คู่มือตรวจสอบ
การพัฒนาและการจัดหาระบบงาน
และโปรแกรม

(Development and Acquisition)

คำนำ

คู่มือตรวจสอบการพัฒนาและการจัดหาระบบงานและโปรแกรม (Development and Acquisition Booklet – D&A) ฉบับนี้เป็นส่วนหนึ่งของการปรับปรุงคู่มือการตรวจสอบระบบเทคโนโลยีสารสนเทศ ฉบับเดือนพฤศจิกายน 2543 ของส่วนตรวจสอบเทคโนโลยีสารสนเทศ ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ ซึ่งได้ยกเลิกเนื้อหาเดิม บทที่ 10 การพัฒนาระบบ และใช้คู่มือฉบับนี้แทน ตามแนวทางของ Federal Financial Institutions Examination Council (FFIEC) ประเทศสหรัฐอเมริกา

คู่มือตรวจสอบ D&A ของสถาบันการเงินฉบับนี้จัดทำขึ้นสำหรับให้ผู้ตรวจสอบใช้เป็นแนวทางในการระบุและควบคุมความเสี่ยงจากการพัฒนาและการจัดหาระบบงานและโปรแกรม (การพัฒนาและการจัดหาฯ) ของสถาบันการเงิน โดยเนื้อหาของคู่มือมุ่งเน้นไปที่การตรวจสอบความเหมาะสมของระบบเทคโนโลยีสารสนเทศ (IT) เกี่ยวกับการระบุ การจัดหา การติดตั้ง และการบำรุงรักษา ระบบระบบงาน IT (ครอบคลุมทั้งการพัฒนาระบบงานและโปรแกรมภายในและการจัดซื้อจัดหาเครื่องมือ โปรแกรม หรือบริการด้านเทคโนโลยีจากบุคคลภายนอก)

กระบวนการพัฒนา การจัดหา และการบำรุงรักษาแต่ละขั้นตอนมีความเสี่ยงเกิดขึ้นมากมาย จึงจำเป็นต้องจัดให้มีกระบวนการบริหารโครงการที่มีประสิทธิภาพเพื่อลดความเสี่ยงด้าน Operationsซึ่งอาจจะก่อให้เกิดความเสียหายทางการเงินที่มีสาเหตุมาจากขั้นตอนการปฏิบัติงานที่ไม่เพียงพอ บุคลากร และระบบงาน หรืออาจจะเกิดความเสียหายอันเนื่องมาจากสาเหตุอื่นๆ เช่น ความผิดพลาด การทุจริต การไม่สามารถส่งมอบผลิตภัณฑ์และบริการตามกำหนด ความสามารถในการแข่งขัน และการบริหารจัดการข้อมูล ซึ่งสามารถดูได้จากคู่มือตรวจสอบการจัดการ

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ หวังว่าแนวทางการตรวจสอบในคู่มือฉบับนี้จะเป็นประโยชน์และช่วยพัฒนาการตรวจสอบให้มีประสิทธิภาพต่อไปในอนาคต

ฝ่ายตรวจสอบความเสี่ยงและเทคโนโลยีสารสนเทศ

ธันวาคม 2551

สารบัญ

หน้าที่

<u>ส่วนที่ 1</u> บทนำ

คู่มือตรวจสอบการพัฒนาและการจัดหาระบบงานและโปรแกรม (Development and Acquisition Booklet: D&A) ฉบับนี้อธิบายถึงกิจกรรมในการบริหารโครงการ และ**เน้นให้เห็นถึงประโยชน์จากการใช้เทคนิคในการบริหารโครงการที่ได้ถูกออกแบบไว้เป็นอย่างดีแล้ว** นอกจากนี้คู่มือ D&A ยังได้ให้**รายละเอียดของมาตรฐานในการบริหารโครงการ ขั้นตอนของการปฏิบัติงาน ระบบการควบคุมดูแล และการอภิปรายให้เห็นถึงความเสี่ยงที่เกิดขึ้นจากการพัฒนา การจัดหา และการบำรุงรักษาโครงการ** อนึ่งคู่มือ D&A จะมีการสรุปภาพรวมของแนวทางการปฏิบัติเพื่อสรุปใจความสำคัญในแต่ละเรื่องให้ผู้ตรวจสอบเข้าไปดูเป็นลำดับแรก แต่ไม่ใช่การสรุปเนื้อหาทั้งหมด ดังนั้นผู้ตรวจสอบจึงควรอ่านหัวข้อสรุปและอ่านรายละเอียดขั้นตอนการดำเนินงานประกอบไปพร้อมๆกันด้วย

วัตถุประสงค์ของการสอบทานกิจกรรมต่างๆ ในการพัฒนา การจัดหา และการบำรุงรักษา ก็**เพื่อระบุจุดอ่อนหรือความเสี่ยงต่างๆ ที่มีผลกระทบที่ไม่ดีต่อองค์กรได้ ระบุหน่วยงานซึ่งมีสถานการณ์หรือผลการปฏิบัติงานที่อยู่ในข่ายที่จำเป็นต้องให้ความสนใจในการกำกับดูแลเป็นพิเศษ** และดำเนินการปรับปรุงแก้ไข ต่อไป

ผู้ตรวจสอบควรจะสอบทานความเสี่ยงจากการประเมินประสิทธิภาพทั้งหมดของมาตรฐานต่างๆ ขั้นตอนการปฏิบัติงาน และระบบการควบคุมต่างๆ สำหรับการบริหารโครงการขององค์กร และแม้ว่าผู้ตรวจสอบไม่ควรคาดหวังว่าองค์กรจะมีการนำเอาเทคนิคต่างๆมาใช้บริหารโครงการอย่างมากมายและกว้างขวาง แต่อย่างน้อยองค์กรควรจะต้องมีการใช้มาตรฐาน ขั้นตอนการปฏิบัติงาน และระบบการควบคุมต่างๆ ให้เหมาะสมกับลักษณะและความเสี่ยงของการพัฒนา การจัดหา และการบำรุงรักษาโครงการต่างๆขององค์กร

เนื่องจาก IT มีความสำคัญอย่างยิ่งยวดต่อการดำเนินงานของสถาบันการเงินจึงมีความจำเป็นที่จะต้องมีการใช้กระบวนการพัฒนา การจัดหา และการบำรุงรักษา IT ที่เหมาะสม อย่างไรก็ดีมาตรฐานการปฏิบัติงานมิได้เป็นเครื่องมือรับประกันว่าองค์กรจะมีการดำเนินงานตามกระบวนการพัฒนา การจัดหา และการบำรุงรักษาระบบงาน IT ได้อย่างเหมาะสม แต่อย่างน้อย**การปฏิบัติตามมาตรฐานก็ช่วยเสริมสร้างความสามารถของฝ่ายจัดการในการควบคุมและบริหารโครงการได้ดีจึงช่วยลดความเสี่ยงจากการบริหารโครงการลงไปได้** นอกจากนี้มาตรฐานการปฏิบัติงานที่ได้กำหนดไว้ดีแล้วยังช่วยให้องค์กรสามารถจัดหาโปรแกรมระบบงานได้อย่างมีประสิทธิภาพ มีสภาพแวดล้อมในการ

ปฏิบัติงานที่ปลอดภัยและเชื่อถือได้ และตรงกับความต้องการขององค์กรและผู้ใช้งาน ดังนั้นองค์กรที่มีการบริหารโครงการเป็นประจำ ควรจะกำหนดให้มีมาตรฐานการปฏิบัติงาน แนวนโยบาย และขั้นตอนการปฏิบัติงานที่เหมาะสมกับโครงการและความต้องการขององค์กรเพื่อลดความเสี่ยงจากการบริหารโครงการลงไป

การรักษาความปลอดภัยด้านข้อมูลสารสนเทศ **(ข้อมูลด้าน IT)** ถือเป็นสิ่งสำคัญอย่างยิ่งสำหรับการพัฒนาระบบงานและโปรแกรม (D&A) ทั้งพัฒนาขึ้นใช้งานเองภายในหรือที่จัดหามาจากภายนอกองค์กร สถาบันการเงินจึงควรตรวจสอบความจำเป็นในการรักษาความปลอดภัยของข้อมูลด้าน IT และเสริมสร้างระบบควบคุมแบบอัตโนมัติเข้าไปใน D&A ก่อนที่จะนำเอาระบบงานและโปรแกรมมาใช้งานจริง ผู้ตรวจสอบ สามารถศึกษาเพิ่มเติมได้จากคู่มือตรวจสอบการรักษาความปลอดภัยข้อมูล และยังสามารถศึกษาเพิ่มเติมจากหนังสือเรื่อง “Security Considerations in the Information System Development Life Cycle”

<u>ส่วนที่ 2</u> แนวทางที่พึงปฏิบัติ

2.1 การบริหารโครงการ

<u>สรุปแนวทางการปฏิบัติ</u>

สถาบันการเงินควรดำเนินการพัฒนา การจัดหา และการบำรุงรักษา กระบวนการบริหารและจัดการโครงการในรูปแบบที่เหมาะสม กับ**ลักษณะเฉพาะและความเสี่ยงต่างๆ ขององค์กร**และควรจะประกอบไปด้วย

- แผนงานโครงการ
- การกำหนดความต้องการของโครงการและความคาดหวัง
- มาตรฐานและขั้นตอนการปฏิบัติงานในการบริหารโครงการ
- การรับประกันคุณภาพและขั้นตอนการปฏิบัติงานในการบริหารความเสี่ยง
- การกำหนดบทบาทและความรับผิดชอบของโครงการ
- การมีส่วนร่วมของผู้ที่มีส่วนเกี่ยวข้องทั้งหมด
- เทคนิคการสื่อสารข้อมูลของโครงการ

การบริหารโครงการมีรูปแบบที่เข้าใจได้ง่ายๆ คือ การวางแผนและการปฏิบัติงานให้สำเร็จตามเป้าหมาย โดยอาจจะเป็นงานที่เกี่ยวข้องกับโครงการ IT แบบทำครั้งเดียวจบ หรือ ต้องดำเนินการในส่วนที่เกี่ยวข้องกับกิจกรรมด้าน Operations ดังนั้น ถ้าโครงการมีผลกระทบกับ Operations องค์กรจะต้องเอาใจใส่เป็นพิเศษในการประเมินผลกระทบจากกิจกรรมต่างๆ ที่เกิดขึ้นในขั้นตอนการพัฒนา การจัดหา และการบำรุงรักษาโครงการ

องค์กรจะสามารถบริหารโครงการให้สำเร็จได้อย่างดีต้องประกอบไปด้วยแผนงานโครงการที่มีรายละเอียดซึ่งแสดงให้เห็นความคาดหวังของโครงการที่ชัดเจน ผู้จัดการโครงการมีประสบการณ์ งบประมาณที่จัดสรรมาสมเหตุผล และการติดต่อสื่อสารที่มีประสิทธิภาพ แต่สำหรับองค์กรที่ไม่มีระบบการบริหารโครงการที่ดีก็จะก่อให้เกิดปัญหาต่างๆ คือ ความล่าช้าในการส่งมอบงาน งบประมาณบานปลาย และโปรแกรมระบบงานที่คุณภาพต่ำ

โปรแกรมระบบงานที่มีคุณภาพต่ำสังเกตได้จากการที่ระบบงานถูกใช้งานน้อย ไม่มีความปลอดภัย และไม่น่าเชื่อถือ ระบบงานมีคุณสมบัติในการทำงานที่มีระบบรักษาความปลอดภัยและระบบการควบคุมภายในไม่ดีพอ เสียค่าใช้จ่ายสูง ใช้เวลาในการพัฒนานาน และไม่มีประสิทธิภาพในการทำงานที่ดี ต้องมีการปรับปรุงเพื่อแก้ไขโปรแกรมระบบงานใหม่ ดังนั้นองค์กรจึงควรบริหารโครงการอย่างระมัดระวังเพื่อให้ได้ผลลัพธ์ตรงตามความต้องการ ภายในระยะเวลาและงบประมาณที่กำหนดไว้

สถาบันการเงินสามารถเลือกใช้กระบวนการบริหารโครงการด้าน IT ได้หลายรูปแบบ แต่ในคู่มือฉบับนี้ เราจะพูดถึงเฉพาะเรื่อง วงจรในการพัฒนาระบบงาน (System Development Life Cycle: SDLC) และถูกใช้เป็นตัวอย่างในการอธิบายวิธีการบริหารโครงการเพราะว่า SDLC สามารถแสดงให้เห็นถึงวิธีบริหารงานที่สามารถอธิบายความหลากหลายของงานที่เกี่ยวข้องกับโครงการพัฒนาโปรแกรมระบบงานได้อย่างเป็นระบบ แต่สถาบันการเงินก็สามารถเลือกใช้วิธีการบริหารโครงการแบบอื่นๆ ในการควบคุมโครงการที่เกี่ยวข้องกับการพัฒนาโปรแกรมระบบงาน เครื่องคอมพิวเตอร์และอุปกรณ์ และการใช้บริการจากภายนอกได้ แต่จะต้องปรับปรุงให้การดำเนินงานดังกล่าวมีความสัมพันธ์กับลักษณะเฉพาะและความเสี่ยงที่เกิดขึ้น นอกจากนี้**คณะกรรมการธนาคารหรือคณะกรรมการอื่นที่ตั้งขึ้นควรจะต้องอนุมัติกระบวนการบริหารโครงการ และฝ่ายจัดการจะต้องจัดทำเอกสารแสดงการอนุมัติในการดำเนินงานที่แตกต่างไปจากแผนงานเป็นลายลักษณ์อักษร**

(1) วงจรในการพัฒนาระบบงาน (SDLC)

เทคนิคการบริหารโครงการที่ดี การออกแบบโครงสร้างต้องดี เช่น SDLC จะช่วยให้ฝ่ายจัดการสามารถควบคุมโครงการได้ดียิ่งขึ้นโดยแบ่งแยกงานที่สลับซับซ้อนออกมาเป็นชิ้นส่วนที่สามารถบริหารได้ และการแบ่งแยกโครงการออกเป็นส่วนๆ ตามกระบวนการควบคุมทางตรรกะ (Phases) ช่วยให้ผู้บริหารโครงการสามารถสอบทานความคืบหน้าในแต่ละขั้นตอนได้ว่าประสบความสำเร็จตามเป้าหมายหรือไม่ก่อนที่จะทำการจัดสรรทรัพยากรสำหรับใน Phases ต่อไป

จำนวนของ Phasesใน SDLC จะขึ้นอยู่กับลักษณะเฉพาะต่างๆของโครงการและแนวทางในการบริหารโครงการ โดยสามารถแบ่งออกเป็นขั้นตอนในการดำเนินการกว้างๆได้ 5 ขั้นคือ 1) การเตรียมการ 2) การได้รับมา 3) การทดสอบ 4) การใช้งาน และ 5) การบำรุงรักษา แต่สำหรับโครงการพัฒนาโปรแกรมระบบงาน ตามปกติจะแบ่งออกเป็น 7 ขั้นคือ 1) การเริ่มโครงการ 2) การวางแผน 3) การออกแบบ 4) การพัฒนา 5) การทดสอบ 6) การใช้งาน และ 7) การบำรุงรักษา แต่ก็มีบางองค์กรจัดให้มีขั้นตอนที่ 8 เพิ่มขึ้นคือ กระบวนการยกเลิกและทำลายในขั้นตอนสุดท้ายด้วย และ

กิจกรรมที่จะต้องทำให้สำเร็จในแต่ละ Phases ก็ขึ้นอยู่กับชนิดของโครงการและวิธีการบริหารโครงการที่เลือกใช้ ดังนั้นการดำเนินงานโครงการต่างๆ จะต้องดำเนินการให้เป็นไปตามแผนงานที่ถูกกำหนดมาไว้อย่างชัดเจนแล้วในแต่ละ Phases

(2) เทคนิคการบริหารโครงการแบบอื่น

วิธี SDLC ได้อธิบายให้เห็นวิธีการบริหารงานโครงการตามลำดับขั้นตอน แต่ก็มีจุดอ่อนคือไม่มีการบริหารความเสี่ยงของโครงการอย่างดีพอถ้าขั้นตอนในการดำเนินงานต่างๆสำเร็จเป็นไปตามเป้าหมาย เช่น เมื่อผู้ใช้งาน (user) ได้กำหนดความต้องการและส่งให้ผู้ออกแบบระบบงาน (system designer) ซึ่งจะทำงานออกแบบและส่งมอบงานต่อไปให้ ผู้พัฒนาโปรแกรม (programmer) แต่ถ้าบังเอิญ programmer ได้พบวิธีการปรับปรุงกระบวนการทำงานที่ดีกว่าได้ เขาจะต้องส่งงานกลับไปให้ system designer ปรับปรุงแก้ไขงานก่อนจึงจะเริ่มดำเนินงานต่อไปได้ แต่ถ้ากลับกัน programmer ได้เข้าไปมีส่วนร่วมด้วยในขั้นตอนการวางแผนและการออกแบบระบบงานเขาก็สามารถจะให้ความเห็นได้ตั้งแต่แรก ดังนั้น **เพื่อเพิ่มประสิทธิภาพในการบริหารโครงการองค์กรควรจะเลือกใช้วิธีบริหารโครงการที่กำหนดให้ผู้ที่เกี่ยวข้องเข้าไปมีส่วนร่วมในทุก Phases**

เทคนิคการบริหารโครงการ เช่น spiral, iterative และ modifies SDLC ได้มุ่งเน้นไปที่การบริหารความเสี่ยงและการดำเนินงานแบบที่เกิดขึ้นซ้ำๆมากขึ้น จึงสามารถแก้ไขจุดอ่อนของวิธีการบริหารโครงการแบบ SDLC แบบเดิมได้ (แต่จะไม่มีการกล่าวถึงเทคนิคการบริหารเหล่านี้ในคู่มือเล่มนี้) การดำเนินงานแบบซ้ำๆ จะช่วยเสริมสร้างความสามารถของผู้บริหารโครงการในการกำหนดความต้องการของผู้ที่เกี่ยวข้อง (ผู้ใช้งาน ผู้บริหารระบบรักษาความปลอดภัย ผู้ออกแบบระบบ ผู้พัฒนา ผู้เชี่ยวชาญด้านเทคนิคระบบ และอื่นๆ) ได้อย่างมีประสิทธิภาพ และยังช่วยให้ผู้บริหารโครงการสามารถทำงานได้สำเร็จ ทบทวน และปรับปรุงขั้นตอนการดำเนินกิจกรรมในแต่ละ phases จนกว่าเขาจะสามารถได้รับผลลัพธ์ที่น่าพอใจได้ในขั้นตอนการส่งมอบงาน

(3) บทบาทและความรับผิดชอบ

ขนาดและความซับซ้อนของโครงการเป็นตัวกำหนดจำนวนบุคลากร และคุณสมบัติของบุคลากรในโครงการ และสำหรับในองค์กรขนาดเล็กหรือโครงการที่มีความเสี่ยงต่ำองค์กรก็อาจจะมีการกำหนดหน้าที่ในการทำงานของบุคลากรที่ทับซ้อนกันได้ แต่ทุกโครงการก็ควรจะมีแนวทางในการแบ่งแยกหน้าที่หรือมีกระบวนการควบคุมอื่นๆ เข้ามาชดเชยที่เหมาะสม

บทบาทและหน้าที่ความรับผิดชอบขั้นต้น มีดังนี้

- ผู้บริหารสูงสุดขององค์กร (Corporate Management) รับผิดชอบในการอนุมัติโครงการที่สำคัญๆ เพื่อให้เกิดความมั่นใจว่าโครงการเหล่านั้นสามารถสนับสนุนเป้าหมายทางธุรกิจได้

- ผู้บริหารระดับสูง (Senior Management) รับผิดชอบในการอนุมัติและส่งเสริมโครงการตามอำนาจหน้าที่ที่มี และให้ความมั่นใจว่ามีทรัพยากรอย่างเพียงพอสำหรับดำเนินงานโครงการจนสำเร็จ

- คณะกรรมการด้าน IT (Technology Steering Committee) หรือคณะทำงานงานที่ได้รับมอบหมายรับผิดชอบในการอนุมัติและ/หรือกำหนดสิ่งส่งมอบของโครงการและการประสานงานด้านกิจกรรมต่างๆ กับฝ่ายงาน ที่เกี่ยวข้อง คณะกรรมการฯ อาจประกอบด้วย ผู้จัดการโครงการ คณะกรรมการบริษัท และผู้บริหารระดับสูง และสำหรับองค์กรขนาดใหญ่อาจตั้งสำนักงานบริหารโครงการ (project management offices-PMO) เพื่อทำหน้าที่ดูแลโครงการทั้งหมด

- ผู้จัดการโครงการ (Project Manager) มีหน้าที่รับผิดชอบ บริหารจัดการให้เกิดความมั่นใจว่าโครงการต่างๆ ในความรับผิดชอบ สามารถสนับสนุนเป้าหมายทางธุรกิจ เป้าหมายของโครงการ และมีการกำหนดความคาดหวังที่ชัดเจน รวมถึงมีการระบุรายละเอียดของงาน กำหนดตารางเวลา การดำเนินโครงการตั้งแต่เริ่มต้นจนสำเร็จ นอกจากนี้ผู้จัดการโครงการยังรับผิดชอบในการติดตามดูแล และรายงานความคืบหน้าของโครงการต่อผู้บริหารระดับสูงด้วย

- ผู้ให้การสนับสนุนโครงการ (Project Sponsor) รับผิดชอบในการให้การสนับสนุนการพัฒนาโปรแกรมแก่ฝ่ายงานที่เป็นผู้ใช้งาน (User Department) ช่วยพิจารณาการกำหนดสิ่งส่งมอบและให้การสนับสนุนการทดสอบของผู้ใช้งาน นอกจากนี้ Project Sponsor ส่วนใหญ่รับผิดชอบ ในการจัดหาทรัพยากรทางการเงินให้กับโครงการด้วย

- ฝ่ายงาน IT (Technology Department) รับผิดชอบในการบำรุงรักษาทรัพยากรด้าน IT ที่ใช้งานในโครงการต่างๆ ให้ความช่วยเหลือใน Phases การทดสอบระบบและการติดตั้งระบบ เพื่อใช้งาน รวมถึงช่วยเหลือในขั้นตอนการกำหนดขอบเขตของโครงการให้สัมพันธ์กับข้อจำกัดต่างๆ ของระบบฐานข้อมูลและระบบเครือข่ายที่องค์กรมีอยู่

- หน่วยงานรับประกันคุณภาพ (Quality Assurance) รับผิดชอบทดสอบสมมุติฐานต่างๆ ของโครงการเพื่อให้เกิดความมั่นใจได้ว่างานที่ส่งมอบในแต่ละ Phases มีคุณภาพ บุคลากรในหน่วยงานนี้หรือคณะทำงานที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ดังกล่าวควรเป็นอิสระจากกระบวนการพัฒนาโครงการและต้องใช้มาตรฐานการปฏิบัติงานและขั้นตอนการดำเนินงานต่างๆ ที่

กำหนดไว้ล่วงหน้าแล้วมาใช้เป็นเครื่องมือในการประเมินคุณภาพของสิ่งส่งมอบตลอดช่วงอายุของโครงการ

- ฝ่ายงานผู้ใช้งาน (User Departments) ทำหน้าที่ช่วยผู้จัดการโครงการ ผู้ออกแบบระบบงาน และผู้พัฒนาโปรแกรม ในการกำหนดและทดสอบคุณสมบัติในการทำงานที่กำหนดไว้ การเข้าไปมีส่วนร่วมของผู้ใช้งานในแต่ละ Phases ตลอดทั้งโครงการเป็นเรื่องที่มีความจำเป็นอย่างยิ่งยวดเพื่อให้เกิดความมั่นใจในความถูกต้องของการกำหนดความต้องการของระบบงานและการทดสอบระบบอย่างเพียงพอ และสำหรับโครงการขนาดใหญ่อาจจะมีการใช้ผู้เชี่ยวชาญเฉพาะเรื่องหรือผู้วิเคราะห์ข้อมูล มาช่วยในการสื่อสารข้อมูลของผู้ใช้งานและข้อกำหนดต่างๆในเรื่องคุณสมบัติของระบบงานที่ผู้ใช้งานต้องการให้กับคณะทำงานของโครงการต่อไป

- ผู้ตรวจสอบ (Auditors) ทำหน้าที่ช่วยให้ข้อเสนอแนะแก่ฝ่ายงานผู้ใช้งาน ผู้จัดการโครงการและผู้ออกแบบระบบ ในการกำหนดความต้องการของระบบควบคุมภายใน และการกำหนดขอบเขตการทดสอบระบบการควบคุมต่างๆ ทั้งในช่วงเวลาของการพัฒนาระบบและหลังจากการนำระบบออกใช้งานแล้ว

อย่างไรก็ตาม สถาบันการเงินควรกำหนดแนวปฏิบัติเกี่ยวกับบทบาทหน้าที่ในลักษณะดังกล่าวเพิ่มเติมเพื่อไม่ให้กระทบกับความเป็นอิสระ ทั้งในขั้นตอนการให้คำแนะนำแก่ผู้ใช้งาน (User) และการทดสอบความเพียงพอของระบบควบคุม

- ผู้จัดการด้านการรักษาความปลอดภัย (Security Managers) ทำหน้าที่ช่วยผู้ใช้งานจากฝ่ายงานต่างๆ ผู้จัดการโครงการ และผู้ออกแบบระบบ ในการกำหนดความต้องการในการรักษาความปลอดภัยและทำการทดสอบคุณสมบัติต่าง ๆเหล่านั้นระหว่างการพัฒนาระบบและหลังจากการนำระบบออกใช้งาน

2.1.1 แผนงานโครงการ

การวางแผนถือเป็นส่วนที่สำคัญที่สุดของการบริหารโครงการเนื่องจากงานโครงการมีส่วนของงานที่ต้องดำเนินการที่มีความสัมพันธ์กันกับหน่วยงานต่างๆจำนวนมาก ดังนั้นการวางแผนที่ไม่ดีอาจจะทำให้โครงการล้มเหลวหรือไม่เป็นไปตามที่คาดหวังได้ **ผู้ตรวจสอบจึงต้องประเมินความเพียงพอของการวางแผนกิจกรรมต่างๆของโครงการอย่างระมัดระวัง** โดยมุ่งเน้นไปที่ความสามารถของฝ่ายจัดการในการพัฒนาและดำเนินการตามแผนงานที่ออกแบบมาอย่างเหมาะสมกับความเสี่ยงและลักษณะเฉพาะของโครงการ

ขั้นแรกเริ่มเมื่อมีการยื่นเสนอโครงการ ซึ่งจะต้องมีการแสดงเหตุผลและความจำเป็นของโครงการ การกำหนดลักษณะเฉพาะของระบบที่ต้องการ และขอบเขตการทำงานที่เป็นไปได้ทั้งหมดของโครงการ รวมไปถึง ข้อมูลที่ต้องการใช้ การเชื่อมต่อระหว่างเครือข่าย เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ (hardware) ที่สามารถสนับสนุนและเชื่อมโยงกับระบบงานที่ต้องการ ส่วนฝ่ายจัดการมีหน้าที่พิจารณาความเหมาะสมทางธุรกิจ ขอบเขตของโครงการ (เช่น ประโยชน์ที่จับต้องได้และที่จับต้องไม่ได้ ประมาณการต้นทุน ผลตอบแทนของโครงการ เป็นต้น) และความเป็นไปได้ของโครงการ ถ้ามีการอนุมัติโครงการที่เสนอแล้วต้องมีเอกสารประกอบในการพัฒนาตามแผนงานโครงการด้วย

แผนงานโครงการต่างๆ ได้ขยายความเข้าใจที่ชัดเจนเกี่ยวกับประเภทของทรัพยากรที่จำเป็นต้องใช้ และกิจกรรมต่างๆ ของโครงการอย่างละเอียดเป็นลายลักษณ์อักษร ทั้งนี้แผนงานจะต้องแสดงให้เห็นกิจกรรมในการทำงาน (การจัดโครงสร้างของทีมงาน กำหนดเวลาของกิจกรรมทั้งหมด การจัดสรรทรัพยากร และอื่นๆ) และกิจกรรมในการบริหารโครงการ (ขั้นตอนการบริหารความเสี่ยงและการบริหารโครงการ การจัดทำบันทึกแสดงวัตถุประสงค์ของโครงการและข้อสมมติฐานต่าง ๆ การจัดทำเอสารประกอบที่ชัดเจนและเป็นไปตามมาตรฐานในการรายงานผล และอื่นๆ) ที่ชัดเจน แผนงานโครงการควรมีองค์ประกอบ ดังต่อไปนี้

- **ภาพรวมของโครงการ (Project Overviews)** แสดงให้เห็นเหตุผลและที่มาของโครงการซึ่งแสดงให้เห็นถึงวัตถุประสงค์หลักและแผนกลยุทธ์ของโครงการ

- **บทบาทและความรับผิดชอบ (Roles and Responsibilities)** มีการกำหนดตัวบุคลากรที่สำคัญและมีการบรรยายถึงความรับผิดชอบหลักเพื่อเสริมสร้างความเข้าใจของคณะทำงานของการมอบหมายงานของโครงการและข้อกำหนดต่างๆในการรายงานผลความคืบหน้า

- **ขั้นตอนในการติดต่อสื่อสาร (Communication Procedures)** มาตรฐานการดำเนินงานและขั้นตอนในการติดต่อสื่อสารช่วยเสริมสร้างการแลกเปลี่ยนข้อมูลระหว่างบุคลากรของโครงการได้ดียิ่งขึ้น โดยเฉพาะอย่างยิ่งกับโครงการขนาดใหญ่

- **รายละเอียดของสิ่งส่งมอบ (Defined Deliverables)** การกำหนดความต้องการของโครงการและเงื่อนไขในการยอมรับผลลัพท์ของโครงการที่ชัดเจนเพื่อสร้างความมั่นใจว่าฝ่ายจัดการและพนักงานได้รับทราบความคาดหวังต่างๆเหล่านั้น

- **มาตรฐานต่าง ๆ (Standards)** การบริหารโครงการ การควบคุมการเปลี่ยนแปลงแก้ไข และมาตรฐานของการรับประกันคุณภาพมีส่วนช่วยเพิ่มโอกาสในการประสบความสำเร็จของโครงการ

-**ข้อกำหนดของระบบควบคุม (Control Requirement) การออกแบบระบบการควบคุมภายในและคุณสมบัติในการรักษาความปลอดภัยแบบอัตโนมัติ**ตั้งแต่ในขั้นตอนเริ่มต้นของการออกแบบระบบงานจะช่วยเสริมสร้างการทำงานได้อย่างมีประสิทธิภาพ

- **แผนการรับประกันคุณภาพ (Quality Assurance Plan)** แผนการรับประกันคุณภาพ ช่วยเสริมสร้างความมั่นใจว่าโครงการและผลิตภัณฑ์ต่างๆ จะมีผลลัพธ์เป็นไปตามมาตรฐานและความคาดหวัง

- **การบริหารความเสี่ยง (Risk Management) การกำหนดประเภท การประเมินและขั้นตอนการปฏิบัติงานเพื่อการควบคุมความเสี่ยง**มีส่วนช่วยเพิ่มโอกาสในการประสบความสำเร็จของโครงการ

- **การบริหารวิธีการกำหนดค่าตัวแปรต่างๆ (Configuration Management-configuration)** แผนการบริหารวิธีการกำหนดค่าตัวแปรต่างๆ จะอธิบายให้ทราบถึงวิธีการในการควบคุมและการจัดทำเอกสารประกอบการเปลี่ยนแปลงต่างๆ ที่เกี่ยวข้องกับแผนงานของโครงการ ความต้องการใช้บริการต่างๆ hardware และ configuration จะมีส่วนช่วยสนับสนุนโครงการและการบำรุงรักษาประสิทธิภาพ

- **การจัดทำเอกสารต่างๆ (Documentation) การกำหนดรูปแบบและระดับของเอกสารประกอบ**ซึ่งสมาชิกของโครงการจะต้องจัดทำในทุกขั้นตอนของโครงการจะมีส่วนช่วยเพิ่มประสิทธิภาพและความสามารถในการบำรุงรักษาระบบได้อย่างดี

- **งบประมาณ (Budget) การจัดทำงบประมาณชั้นต้น**ช่วยให้ฝ่ายจัดการทราบต้นทุนและสามารถประเมินถึงความสำเร็จของโครงการได้ และการเฝ้าติดตามค่าใช้จ่ายตามงบประมาณตลอดโครงการก็มีส่วนช่วยให้ฝ่ายจัดการสามารถประเมินและควบคุมค่าใช้จ่ายต่างๆได้

- **การกำหนดตารางเวลาของโครงการ (Scheduling)** การกำหนดตารางเวลาของโครงการในแต่ละขั้นตอนมีส่วนช่วยเสริมสร้างความมีประสิทธิภาพของโครงการ

- **การทดสอบ (Testing)** แผนการทดสอบและตารางเวลามีส่วนช่วยให้การทดสอบสามารถดำเนินการไปได้อย่างประสิทธิภาพและประสิทธิผล

- **การพัฒนาบุคลากร (Staff Development)** แผนการและตารางเวลาการอบรมมีส่วนช่วยเสริมสร้างประสิทธิภาพและประสิทธิผล

2.1.2 มาตรฐานการบริหารโครงการ

องค์กรควรจะกำหนดมาตรฐานในการบริหารโครงการ (มาตรฐาน)และสำหรับ**สถาบันการเงินที่มีความจำเป็นต้องดำเนินการเป็นประจำในการพัฒนาโครงการหลายๆโครงการให้สำเร็จผลพร้อมๆกันก็ควรจัดให้มี PMO** ขึ้นมาเพื่อช่วยประสานงานกิจกรรมต่างๆของโครงการ

มาตรฐานควรกล่าวถึงกิจกรรมต่างๆ โดยทั่วไปของโครงการ เช่น คำขอจัดตั้งโครงการ การสอบทาน ขั้นตอนในการอนุมัติ การคัดเลือกวิธีการในการบริหารโครงการ การรายงานความคืบหน้า และข้อกำหนดในการจัดทำเอกสารประกอบต่าง ๆ นอกจากนี้ควรระบุถึงความต้องการเฉพาะของแต่ละโครงการด้วย เช่น โครงการพัฒนาโปรแกรมระบบงาน (software) ควรจะมีมาตรฐานในการปฏิบัติงานที่เกี่ยวข้องกับ การออกแบบโปรแกรมระบบงาน วิธีการเขียนโปรแกรม และข้อกำหนดของการทดสอบ

มาตรฐานควรจะสามารถนำมาใช้ชดเชยได้เหมาะสมกับลักษณะและความเสี่ยงของโครงการและองค์กรด้วย และควรกำหนดให้มีผู้แทนจากทุกฝ่ายงานที่เกี่ยวข้องหรือได้รับผลกระทบมาช่วยกำหนดภาระหน้าที่และสิ่งส่งมอบจากโครงการ นอกจากนี้ควร**มีข้อมูลที่มีรายละเอียดเพียงพอที่สร้างความมั่นใจได้ว่าบุคลากรในทีมงานสามารถระบุวัตถุประสงค์และความคาดหวังของโครงการได้** เพราะว่าความคาดหวังที่ชัดเจนของโครงการเป็นข้อกำหนดประการแรกที่จะทำให้โครงการประสบความสำเร็จและนำมาสู่การยอมรับของบุคลากรภายในองค์กร

องค์กรที่มีความจำเป็นต้องประสานงานโครงการจำนวนหลายๆโครงการพร้อมกัน ควรกำหนดมาตรฐานเพื่อการประสานงานและการบริหารโครงการในภาพกว้างทั้งองค์กร และควรกำหนดให้มาตรฐานมีรายละเอียดเกี่ยวกับขั้นตอนการปฏิบัติงานในการกำหนดระดับความสำคัญของโครงการ การประสานงานในการใช้ทรัพยากร การจัดทำรายงานแสดงความคืบหน้า และผลการแก้ไขปัญหาโครงการที่ค้างอยู่ และอื่น ๆ อีก

(1) มาตรฐานการวางแผนโครงการ

องค์กรควรจะจัดสร้างมาตรฐานการวางแผนโครงการที่เหมาะสม ซึ่งจะต้องกำหนดให้ฝ่ายจัดการจัดทำแผนการพัฒนาโครงการที่แสดงรายละเอียดให้เหมาะสมกับลักษณะและความเสี่ยงของโครงการ และฝ่ายจัดการควรจัดทำแผนการพัฒนาโครงการที่มีรายละเอียดที่ชัดเจนสำหรับทุกๆโครงการ

แผนงานโครงการควรจะอธิบายถึงจุดอ่อนจุดแข็งของระบบที่มีอยู่เดิม อธิบายเป้าหมายหลักของโครงการ กำหนดตัวของผู้ใช้งาน ข้อมูล ระบบงาน และเครือข่ายที่ต้องการและการอธิบายและแสดงรายละเอียดจะช่วยเสริมสร้างความสามารถของบุคลากรในทีมให้สามารถเข้าใจวัตถุประสงค์ของโครงการและการพัฒนาระบบงานที่ตรงกับความต้องการขององค์กร นอกจากนี้แผนงานควรจะต้อง**กำหนดขั้นตอนการปฏิบัติงานในการรับประกันคุณภาพ การบริหารความเสี่ยงและการรักษาความปลอดภัย การทดสอบ การจัดทำเอกสารประกอบ และความต้องการเกี่ยวกับงบประมาณ จำนวนบุคลากร ทรัพยากร และการฝึกอบรม**

