกสาร โดยพิจารณา

- การเชื่อมต่อระหว่างระบบการทำสำเนาภาพเอกสารกับเครื่องประมวลผลหลัก
- กำลังความสามารถของระบบทำสำเนาภาพเอกสารในปัจจุบันและการขยายกำลังความสามารถของระบบในอนาคต
- ระบบคอมพิวเตอร์ที่ใช้เป็นระดับ mainframe Midrange หรือ คอมพิวเตอร์ส่วนบุคคล
- ผู้จำหน่ายสินค้าหรือบริการ
- มาตรฐานของการทำสำเนาภาพเอกสารที่ใช้
- กระบวนการแปลงสภาพเอกสาร

2. สอบทานและประเมินกระบวนการสำรองข้อมูลและระบบงาน และกระบวนการกู้ระบบ

3. สอบทานและประเมินกระบวนการที่ใช้กู้สำเนาภาพเอกสารที่ไม่ชัดเจน เช่น ใช้วิธีการสแกนซ้ำใหม่ทั้งหมด หรือสแกนใหม่เฉพาะหน้าที่เสีย

4. สอบทานและประเมินกระบวนการและการควบคุมที่เกี่ยวข้องกับการจัดทำดัชนี (indexing) ของเอกสาร การทำงานของระบบจัดทำดัชนีเป็นอย่างไรระหว่าง ระบบจะทำดัชนี (index) ของเอกสารหลังจากสแกนเสร็จแต่ละแผ่น หรือระบบจะทำดัชนีหลังจากสแกนเอกสารได้ครบทั้งหมดแล้ว

5. สอบทานและประเมินว่า hardware และ softwareของระบบสำเนาภาพเอกสารสามารถแลกเปลี่ยนกันได้ระหว่างผู้ให้บริการรายอื่น ๆ ได้หรือไม่ ถ้าสามารถแลกเปลี่ยนกันได้ ผู้บริหารได้จัดให้มีการใช้กระบวนการปกติเมื่อจะมีการเปลี่ยนหรือซ่อมหรือไม่ ถ้าไม่สามารถแลกเปลี่ยนได้ผู้บริหารได้กำหนดช่องทางเลือกอื่นสำหรับเมื่อระบบสำเนาภาพเอกสารที่ใช้งานอยู่ในปัจจุบันไม่สามารถทำงานได้ไว้อย่างไร

6. สอบทานและประเมินอายุการจัดเก็บเอกสารต้นฉบับ ประเมินว่าอายุการจัดเก็บดังกล่าวเป็นไปตามข้อกำหนดของกฎหมายของประเทศหรือไม่ ผู้บริหารมีการปรึกษากับทนายความหรือที่ปรึกษากฎหมายเกี่ยวกับข้อกำหนดกฎหมายในเรื่องที่เกี่ยวกับการทำลายเอกสารต้นฉบับหรือไม่

7. สอบทานและประเมินการควบคุมความปลอดภัยเกี่ยวกับสิทธิการเข้าถึงในเรื่องดังต่อไปนี้

- สิทธิของผู้ที่เป็นผู้บริหารความปลอดภัยข้อมูล (Data security administrator)
- การควบคุมดูแลไฟล์อิเล็กทรอนิกส์ของสำเนาภาพเอกสาร (electronic image files)
- การควบคุมการจัดทำดัชนีของสำเนาภาพเอกสารเพื่อป้องกันการเขียนทับ การควบคุมการแก้ไขสำเนาภาพเอกสาร หรือ การควบคุมการแทรกสำเนาภาพเอกสารเพื่อการทุจริต
- การควบคุมดูแลเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับไฟล์ดัชนี
- การเข้ารหัสไฟล์ของสำเนาภาพเอกสารที่เก็บอยู่บนดิสก์ของระบบงานจริง (Production) และที่อยู่ในสื่อสำรองข้อมูล

ภาคผนวก : อภิธานศัพท์ (Glossary)

