

สรุปผลการวิจัยและข้อเสนอแนะ

งานวิจัยเรื่อง การนำมาตรฐาน COBIT มาประยุกต์ใช้ในองค์กร เพื่อปรับปรุงกระบวนการตรวจสอบระบบสารสนเทศ กรณีศึกษา ผู้ประกอบธุรกิจทางการเงินที่ไม่ใช่สถาบันการเงิน (Non-bank) แห่งหนึ่ง มีวัตถุประสงค์ เพื่อให้ทราบถึงปัญหาและอุปสรรคของกระบวนการตรวจสอบระบบสารสนเทศ (IT Audit Process) เฉพาะการตรวจรับระบบงานในส่วนของการบริหารโครงการเทคโนโลยีสารสนเทศ (IT Project Management) ขององค์กรที่นำมาเป็นกรณีศึกษามีอยู่ในปัจจุบัน และการนำมาตรฐาน COBIT มาประยุกต์ใช้จัดปัญหาและอุปสรรคที่มีอยู่ให้เหมาะสม โดยองค์กรที่นำมาเป็นกรณีศึกษาในงานวิจัยครั้งนี้ เป็นองค์กรที่ประกอบธุรกิจทางการเงินด้านบัตรเครดิต และการให้สินเชื่อบุคคลที่ไม่ใช่สถาบันการเงิน (Non-bank) ที่มีการลงทุนด้านเทคโนโลยีสารสนเทศเพื่อสนับสนุนธุรกิจขององค์กรด้วยการ “Outsource” จากบริษัทภายนอกหลายราย

งานวิจัยนี้ใช้เทคนิคการวิจัยหลัก คือ การสัมภาษณ์ผู้ปฏิบัติงาน และผู้บริหารของส่วนตรวจสอบเทคโนโลยีสารสนเทศ เครื่องมือที่ใช้ในการวิจัย คือ แบบสัมภาษณ์ มีการออกแบบแบบสัมภาษณ์โดยอิงกับมาตรฐาน COBIT ใช้การสัมภาษณ์แบบเป็นทางการ (Formal Interview) เพื่อให้ทราบถึงปัญหาและอุปสรรคในการปฏิบัติงาน รวมทั้งข้อเสนอแนะแก้ไขปัญห และทำการศึกษาเอกสารการดำเนินงาน

เมื่อทำการรวบรวมข้อมูลแล้ว จึงนำมาวิเคราะห์สาเหตุ แล้วนำมาตรฐาน COBIT มาวิเคราะห์ปัญหา เพื่อให้ทราบถึงความไม่สอดคล้องกับมาตรฐานการควบคุมภายใน จากนั้นจึงนำเสนอแนวทางปรับปรุงการปฏิบัติงาน โดยตรวจสอบความเป็นไปได้ในการนำแนวทางนั้นมาปฏิบัติจริง ด้วยการสัมภาษณ์ความคิดเห็นในมุมมองของผู้เชี่ยวชาญด้านการตรวจสอบระบบสารสนเทศจากองค์กรภายนอก ผู้บริหาร และเจ้าหน้าที่ส่วนตรวจสอบเทคโนโลยีสารสนเทศขององค์กรที่นำมาเป็นกรณีศึกษา

5.1 สรุปผลการวิจัย

5.1.1 ปัญหาและอุปสรรคของการตรวจรับระบบงาน

5.1.1.1 กรณี New Project

- โครงการจบไม่ทันตามระยะเวลาที่กำหนด เนื่องจากโปรแกรมระบบงานทำงานไม่เป็นไปตาม User Requirement หรือไม่มีการกำหนดทีมงานของโครงการ เกิดความไม่ชัดเจนในการแบ่งแยกหน้าที่ความรับผิดชอบ และความต้องการ (Requirement) ของโครงการมีการเปลี่ยนแปลงบ่อย
- ขาดการวางแผน การควบคุมการดำเนินงาน และการประสานงานที่ดีระหว่างผู้ปฏิบัติงาน และ/หรือ หน่วยงานที่เกี่ยวข้องในการดำเนินงานโครงการ ทำให้โปรแกรมระบบงานไม่ตอบสนองความต้องการของผู้ใช้
- User หรือ IT Audit รับทราบโครงการล่าช้า เนื่องจาก Project Owner และ/หรือ Project Manager ไม่เข้าใจหรือไม่ปฏิบัติตามขั้นตอนของการตรวจรับระบบงาน
- ขาดการวางแผนการทดสอบที่ดี และ Test Scenario ในการทดสอบทำได้ไม่ครบถ้วน ทำให้การดำเนินการทดสอบอาจไม่ครอบคลุมในทุกกรณี
- มีการกำหนดบทบาทหน้าที่ให้ IT Audit ตรวจสอบความถูกต้องของผลการทดสอบระบบงาน (UAT) ก่อนใช้จริงบน Production System ทำให้ IT Audit ไม่มีความเป็นอิสระในการตรวจสอบระบบงาน และเกิดความขัดแย้งในการปฏิบัติงานตรวจรับระบบงาน
- User ไม่สามารถเชื่อมโยง Requirement เข้ากับการเพิ่มเติม หรือการเปลี่ยนแปลงขั้นตอนการปฏิบัติงานใน Procedure Manual ที่ใช้ปฏิบัติงานอยู่ในปัจจุบัน ทำให้ Procedure Manual ที่ใช้เป็นคู่มือในการปฏิบัติงานไม่มีความต่อเนื่องและไม่ทันสมัย
- User ไม่เข้าใจหน้าที่ความรับผิดชอบของตนเอง จึงต้องการให้ IT Audit เข้าร่วมในการ UAT Sign-off

5.1.1.2 กรณี Production Problem

- ไม่มีหน่วยงานต้นเรื่องในการขอปรับปรุงแก้ไขโปรแกรมระบบงานภายหลังการ Implementation เนื่องจากการแก้ไข Parameter หรือปัญหาที่เกิดขึ้นบางกรณีมีผลกระทบต่อการทำงานของหลายๆ หน่วยงาน
- ไม่มีการกำหนดให้ทีมงานโครงการทำการประเมินผลหลังจากนำระบบออกใช้งานจริง (Post Implementation Review)
- ไม่มีการทดสอบความถูกต้องของโปรแกรมระบบงานที่ปรับปรุงแก้ไข เนื่องจากต้องดำเนินการ Implement แบบเร่งด่วน เพื่อแก้ปัญหาที่เกิดขึ้น