(2) มาตรฐานในการบริหารวิธีการกำหนดค่าตัวแปรต่าง ๆ

องค์กรควรจัดสร้างมาตรฐานในการบริหาร configuration (เกี่ยวข้องกับการควบคุมการเปลี่ยนแปลงต่างๆของโครงการเพื่อลดโอกาสที่จะเกิดการหยุดชะงักของโครงการและรักษาวัตถุประสงค์เดิมของโครงการ) ทั้งนี้มาตรฐานดังกล่าวควรกำหนดให้มีการเก็บรักษารายละเอียดของการกำหนดค่าตัวแปรพื้นฐานดั้งเดิมของ hardware software service เอกสารประกอบ และแผนการบริหารโครงการ รวมทั้งมีการกำหนดให้มีการประเมิน การอนุมัติ การจัดทำเอกสารมีเอกสารประกอบและมีการเผยแพร่ให้คนที่เกี่ยวข้องทราบ (ดูเพิ่มเติมในคู่มือนี้ในส่วน Maintenance)

(3) มาตรฐานการรับประกันคุณภาพ

การรับประกันคุณภาพถือเป็นส่วนสำคัญอย่างยิ่งของ D&A ที่มีการบริหารจัดการที่ดีเพราะว่าการรับประกันคุณภาพอย่างครบถ้วน การบริหารความเสี่ยง และมาตรฐานในการทดสอบทั้งหมดเป็นเครื่องมือที่ดีของฝ่ายจัดการในการบริหารความเสี่ยงของโครงการและสร้างความมั่นใจว่าโปรแกรมระบบงานจะสามารถทำหน้าที่ได้ตามที่ต้องการ มีระบบการรักษาความปลอดภัย และสามารถดำเนินการให้บริการได้ ดังนั้น**องค์กรจึงควรจัดให้มีการรับประกันคุณภาพสำหรับ D&A ทั้งจากภายในหรือจากภายนอกองค์กร**

ฝ่ายจัดการควรจัดสร้างมาตรฐานการรับประกันคุณภาพ ให้ครอบคลุมในหัวข้อเรื่อง ดังต่อไปนี้

- **ข้อผูกมัดตามสัญญา (Commitment)** โครงการที่ประสบผลสำเร็จจะต้องได้รับการปฏิบัติตามข้อผูกมัดตามสัญญาจากทุกฝ่ายที่เกี่ยวข้อง โดยที่ผู้บริหารระดับสูงมีข้อผูกมัดที่จะต้องให้การสนับสนุนอย่างเพียงพอและส่งเสริมให้มีการยอมรับโครงการต่างๆ ทั้งองค์กร ผู้ใช้งานมีข้อผูกมัดให้ช่วยกำหนดและทดสอบการทำงานของระบบให้ตรงความต้องการ ทีมงานโครงการมีข้อผูกมัดให้ทำโครงการให้สำเร็จ และผู้ที่เกี่ยวข้องทั้งหมดมีข้อผูกมัดให้กำหนดความคาดหวังเกี่ยวกับ

โครงการที่ชัดเจนและสื่อสารให้รับทราบทั่วทั้งองค์กร อนึ่งความล้มเหลวของฝ่ายจัดการในการติดตั้งหรือสนับสนุนโครงการรับประกันคุณภาพจะลดความสามารถขององค์กรในการค้นหาจุดอ่อนและความผิดพลาดของโครงการได้อย่างรวดเร็ว และยิ่งเกิดความล่าช้าในการค้นพบจุดอ่อนและความผิดพลาดเท่าใดก็ก่อให้เกิดค่าใช้จ่ายและความยุ่งยากในการแก้ไขปัญหามากยิ่งขึ้น

- **ความสมบูรณ์ครบถ้วน (Completeness) ในแต่ละ phases** ของวงจรชีวิตของโครงการ (วงจรชีวิต) จะประกอบไปด้วยขั้นตอนการปฏิบัติงานที่จะต้องดำเนินการและมีสิ่งของต่างๆที่ต้องส่งมอบ เพราะฉะนั้นควรจะต้องมีการดำเนินการตามโครงการรับประกันคุณภาพในทุกขั้นตอนของวงจรชีวิต เช่น ใน phases เริ่มต้นของโครงการจะต้องมีการนำเสนอกรณีศึกษาทางธุรกิจ การกำหนดคุณสมบัติที่ต้องการจากระบบงาน และการกำหนดองค์ประกอบของระบบที่ทำงานเกี่ยวข้องกับระบบงานอื่น หน่วยงานรับประกันคุณภาพหรือหน่วยงานซึ่งมีความเป็นอิสระที่ได้รับมอบหมายควรทำการตรวจสอบความเหมาะสมของโครงการ คุณสมบัติในการทำงานที่จำเป็นของระบบ และความถูกต้องในการเชื่อมต่อระบบงานต่างๆ ก่อนที่จะเริ่มต้น phases ของการวางแผนโครงการ บุคลากรของฝ่ายตรวจสอบและฝ่ายควบคุมการปฏิบัติงานตามกฎหมายและระเบียบงานควรช่วยสนับสนุนบุคลากรจากหน่วยงานรับประกันคุณภาพหรือหน่วยงานซึ่งมีความเป็นอิสระที่ได้รับมอบหมายตรวจสอบความถูกต้องของการปฏิบัติตามข้อกำหนดของโครงการทั้งจากภายในและภายนอกองค์กร

- **การดำเนินการตามความเหมาะสม (Scalability)** โครงการมีขนาดและความซับซ้อนที่แตกต่างกันไป การจัดทำมาตรฐานในการรับประกันคุณภาพจึงต้องจัดทำให้เหมาะสมกับความเสี่ยงและลักษณะเฉพาะของโครงการด้วย

- **การตรวจวัด (Measurability)** องค์กรไม่สามารถประเมินความสำเร็จของโครงการได้อย่างถูกต้องจนกว่าจะได้ทำการประเมินผลลัพธ์ของงานต่อความคาดหมายเดิมที่กำหนดไว้ ดังนั้น บุคลากรของหน่วยรับประกันคุณภาพควรจะประเมินคุณภาพของผลิตภัณฑ์และขั้นตอนการปฏิบัติงานเปรียบเทียบกับมาตรฐานต่างๆ ผลลัพธ์เชิงเมตริก และความคาดหวังต่างๆที่สามารถตรวจวัดได้

- **การติดตามผล (Tracking)** บุคลากรของโครงการควรจัดทำบันทึก รายงานและเฝ้าติดตามปัญหาเพื่อให้แน่ใจว่าได้มีการแก้ไขปัญหาอย่างมีประสิทธิภาพ

- **ความเป็นอิสระ (Independence)** บุคลากรของฝ่ายตรวจสอบและหน่วยงานรับประกันคุณภาพควรจะมีความเป็นอิสระจากโครงการที่ตนเองต้องเข้าไปสอบทาน

(4) มาตรฐานในการบริหารความเสี่ยง

องค์กรควรจัดสร้างมาตรฐานและขั้นตอนในการปฏิบัติงานเพื่อใช้ในการบริหารความเสี่ยงสำหรับทุกโครงการที่ซับซ้อนหรือมีความสำคัญ และกิจกรรมในการบริหารความเสี่ยง (บางครั้งอาจจะถูกรวมเป็นส่วนหนึ่งของการรับประกันคุณภาพ) ควรจะประกอบไปด้วยขั้นตอนการปฏิบัติงานในการกำหนดและบริหารความเสี่ยงของโครงการที่มีสาเหตุมาจากทั้งภายในและภายนอกองค์กร

ขั้นตอนการปฏิบัติงานควรจะถูกออกแบบมาเพื่อให้เกิดความมั่นใจว่าความเสี่ยงของโครงการที่เกิดจากภายในหรือภายนอกองค์กรได้ถูกกำหนดและประเมิน รายงานผลและเฝ้าติดตามดูแล และจัดการอย่างเหมาะสม เพราะว่าในขั้นตอนของการจัดการกับความเสี่ยงที่กำหนดไว้แล้ว องค์กรจะต้องพัฒนากลยุทธ์เกี่ยวกับระดับความเสี่ยงที่ยอมรับได้ การลดและบรรเทา และการถ่ายโอนความเสี่ยง หรือการผสมผสานแนวทางทั้งหมดเข้าด้วยกัน เช่น กลยุทธ์ในการลดความเสี่ยงสามารถดำเนินการได้โดยการทบทวนความเสี่ยงที่เกิดจากการกำหนดคุณสมบัติในการทำงานของโครงการตั้งแต่เริ่มต้นโครงการที่มีจำนวนมากเกินไป จึงควรตัดข้อกำหนดคุณสมบัติของโครงการที่ไม่จำเป็นออกไป **ส่วนการโอนความเสี่ยงจากภัยพิบัติตามธรรมชาติก็สามารถดำเนินการได้โดยการจัดหากรมธรรม์ประกันภัย**

เทคนิคการบริหารโครงการที่ดีจะช่วยลดความเสี่ยงได้ อย่างไรก็ตาม การบริหารโครงการมีความแตกต่างจากการบริหารความเสี่ยง เพราะว่า**การบริหารโครงการมุ่งเน้นที่การควบคุมกิจกรรมของโครงการซึ่งตรงข้ามกับการควบคุมความเสี่ยงของโครงการ** เช่น ขั้นตอนของการบริหารโครงการจะเกี่ยวข้องกับการกำหนดเวลาให้ programmer เขียนโปรแกรมตามกำหนดเวลา แต่กระบวนการบริหารความเสี่ยงจะเกี่ยวข้องกับแผนฉุกเฉินที่จะรองรับกรณีที่ programmer ลาออกจากงานก่อนที่จะทำงานเสร็จ ในทำนองเดียวกัน ขั้นตอนของการบริหารโครงการจัดหาระบบงานจากภายนอกจะเกี่ยวข้องกับการประเมินความมั่นคงทางการเงินของผู้ให้บริการ แต่กระบวนการบริหารความเสี่ยงจะเกี่ยวข้องกับการสอบทานความถูกต้องของการประเมินและการสร้างแผนฉุกเฉินในกรณีที่ผู้ให้บริการไม่สามารถให้บริการได้ตามเงื่อนไขที่ได้ตกลงกันไว้

(5) มาตรฐานการทดสอบ

ฝ่ายจัดการควรจัดสร้างมาตรฐานการทดสอบซึ่งกำหนดให้มีการใช้แผนการทดสอบที่มีขอบเขตการทดสอบที่ครอบคลุมและถูกกำหนดไว้ล่วงหน้า ผู้ใช้งาน (user) ต้องเข้ามามีส่วนร่วม และมีการจัดเก็บผลการทดสอบไว้เป็นหลักฐาน นอกจากนี้ มาตรฐานการทดสอบควรจะห้าม

ไม่ให้มีการทดสอบบนสภาพแวดล้อมที่ใช้งานจริง (production) หรือการใช้ข้อมูลจริงแต่ถ้ามีการคัดลอกข้อมูลจริงมาทำการทดสอบ ฝ่ายจัดการจะต้องมั่นใจว่าได้มีการกำหนดมาตรฐานในการป้องกันความลับของลูกค้ารั่วไหลอย่างเหมาะสม หรือฝ่ายจัดการสามารถใช้ software ในการสร้างตัวอย่างของข้อมูลได้ตามข้อกำหนดไว้ก่อนหน้านี้แล้วเพื่อประโยชน์ในการพัฒนาข้อมูลสำหรับทดสอบให้มีความเหมาะสม (มีโปรแกรมระบบงานอัตโนมัติอีกจำนวนมากที่สามารถทดสอบความสมเหตุสมผลของ software ความสามารถในหน้าที่การทำงานของระบบงาน และความสามารถในการเชื่อมโยงกันระหว่างเครือข่ายได้)

(6) มาตรฐานการจัดทำเอกสารประกอบ

องค์กรควรจัดสร้างมาตรฐานด้านเอกสารประกอบให้เหมาะสม โดยการจัดเอกสารประกอบให้มีคำอธิบายและรายละเอียดด้าน IT ระบบงาน และขั้นตอนการปฏิบัติงาน **เนื่องจากเอกสารประกอบช่วยส่งเสริมความสามารถของ user ในการใช้งาน การสอบทาน การปรับปรุง software system และขั้นตอนการปฏิบัติงาน (procedure)** ดังนั้นฝ่ายจัดการจึงควรจัดเก็บรักษาเอกสารประกอบที่เกี่ยวข้องกับทรัพยากรด้าน IT ทั้งหมด รวมถึงนโยบายที่ไม่ใช่ทางเทคนิคและขั้นตอนการปฏิบัติงาน และข้อมูลทางเทคนิค เช่น configuration ของ hardware software system และโปรแกรมระบบงานต้นฉบับ (source code) อีกประการหนึ่ง คุณภาพและปริมาณของเอกสารประกอบควรจะมีความเหมาะสมกับลักษณะและความเสี่ยงของทรัพยากรที่สัมพันธ์กัน ตัวอย่างเช่น software ที่สถาบันการเงินพิจารณาว่ามีความเสี่ยงสูงและมีนัยสำคัญต่อการดำเนินธุรกิจ ควรต้องจัดทำเอกสารประกอบที่เป็นลายลักษณ์อักษรตามมาตรฐานที่สถาบันการเงินกำหนดหรือตามมาตรฐานสากล**อย่างเต็มรูปแบบ** ส่วน software ที่สถาบันการเงินพิจารณาว่ามีความเสี่ยงต่ำอาจพิจารณาจัดทำเอกสารประกอบที่เป็นลายลักษณ์อักษรตามมาตรฐาน**ขั้นต่ำ** เป็นต้น

เอกสารประกอบ D&A ควรจะรวมไปถึง คำขอตั้งโครงการ การศึกษาความเป็นไปได้ของโครงการ แผนงานโครงการ แผนการทดสอบ และอื่น ๆ ส่วนเอกสารประกอบระบบ (system documentation) ที่มุ่งเน้นในการวิเคราะห์และการออกแบบระบบ ควรจะต้องมีคำอธิบายแนวคิดของระบบ ผังทางเดินข้อมูล (data flow) และรายละเอียดของระบบฐานข้อมูล (database specification) และ สำหรับเอกสารประกอบโปรแกรมระบบงาน (application documentation) ควรจะรวมถึงการอธิบายโปรแกรมระบบงาน ผังประกอบการเขียนโปรแกรม และคำแนะนำสำหรับ user และ operations

2.1.3 เครื่องมือที่ใช้บริหารโครงการ

ผู้จัดการโครงการสามารถใช้เครื่องมือได้หลายอย่างในการกำหนดตารางการปฏิบัติงานและการเฝ้าติดตามดูแลชิ้นงานต่างๆ ของโครงการ เพื่อประโยชน์ในการประมาณค่าใช้จ่ายและวันที่แล้วเสร็จของโครงการ เช่น ผู้จัดการโครงการที่มีประสบการณ์สามารถจะใช้โปรแกรม Excel ที่พัฒนาเองสำหรับโครงการขนาดเล็กที่ไม่ซับซ้อนได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม แต่ว่าส่วนใหญ่แล้วผู้จัดการโครงการควรจะพัฒนาหรือซื้อ software ที่สามารถทำงานได้ละเอียดกว่าเมื่อต้องทำงานโครงการที่มีขนาดใหญ่และซับซ้อน

ตารางข้างล่างต่อไปนี้เป็นตัวอย่างของเครื่องมือบริหารโครงการอย่างง่าย แต่สำหรับโครงการที่ใหญ่กว่าและผู้จัดการโครงการ (ผู้จัดการ) จำเป็นต้องอาศัยข้อมูลที่ชัดเจนมากกว่าเพื่อประกอบการตัดสินใจ ผู้จัดการจะต้องใช้เครื่องมือที่มีรายละเอียดมากกว่านี้ เช่น ผู้จัดการสามารถใช้เครื่องมือช่วยเมื่อโครงการพัฒนามาถึงจุดหมายหลักที่สำคัญในการออกรายงานแสดงผลว่าโครงการทำงานได้สำเร็จตามกำหนดเวลาและงบประมาณหรือไม่ และอาจจะใช้โปรแกรมระบบงานประยุกต์ (application) ในการแทรกรายงานข้อสังเกตเพื่ออธิบายประเด็นหรือปัญหาที่มีผลกระทบกับโครงการ อนึ่ง ฝ่ายจัดการควรจะสร้างการควบคุมการเข้าถึงที่เหมาะสม และจัดทำขั้นตอนการปฏิบัติงานในการสำรองข้อมูลเพื่อให้เกิดความมั่นใจด้านการรักษาความปลอดภัยและความน่าเชื่อถือของเครื่องมือในการบริหารจัดการโครงการที่สำคัญเหล่านี้

(1) ตาราง GANTT CHARTS

ผู้จัดการสามารถใช้ Gantt charts ข้างท้ายนี้ในการติดตามความคืบหน้าของชิ้นงานต่างๆ ของโครงการได้ เพราะว่าตารางได้แสดงให้เห็นความสัมพันธ์ของการดำเนินการที่เป็นไปตามเป้าหมายหลักต่างๆ ทางแนวตั้งของตาราง และแสดงระยะเวลาประมาณการไว้ในแนวนอน ซึ่งง่ายต่อการใช้งาน แต่ไม่สามารถแสดงความสัมพันธ์และปัญหาในการดำเนินงานต่างๆ ที่เกี่ยวข้องกันได้

Gantt Chart	Jan	Feb	Mar	Apr
Initiation Phase	xxxxxxxx			
Planning Phase	===	=======		
Design Phase		----	----------	
Development Phase			----	----------
Scheduled: ----- Started: ===== Completed: xxxxx				

(2) เทคนิคในการสอบทานผลการประเมินโครงการ

ผู้จัดการสามารถใช้เทคนิคในการสอบทานผลการประเมินโครงการ (PERT) ร่วมกับGantt chart เพื่อกำหนดและบริหารชิ้นงานของโครงการที่เกี่ยวข้องกันได้ เพราะว่า PERT จะแสดงข้อมูลของชิ้นงานโครงการ ความสัมพันธ์ระหว่างกัน และประมาณการเวลาที่ต้องใช้ในรูปแบบของแผนผังแสดงเครือข่ายการสื่อสาร ทำให้ผู้ใช้งานสามารถมองเห็นภาพที่ชัดเจนของการเชื่อมต่อกันระหว่าง phases ของโครงการและจุดหมายหลักสำคัญๆ ของโครงการ

(3) กลุ่มเครื่องมือ (Groupware)

เครื่องมือที่ใช้บริหาร โครงการรวมถึงกลุ่มเครื่องมือ (Groupware)บางครั้งก็เรียกว่า software ร่วม ซึ่งเป็นการรวมตัวกันของ software เพื่อช่วยอำนวยความสะดวกในการสื่อสารและแลกเปลี่ยนข้อมูลระหว่างคณะทำงานในโครงการมีความสามารถในการให้บริการจดหมายอิเล็กทรอนิกส์ ปฏิทินการนัดหมาย และการจัดทำเอกสารประกอบการบริหารงานเพื่อเพิ่มผลผลิตของงาน ทั้งนี้เครื่องมือดังกล่าวมักจะใช้กับเครือข่ายการสื่อสารแบบปิดคือ LAN หรือ WAN เพราะว่าองค์กรสามารถปรับปรุงแก้ไขข้อมูลได้ง่ายกว่าการปรับปรุงข้อมูลงานที่สื่อสารผ่านเครือข่าย Internet (อย่างไรก็ดีการสื่อสารข้อมูลในรูปแบบ XML ผ่านเครือข่าย Internet ก็เริ่มได้รับความนิยมมากขึ้นแล้ว)

<u>หมายเหตุ</u> ผู้ตรวจสอบควรประเมินประสิทธิภาพของเครื่องมือบริหาร โครงการโดยการตรวจสอบความถูกต้องในขั้นตอนการนำข้อมูลเข้าและประเมินความซับซ้อนของแผนงานโครงการประกอบด้วย เพราะว่าการนำเข้าข้อมูลของโครงการที่ไม่ชัดเจนหรือไม่ตรงกับเป้าหมายที่ตั้ง

ไว้ทำให้ได้แผนงานที่ไม่มีความเป็นไปได้และการจัดทำแผนที่มีความซับซ้อนมากเกินไปทำให้เกิดปัญหาในการทำความเข้าใจและลดประสิทธิภาพในการดำเนินการตามแผนงานดังกล่าว

2.1.4 ความมีประสิทธิผลของการบริหารโครงการ

มีหลากหลายวิธีการในการเพิ่มประสิทธิภาพและทักษะในการบริหารโครงการขององค์กร โดยทั่วไปแบ่งออกเป็น 2 แนวทางคือ 1) การฝึกอบรมบุคลากรที่ปฏิบัติงานโครงการ 2) การพัฒนาเทคนิคเพื่อใช้ในการบริหารโครงการ ตัวอย่างที่จะกล่าวถึง 2 ตัวอย่างต่อไปนี้ ไม่ครอบคลุมวิธีการในการเพิ่มประสิทธิผลของการบริหารโครงการทั้งหมด หากมีวัตถุประสงค์เพื่อช่วยให้เห็นภาพของเทคนิคที่ใช้ในการบริหารโครงการชัดเจนขึ้น

(1) แบบจำลองที่ใช้วัดเมื่องานสำเร็จ (Capability Maturity Model-CMM)

Carnegie Mellon University Software Engineering Institution ได้พัฒนา CMM ขึ้นมาเพื่อช่วยองค์กรในการประเมินและการเพิ่มประสิทธิภาพในขั้นตอนการบริหารโครงการ และได้แบ่งระดับความสามารถในการพัฒนา software ขององค์กรเป็น 5 ระดับ โดยเริ่มจากระดับที่ 1 และสามารถพัฒนาความสามารถขึ้นไปได้ถึงระดับที่ 5 การกำหนดลักษณะมีดังนี้

- Initial ระดับเริ่มต้นใช้เทคนิคการพัฒนาที่พัฒนาขึ้นใช้เฉพาะกิจและมีขั้นตอนการดำเนินงานที่เป็นมาตรฐานในวงจำกัด

- Repeatable ระดับที่สองมีการวางแผนงานชั้นต้น มีรายละเอียดของกรอบเวลา และขั้นตอนปฏิบัติงานในการเฝ้าติดตามดูแล (มีระบบควบคุม เช่น ข้อกำหนด configuration การควบคุมดูแลผู้รับช่วงในการพัฒนา การวางแผนโครงการด้วย software การติดตามความคืบหน้าขั้นตอนการปฏิบัติงานในการควบคุมดูแล และการรับประกันคุณภาพของ software)

- Defined ระดับที่สาม มีกระบวนการบริหาร มาตรฐานการพัฒนา และขั้นตอนการปฏิบัติงานที่ผ่านการอนุมัติอย่างเป็นทางการ และมีการปรับปรุงรายละเอียดอื่นๆ ให้ตรงกับข้อกำหนดของแต่ละโครงการ (มีกระบวนการที่มุ่งเน้นไปที่ประเด็นปัญหาของโครงการและองค์กร การฝึกอบรม มีการใช้ software ในการบริหาร การพัฒนา software ด้วยเทคโนโลยีใหม่ การประสานงานระหว่างกลุ่ม และการเปรียบเทียบผลงานกับผู้ให้บริการรายอื่น)

- Managed ระดับที่สี่ ฝ่ายจัดการสามารถตรวจวัด เข้าใจ และสามารถควบคุมขั้นตอนปฏิบัติในการพัฒนาโครงการและคุณภาพของผลิตภัณฑ์ได้ (มีการบริหารและจัดการเกี่ยวกับคุณภาพของผลิตภัณฑ์)

- Optimizing ระดับที่ห้า มีการใช้เทคนิคในการติดต่อสื่อสารที่มีประสิทธิภาพ มีความคิดเห็นใหม่ๆเชิงสร้างสรรค์ และมีเทคโนโลยีที่จะช่วยพัฒนาวิธีการทำงานและผลิตภัณฑ์ได้อย่างต่อเนื่อง (มีการป้องกันความบกพร่อง ควบคุมการเปลี่ยนแปลงของเทคโนโลยี และมีการบริหารขั้นตอนในการเปลี่ยนแปลงต่างๆ)

(2) มาตรฐานองค์กรระหว่างประเทศ (ISO)

ISO ประกอบด้วยสถาบันมาตรฐานต่าง ๆ จากทั่วโลก เป็นองค์กรที่ไม่ใช่รัฐบาล ประมาณ 150 องค์กร และมีผู้แทนจากทั้งภาครัฐและเอกชนเข้าร่วม และ เป้าหมายหลักขององค์กร คือ ต้องอำนวยความสะดวกในการพัฒนาและประสานงานเกี่ยวกับมาตรฐานต่างๆ ในการผลิตและการให้บริการเพื่อส่งเสริมการค้าภาคเอกชนและการพัฒนากฎหมายของหน่วยงานภาครัฐ

มาตรฐานที่ ISO ดำเนินการมีทั้งมาตรฐานการดำเนินงานสำหรับผลิตภัณฑ์และการดำเนินงานที่เน้นไปในหัวข้อเฉพาะเป็นพิเศษ และการออกมาตรฐานที่เป็นเรื่องทั่วไป แต่ ISO ไม่ได้ให้บริการในการตรวจสอบการดำเนินงานตามมาตรฐาน ดังนั้นจึงมีหน่วยงานเอกชนและภาครัฐ (ในบางประเทศ) เป็นผู้ดำเนินการแทน โดยมีมาตรฐานที่เกี่ยวข้องคือ ISO 9001 ด้วย ซึ่งกล่าวถึงแนวทางในการบริหารงานออกแบบ การพัฒนา ผลิตภัณฑ์ การติดตั้ง และกิจกรรมการให้บริการ และ ISO 9000-3 ซึ่งใช้งานร่วมกับ ISO 9001 เพื่อช่วยให้ผู้บริหารโครงการสามารถนำแนวทางไปใช้กับสภาพแวดล้อมของการพัฒนา software

2.2 การพัฒนา

สรุปแนวทางการปฏิบัติ

สถาบันการเงินควรสร้างระเบียบวิธีการพัฒนาระบบงานและโปรแกรมที่เหมาะสม ซึ่งมีวิธีการที่เหมาะสมกับลักษณะและความเสี่ยงของโครงการ ดังต่อไปนี้

- แผนงานโครงการ
- การกำหนดความคาดหวังของโครงการ
- มาตรฐานของโครงการและขั้นตอนการปฏิบัติงาน
- ข้อกำหนดใน phases ของการส่งมอบรวมถึงการรับประกันคุณภาพว่าสิ่งที่ส่งมอบเป็นไปตามกฎหมายและระเบียบกฎเกณฑ์ของหน่วยงานภาครัฐ
- การพัฒนาคุณสมบัติในการรักษาความปลอดภัย การตรวจสอบ และการควบคุมที่เป็นแบบอัตโนมัติ
- มาตรฐานและวิธีปฏิบัติในการรับประกันคุณภาพ การบริหารความเสี่ยง และการทดสอบ
- การมีส่วนร่วมของผู้ที่มีส่วนเกี่ยวข้องทั้งหมด
- เทคนิคในการสื่อสารโครงการ

โครงการพัฒนาเกี่ยวข้องกับการสร้าง Softwareใหม่ หรือการเชื่อมระบบงานเข้าด้วยกัน และ**การพัฒนาอาจจะดำเนินการเองหรือว่าจ้างบุคคลภายนอกก็ได้** และตามปกติองค์กรจะเลือกใช้วิธีการบริหารโครงการพัฒนาอย่างเป็นระบบ โดยการแบ่งแยกโครงการขนาดใหญ่และซับซ้อนออกเป็นงานเล็ก ๆ เป็นส่วน ๆ เพื่อง่ายแก่การจัดการ

โดยปกติแล้วองค์กรจะเลือกใช้ SDLC ในการพัฒนา software ที่ทำงานร่วมกับระบบคอมพิวเตอร์ mainframe เนื่องจากมีรายละเอียดของข้อกำหนดเกี่ยวกับคุณสมบัติของระบบงาน (ถูกจำกัดตามการประมวลผลและการออกรายงาน) และการรักษาความปลอดภัย (ถูกจำกัดเพราะเป็นระบบปิด) นอกจากนี้คอมพิวเตอร์ mainframe ตั้งอยู่ในเขตหวงห้ามและมีผู้เข้าถึงด้านกายภาพ ด้านตรรกะและระบบข้อมูลได้น้อยมาก สำหรับระบบแม่ข่ายลูกข่าย client/server ซึ่งมี user จำนวนมาก และระบบงานมีคุณสมบัติในการให้บริการที่มากยิ่งขึ้นต้องมีระบบการควบคุมภายในที่มากขึ้นด้วย

สำหรับเทคนิคในการพัฒนา เช่น spiral, iterative, and modified SDLC methodologies เป็นต้น เทคนิคดังกล่าว มีส่วนเกี่ยวข้องกับความสำเร็จของโครงการ ช่วยลดความเสี่ยง สร้างความมั่นใจว่า ตลอดระยะเวลาการดำเนินโครงการ ความต้องการของผู้เกี่ยวข้องทุกฝ่าย (user ผู้ตรวจสอบ ผู้บริหารระบบความปลอดภัย designer ผู้พัฒนาระบบ และผู้เชี่ยวชาญของระบบ) ที่ระบุไว้ได้รับการรวบรวมเพื่อใช้ประกอบการพิจารณาอย่างครบถ้วน การมีส่วนร่วมของทุกฝ่ายที่เกี่ยวข้องตลอดระยะเวลาการดำเนินโครงการ ทำให้ทราบถึงปัญหาและสามารถพิจารณาแนวทางแก้ไขได้ทันเวลา นอกจากนี้มีวิธีการใหม่คือการสร้างตัวต้นแบบตั้งแต่ phases แรกเพื่อจะได้ช่วยให้ user สามารถเห็นภาพของระบบและการใช้งานภายหลังติดตั้งระบบได้ก่อนเวลาจริง

มาตรฐานการพัฒนา

องค์กรควรจะสร้าง**มาตรฐานการพัฒนา**ขึ้น โดยมีองค์ประกอบ**อย่างน้อย 3 ประการ**คือ **1) การบริหารโครงการ** ซึ่งกล่าวถึงแนวทางการบริหารโครงการ ความเสี่ยง และการอนุมัติโครงการ **2) การควบคุมระบบ** ซึ่งกล่าวถึงหน้าที่การทำงาน การรักษาความปลอดภัย และการควบคุมแบบอัตโนมัติของระบบงาน **3) การรับประกันคุณภาพ** ซึ่งกล่าวถึง ความถูกต้องของสมมติฐานของโครงการ การปฏิบัติงานตามมาตรฐานของโครงการ และการทดสอบผลการปฏิบัติงานของโครงการ

มาตรฐานการพัฒนาต้องครอบคลุมถึงการบริหารการเปลี่ยนแปลงในระหว่างขั้นตอนการพัฒนา เช่น scope creep คือ การที่ผู้พัฒนาได้รับการร้องขอให้เพิ่มหรือปรับปรุงการทำงานของโปรแกรมในขณะที่อยู่ระหว่างการพัฒนา และถึงแม้ว่าการเพิ่มหรือปรับปรุงต่างๆ เช่น คุณสมบัติของระบบในการให้บริการ การรักษาความปลอดภัย และระบบการควบคุม อาจจะมีความเหมาะสมอยู่แล้ว แต่การเปลี่ยนแปลงโดยไม่มีการควบคุมอาจจะมีผลกระทบต่อขั้นตอนในการพัฒนาได้ ดังนั้นจึงควรกำหนดเวลา cut-off คือการที่คำขอเปลี่ยนแปลงแก้ไขจะถูกเลื่อนไปดำเนินการในขั้นตอนถัดไปแทนการดำเนินการในงวดนี้ นอกจากนี้องค์กรที่อาศัยระบบรายงานผลจาก spreadsheet และระบบ database ควรทำการทดสอบ จัดทำเอกสารประกอบ มีขั้นตอนการควบคุมการเปลี่ยนแปลง และจัดทำระบบสำรองข้อมูลไว้ด้วย

2.2.1 วงจรในการพัฒนาระบบงาน (SDLC)

วงจรการพัฒนา SDLC เป็นเทคนิคการบริหารโครงการอย่างหนึ่งที่แบ่งแยกโครงการที่ซับซ้อนออกเป็นงานย่อย ๆ เป็นส่วน ๆ ที่ง่ายแก่การจัดการ ประกอบไปด้วยขั้นตอนเริ่มต้นยื่นความต้องการ การวางแผน การออกแบบ การพัฒนา การทดสอบ การนำไปใช้ และการบำรุงรักษา อย่างไรก็ตาม แต่ละขั้นตอนอาจจะถูกปรับปรุงให้เหมาะสมกับประเภทของธุรกิจด้วย

หมายเหตุ ผู้ตรวจสอบควรจะเน้นในการประเมินคุณภาพ (ความลึก คุณภาพ และความซับซ้อน) ของเทคนิคการบริหารโครงการว่าเหมาะสมกับลักษณะและความเสี่ยงของโครงการหรือไม่ โดยเน้นการประเมินไปที่คุณภาพของการบริหารโครงการในขั้นตอนของการพัฒนา การจัดหา การบำรุงรักษา เป็นหลัก

(1) ขั้นตอนเริ่มต้น

ขั้นตอนเริ่มต้นคือการขอเพิ่ม ขอปรับปรุงคุณสมบัติ หรือ ขอแก้ไขเปลี่ยนแปลงระบบที่นำออกใช้งานแล้วโดยการนำเสนอข้อมูลเกี่ยวกับความจำเป็นทางธุรกิจ (business case) ซึ่งควรให้ข้อมูลเกี่ยวกับวัตถุประสงค์ ประโยชน์ที่คาดหวังไว้ และเหตุผลว่าระบบงานใหม่จะไปสนับสนุนกลยุทธ์ทางธุรกิจขององค์กรได้อย่างไร อนึ่งควรมีการนำเสนอทางเลือกอื่นพร้อมทั้งข้อมูลที่เกี่ยวข้องทั้งหมดด้วย

ข้อมูลจาก business case ช่วยให้ฝ่ายจัดการได้เห็นประเด็นว่าโครงการมีความเป็นไปได้หรือไม่ และสามารถประหยัดงบประมาณในการศึกษาความเป็นไปได้ของโครงการที่ไม่เหมาะสม ดังนั้น ฝ่ายจัดการควรจะพิจารณาข้อมูลจากทุกฝ่ายงานที่เกี่ยวข้อง และควรพิจารณาอย่างใกล้ชิดถึงความจำเป็นในการพัฒนาคุณสมบัติในการให้บริการใดเพิ่มเติม เพื่อประหยัดเวลา ค่าใช้จ่ายจำนวนมากโดยไม่จำเป็น

เมื่อได้รับเอกสารอนุมัติโครงการชั้นต้นแล้ว ขั้นตอนต่อไปคือการจัดเก็บเอกสารไว้ประกอบหลักฐานในการดำเนินการในขั้นตอนการศึกษาความเป็นไปได้ต่อไป ซึ่งจะเน้นที่การตรวจสอบความถูกต้องของสมมติฐานขั้นต้นและกำหนดรายละเอียดของทรัพยากรที่จะต้องใช้อย่างละเอียดต่อไป

ประเด็นหลักๆ ที่องค์กรควรจะพิจารณาในการจัดทำเอกสารประกอบการพิจารณาความเป็นไปได้ของโครงการ มี 4 ข้อ ดังนี้

1. การพิจารณาด้านธุรกิจ

- วัตถุประสงค์และเป้าหมายทางกลยุทธ์ด้านทางธุรกิจและ IT
- ผลประโยชน์ที่คาดว่าจะได้เมื่อเปรียบเทียบกับ IT ที่ใช้อยู่ในปัจจุบัน
- การเปลี่ยนแปลงภายในองค์กรในเรื่องสิ่งอำนวยความสะดวก หรือการเพิ่ม/ลด user ผู้เชี่ยวชาญ หรือผู้จัดการ
- งบประมาณ ตารางการปฏิบัติงาน และข้อจำกัดของบุคลากร

- ความเป็นไปได้ของปัญหาที่เกี่ยวข้องกับธุรกิจ กฎหมาย หรือหน่วยงานภาครัฐซึ่งอาจจะมีผลกระทบกับความเป็นได้ของโครงการ