Application	โปรแกรมประยุกต์ ซึ่งโปรแกรมประยุกต์เป็นโปรแกรมที่ได้รับการออกแบบให้ทำงานด้วยหน้าที่ที่เจาะจงโดยตรงสำหรับผู้ใช้ หรือในบางกรณี สำหรับโปรแกรมประยุกต์อื่น ๆ ตัวอย่าง ของโปรแกรมประยุกต์ เช่น โปรแกรมประมวลผลคำ (word processing เช่น MS Word) โปรแกรมเงินเดือน เป็นต้น
ATM (Asynchronous transfer mode)	เป็นเทคโนโลยีระบบเครือข่ายความเร็วสูงที่ใช้สำหรับส่งข้อมูลได้หลากหลายรูปแบบ เช่น การประชุมผ่าน Video Conference การแสดงมัลติมีเดีย ทั้งข้อมูล เสียง ภาพ และภาพเคลื่อนไหว (VDO) โดยข้อมูลจะถูกแปลงให้มีขนาดคงที่และเล็กลงเหลือเพียง 53 ไบต์ ทำให้ไม่เสียเวลาในการจัดการข้อมูล ซึ่งจะเหมาะกับการส่งข้อมูลแบบ Real Time
Bandwidth	bandwidth ของการส่งผ่านสัญญาณสื่อสารเป็นการวัดช่วงความถี่ ที่สัญญาณใช้งาน คำนี้สามารถใช้อ้างถึงคุณลักษณะการตอบสนองความถี่ ของระบบรับการสื่อสาร ของสัญญาณทุกประเภท คือ ทั้งแบบอะนาล็อก และ ดิจิตอล ในความหมายทั่วไป bandwidth เป็นสัดส่วนโดยตรงของจำนวนข้อมูลทั้งหมดที่ส่งผ่าน หรือรับต่อหน่วยเวลา ในระบบดิจิตอล bandwidth คือความเร็วข้อมูลเป็น bits per second (จำนวนบิตต่อวินาที) ดังนั้นโมเด็มซึ่งทำงานที่ 57,600 bps จะมี bandwidth เป็น 2 เท่าของ โมเด็ม ซึ่งทำงานที่ 28,800 bps ในระบบอะนาล็อก ความหมายของ bandwidth หมายถึงความแตกต่างระหว่างความถี่สูงสุดและต่ำสุดของสัญญาณ มีหน่วยวัดเป็น hertz สัญญาณเสียงมี bandwidth ประมาณ 33 kilohertz(33 KHz) และการกระจายภาพของโทรทัศน์แบบอะนาล็อก ใช้สัญญาณวิดีโอ ซึ่งมี bandwidth ประมาณ 6 megahertz (6 MHz)

BPS (Bits per second)	การวัดความเร็วข้อมูลที่วิ่งผ่านจากจุดหนึ่งไปยังอีกจุดหนึ่ง เช่น โมเด็ม 28.8 สามารถส่งข้อมูลที่ 28,800 bits per second
Change management	เป็นกระบวนการในการบริหารจัดการเกี่ยวกับการเปลี่ยนแปลงต่าง ๆ ทั่วทั้งองค์กร ซึ่งกระบวนการ Change management นี้ต้องประกอบด้วย การวางแผน การกำกับดูแล การบริหารโครงการ การทดสอบ และการนำไปใช้งาน
Clustering	ระบบคลัสเตอร์ หรือคลัสเตอริ่ง หมายถึงการเชื่อมระบบการทำงานของเซิร์ฟเวอร์เข้าด้วยกันให้ทำงานเสมือนเป็นเครื่อง ๆ เดียวกัน เพื่อเพิ่มกำลังและความสามารถในการประมวลผล ซึ่งอาจเทียบเท่าระดับซูเปอร์คอมพิวเตอร์หรือสูงกว่าก็ได้ สำหรับการประมวลผลงานที่มีความซับซ้อน โดยเฉพาะงานด้านวิทยาศาสตร์ ข้อดีคือประหยัดค่าใช้จ่าย คือถูกกว่าเครื่องซูเปอร์คอมพิวเตอร์จริงๆ แต่ข้อเสียคือยุ่งยาก
COTS (Commercial off-the-shelf)	เป็นผลิตภัณฑ์ทั้งด้าน software หรือ hardwareที่สำเร็จรูปผลิตขึ้นมาให้พร้อมใช้งานได้ทันทีไม่ต้องทำการปรับปรุงแก้ไข มีวางจำหน่ายโดยทั่วไป ซึ่งรู้จักในอีกชื่อหนึ่งว่า “shrink-wrap” applications
DASD (Direct access storage device)	อุปกรณ์เก็บข้อมูลในรูปแบบของ magnetic ซึ่งเดิมมักใช้กับเครื่อง mainframe แต่ปัจจุบันยังหมายถึง ฮาร์ดดิสก์ในเครื่องคอมพิวเตอร์ส่วนบุคคลด้วย
DSL (Digital subscriber line)	สายสื่อสารที่เป็นระบบดิจิตอลซึ่งมีความเร็วในการส่งข้อมูลสูง สามารถใช้ได้ทั้งกับผู้ใช้ตามบ้านและธุรกิจ
Encryption	เป็นวิธีที่ใช้ป้องกันการจารกรรม โดยก่อนส่งข้อมูลไปตามสายสื่อสาร ผู้ส่งข้อมูลจะแปลงข้อมูล (Encrypt) โดยใช้ข้อมูลฐาน (seed base), รหัสลับ (encrypt key) เพื่อแปลงเป็นข้อมูลอื่น ด้วยสูตรทางคณิตศาสตร์ และทางตรรกที่ซับซ้อนและไม่สื่อความหมาย เพื่อให้ยากต่อการแปลงกลับเป็นข้อมูลเดิม
Frame Relay	โปรโตคอล WAN ที่มีประสิทธิภาพสูงซึ่งปฏิบัติงานใน physical และ data link layers ของมาตรฐาน OSI (Open Systems Interconnect