5.1.2 การวิเคราะห์ปัญหาคด้วยมาตรฐาน COBIT

5.1.2.1 กรณี New Project

- การจัดการโครงการ (Manage Projects) จากการขาดการจัดตั้งทีมงานโครงการ ขาดการกำหนดหน้าที่ความรับผิดชอบให้ชัดเจน และขาดการมีส่วนร่วมในการริเริ่มโครงการของหน่วยงานผู้ใช้
- การประเมินความเสี่ยง (Assess Risk) การจัดการคุณภาพ (Manage Quality) และการติดตั้งและรับรองระบบ (Install and Accredited Systems) จากการดำเนินการทดสอบไม่ครอบคลุมในทุกกรณี
- การจัดหาและบำรุงรักษาโปรแกรมระบบงาน (Acquire and Maintain Application Software) จากการขาดการ Sign-off User Requirement และขาดการอนุมัติการออกแบบ
- การรับรองความเป็นอิสระ (Obtain Independent Assurance) และความเป็นอิสระในการตรวจสอบ (Provide for Independent Audit) จากการกำหนดหน้าที่ความรับผิดชอบให้ IT Audit ตรวจสอบความถูกต้องของผลการทดสอบระบบงาน (User Acceptance Test : UAT) ก่อนนำใช้จริงบน Production System

5.1.2.2 กรณี Production Problem

- การจัดโครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศและความสัมพันธ์กับหน่วยงานอื่นๆ (Define the IT Organisation and Relationships) จากการขาดการกำหนดเจ้าของระบบงานและข้อมูล (Application / Data Owner)
- การติดตั้งและรับรองระบบ (Install and Accredite Systems) จากการขาดการกำหนดให้ทีมงานโครงการประเมินผลหลังจากนำระบบออกใช้งานจริง (Post Implementation Review)
- การจัดการการเปลี่ยนแปลง (Manage Changes) จากการขาดการทดสอบความถูกต้องของโปรแกรมระบบงานที่ปรับปรุงแก้ไข