2. การกำหนดภาระหน้าที่ในการปฏิบัติงานของระบบ

- ความต้องการของ user
- ความต้องการของระบบควบคุมภายในและระบบการรักษาความปลอดภัยข้อมูล
- ความต้องการเกี่ยวกับชนิด กำลังการผลิต และประสิทธิภาพในการปฏิบัติงานของ ระบบปฏิบัติการ ระบบฐานข้อมูล และระบบสำรองข้อมูล
- รูปแบบของเครือข่ายที่ต้องการ (stand-alone, LAN, WAN หรือระบบเครือข่ายภายนอก)
- ความต้องการทางด้านเครือข่าย (จำนวน user ชนิด ปริมาณ ความถี่ในการโอนข้อมูล)
- ความต้องการเกี่ยวกับการเชื่อมต่อกับระบบงานอื่น (โปรแกรมระบบงานภายในหรือโปรแกรมระบบงานภายนอก)

3. ปัจจัยที่จำเป็นต่อโครงการ

- ระเบียบวิธีการบริหารโครงการ
- ระเบียบวิธีการบริหารความเสี่ยง
- ประมาณการวันที่สำเร็จของโครงการและขั้นตอนหลักๆของโครงการ
- ประมาณการต้นทุนและจำนวน phases หลักๆของโครงการ

4. การวิเคราะห์ต้นทุนและประโยชน์ที่ได้รับ

- อายุการใช้งานของผลิตภัณฑ์ที่คาดไว้
- ทางเลือกในการพัฒนาโครงการ (ซื้อหรือพัฒนาเอง)
- ค่าใช้จ่ายของโครงการแบบจ่ายครั้งเดียว (บุคลากร hardware, software และค่าใช้จ่ายต่าง ๆ)
- ค่าใช้จ่ายของโครงการแบบจ่ายอย่างต่อเนื่อง (บุคลากร การบำรุงรักษา การติดต่อสื่อสาร และค่าใช้จ่ายต่าง ๆ)
- ประโยชน์ที่จับต้องได้ (รายได้เพิ่มขึ้น ต้นทุนลดลง ผลตอบแทนจากการลงทุน)

- ประโยชน์ที่ไม่สามารถจับต้องได้ (ปรับปรุงทัศนคติของสาธารณะชน หรือมีข้อมูลที่ใช้ประโยชน์ได้ดีขึ้น)

ผลการศึกษาความเป็นไปได้ที่นำเสนอให้คณะกรรมการบริหารและคณะผู้บริหารระดับสูงพิจารณาอนุมัติควรจะต้องให้ภาพรวมของโครงการ แสดงต้นทุนและผลประโยชน์ตอบแทน มีข้อมูลด้านเทคนิค และ operations พร้อมทั้งแนวทางในการอนุมัติหรือปฏิเสธ และมีการลงนามรับทราบโดยผู้ที่ได้รับผลกระทบ เพื่อใช้เป็นเอกสารเริ่มต้นใน phases การวางแผนต่อไป

(2) ขั้นตอนการวางแผน

ขั้นตอนการวางแผนเป็นขั้นตอนที่สำคัญที่สุดในการพัฒนา การจัดหา และการบำรุงรักษาโครงการ ดังนั้นการวางแผนอย่างระมัดระวัง (เหมาะสมกับลักษณะและความเสี่ยงของโครงการ)ในช่วงเริ่มต้นของโครงการมีความจำเป็นอย่างยิ่งในการประสานงานกิจกรรมต่างๆ และการบริหารความเสี่ยงได้อย่างมีประสิทธิภาพ

แผนงานโครงการจะช่วยปรับปรุงข้อมูลในการเริ่มต้นโครงการในการชี้กิจกรรมเฉพาะและทรัพยากรที่ต้องการใช้ในโครงการ โดยมีส่วนสำคัญซึ่งผู้จัดการโครงการจะต้องดำเนินการ คือ การประสานงานในการหารือกับ user ผู้ตรวจสอบ ผู้รักษาความปลอดภัย ผู้ออกแบบ ผู้พัฒนาและผู้ดูแลเครือข่ายเพื่อกำหนดและจัดทำเอกสารประกอบความต้องการเกี่ยวกับคุณสมบัติในการทำงานของระบบ การรักษาความปลอดภัย และระบบเครือข่าย

องค์ประกอบต่างๆ ที่องค์กรควรคำนึงถึงในการวางแผนโครงการ มีดังนี้

- ภาพรวมของโครงการ (Project Overview) แสดงให้เห็นโครงร่างของแผนงานโครงการ และควรมีรายละเอียดของโครงการ ผู้สนับสนุนโครงการ ผู้จัดการโครงการ เป้าหมายของโครงการ ข้อมูลเบื้องหลัง และกลยุทธ์ในการพัฒนา

- บทบาทและหน้าที่ความรับผิดชอบ (Roles and Responsibilities) ควรกำหนดความรับผิดชอบหลักของบุคลากรที่สำคัญคือ ผู้สนับสนุนโครงการ ผู้จัดการ และสมาชิกในโครงการ รวมถึงการกำหนดความรับผิดชอบของผู้ให้บริการภายนอก (TSP) ผู้ตรวจสอบภายใน ผู้ดูแลระบบรักษาความปลอดภัย และระบบเครือข่าย

- การติดต่อสื่อสาร (Communication) การติดต่อสื่อสารที่ได้กำหนดไว้ดีแล้วจะช่วยเพิ่มประสิทธิผลในการพัฒนาโครงการ ดังนั้นฝ่ายจัดการควรจัดให้มีขั้นตอนการปฏิบัติงานเกี่ยวกับการรวบรวมและแจกจ่ายข้อมูล มีการจัดทำรูปแบบรายงานที่เป็นมาตรฐานเดียวกันและ

สามารถเปรียบเทียบกันได้ มีข้อกำหนดในการรายงานข้อมูลที่ชัดเจน มีตารางการประชุมที่อำนวยความสะดวกในการติดต่อสื่อสารงานโครงการ

- สิ่งส่งมอบที่กำหนดไว้ (Defined Deliverables) ความคาดหวังที่กำหนดไว้อย่างชัดเจนถือเป็นสิ่งจำเป็นอันดับแรกในการดำเนินการโครงการให้สำเร็จ ดังนั้นผู้ที่เกี่ยวข้องทั้งหมดในการพัฒนาโครงการจึงควรช่วยกำหนดวัตถุประสงค์โครงการที่แท้จริง มีข้อมูลที่ถูกต้อง กำหนดความต้องการของระบบที่ชัดเจน ข้อกำหนดในการเชื่อมต่อระบบ และเกณฑ์ในการยอมรับตามวัตถุประสงค์

ฝ่ายจัดการควรจะสร้างเกณฑ์ในการยอมรับในแต่ละ phases ของโครงการ และควรทบทวนขั้นตอนในการอนุมัติเพื่อให้เกิดความมั่นใจว่าทีมงานได้ดำเนินการเสร็จสิ้นในแต่ละ phases แล้วก่อนที่จะขยับไปดำเนินการในขั้นตอนต่อไป

- ข้อกำหนดในการควบคุม (Control Requirements) **ส่วนที่สำคัญมากของกระบวนการวางแผน คือ การออกแบบและสร้างระบบการควบคุมและการรักษาความปลอดภัยอัตโนมัติเข้าไปในระบบงาน** (การดำเนินการดังกล่าวมักจะไม่สามารถดำเนินการได้ phases การเริ่มต้นโครงการ) ดังนั้นฝ่ายจัดการควรจะพิจารณาประเด็นดังกล่าวและเพิ่มระบบการควบคุมเข้าไปในระบบให้เร็วที่สุดใน phases ใดๆ ก็ตามที่สามารถดำเนินการได้

- การบริหารความเสี่ยง (Risk Management) เป็นส่วนที่สำคัญของขั้นตอนในการวางแผน ดังนั้นองค์กรควรจะสร้างขั้นตอนการดำเนินงานเพื่อให้เกิดความมั่นใจว่าฝ่ายจัดการได้ประเมิน เฝ้าติดตามดูแล และบริหารความเสี่ยงทั้งภายในและภายนอก (ระดับของการยอมรับความเสี่ยง การลดความเสี่ยง และกลยุทธ์ในการโอนย้ายความเสี่ยง) ตลอดช่วงอายุ SDLC

ความเสี่ยงจากภายนอก ได้แก่ ความล้มเหลวของผู้ให้บริการ การเปลี่ยนแปลงด้านกฎหมาย และภัยธรรมชาติ ส่วนความเสี่ยงจากภายในองค์กรได้แก่ การประมาณการต้นทุนที่ผิดพลาดหรือการเปลี่ยนคุณสมบัติในการทำงานของระบบ ความยุ่งยากในการจัดตารางเวลาการปฏิบัติงาน เช่น การเปลี่ยนแปลงบุคลากรโดยไม่คาดหมาย หรือการตั้งสมมุติฐานการพัฒนาที่ไม่ถูกต้อง และความยากของขั้นตอนการปฏิบัติงาน เช่น การติดต่อสื่อสารที่ผิดพลาดหรือไม่สามารถติดต่อได้ หรือ ผู้จัดการโครงการที่ไม่มีประสบการณ์

- การบริหารการเปลี่ยนแปลง (Change Management) การร้องขอเพิ่มหรือปรับปรุงแก้ไขคุณสมบัติในการทำหน้าที่ของระบบงาน (คุณสมบัติของระบบ) ในระหว่าง SDLC สามารถดำเนินการได้แต่จะต้องมีมาตรฐานในการดำเนินงานรองรับ มีการจัดทำเอกสารขออนุญาต

อย่างเป็นทางการ มีตัวแทนจากทุกฝ่ายงานร่วมพิจารณาความเหมาะสมในการเปลี่ยนแปลง และมีวัน cut-off ที่ไม่รับดำเนินการเปลี่ยนแปลงความต้องการของโครงการอีก

- มาตรฐาน (Standards) ที่สามารถใช้ในกิจกรรมการกำกับดูแลโครงการ การควบคุมระบบ และการรับประกันคุณภาพ ควรจะระบุถึงกระบวนงานการคัดเลือกวิธีบริหารโครงการ อำนาจในการอนุมัติ และกระบวนงานบริหารความเสี่ยง สำหรับมาตรฐานในการควบคุมระบบควรจะระบุถึงคุณสมบัติของระบบ การรักษาความปลอดภัย และการควบคุมอัตโนมัติ ส่วนมาตรฐานในการรับประกันคุณภาพควรระบุถึงสมมุติฐานของโครงการที่ใช้ได้ การยึดมั่นในมาตรฐานโครงการและการทดสอบการทำงานทั้งหมด แต่ถ้ามีการเปลี่ยนแปลงแก้ไขฝ่ายจัดการควรจะสอบทาน อนุมัติ และจัดทำเอกสารประกอบสิ่งที่เบี่ยงเบนไปจากมาตรฐานที่กำหนดไว้แล้ว

- การจัดทำเอกสาร (Documentation) ควรกำหนดรูปแบบและระดับของการจัดทำเอกสารที่บุคลากรจะต้องจัดทำขึ้นระหว่างการพัฒนาในแต่ละ phases ของการพัฒนาโครงการ เช่น เอกสารแสดงวัตถุประสงค์ของโครงการ ความต้องการระบบ และกลยุทธ์ในการพัฒนาโครงการตั้งแต่ phasesขั้นเริ่มต้นโครงการ นอกจากนี้ เอกสารประกอบควรจะถูกทบทวนและปรับปรุงแก้ไขตามความจำเป็นตลอดช่วงเวลาการพัฒนาโครงการ เช่น คู่มือการใช้งานเบื้องต้น คู่มือผู้ปฏิบัติงานห้องเครื่องและคู่มือบำรุงรักษาที่ถูกสร้างขึ้นระหว่างขั้นตอนการออกแบบควรจะถูกปรับปรุงแก้ไขระหว่าง phasesของการพัฒนา การทดสอบ และขั้นตอนการนำออกใช้งาน

- การกำหนดตารางเวลาของโครงการ (Scheduling) ฝ่ายจัดการควรจะกำหนดตารางเวลาแล้วเสร็จของ phases ต่างๆ พร้อมกับชิ้นงานย่อยใน phases ต่างๆ และแม้ว่าการจัดตารางเวลาจะได้มีการพิจารณาถึงความไม่แน่นอนและมีความยืดหยุ่นในระดับหนึ่งแล้ว แต่เมื่อโครงการดำเนินการไปมากและมีความชัดเจนมากขึ้นแล้ว ตารางกำหนดเวลาก็จะลดความยืดหยุ่นเป็นสัดส่วนผกผันกันไปเท่านั้น

- งบประมาณ (Budget) ผู้จัดการควรประมาณการงบประมาณที่ต้องใช้ในขั้นแรกเริ่มโครงการเพื่อดูความเป็นไปได้ของโครงการ และควรติดตามดูแลการใช้งบประมาณทั้งหมดตลอดโครงการ (สามารถปรับเปลี่ยนงบประมาณได้ถ้ามีความจำเป็น) และจัดเก็บข้อมูลไว้เพื่อวิเคราะห์ผลแตกต่างจากประมาณการครั้งแรก อนึ่งสำหรับการพิจารณาค่าใช้จ่ายเกี่ยวกับบุคลากรและการใช้บริการจากบุคคลภายนอก ควรจะต้องมีการคิดค่าใช้จ่ายเกี่ยวกับ การเช่าใช้พื้นที่ทำงาน hardware และ software รวมเข้าเป็นต้นทุนดำเนินการด้วย

- การทดสอบ (Testing) ฝ่ายจัดการควรจะพัฒนาแผนการทดสอบโดยการกำหนดวัตถุประสงค์ในการทดสอบและจัดตารางเวลาทดสอบให้เสร็จใน phasesขั้นตอนเริ่มต้นของโครงการและจำเป็นต้องให้ user ผู้ออกแบบ ผู้พัฒนา และผู้เชี่ยวชาญระบบมีส่วนเกี่ยวข้องในกระบวนการทดสอบด้วย

- การพัฒนาบุคลากร (Staff Development) ฝ่ายจัดการควรจะพัฒนาแผนการฝึกอบรมที่แสดงให้เห็นความจำเป็นในการฝึกอบรม และตารางเวลาในการฝึกอบรมเพื่อให้เกิดความมั่นใจว่า user จะสามารถใช้งานและบำรุงรักษาระบบงานได้หลังจากมีการใช้ระบบงานจริงแล้ว

(3) ขั้นตอนออกแบบ

ขั้นตอนออกแบบคือการปรับเปลี่ยนความต้องการข้อมูล คุณสมบัติของระบบ ข้อกำหนดของระบบเครือข่าย ที่ได้กำหนดไว้ในระหว่าง phases ขั้นตอนแรก และ ขั้นตอนการวางแผน ออกมาเป็นข้อกำหนดในการออกแบบสำหรับผู้พัฒนาระบบใช้ในการเขียนโปรแกรมใน phases ของการพัฒนาระบบ การออกแบบโปรแกรมจะถูกสร้างขึ้นมาหลายรูปแบบ เช่น วิธีออกแบบจากบนลงล่างซึ่งผู้ออกแบบจะกำหนดและเชื่อมโยงส่วนประกอบหลักของโปรแกรมกับจุดเชื่อมต่อแล้วขยายต่อภาพแผนผังลงไปสู่ระบบงานขนาดเล็กและจุดเชื่อมต่อ หรืออีกวิธีใช้ การออกแบบจากล่างขึ้นบนซึ่งผู้ออกแบบจะดำเนินการจากการเชื่อมต่อองค์ประกอบย่อยๆ และจุดเชื่อมต่อต่างๆเข้าด้วยกันก่อนที่จะขยายภาพความสัมพันธ์จนเป็นภาพใหญ่ขึ้น

เทคนิคการออกแบบร่วมสมัยในปัจจุบันมักจะใช้เครื่องมือในการสร้างแบบจำลองขึ้นมาทดลองดำเนินการ ซึ่งมีการจำลองทั้งหน้าจอแสดงผลของระบบงาน แผนผังของระบบฐานข้อมูลและโครงสร้างพื้นฐาน ดังนั้นผู้ที่เกี่ยวข้องทั้งหมดคือ user ผู้ออกแบบ ผู้พัฒนา ผู้จัดการระบบฐานข้อมูล และผู้บริหารเครือข่ายควรจะร่วมกันทดสอบและปรับปรุงแบบจำลองบ่อยๆ จนกว่าแบบจำลองจะถูกต้องตามความต้องการของทุกฝ่าย ส่วนบุคลากรด้านการตรวจสอบ การรักษาความปลอดภัย และการรับประกันคุณภาพควรเข้าร่วมทดสอบเฉพาะในขั้นตอนของการอนุมัติเท่านั้น

ฝ่ายจัดการควรจะขยันทำการทดสอบเมื่อใช้เครื่องมือในการสร้างแบบจำลองในการพัฒนาระบบควบคุม เพราะว่าบุคลากรมักจะต่อต้านการเพิ่มระบบการควบคุมที่กระทำขึ้นในภายหลัง phases การออกแบบระบบ

ผู้ออกแบบระบบควรจัดทำเอกสารประกอบการออกแบบอย่างระมัดระวัง เพราะว่าเอกสารดังกล่าวจะเป็นประโยชน์ในการพัฒนาและปรับปรุงโปรแกรมในภายหลัง และยังเป็นหลักฐานว่าโปรแกรมมีคุณสมบัติตรงตามวัตถุประสงค์เริ่มแรกในการพัฒนาโปรแกรม

องค์กรควรจะกำหนดแผนการทดสอบเริ่มต้น การแปลงโครงสร้างของข้อมูล การติดตั้งและใช้งาน และแผนการฝึกอบรมในระหว่าง phases ของการออกแบบนี้ พร้อมทั้งจัดทำร่างคู่มือสำหรับ user ผู้ปฏิบัติงานประจำวัน และคู่มือการบำรุงรักษาไปพร้อมกันด้วย

มาตรฐานการควบคุมโปรแกรมระบบงานประยุกต์

การควบคุมโปรแกรมระบบประยุกต์รวมความไปถึงแนวนโยบายและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับกิจกรรมของ user และระบบควบคุมอัตโนมัติที่ออกแบบไว้ภายในโปรแกรมระบบงานประยุกต์ (ระบบการควบคุมอาจจะเป็นแบบประมวลผลทันทีหรือไม่ทันทีก็ได้) แต่จะต้องกล่าวถึงมาตรฐานการปฏิบัติงานที่ฝ่ายจัดการจะต้องมีวิธีการอนุมัติรายการที่เหมาะสม และจะต้องมีการควบคุมการใช้สิทธิพิเศษที่สูงกว่าในการก้าวข้ามจากระบบการควบคุมปกติ ผู้ตรวจสอบควรศึกษาเพิ่มเติมจากคู่มือตรวจสอบการปฏิบัติการ

การออกแบบระบบการรักษาความปลอดภัย การตรวจสอบและการควบคุมแบบอัตโนมัติไว้ในโปรแกรมระบบงานได้อย่างเหมาะสมเป็นงานที่ท้าทายมาก เพราะว่าความซับซ้อนของการไหลเวียนของข้อมูล กลไกทางตรรกะของโปรแกรม การเชื่อมต่อระหว่างเครื่องแม่ข่ายและลูกข่ายและการเชื่อมต่อกับเครือข่ายการสื่อสารทำให้องค์กรไม่สามารถกำหนดจุดควบคุมและคุณลักษณะในการทำงานที่เหมาะสมได้จนกว่าการดำเนินงานได้ผ่านมาถึง phases การออกแบบ และการพัฒนาระบบ แต่อย่างไรก็ตาม ถ้าองค์กรยังสามารถเสริมสร้างระบบรักษาความปลอดภัย การตรวจสอบ และการควบคุมแบบอัตโนมัติเข้าไปในช่วงเริ่มต้นของการเริ่มต้นโครงการ ระบบยังมีความปลอดภัย มีความถูกต้องและน่าเชื่อถือของข้อมูลได้ แต่ถ้าการตรวจสอบพบข้อบกพร่องเกิดขึ้นใน phases ที่นำระบบออกใช้งานจริงแล้ว องค์กรจะต้องเสียค่าใช้จ่ายสูงมาก ใช้เวลานานมาก และได้ระบบควบคุมที่ไม่มีประสิทธิภาพ

มาตรฐานควรจะกำหนดให้ user ผู้บริหารเครือข่าย ผู้ตรวจสอบ และผู้ดูแลระบบรักษาความปลอดภัย เข้าไปมีส่วนร่วมอย่างเหมาะสมใน phases ของการเริ่มต้นโครงการ (กลุ่มผู้เกี่ยวข้องทั้งหมดควรจะมีส่วนร่วมตลอดโครงการในการปรับปรุงและทดสอบระบบ) ซึ่งจะช่วยให้ผู้บริหารโครงการสามารถดูแลระบบการรักษาความปลอดภัยในภาพรวม การตรวจสอบ และข้อกำหนดในการควบคุมภายในได้ดียิ่งขึ้น

มาตรฐานการควบคุมโปรแกรมระบบงานช่วยเสริมสร้างระบบรักษาความปลอดภัย ความถูกต้องของข้อมูล และความน่าเชื่อถือของข้อมูลให้กับระบบงานโดยการให้ความมั่นใจว่าการนำเข้าข้อมูล การประมวลผลข้อมูล และผลลัพธ์ของข้อมูล ได้รับการอนุมัติ มีความถูกต้อง

สมบูรณ์ และปลอดภัย ทั้งนี้เพราว่ามีระบบควบคุมถึง 3 ประเภท คือ 1) การป้องกันซึ่งออกแบบมาเพื่อป้องกันการทำรายการโดยไม่มีสิทธิหรือการนำเข้าข้อมูลที่ไม่ถูกต้อง 2) การตรวจจับใช้ในการค้นหาการเข้าสู่ระบบอย่างไม่ถูกต้องหรือไม่ได้รับอนุญาต 3) การแก้ไขใช้ในการกู้คืนจากสถานการณ์ที่ไม่พึงประสงค์

<u>การควบคุมการนำเข้า</u>

การควบคุมการนำเข้าแบบอัตโนมัติช่วยให้มั่นใจได้ว่าพนักงานได้นำข้อมูลเข้าระบบได้ถูกต้อง ระบบบันทึกข้อมูลนำเข้าได้อย่างเหมาะสม และระบบได้ปฏิเสธ/ยอมรับและบันทึกรายการธุรกรรม และได้จัดเก็บข้อมูลที่ผิดพลาดเพื่อการสอบทานและแก้ไขในภายหลัง ตัวอย่างของการควบคุมการนำเข้าข้อมูลแบบอัตโนมัติ มีดังนี้

- Check Digits คือการตรวจสอบตัวเลขจากการคำนวณทางคณิตศาสตร์เพื่อใช้ในการนำเข้าข้อมูล เช่น เลขที่บัญชี เพื่อยืนยันความถูกต้องของหมายเลขบัญชี โดยเฉพาะตัวเลขหลักสุดท้าย
- Completeness Checks คือการตรวจสอบว่าไม่มีการเว้นช่องว่างของข้อมูลนำเข้า และผลรวมของตัวเลขนำเข้าตรงกับยอดรวมที่กำหนดไว้
- Duplication Checks คือการตรวจสอบว่าไม่มีการนำเข้าข้อมูลที่ซ้ำซ้อนเข้าสู่ระบบ
- Limit Checks คือการตรวจสอบว่าตัวเลขที่ได้ไม่เกินกว่ามูลค่าที่กำหนดไว้ก่อนหน้านี้
- Range Checks คือการตรวจสอบว่าตัวเลขที่นำเข้าอยู่ในช่วงของค่าตัวแปรที่กำหนดไว้ก่อนหน้านี้
- Reasonableness Checks คือการตรวจสอบความสมเหตุผลว่าตัวเลขที่ได้ตรงกับเงื่อนไขที่กำหนดไว้ก่อนหน้านี้แล้ว
- Sequence Checks คือการตรวจสอบว่าตัวเลขได้ถูกนำเข้าหรือประมวลผลตามลำดับที่กำหนดไว้
- Validity Checks คือการตรวจสอบว่าตัวเลขที่นำเข้ามีความถูกต้องตรงตามเงื่อนไขในการนำเข้า

การควบคุมการประมวลผล

การควบคุมการประมวลผลอัตโนมัติช่วยให้เกิดความมั่นใจว่าระบบมีการประมวลผลบันทึกข้อมูลได้อย่างถูกต้อง และมีการปฏิเสธ/ประมวลผลและบันทึกรายการ และการบันทึกข้อผิดพลาดเพื่อสอบทานและแก้ไขในภายหลัง ทั้งนี้ การประมวลผลประกอบไปด้วย การรวมไฟล์ การปรับปรุงข้อมูล การปรับปรุงไฟล์หลักให้เป็นปัจจุบัน และการบำรุงรักษาไฟล์ ตัวอย่างของการควบคุมการประมวลผลมีดังนี้

- Batch Controls คือตรวจสอบความถูกต้องในการประมวลผลเปรียบเทียบกับตัวเลขนำเข้าทั้งหมด เช่น ยอดรวมเงินทั้งหมด จำนวนรายการทั้งหมด เอกสารที่นำเข้าประมวลผลทั้งหมด

- Error Reporting คือรายงานแสดงรายการหรือ Batch ที่เกิดข้อพลาด รายการหรือ Batch ที่เกิดข้อพลาดนั้นจะไม่ถูกประมวลผล และจะถูกตั้งบัญชีพักไว้จนกว่าจะแก้ไขให้ถูกต้อง หรือประมวลผลโดยทำเครื่องหมายไว้เพื่อในการแก้ไขภายหลัง

- Transaction Logs คือรายงานที่ user.ใช้ตรวจสอบบันทึกข้อมูลจากการทำรายการเปรียบเทียบกับเอกสารต้นฉบับ และผู้บริหารระบบใช้เพื่อติดตามข้อผิดพลาด การปฏิบัติงานของ user การใช้ทรัพยากรและการเข้าถึงระบบโดยไม่ได้รับอนุญาต

- Run-to-Run Totals คือการตรวจสอบความถูกต้องของตัวเลขเปรียบเทียบที่เกิดจากการดำเนินการตั้งแต่การนำข้อมูลเข้า ประมวลผล และผลลัพธ์ที่ได้จากการประมวลผล

- Sequence Checks คือการตรวจสอบเพื่อค้นหาและปฏิเสธข้อมูลนำเข้าที่หายไปหรือข้อมูลที่ซ้ำซ้อน

- Interim Files ผู้ปฏิบัติงานประจำได้ใช้ไฟล์ที่สร้างขึ้นแบบอัตโนมัติระหว่างการประมวลผลเพื่อใช้ตรวจสอบความถูกต้องเชื่อถือได้ และความสมบูรณ์ของข้อมูลการประมวลผล

- Backup Files ผู้ปฏิบัติงานประจำได้ใช้ไฟล์หลักชุดสำรองที่สร้างขึ้นแบบอัตโนมัติเมื่อไฟล์ข้อมูลหลักที่ประมวลผลจริงเสียหาย

การควบคุมผลลัพธ์

การควบคุมผลลัพธ์แบบอัตโนมัติช่วยให้แน่ใจว่าระบบมีความปลอดภัยและส่งข้อมูลผลลัพธ์ให้ผู้ใช้ได้อย่างเหมาะสม ตัวอย่างการควบคุมการประมวลผลแบบอัตโนมัติมีดังนี้

- Batch Logs บันทึกการทำรายการ Batch ทั้งหมด ซึ่งผู้รับข้อมูลผลลัพธ์สามารถตรวจสอบผลลัพธ์เปรียบเทียบได้กับบันทึกผลการประมวลผลทั้งหมด

- Distribution Controls คือการควบคุมเพื่อให้เกิดความมั่นใจได้ว่าผลลัพธ์จะถูกแจกจ่ายไปให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ดังนั้นรายชื่อผู้ที่ได้รับผลลัพธ์อัตโนมัติ และการควบคุมการเข้าถึงข้อมูลอิเล็กทรอนิกส์ที่สำคัญ หรือการส่งข้อมูลไปเก็บในรูปของข้อมูลรอการพิมพ์ก็คือตัวอย่างของการควบคุมการแจกจ่ายข้อมูลผลลัพธ์

- Destruction Controls คือการควบคุมในการทำลายข้อมูลอิเล็กทรอนิกส์ที่แจกจ่ายและจัดเก็บอย่างเหมาะสมโดยการบันทึกทับข้อมูลที่หมดอายุแล้วหรือทำลายสภาพของการเป็นสื่อจัดเก็บข้อมูลบนแผ่น disk และเทป ผู้ตรวจสอบควรศึกษาข้อมูลเพิ่มเติมจากคู่มือตรวจสอบการรักษาความปลอดภัยข้อมูล

(4) ขั้นตอนการพัฒนา

ขั้นตอนการพัฒนา คือ การปรับเปลี่ยนข้อกำหนดต่างๆ ออกมาเป็นโปรแกรมที่สามารถดำเนินการได้ ทั้งนี้มาตรฐานการพัฒนาที่มีประสิทธิภาพได้กำหนดให้ผู้พัฒนาและผู้ที่มีส่วนร่วมในโครงการมาร่วมปรึกษาหารือถึงข้อกำหนดในการออกแบบก่อนเริ่มเขียนโปรแกรม เพื่อให้เกิดความมั่นใจว่าผู้พัฒนามีความรูปแบบของโปรแกรมและคุณสมบัติของระบบงานที่ต้องการอย่างชัดเจน

ผู้พัฒนาใช้เทคนิคหลายอย่างในการพัฒนา แต่สำหรับการเขียนโปรแกรมสำหรับการทำรายการธุรกรรมจำนวนมาก เช่น สถาบันการเงิน มีการใช้เทคนิคการเขียนโปรแกรมแบบเป็นลำดับขั้นตอน และต้องเขียนโปรแกรมออกมาเป็นรายบรรทัดต่อบรรทัดแล้วรวมกันเป็นโปรแกรม

วิธีการเขียนโปรแกรมที่เป็นมาตรฐานประกอบด้วยการสร้าง การทดสอบโปรแกรมต้นฉบับ การปรับปรุงแผนการทดสอบ โดยทั่วไปแล้วผู้พัฒนาแต่ละคนจะเขียนและสอบทานในแต่ละส่วนประกอบของโปรแกรมย่อยๆ ซึ่งทำงานเฉพาะส่วนภายในโปรแกรมระบบงาน ส่วนประกอบที่สมบูรณ์จะถูกรวมกันและถูกสอบทานโดยกลุ่มผู้พัฒนาเพื่อให้แน่ใจว่าส่วนประกอบย่อยทุกส่วนทำงานสัมพันธ์กันอย่างเหมาะสม และจะมีกระบวนการทดสอบการทำงานระหว่างกลุ่มและข้ามกลุ่มด้วย

เทคนิคการเขียนโปรแกรมขั้นสูงรวมถึงแนวคิดของ Object-oriented programming ที่ถือเป็นหลักในการพัฒนาโปรแกรมแบบเป็นชิ้นๆ ที่สามารถนำกลับมาใช้งานใหม่ได้ตามแนวทางในการกำหนด class ของชิ้นส่วนย่อยๆ เพื่อความรวดเร็วในการเขียนโปรแกรมและสามารถแก้ไขได้อย่างง่ายดาย

องค์กรควรจะจัดทำแผนการทดสอบให้สมบูรณ์ในระหว่าง phases ของการพัฒนา นอกจากนี้ควรที่จะปรับปรุง เปลี่ยนแปลง นำไปใช้งานจริง ฝึกอบรม และจัดทำคู่มือสำหรับ user ผู้ปฏิบัติงานประจำ และผู้บำรุงรักษาระบบ

มาตรฐานการพัฒนา

มาตรฐานการพัฒนาควรจะระบุความรับผิดชอบของผู้พัฒนาโปรแกรมระบบงานและระบบปฏิบัติการ โดยที่ผู้พัฒนาโปรแกรมระบบงานจะรับผิดชอบในการพัฒนาและบำรุงรักษาโปรแกรมระบบงานสำหรับ user .แต่ผู้พัฒนาระบบปฏิบัติการจะรับผิดชอบในการพัฒนาและบำรุงรักษาทั้งระบบปฏิบัติการภายในที่พัฒนาเองและระบบปฏิบัติการที่มาจากภายนอก (open-source) ซึ่งเชื่อมโยงโปรแกรมระบบงานกับระบบปฏิบัติการและ hardware ดังนั้นฝ่ายจัดการจะต้องเข้าใจสภาพเกี่ยวกับการพัฒนาและสภาพแวดล้อมของระบบงานจริงก่อนจึงจะสามารถมอบหมายความรับผิดชอบให้กับผู้พัฒนาได้อย่างเหมาะสม

มาตรฐานการพัฒนาควรจะห้ามไม่ให้ผู้พัฒนาเข้าถึงข้อมูล โปรแกรม และโปรแกรมอรรถประโยชน์ และระบบอื่น ๆ ที่อยู่นอกเหนือความรับผิดชอบของผู้พัฒนาแต่ละคน ดังนั้นการควบคุมแบบแยกเป็นห้องจัดเก็บข้อมูล (library) จึงสามารถนำมาใช้ในการควบคุมการเข้าถึง การเคลื่อนย้ายโปรแกรมไปมาระหว่างสภาพแวดล้อมในการพัฒนา การทดสอบและการใช้งานจริง (ฝ่ายจัดการควรจะสร้างมาตรฐานที่กำหนดให้ผู้พัฒนาต้องจัดทำเอกสารประกอบการพัฒนาและการทดสอบอย่างครบถ้วน เพราะว่าเอกสารดังกล่าวจะช่วยให้ผู้พัฒนาสามารถแก้ไขข้อผิดพลาดของโปรแกรมและการปรับปรุงแก้ไขโปรแกรมที่ใช้งานจริงได้)

มาตรฐานการเขียนโปรแกรมควรกำหนดชื่อของภาษาและเครื่องมือที่ใช้ เครื่องมือ แผนผังหรือรูปแบบในการเขียนโปรแกรม การตั้งชื่อห้องจัดเก็บโปรแกรมและการตั้งชื่อโปรแกรมขนาดย่อย (the naming conventions of code routines and program libraries) (อยู่นอกเหนือเนื้อหาของคู่มือฉบับนี้) อย่างไรก็ตาม การมีมาตรฐานที่สามารถยืดหยุ่นได้ จะช่วยให้องค์กรลดความเสียหายจากการเขียนโปรแกรมและเพิ่มการรักษาความปลอดภัย ความเชื่อถือได้และการบำรุงรักษาโปรแกรมระบบงานให้ดียิ่งขึ้น ผู้ตรวจสอบควรจะประเมินมาตรฐานการเขียนโปรแกรมขององค์กรและสอบทานกระบวนงานทำงานที่เกี่ยวข้องกับการเขียนโปรแกรม

การควบคุมห้องจัดเก็บโปรแกรมระบบงาน

ห้องจัดเก็บโปรแกรมระบบงานทำหน้าที่เก็บรวบรวมเอกสาร โปรแกรม และข้อมูล รวมถึงโปรแกรมขนาดเล็กที่มีการใช้งานบ่อยๆ ทั้งที่จัดเก็บในรูปของโปรแกรมต้นฉบับและ

โปรแกรมที่อยู่ในรูปแบบพร้อมใช้งานได้ อนึ่งห้องจัดเก็บโปรแกรมระบบงาน เช่น Dynamic link library จะอนุญาตให้ผู้พัฒนาเข้าถึงเพื่อเรียกใช้งานโปรแกรมขนาดย่อมหรือนำไปประกอบกับโปรแกรมได้ทันที ห้องเก็บที่เก็บการเชื่อมโยงรวมถึงโปรแกรมที่สามารถนำไปใช้งานได้ที่สามารถทำงานได้อัตโนมัติซึ่งเป็นส่วนของระบบงานที่ใหญ่กว่า

การควบคุมห้องจัดเก็บโปรแกรมระบบงานจะรวมถึงสิ่งต่อไปนี้

- Automated Password Controls ฝ่ายจัดการควรจะสร้างระบบการควบคุมด้านตรรกะในการเข้าถึงห้องจัดเก็บโปรแกรมระบบงาน หรือโปรแกรมที่อยู่ในสภาพพร้อมใช้งาน แต่การสร้างระบบควบคุมบนโปรแกรมที่อยู่ในสภาพพร้อมใช้งาน แต่ละชุดเป็นภาระที่หนักมากในการรักษาความปลอดภัย ยกเว้นว่าจะมีการจัดแบ่งกลุ่มของโปรแกรมหรือข้อมูลออกเป็นคนละส่วนและทำการควบคุมการเข้าถึงในระดับ ห้องจัดเก็บโปรแกรมระบบงานแทน

- Automated Library Applications ฝ่ายจัดการควรจะใช้โปรแกรมควบคุมห้องจัดเก็บโปรแกรมระบบงานแบบอัตโนมัติ (ถ้ามี) โปรแกรมดังกล่าวสามารถหาซื้อได้ผู้ผลิตอุปกรณ์คอมพิวเตอร์หรือผู้จำหน่ายโปรแกรมระบบงาน เนื่องจากโปรแกรมดังกล่าวมีคุณสมบัติในการควบคุมการเข้าถึงได้ทั้ง 2 ระดับ คือ 1) ห้องจัดเก็บโปรแกรมระบบงาน 2) ระดับของตัวโปรแกรมที่จัดเก็บอยู่ (object)