	model) Frame relay เป็นตัวอย่างของเทคโนโลยี packet-switched ซึ่งช่วยให้สามารถใช้สายสื่อสาร หรือ bandwidth ร่วมกันได้
Hub	อุปกรณ์สื่อสารที่ช่วยส่งผ่านข้อมูลทั้งหมด ทั้งไปและกลับระหว่าง LAN ทั้งสองจุดที่ hub เชื่อมต่ออยู่
HVAC	Heating, ventilation and air conditioning คือ อุณหภูมิความร้อน การระบายอากาศ และระบบปรับอากาศ
I/O	Input/Output ข้อมูลนำเข้า/ผลลัพท์
ISDN (Integrated systems digital networking)	การจัดระบบตามลำดับขั้นของระบบการสื่อสารและส่งผ่านแบบดิจิตอล ที่สามารถส่งได้ทั้งเสียง ข้อมูล และภาพที่อยู่รวมเป็นหน่วยเดียวกัน ISDN คือ การสื่อสารองค์ประกอบที่เป็นดิจิตอลต่าง ๆ ที่กล่าวไปข้างต้นในเวลาเดียวกันภายใต้โปรโตคอลและความเร็วที่เท่ากัน
Mainframe	คอมพิวเตอร์ขนาดใหญ่ ใช้สำหรับการประมวลผลโปรแกรมของธุรกิจที่มีธุรกรรมจำนวนมาก มักเป็นการประมวลผลในลักษณะรวมศูนย์ (Centralized computing) มากกว่าแบบกระจายศูนย์ (Distributed computing)
Media	สื่อที่ใช้ในการเก็บข้อมูลสารสนเทศ หมายรวมถึง กระดาษ ดิสก์ เทป และ ออฟติคอลดิสก์
MICR : Magnetic Ink Character Recognition	คือ รหัสแม่เหล็กในรูปแบบของตัวเลข 0-9 และเครื่องหมายจำนวน 4 ตัวที่ออกแบบโดยมีวัตถุประสงค์เบื้องต้นในการพิมพ์บนเช็คเพื่อให้เครื่องอ่านเช็คอ่านค่าที่พิมพ์และนำไปประมวลผลได้ MICR ชุดที่ใช้กันทั่วไปในปัจจุบันคือแบบ E13B ออกแบบโดยสถาบันวิจัยแสตนฟอร์ด หลักการทำงานของระบบ MICR คือเครื่องอ่านเช็คจะทำให้ตัวพิมพ์ E13B บนเช็คเป็นแม่เหล็ก สนามแม่เหล็กที่เกิดจากตัวอักษรจะกำเนิดกระแสไฟฟ้าในหัวอ่าน ความแตกต่างของกำลังแม่เหล็กแต่ละส่วนและระยะเวลาจะเป็นตัวบอกว่าตัวอักษรที่อ่านเป็นตัวใด