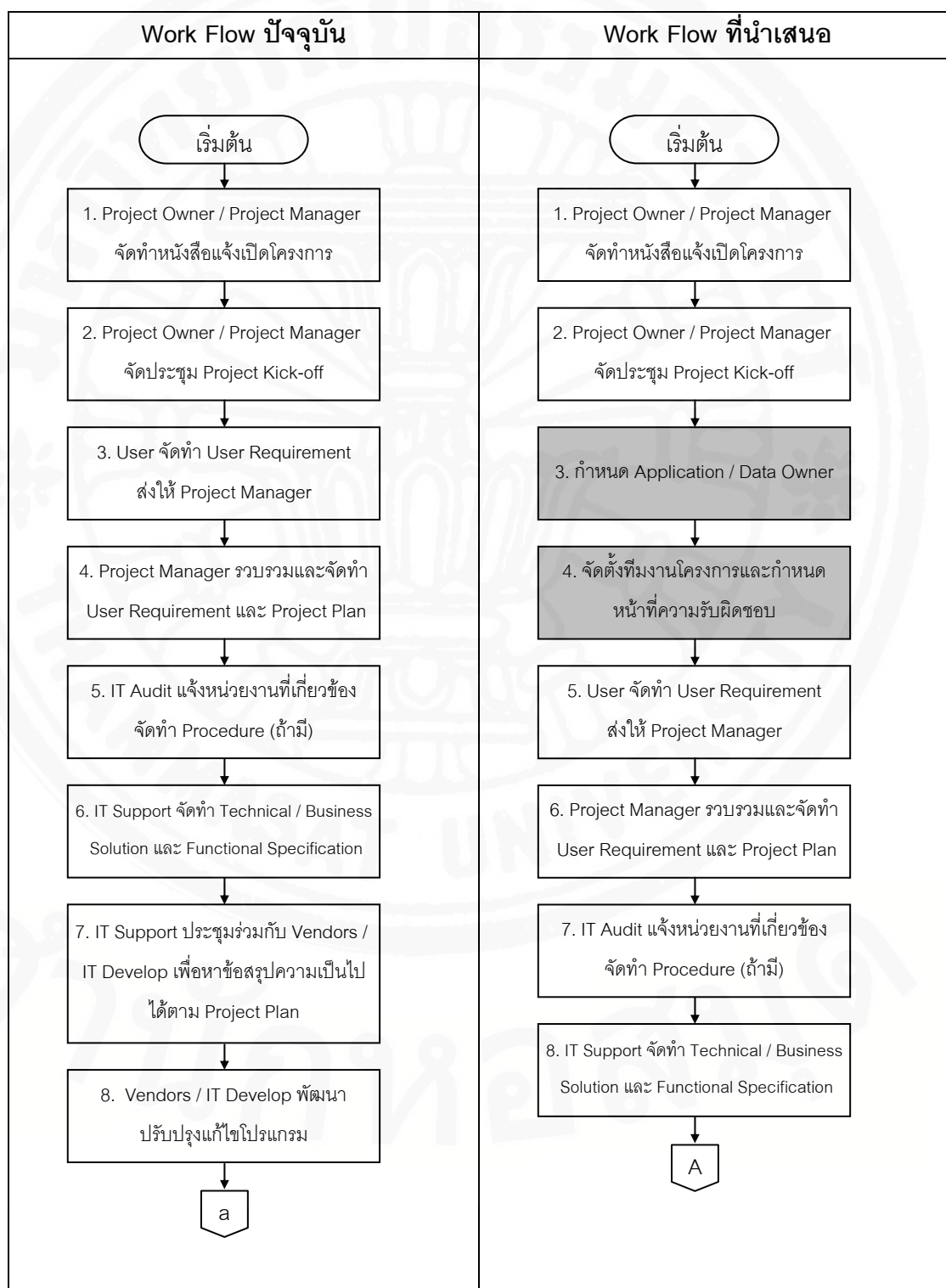
5.1.3 แนวทางปรับปรุงตามมาตรฐาน COBIT

5.1.3.1 กรณี New Project

- ควรกำหนดให้มีการ Sign-off User Requirement และสร้างตัวต้นแบบ (Prototype) นำเสนอแก่เจ้าของระบบและผู้ใช้งาน เพื่อเก็บรวบรวมความคิดเห็นและความต้องการของผู้ใช้
- ควรมีการจัดตั้งทีมงานโครงการ และกำหนดหน้าที่ความรับผิดชอบ (Responsibility) ของแต่ละฝ่ายที่เกี่ยวข้อง ว่ามีขอบข่ายงานอย่างไร ทำให้มีการทำงานที่ชัดเจนขึ้น รวมทั้งกำหนดให้มีการ Monitor Project Progress และ Solve Problem ด้วย
- ควรมีการกำหนดมาตรฐานการทดสอบโปรแกรมระบบงาน กำหนดแผนและกลยุทธ์ในการทดสอบให้เหมาะสมตามระดับความเสี่ยงที่ประเมินได้ โดยผู้ใช้งานต้องมีส่วนร่วมในการกำหนดแผน กลยุทธ์ และเงื่อนไขในการทดสอบด้วย
- ควรมีการกำหนดมาตรฐานด้านการตรวจสอบคุณภาพ (Quality Checks) เป็นการตรวจสอบการปฏิบัติงานในการพัฒนาระบบว่าเป็นไปตามความต้องการของเจ้าของระบบหรือผู้ใช้งานหรือไม่
- ควรกำหนดบทบาทความรับผิดชอบที่เป็นอิสระของ IT Audit

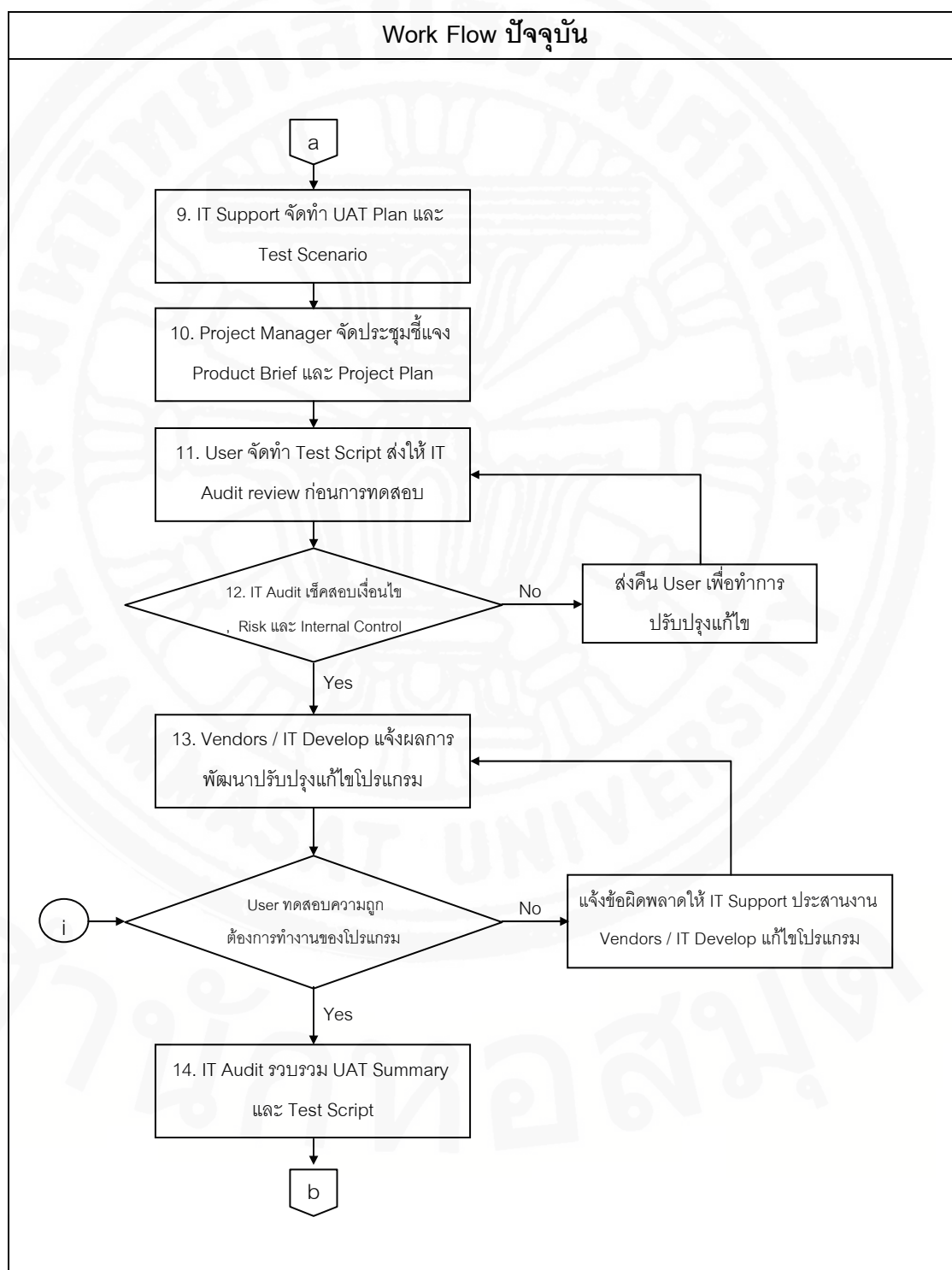
ภาพที่ 5.1

เปรียบเทียบ Work Flow ปัจจุบันและ Work Flow ตามแนวทางที่นำเสนอ
ของการตรวจรับระบบงาน กรณี New Project