นอกจากนี้โปรแกรมควบคุมยังสามารถจัดทำรายงานแสดงข้อมูลได้ว่ามีใครเข้าไปในห้องจัดเก็บโปรแกรมระบบงาน หรือมีใครได้เข้าไปเปลี่ยนแปลงแก้ไขอะไรในห้องจัดเก็บโปรแกรมระบบงาน หรือไม่

การควบคุมรุ่นหรือชุดที่แก้ไข

การควบคุมห้องจัดเก็บโปรแกรมระบบงาน ช่วยให้องค์กรสามารถควบคุมรุ่น (version) ของโปรแกรมระบบงานได้ โดยการควบคุม version เป็นการรักษาลำดับของการจัดเก็บสำเนาข้อมูลของโปรแกรมระบบงานและเอกสารประกอบระบบต่างๆ อย่างเป็นระบบ

การพัฒนาระบบควบคุม version ช่วยให้องค์กรสามารถติดตามและแยกแยะ version ของโปรแกรมที่จัดเก็บอยู่ แต่อย่างไรก็ดีระบบควบคุม version ไม่ได้จัดเก็บโปรแกรมทุก version ที่มีการเปลี่ยนแปลงไว้ทุกชุด แต่ระบบจะจัดเก็บแฟ้มข้อมูลเพียงชุดเดียวและจัดเก็บรายละเอียดของการเปลี่ยนแปลงต่างๆ แยกออกมาต่างหาก ถ้ามีการเรียกหาโปรแกรมรุ่นใดก็ตามระบบก็จะนำเอาข้อมูลการเปลี่ยนแปลงต่างๆ ไปปรับปรุงข้อมูลเพื่อให้ได้โปรแกรม version ที่ต้องการต่อไป การควบคุม version ของโปรแกรมช่วยให้ผู้พัฒนาสามารถแก้ไขโปรแกรมระบบงานได้ง่ายขึ้น

เพราะว่าเขาสามารถแน่ใจได้ว่าข้อผิดพลาดเกิดจากการเขียนโปรแกรมผิดพลาด ไม่ได้เกิดจากการเลือกใช้โปรแกรมผิด version ไป

เอกสารประกอบการพัฒนาโปรแกรม

องค์กรควรจะจัดเก็บเอกสารอย่างละเอียดสำหรับโปรแกรมระบบงานและระบบปฏิบัติการในเครื่องที่ใช้งานจริง ทั้งนี้การจัดเก็บเอกสารอย่างครบถ้วนช่วยให้องค์กรสามารถเข้าใจหน้าที่การปฏิบัติงาน การรักษาความปลอดภัย และลักษณะของการควบคุมซึ่งจะช่วยปรับปรุงความสามารถในการใช้และบำรุงรักษาโปรแกรม (ตัวอย่างเอกสารที่จัดเก็บคือ คำอธิบายรายละเอียดของโปรแกรมระบบงาน เอกสารการเขียนโปรแกรม และคำแนะนำเกี่ยวกับระบบปฏิบัติการ) นอกจากนี้ควรมีมาตรฐานในการจัดเก็บเอกสารซึ่งระบุถึงประเภท และรูปแบบของเอกสารที่ต้องการ เช่น คำอธิบาย ผังทางเดินระบบ การเขียนคำสั่งโปรแกรมระบบงานพิเศษ ระบบการควบคุมภายใน และรูปแบบการจัดเรียงข้อมูลของแฟ้มข้อมูลซึ่งไม่มีกล่าวถึงในโปรแกรมระบบงานใด

ฝ่ายจัดการควรเก็บรักษาเอกสารประกอบโปรแกรมทั้งที่พัฒนาขึ้นภายในหรือจัดหาจากภายนอก และในกรณีที่มีการจัดหาโปรแกรมจากภายนอก ฝ่ายจัดการควรสร้างความมั่นใจให้ได้ว่าผู้จำหน่ายโปรแกรมสามารถจัดส่งเอกสารประกอบโปรแกรมระบบงานได้ครบถ้วนและถูกต้องตามมาตรฐานขององค์กร นอกจากนี้ ผู้ตรวจสอบควรศึกษาข้อมูลเพิ่มเติมในส่วนของการจัดหาโปรแกรมจากภายนอกองค์กรในหัวข้อเรื่อง Escrowed Documentation ในส่วนของ Acquisition

ผู้ตรวจสอบควรจะพิจารณาการควบคุมการเข้าถึงและการควบคุมการเปลี่ยนแปลงเมื่อประเมินเรื่องการจัดทำเอกสารประกอบระบบงาน เนื่องจากการควบคุมการเปลี่ยนแปลงจะช่วยให้องค์กรมั่นใจได้ว่าได้มีการอนุมัติ ทดสอบ และบันทึกการเปลี่ยนแปลงอย่างเหมาะสม ส่วนการควบคุมการเข้าถึงจะช่วยให้องค์กรมั่นใจได้ว่าบุคลากรแต่ละคนมีสิทธิเข้าถึงเอกสารเฉพาะในส่วนที่เกี่ยวข้องกับหน้าที่ของตนเองเท่านั้น

องค์กรควรมีเอกสารประกอบระบบงาน ดังต่อไปนี้

- System Descriptions อธิบายให้ทราบรายะเอียดของระบบปฏิบัติการและการนำเข้าข้อมูล การประมวลผล และการแสดงผลลัพธ์จากการทำงานร่วมกันของโปรแกรมระบบงาน

- System Documentation ประกอบไปด้วยผังทางเดินระบบ และแบบจำลองที่ระบุที่มาและรูปแบบของข้อมูล การประมวลผล และการควบคุมการดำเนินการ (ทั้งแบบอัตโนมัติหรือทำด้วยมือ) และลักษณะและสถานที่จัดเก็บข้อมูลผลลัพธ์

- System File Layouts อธิบายถึงการเก็บรวบรวม record ที่เกี่ยวข้องกับการประมวลผลโดยแต่ละโปรแกรมระบบงาน เช่น พนักงานอาจจะต้องการผัง System File Layouts เพื่ออธิบายรูปแบบของ แฟ้มจัดเก็บข้อมูลระหว่างการประมวลผล (interim file) เช่น แฟ้มข้อมูลที่จัดเรียงตามลำดับของการทำรายการฝากเงินเพื่อประโยชน์ในการกำหนดรูปแบบของแฟ้มข้อมูลหลัก ในการประมวลผลเอกสารประกอบระบบงานควรจะประกอบไปด้วย

- Application Descriptions อธิบายวัตถุประสงค์ของโปรแกรมระบบงาน และภาพรวมของข้อมูลนำเข้า การประมวลผล และภาระหน้าที่ในการแสดงผลลัพธ์

- Layouts แสดงรูปแบบของข้อมูลที่เก็บและข้อมูลที่แสดงผล เช่น ผังแสดงระบบฐานข้อมูล การแสดงผลบนหน้าจอ และข้อมูลที่เป็นกระดาษ

- Program Documentation แสดงรายละเอียดของข้อมูลเฉพาะที่นำเข้า การประมวลผล และคำสั่งให้แสดงผลลัพธ์ รวมไปถึงเอกสารประกอบระบบรักษาความปลอดภัย รายชื่อโปรแกรม และโปรแกรมต้นฉบับ (program listing/source code) และคำอธิบายที่เกี่ยวข้องกับข้อสังเกตของโปรแกรม เป็นเอกสารพื้นฐานที่มีรายละเอียดทั้งด้านเทคนิคของการเขียนโปรแกรมและคำอธิบาย ดังนั้นผู้พัฒนาโปรแกรมจึงควรปรับปรุงรายชื่อและข้อสังเกตเมื่อทำการปรับปรุงแก้ไขโปรแกรมหรือความเห็น ให้ทันสมัย แต่ปัจจุบันก็มีโปรแกรมช่วยในการพัฒนาซึ่งจะสามารถทำงานได้แบบอัตโนมัติในการจัดทำทะเบียนคุมโปรแกรมระบบงานและคำอธิบายที่เกี่ยวข้องได้

โดยทั่วไปแล้วผู้ออกแบบและผู้พัฒนาจะใช้ผังรูปภาพแสดงให้เห็นลำดับของการทำงานของโปรแกรม เช่น ในภาษา COBOL และ Assembler ผังทางเดินจะแสดงภาพอย่างง่ายของการดำเนินงานที่ซับซ้อนของโปรแกรมและโปรแกรมประกอบย่อยๆ อนึ่งในปัจจุบันนี้ได้มีการนำเอาโปรแกรมสำเร็จรูปที่ทำหน้าที่ช่วยเขียนผังทางเดินของโปรแกรมแบบอัตโนมัติมาช่วยให้ผู้พัฒนาสามารถปรับเปลี่ยนโปรแกรมได้เองตลอดเวลา โดยไม่มีความจำเป็นต้องไปเขียนผังทางเดินของ โปรแกรมใหม่ทุกครั้งที่มีการปรับเปลี่ยนแก้ไขโปรแกรม

เทคนิคการเขียนโปรแกรม อย่างเช่น Object-oriented Programming มีส่วนช่วยสนับสนุนให้มีการเลือกใช้โปรแกรมระบบงานที่สามารถปรับปรุงผังทางเดินของโปรแกรมแบบอัตโนมัติ ทั้งนี้เพราะว่าการจัดเก็บรายละเอียดของการเขียนโปรแกรมแบบ Object-oriented ถือเป็นสิ่งสำคัญมากเพราะว่าประโยชน์สูงสุดของเทคนิคการเขียนโปรแกรมแบบนี้ก็คือการนำเอาโปรแกรมเก่ามาปรับปรุงและใช้งานได้อีก

- Naming Conventions คือส่วนสำคัญของเอกสารประกอบ Program Documentation ทั้งนี้เพราะว่าโปรแกรมระบบงานซึ่งมีการเขียนคำสั่งจำนวนมากเรียงตามลำดับลงมาถึงลำดับของการทำงานของโปรแกรมขนาดย่อยๆ ซึ่งทำหน้าที่เฉพาะบางอย่างภายในโปรแกรม (modules, subroutines, components) ดังนั้นผู้พัฒนาจะต้องบันทึกชื่อเรียกของโปรแกรมย่อยๆ เหล่านี้ รวมทั้งชื่อของโปรแกรมระบบงาน ระบบฐานข้อมูลและระบบการทำงานร่วมกับโปรแกรมที่กำลังพัฒนาอยู่ ดังนั้นการตั้งชื่อปรแกรม และโปรแกรมย่อยต่างๆ ที่เป็นมาตรฐานจะช่วยให้ผู้พัฒนาสามารถเชื่อมต่อโปรแกรมย่อยต่างๆเข้าด้วยกันได้อย่างดีและมีประสิทธิภาพและยังช่วยให้ผู้พัฒนาสามารถเข้าใจการทำงานของโปรแกรมได้อย่างดีและสามารถแก้ไขโปแกรมดังกล่าวได้ในอนาคต

- Operator Instructions คู่มือการปฏิบัติงานของ operators จะอธิบายถึงวิธีการปฏิบัติงานที่เกี่ยวข้องกับการประมวลผลโปรแกรมระบบงาน ภาระหน้าที่ของ operator รวมถึงวิธีการโต้ตอบกับระบบหรือการหยุดชะงักของระบบ และ**ควรมีรายละเอียดเพียงพอที่ operator ที่มีประสบการณ์จะสามารถสั่งให้โปรแกรมระบบงานที่ตัวเองไม่มีความคุ้นเคยมาก่อนให้ทำงานได้โดยไม่ต้องอาศัยความช่วยเหลือจากใคร**แต่ operator จะต้องถูกกันไม่ให้เข้าถึงคู่มือต่างๆ ที่เกี่ยวข้องกับรายชื่อโปรแกรมต้นฉบับ ผังแสดงการจัดเก็บข้อมูลระดับ record และผังทางเดินของโปรแกรม

- End-User Instructions องค์กรควรจะสร้างคู่มือผู้ใช้งานที่อธิบายการใช้ระบบงาน คู่มือการปฏิบัติงาน ตัวช่วยเหลือแบบ Online และข้อความเตือนความผิดพลาดที่แสดงบนระบบถือเป็นรูปแบบของคำแนะนำที่ช่วยให้แต่ละคนสามารถใช้ระบบงานและแก้ปัญหาได้

(5) ขั้นตอนการทดสอบ

ในขั้นตอนการทดสอบนี้องค์กรต้องทดสอบให้ครอบคลุมเพื่อให้แน่ใจว่าโปรแกรมมีความถูกต้อง รวมถึงหน้าที่การทำงานของระบบและความสามารถในการปฏิบัติงานเชื่อมโยงกันของระบบงานและส่วนประกอบต่าง ๆ ของเครือข่าย การทดสอบถือเป็นสิ่งสำคัญที่ทำให้แน่ใจว่าระบบถูกพัฒนาตามความต้องการขององค์กรและผู้ใช้งาน

ถ้าองค์กรจะใช้เทคนิคการบริหารโครงการให้มีประสิทธิภาพ องค์กรต้องทำแผนทดสอบให้สมบูรณ์ในขณะพัฒนาและต้องเสร็จก่อนเข้าถึงขั้นตอนการทดสอบ ส่วนเทคนิคการบริหารโครงการที่ไม่ดีหรือมีความต้องการให้โครงการเสร็จอย่างรวดเร็วอาจทำให้เกิดความกดดันในการจัดทำแผนการทดสอบในช่วงเริ่มเข้าขั้นตอนการทดสอบ แผนการทดสอบที่ถูกสร้างในระหว่างขั้นตอนเริ่มพัฒนาโครงการ จะช่วยให้องค์กรกำหนดรายละเอียดการทดสอบได้ดียิ่งขึ้น การใช้แผนการทดสอบที่มีรายละเอียดเพียงพอจะช่วยทำให้ผู้ทดสอบพบจุดอ่อนได้ก่อนที่จะนำระบบออกใช้งานจริง

กลุ่มที่ทดสอบประกอบด้วยผู้เชี่ยวชาญและผู้ใช้งานที่รับผิดชอบเข้าร่วมประชุมและทำหน้าที่ดึงข้อมูลที่จะทดสอบเข้าไปในระบบที่ต้องการทดสอบ โดยทั่วไปแล้วกลุ่มดังกล่าวจะทำการทดสอบเป็นขั้นตอนจากวิธีบนลงล่างหรือจากวิธีล่างขึ้นบน วิธีล่างขึ้นบนเป็นการทดสอบส่วนประกอบย่อยก่อนแล้วขยายการทดสอบขึ้นไปจนถึงส่วนประกอบใหญ่และระบบ ส่วนวิธีบนลงล่างจะทดสอบส่วนประกอบใหญ่ก่อน การเชื่อมต่อและส่วนประกอบย่อย ความก้าวหน้าในการทดสอบและการระบุความสำเร็จของการทดสอบจะผันแปรไม่แน่นอนขึ้นอยู่กับแต่ละองค์กร

การทดสอบจากล่างขึ้นบนจะเริ่มจากการทดสอบหน้าที่การทำงานของระบบ การทดสอบนี้ควรจะทำให้แน่ใจว่าหน้าที่การทำงาน การรักษาความปลอดภัยและการควบคุมภายในตามความต้องการที่กำหนดไว้สามารถทำงานได้อย่างเหมาะสม ผู้ทดสอบจะทดสอบการรวมระบบเข้ากับส่วนประกอบอื่นและทดสอบตั้งแต่ต้นจนจบการทำงานเพื่อให้แน่ใจว่าส่วนประกอบต่างๆ ของระบบสามารถทำงานประสานสัมพันธ์กับระบบงานได้อย่างเหมาะสม ผู้ใช้จะทำการทดสอบการยอมรับระบบเพื่อให้แน่ใจว่าระบบถูกพัฒนาขึ้นตามความต้องการและเงื่อนไขที่กำหนดไว้

ผู้ทดสอบจะทราบถึงข้อบกพร่องและจุดอ่อนของโปรแกรมระหว่างที่ดำเนินการทดสอบ กระบวนงานควรจะระบุขั้นตอนการปฏิบัติดังกล่าวเพื่อให้แน่ใจว่าผู้พัฒนาได้แก้ไขข้อบกพร่องได้อย่างรวดเร็วและจัดทำเอกสารประกอบการปรับปรุงเปลี่ยนแปลงนั้นด้วย การแก้ไขปัญหาได้อย่างรวดเร็วจะช่วยเพิ่มประสิทธิภาพการทดสอบโดยการลดเวลาการหยุดชะงักของผู้ทดสอบและเพื่อให้แน่ใจว่าผู้พัฒนาไม่เสียเวลาในการพยายามแก้ไขปัญหากับบางส่วนของโปรแกรมที่ไม่มีความบกพร่องที่ไม่สามารถทำงานได้เพราะผู้พัฒนาคนอื่นไม่ได้แก้ไขข้อบกพร่องนั้น **การจัดทำเอกสารประกอบการปรับปรุงแก้ไขถือว่ามีความจำเป็นเพื่อเก็บรักษาความถูกต้องเชื่อถือได้ของเอกสารประกอบการพัฒนาทั้งหมด**

องค์กรควรจะสอบทานและจัดทำคู่มือผู้ใช้ คู่มือผู้ปฏิบัติงานและคู่มือการบำรุงรักษาให้เสร็จสิ้นในระหว่างที่อยู่ในขั้นตอนการทดสอบ นอกจากนี้ องค์กรควรจัดทำแผนการเปลี่ยนแปลง แผนการนำไปใช้และแผนการฝึกอบรมให้เสร็จสิ้นด้วย **การทดสอบควรรวมถึงสิ่งต่อไปนี้**

- Acceptance Testing ผู้ใช้งานจะทำการทดสอบการยอมรับระบบเพื่อประเมินหน้าที่การทำงานและการประสานสัมพันธ์การปฏิบัติงานของระบบงานทั้งหมด

- End-to-End Testing ผู้ใช้งานและผู้เชี่ยวชาญระบบทำการทดสอบตั้งแต่ต้นจนจบเพื่อประเมินการประสานสัมพันธ์การปฏิบัติงานของระบบงานและส่วนประกอบของระบบอื่น เช่น ฐานข้อมูล hardware software หรืออุปกรณ์การติดต่อสื่อสารอื่น

- Functional Testing ผู้ใช้งานทำการทดสอบหน้าที่การทำงานของระบบเพื่อประเมินความสามารถในการปฏิบัติงานของโปรแกรมกับความต้องการที่กำหนดไว้แล้ว การทดสอบหน้าที่การทำงานรวมถึงการทดสอบกล่องดำที่เป็นการประเมินหน้าที่การทำงานของระบบกับความต้องการที่กำหนดไว้แล้ว หรือการทดสอบกล่องขาวที่เป็นการประเมินหน้าที่การทำงานของรหัส (feature's code)

- Integration Testing ผู้ใช้งานและผู้เชี่ยวชาญระบบทำการทดสอบแบบรวมเพื่อประเมินการเชื่อมต่อกับส่วนประกอบต่าง ๆ ที่เกี่ยวข้องทั้งหมด

- Parallel Testing ผู้ใช้งานทำการทดสอบแบบคู่ขนานเพื่อเปรียบเทียบผลลัพธ์จากระบบงานที่พัฒนาใหม่กับระบบเดิม

- Regression Testing ผู้ใช้งานลองทำการทดสอบระบบงานใหม่อีกครั้งเพื่อประเมินหน้าที่การทำงานของระบบหลังจากผู้พัฒนาทำการเขียนโปรแกรมแก้ไขหลังจากที่มีการทดสอบไปแล้ว

- Stress Testing ผู้เชี่ยวชาญทำการทดสอบแบบหนักเพื่อประเมินข้อจำกัดสูงสุดของระบบงาน

- String Testing ผู้พัฒนาทำการทดสอบเพื่อยืนยันการสื่อสารระหว่างโปรแกรมระบบงานหรือองค์ประกอบของโปรแกรมระบบงานที่เชื่อมโยงและจำเป็นต้องทำงานไปพร้อมๆ กัน

- System Testing ผู้เชี่ยวชาญทำการทดสอบระบบเพื่อประเมินหน้าที่การทำงานตลอดทั้งระบบ

- Unit Testing ผู้พัฒนาทำการทดสอบส่วนย่อยเพื่อประเมินหน้าที่การทำงานของส่วนประกอบย่อย

(6) ขั้นตอนการนำออกใช้งาน

ขั้นตอนการนำออกใช้งานเป็นการติดตั้งระบบงานที่ผ่านการอนุมัติแล้วให้ลงในสภาพแวดล้อมการใช้งานจริงได้ งานแรก คือ การประกาศตารางการนำออกใช้งาน การฝึกอบรมผู้ใช้งานและการติดตั้งบนเครื่องคอมพิวเตอร์ นอกจากนี้ องค์กรควรจะนำข้อมูลเข้า ตรวจสอบข้อมูล

ตั้งค่าและทดสอบระบบ และการตั้งค่าการรักษาความปลอดภัย และการสอบทานหลังการนำออกใช้งาน ฝ่ายจัดการควรจะส่งตารางการนำระบบออกใช้งานให้กับทุกคนที่เกี่ยวข้องและควรประกาศให้ผู้ใช้งานทราบถึงความรับผิดชอบในการใช้งาน

หลังจากองค์กรติดตั้งใช้งานจริงแล้ว จะทำการโอนข้อมูลเดิมทั้งแบบที่เป็นอิเล็กทรอนิกส์และที่ต้องป้อนข้อมูลเองเข้าสู่ระบบงานใหม่ การตรวจสอบความถูกต้องของข้อมูลนำเข้าและการตั้งค่าการรักษาความปลอดภัยถือเป็นส่วนสำคัญของกระบวนการนำระบบงานออกใช้ บ่อยครั้งที่องค์กรใช้ระบบงานใหม่ขนานไปกับการใช้ระบบงานเก่าจนกว่าจะมีการตรวจสอบความถูกต้องเชื่อถือได้ของระบบงานใหม่ พนักงานควรจะจัดทำเอกสารประกอบเกี่ยวกับการเขียนโปรแกรม กระบวนงาน หรือการเปลี่ยนแปลงการตั้งค่าที่เกิดขึ้นในระหว่างกระบวนการตรวจสอบความถูกต้อง

การประเมินโครงการ

ฝ่ายจัดการควรจะใช้การสอบทานหลังจากนำระบบออกใช้งานแล้วเพื่อตรวจสอบความสมบูรณ์ตามวัตถุประสงค์โครงการและประเมินผลการดำเนินงานโครงการ ฝ่ายจัดการควรจะสัมภาษณ์ทุกคนที่เกี่ยวข้องกับการใช้ระบบงานใหม่และจัดทำเอกสารประกอบ และระบุถึงปัญหาที่เกิดขึ้น

ฝ่ายจัดการควรจะวิเคราะห์ประสิทธิผลของการดำเนินงานโครงการโดยการเปรียบเทียบกับสิ่งอื่น เช่น งบประมาณตามแผนกับที่ต้องใช้จริง ประโยชน์ที่ได้รับกับเวลาที่ใช้ในการพัฒนา ฝ่ายจัดการควรจะจัดทำเอกสารประกอบผลสรุปและนำเสนอผู้บริหารระดับสูง **ผู้บริหารระดับสูงควรจะได้รับทราบถึงการปฏิบัติงานต่าง ๆ และข้อบกพร่องที่เกิดขึ้นในการบริหารจัดการโครงการ**

(7) ขั้นตอนการบำรุงรักษา

ขั้นตอนการบำรุงรักษาเป็นการทำการเปลี่ยนแปลง hardware software และเอกสารประกอบให้การปฏิบัติงานมีประสิทธิผล รวมถึงการเปลี่ยนแปลงเกี่ยวกับการปรับปรุงการทำงานของระบบให้ดีขึ้น การแก้ไขปัญหา การเสริมสร้างการรักษาความปลอดภัย หรือการระบุความต้องการของผู้ใช้งาน และเพื่อให้แน่ใจว่าการปรับปรุงเปลี่ยนแปลงไม่มีผลกระทบกับการปฏิบัติงานหรือลดประสิทธิภาพของระบบหรือการรักษาความปลอดภัยลง องค์กรควรจะสร้างมาตรฐานและกระบวนงานในการบริหารการเปลี่ยนแปลง

การบริหารการเปลี่ยนแปลงเกี่ยวข้องกับการสร้างรุ่นที่เป็นพื้นฐานของระบบงานการให้บริการ และกระบวนงาน และทำให้แน่ใจว่าการเปลี่ยนแปลงทั้งหมดได้รับการอนุมัติ มีการจัดทำ

เอกสารประกอบ และแจ้งให้บุคคลที่เกี่ยวข้องทราบ การควบคุมการเปลี่ยนแปลงควรจะระบุถึงรูปแบบทั้งหมดของสภาพแวดล้อมด้านเทคโนโลยีขององค์กร รวมถึง hardware software การตั้งค่า software มาตรฐานและกระบวนการปฏิบัติงาน และการดำเนินการบริหารโครงการ ฝ่ายจัดการควรจะสร้างการควบคุมการเปลี่ยนแปลงที่ระบุถึงระบบงานหลัก ระบบงานที่ใช้ประจำ การปรับปรุงระบบงานแบบเร่งด่วนและการเสริมสร้างการรักษาความปลอดภัย

การปรับปรุงระบบงานหลักถือเป็นการเปลี่ยนแปลงที่มีความสำคัญเกี่ยวกับหน้าที่การทำงานของระบบ ฝ่ายจัดการควรจะสร้างกระบวนการที่เป็นมาตรฐานสำหรับการเปลี่ยนแปลงระบบงานหลัก เช่น การใช้วิธี SDLC

การปรับปรุงระบบงานที่ใช้ประจำจะไม่ซับซ้อนเหมือนกับการปรับปรุงระบบงานหลักและสามารถนำมาใช้กับการดำเนินงานปกติของธุรกิจได้ การควบคุมการเปลี่ยนแปลงระบบงานประจำควรจะรวมถึงกระบวนงานในการร้องขอแก้ไข การประเมิน การอนุมัติ การทดสอบ การติดตั้งและการจัดทำเอกสารประกอบการเปลี่ยนแปลง

การปรับปรุงระบบงานแบบเร่งด่วนอาจจะเกี่ยวกับปัญหาที่เกิดขึ้นเป็นปกติกับระบบงานประจำอยู่แล้ว อย่างไรก็ตาม ถ้าปัญหาเกิดจากการรักษาความปลอดภัยหรือการประมวลผล การปรับปรุงแก้ไขนั้นต้องดำเนินการโดยเร็ว การควบคุมการเปลี่ยนแปลงแบบเร่งด่วนควรจะมีกระบวนงานเหมือนกับการควบคุมการเปลี่ยนแปลงระบบงานประจำ **ฝ่ายจัดการควรจะสร้างกระบวนงานแบบย่อ**ที่เป็นการร้องขอ การประเมินและการอนุมัติเพื่อให้แน่ใจว่าฝ่ายจัดการสามารถนำระบบงานที่ปรับปรุงแล้วมาใช้ได้อย่างรวดเร็ว การประเมินอย่างละเอียดและการจัดทำเอกสารประกอบการปรับปรุงระบบงานแบบเร่งด่วนควรจะทำให้เสร็จสมบูรณ์โดยเร็วที่สุดหลังจากระบบงานที่ปรับปรุงถูกนำออกใช้แล้ว ฝ่ายจัดการควรจะทดสอบระบบงานประจำเมื่อใดก็ตามที่สามารถทำได้ ระบบงานที่ปรับปรุงแบบเร่งด่วนต้องนำออกใช้และแจ้งให้ผู้ที่เกี่ยวข้องทราบถึงการปรับปรุงนั้นอย่างรวดเร็ว **ถ้าฝ่ายจัดการไม่สามารถทดสอบระบบงานที่ปรับปรุงแบบเร่งด่วนได้ทันก่อนติดตั้ง ฝ่ายจัดการจะต้องทำการสำรองข้อมูลและโปรแกรม และสร้างกระบวนงานรองรับการกลับมาใช้ระบบงานเดิมก่อนปรับปรุง**

การเสริมสร้างความปลอดภัยให้กับเครื่องคอมพิวเตอร์ (software patch) ถือเป็นการปรับปรุงเช่นเดียวกับการปรับปรุงระบบงานประจำ ซึ่งเป็นการปรับปรุง software ที่ซื้อมาโดยการ patch อย่างไรก็ตาม การปรับปรุงระบบงานประจำที่พัฒนาเองก็ถือว่าเป็นการ patch เช่นกัน การบริหารการ patch ควรจะระบุไว้ในกระบวนงานเพื่อใช้ในการประเมิน การอนุมัติ การทดสอบ การติดตั้ง และ

การจัดทำเอกสารประกอบการปรับปรุงระบบงาน อย่างไรก็ตาม **สิ่งสำคัญในกระบวนการบริหารการ patch คือ การตระหนักถึงจุดอ่อนของระบบต่อภายนอกองค์กรกับการป้องกัน (patch)**

ความถูกต้องในการบำรุงรักษาเกี่ยวกับการปรับปรุงรายชื่อทรัพย์สินที่เป็น hardware software ให้ทันสมัยนั้นถือเป็นส่วนที่สำคัญในกระบวนการบริหารการเปลี่ยนแปลงทั้งหมด ฝ่ายจัดการควรจะจัดทำเอกสารประกอบการปรับปรุงอย่างระมัดระวังเพื่อให้แน่ใจว่าทรัพย์สินในระบบมีความถูกต้อง ถ้า software patch ที่กำหนดไว้แล้วไม่ได้ถูกนำมาปรับปรุง ฝ่ายจัดการควรจะจัดทำเอกสารประกอบเหตุผลการไม่ติดตั้งนั้น

ฝ่ายจัดการควรจะประสานงานการเปลี่ยนแปลงที่เกี่ยวข้องกับเทคโนโลยีทั้งหมดผ่านคณะกรรมการและกำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องอย่างเหมาะสมในการบริหารจัดการ software patch บุคลากรที่ทำหน้าที่การรับรองคุณภาพ การรักษาความปลอดภัย การตรวจสอบ การปฏิบัติตามกฎ ดูแลเครือข่ายสื่อสาร และผู้ใช้งานควรจะถูกระบุอยู่ในกระบวนการบริหารการเปลี่ยนแปลงอย่างเหมาะสม การสอบทานความเสี่ยงและการรักษาความปลอดภัยควรจะถูกดำเนินการเมื่อไรก็ตามที่ระบบงานที่ปรับปรุงแล้วถูกนำออกมาใช้เพื่อให้แน่ใจว่าได้คำนึงถึงการควบคุมด้วย สามารถดูรายละเอียดเพิ่มเติมได้จากส่วนของ “การบำรุงรักษา”

(8) ขั้นตอนการปรับเปลี่ยน โอนย้ายหรือจัดการทรัพยากรส่วนเกินหรือส่วนที่ไม่ได้ใช้งาน (Disposal Phase)

ขั้นตอนการปรับเปลี่ยน โอนย้ายหรือจัดการทรัพยากรส่วนเกินหรือส่วนที่ไม่ได้ใช้งาน เป็นกระบวนการโอนย้ายทรัพยากรที่ไม่ได้ใช้งานหรือส่วนที่ล้าสมัยแล้วทั้ง hardware software และข้อมูลออกจากสภาพแวดล้อมที่ใช้งานปัจจุบัน โดยเริ่มจากงานแรก ควรประกอบด้วยการถ่ายโอนข้อมูล กระบวนการจัดเก็บเอกสารสำคัญ หรือกระบวนการทำลายข้อมูลที่ไม่ใช้งาน ฝ่ายจัดการ ควรพิจารณา มอบหมายผู้รับผิดชอบ และดูแลติดตามให้มีการโอนข้อมูลจากระบบงานที่ใช้งานจริง กระบวนการสำรองข้อมูลและการทดสอบข้อมูลสำรองที่เหมาะสมและดำเนินการตามแผนที่กำหนดไว้ องค์กรควรพิจารณาวิธีการเก็บรักษาข้อมูลสำคัญและจำเป็นแต่ละประเภทให้เหมาะสมกับลักษณะและความต้องการในการใช้งาน ซึ่งเอกสารประกอบระบบงานเป็นเอกสารประเภทหนึ่งที่จำเป็นต้องจัดเก็บเพื่อใช้ประโยชน์ในกรณีที่จำเป็นต้องติดตั้งระบบงานใหม่อีกครั้ง นอกจากนี้ฝ่ายจัดการควรพิจารณามอบหมายผู้รับผิดชอบในการดำเนินการทำลายข้อมูล (โดยการนำข้อมูลใหม่เขียนทับลงบนข้อมูลเก่าหรือการใช้แม่เหล็กลบล้างข้อมูลบนแผ่นดิสก์และเทป ศึกษารายละเอียดเพิ่มเติมได้จากคู่มือ “การรักษาความปลอดภัย”)

2.2.2 ระบบงานรวมทั้งหมด

ระบบงานรวมประกอบด้วยหลายระบบงานที่ทำงานร่วมกันเป็นหนึ่งเดียว หลายระบบถูกออกแบบมาเพื่อให้ใช้ได้กับการเขียนโปรแกรมหลายภาษา หลายระบบปฏิบัติการ และหลายโปรโตคอลที่ใช้ติดต่อสื่อสารเพื่อเพิ่มความสามารถในการปฏิบัติงานร่วมกันและความต้องการการบำรุงรักษาที่ง่าย

ระบบรวมที่นำออกใช้ได้อย่างมีประสิทธิภาพจะเป็นงานที่ซับซ้อนที่ต้องใช้ทรัพยากรมาก เป็นโครงการที่ใหญ่มากและต้องใช้เทคนิคการบริหารความเสี่ยงหลากหลาย และใช้เวลายาวนานมากในการดำเนินการ

ถึงแม้ว่าประโยชน์ที่คาดหวังของระบบรวมอาจจะถูกกำหนดไว้แล้วก็ตาม ก็ยังมีสิ่งสำคัญที่ท้าทายเกี่ยวกับกระบวนการพัฒนา บางองค์กรประมาณการความต้องการพัฒนาโครงการต่ำกว่าที่คาดไว้ ทำให้เกิดความเสียหายทางการเงินที่สำคัญและทำให้มีโอกาสมากที่จะละทิ้งโครงการ

ผู้ตรวจสอบที่จะเข้าไปตรวจสอบองค์กรที่จะนำระบบรวมมาใช้ต้องทำการสอบทานกระบวนงานพัฒนาตลอดทั้งวงจร การสอบทานควรจะรวมถึงการประเมินความเข้าใจของคณะกรรมการต่อความต้องการโครงการและข้อผูกมัดต่อโครงการ ผู้ตรวจสอบต้องสอบทานคุณสมบัติของผู้จัดการโครงการอย่างละเอียด ความเพียงพอของแผนงานโครงการ และความพอเพียงของกระบวนงานบริหารความเสี่ยง

2.2.3 เทคนิคการพัฒนา

(1) การเขียนโปรแกรมเชิงวัตถุ (Object-Oriented Programming)

โดยทั่วไปแล้วผู้พัฒนาเขียนโปรแกรมระดับสูงโดยเรียงเป็นรายบรรทัดลงมา ภาษาที่ใช้เขียน เช่น COBOL ผู้พัฒนาที่เขียนโปรแกรมระดับสูงแบบวัตถุ เช่น ภาษา C++ และ Java อย่างไรก็ตาม การเขียนโปรแกรมเชิงวัตถุจะเขียนน้อยกว่าแบบเรียงลำดับเป็นรายบรรทัด

การเขียนโปรแกรมเชิงวัตถุมีหลักอยู่ที่เป็นการพัฒนาจากส่วนย่อยและสามารถนำมาใช้ร่วมกันได้อีกโดยการเชื่อมโยงเข้าด้วยกันและถือว่าหนึ่งวัตถุเป็นหนึ่งโปรแกรม ส่วนประกอบหลักของการเขียนโปรแกรมเชิงวัตถุ คือ การจัดเรียงประเภทแบบของข้อมูลที่สัมพันธ์กัน เช่น ตัวเลข ตัวอักษร และจำนวนเงิน และโครงสร้าง เช่น การบันทึก ไฟล์ ตาราง เป็นต้น การจัดทำแบบจำลองจะช่วยให้ผู้พัฒนาสามารถเชื่อมโยงโปรแกรมวัตถุเดิมกับระดับชั้นของข้อมูลที่เป็นแบบจำลอง และจะช่วยลดเวลาในการพัฒนาและง่ายแก่การปรับปรุงแก้ไข

ผู้พัฒนาใช้วิธีหลากหลายในการกำหนดและเชื่อมโยงโปรแกรมวัตถุเดิมที่พัฒนาแล้ว เริ่มต้นด้วยเทคนิคการเขียนโปรแกรมที่ดีถูกพัฒนาโดยการเน้นที่การจัดเรียงบรรทัดของการเขียนโปรแกรมที่เป็นมาตรฐาน เทคนิคเฉพาะเรื่องจะช่วยให้ผังงานของโปรแกรมวัตถุและการออกแบบทั้งหมดทำได้ง่ายกว่าเพื่อรวมแต่ละวัตถุเข้าไว้ด้วยกัน การเขียนโปรแกรมเชิงวัตถุใช้เป็นแบบของการเขียนโปรแกรมแบบเดิมแต่เพิ่มวิธีในการกำหนดระดับชั้นของข้อมูลที่ใช้เชื่อมโยงกับระบบงานประจำ