Midrange	คอมพิวเตอร์ที่มีประสิทธิภาพและความสามารถสูงกว่าเครื่องคอมพิวเตอร์ส่วนบุคคล แต่น้อยกว่าเครื่องคอมพิวเตอร์ mainframe
MIPS	Millions of instructions per second เป็นมาตรวัดโดยทั่วไปเพื่อใช้วัดกำลังความสามารถของเครื่องคอมพิวเตอร์ และมีความหมายโดยนัยถึงปริมาณของงานที่คอมพิวเตอร์สามารถทำงานได้
Mirroring	กระบวนการสำเนาข้อมูลไปเก็บไว้ในหลาย ๆ ดิสก์โดยผ่านทางระบบเครือข่ายสื่อสารในลักษณะทันทีทันใด (real time) หรือเกือบจะทันที (close to real time) Mirroring ช่วยให้เกิดความพร้อมใช้งานต่อเวบไซต์ หรือไฟล์
MIS (Management information systems)	ระบบสารสนเทศเพื่อการจัดการ เป็นระบบคอมพิวเตอร์ที่ใช้สำหรับให้บริการสารสนเทศเพื่อการดำเนินธุรกิจของทั้งองค์กร
NAS (Network attached storage)	ที่บรรจุฮาร์ดดิสก์ซึ่งจัดเตรียม network address ของตนเองมากกว่าที่จะยึดติดกับ the department computer ที่ให้บริการเกี่ยวกับ applications ต่อเครื่องคอมพิวเตอร์ต่าง ๆ ของผู้ใช้งานบนเครือข่าย อุปกรณ์ NAS นี้จะต่ออยู่กับ LAN (เช่น เครือข่าย Ethernet) และจะช่วยกำหนด IP address ให้ การเรียกขอไฟล์จะถูกจับคู่ระหว่าง main server กับ NAS file server
Operating system	โปรแกรมระบบปฏิบัติการ เป็นโปรแกรมซึ่งจัดการฟังก์ชันและโปรแกรมการทำงานเบื้องต้นทั้งหมดของคอมพิวเตอร์
Packet	แพ็คเกต เป็นหน่วยของข้อมูลที่ส่งระหว่างจุดเริ่มต้นกับปลายทางบนอินเตอร์เน็ต หรือเครือข่าย packet – switched แบบอื่นๆ เมื่อไฟล์ต่างๆ จะได้รับการส่งจากที่หนึ่งไปยังอีกที่บนอินเตอร์เน็ต เลเยอร์ของ Transmission Control Protocol (TCP) จะแบ่งไฟล์เป็นชิ้นที่มีขนาดเหมาะสมในการส่ง แต่ละแพ็กเกตจะแยกหมายเลข และรวม Internet address ปลายทาง แพ็คเกตทั้งหมดไฟล์อาจเดินทาง ด้วยเส้นทางที่ต่างกันบนอินเตอร์เน็ต เมื่อแพ็คเกตมาถึงทั้งหมด จะมีการประกอบใหม่เป็นไฟล์เดิม

PBX (Private branch exchange)	ระบบโทรศัพท์ภายในองค์กรซึ่งช่วยในการสลับสายโทรศัพท์ของผู้ใช้ในองค์กรภายใต้สายโทรศัพท์ภายในขององค์กร เพื่อให้ผู้ใช้งานทุกคนสามารถใช้สายร่วมกันได้
Platform	ระบบคอมพิวเตอร์ที่เป็นพื้นฐานให้ระบบงานประยุกต์ (applications programs) ประมวลผลอยู่ ซึ่ง Platform ประกอบด้วย โปรแกรมระบบปฏิบัติการ (Operating system) และโปรแกรมที่ช่วยในการประสานงานอื่น ๆ
Protocol	โปรโตคอล เป็นวิธีการส่งข้อมูลผ่านเครือข่ายสื่อสารระหว่างเครื่องคอมพิวเตอร์
RAID (Redundant array of independent 1disks)	เป็นการใช้ฮาร์ดิสก์หลาย ๆ ลูกเพื่อเก็บข้อมูลที่เหมือน ๆ กันในหลาย ๆ ที่
Recovery site	ศูนย์คอมพิวเตอร์สำรอง ซึ่งใช้ประมวลผลระบบงานคอมพิวเตอร์ในกรณีที่เกิดเหตุการณ์ฉุกเฉิน โดยมักจะแบ่งเป็น - Hot sites เป็นศูนย์ที่มีอุปกรณ์คอมพิวเตอร์ครบถ้วน - Warm sites เป็นศูนย์ที่มีอุปกรณ์บางส่วนแต่ไม่ครบ - Cold sites เป็นศูนย์ที่มีแต่ห้องเปล่า ๆ ไม่มีอุปกรณ์คอมพิวเตอร์
Routing	เป็นกระบวนการเคลื่อนย้ายสารสนเทศจากต้นทางไปยังปลายทาง
SAN (Storage area network)	ระบบเครือข่ายความเร็วสูงที่ใช้เพื่อการเฉพาะ โดยใช้เชื่อมต่ออุปกรณ์จัดเก็บข้อมูลประเภทต่าง ๆ กับ data servers
Scalability	การวัดว่าระบบ hardware และ softwareสามารถปรับตัวให้เข้ากับความต้องการที่เพิ่มขึ้น
SCSI (Small computer systems interface)	เรียกว่า “ สกัซซี่ (skuzzy)” เป็นวิธีการมาตรฐานของการเชื่อมต่อคอมพิวเตอร์กับดิสก์ไดร์ฟ เทปไดร์ฟ และอุปกรณ์อื่น ๆ ซึ่งต้องการการส่งข้อมูลแบบความเร็วสูง
SDLC (Systems development life cycle)	ขั้นตอนในการพัฒนาระบบงานคอมพิวเตอร์ที่เป็นมาตรฐาน