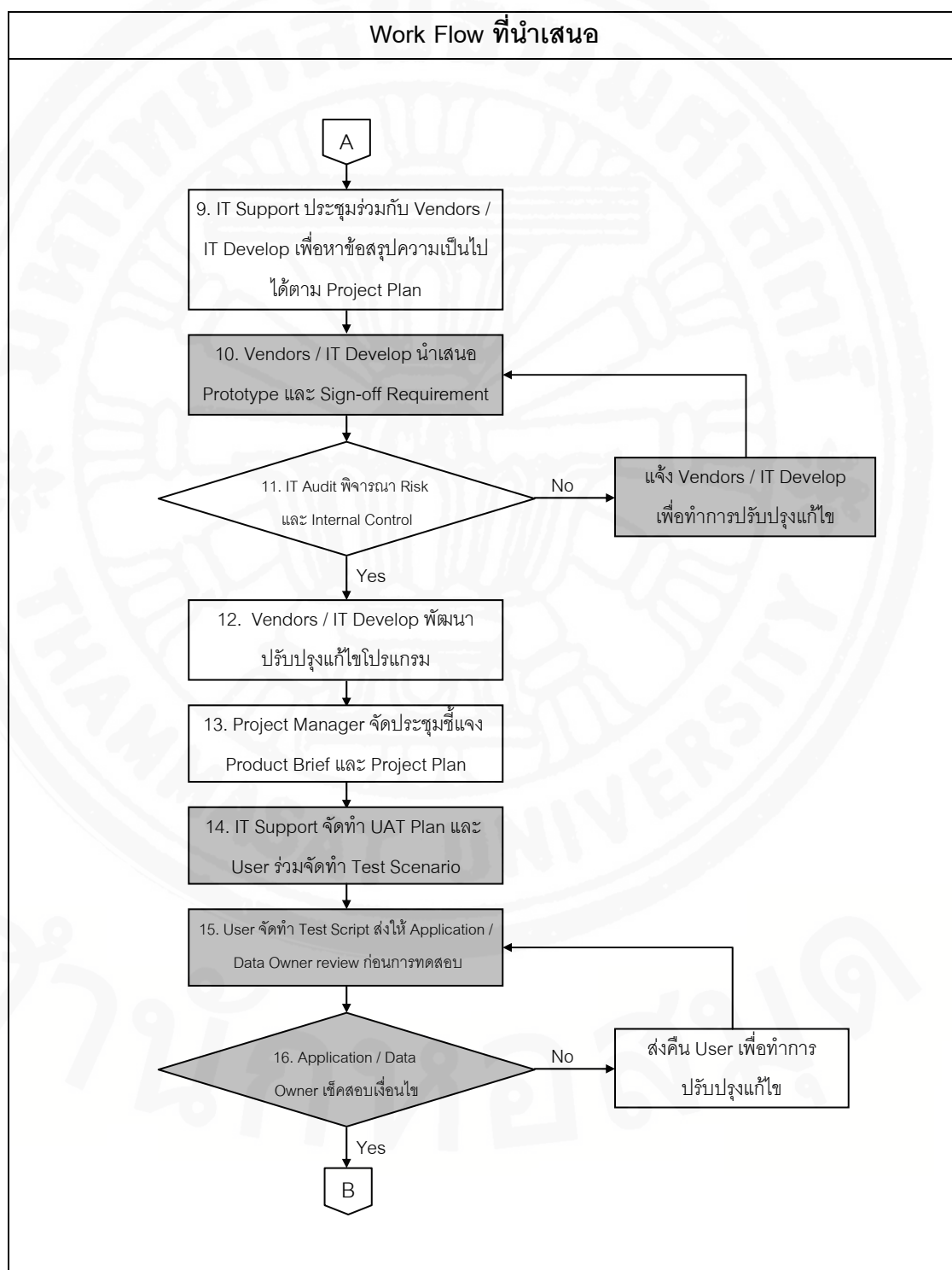
ภาพที่ 5.1 (ต่อ)

เปรียบเทียบ Work Flow ปัจจุบันและ Work Flow ตามแนวทางที่นำเสนอ
ของการตรวจรับระบบงาน กรณี New Project



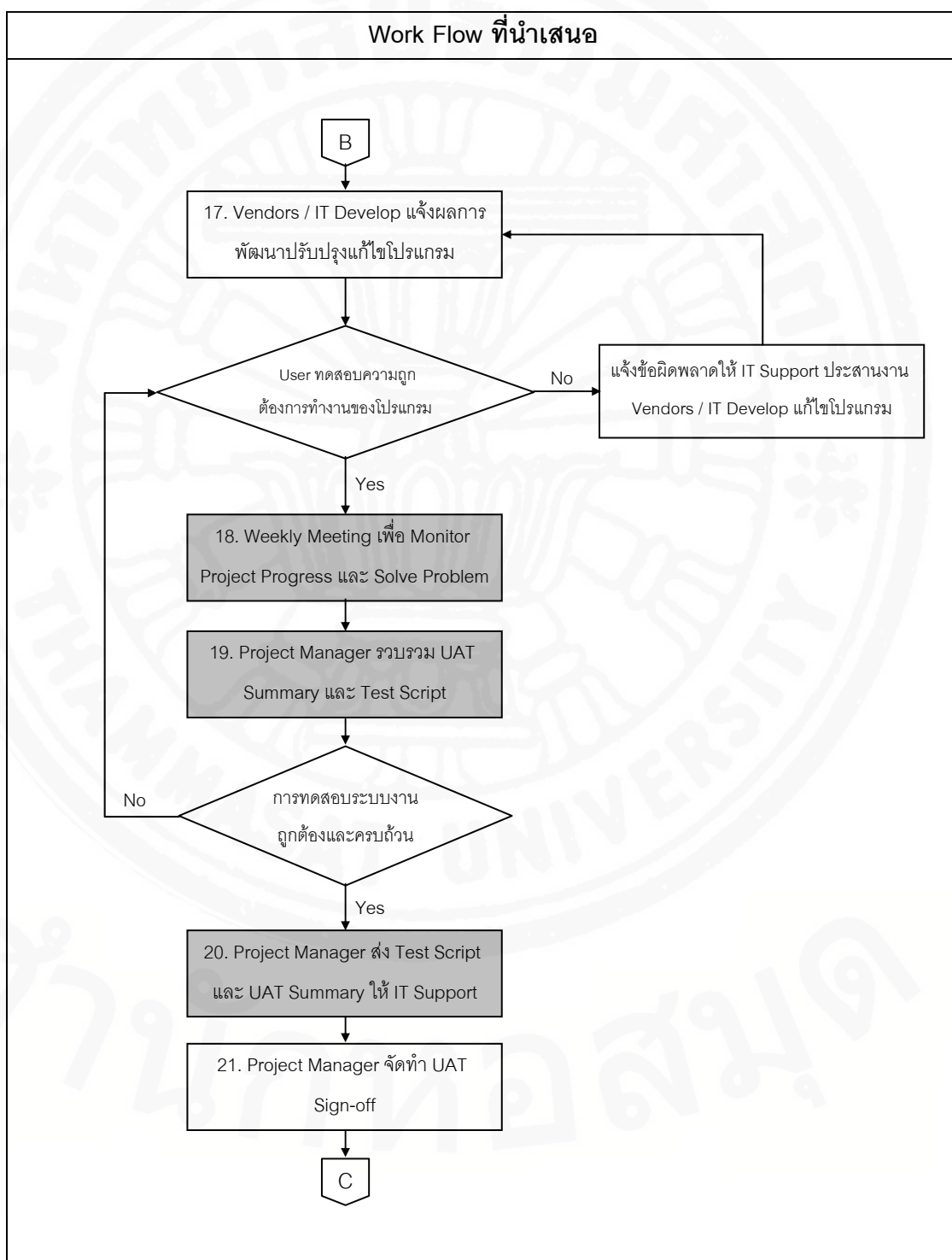
ภาพที่ 5.1 (ต่อ)