การกลับไปใช้การเขียนโปรแกรมแบบเดิม และเนื่องจากมีหลายวิธี เช่น การเขียนโปรแกรมเชิงวัตถุที่ใช้เทคนิคการเขียนโปรแกรมแบบเดิมจะทำให้ขาดกระบวนงานเขียนโปรแกรมที่เป็นมาตรฐาน การขาดกระบวนงานที่เป็นมาตรฐานนี้ทำให้เป็นข้อจำกัดความสามารถในการเชื่อมโยงระหว่างกันของแต่ละระบบงานรวมถึงการออกแบบและการพัฒนาระบบงานแบบอัตโนมัติ หรือเรียกว่าเครื่องมือ computer-aided software engineering (CASE) อย่างไรก็ตาม อุตสาหกรรม software กำลังจะยอมรับมาตรฐานการเชื่อมต่อโปรโตคอลของการเขียนโปรแกรมเชิงวัตถุ

(2) Computer-Aided Software engineering (CASE)

เครื่องมือ CASE เป็น software ประเภทหนึ่งที่ดำเนินการหลายอย่างแบบอัตโนมัติในหลายขั้นตอนของวงจรพัฒนา เช่น เมื่อมีการสร้างความต้องการหน้าที่การทำงานของระบบงานหนึ่ง เครื่องมือการจัดทำต้นแบบสามารถถูกนำมาใช้พัฒนาภาพจำลองของหน้าจอระบบงานได้เพื่อช่วยให้ผู้ใช้งานมองเห็นภาพการทำงานของระบบงานเมื่อพัฒนาเสร็จ ต่อมาผู้ออกแบบระบบสามารถใช้เครื่องมือการออกแบบอัตโนมัติในการแปลงความต้องการหน้าที่การทำงานต้นแบบไปเป็นเอกสารรายละเอียดประกอบการออกแบบได้ ผู้พัฒนาสามารถใช้ตัวสร้างการเขียนโปรแกรมอัตโนมัติในการแปลงเอกสารการออกแบบที่มีอยู่ไปเป็นการเขียนโปรแกรม เครื่องมืออัตโนมัตินำมาใช้ร่วมกันได้ตามที่กล่าวอ้างหรือใช้เฉพาะเรื่องก็ได้ เช่น เครื่องมือการจัดทำต้นแบบสามารถถูกนำมาใช้ในการกำหนดความต้องการระบบงานที่ผ่านการออกแบบจากผู้เชี่ยวชาญมาแล้วทำการแปลงความต้องการเป็นรายละเอียดการออกแบบตามวิธีทั่วไปโดยใช้ผังทางเดินระบบงานและรายละเอียดเอกสารประกอบ

เครื่องมืออัตโนมัติสามารถช่วยอำนวยความสะดวกในการประสานงานการดำเนินการพัฒนาระบบงานผ่านการใช้คลังข้อมูล คลังข้อมูลจะเป็นทางที่เก็บและเข้าถึงข้อมูลเกี่ยวกับโครงการ เช่น แผนงานโครงการ ความต้องการหน้าที่การทำงาน เอกสารประกอบการออกแบบ ห้องเก็บโปรแกรม ที่เก็บการทดสอบ

โดยทั่วไปองค์กรนำเครื่องมือการพัฒนาอัตโนมัติมาใช้เพื่อเพิ่มผลผลิต (productivity) ให้ทำงานได้เร็วขึ้น ลดต้นทุน เพิ่มการควบคุมโครงการ และเพิ่มคุณภาพของงานพัฒนา

อย่างไรก็ตาม การจัดการความเสี่ยงที่หลากหลายที่มากับเทคโนโลยีแบบอัตโนมัติทำให้องค์กรต้องแน่ใจว่าได้พัฒนาระบบให้มีหน้าที่การทำงานของระบบ การรักษาความปลอดภัย และความถูกต้องเชื่อถือได้อย่างเหมาะสม ความเสี่ยงและการควบคุมที่เกี่ยวข้องกับการใช้ CASE มีดังนี้

- Inadequate Standardization **เครื่องมือ CASE ที่สร้างมาจากหลายผู้ผลิตอาจใช้ยากถ้าระบบงานไม่ได้ถูกเขียนขึ้นเป็นมาตรฐานและการแบ่งประเภทข้อมูลที่ไม่มีมาตรฐาน รูปแบบไฟล์สามารถถูกแปลงได้แต่ปกติแล้วไม่ได้มีการใช้กันในทางธุรกิจ** การควบคุมรวมถึงการใช้เครื่องมือจากผู้ผลิตรายเดียวกัน หรือการใช้เครื่องมือที่มีการติดต่อโปรโตคอลที่เป็นมาตรฐานและการยืนยันโดยการสาธิตให้เห็นว่าใช้ได้ นอกจากนี้ ถ้าองค์กรใช้เครื่องมือเพียงบางส่วนของกระบวนการพัฒนา องค์กรควรจะพิจารณาว่าเครื่องมือที่ใช้เป็นของผู้ผลิตรายใดที่มีเครื่องมือที่ใช้ได้กับทั้งกระบวนการพัฒนาเพื่อให้แน่ใจได้ว่าในอนาคตยังสามารถใช้ได้กับเครื่องมืออื่นด้วย

- Unrealistic Expectations บ่อยครั้งที่องค์กรนำเทคโนโลยี CASE มาใช้ในการลดต้นทุนการพัฒนา กลยุทธ์การนำ CASE มาใช้โดยปกติแล้วจะเป็นการลงทุนสูงเมื่อเริ่มต้นโดยทั่วไปแล้ว ฝ่ายจัดการต้องยอมรับว่ามีระยะเวลายาวกว่าจะได้คืนทุน การควบคุมรวมถึงความต้องการให้ผู้บริหารระดับสูงกำหนดจุดมุ่งหมายและกลยุทธ์ในการนำเทคโนโลยี CASE มาใช้

- Quick Implementation การนำเทคโนโลยี CASE มาใช้เกี่ยวข้องกับการเปลี่ยนแปลงอย่างมีนัยสำคัญจากระบบงานเดิมที่ใช้อยู่ โดยทั่วไปแล้ว องค์กรไม่ควรใช้เครื่องมือ CASE เป็นครั้งแรกที่มีการพัฒนาโครงการสำคัญหรือโครงการที่ใกล้ถึงกำหนดส่งมอบเพราะกระบวนการฝึกอบรมต้องใช้เวลานาน นอกจากนี้ องค์กรควรจะพิจารณาการใช้เครื่องมือกับโครงการที่เล็กกว่า ซับซ้อนน้อยกว่า และการใช้เครื่องมืออย่างค่อยเป็นค่อยไปเพื่อมีเวลาในการฝึกอบรมมากพอ

- Weak Repository Controls ความล้มเหลวในการเข้าถึงการควบคุมที่เก็บข้อมูลในระบบ CASE อาจจะมีผลให้เกิดช่องโหว่ในการรักษาความปลอดภัยหรือทำลายเอกสารประกอบการทำงาน การออกแบบระบบหรือการเขียนโปรแกรมที่เก็บไว้ในคลังข้อมูล การควบคุมรวมถึงการป้องกันคลังข้อมูลโดยการสร้างการควบคุมการเข้าถึง การควบคุมรุ่น และการสำรองข้อมูลที่เหมาะสม

(3) การพัฒนาระบบงานอย่างเร่งด่วน (Rapid Application Development (RAD))

RAD เป็นเทคนิคการพัฒนาอย่างหนึ่งที่ต้องใช้เวลาสั้น ๆ ในการพัฒนา 30 – 90 วัน **เทคนิคนี้ไม่สามารถใช้ได้กับการพัฒนาระบบงานที่ซับซ้อนหรือระบบงานที่ต้องการประมวลผล**

อย่างรวดเร็วกับปริมาณรายการที่มีมาก เช่น การประมวลผลแบบ batch องค์กรอาจจะใช้เทคนิคในการพัฒนาหรือออกแบบใหม่อีกครั้งกับระบบงานที่มีความเสี่ยงต่ำหรือระบบงานที่มีความซับซ้อนน้อยกว่า เช่น การทำรายการบนอินเทอร์เน็ตที่มีปริมาณงานในช่วงเวลาหนึ่งไม่มาก นอกจากนี้ การยึด**ถือ**เกณฑ์ความเสี่ยงที่องค์กรยอมรับได้และการออกแบบระบบงานที่มีความสำคัญ องค์กรอาจจะใช้เทคนิค RAD ในระหว่างขั้นตอนการออกแบบและพัฒนาก็ได้ตามระเบียบวิธีการพัฒนาที่กำหนดไว้แล้ว

ฝ่ายจัดการควรจะพิจารณาความซับซ้อนของหน้าที่การทำงานและความเสี่ยงด้านการรักษาความปลอดภัยของระบบงานเมื่อมีการเลือกใช้วิธีการพัฒนา ฝ่ายจัดการควรจะแน่ใจได้ว่าเทคนิคการพัฒนาที่เลือกนั้นมีความเหมาะสมในการบริหารจัดการความซับซ้อนและความเสี่ยงของระบบงานในการพัฒนา

กระบวนการ RAD อาจจะเข้ามาเกี่ยวข้องเพียง 3 ขั้นตอน คือ ขั้นเริ่มต้น ขั้นพัฒนา และขั้นตอนการนำออกใช้งาน การใช้ระยะเวลาสั้นกับโครงการที่ใช้เทคนิค RAD มีความจำเป็นต้องกำหนดความต้องการหน้าที่การทำงานอย่างรวดเร็ว และความต้องการนั้นต้องไม่มีการเปลี่ยนแปลงมากมายในระหว่างกระบวนการพัฒนา โดยทั่วไปแล้ว ผู้จัดการจะกำหนดให้ผู้ใช้งานมีเวลาเต็มที่กับโครงการและให้อำนาจในการตัดสินใจออกแบบในภาพรวม อย่างไรก็ตาม ปกติแล้วผู้ใช้งานจะปรึกษาผู้เชี่ยวชาญโครงการอยู่แล้ว เช่น ผู้บริหารฐานข้อมูล ผู้เชี่ยวชาญเครือข่ายและผู้พัฒนาระบบเมื่อผู้ใช้งานต้องตัดสินใจในเรื่องที่สำคัญ

โดยปกติแล้วผู้ใช้งานและทีมงาน RAD จะสร้างการออกแบบหน้าที่การทำงานโดยใช้เครื่องมือการออกแบบต้นแบบในกระบวนการพัฒนา โดยสร้าง สอบทานและแก้ไขต้นแบบตามความจำเป็นจนกว่าจะเห็นชอบร่วมกัน

วิธี RAD จะใช้บ่อยกับเทคนิคการเขียนโปรแกรมเชิงวัตถุที่สามารถนำวัตถุที่เขียนแล้วกลับมาใช้ได้อีก ในกรณีของระบบงานที่ถูกออกแบบใหม่อีกครั้ง ผู้ออกแบบและผู้พัฒนาจะเลือกวัตถุที่มีหน้าที่การทำงานพื้นฐานอยู่แล้วโดยนำวัตถุนั้นมาเชื่อมโยงกับวัตถุอื่นที่ต้องการใช้งานทั้งที่เป็นวัตถุที่พัฒนาแล้วและวัตถุที่พัฒนาขึ้นใหม่

การทดสอบจะเกิดขึ้นพร้อม ๆ กับการพัฒนาหน้าที่การทำงานของระบบ องค์กรอาจจะนำกระบวนงานการทดสอบและนำออกใช้งานมาใช้อย่างรวดเร็วหรือกระบวนการทดสอบอื่นที่กำหนดไว้แล้วเหมือนกับแบบวิธี SDLC มาใช้ก็ได้ ความรวดเร็วและโครงสร้างของกระบวนงานทดสอบและนำออกใช้จะขึ้นอยู่กับเกณฑ์ความเสียงที่องค์กรยอมรับได้ การออกแบบระบบงานที่สำคัญและการกำหนดวันสิ้นสุดโครงการ

ผู้พัฒนาจะสร้างระบบงานที่ใช้บนอินเทอร์เน็ตกันมากขึ้นโดยใช้เทคนิค RAD ส่วนการสร้างโดยใช้ CASE ก็มีมากโดยผู้พัฒนาสามารถใช้การรวมการออกแบบหน้าที่การทำงานเชิงวัตถุให้รวมอยู่ในระบบงานได้ **มาตรฐานและการควบคุมที่เหมาะสมควรจะถูกกำหนดไว้เพื่อให้แน่ใจว่า**

- องค์กรใช้เทคนิค RAD เพื่อความเหมาะสมเท่านั้น
- ฝ่ายจัดการได้รวมหน้าที่การรักษาความปลอดภัยและการควบคุมอย่างเพียงพอไว้ในระบบงานที่พัฒนาแล้ว
- ผู้รับรองคุณภาพจะทำการตรวจสอบว่าหน้าที่การทำงานการรักษาความปลอดภัยและการควบคุมนั้นมีอยู่และเป็นไปตามจุดมุ่งหมายที่ตั้งไว้
- ผู้ใช้งานมีส่วนเกี่ยวข้องกับโครงการที่ใช้เทคนิค RAD อย่างเหมาะสม
- ผู้จัดการโครงการต้องดูแลการดำเนินโครงการอย่างใกล้ชิด

2.2.4 ฐานข้อมูล

ฐานข้อมูลจะใช้เก็บข้อมูลและสามารถสร้างได้หลายวิธี ระบบ Legacy จะมีโครงสร้างเป็นลำดับชั้นและเป็นแบบเครือข่าย ฐานข้อมูลแบบลำดับชั้นจะถูกสร้างเหมือนกับผังโครงสร้างองค์กร ข้อมูลส่วนย่อยระดับล่างจะสัมพันธ์กับข้อมูลส่วนย่อยระดับบนหนึ่งชั้น แต่ละส่วนย่อยของข้อมูลสามารถมีหลายส่วนย่อยที่สัมพันธ์กับข้อมูลระดับล่างลงไป แต่มีเพียงหนึ่งเดียวที่เชื่อมโยงกับข้อมูลส่วนย่อยที่เหนือขึ้นไป ฐานข้อมูลแบบเครือข่ายจะเหมือนกับฐานข้อมูลแบบลำดับชั้น แต่ข้อมูลย่อยสามารถเชื่อมโยงกับหลายข้อมูลส่วนย่อยที่เหนือขึ้นไปและที่ต่ำลงมา

ฐานข้อมูลแบบสัมพันธ์กันถือเป็นฐานข้อมูลที่ใช้กันมากที่สุดในปัจจุบันที่เป็นลักษณะตารางที่มีข้อมูลทั้งแนวตั้งและแนวนอน (ทางเดินของข้อมูลไม่ได้ถูกกำหนดไว้ก่อนเพราะว่าความสัมพันธ์ได้ถูกกำหนดไว้ที่ระดับที่เป็นมูลค่าของข้อมูล) ในแนวนอนจะมีข้อมูลที่สัมพันธ์กับหนึ่งหัวข้อในแนวตั้ง เช่น ลูกค้า พนักงาน และผู้ขาย ในแนวตั้งจะมีข้อมูลที่สัมพันธ์กับแต่ละหัวข้อในแนวนอน เช่น เลขบัตรประชาชนของลูกค้า วันเกิด หรือที่อยู่ ในแต่ละแถวของตารางในแนวนอนจะสัมพันธ์กับหัวข้อในแนวตั้งที่ได้ถูกกำหนดไว้แล้วให้เป็นแถวหลัก แถวหลักจะเป็นตัวเชื่อมโยงหลักเกี่ยวกับข้อมูลที่เก็บและความสะดวกในการเข้าถึงข้อมูล โดยทั่วไปแล้ว แถวหลักอาจจะประกอบด้วยข้อมูลที่มากกว่าหนึ่งแถวก็ได้

โดยปกติแล้ว ฐานข้อมูลแบบสัมพันธ์กันจะประกอบด้วยหลายตาราง ที่อาจจะอยู่บนเครื่องคอมพิวเตอร์แม่แบบเดี่ยวหรือแบบหลายเครื่องก็ได้ ถ้าข้อมูลที่สัมพันธ์กันถูกเก็บอยู่ในหลายตาราง แถวหลักที่เหมือนกันจะดึงข้อมูลมาจากแต่ละตารางเพื่อความถูกต้องเชื่อถือได้ของข้อมูล

ฐานข้อมูลแบบสัมพันธ์กันเชิงวัตถุถูกพัฒนาขึ้นให้ใช้กับตัวเชื่อมต่อโปรโตคอลแบบเชิงวัตถุเฉพาะเรื่องในสภาพแวดล้อมของฐานข้อมูลแบบสัมพันธ์กัน มาตรฐานที่ใช้กันอยู่ในปัจจุบันล่าสุดที่เป็นฐานข้อมูลเชิงวัตถุและระบบบริหารฐานข้อมูลยังไม่ได้รับการยอมรับ อย่างไรก็ตาม มาตรฐานหลากหลายก็ยังมีการใช้อยู่และองค์กรพยายามที่จะพัฒนาตัวเชื่อมต่อโปรโตคอลฐานข้อมูลเชิงวัตถุให้เป็นมาตรฐาน

ระบบการบริหารฐานข้อมูล (Database Management Systems (DBMS))

DBMS เป็นโปรแกรมที่ควบคุมสิทธิในการเข้าถึงฐานข้อมูลของผู้ใช้งานและการเข้าแก้ไข ระบบจะช่วยให้สามารถอ้างอิงความถูกต้องได้ สนับสนุนหน้าที่การนำเข้าและการส่งออกข้อมูล และช่วยในการทำสำรองข้อมูลและกู้ข้อมูลคืน

DBMS อาจจะช่วยการเข้าถึงคำอธิบายข้อมูล (data dictionaries) ซึ่งเป็นเครื่องมือการจัดทำเอกสารประกอบอย่างหนึ่งที่เก็บคำอธิบายโครงสร้างและรูปแบบข้อมูลและตารางข้อมูล คำอธิบายข้อมูลขั้นสูง (advanced data dictionaries) อาจจะเก็บข้อมูลการเขียนโปรแกรมต้นฉบับเกี่ยวกับตารางและคำอธิบายการเขียนโปรแกรมเพื่อใช้ระหว่างการออกแบบและพัฒนา

ประเด็นแรกที่ควรพิจารณาเมื่อมีการสอบทานการออกแบบและการจัดเรียงตั้งค่าระบบการบริหารฐานข้อมูล ซึ่งรวมถึงหน้าที่การทำงานของระบบการควบคุมการเข้าถึงและการตรวจสอบ ฝ่ายจัดการควรจะจำกัดการเข้าถึงฐานข้อมูลโดยตรงของบุคคลที่ได้รับอนุญาต

DBMS ส่วนใหญ่มีการทำงานเป็นแบบรายวันในการกำหนดให้มีการติดตามการเปลี่ยนแปลงของข้อมูล ระบบรายวันจะมีร่องรอยให้สามารถตรวจสอบการเปลี่ยนแปลงข้อมูล และช่วยให้การกู้คืนข้อมูลมีความปลอดภัยในกรณีที่เกิดข้อผิดพลาด ถ้ามีการใช้งานระบบนี้ องค์กรควรจะใช้เครื่องมือการตรวจสอบแบบอัตโนมัติ เช่น ระบบรายวันนี้ในการกำหนดให้ใครเข้าถึงหรือพยายามเข้าถึงฐานข้อมูลอะไรเพื่อทราบการเปลี่ยนแปลงของข้อมูล

DBMS ส่วนใหญ่สามารถตรวจสอบผู้ใช้ได้ในระดับของการบันทึกข้อมูลแต่ละรายการและบันทึกการทำงานของผู้ใช้งาน ระดับของการตรวจสอบที่ละเอียดนี้จะช่วยให้มีการควบคุมการรักษาความปลอดภัยที่เข้มแข็งขึ้น **ผู้ตรวจสอบควรจะพิจารณาระดับของการตรวจสอบนี้เมื่อทำการประเมินความเพียงพอของการควบคุม DBMS การควบคุม DBMS ที่ดีรวมถึงมีการบันทึกการ**

เปลี่ยนแปลงข้อมูล การตรวจสอบความถูกต้องของข้อมูลนำเข้า การห้ามการเข้าถึงและการถอยกลับ (ความสามารถในการกู้ข้อมูลคืนก่อนหน้าที่เกิดข้อผิดพลาด) การใช้รหัสลับและการเข้ารหัสลับข้อมูล ผู้พัฒนาระบบควรจะพิจารณารวมถึงแบบของหน้าที่การทำงานของระบบรักษาความปลอดภัยตั้งแต่ขั้นตอนการออกแบบฐานข้อมูล ถ้าไม่มีหน้าที่การทำงานระบบเกี่ยวกับการควบคุมและการตรวจสอบฝ่ายจัดการควรจะนำการควบคุมอื่นมาใช้ทดแทน เช่น การแบ่งแยกหน้าที่และการควบคุมคู่

2.3 การจัดซื้อจัดหา (Acquisition)

สรุปแนวทางการปฏิบัติ

สถาบันการเงินควรจัดให้มีระเบียบวิธีการจัดหาระบบงานและโปรแกรม: การจัดหา ที่เหมาะสมและสอดคล้องกับลักษณะและความเสี่ยงของการดำเนินโครงการรวมถึงความเหมาะสมของปัจจัยดังต่อไปนี้

- แผนงานโครงการจัดหา
- มาตรฐานและกระบวนการดำเนินโครงการ
- การรับประกันคุณภาพ การบริหารความเสี่ยงและมาตรฐานการทดสอบและกระบวนการทดสอบ
- คุณลักษณะของผลิตภัณฑ์ที่ต้องการ
- ผู้ที่มีส่วนเกี่ยวข้องตลอดทั้งกระบวนการ
- การพิจารณาบริษัทผู้จำหน่าย (Vendor) สัญญา (Contract) และเอกสารสิทธิในการใช้งาน (License)

โครงการจัดหา มีลักษณะคล้ายกับโครงการพัฒนาระบบงาน ซึ่งจะประกอบด้วยขั้นตอนการให้ความเห็นชอบโดยระดับบริหาร การกำหนดหน้าที่การทำงานของแต่ละองค์ประกอบของระบบงาน ระบบรักษาความปลอดภัย การกำหนดคุณลักษณะของระบบงานที่ต้องการ กระบวนการทดสอบที่เหมาะสมรวมถึงกระบวนการนำระบบไปใช้งาน สถาบันการเงินมักกำหนดรูปแบบของระเบียบวิธีการจัดหา คล้ายกับวงจรการพัฒนาระบบงาน (SDLC) เมื่อมีความต้องการ hardware และ software ที่สำคัญ อย่างไรก็ดี บางสถาบันการเงินอาจใช้การประกวดราคาเพื่อหาผู้ให้บริการจากภายนอก เพื่อทำหน้าที่ออกแบบวงจรการพัฒนาระบบงาน กระบวนการพัฒนาแต่ละ

ขั้นตอน รายละเอียดหน้าที่การทำงานของแต่ละองค์ประกอบของระบบงาน ระบบรักษาความปลอดภัย และการกำหนดคุณลักษณะของระบบงานที่ต้องการแทนการดำเนินการโดยสถาบันการเงินเอง " แนวทางการดำเนินโครงการจัดหา" พิจารณาจากกิจกรรมต่างๆที่เกี่ยวข้อง (อ้างถึงการบริหารโครงการและงานการพัฒนาระบบงานในส่วนของรายละเอียดที่ต้องพิจารณาเพิ่มเติมเกี่ยวกับวงจรการพัฒนาโดยทั่วไป)

นอกจากนี้ ในการพัฒนากระบวนการจัดหาระบบงานที่มีการแจกแจงรายละเอียดหน้าที่การทำงานของแต่ละองค์ประกอบ ระบบรักษาความปลอดภัย และคุณลักษณะของระบบงานตามที่ต้องการนั้น **สถาบันการเงินควรกำหนดหลักเกณฑ์การคัดเลือกบริษัทผู้จำหน่ายหรือผู้ให้บริการ (Vendor) โดยพิจารณาความมั่นคงของฐานะทางการเงิน ระดับการให้บริการ กระบวนการควบคุมการรักษาความปลอดภัย** และประเด็นที่เกี่ยวข้องอื่นๆ ก่อนการตัดสินใจคัดเลือกผลิตภัณฑ์หรือใช้บริการ รวมถึงการพิจารณาข้อความในสัญญา เพื่อให้มั่นใจว่าสัญญาได้ระบุหน้าที่ความรับผิดชอบของคู่สัญญาแต่ละฝ่ายชัดเจน มีความยุติธรรม และเอกสารสิทธิในการใช้งานระบุว่าสถาบันการเงินมีสิทธิที่ถูกต้องตามกฎหมาย **ความเสี่ยงลำดับแรกมักเกิดจากการระบุความต้องการที่ไม่ครบถ้วน ขาดการประเมินบริษัทผู้จำหน่ายหรือผู้ให้บริการ และไม่ได้ทบทวนสัญญาและข้อตกลงต่างๆ โดยละเอียด**

ประเด็นเกี่ยวกับสัญญาและสิทธิในการใช้งานเป็นสิ่งสำคัญที่ต้องคำนึงถึงในการจัดซื้อ **ฝ่ายกฎหมายของสถาบันการเงิน ควรพิจารณาถึงความชัดเจน รัดกุมเหมาะสมของสัญญา ก่อนนำเสนอผู้บริหารเพื่อลงนาม**

ในบางครั้ง สถาบันการเงินมีความจำเป็นต้องจัดหา software หรือใช้บริการจากบุคคลอื่นที่อยู่ในต่างประเทศ สถาบันการเงิน ควรพิจารณาถึงความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการดังกล่าว เช่นการปฏิบัติตามกฎหมายหรือระเบียบที่เกี่ยวข้องของประเทศคู่สัญญาทุกฝ่าย (อ้างถึง " Software Development Contracts and Licensing Agreements" และ IT Booklet' s Outsourcing Technology Services Booklet ซึ่งกล่าวถึงรายละเอียดเพิ่มเติมต่างๆที่เกี่ยวข้องกับการมีปฏิสัมพันธ์กับบุคคลที่สามในต่างประเทศ)

2.3.1 มาตรฐานการจัดซื้อ (Acquisition Standards)

คณะผู้บริหาร ควรจัดให้มีมาตรฐานการจัดหา ซึ่งประกอบด้วยระบบรักษาความปลอดภัย และปัจจัยอื่นที่เกี่ยวข้องเช่นเดียวกับมาตรฐานการพัฒนาระบบงาน เพียงแต่มาตรฐานการจัดซื้อจะมุ่งเน้นที่ ความรัดกุมของระบบรักษาความปลอดภัย ความน่าเชื่อถือของบริษัทผู้จำหน่าย และผลิตภัณฑ์มีความครบถ้วนตามคุณลักษณะที่ต้องการ มาตรฐานการจัดซื้อควรครอบคลุมถึงหลักเกณฑ์

ในการคัดเลือกบริษัทผู้จำหน่ายที่เหมาะสม การพิจารณาสัญญาและสิทธิในการใช้งานรวมถึงกระบวนการรับมอบผลิตภัณฑ์ที่สามารถทำงานร่วมกับระบบงานอื่นที่มีอยู่เดิมได้

เครื่องมือในการบริหารโครงการจัดซื้อ ที่สำคัญคือ invitation-to-tender หรือrequest for proposals (โดย **invitation-to-tender** ควรใช้ในกรณีที่เกี่ยวข้องกับกระบวนการประกวดราคาของบริษัทผู้จำหน่ายต่างๆ ในกรณีที่ต้องการจัดซื้อ hardware หรือ**ชุดระบบงานรวม** (Integrated system) ของ hardware และ software ส่วน **request for proposals** ควรใช้ในกรณีที่เกี่ยวข้องกับกระบวนการประกวดราคาในกรณีที่ต้องการจัดหาโปรแกรมสำเร็จรูป (off-the-shelf software) จากตัวแทนจำหน่ายหรือจากบริษัทผู้พัฒนา software หรือการจัดหากรณีอื่น ซึ่งบางครั้งใช้คำสลับกัน)

เหตุที่ควรมีมาตรฐานการจัดหารวมอยู่ในกระบวนการบริหารงานจัดหา เพื่อให้มั่นใจว่า คุณลักษณะหน้าที่การทำงานขององค์ประกอบต่างๆ ระบบรักษาความปลอดภัย และกระบวนการปฏิบัติงานที่ต้องการได้ระบุไว้ใน invitation-to-tender หรือ request for proposals อย่างชัดเจนครอบคลุม โดยที่มาตรฐานจะกำหนดให้ผู้ทำหน้าที่บริหารงานต้องพิจารณาเปรียบเทียบระหว่างความต้องการของสถาบันการเงินที่ระบุไว้กับข้อมูลที่บริษัทผู้จำหน่ายต่างๆหรือผู้ให้บริการ นำเสนอเกี่ยวกับผลิตภัณฑ์ ฐานะทางการเงินของบริษัทผู้จำหน่ายหรือผู้ให้บริการ ข้อตกลงในการให้บริการรวมถึงการพิจารณาทบทวนสัญญาโดยฝ่ายกฎหมายของสถาบันการเงินก่อนมีการลงนาม

Note : ความเสี่ยงในการใช้โปรแกรมระบบงานสำเร็จรูปที่ใช้กับธุรกิจทั่วไป เช่น word จะระบุรายละเอียดในข้อตกลงหรือสัญญา รวมถึงมีขั้นตอนในกระบวนการจัดหาน้อยกว่าการจัดหาโปรแกรมระบบงานที่ใช้กับธุรกิจด้านการเงิน ทั้งนี้การกำหนดระดับความสำคัญของการจัดหาขึ้นอยู่กับความเสี่ยงและความมีนัยสำคัญของโปรแกรมระบบงานนั้นๆ ที่มีต่อสถาบันการเงินเป็นรายกรณี

2.3.2 แนวทางการดำเนินโครงการจัดซื้อ (Acquisition Project Guidance)

การดำเนินโครงการจัดซื้อเริ่มจากผลสรุปความต้องการของโครงการ การกำหนดกระบวนการดำเนินงานต่างๆ และ**กระบวนการบริหารจัดการที่ครบวงจร เพื่อสนับสนุนให้การจัดหาได้ผลิตภัณฑ์ที่มีคุณลักษณะตามความต้องการที่ระบุไว้** คุณลักษณะของผลิตภัณฑ์ที่ต้องการแสดงให้ทราบถึง เงื่อนไขที่ธุรกิจต้องการ (business case) หน้าที่การทำงานขององค์ประกอบต่างๆ ของระบบงาน ขอบเขตความสามารถ รายละเอียดอื่นๆที่เกี่ยวข้อง การเชื่อมโยงเครือข่ายสื่อสาร องค์ประกอบของ hardware และ software application ซึ่งสนับสนุนการทำงานของผลิตภัณฑ์ที่ต้องการจัดซื้อหา ผู้บริหารควรมีกระบวนการศึกษาความเป็นไปได้เพื่อพิจารณาตัดสินใจในการคัดเลือกซื้อ

ผลิตภัณฑ์ให้สนับสนุนเงื่อนไขที่ธุรกิจต้องการ (business case) อย่างเหมาะสมระหว่างโปรแกรมระบบงานแบบที่ต้องพัฒนาเพิ่ม (customized) หรือโปรแกรมระบบงานสำเร็จรูป (off-the-shelf software) นอกจากนี้ผู้เกี่ยวข้องทุกฝ่ายควรจัดทำเอกสารประกอบการพิจารณาให้ความเห็นชอบในทุกขั้นตอน

กระบวนการพิจารณาความเป็นไปได้ของข้อเสนอในการจัดหาและแนวคิดเกี่ยวกับประเด็นที่ใช้ประกอบการพิจารณา ซึ่งอาจเลือกใช้ตามความเหมาะสมสำหรับการจัดหาแต่ละกรณี

- เป้าหมายทางธุรกิจ (Business objectives)
- เป้าหมายของเทคโนโลยีที่ต้องการ (Technology objectives)
- หน้าที่การทำงานของระบบงานที่ต้องการ (Functional requirements)
- ระบบรักษาความปลอดภัยที่ต้องการ (Security requirements)
- กระบวนการควบคุมภายในที่ต้องการ (Internal control requirements)
- เอกสารประกอบที่เกี่ยวข้องที่ต้องการ (Documentation requirements)
- ประสิทธิภาพที่ต้องการ (Performance requirements)
- รูปแบบระบบเครือข่ายสื่อสารที่ต้องการ (Network requirements)
- ระบบงานที่ต้องการให้เชื่อมโยงกัน (System interface requirements)
- การเอื้ออำนวยต่อการปรับปรุงเพิ่มเติมที่ต้องการ (Expandability requirements)
- ความน่าเชื่อถือของบริษัทผู้จำหน่าย (Reliability requirements)
- การซ่อมแซมบำรุงรักษา (Maintenance requirements)
- รูปแบบการติดตั้งใช้งานที่ต้องการ (Installation requirements)
- รูปแบบการเปลี่ยนแปลงโอนย้ายงานที่ต้องการ (Conversion requirements)
- ความต้องการด้านบุคลากร (Personnel requirements)
- กระบวนการประมวลผลที่ต้องการ (Processing requirements)
- มาตรฐานการพัฒนาผลิตภัณฑ์ (Product development standards)
- มาตรฐานการออกแบบผลิตภัณฑ์ (Product design standard)
- กระบวนการทดสอบที่ต้องการ (Testing requirements)
- กระบวนการฝึกอบรมที่ต้องการ (Training requirements)
- ความมั่นคงทางการเงินของบริษัทผู้จำหน่ายหรือผู้ให้บริการ (Vendor's financial strength)

- ระดับการให้บริการของบริษัทผู้จำหน่ายหรือผู้ให้บริการ (Vendor's support levels)

- การวิเคราะห์ต้นทุนและผลตอบแทน (Cost/benefit analysis)

การพิจารณาความเป็นไปได้ของโครงการ **ผู้ทำหน้าที่บริหารควรปรึกษากับตัวแทนของหน่วยงานต่าง ๆ** ดังที่แสดงด้านล่าง ซึ่งตัวแทนเหล่านี้อาจเข้าร่วมให้คำปรึกษาตลอดการดำเนินโครงการหรืออาจเข้าร่วมเฉพาะบางกรณีขึ้นอยู่กับความเหมาะสมและหน้าที่ความรับผิดชอบที่กำหนด ได้แก่

- หน่วยงานตรวจสอบภายใน (Audit personnel)
- ผู้บริหารหน่วยงานธุรกิจที่เกี่ยวข้อง (Business unit managers)
- ผู้บริหารฐานข้อมูล (Database administrators)
- ตัวแทนผู้ใช้งาน (End users)
- หน่วยงานกฎหมาย (Legal counsel)
- ผู้บริหารด้านเครือข่ายสื่อสาร (Network administrators)
- เจ้าหน้าที่เทคนิคด้านเครือข่ายสื่อสาร (Network technicians)
- หน่วยงานควบคุมคุณภาพ (Quality assurance personnel)
- ผู้บริหารด้านการรักษาความปลอดภัย (Security administrators)
- เจ้าหน้าที่วิเคราะห์ระบบ (System analysts)
- ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ (Technology department managers)
- ตัวแทนของบริษัทผู้จำหน่ายหรือผู้ให้บริการ (Vendor personnel)

กรณีที่ได้รับข้อมูลแสดงคุณลักษณะของความต้องการที่มีความเป็นไปได้ในการจัดหา การศึกษาข้อมูลจากแหล่งอื่นๆจะช่วยสนับสนุนเกี่ยวกับรายละเอียดคุณลักษณะของหน้าที่ต่างๆ รายละเอียดการทำงานของระบบงานที่ต้องการ ที่ควรจะต้องระบุไว้ใน request for proposals หรือ invitation of tender ซึ่งผู้ทำหน้าที่บริหารจะต้องแจ้งให้ผู้ให้บริการหรือบุคคลที่สามที่เสนอชื่อเข้ามาในกระบวนการประกวดราคาทราบ

หลังจากที่สถาบันการเงินได้รับคำเสนอหรือซองประกวดราคา จะต้องพิจารณาเปรียบเทียบระหว่างความต้องการที่ระบุไว้กับรายละเอียดจากบริษัทผู้จำหน่ายหรือผู้ให้บริการที่ผู้ยื่นคำเสนอหรือซองประกวดราคาทุกราย ซึ่งรายละเอียดดังกล่าวควรต้องแสดงข้อมูลรายการที่สามารถ

สนองความต้องการที่สถาบันการเงินระบุไว้อย่างชัดเจนและควรระบุถึงข้อมูลเกี่ยวกับคุณสมบัติอื่นที่ผลิตภัณฑ์ของตนมีนอกเหนือจากที่ระบุไว้ใน request for proposals หรือ invitation of tender เช่น