Server	เครื่องคอมพิวเตอร์หรืออุปกรณ์อื่น ๆ ที่จัดการเกี่ยวกับบริการเครือข่าย เช่น print server เป็นอุปกรณ์ที่จัดการเกี่ยวกับเครือข่ายการพิมพ์
SLA (Service level agreement)	ข้อตกลงในการให้บริการระหว่างผู้ใช้งานและผู้ให้บริการด้านเทคโนโลยีสารสนเทศซึ่งมีการตกลงเรื่องการคิดค่าปรับหรือการลงโทษ หากทำไม่ได้ตามข้อตกลง
SONET (Synchronous optical network)	มาตรฐานที่กำหนดมาตรฐานในการเชื่อมต่อสำหรับระบบการส่งผ่านข้อมูลด้วย fiber-optic
Storage virtualization	กระบวนการที่นำเอาอุปกรณ์จัดเก็บข้อมูลที่แตกต่างกันหลาย ๆ ตัวมาเชื่อมต่อกันทางเครือข่ายเพื่อให้มองเห็นเสมือนเป็นเครื่องเดียวกัน
Switch	อุปกรณ์ที่เชื่อมต่อวง LAN มากกว่า 2 วงขึ้นไปโดยใช้โปรโตคอล data link และโปรโตคอล network
T-1 line	เป็นสายโทรศัพท์ชนิดพิเศษที่ใช้สำหรับการสื่อสารและส่งผ่านข้อมูลในรูปแบบดิจิตอล ด้วยอัตราความเร็ว 1.544 Mbps (1,544,000 bits per second) ซึ่งมักจะเป็นสายไฟเบอร์ออฟติก
TCO (Total cost of ownership)	ค่าใช้จ่ายที่เกิดขึ้นจริงของการถือครองเครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีอื่น ๆ ซึ่งประกอบด้วย - ต้นทุนค่าใช้จ่ายเริ่มแรกของคอมพิวเตอร์และ software - ค่าใช้จ่ายในการปรับปรุง(upgrades) hardwareและ software - ค่าบำรุงรักษา - ค่าใช้จ่ายเกี่ยวกับการได้รับความช่วยเหลือทางเทคนิค (Technical support) - ค่าใช้จ่ายในการอบรม
TCP/IP (Transmission control protocol / Internet protocol)	มาตรฐานการสื่อสารที่ใช้ส่งผ่านข้อมูลในรูปแบบ packets จากคอมพิวเตอร์เครื่องหนึ่งไปยังคอมพิวเตอร์อีกเครื่องหนึ่ง
UPS (Uninterruptible power supply)	อุปกรณ์ที่ช่วยให้คอมพิวเตอร์ยังทำงานต่อไปได้เมื่อขาดกระแสไฟฟ้าจากแหล่งพลังงานไฟฟ้าหลัก และ UPS จะช่วยในการป้องกันคอมพิวเตอร์ต่อกรณีของกระแสไฟฟ้าที่กระชากขึ้น ๆ ลง ๆ สูง ๆ ต่ำ ๆ ด้วย

VESDA (Very early smoke detection alert)	ระบบสุ่มตรวจอากาศอย่างต่อเนื่องและมีความว่องไวในการตรวจจับ โดยสามารถตรวจเพลิงไหม้ได้ตั้งแต่ที่ขั้นก่อนการเผาไหม้ ตั้งแต่เริ่มมีควันแต่ยังไม่มีเปลวไฟจึงสามารถที่จะเตือนได้ก่อนที่จะเกิดเพลิงไหม้
VOIP (Voice over Internet protocol)	ระบบโทรศัพท์แบบใช้เทคโนโลยี Internet Protocol
Workstation	คอมพิวเตอร์ที่เชื่อมต่อกับวง LAN (Local-area network)
WORM (Write once, read many times)	ออฟติคอลดิสก์ชนิดหนึ่งซึ่งคอมพิวเตอร์สามารถเก็บข้อมูลเข้าไปได้เพียงครั้งเดียวและไม่สามารถเปลี่ยนแปลงหรือเขียนทับอีกได้ แต่อ่านได้หลายครั้ง