เปรียบเทียบ Work Flow ปัจจุบันและ Work Flow ตามแนวทางที่นำเสนอ
ของการตรวจรับระบบงาน กรณี New Project



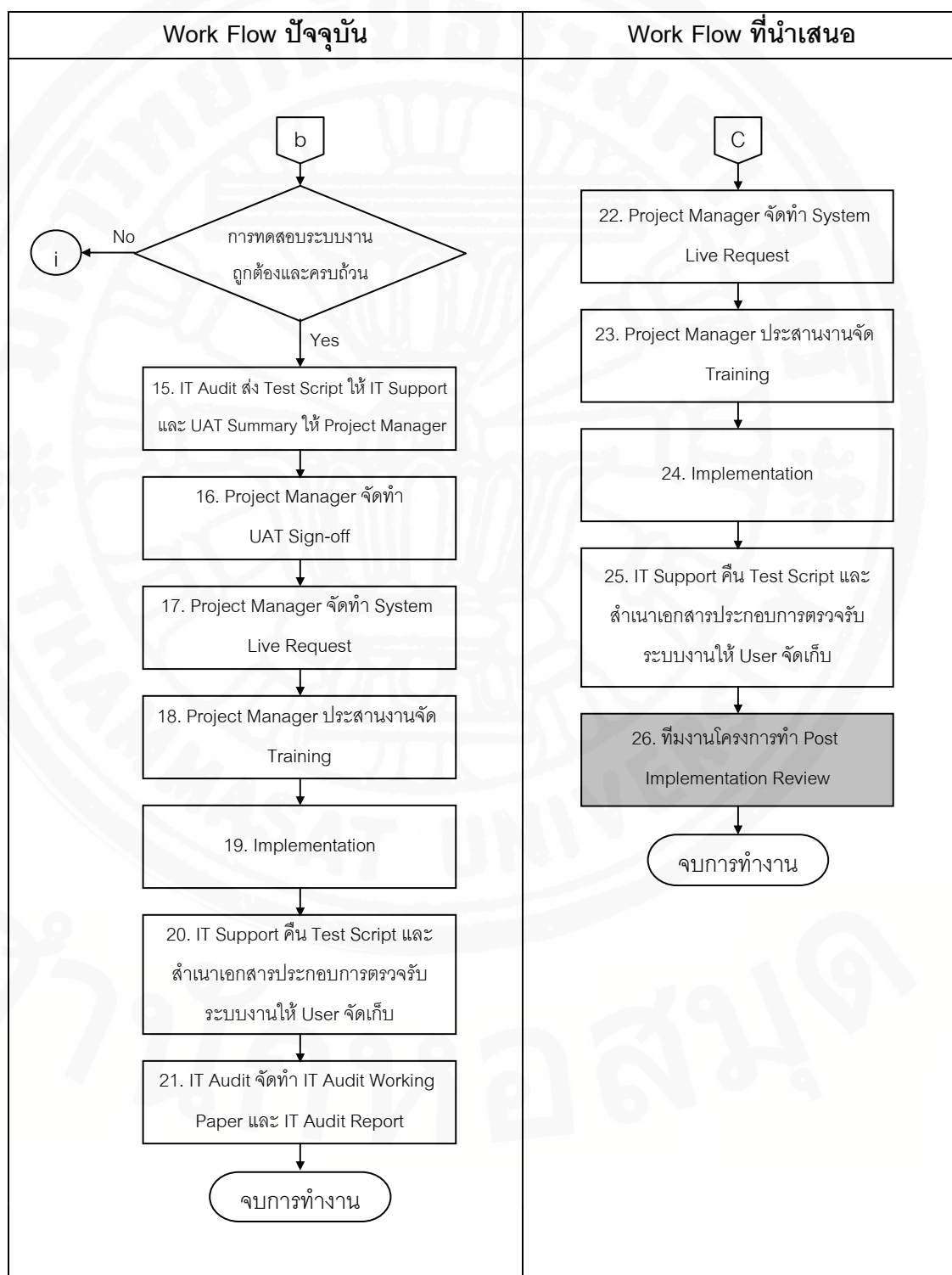
ภาพที่ 5.1 (ต่อ)

เปรียบเทียบ Work Flow ปัจจุบันและ Work Flow ตามแนวทางที่นำเสนอ
ของการตรวจรับระบบงาน กรณี New Project



ภาพที่ 5.1 (ต่อ)

เปรียบเทียบ Work Flow ปัจจุบันและ Work Flow ตามแนวทางที่นำเสนอ
ของการตรวจรับระบบงาน กรณี New Project