(1) Software ควรระบุถึง

- มาตรฐานกระบวนการรักษาความลับ (Confidentiality standard)
- **ความสามารถในการทำงานร่วมกับระบบปฏิบัติการใดได้บ้าง** (Compatible operating systems)
- มาตรฐานเกี่ยวกับลิขสิทธิ์ (Copyright standards)
- ระยะเวลาในการส่งมอบงาน (Delivery dates)
- ขอบเขตในการทำสัญญาข้อตกลงกับบุคคลที่สาม (Escrow criteria)
- ขอบเขตหน้าที่ความรับผิดชอบ (Liability limitations)
- ข้อจำกัดเกี่ยวกับการอนุญาตใช้งาน (Licensing restrictions)-
- กระบวนการเกี่ยวกับการซ่อมแซม บำรุงรักษา (Maintenance procedures)
- วันที่ที่จะออกผลิตภัณฑ์รุ่นใหม่ (Next release date)
- ข้อกำหนดของหน่วยงานผู้กำกับดูแล (Regulatory requirements)
- ภาษาของ software (Software language)
- รายละเอียดของตัวแทนจำหน่าย (Subcontractor detail)
- มาตรฐานเกี่ยวกับการทดสอบ (Testing standards)
- รายละเอียดเกี่ยวกับการรับประกัน (Warranty specifications)

(2) Hardware ควรระบุถึง

- รายละเอียดเกี่ยวกับกระบวนการสำรอง (Backup option)
- รายละเอียดเกี่ยวกับการซ่อมแซม บำรุงรักษา (Maintenance requirements)
- ปริมาณความจุของหน่วยความจำ (Memory capacities)
- ระดับประสิทธิภาพ (Performance capabilities)
- รายละเอียดกระบวนการให้บริการ (Servicing option)

กระบวนการดำเนินการต่างๆ ที่กำหนดขึ้น เพื่อให้มั่นใจว่าสถาบันการเงินมีการพิจารณาทบทวนกระบวนการประกวดราคาที่เหมาะสม หลังจากผ่านขั้นตอนการคัดเลือกบริษัทผู้จำหน่ายหรือผู้ให้บริการแล้ว ผู้ทำหน้าที่บริหารงานต้องพิจารณาทบทวน ฐานะทางการเงิน และข้อตกลงในการให้บริการของบริษัทที่คัดเลือก และฝ่ายกฎหมายควรพิจารณาสัญญาก่อนมีการลงนาม

2.3.3 การจัดทำเอกสารข้อตกลงกับบุคคลที่สาม (Escrowed Documentation)

โปรแกรมระบบงานที่ถูกเขียนขึ้น จำแนกในลักษณะต่างๆ คือ open source code แบบไม่มีกรรมสิทธิ์ open source code แบบมีกรรมสิทธิ์ หรือ closed source code แบบมีกรรมสิทธิ์

โปรแกรมระบบงาน **open source code แบบไม่มีกรรมสิทธิ์** ในบางครั้งจะหมายถึง software ที่สามารถนำมาใช้งานได้โดยไม่มีค่าใช้จ่าย ซึ่งเป็นการพัฒนาขึ้นเพื่อประโยชน์แก่สาธารณชน โดยปกติสามารถใช้งาน คัดลอก ปรับปรุงแก้ไขโดยไม่มีข้อจำกัด **โปรแกรมระบบงาน open source code แบบมีผู้ถือครองสิทธิ์** เป็นโปรแกรมระบบงานที่พัฒนาเพื่อประโยชน์แก่สาธารณชนเช่นกัน แต่สิทธิ์ในการคัดลอกและแจกจ่ายเพื่อใช้งานต้องเป็นไปตามสัญญาที่ระบุไว้ในสัญญาการใช้งาน ผู้บริหารต้องพิจารณาสัญญาการใช้งานโปรแกรมระบบงานทั้งหมดภายในองค์กรเพื่อให้แน่ใจว่าการนำไปใช้งาน การปรับปรุงแก้ไข หรือการจัดสรรแจกจ่ายไปยังหน่วยงานต่างๆ เป็นไปตามสัญญา [1]

โดยปกติ **โปรแกรมระบบงาน closed source code แบบมีกรรมสิทธิ์ เป็นลิขสิทธิ์ทางการค้าและถือเป็นความลับของบริษัทผู้พัฒนาหรือเป็นเจ้าของโปรแกรม** บริษัทผู้จำหน่ายส่วนใหญ่จะไม่ส่งมอบ closed source code ให้แก่องค์กรที่ซื้อหรือเช่า เพื่อป้องกันความถูกต้องครบถ้วนและลิขสิทธิ์ของ software อีกแนวทางหนึ่งที่จะให้มี source information คือการลงโปรแกรมระบบงานด้วย object code และนำ source code ไปทำสัญญากับบุคคลที่สาม (escrow agreement) การทำสัญญาดังกล่าว **องค์กรผู้ซื้อสามารถนำ source code ไปใช้งานได้ได้ตามเงื่อนไขที่ตกลงไว้ในสัญญา เช่น กรณีที่ผู้ทำหน้าที่ดูแลให้บริการสนับสนุนหรือบริษัทผู้จำหน่ายเลิกกิจการ**

โดยทั่วไป แม้ว่ามีบุคคลที่สามที่มีความเป็นอิสระทำหน้าที่เก็บรักษา source code ตามสัญญา (Escrow) แต่สถาบันการเงินยังคงต้องมีการตรวจสอบเป็นระยะอย่างน้อยปีละครั้งเพื่อให้แน่ใจว่า บุคคลที่สามที่ทำหน้าที่รักษา source code นั้น ถือชุด source code ที่เป็นปัจจุบัน ขณะนี้พบว่ามี Escrow agent ทำหน้าที่ให้บริการตรวจสอบเพื่อรับรองเลขที่ของ version และวันที่ที่มีการปรับปรุงครั้งล่าสุดของ source code บาง escrow agent ใช้ automated code ตรวจสอบความถูกต้องครบถ้วนของ source code ที่เก็บรักษาไว้ที่บุคคลที่สาม [2]

---

[1] ข้อมูลเพิ่มเติม องค์กรที่ใช้ หรือพิจารณาเลือกใช้ open source software ควรหารือฝ่ายกฎหมายเพื่อพิจารณาทบทวน คำนิยามของ open source มาตรฐานเกี่ยวกับลิขสิทธิ์การใช้งาน ขอบเขตของเอกสารการรับรอง และรายละเอียดเกี่ยวกับการแจกจ่ายแก่หน่วยงานต่างๆขององค์กรเพื่อใช้งาน ตัวอย่าง เช่น www.opensource.org

[2] ฝ่ายบริหารควรพิจารณาถึงแนวทางปฏิบัติและผลทางกฎหมายกรณีการทำสัญญากับบริษัทที่อยู่ในต่างประเทศ หากมีความจำเป็นต้องติดต่อกับคู่สัญญาที่อยู่ในต่างประเทศ

นอกจากนี้เพื่อป้องกันการเข้าใช้งานเอกสารที่เกี่ยวข้องซึ่งเก็บรักษาไว้ที่บุคคลที่สาม (current documentation) จากผู้ไม่มีสิทธิ์ สถาบันการเงินควรพิจารณาถึงการป้องกันสิทธิในทรัพย์สินที่เก็บรักษาไว้กับบุคคลที่สาม (escrow rights) โดยการทำข้อตกลงกับบริษัทผู้จำหน่ายเกี่ยวกับการรายงานให้สถาบันการเงินทราบกรณีที่บริษัทผู้จำหน่ายนำสิทธิใน software ดังกล่าวไปเป็นหลักประกันเงินกู้ยืม

ในการบริหารงานควรพิจารณาถึงรายละเอียดต่างๆ ของสัญญาการเก็บรักษาทรัพย์สิน (Escrow agreement) ซึ่งควรรวมถึง

- คำนิยามของโปรแกรมและระบบงานขั้นต่ำ [3]
- คำนิยามของวิธีปฏิบัติในการบำรุงรักษา software
- เงื่อนไขเกี่ยวกับการแจ้งให้บริษัทผู้จำหน่ายทราบก่อนที่สถาบันการเงินจะนำ source information ที่เก็บรักษาไว้กับบุคคลที่สามไปใช้งาน
- การรับรองว่า source program และเอกสารที่เกี่ยวข้อง (escrow information) ที่เก็บรักษาไว้ที่ escrow agent จะต้องเป็นชุดล่าสุดหรือชุดที่เป็นปัจจุบัน รวมถึง source program จะต้องได้รับการปรับปรุงให้เป็นปัจจุบันทุกครั้งที่บริษัทผู้จำหน่ายมีการปรับปรุงเปลี่ยนแปลงโปรแกรมดังกล่าว
- การเตรียมการในการตรวจสอบหรือทดสอบ escrow code
- รายละเอียดของสื่อที่ใช้บันทึก source information เช่น magnetic tape disc หรือเอกสารข้อมูลที่พิมพ์ออกมาจากคอมพิวเตอร์ (hard copy) และการรับรองความสามารถในการใช้งานสื่อบันทึกข้อมูลดังกล่าวกับระบบเทคโนโลยีของสถาบันการเงิน
- การรับรองความสามารถในการใช้งานของ escrow code ที่เก็บรักษาไว้

อนึ่ง การนำ source code ไปทำสัญญากับบุคคลที่สาม (escrow agreement) เพื่อป้องกันความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากกรณีที่บริษัทผู้จำหน่ายหรือบริษัทเจ้าของโปรแกรม

---

[3] เอกสารที่เกี่ยวข้องกับ software ที่เก็บรักษาที่ escrow agent อย่างต่ำควรต้องมี คำบรรยายลักษณะระบบงาน (system narratives) system flow charts สารบัญรายชื่อ source program (program source listing) คำบรรยายลักษณะโปรแกรม (program narratives)โครงแบบ file และ record (file and record layout) รายละเอียดของ field ในแต่ละ record (descriptions of individual fields within the records) และ ชุดคำสั่งย่อยที่ใช้ในการคำนวณ (calculation routines) รวมถึงคู่มือสำหรับผู้ใช้งานสำหรับระบบงานที่ส่งมอบให้สถาบันการเงิน , transaction code และ รายละเอียดเกี่ยวกับ รูปแบบของข้อมูลนำเข้า และรายงานที่ออกจากระบบ (input forms and output reports)

ระบบงานเลิกกิจการ อย่างไรก็ดี สถาบันการเงินอาจพิจารณาใช้แนวทางป้องกันความเสี่ยงวิธีอื่นทดแทนตามความความเหมาะสมกับระดับนัยสำคัญของความเสี่ยงและผลกระทบจากกรณีดังกล่าว

2.3.4 สัญญาการพัฒนาและข้อตกลงการอนุญาตให้ใช้ Software (Software Development Contracts And Licensing Agreements)

(1) ภาพรวม

ข้อตกลงระหว่างสถาบันการเงินและบริษัทผู้จำหน่าย จะต้องระบุถึงรายละเอียดเกี่ยวกับสิทธิในการใช้งานและหน้าที่ความรับผิดชอบของคู่สัญญาแต่ละฝ่ายอย่างชัดเจน สัญญาควรจัดทำเป็นลายลักษณ์อักษรระบุรายละเอียดเกี่ยวกับประสิทธิภาพของ software สิทธิในการนำ source code มาใช้งาน ระบบรักษาความปลอดภัยของโปรแกรมระบบงานและข้อมูล และรายละเอียดอื่นที่สำคัญ และควรให้ฝ่ายกฎหมายพิจารณาทบทวนสัญญาก่อนที่จะนำเสนอฝ่ายบริหารเพื่อลงนาม

สถาบันการเงินอาจประสบกับภาวะที่บริษัทผู้จำหน่าย software ไม่สามารถหรือไม่ยินยอมตามเงื่อนไขที่สถาบันการเงินต้องการ ภายใต้สภาวะดังกล่าว **สถาบันการเงินควรพิจารณาเปรียบเทียบระหว่างประโยชน์ที่คาดว่าจะได้รับจากการใช้ software กับความเสี่ยงจากการที่ Softwareไม่มีเงื่อนไขตามที่สถาบันการเงินต้องการ** หรือจะพิจารณาใช้ software แบบอื่นหรือของบริษัทผู้จำหน่ายอื่นแล้วแต่ความเหมาะสม

(2) สิทธิบัตรการใช้ software (โดยทั่วไป) (Software Licenses –General)

ตามปกติเราใช้**คำว่าจ่ายค่าสิทธิบัตรการใช้ software** เมื่อกล่าวถึง software ไม่ใช้คำว่าได้ซื้อ software ภายใต้สัญญาเกี่ยวกับสิทธิบัตรการใช้ software สถาบันการเงินจะไม่ได้รับสิทธิความเป็นเจ้าของ software แม้ในกรณีที่สถาบันการเงินเสียค่าใช้จ่ายในการพัฒนา software ดังกล่าวก็ตาม ในฐานะผู้รับผิดชอบค่าใช้จ่ายในการพัฒนา software สถาบันการเงินจะได้รับเพียงสิทธิบัตรในการใช้งาน software ที่พัฒนาขึ้นเท่านั้น โดยหลักการทั่วไป **บริษัทผู้จำหน่ายจะมอบสิทธิบัตรในการใช้ software โดยกำหนดระยะเวลาของสิทธิบัตรและคิดค่าธรรมเนียมในการใช้งาน software เป็นรายปี** บริษัทผู้จำหน่ายจะต้องจัดทำสัญญาการบำรุงรักษา (maintenance agreement) เพื่อให้สถาบันการเงินมั่นใจว่าจะได้รับการบำรุงรักษา หรือปรับปรุง software ให้เป็นปัจจุบันทุกครั้งที่บริษัทผู้จำหน่ายออก version หรือ release ใหม่

สิ่งสำคัญเกี่ยวกับสิทธิบัตรในการใช้ software คือ คำนิยามเกี่ยวกับขอบเขตของสิทธิ์ สถาบันการเงินต้องมั่นใจว่าสิทธิบัตรการใช้ software มีความชัดเจน เป็นการให้สิทธิ์เพื่อใช้เฉพาะในองค์กรใดองค์กรหนึ่งหรือไม่เฉพาะเจาะจง ผู้ได้รับอนุญาตใช้งานเป็นใครบ้างและมีจำนวน

เท่าไรรวมถึงมีการจำกัดสถานที่ในการใช้หรือไม่ ก่อนการตกลงทำสัญญาเกี่ยวกับลิขสิทธิ์การใช้ software **สถาบันการเงินควรพิจารณาว่า software ที่เลือกใช้สามารถรองรับความต้องการขององค์กรได้ทั้งในปัจจุบันและในอนาคต**

สิทธิบัตรควรระบุ ถึงผู้ที่ได้รับอนุญาตให้ใช้งานและสถานที่ที่กำหนดให้ใช้งานที่ชัดเจน กรณีที่สถาบันการเงินพิจารณาเลือกการกำหนดสถานที่ใช้งานแต่ไม่จำกัดจำนวนผู้ใช้งาน จะต้องมั่นใจว่าสิทธิบัตรมีความครอบคลุมถึงกรณีดังกล่าว **กรณีที่สถาบันการเงินต้องการให้ผู้ที่เกี่ยวข้องมีสิทธิใช้งาน software ด้วย เช่น บริษัทในเครือหรือบริษัทลูก จะต้องระบุขอบเขตดังกล่าวไว้ในสิทธิบัตร** สถาบันการเงินจะ**ต้องมั่นใจว่าสิทธิบัตรครอบคลุมถึงการยินยอมให้ทำสำเนาชุด software ของระบบงานสำคัญ (mission critical software) และนำไปเก็บรักษาไว้ที่ศูนย์คอมพิวเตอร์สำรองเพื่อเตรียมความพร้อมตามแผนกู้คืนระบบ (disaster recovery Program) หรือแผนดำเนินธุรกิจอย่างต่อเนื่อง (business continuity program)**

สถาบันการเงินควรทำความเข้าใจเกี่ยวกับระยะเวลาสิ้นสุดของสิทธิ์การใช้งานให้ชัดเจน เพื่อป้องกันมิให้เกิดกรณีของสิทธิบัตรหมดอายุโดยไม่ทราบล่วงหน้า ถ้าสถาบันการเงินใช้ software ประเภทที่สิทธิบัตรไม่มีระยะเวลา จะต้องพิจารณาด้วยว่าข้อตกลงกับบริษัทผู้จำหน่ายรองรับสิทธิการใช้งานดังกล่าว โดยไม่ควรสันนิษฐานเองว่ากรณีที่สิทธิบัตรไม่ระบุระยะเวลาของสิทธิ์หรือแสดงเวลาสิ้นสุดไว้หมายความว่าเป็นสิทธิบัตรประเภทที่ไม่มีระยะเวลาสิ้นสุด สถาบันการเงินควรระบุระยะเวลาของสิทธิการใช้งานไว้ในข้อตกลงในกรณีของสิทธิบัตรที่มีกำหนดเวลารวมถึง**ระยะเวลาขั้นต่ำที่ต้องแจ้งให้ทราบล่วงหน้าก่อนที่สิทธิ์การใช้งานจะสิ้นสุดลง**

(3) สิทธิบัตรการใช้ software และการละเมิดลิขสิทธิ์ (Software Licenses And Copyright Violations)

การใช้ software โดยไม่ได้รับสิทธิ์หรือละเมิดสัญญาเกี่ยวกับสิทธิ์การใช้งาน อาจทำให้สถาบันการเงินต้องคดีความ การบริหารจัดการกรณีที่ซื้อ software เกี่ยวกับเครือข่ายควรเป็นไปด้วยความระมัดระวังเนื่องจากบางโปรแกรมไม่อนุญาตให้ใช้งานร่วมกับผู้อื่นซึ่งสถาบันการเงินจะต้องจัดซื้อสำหรับผู้ใช้งานแต่ละบุคคล นอกจากนี้สิทธิบัตรเครือข่ายบางประเภทยินยอมให้มีผู้ใช้งานในเวลาเดียวกันตามจำนวนที่กำหนดไว้เท่านั้น

มาตรการที่สถาบันการเงินควรใช้ในการป้องกันการฝ่าฝืนลิขสิทธิ์รวมถึงการได้รับอนุญาตให้ใช้software ณ ที่ทำการของสถาบันการเงิน คือการสื่อสารให้พนักงานได้ทราบถึงระเบียบในการใช้งานและจัดหาโปรแกรมตรวจจับการใช้ software ที่ไม่ได้รับอนุญาตหรือการฝ่าฝืน

ลิขสิทธิ์ เครื่องมือดังกล่าวช่วยป้องกันการละเมิดลิขสิทธิ์ได้ในระดับหนึ่ง **การควบคุมที่ดีที่สุดคือการกำหนดนโยบายในการบริหารจัดการที่รัดกุม มีผู้ตรวจสอบติดตามดูแลให้มีการปฏิบัติตามนโยบายการบริหารจัดการไม่ควรมีการผ่อนผันในกรณีของการละเมิดลิขสิทธิ์** ผู้ดูแลด้านรักษาความปลอดภัยของสถาบันการเงิน (Security Administrator) ควรทำหน้าที่ติดตามดูแลให้มีการปฏิบัติตามนโยบายดังกล่าว

(4) ข้อกำหนดทางคุณลักษณะของการพัฒนา software และมาตรฐานในการวัดประสิทธิผลของการพัฒนา (Software Development Specifications And Performance Standards)

ข้อตกลงในการพัฒนา software ให้เหมาะสมตามที่สถาบันการเงินต้องการ ควรระบุรายละเอียดคุณลักษณะและหน้าที่การทำงานของแต่ละองค์ประกอบที่สถาบันการเงินต้องการ ข้อตกลงควรระบุถึง hardware ที่จัดหามาใช้ปฏิบัติงานกับ software ที่จะพัฒนาขึ้นจะต้องสามารถใช้งานร่วมกับ hardware เดิมของสถาบันการเงินได้ บริษัทผู้จำหน่ายที่ได้รับการคัดเลือกควรเป็นบริษัทที่สามารถปฏิบัติตามนโยบายและมาตรฐานการพัฒนาระบบงานที่สถาบันการเงินกำหนด ทั้งนี้เนื่องจากก่อนที่สถาบันการเงินจะมีการตกลงหรือออก request-for-proposal สำหรับการพัฒนา software ตามลักษณะเฉพาะที่ต้องการ สถาบันการเงินจะควรต้องกำหนดแนวทางในการจัดหา software ที่ชัดเจน สามารถระบุคุณลักษณะ software ที่เหมาะสมกับความต้องการทางธุรกิจ รวมถึงต้องมีความเข้าใจเกี่ยวกับสถาปัตยกรรมของระบบงานทั้งในปัจจุบันและในอนาคต

ข้อตกลงควรระบุถึงรายละเอียดคุณสมบัติขององค์ประกอบในแต่ละกระบวนการทำงานของ software ที่สถาบันการเงินต้องการ รวมถึงวัตถุประสงค์ที่ต้องการให้บริษัทผู้จำหน่ายดำเนินการในช่วงเวลาการพัฒนา ข้อตกลงในการพัฒนาควรครอบคลุมถึงเงื่อนไขการอนุญาตให้เปลี่ยนแปลงแก้ไขคุณสมบัติและประสิทธิภาพจากมาตรฐานเดิมในระหว่างเวลาที่ดำเนินการพัฒนา

ข้อตกลงการพัฒนาระบบงานควรระบุถึงประสิทธิภาพขององค์ประกอบต่างๆ ของ software ที่ต้องการให้มี ก่อนการตรวจรับระบบงานตามมาตรฐานที่สถาบันการเงินกำหนด ข้อตกลงจะต้องระบุถึงลักษณะเฉพาะที่ต้องการทดสอบที่สนับสนุนว่า software ที่พัฒนาขึ้นเป็นไปตามมาตรฐานที่กำหนด และ**ควรระบุถึงหน้าที่ความรับผิดชอบของบริษัทผู้จำหน่ายกรณีที่ software ไม่ผ่านการทดสอบมากกว่าหนึ่งครั้ง**

(5) กระบวนการจัดทำเอกสารประกอบ การปรับปรุงเปลี่ยนแปลง การปรับให้เป็นปัจจุบัน และการโอนย้ายข้อมูล (Documentation, Modification, Update And Conversion)

การจัดทำร่างเอกสารสิทธิ์ในการใช้ software หรือสัญญาการพัฒนา software ควรระบุให้บริษัทผู้จำหน่ายส่งมอบเอกสารประกอบต่างๆ ที่เกี่ยวข้องซึ่งรวมถึงเอกสารประกอบโปรแกรมระบบงานและคู่มือผู้ใช้งาน

สิทธิบัตรหรือสัญญาการบำรุงรักษาควรระบุถึงสิทธิ์ประโยชน์ที่สถาบันการเงินจะได้รับตามสัญญาและค่าใช้จ่ายในการปรับปรุงเปลี่ยนแปลงหรือปรับ software ให้เป็น Version ปัจจุบัน ในการจัดทำร่างสัญญาการบำรุงรักษาสถาบันการเงินควรพิจารณาถึงกรณีของการยินยอมให้บริษัทผู้จำหน่ายมีสิทธิในการเข้าถึง source code หรือ object code (ไม่ว่าจะให้สิทธิเข้าถึงได้เฉพาะ object code หรือให้สิทธิในการเข้าถึง source code ด้วยก็ตาม) การให้สิทธิแก่บริษัทผู้จำหน่ายในการเข้าถึงแบบจำกัดขอบเขตและการให้ความร่วมมือของบริษัทผู้จำหน่าย เป็นสิ่งจำเป็นที่ควรพิจารณา ในกรณีของการดำเนินการปรับปรุงเปลี่ยนแปลง software ให้มีคุณสมบัติตามที่สถาบันการเงินต้องการ **นอกจากนี้การปรับปรุงเปลี่ยนแปลง source code อาจเป็นผลให้สัญญาบำรุงรักษาเป็นโมฆะได้**

ในการเจรจาตกลงเรื่องสิทธิบัตรการใช้ software สถาบันการเงินควรคำนึงถึงกรณีของการโอนย้ายไปใช้งานกับ software ที่แตกต่างออกไปในอนาคต สิทธิบัตรควรเอื้อต่อการเปลี่ยนแปลง ไม่ควรจำกัดการโอนย้ายข้อมูลไปสู่รูปแบบอื่น หากเป็นไปได้สถาบันการเงินควรเจรจาให้สิทธิบัตรระบุถึงการยินยอมให้บริษัทอื่นสามารถเข้าถึง software เพื่อสนับสนุนการย้ายข้อมูลโดยไม่ถือเป็นการละเมิดลิขสิทธิ์

(6) การล้มละลาย (Bankruptcy)

นอกจากนี้**ในส่วนของสัญญากับบุคคลที่สาม (Escrow agreement)** สถาบันการเงินควรจะต้องพิจารณาถึงสาระสำคัญที่จำเป็นอื่นๆที่เกี่ยวข้องกับสัญญาสิทธิบัตร เพื่อป้องกันความเสี่ยงในกรณีที่บริษัทผู้จำหน่ายประสบภาวะล้มละลาย ในการจัดหา software ที่สำคัญ (mission critical software) **สถาบันการเงินควรหารือฝ่ายกฎหมายเพื่อให้มีข้อตกลงที่ดีที่สุดที่เกี่ยวข้องกับกฎหมายล้มละลาย** สัญญาที่มีความครบถ้วนสมบูรณ์จะพิทักษ์สิทธิประโยชน์แก่สถาบันการเงินหากบริษัทผู้จำหน่ายประสบภาวะล้มละลาย

(7) ข้อกำหนดของผู้กำกับดูแล (Regulatory Requirements)

สถาบันการเงินควรนำข้อกำหนดของผู้ทำหน้าที่กำกับดูแลในส่วนของหน้าที่โดยเฉพาะของ software เข้าเป็นส่วนหนึ่งของสัญญา โดยสัญญาควรต้องระบุให้บริษัทผู้จำหน่ายดำเนินการปรับปรุง software ให้มีการทำงานตามข้อกำหนดของผู้ทำหน้าที่กำกับดูแลในเรื่องที่เกี่ยวข้อง

(8) การชำระเงิน (Payments)

โดยปกติสัญญาจ้างพัฒนา software จะกำหนดให้มีการชำระค่าใช้จ่ายบางส่วนเป็นระยะตามขั้นตอนความสำเร็จของงานที่ระบุไว้และชำระงวดสุดท้ายหลังจากการเสร็จสิ้นกระบวนการทดสอบและลงนามรับรองการทดสอบแล้ว (acceptance test) **สถาบันการเงินควรกำหนดระยะเวลาการชำระเงินกับขั้นตอนความสำเร็จของงานอย่างเหมาะสมเพื่อกระตุ้นให้ผู้พัฒนาดำเนินงานโครงการที่ตกลงกันให้แล้วเสร็จสมบูรณ์โดยเร็ว** การกำหนดช่วงการชำระเงินตามขั้นตอนความสำเร็จของงานที่เหมาะสมเป็นผลให้สถาบันการเงินสามารถติดตามความคืบหน้าในการดำเนินโครงการของผู้พัฒนาได้อย่างใกล้ชิดและทราบถึงปัญหาในการดำเนินงาน

สถาบันการเงินควรระบุเรื่องการผิดสัญญาและค่าสินไหมทดแทนในกรณีที่ผู้พัฒนาไม่ปฏิบัติตามข้อตกลงในสัญญาเกี่ยวกับระยะเวลาและสาระสำคัญของงานไว้ในสัญญาการพัฒนาsoftware ด้วย การระบุจำนวนเงินที่จะจ่ายในแต่ละงวดของขั้นตอนความสำเร็จไว้ในสัญญาทำให้สถาบันการเงินสามารถควบคุมดูแลการพัฒนาได้ครอบคลุมทั้งกระบวนการรวมถึงสามารถควบคุมค่าใช้จ่ายโครงการได้อีกด้วย

สัญญาการพัฒนา software จะต้องระบุถึงรายละเอียดของคุณลักษณะที่สำคัญและหน้าที่การทำงานของแต่ละองค์ประกอบที่ต้องการทั้งหมด กรณีที่ผู้พัฒนาไม่สามารถส่งมอบงานที่เป็นไปตามความต้องการในสัญญาไม่ว่าส่วนหนึ่งส่วนใดสถาบันการเงินมีสิทธิ์ที่จะปฏิเสธหรือไม่ชำระเงินส่วนที่เหลือได้จนกว่าคู่สัญญาจะมีการดำเนินการให้เป็นไปตามข้อตกลงทุกประการ

(9) บริษัทตัวแทนและการรับประกันการใช้งาน (Representations and Warranties)

สถาบันการเงินส่วนใหญ่เลือกหา software ประเภทที่มีสิทธิบัตรการใช้งานซึ่งมีบริษัทตัวแทนพร้อมการให้บริการตามข้อตกลงการรับประกันที่รวดเร็ว ซึ่งใบรับประกันการใช้งานในลักษณะดังกล่าวเป็นใบรับประกันที่ไม่ละเมิดทรัพย์สินทางปัญญาของบุคคลที่สามไม่ว่าจะใช้งาน software ที่ใดในโลก ภายใต้กฎหมายของบางประเทศการออกใบรับรองในลักษณะดังกล่าวจำกัดให้เป็นการเฉพาะกับบริษัทผู้จำหน่ายบางรายเท่านั้น

กรณีของบริษัทผู้จำหน่าย บริษัทตัวแทนและการรับประกันการใช้งาน software แบบที่ไม่ระบุขอบเขตการใช้ code หรือไม่ระบุการควบคุมลิขสิทธิ์ที่เฉพาะเจาะจงลงในสัญญา (ดูการอภิปรายเรื่อง การรักษาความปลอดภัย)

สิทธิบัตรการใช้งาน software ควรครอบคลุมถึงหน้าที่ความรับผิดชอบของบริษัทตัวแทนและการรับประกันกรณีที่ softwareไม่สามารถใช้งานได้ตรงตามคุณลักษณะที่ระบุไว้ในสัญญาหรือกรณีที่เกิดปัญหาในการใช้งาน **การรับประกันควรแยกออกเป็นกรณีของความล้มเหลวของระบบงานที่มีนัยสำคัญ (mission critical failures) ซึ่งต้องแก้ไขเร่งด่วนและกรณีของความล้มเหลวที่ไม่มีนัยสำคัญซึ่งสถาบันการเงินสามารถแก้ไขด้วยกระบวนการปฏิบัติโดยทั่วไปได้** เอกสารสิทธิ์ควรกำหนดขอบเขตของการรับประกันว่ากรณีใดบ้างที่อยู่ภายใต้การให้บริการบำรุงรักษาตามข้อกำหนดในการรับประกัน

(10) การแก้ปัญหาข้อขัดแย้ง (Dispute Resolution)

ในการเจรจาข้อตกลงและทำสัญญาสิทธิบัตรการใช้ software สถาบันการเงินควรพิจารณาให้ครอบคลุมถึงแนวทางการแก้ไขปัญหาข้อขัดแย้ง เช่นแนวทางในการปรับปรุงแก้ไข สิทธิของสถาบันการเงินที่อาจต้องจัดหาบุคคลอื่นมาแก้ไข software กรณีจำเป็นเร่งด่วนระหว่างช่วงเวลาที่ข้อขัดแย้งยังไม่มีข้อยุติ

(11) การแก้ไขปรับปรุงสัญญา (Agreement Modifications)

สถาบันการเงินต้องพิจารณาจนมั่นใจว่าสัญญาเกี่ยวกับสิทธิบัตรระบุข้อความเกี่ยวกับกรณีที่บริษัทผู้จำหน่ายไม่สามารถเปลี่ยนแปลงแก้ไขข้อความได้โดยไม่มีลายมือชื่อการยินยอมของคู่สัญญาทั้งสองฝ่าย ข้อความดังกล่าวจะช่วยให้มั่นใจได้ว่าจะไม่มีการปรับปรุงแก้ไขข้อความใดๆในสัญญาหากคู่สัญญาฝ่ายใดฝ่ายหนึ่งไม่ยินยอม

(12) ข้อจำกัดความรับผิดชอบของบริษัทผู้จำหน่าย (Vendor Liability Limitations)

ผู้ขายบางรายอาจจะเสนอร่างสัญญาที่มีหัวข้อจำกัดความรับผิดชอบโดยจะพยายามเพิ่มเติมข้อกำหนดที่จะไม่ต้องรับผิดชอบการรับประกันหรือการชดใช้เงินตามมูลค่าของสินค้าการพิจารณาจ่ายเงินหรือการจ่ายเงินเฉพาะส่วนเสียหาย โดยทั่วไปศาลให้ความรับรองสัญญาที่มีข้อจำกัดความรับผิดชอบในข้อกำหนดทางการค้า เว้นแต่ข้อกำหนดเหล่านั้นเป็นไปโดยมิชอบ ดังนั้นถ้าสถาบันการเงินต้องพิจารณาร่างสัญญาที่มีหัวข้อดังกล่าวประกอบอยู่ ควรจะพิจารณาว่าการเสนอข้อ**กำหนดความรับผิดชอบต่อความเสียหายรองรับมูลค่าความเสียหายทางการเงินที่องค์กรจะต้องเผชิญอย่างพอเพียง** สืบเนื่องจากผลของการไม่สามารถรับผิดชอบของผู้ขายตามสัญญาที่ให้ไว้สำหรับsoftware ที่มีความสำคัญ (mission critical software) ข้อกำหนดการยกเว้นความผิดที่จำกัดความ

รับผิดชอบของผู้ขายอย่างกว้างๆ จะมีผลกระทบต่อการดำเนินงานของสถาบันการเงิน เนื่องจากอาจไม่เพียงพอรองรับความเสียหายและสถาบันการเงินไม่มีทางตอบโต้ได้

(13) การรักษาความปลอดภัย (Security)

สถาบันการเงินควรพัฒนาข้อกำหนดในการรักษาความปลอดภัยสำหรับระบบสารสนเทศและมาตรฐานด้านประสิทธิภาพภายในองค์กร เกี่ยวกับลักษณะความปลอดภัยของลิขสิทธิ์การใช้ software และสัญญาการพัฒนาระบบความปลอดภัย **มาตรฐานที่กำหนดต้องมั่นใจว่า software มีความสอดคล้องกับระบบรักษาความปลอดภัยโดยรวมขององค์กร** ในการพัฒนามาตรฐานระบบความปลอดภัย สถาบันการเงินควรจะอ้างอิงรายละเอียดวิธีการใน IT Handbook's "Information Security Booklet" หรือควรจะอ้างอิงถึงมาตรฐานอุตสาหกรรมที่ได้รับการยอมรับโดยทั่วไป

ในสัญญาควรจะระบุถึงความรับผิดชอบของบริษัทผู้จำหน่าย เพื่อป้องกันความปลอดภัยและความลับของข้อมูลและแหล่งที่มาของข้อมูลขององค์กร **ข้อตกลงควรห้ามมิให้บริษัทผู้จำหน่ายคู่สัญญาหรือตัวแทนใช้หรือเปิดเผยข้อมูลของสถาบันการเงินเว้นแต่การใช้เพื่อการให้บริการแก่สถาบันการเงิน** และในกรณีการจัดหาระบบงานสำคัญ (mission critical software) สถาบันการเงินควรเลือกหาการรับประกันจากผู้จำหน่าย software ว่าจะไม่มีการเปิดช่องว่างให้กับผู้ที่ไม่ได้รับอนุญาตเข้ามาในระบบหรือเข้าถึงระบบข้อมูลได้ (Back door and Disabling devices) สัญญาและสิทธิบัตรควรมีการเน้นอย่างชัดเจนว่าผู้จำหน่ายจะไม่ใช้ software features ที่สามารถทำให้ผู้จำหน่ายควบคุมการ disable software ในกรณีที่เกิดความขัดแย้งขึ้นกับผู้ซื้อ สัญญาและสิทธิบัตรควรจะกำหนดว่าสถาบันการเงินจะถูกระงับการใช้ได้จากคำสั่งศาลเท่านั้น

(14) ผู้รับช่วงและความสัมพันธ์ของผู้ขายหลายราย (Subcontracting and Multiple Vendor Relationships)

ผู้จำหน่ายบางรายอาจทำสัญญากับบุคคลที่สาม เพื่อทำการพัฒนา software ให้ลูกค้า สถาบันการเงินจะได้รับประโยชน์จากบุคคลที่สามที่ผู้จำหน่ายมีการทำสัญญาระหว่างกันไว้ **สถาบันการเงินควรจะระบุถึงคุณลักษณะการจัดหาว่าผู้จำหน่ายที่เป็นคู่สัญญากับสถาบันการเงินจะต้องเป็นผู้รับผิดชอบต่อ software โดยไม่คำนึงว่าองค์กรใดเป็นผู้พัฒนาหรือคิดค้นขึ้น** สถาบันการเงินควรพิจารณาข้อกำหนดในการอนุมัติ โดยอ้างถึงความเปลี่ยนแปลงของ vendor's significant subcontractors ตามคู่มือตรวจสอบการให้บริการด้านเทคโนโลยีจากบุคคลภายนอก