5.1.3.2 กรณี Production Problem

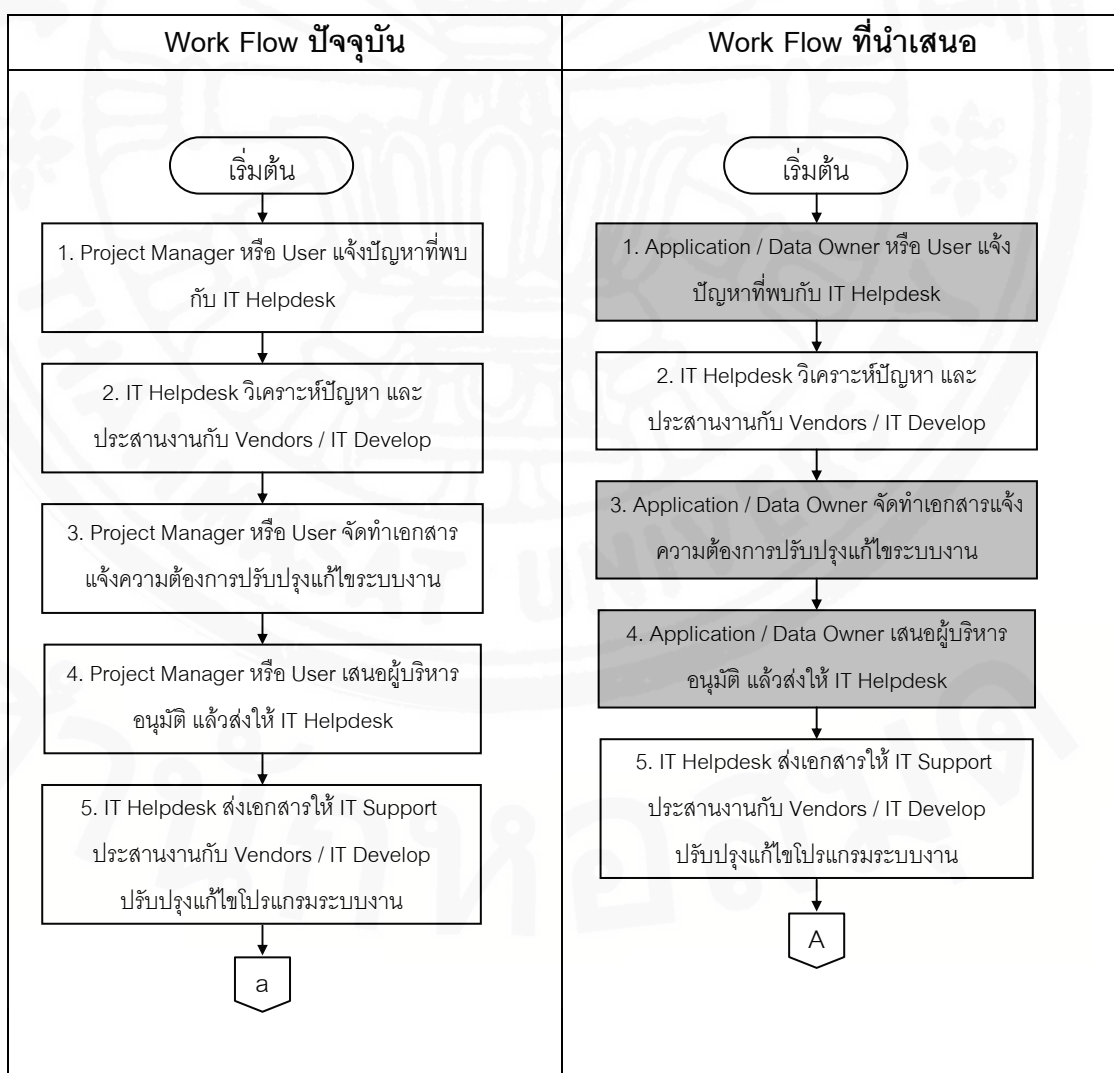
- ควรกำหนดเจ้าของระบบงานและข้อมูล (Application / Data Owner) ให้ชัดเจน
- ควรกำหนดให้ทีมงานโครงการทำการประเมินผลหลังจากนำระบบออกใช้งานจริง

(Post Implementation Review)

- กำหนดให้มีการจัดทำคำขอปรับปรุงแก้ไขระบบงาน และทดสอบความถูกต้องของโปรแกรมระบบงานย้อนหลัง

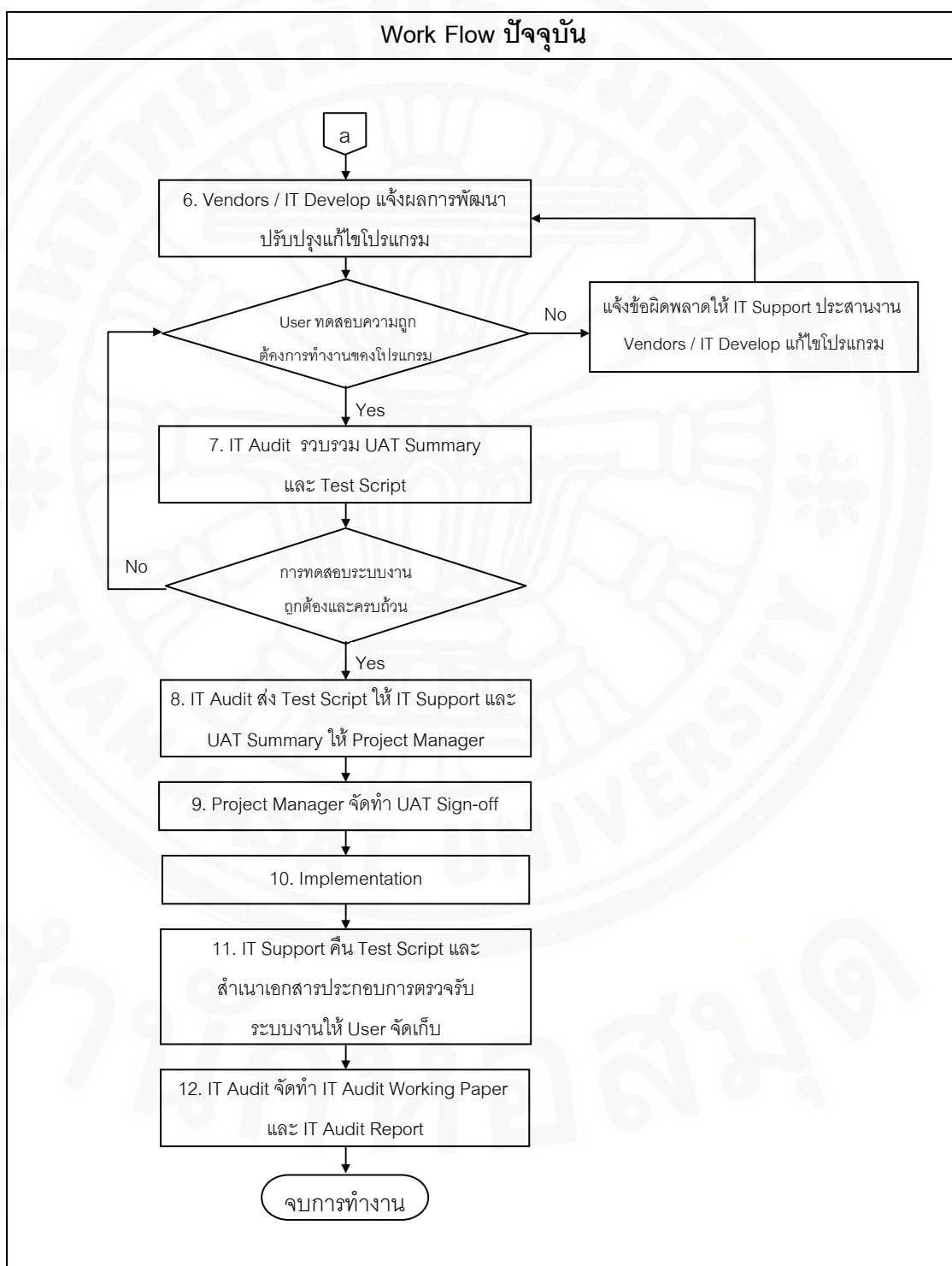
ภาพที่ 5.2

เปรียบเทียบ Work Flow ปัจจุบันและ Work Flow ตามแนวทางที่นำเสนอ
ของการตรวจรับระบบงาน กรณี Production Problem



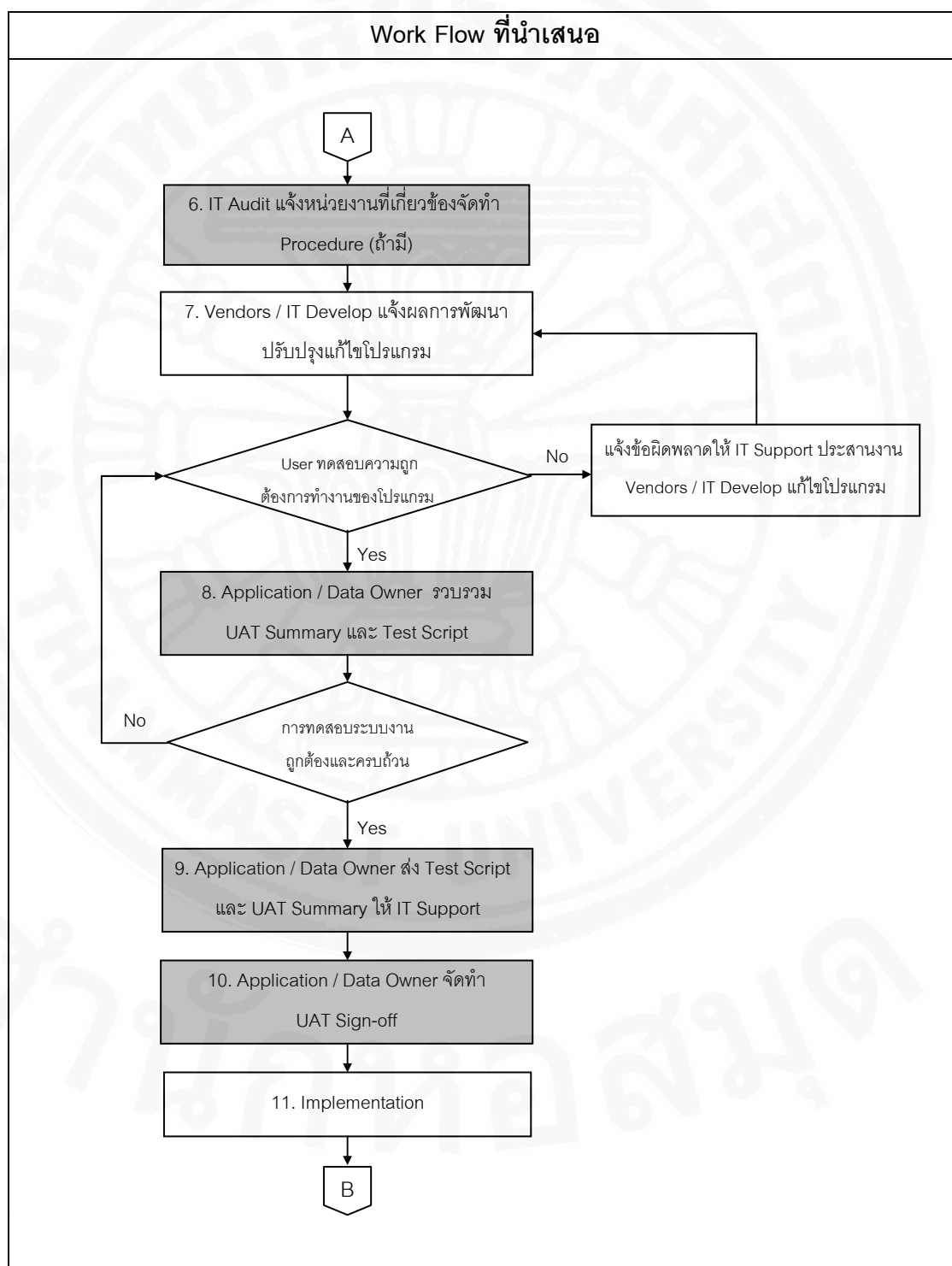
ภาพที่ 5.2 (ต่อ)