สถาบันการเงินควรกำหนดลงในข้อสัญญาเกี่ยวกับการไม่อนุญาตให้ผู้จำหน่ายคู่สัญญาทำสัญญากับบุคคลที่สามโดยไม่ได้รับความยินยอมจากสถาบันการเงิน ในทางตรงกันข้าม

สถาบันการเงินที่มีแผนจะต้องเปลี่ยนผู้เป็นเจ้าของหรือได้รับการปรับปรุงโครงสร้างองค์กร ควรจะตัดสินใจว่าข้อตกลงต่างๆ จะได้รับการปฏิบัติอย่างต่อเนื่อง หลังจากการเปลี่ยนแปลงดังกล่าว ซึ่งข้อตกลงเกี่ยวกับสิทธิบัตรบางอย่างอาจต้องมีการเปลี่ยนแปลงหรือมีการถ่ายโอนข้อจำกัดหลังจากมีการรวมองค์กร ขายหรือเปลี่ยนเจ้าของ

(15) จำกัดในการแสดงความเห็นด้านไม่ดีของโปรแกรม (Restrictions on Adverse Comments)

สิทธิบัตรในการใช้โปรแกรมบางประเภทห้ามมิให้ผู้ใช้สิทธิบัตรเปิดเผยข้อมูลเกี่ยวกับประสิทธิภาพของการทำงานของ software ให้กับบุคคลที่มีความสนใจหรือใช้โปรแกรมแบบเดียวกัน (user group) ทำให้ไม่สามารถแลกเปลี่ยนประสบการณ์หรือความคิดเห็นในการใช้โปรแกรมระบบงานได้ **สถาบันการเงินจึงไม่ควรยินยอมให้ปรากฏข้อกำหนดในลักษณะนี้ในสิทธิบัตรการใช้งาน**

2.4 การบำรุงรักษา (Maintenance)

สรุปแนวทางการปฏิบัติ

สถาบันการเงินควรจัดให้มีระเบียบวิธีการบำรุงรักษาทรัพยากรด้านเทคโนโลยีสารสนเทศ ที่เหมาะสมและสอดคล้องกับลักษณะและความเสี่ยงของการดำเนินโครงการรวมถึงความเหมาะสมของปัจจัย ดังต่อไปนี้

- แผนงานโครงการบำรุงรักษา
- มาตรฐานการบำรุงรักษาและกระบวนการดำเนินงาน
- การควบคุมการเปลี่ยนแปลง ทั้งในกรณีของการเปลี่ยนแปลงองค์ประกอบหลัก การเปลี่ยนแปลงย่อยๆ ตามปกติ และการเปลี่ยนแปลงกรณีฉุกเฉิน (Major routine and emergency change controls)
- การควบคุมการจัดการเกี่ยวกับโปรแกรมเสริม (Patch management controls)
- การมีส่วนร่วมของผู้เกี่ยวข้องทั้งหมด
- มาตรฐานการจัดทำเอกสารประกอบ
- การควบคุมการจัดเก็บโปรแกรมระบบงานและโปรแกรมอรรถประโยชน์ (Library and utility controls)
- มาตรฐานการรับประกันคุณภาพ การบริหารความเสี่ยง และระเบียบวิธีปฏิบัติในเรื่องดังกล่าว (Quality assurance and risk management standards and procedures)

กิจกรรมการบำรุงรักษา hardware , software และเอกสารที่เกี่ยวข้อง ทั้งในกรณีของการให้บริการประจำวันตามปกติและการปรับปรุงเปลี่ยนแปลงตามกำหนดเวลานั้น ในส่วนของ hardware ความต้องการปรับปรุงเปลี่ยนแปลงต่างๆ เป็นไปตามระยะเวลาของการใช้งาน ได้แก่การเปลี่ยนอุปกรณ์ใหม่มาทดแทนอุปกรณ์ส่วนที่ล้าสมัยหรือส่วนที่ไม่สามารถใช้งานได้ตามหน้าที่ การปรับเปลี่ยนเพื่อเพิ่มประสิทธิภาพในการทำงานหรือการปรับปรุงเพื่อเพิ่มขีดความสามารถของหน่วยความจำ ส่วนกรณีของ software การปรับปรุงเปลี่ยนแปลงมาจากความต้องการของผู้ใช้งาน (user requirement) ได้แก่ การแก้ไขปัญหาในการใช้งาน (rectify software problems) แก้ไขความไม่รัดกุมของระบบรักษาความปลอดภัย (correct security vulnerabilities) หรือการเปลี่ยนไปใช้เทคโนโลยีแบบใหม่ สิ่งสำคัญในเรื่องของการบำรุงรักษาเพื่อให้มีกระบวนการบำรุงรักษาเป็นประจำหรือตรงตามระยะเวลาที่กำหนด คือกระบวนการจัดทำเอกสารที่เกี่ยวข้อง ซึ่งจะทำให้ทราบถึงข้อมูลด้านเทคโนโลยีที่มีความสัมพันธ์กัน มาตรฐาน และระเบียบวิธีปฏิบัติต่างๆ

ความล้มเหลวในการควบคุมการเปลี่ยนแปลงที่เหมาะสมขององค์กร เป็นผลให้เกิดการละเลยไม่ปฏิบัติตามข้อกำหนด ระบบงานลดประสิทธิภาพลง หรือการรักษาความปลอดภัยลดความรัดกุมลง การควบคุมการเปลี่ยนแปลง (บางครั้งจะหมายถึงการบริหารจัดการโครงสร้าง) เกี่ยวข้องสัมพันธ์ในเรื่องของการเพิ่มสายงานธุรกิจใหม่ด้านผลิตภัณฑ์ ด้านบริการหรือการปรับเปลี่ยนระเบียบวิธีปฏิบัติใหม่ รวมถึงความมั่นใจว่าในการเปลี่ยนแปลงทุกครั้งได้รับความเห็นชอบจากผู้มีอำนาจ มีเอกสารประกอบการเปลี่ยนแปลงครบถ้วนและมีการเผยแพร่ให้ผู้เกี่ยวข้องทราบอย่างทั่วถึง การควบคุมการเปลี่ยนแปลงควรกำหนดให้ครอบคลุมทุกสภาพแวดล้อมด้านเทคโนโลยีขององค์กร อันประกอบด้วย software โปรแกรมระบบงาน hardware และโครงสร้างของ software มาตรฐานและระเบียบวิธีปฏิบัติงาน ตลอดจนกระบวนการบริหารโครงการ

การควบคุมการเปลี่ยนแปลงควรกำหนดในรูปแบบที่เป็นสากลซึ่งสามารถปรับใช้ได้กับทุกระบบงาน ทุกสภาพแวดล้อมหรือแบ่งเป็นหลายระดับ เช่น ระดับของระบบงานที่มีลักษณะเฉพาะ ระดับของสายงานธุรกิจ ระดับของส่วนของงานสนับสนุน เป็นต้น การแบ่งระดับของระเบียบวิธีปฏิบัติก็เป็นสิ่งจำเป็นที่ช่วยในการระบุความต้องการในการควบคุมที่แตกต่างกัน ระหว่างเครื่อง mainframe ระบบเครือข่ายสื่อสาร และการควบคุมสภาพแวดล้อมของเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย โปรแกรมระบบปฏิบัติการและโปรแกรมระบบงาน รวมถึงโครงการพัฒนาและการจัดซื้อจัดหาทรัพยากรด้านเทคโนโลยีสารสนเทศ

ผู้ทำหน้าที่บริหารควรพิจารณากำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการควบคุมการเปลี่ยนแปลง เพื่อให้มั่นใจว่าการปรับปรุงเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศมีความเหมาะสม ผ่านการเห็นชอบจากผู้มีอำนาจ มีกระบวนการทดสอบ มีเอกสารประกอบ มีการนำลงใช้งานจริง และมีการเผยแพร่อย่างทั่วถึง คุณลักษณะ ความเสี่ยงของระบบงาน กิจกรรมต่างๆหรือกระบวนการปรับเปลี่ยนเป็นไปตามระบบการควบคุมการเปลี่ยนแปลง หน่วยงานรับประกันคุณภาพ หน่วยงานรักษาความปลอดภัย หน่วยงานตรวจสอบ หน่วยงานเครือข่ายสื่อสารเข้ามามีส่วนร่วมในกระบวนการปรับเปลี่ยนดังกล่าวอย่างเหมาะสม

2.4.1 การปรับปรุงระบบงานหลัก (Major Modification)

การปรับปรุงเปลี่ยนแปลง องค์ประกอบที่สำคัญหมายถึงการปรับเปลี่ยนองค์ประกอบในการปฏิบัติงานที่มีนัยสำคัญ (significant functional change) ได้แก่การโอนย้ายการปฏิบัติงานจากระบบงานเดิมไปปฏิบัติงานกับระบบงานใหม่ หรือการโอนข้อมูลไปใช้กับระบบงานของบริษัทในเครือหรือบริษัทลูกหรือระบบงานที่จัดซื้อใหม่ การปรับปรุงเปลี่ยนแปลงองค์ประกอบที่สำคัญประกอบด้วย กระบวนการดำเนินการที่เป็นระบบเช่นเดียวกับกระบวนการพัฒนาระบบงาน (SDLC) ซึ่งได้กล่าวไว้ในเรื่องการพัฒนาระบบงานแล้ว (Development)

มาตรฐานการปรับปรุงเปลี่ยนแปลงองค์ประกอบที่สำคัญ ควรระบุถึงกิจกรรมต่างๆที่โครงการต้องดำเนินการ เช่น ระเบียบวิธีปฏิบัติเกี่ยวกับ การวิเคราะห์ความต้องการ การศึกษาความเป็นไปได้ของความต้องการ การวางแผนโครงการ software design การพัฒนาโปรแกรมระบบงาน (programming) การทดสอบ และการนำลงใช้งานจริง (สามารถดูรายละเอียดการบริหารโครงการเพิ่มเติมได้จากเรื่องการบริหารโครงการและการพัฒนาระบบงาน และเรื่องการโอนย้าย (conversion) ที่จะกล่าวถึงในส่วนต่อไป)

2.4.2 การปรับปรุงระบบงานประจำ (Routine Modification)

การปรับปรุงเปลี่ยนแปลงองค์ประกอบส่วนย่อยหมายถึงการปรับปรุงโปรแกรมระบบงานหรือ software ระบบปฏิบัติการเพื่อเพิ่มประสิทธิภาพในการทำงานหรือเพื่อแก้ไขปัญหาการทำงานหรือเพื่อเพิ่มระบบรักษาความปลอดภัย กระบวนการในการปรับปรุงเปลี่ยนแปลงองค์ประกอบส่วนย่อยมีความซับซ้อนและขั้นตอนไม่มากเท่ากับการปรับปรุงเปลี่ยนแปลงองค์ประกอบที่สำคัญ และสามารถนำส่วนที่ปรับปรุงเปลี่ยนแปลงลงใช้งานเมื่อดำเนินการตามมาตรฐานที่สถาบันการเงินกำหนด

มาตรฐานการปรับปรุงเปลี่ยนแปลงองค์ประกอบส่วนย่อยควรครอบคลุมถึงการเสนอความต้องการที่จะปรับเปลี่ยน การพิจารณาทบทวนประเด็นความต้องการ การอนุมัติระเบียบวิธีปฏิบัติและการบริหารจัดการเกี่ยวกับการวางแผน การทดสอบ การจัดทำเอกสารประกอบและการจัดลำดับในการนำลงใช้งานจริงต้องสอดคล้องเหมาะสมกับความจำเป็นในการใช้งานของแต่ละองค์ประกอบ การกำหนดแผนในการนำลงใช้งานจริงที่เป็นระบบซึ่งรวมถึงการใช้เครื่องมืออัตโนมัติในการติดตั้งเพื่อใช้งาน (automated deployment tool) เป็นสิ่งสำคัญสำหรับสถาบันการเงินขนาดใหญ่ ซึ่งต้องนำองค์ประกอบที่ปรับปรุงเปลี่ยนแปลงไปใช้งานหลายสายงานธุรกิจหรือแจกจ่ายให้หน่วยงานต่างๆทั้งองค์กรทางเครือข่ายสื่อสาร มาตรฐานการเปลี่ยนแปลงควรระบุถึง ระเบียบวิธีปฏิบัติในการติดต่อสื่อสารด้วย เพื่อให้มั่นใจว่ากระบวนการบริหารสามารถสื่อสารไปถึงผู้เกี่ยวข้องทุกฝ่ายอย่างรวดเร็วและครอบคลุมทุกการเปลี่ยนแปลง

ในกรณีที่ใช้ระบบเทคโนโลยีและระบบปฏิบัติการร่วมกันภายในกลุ่ม สถาบันการเงินควรดำเนินการในเรื่องของการปรับเปลี่ยนโปรแกรมระบบงานและโปรแกรมเสริม (patch) ให้เป็นไปในแนวทางเดียวกับกระบวนการบริหารการเปลี่ยนแปลงของกลุ่มหรือของส่วนกลาง สำหรับองค์กรขนาดใหญ่อาจพิจารณาแต่งตั้งคณะกรรมการควบคุมการเปลี่ยนแปลงที่มีความเชี่ยวชาญ (specialized change control committee) เพื่อควบคุมกระบวนการดำเนินการให้เป็นไปตามระเบียบวิธีปฏิบัติที่กำหนด ส่วนองค์กรขนาดเล็กลงมาอาจพิจารณาแต่งตั้งคณะกรรมการเทคโนโลยี (technology steering committee) ทำหน้าที่ควบคุมการบริหารกระบวนการให้เกิดประสิทธิผล การดูแลติดตามโดยคณะกรรมการหรือผู้ที่ได้รับมอบหมายช่วยให้เกิดความชัดเจนในเรื่องของการเสนอความต้องการ และช่วยให้มั่นใจว่าทุกฝ่ายงานที่เกี่ยวข้องตระหนักถึงหน้าที่ความรับผิดชอบในระหว่างดำเนินการปรับปรุงเปลี่ยนแปลง **คณะกรรมการควรมาจากผู้แทนของแต่ละสายงานที่เกี่ยวข้องได้แก่ สายงานธุรกิจ สายงานเทคโนโลยีสารสนเทศ สายงานรักษาความปลอดภัย สายงานรับประกันคุณภาพ และสายงานตรวจสอบ** เพื่อให้มั่นใจว่าการเปลี่ยนแปลงต่างๆสามารถสนับสนุนเป้าหมายทางธุรกิจและไม่มีผลกระทบต่อการปฏิบัติงานและการรักษาความปลอดภัยขององค์กร

ผู้บริหารควรพิจารณาทบทวนวัตถุประสงค์ในการขอเปลี่ยนแปลง เพื่อให้มั่นใจว่าการปรับปรุงเปลี่ยนแปลงมีความเหมาะสมกับระบบงานที่เกี่ยวข้อง นอกจากนี้การบริหารจัดการควรให้เกิดความมั่นใจว่าโปรแกรมที่ปรับเปลี่ยนหรือแก้ไขและนำลงใช้งานเป็นชุดเดียวกับที่ได้รับอนุญาตให้แก้ไขและได้รับการอนุมัติตามเอกสารประกอบ การขาดการควบคุมที่รัดกุมและไม่มีเอกสารประกอบครบถ้วนถูกต้อง อาจเป็นสาเหตุให้เกิดปัญหาเมื่อมีการติดตั้งระบบงานอื่นในภายหลัง มาตรฐานแบบ

เสนอความต้องการ ดังนั้นผู้บริหารจึงควรจัดให้มีกระบวนการจัดเก็บ การควบคุมเวอร์ชัน (version control) ด้วยโปรแกรม spreadsheets หรือ ระบบจัดเก็บข้อมูลเกี่ยวกับการเปลี่ยนแปลงแบบอัตโนมัติ (automated change logs facilitate management' ability) เพื่อใช้เป็นเครื่องมือเพื่อติดตามการทำงาน ออกรายงาน และวิเคราะห์การเปลี่ยนแปลง รายงานการเปลี่ยนแปลงที่มีรายละเอียดครอบคลุมเป็นเงื่อนไขที่ต้องกำหนดขึ้นก่อนกระบวนการคุมการเปลี่ยนแปลงอื่นๆ

แบบคำขอเปลี่ยนแปลง (change request form) ควรระบุรายละเอียดการเรียงลำดับ record และรายละเอียดอื่นที่ต้องการเปลี่ยนแปลงทั้งหมด แบบคำขอดังกล่าวควร**ส่งถึงฝ่ายต่างๆ ที่เกี่ยวข้องเพื่อให้รับทราบข้อมูลและผลกระทบ**ของการปรับเปลี่ยนซึ่งรายละเอียดที่ควรระบุคือ

- แบบคำขอลงวันที่ (Request date)
- ชื่อผู้ยื่นแบบ (Requestor' name)
- คำบรรยายลักษณะต่างๆของสิ่งที่ต้องการ (Description of change)
- เหตุผลที่ต้องการนำมาใช้งานหรือต้องการยกเลิกการใช้งาน (Reasons for implementing or rejecting a change)
- ผลการพิจารณาเหตุผลในการขอเปลี่ยนแปลง (Justification for change)
- การลงนามอนุมัติให้ดำเนินการเปลี่ยนแปลง (approval signatures)
- ลำดับของการเปลี่ยนแปลงตามทะเบียนคุม (Change control number)

กรณีที่คำขอเปลี่ยนแปลงได้รับการอนุมัติ แบบคำขอจะถูกส่งต่อไปที่ฝ่ายงานเทคโนโลยีสารสนเทศที่รับผิดชอบ ในระหว่างการดำเนินกระบวนการเปลี่ยนแปลงสถาบันการเงินควรจัดทำเอกสารประกอบที่เกี่ยวข้องไปพร้อมกันซึ่งเอกสารควรประกอบด้วย

- รายละเอียดเกี่ยวกับลำดับความสำคัญ (Priority information)
- การระบุรายละเอียดเกี่ยวกับ ระบบงาน ฐานข้อมูล และฝ่ายงาน ที่เกี่ยวข้องกับการเปลี่ยนแปลง (Identification of effected systems, databases and department)
- ชื่อผู้รับผิดชอบดำเนินการเปลี่ยนแปลง (Name of individual responsible for making the change)
- ทรัพยากรด้านต่างๆ ที่ต้องการ (Resource requirements)
- ต้นทุนในการดำเนินโครงการ (Project costs)
- กำหนดเวลาที่โครงการจะแล้วเสร็จ (Project completion date)
- กำหนดเวลาในการนำลงใช้งานจริง (Project implementation date)

- ศักยภาพด้านการรักษาความปลอดภัย และการพิจารณาถึงความน่าเชื่อถือ (Potential security and reliability consideration)

- ขอบเขตที่ต้องการให้ทดสอบ (Testing requirements)

- กระบวนการในการนำลงใช้งานจริง (Implementation procedures)

- ประมาณเวลาที่ระบบงานหยุดให้บริการจนกว่าจะสามารถติดตั้งระบบที่ปรับปรุงเปลี่ยนแปลงแล้วเสร็จ (Estimated downtime for implementation)

- กระบวนการสำรอง/ การกู้คืน (Backup/Back-out procedures)

- กำหนดเวลาในการปรับปรุงเอกสารที่เกี่ยวข้องให้เป็นปัจจุบัน (Documentation updates : program designs and scripts, network topologies, user manuals , contingency plans etc.)

- เอกสารการตรวจรับจากฝ่ายงานที่เกี่ยวข้อง (Change acceptance documentation from all applicable departments : users, technology, quality assurance, security, audit etc.)

- เอกสารแสดงผลของการเปรียบเทียบระหว่างการตรวจประเมินผลหลังจากการใช้งานจริงกับความคาดหวังที่ต้องการ (Post –implementation audit documentation : comparison of expectations and results)

หลังจากการปรับปรุงเปลี่ยนแปลงโปรแกรมระบบงานได้ดำเนินการแล้วเสร็จ บรรดา program code (source code, object code, patch code, load module, etc.) ควรเก็บรักษาอย่างปลอดภัย การดูแลให้ codes มีความปลอดภัยสามารถใช้บริการจากผู้ให้บริการซึ่งทำหน้าที่ตรวจสอบเพื่อรับประกันว่าโปรแกรมระบบงานที่นำลงใช้งานจริงเป็น version เดียวกับที่ได้รับอนุมัติและผ่านการทดสอบ ผู้บริหารควรกำหนดมาตรฐานและระเบียบวิธีปฏิบัติเกี่ยวกับการอนุมัติโปรแกรมระบบงานเพื่อให้สามารถสอบทานผลการทดสอบ ตรวจทานการปรับปรุงแก้ไข code และการยืนยันการจับคู่ระหว่าง source code และ object code

2.4.3 การปรับปรุงแบบเร่งด่วน (Emergency Modification)

การปรับปรุงเปลี่ยนแปลงกรณีฉุกเฉินหรือเร่งด่วนอาจเกิดขึ้นเป็นระยะๆ เพื่อแก้ไขปัญหาของ software หรือกู้ระบบปฏิบัติการให้คืนสู่สภาพปกติอย่างเร่งด่วน แม้ว่าการปรับเปลี่ยนสามารถดำเนินการแล้วเสร็จในเวลารวดเร็วก็ตามแต่ควรมีกระบวนการควบคุมอย่างเป็นระบบเช่นกัน

มาตรฐานและระเบียบวิธีปฏิบัติของการปรับปรุงเปลี่ยนแปลงกรณีฉุกเฉินหรือเร่งด่วน ควรมีแนวทางเช่นเดียวกับการควบคุมการปรับปรุงเปลี่ยนแปลงองค์ประกอบส่วนย่อย อย่างไรก็ดีมาตรฐานอาจลดขั้นตอนในกระบวนการเสนอแบบคำขอ การประเมินความคุ้มค่า และการ

พิจารณาอนุมัติ เพื่อให้การขอปรับเปลี่ยนดำเนินไปอย่างรวดเร็ว และควรกำหนดไว้ในมาตรฐานการบริหารจัดการ**ให้จัดทำรายละเอียดการประเมินความคุ้มค่า เอกสารประกอบที่เกี่ยวข้องให้แล้วเสร็จภายหลังการนำระบบงานที่ปรับปรุงเปลี่ยนแปลงกรณีฉุกเฉินหรือเร่งด่วนลงใช้งานโดยเร็วที่สุดเท่าที่จะทำได้**

หากเป็นไปได้ควรมีการทดสอบระบบงานกรณีดังกล่าวก่อนนำลงใช้งานจริง หากผู้บริหารไม่สามารถดำเนินการให้มีการทดสอบโปรแกรมระบบงานกรณีดังกล่าวก่อนนำลงติดตั้งเพื่อใช้งานอาจมีผลกระทบกับการกำหนดกระบวนการสำรองไฟล์และโปรแกรมระบบงานในกระบวนการกู้คืนระบบที่ไม่สอดคล้องเหมาะสมได้

ระเบียบวิธีปฏิบัติในการสำรองที่เหมาะสม กำหนดขึ้นโดยพิจารณาจากกระบวนการกู้คืน(back-out) และรายละเอียดจากเอกสารประกอบการเปลี่ยนแปลงที่เกี่ยวข้อง ซึ่งใช้เป็นข้อมูลสนับสนุนให้การบริหารจัดการกระบวนการฟื้นฟูระบบงานส่วนที่ได้รับการปรับปรุงเปลี่ยนแปลงในกรณีที่ระบบงานดังกล่าวหยุดชะงักให้มีความสอดคล้องเหมาะสมขึ้น รายละเอียดในเอกสารประกอบที่เกี่ยวข้องยังเป็นข้อมูลที่ช่วยสนับสนุนการวิเคราะห์เพื่อประเมินความคุ้มค่าหลังการเปลี่ยนแปลง ระเบียบวิธีปฏิบัติเกี่ยวกับการปรับปรุงเปลี่ยนแปลงกรณีฉุกเฉินหรือเร่งด่วนอย่างน้อยที่สุดควรประกอบด้วย

(1) การประเมินก่อนดำเนินการและการพิจารณาให้ความเห็นชอบ (Pre-change reviews and authorizations)

(2) การทดสอบก่อนการนำระบบที่เปลี่ยนแปลงลงใช้งานจริง (ในสภาพแวดล้อมของการทดสอบ) (Pre-change testing : in segregated testing environment)

(3) กระบวนการสำรอง/กู้คืน (Backup/Back-out procedures)

(4) การจัดทำเอกสารประกอบที่เกี่ยวข้อง ที่ควรมี

- คำบรรยายลักษณะขององค์ประกอบที่ต้องการเปลี่ยนแปลง (Descriptions of a change)
- เหตุผลที่ต้องการนำมาใช้งานหรือต้องการยกเลิกการใช้งาน (Reasons for implementing or rejecting a proposed change)
- ชื่อของบุคคลผู้รับผิดชอบดำเนินการเปลี่ยนแปลง (The name of the individual who made the change)
- จำนวนชุดของ code (A copy of the changed code)

- วันที่และระยะเวลาดำเนินการ (The date and time a change was made)

(5) การประเมินความคุ้มค่าหลังการเปลี่ยนแปลง (Post-change evaluations)

2.4.4 การจัดการเพิ่มการรักษาความปลอดภัย (Patch Management)

การบริหาจัดการ Software patch มีกระบวนการเช่นเดียวกับการปรับปรุงเปลี่ยนแปลงโปรแกรมที่พัฒนาโดยบริษัทผู้ให้บริการภายนอก มาตรฐานการจัดการ patch ควรจะรวมถึงกระบวนงานในการกำหนดความต้องการ การประเมินความคุ้มค่า การอนุมัติ การทดสอบ การติดตั้งและการจัดทำเอกสารประกอบการ patch

ผู้ให้บริการภายนอกส่วนใหญ่จะพัฒนาและเผยแพร่ข้อมูลเกี่ยวกับ patch เพื่อแก้ไขปัญหา software เพิ่มประสิทธิภาพการดำเนินงาน และเพิ่มการรักษาความปลอดภัย องค์กรควรจะใช้กระบวนงานที่สามารถระบุ patch ที่สามารถใช้ได้และได้มาจากที่ที่เชื่อถือได้ กระบวนงานในการระบุจุดอ่อนของ software และข้อมูลการ patch ที่รวมถึงการอธิบายรายชื่อจดหมายอิเล็กทรอนิกส์ที่เตือนการ patch และการติดตามผู้ให้บริการภายนอกและการรักษาความปลอดภัยบน websites **ฝ่ายจัดการควรจะได้รับข้อความเกี่ยวกับการเพิ่มประสิทธิภาพผลิตภัณฑ์และประเด็นการรักษาความปลอดภัยที่เป็น patch ที่สามารถใช้ได้และได้รับการปรับปรุงจากผู้ให้บริการโดยตรงหรือจากข้อมูลการรักษาความปลอดภัยที่เชื่อถือได้**

เมื่อมีการระบุ patch ที่สามารถใช้ได้แล้ว ฝ่ายจัดการควรจะประเมินผลกระทบของการติดตั้ง patch โดยการประเมินทางเทคนิค ธุรกิจและการรักษาความปลอดภัย **ถ้าฝ่ายจัดการกำหนด patch ที่สำคัญแต่ไม่ติดตั้งลงในระบบ ฝ่ายจัดการควรจะจัดทำเอกสารประกอบเหตุผลที่ไม่ติดตั้งนั้น**

การที่จะลดความเสียหายจากการปฏิบัติงาน ฝ่ายจัดการควรจะทดสอบ patch ทั้งหมดก่อนการนำออกใช้งาน นอกจากนี้ **ฝ่ายจัดการควรจะทำสำรองไฟล์และโปรแกรมอย่างเหมาะสม และสร้างกระบวนงานการย้อนกลับไปใช้ระบบเดิมก่อนการนำออกใช้งาน**

การปรับปรุง software ทั้งหมดก็ต้องมีกระบวนงานที่เหมาะสมในการทำสำเนาข้อมูลและการย้อนกลับ การประเมินหลังการนำออกใช้งาน รายละเอียดเอกสารประกอบ และแผนการนำออกใช้งานที่กำหนดขึ้นเพื่อเพิ่มความสามารถในการจัดการควบคุมการดำเนินการ patch ได้อย่างมีประสิทธิภาพ

<u>หมายเหตุ</u> การติดตั้ง software patch อาจจะเป็นการปรับเปลี่ยนการตั้งค่าการรักษาความปลอดภัยหรือการตั้งค่าในระบบกลับไปเหมือนการเริ่มต้น ฝ่ายจัดการควรจะสอบทานการตั้งค่า

ทั้งหมดและการตั้งค่าหลังจาก patch แล้วเพื่อให้แน่ใจว่าการตั้งค่านั้นตรงตามนโยบายและกระบวนงานที่ได้รับอนุมัติแล้ว

2.4.5 การควบคุมห้องเก็บ (Library Controls)

ห้องเก็บจะเก็บข้อมูลโดยแบ่งเก็บตามรูปแบบข้อมูล เช่น การพัฒนา การทดสอบ และโปรแกรมที่เกี่ยวข้องกับผลิตภัณฑ์ ข้อมูล และเอกสารประกอบ

ฝ่ายจัดการควรจะควบคุมการเข้าถึงห้องเก็บและการเคลื่อนย้ายโปรแกรมและไฟล์ระหว่างห้องเก็บอย่างเข้มงวด ผู้พัฒนาไม่ควรย้ายโปรแกรมเข้าหรือออกจากห้องเก็บโปรแกรมที่ใช้งานจริง การควบคุมห้องเก็บเป็นวิธีจัดการย้ายโปรแกรมระหว่างการพัฒนา การทดสอบและสภาพแวดล้อมที่ใช้งานจริง ฝ่ายจัดการควรจะกำหนดหน้าที่การทำงานของห้องเก็บเพื่อให้ผู้รับรองคุณภาพและผู้ควบคุมระบบที่ใช้งานจริงมีความเป็นอิสระสำหรับสถาบันการเงินขนาดใหญ่ หรือผู้กำกับดูแลสำหรับสถาบันการเงินขนาดเล็ก

การวัดความซับซ้อนของการใช้เทคโนโลยีนั้น องค์กรควรจะพิจารณาการใช้การควบคุมการเปลี่ยนแปลงแบบอัตโนมัติ การที่ไม่ใช้เครื่องมือการควบคุมการเปลี่ยนแปลงแบบอัตโนมัตินั้น ฝ่ายจัดการควรจะควบคุมการเข้าถึงห้องเก็บโปรแกรมที่ใช้งานจริงอย่างเข้มงวด โดยเฉพาะในสภาพแวดล้อมที่มีการใช้เครื่องคอมพิวเตอร์แบบเครือข่าย

ฝ่ายจัดการควรจะสร้างการควบคุมที่เหมาะสมเพื่อบริหารจัดการการเคลื่อนย้ายโปรแกรมที่มีการปรับปรุงเข้าไว้ในห้องเก็บแต่ละห้อง **การควบคุมควรจะรวมถึง**

- การกำหนดความรับผิดชอบของผู้ดูแลห้องเก็บ
- การตรวจสอบความถูกต้องเชื่อถือได้ของโปรแกรมก่อนนำออกใช้งานจริง
- กระบวนงานอนุมัติการเคลื่อนย้ายโปรแกรมเข้าสู่การใช้งานจริง
- การควบคุมรหัสผ่านของห้องเก็บโปรแกรมทั้งหมด
- โปรแกรมควบคุมห้องเก็บอัตโนมัติจะจำกัดการเข้าถึงและระบุว่าใครสามารถเข้าถึงห้องเก็บได้มากน้อยแค่ไหน เมื่อมีการเปลี่ยนแปลง

2.4.6 การเปลี่ยนแปลง (Conversions)

การเปลี่ยนแปลงระบบ หมายถึงการเปลี่ยนแปลงระบบงานและระบบปฏิบัติการหลักไปเป็นระบบงานใหม่หรือการโอนข้อมูลไปใช้กับระบบงานใหม่เนื่องจากการควบรวมกิจการ หรือการจัดหาระบบงานใหม่ทดแทนระบบงานเดิม การเปลี่ยนแปลงระบบเป็นกระบวนการที่ซับซ้อนซึ่งโดยทั่วไประบบปฏิบัติการมีหลากหลายรูปแบบ (multiple platforms) ระบบที่มีความซับซ้อนมากจะ

เพิ่มระดับความเสี่ยง ซึ่งต้องการรายละเอียดในการดำเนินงานและการควบคุมอย่างเป็นระบบมากขึ้น การควบคุมการเปลี่ยนแปลงระบบที่รัดกุมสิ่งสำคัญ คือ การป้องกันความเสียหายของข้อมูล การรักษาระดับความสำเร็จของงานและการควบคุมการปฏิบัติงานให้เป็นไปตามแผนที่กำหนด **การควบคุมการเปลี่ยนแปลงระบบงานที่ไม่รัดกุมจะส่งผลให้เกิดปัญหาด้านการรักษาความปลอดภัย รายการข้อมูลที่ผิดพลาด ความไม่พอใจของผู้ใช้และลูกค้า หรือเสื่อมเสียชื่อเสียง**

การเปลี่ยนแปลงระบบงานจะส่งผลกระทบกับการดำเนินการปฏิบัติงาน เพราะฉะนั้น ฝ่ายจัดการควรจะประเมินผลการปฏิบัติงานด้านเทคโนโลยีทั้งหมดอย่างใกล้ชิด และตัดสินใจดำเนินการถ้าการเปลี่ยนแปลงระบบงานที่เสนอนั้นมีความเป็นไปได้และสนับสนุนวัตถุประสงค์ขององค์กร การเปลี่ยนแปลงระบบงานที่ประสบความสำเร็จต้องมีการจัดการโดยใช้ระเบียบวิธีในการปฏิบัติงานอย่างมากรวมถึงการวางแผนด้านกลยุทธ์ การบริหารโครงการ การกำหนดความต้องการ การทดสอบ การนำออกใช้งาน การวางแผนฉุกเฉิน การบริหารผู้ให้บริการภายนอก และการสอบทานหลังการนำออกใช้งาน

การควบคุมการเปลี่ยนแปลงระบบงานควรจะรวมถึงการจัดทำเอกสารประกอบแผนงานโครงการ เทคนิคการบริหารโครงการที่เหมาะสม และการติดตามดูแลโดยผู้บริหารระดับสูงหรือผู้ที่ได้รับมอบหมายที่มีความรู้ความเข้าใจ โดยทั่วไป สถาบันการเงินจะดำเนินกระบวนการเปลี่ยนแปลงระบบงานหลักเพื่อนำออกใช้งานด้วยการใช้วิธีการบริหารโครงการ เช่นเดียวกับ SDLC ที่ได้อธิบายไว้แล้ว สถาบันการเงินที่มีการจัดซื้อจัดหาเป็นประจำ หรือมีการควบรวมกิจการ ควรจะนำวิธีการเปลี่ยนแปลงระบบงานที่เป็นมาตรฐานมาใช้โดยมอบให้ทีมงานที่มีความชำนาญดูแลรับผิดชอบการเปลี่ยนแปลงนั้น

การบริหารการเปลี่ยนแปลงระบบงานที่มีประสิทธิภาพเริ่มจากการตรวจสอบความพร้อมของทรัพยากรที่เกี่ยวข้องทั้งหมดซึ่งรวมถึงการวิเคราะห์ผลกระทบจากการเปลี่ยนแปลงระบบงานใหม่ที่มีต่อการปฏิบัติงานในปัจจุบัน ฝ่ายจัดการควรจะประเมินความต้องการเรื่องรายการธุรกรรม การจัดเก็บข้อมูล การติดต่อสื่อสารและการประมวลผลที่ใช้อยู่ในปัจจุบันกับโครงการที่ต้องการเปลี่ยนแปลง นอกจากนี้ผู้จัดการโครงการควรจะตระหนักถึงและประเมินความต้องการปัจจัยอื่นที่เพิ่มขึ้นตามมาอย่างระมัดระวัง ในเรื่องงบดุล การกระทบยอด การจัดการข้อยกเว้น การแก้ไขปัญหา การสนับสนุนผู้ใช้งานและลูกค้า การเชื่อมโยงเครือข่าย และการบริหารระบบ เพื่อให้แน่ใจว่าสามารถดำเนินการเปลี่ยนแปลงได้อย่างสมบูรณ์และมีประสิทธิภาพ

องค์กรควรจะพิจารณาความต้องเกี่ยวกับการฝึกอบรมเพื่อให้ผู้เกี่ยวข้องทราบถึงการเปลี่ยนแปลงระบบงานและการปรับปรุง hardware และ software ด้วย ฝ่ายจัดการควรจะพิจารณารูปแบบ ปริมาณ และเวลาที่จำเป็นต้องใช้ในการฝึกอบรมเกี่ยวกับการเปลี่ยนแปลงระบบงานสำหรับแต่ละสายงานธุรกิจและประสานงานเรื่องแผนการฝึกอบรมกับผู้ให้บริการภายนอกด้วย

การเปลี่ยนแปลงที่ประสบความสำเร็จต้องมีการประสานงานกันอย่างใกล้ชิดภายในองค์กรและระหว่างองค์กรและผู้ให้บริการ ฝ่ายจัดการควรจะสร้างกระบวนงานติดต่อสื่อสารกำหนดขอบเขตและขั้นตอนการรายงาน และสายการบังคับบัญชาในการดำเนินการเพื่อให้แน่ใจว่าสามารถติดต่อสื่อสารได้อย่างรวดเร็วและตัดสินใจได้ทันเวลา

การเปลี่ยนแปลงที่ประสบความสำเร็จต้องมีรายละเอียดเพียงพอในการจัดทำภาพรวมผู้เชี่ยวชาญ ผู้ปฏิบัติงานและบุคลากรจากฝ่ายงานธุรกิจจากทั่วทั้งองค์กรซึ่งมีส่วนเกี่ยวข้องกับการควบรวมสถาบันการเงินหรือการจัดหาต้องให้ความร่วมมือในกระบวนการจัดทำภาพรวม กรณีของสถาบันการเงินที่ควบรวมกันควรจะทำความเข้าใจในเรื่องผลิตภัณฑ์ของทั้งสองสถาบันการเงินว่าสามารถใช้งานร่วมกันและถ่ายโอนข้อมูลจากระบบงานของสถาบันการเงินหนึ่งสู่อีกสถาบันการเงินหนึ่ง ความล้มเหลวในการรวมไฟล์และบัญชีสามารถส่งผลกระทบต่อความเชื่อถือของลูกค้าและพนักงาน ประเด็นผิดกฎหมาย การทำลายชื่อเสียง และมีความเป็นไปได้ที่จะสูญเสียลูกค้า การเปลี่ยนแปลงระบบงานในทุกกรณีควรจะรวมถึงการทดสอบที่เพียงพอด้วย

2.4.7 การควบคุมโปรแกรมอรรถประโยชน์ (Utility controls)

สถาบันการเงินควรกำหนดมาตรฐานการควบคุมการใช้โปรแกรมอรรถประโยชน์ โปรแกรมอรรถประโยชน์จะช่วยจัดการเนื้อที่เก็บข้อมูล เครื่องพิมพ์และทรัพยากรเกี่ยวกับการปฏิบัติงานอื่น ๆ **โปรแกรมอรรถประโยชน์ที่มีส่วนใหญ่จะเป็นส่วนหนึ่งของระบบปฏิบัติการและมีเครื่องมือช่วยในการแก้ไขโปรแกรม บำรุงรักษาไฟล์ และแก้ไขข้อมูลที่เสียหาย** โปรแกรมอรรถประโยชน์สามารถช่วยให้ผู้ใช้งานสร้าง ปรับปรุง เคลื่อนย้าย เปลี่ยนชื่อ ทำสำเนา และลบโปรแกรมที่เขียนและข้อมูลในห้องเก็บโปรแกรมและข้อมูลได้ เพราะฉะนั้น **ฝ่ายจัดการควรจะควบคุมการใช้งานโปรแกรมอรรถประโยชน์นี้อย่างเข้มงวด**

องค์กรควรจะจำกัดการใช้งานโปรแกรมอรรถประโยชน์ด้วยการควบคุมการเข้าถึงและโอนย้ายโปรแกรมดังกล่าวออกจากส่วนที่ใช้งาน (program libraries) มอบหมายให้มีผู้รับผิดชอบร่วมกันและนำกลับมาติดตั้งที่ส่วนที่ใช้งาน (program libraries) เมื่อจำเป็นต้องใช้งานเท่านั้น ฝ่าย

จัดการควรพิจารณาอย่างระมัดระวังเพื่อให้แน่ใจว่าการโอนย้ายโปรแกรมอรรถประโยชน์ออกไปนั้นไม่มีผลกระทบกับระบบปฏิบัติการหรือระบบงานอื่น

2.4.8 การบำรุงรักษาเอกสารประกอบ

เอกสารประกอบช่วยอธิบายถึงการพัฒนา การจัดหาและสภาพแวดล้อมการปฏิบัติงานขององค์กร และช่วยส่งเสริมให้องค์กรสามารถบริหาร ปฏิบัติงานและบำรุงรักษาระบบเทคโนโลยีได้เป็นอย่างดี ประโยชน์ที่ได้รับสำหรับผู้ใช้งานจะเกี่ยวกับการเข้าถึงคู่มือการปฏิบัติงานและเข้าหาตัวช่วยในระบบงานแบบ on-line เอกสารประกอบ**ยังช่วยให้ผู้บริหารระบบและผู้เชี่ยวชาญสามารถบำรุงรักษาและปรับปรุงระบบได้อย่างมีประสิทธิภาพและระบุข้อบกพร่องและแก้ไขโปรแกรมได้ถูกต้อง**

ปัจจุบันการพัฒนาและการบำรุงรักษาเอกสารประกอบให้ถูกต้องเป็นปัจจุบันทำได้ยาก เสียเวลาและเสียค่าใช้จ่ายสูง อย่างไรก็ตาม กระบวนงานการจัดทำเอกสารประกอบที่เป็นมาตรฐานและการใช้ software ช่วยดำเนินการจัดทำเอกสารประกอบจะช่วยให้องค์กรสามารถบำรุงรักษาเอกสารประกอบได้ดียิ่งขึ้น

มาตรฐานเอกสารประกอบควรจะกำหนดผู้ทำหน้าที่เก็บรักษาเอกสารประกอบและรายละเอียดเกี่ยวกับความต้องการผู้มีอำนาจจัดทำ การอนุมัติและรูปแบบการจัดทำ พนักงานควรจะจัดทำเอกสารประกอบการเปลี่ยนแปลงทั้งหมดของระบบ ระบบงาน และ configuration ตามที่มาตรฐานได้กำหนดไว้ นอกจากนี้ ฝ่ายจัดการควรจะควบคุมการเข้าถึงห้องเก็บเอกสารประกอบและรุ่นของเอกสารประกอบให้เหมาะสม

<u>ส่วนที่ 3</u> แนวทางการตรวจสอบ

3.1 วัตถุประสงค์ของการตรวจสอบ

วัตถุประสงค์ของการประเมินการพัฒนาและการจัดหาเพื่อระบุจุดอ่อนและความเสี่ยงที่มีผลกระทบกับองค์กร และเพื่อระบุเงื่อนไขหรือการดำเนินงานที่ต้องการความใส่ใจเป็นพิเศษในการกำกับดูแล และการดำเนินการแก้ไขผลกระทบตามลำดับความสำคัญ

ผู้ตรวจสอบไม่ควรคาดหวังว่าทุกองค์กรจะใช้เทคนิคการบริหารโครงการอย่างเต็มรูปแบบ การสอบทานควรจะเน้นความเสี่ยงและสิ่งสำคัญที่ทำให้เกิดความมั่นใจว่ามาตรฐานการบริหารโครงการ การควบคุม และกระบวนการดำเนินโครงการที่ใช้มีความเหมาะสมกับลักษณะและความเสี่ยงของโครงการที่ต้องการสอบทาน

ผู้ตรวจสอบไม่ควรใช้เวลากับประเด็นย่อยบางรายการ ผู้ตรวจสอบควรจะบันทึกว่าใช่หรือไม่ สำหรับรายการย่อยที่ตรวจสอบ อย่างไรก็ตาม ผู้ตรวจสอบต้องจัดทำเอกสารประกอบการตรวจสอบให้เพียงพอตามข้อสังเกตที่ตรวจพบ การจัดทำเอกสารประกอบต้องเพียงพอและสนับสนุนการประเมินการจัดอันดับเรื่องการพัฒนาและการจัดซื้อ

3.2 วัตถุประสงค์และกระบวนการตรวจสอบ

<u>วัตถุประสงค์ที่ 1</u> **:** การ**กำหนดขอบเขตการสอบทาน**การพัฒนาและการจัดหา

1. **ระบุจุดแข็งจุดอ่อนในการดำเนินงานพัฒนา จัดซื้อ และการบำรุงรักษา** โดยการสอบทาน ดังนี้

- รายงานผลการตรวจสอบครั้งก่อน
- รายงานผลการตรวจสอบภายในและภายนอก
- รายงานของผู้กำกับดูแล ผู้ตรวจสอบ และการรักษาความปลอดภัยจากผู้ให้บริการหลัก
- ผังโครงสร้างองค์กร
- ผังแสดงการจัดวางเครือข่าย
- ประวัติของผู้จัดการฝ่ายเทคโนโลยี

2. สอบทาน**ผลการดำเนินการของฝ่ายจัดการที่มีต่อรายงานและข้อสังเกตที่พบจากการตรวจสอบ**เพื่อกำหนด ดังนี้

- ความเหมาะสมและเวลาที่ใช้ในการแก้ไขปัญหา
- การแก้ไขปัญหาจากต้นเหตุมากกว่าการแก้ไขเป็นแต่ละกรณี
- ประเด็นปัญหาที่ยังไม่ได้รับการแก้ไข

3. **สอบทานเอกสารประกอบที่จำเป็นและสัมภาษณ์ผู้จัดการฝ่ายเทคโนโลยี**เพื่อระบุ ดังนี้

- รูปแบบและความถี่ของโครงการด้าน การพัฒนา การจัดหา และการบำรุงรักษา
- รูปแบบและลักษณะของเทคนิคในการบริหารโครงการ
- การเปลี่ยนแปลงที่สำคัญและมีผลกระทบกับการพัฒนา การจัดหา และการบำรุงรักษา เช่น การเปลี่ยนแปลงจริงหรือแผนการเปลี่ยนแปลงเกี่ยวกับ hardware software และผู้ขาย การเปลี่ยนแปลงจริงหรือแผนการเปลี่ยนแปลงเกี่ยวกับวัตถุประสงค์ทางธุรกิจและโครงสร้างการองค์กร และการเปลี่ยนแปลงจริงหรือแผนการเปลี่ยนแปลงเกี่ยวกับตำแหน่งงานของบุคลากรที่สำคัญ

<u>วัตถุประสงค์ที่ 2</u> **:** การ**ประเมินระดับของการกำกับดูแลและการสนับสนุนจากคณะกรรมการและฝ่ายจัดการ**ที่เกี่ยวข้องกับกิจกรรมในการพัฒนาการจัดหา และการบำรุงรักษา

1. ประเมินระดับของการกำกับดูแลและการสนับสนุน โดยการประเมิน ดังนี้

- ความสอดคล้องกันของวัตถุประสงค์ทางธุรกิจและ IT
- ความถี่และคุณภาพของรายงานด้าน IT ที่เสนอคณะกรรมการสถาบันการเงิน
- ข้อผูกมัดของกรรมการและผู้บริหารระดับสูงในการส่งเสริมการพัฒนาผลิตภัณฑ์ใหม่
- ระดับและคุณภาพของมาตรฐานและขั้นตอนการปฏิบัติงานที่ผ่านการอนุมัติโดยคณะกรรมการสถาบันการเงิน
- คุณสมบัติของผู้จัดการฝ่าย IT
- ความเพียงพอของงบประมาณด้าน IT

วัตถุประสงค์ที่ 3 **: ประเมินโครงสร้างขององค์กรที่เกี่ยวกับความเหมาะสมของการมอบหมายความรับผิดชอบด้าน IT** และการเริ่มต้นโครงการ

1. ประเมินความรับผิดชอบภายในองค์กรเพื่อให้มั่นใจว่าคณะกรรมการสถาบันการเงินและฝ่ายจัดการ

- กำหนดหน้าที่ความรับผิดชอบได้อย่างเหมาะสมและชัดเจน
- กำหนดให้บุคลากรการรักษาความปลอดภัย การตรวจสอบ และการรับประกันคุณภาพให้เข้าไปดำเนินงานในโครงการ ที่เกี่ยวข้องกับ IT
- กำหนดให้มีการแบ่งแยกหน้าที่การทำงานหรือระบบการควบคุมอื่นชดเชยแทน
- กำหนดความต้องการของโครงการ การประชุมด้านเทคโนโลยี และการรายงานคณะกรรมการได้อย่างเหมาะสม

วัตถุประสงค์ที่ 4 **: ประเมินระดับและลักษณะของความเสี่ยง**ที่เกี่ยวกับการพัฒนาการจัดหา และการบำรุงรักษาซึ่งอาจจะมีผลกระทบที่สำคัญต่อองค์กร

1. ประเมินความเสี่ยงที่ระบุไว้ตามวัตถุประสงค์อื่นและประเมินความเพียงพอของการบริหารความเสี่ยง ที่เกี่ยวข้องกับ

- ขั้นตอนการปฏิบัติงานในการประเมินและระบุความเสี่ยง
- ขั้นตอนการปฏิบัติงานในการรายงานผลและการเฝ้าติดตามดูแลความเสี่ยง
- กลยุทธ์ในการยอมรับ การบรรเทา และการถ่ายโอนความเสี่ยง

วัตถุประสงค์ที่ 5 **: ประเมินความเพียงพอของมาตรฐาน ระเบียบวิธี และแนวทางปฏิบัติในการบริหารและการพัฒนาโครงการ**

1. ประเมินความเพียงพอของกิจกรรมในการพัฒนาโดยการประเมิน

- ความเพียงพอและการยึดมั่นตามมาตรฐานและระบบควบคุมในการพัฒนา
- ความมีประสิทธิผลและความเป็นไปได้ในการนำระเบียบวิธีการบริหารโครงการมาสู่การปฏิบัติ
- ประสบการณ์ของผู้จัดการโครงการ
- ความเพียงพอของแผนงานโครงการ โดยเฉพาะการดูแลติดตามซึ่งรวมถึงการกำหนดที่ชัดเจนเกี่ยวกับความคาดหวังในแต่ละขั้นตอน เงื่อนไขการยอมรับแต่ละขั้นตอน ความต้องการการรักษาความปลอดภัยและการควบคุม ความต้องการทดสอบ ความต้องการเอกสารประกอบ

- ระเบียบวิธีการและประสิทธิผลของแผนการรับรองคุณภาพ
- ประสิทธิผลของแผนการบริหารความเสี่ยง
- ความเพียงพอของกระบวนงานร้องขอพัฒนาและอนุมัติโครงการ
- ความเพียงพอของการศึกษาความเป็นไปได้
- ความเพียงพอและการปฏิบัติตามมาตรฐานและกระบวนงานเกี่ยวกับขั้นตอนการออกแบบ การพัฒนา การทดสอบ และการนำออกใช้
- ความเพียงพอของการควบคุมการเปลี่ยนแปลงโครงการ
- ความเหมาะสมของบุคลากรในองค์กรที่มีส่วนร่วมในวงจรการพัฒนาโครงการ
- ความมีประสิทธิผลของการสื่อสารโครงการและกระบวนงานการรายงาน
- ความถูกต้อง ความมีประสิทธิผล และการควบคุมเครื่องมือบริหารโครงการ

วัตถุประสงค์ที่ 6 **: ประเมินความเพียงพอของมาตรฐาน ระเบียบวิธี และแนวปฏิบัติในการบริหารโครงการจัดซื้อ**

1. ประเมินความเพียงพอของการดำเนินงานจัดซื้อ โดยการประเมิน
   - ความเพียงพอและการปฏิบัติตามมาตรฐานและการควบคุมการจัดซื้อ
   - ความสามารถในการใช้และความมีประสิทธิผลของระเบียบวิธีการบริหารโครงการ
   - ประสบการณ์ของผู้จัดการโครงการ
   - ความเพียงพอของแผนงานโครงการ โดยเฉพาะการดูแลติดตามซึ่งรวมถึงการกำหนดที่ชัดเจนเกี่ยวกับความคาดหวังในแต่ละขั้นตอน เงื่อนไขการยอมรับแต่ละขั้นตอน ความต้องการการรักษาความปลอดภัยและการควบคุม ความต้องการทดสอบ การฝึกอบรม และการนำออกใช้
   - ระเบียบวิธีการและประสิทธิผลของแผนการรับรองคุณภาพ
   - ประสิทธิผลของแผนการบริหารความเสี่ยง
   - ความเพียงพอของกระบวนงานร้องขอพัฒนาและอนุมัติโครงการ
   - ความเพียงพอของการศึกษาความเป็นไปได้
   - ความเพียงพอและการปฏิบัติตามมาตรฐานที่เกี่ยวกับความต้องการขององค์กรกับผู้เสนอขายโครงการโดยการประมูลรวมถึงรายละเอียดการรักษาความปลอดภัย ความเชื่อถือ

ได้ และหน้าที่การทำงานของระบบที่ชัดเจน รายละเอียดการดำเนินงานและสิ่งที่ใช้ร่วมกันได้ที่ชัดเจน และความต้องการเอกสารประกอบการออกแบบและการพัฒนาที่ชัดเจน

- ความเพียงพอและการปฏิบัติตามมาตรฐานที่เกี่ยวกับความต้องการการสอบทานเงื่อนไขและข้อผูกมัดทางการเงินของผู้ขายในการให้บริการอย่างละเอียด
- ความเพียงพอของข้อกำหนดในสัญญาและการอนุญาตเกี่ยวกับการรับรองการดำเนินงาน ข้อกำหนดการรักษาความปลอดภัยข้อมูลและ software และความสามารถในการเข้าถึงโปรแกรมต้นฉบับหรือสิทธิในการเข้าใช้งานโปรแกรมต้นฉบับที่ฝากไว้กับบุคคลที่สาม (Escrow)
- ความเพียงพอของการควบคุมการเปลี่ยนแปลงโครงการ
- ความเหมาะสมของบุคลากรในองค์กรที่มีส่วนร่วมในวงจรการพัฒนาโครงการ
- ความมีประสิทธิผลของการสื่อสารโครงการและกระบวนงานการรายงาน
- ความถูกต้อง ความมีประสิทธิผล และการควบคุมเครื่องมือบริหารโครงการ

วัตถุประสงค์ที่ 7 **: ประเมินความเพียงพอของมาตรฐาน ระเบียบวิธี และแนวปฏิบัติในการบำรุงรักษาโครงการ**

1. ประเมินความเพียงพอและการปฏิบัติตามมาตรฐานและการควบคุมการบำรุงรักษา ดังนี้
   - กระบวนงานร้องขอและอนุมัติการเปลี่ยนแปลง
   - กระบวนงานการทดสอบการเปลี่ยนแปลง
   - กระบวนงานการนำสิ่งที่เปลี่ยนแปลงออกใช้งาน
   - กระบวนงานสอบทานการเปลี่ยนแปลง
   - กระบวนงานจัดทำเอกสารประกอบการเปลี่ยนแปลง
   - กระบวนงานแจ้งให้ทราบการเปลี่ยนแปลง
   - การควบคุมห้องเก็บโปรแกรม
   - การควบคุมโปรแกรมใช้งานอื่น

วัตถุประสงค์ที่ 8 **:** ประเมินประสิทธิผลของโครงการที่เปลี่ยนแปลง

1. ประเมินประสิทธิผลของโครงการที่เปลี่ยนแปลงโดย
   - การ**เปรียบเทียบงบประมาณที่ตั้งไว้และเวลาที่ใช้พัฒนาโครงการกับผลที่เกิดขึ้นจริง**

- การสอบทานการบริหารโครงการและรายงานการประชุมด้านเทคโนโลยี
- การสอบทานเอกสารประกอบการทดสอบและรายงานการดำเนินการเกี่ยวกับผลการทดสอบ
- การสอบทานรายงานหลังจากการดำเนินการเปลี่ยนแปลง
- การสัมภาษณ์พนักงานด้านเทคโนโลยีและผู้ใช้งานทางธุรกิจ
- การสอบทานบัญชีพักที่เป็นยอดคงค้าง

วัตถุประสงค์ที่ 9 **:** ประเมินความเพียงพอของแผนการรับรองคุณภาพ

1. ประเมินความเพียงพอของแผนการรับรองคุณภาพโดยการประเมิน
   - ความตั้งใจของคณะกรรมการในการจัดเตรียมทรัพยากรให้พอเหมาะกับแผนการรับรองคุณภาพ
   - ความสมบูรณ์ของกระบวนงานการรับรองคุณภาพ (การส่งมอบแต่ละโครงการ แต่ละขั้นตอนของโครงการ รวมถึงการตรวจสอบสมมติฐานโครงการ การอนุมัติ และการรับรองอย่างเหมาะสม)
   - ความสามารถในการแบ่งแยกกระบวนงานการรับรองคุณภาพ (การแบ่งงานรับรองคุณภาพตามลักษณะของโครงการได้อย่างเหมาะสม)
   - ความสามารถในการวัดมาตรฐานการรับรองคุณภาพ (ประเมินสิ่งที่ส่งมอบกับมาตรฐานหรือความคาดหวังที่ได้กำหนดไว้แล้ว)
   - การปฏิบัติตามมาตรฐานการติดตามปัญหานั้นต้องมีการบันทึกปัญหา การรายงานปัญหา การดูแลติดตามปัญหา และการแก้ไขปัญหาได้อย่างเหมาะสม
   - ความเพียงพอและการปฏิบัติตามมาตรฐานการทดสอบนั้นต้องใช้มาตรฐานที่กำหนดไว้แล้ว แผนการทดสอบที่เข้าใจง่าย ส่วนที่เกี่ยวข้องกับผู้ใช้งาน เอกสารประกอบผลการทดสอบ การ**ห้ามทดสอบบนสภาพแวดล้อมจริงและข้อมูลที่ใช้งานในปัจจุบัน**
   - ความเพียงพอและความมีประสิทธิผลของแผนการทดสอบที่ต้องดูแลความถูกต้องของการเขียนโปรแกรม การสรุปหน้าที่การทำงานของระบบที่กำหนดไว้ และความสามารถในการทำงานร่วมกันของระบบงานกับส่วนประกอบของเครือข่าย
   - **ความเป็นอิสระของผู้รับรองคุณภาพ**

วัตถุประสงค์ที่ 10 **: ประเมินความเพียงพอของการควบคุมการเปลี่ยนแปลงโปรแกรม**

1. ประเมินความเพียงพอและการปฏิบัติตาม

- มาตรฐานการเปลี่ยนแปลงโปรแกรมที่เป็นระบบงานประจำและแบบเร่งด่วนที่ต้องการความเหมาะสมของกระบวนงานร้องขอและอนุมัติ กระบวนงานการทดสอบ การนำออกใช้ การสำรองและการกู้คืน การจัดทำเอกสารประกอบ และการแจ้งให้ผู้เกี่ยวข้องทราบ

- การควบคุมที่จำกัดการเคลื่อนย้ายโปรแกรมที่ไม่ได้รับอนุญาตระหว่างการพัฒนา การทดสอบ และสภาพแวดล้อมที่ใช้งานจริง

- **การควบคุมที่จำกัดการใช้โปรแกรมอรรถประโยชน์**ที่ไม่ได้รับอนุญาต เช่น ออกเป็นนโยบายห้ามกระทำ การติดตามดูแลการใช้งาน และการควบคุมการเข้าถึงระบบงาน

- การควบคุมห้องเก็บโปรแกรมที่จำกัดการเข้าถึงโปรแกรมจากภายนอกของผู้ที่ไม่ได้รับอนุญาต โดยกำหนดสิทธิความรับผิดชอบเป็นรายบุคคล เช่น การควบคุมการเข้าถึงห้องเก็บโปรแกรม และการควบคุมห้องเก็บโปรแกรมแบบอัตโนมัติที่จำกัดการเข้าถึงและสร้างรายงานการเข้าถึงเพื่อกำหนดบุคคลที่สามารถเข้าถึงได้เมื่อใดและเปลี่ยนแปลงอะไรได้บ้าง

- การควบคุมรุ่นของโปรแกรมที่พัฒนาช่วยให้การเก็บโปรแกรมมีความเหมาะสม รวมถึงการแก้ไขและการจัดทำเอกสารประกอบ

วัตถุประสงค์ที่ 11 **:** ประเมินความเพียงพอของ**มาตรฐานและการควบคุมการบริหารการเสริมสร้างการรักษาความปลอดภัย (patch)**

1. ประเมินความเพียงพอและการปฏิบัติตามมาตรฐานและการควบคุมการบริหารการ patch นั้นต้องปฏิบัติ ดังนี้

- รายละเอียดทรัพย์สินที่เป็น hardware และ software
- กระบวนงานการกำหนดให้ patch
- กระบวนงานการประเมิน patch
- กระบวนงานการร้องขอและอนุมัติให้ patch
- กระบวนงานการทดสอบการ patch
- กระบวนงานการสำรองและการกู้คืน
- กระบวนงานการนำ patch ออกใช้งาน
- การจัดทำเอกสารประกอบการ patch

วัตถุประสงค์ที่ 12 **: การประเมินคุณภาพของเอกสารประกอบระบบงาน ระบบโปรแกรมต้นฉบับ** และ**ความเพียงพอของการควบคุมเอกสารประกอบ**

1. ประเมินความเพียงพอของการควบคุมเอกสารประกอบโดยการประเมินความ

เพียงพอและการปฏิบัติตามมาตรฐานการจัดทำเอกสารประกอบที่ต้องปฏิบัติ ดังนี้

- การกำหนดความรับผิดชอบในการเก็บเอกสารประกอบ
- การกำหนดความรับผิดชอบในการให้อำนาจและอนุมัติการจัดทำเอกสารประกอบ
- การสร้างรูปแบบการจัดทำเอกสารประกอบที่เป็นมาตรฐาน
- การสร้างการควบคุมห้องเก็บและรุ่นของเอกสารประกอบอย่างเหมาะสม

2. ประเมินคุณภาพของเอกสารประกอบระบบงานโดยการประเมินความเพียงพอของการประเมินจากภายในและภายนอกองค์กร ดังนี้

- มาตรฐานการออกแบบและการเขียนโปรแกรมระบบงาน
- คำอธิบายระบบงาน
- เอกสารประกอบการออกแบบระบบงาน
- รายชื่อโปรแกรมต้นฉบับหรือโปรแกรมเชิงวัตถุ
- ระเบียบวิธีการตั้งชื่อระบบงานประจำ
- คู่มือผู้ปฏิบัติงานและคู่มือการใช้งานระบบงานย่อย

3. ประเมินคุณภาพของเอกสารประกอบโปรแกรมต้นฉบับของระบบเปิดโดยการประเมินความเพียงพอของการประเมินจากภายในและภายนอก ดังนี้

- มาตรฐานการออกแบบและการเขียนโปรแกรมระบบงาน
- คำอธิบายระบบงาน
- เอกสารประกอบการออกแบบระบบงาน
- รายชื่อโปรแกรมต้นฉบับหรือโปรแกรมเชิงวัตถุ
- ระเบียบวิธีการตั้งชื่อระบบงานประจำ
- คู่มือการปฏิบัติงานระบบ

4. ประเมินคุณภาพของเอกสารประกอบโครงการโดยการประเมินความเพียงพอของเอกสารประกอบเกี่ยวกับ

- คำร้องขอพัฒนาโครงการ
- กรณีศึกษาความเป็นไปได้
- ขั้นตอนการเริ่มต้น
- ขั้นตอนการวางแผน

- ขั้นตอนการออกแบบ
- ขั้นตอนการพัฒนา
- ขั้นตอนการทดสอบ
- ขั้นตอนการนำออกใช้งาน
- การสอบทานหลังการนำออกใช้งาน

หมายเหตุ : ถ้าผู้ตรวจสอบใช้เทคนิคการสุ่มตัวอย่าง ก็ควรจะรวมถึงเอกสารประกอบในขั้นตอนการวางแผนและการทดสอบด้วย

วัตถุประสงค์ที่ 13 **:** ประเมินการรักษาความปลอดภัยและความถูกต้องเชื่อถือได้ของระบบและระบบงาน

1. ประเมินการรักษาความปลอดภัยและความถูกต้องเชื่อถือได้ของระบบและระบบงานโดยการสอบทาน

- ความเพียงพอของแผนการรับรองคุณภาพและแผนการทดสอบ
- ความเพียงพอของมาตรฐานการรักษาความปลอดภัยและการออกแบบการควบคุมภายใน
- ความเพียงพอของการควบคุมการเปลี่ยนแปลงโปรแกรม
- ความเพียงพอของการมีส่วนร่วมของผู้ตรวจสอบและผู้ที่ดูแลการรักษาความปลอดภัยในโครงการพัฒนาและการจัดซื้อ
- ความเพียงพอของการรักษาความปลอดภัยทั้งจากภายในและภายนอก และการตรวจสอบการควบคุม

วัตถุประสงค์ที่ 14 **:** ประเมินความสามารถในการแก้ไขปัญหาข้อมูลเทคโนโลยีสารสนเทศได้ตรงตามความต้องการของผู้ใช้งาน สัมภาษณ์ผู้ใช้งานเพื่อสรุปการประเมินการแก้ปัญหาเทคโนโลยีของผู้ใช้งาน

วัตถุประสงค์ที่ 15 **:** ประเมินขอบเขตของการมีส่วนร่วมของผู้ใช้งานในกระบวนการพัฒนาและการจัดซื้อระบบสัมภาษณ์ผู้ใช้งานและสอบทานเอกสารประกอบการพัฒนาและการจัดซื้อโครงการเพื่อสรุปขอบเขตการมีส่วนร่วมของผู้ใช้งาน

สรุปผลการตรวจสอบ

วัตถุประสงค์ที่ 16 **:** การดำเนินการจัดทำเอกสารประกอบและการอภิปรายข้อสังเกตที่พบจากการตรวจสอบและข้อแนะนำในการแก้ไข

1. การจัดทำเอกสารประกอบข้อสังเกตที่พบจากการตรวจสอบและข้อแนะนำให้แก้ไขแสดงให้เห็นคุณภาพและประสิทธิผลของมาตรฐานและกระบวนงานการพัฒนาและจัดซื้อขององค์กร

2. อภิปรายข้อสังเกตเบื้องต้นกับหัวหน้าผู้ตรวจสอบ ดังนี้

- การกระทำที่ผิดกฎหมาย กฎเกณฑ์ และการกำกับดูแลของทางการ
- สรุปประเด็นในรายงานการตรวจสอบ

3. อภิปรายข้อสังเกตของคุณกับฝ่ายจัดการและรับข้อผูกมัดในการดำเนินการแก้ไขและกำหนดวันสุดท้ายที่ต้องแก้ไขสำหรับข้อบกพร่องที่มีความสำคัญ

4. อภิปรายข้อสังเกตกับหัวหน้าผู้ตรวจสอบ ดังนี้

- ข้อแนะนำให้แก้ไขการจัดระดับในเรื่องการพัฒนาและการจัดซื้อ
- ข้อแนะนำให้แก้ไขข้อสังเกตที่มีผลกับการจัดระดับในภาพรวม

5. จัดทำข้อสรุปเสนอหัวหน้าผู้ตรวจสอบเพื่อเตรียมการจัดทำรายงานข้อสังเกตให้กับส่วนที่เกี่ยวข้องทั้งหมดในการออกรายงานการตรวจสอบรวม

6. รวบรวมกระดาษทำการเพื่อให้แน่ใจว่ามีเอกสารสนับสนุนที่ชัดเจนเกี่ยวกับข้อสังเกตและข้อแนะนำที่สำคัญ

ภาคผนวก : อภิธานศัพท์ (Glossary)

Application (ระบบงาน)	โปรแกรมที่ออกแบบให้ผู้ใช้งาน
Acceptance Criteria (เงื่อนไขการยอมรับ)	มาตรฐานหรือความต้องการที่กำหนดไว้ของผลิตภัณฑ์หรือโครงการที่ต้องเป็นไปตามวัตถุประสงค์
Automated Controls (การควบคุมแบบอัตโนมัติ)	Software ที่ถูกออกแบบอยู่ในโปรแกรมเพื่อการตรวจสอบ ความถูกต้อง ความสมบูรณ์ของข้อมูลและการนำมาใช้ ประมวลผลและเก็บข้อมูล
Baseline (บรรทัดฐาน)	รุ่นของเอกสารที่แสดง รายละเอียดของ hardware และโปรแกรมและการกำหนดค่าตัวแปรมาตรฐาน (configuration) ขั้นตอนการปฏิบัติงาน และการบริหารโครงการ
Code (การเขียนโปรแกรม)	ชุดคำสั่งเกี่ยวกับ software โปรแกรม
Database (ฐานข้อมูล)	การจัดข้อมูลให้เก็บแบบอิเล็กทรอนิกส์
Deliverable (สามารถส่งมอบได้)	เป้าหมายหรือความคาดหวังของโครงการ การสามารถส่งมอบได้รวมถึงการกำหนดเสร็จของโครงการ หรือเสร็จแต่ละขั้นตอน หรือเสร็จในแต่ละงาน
Distributed Environment (เครือข่ายที่เป็นกายภาพ)	ระบบคอมพิวเตอร์กับส่วนประกอบของข้อมูลและโปรแกรมที่เป็นลักษณะกายภาพที่เชื่อมโยงกันมากกว่า 1 เครื่อง
End User (ผู้ใช้งาน)	บุคคลที่ใช้งานโปรแกรมที่พัฒนาเสร็จแล้ว
Enterprise Architecture (สถาปัตยกรรมองค์กร)	กรอบการทำงานขององค์กรที่เกี่ยวกับนโยบายด้านเทคโนโลยีทั้งที่เป็น hardware และ software
Flowcharts (ผังทางเดินงาน)	ผังทางเดินงานจะเป็นการใช้สัญลักษณ์แทนงาน เช่น เพชร รูปไข่ สี่เหลี่ยม เพื่อแสดงถึงลำดับการทำงานของโปรแกรม ถ้าเป็น software ที่ใช้ในการเขียนผังทางเดินงานจะสามารถทำได้โดยอัตโนมัติในการสร้างหรือลบได้ โดยที่ไม่ต้องวาดบนกระดาษ
Functional Requirements (ความต้องการหน้าที่การ	ลักษณะการทำงานทางธุรกิจ การปฏิบัติงาน และการรักษาความปลอดภัยที่องค์กรต้องการให้รวมอยู่ในโปรแกรม

ทำงานของระบบ)	
Iterative (วงจรการพัฒนา)	การทำซ้ำหรือวงจรการพัฒนา การพัฒนาที่เป็นวงจรเกี่ยวกับความสมบูรณ์ของงานโครงการหรือแต่ละขั้นตอนในวงจรการพัฒนา การดำเนินงานและแต่ละขั้นตอนจะถูกกระทำจนกว่าจะได้ผลลัพธ์ตามที่ต้องการ
LAN (เครือข่ายภายใน)	เครือข่ายเชื่อมโยงภายในอาคาร
Load Module	กลุ่มของโปรแกรม (Object Code) ที่สัมพันธ์กันและพร้อมจะทำงานบนคอมพิวเตอร์แบบต่อเนื่องกันไป
Metrics (ตารางการวัด)	การวัดปริมาณ
Milestone (ขั้นตอนที่สำคัญ)	ใช้กับโครงการหลัก
Network (ระบบเครือข่ายคอมพิวเตอร์)	ระบบคอมพิวเตอร์ตั้งแต่ 2 เครื่องที่อยู่ในกลุ่มเดียวกันเพื่อแบ่งกันใช้ข้อมูล software และ hardware ร่วมกัน
Object Code (การเขียนโปรแกรมส่วนย่อย)	ชุดคำสั่ง software โปรแกรมที่แปลงจากโปรแกรมต้นฉบับให้เป็นภาษาที่เครื่องสามารถอ่านได้
Outsourcing (การใช้บริการจากบุคคลภายนอก)	การทำสัญญากับบุคคลภายนอกเพื่อดำเนินการ หรือทำหน้าที่บางอย่าง
Operating System (ระบบปฏิบัติการ)	โปรแกรมที่ทำหน้าที่จัดการระบบงาน ระบบปฏิบัติการจะจัดแบ่งเนื้อที่การทำงาน การควบคุมการเข้าถึงและการรักษาความปลอดภัย การรักษาไฟล์ และจัดการการติดต่อสื่อสารระหว่างผู้ใช้งานกับอุปกรณ์ hardware
Patch Code (การเขียนโปรแกรมเพิ่มการรักษาความปลอดภัย)	การเขียนโปรแกรมส่วนย่อย เพื่อเพิ่มการรักษาความปลอดภัยบน Software และ Hardware ต่าง ๆ
Phase (ขั้นตอนโครงการ)	ส่วนย่อยของโครงการ
Project (โครงการ)	งานที่เป็นการจัดซื้อ การพัฒนา และการบำรุงรักษาด้านเทคโนโลยีของผลิตภัณฑ์ที่สร้างขึ้นใหม่
Project Management (การบริหารโครงการ)	การวางแผนงาน การดูแลติดตามและการควบคุมการดำเนินงาน

Script (ส่วนย่อยโปรแกรม)	ชุดคำสั่ง software โปรแกรม
Source Code (โปรแกรมต้นฉบับ)	ชุดคำสั่งการเขียนโปรแกรมในรูปแบบที่คนอ่านได้
Spiral Development (แบบจำลองการพัฒนา)	แบบจำลองการบริหารโครงการแบบวงจรการพัฒนาที่เน้นการกำหนดความเสี่ยงของโครงการและผลิตภัณฑ์ใหม่ และการคัดเลือกเทคนิคการบริหารโครงการที่สามารถควบคุมความเสี่ยงที่กำหนดไว้ได้ดีที่สุด
SDLC (วงจรการพัฒนา)	วงจรการพัฒนาระบบถือเป็นเทคนิคการบริหารโครงการอย่างหนึ่ง