เปรียบเทียบ Work Flow ปัจจุบันและ Work Flow ตามแนวทางที่นำเสนอ
ของการตรวจรับระบบงาน กรณี Production Problem



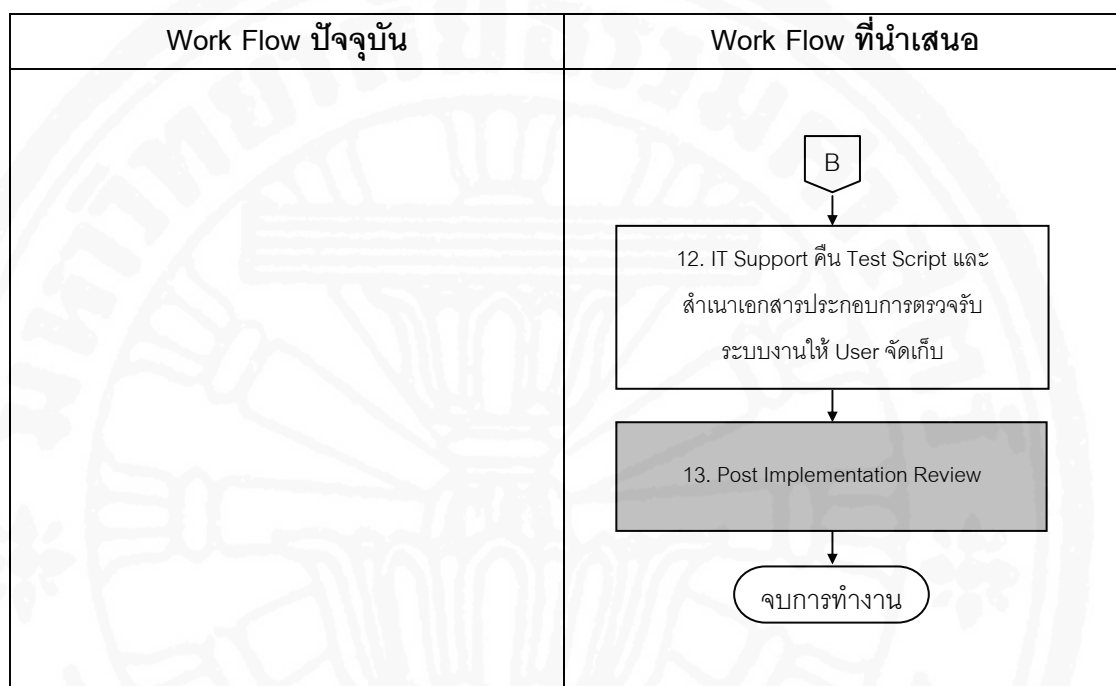
ภาพที่ 5.2 (ต่อ)

เปรียบเทียบ Work Flow ปัจจุบันและ Work Flow ตามแนวทางที่นำเสนอ
ของการตรวจรับระบบงาน กรณี Production Problem



ภาพที่ 5.2 (ต่อ)

เปรียบเทียบ Work Flow ปัจจุบันและ Work Flow ตามแนวทางที่นำเสนอ
ของการตรวจรับระบบงาน กรณี Production Problem



5.2 ข้อเสนอแนะเกี่ยวกับงานวิจัย

1. แนวทางปรับปรุงที่นำเสนอในครั้งนี้นี้ยังไม่มีนำไปใช้ปฏิบัติงานจริง เนื่องจากข้อจำกัดด้านระยะเวลาของการทำงานวิจัย จึงยังไม่สามารถประเมินผลสำเร็จของแนวทางปรับปรุงที่นำเสนอได้ ดังนั้น ในการศึกษาวิจัยต่อไปควรมีการศึกษาถึงการประเมินความสำเร็จในการปฏิบัติงานตามแนวทางที่นำเสนอ

2. การเลือกมาตรฐาน COBIT มาประยุกต์ใช้ เพื่อจัดปัญหาและอุปสรรคของกระบวนการตรวจสอบระบบสารสนเทศ เฉพาะการตรวจรับระบบงานในส่วนของการบริหารโครงการเทคโนโลยีสารสนเทศ (IT Project Management) ขององค์กรที่นำมาเป็นกรณีศึกษามีอยู่ในปัจจุบันให้เหมาะสมนั้น อาจใช้มาตรฐานอื่นๆ เพื่อใช้ในการศึกษาได้ เช่น มาตรฐาน ISO / IEC17799 หรือ ITIL เป็นต้น

3. ผลของการศึกษาค้างนี้ ทำการศึกษาเฉพาะองค์กรที่นำมาเป็นกรณีศึกษาเพียงองค์กรเดียว ดังนั้น จึงสามารถใช้จัดปัญหาและอุปสรรคของกระบวนการตรวจรับระบบงานในส่วนของการบริหารโครงการเทคโนโลยีสารสนเทศ (IT Project Management) ได้เฉพาะองค์กรนี้เท่านั้น

4. การศึกษาค้างนี้มีข้อจำกัดในช่วงเวลาที่ใช้ในการศึกษา ทำให้การเก็บรวบรวมข้อมูล และการนำข้อมูลมาวิเคราะห์เพื่อสรุปผล อาจทำได้ไม่สมบูรณ์เท่าที่ควร รวมทั้งเป็นผลการศึกษาเฉพาะการตรวจรับระบบงานในส่วนของการบริหารโครงการเทคโนโลยีสารสนเทศ (IT Project Management) เท่านั้น ไม่ครอบคลุมงานด้านการตรวจสอบระบบสารสนเทศทั้งหมด

5. การนำมาตรฐาน COBIT มาประยุกต์ใช้กับงานตรวจสอบระบบสารสนเทศนั้น ควรนำไปประยุกต์ใช้กับทุกงานในหน้าที่ความรับผิดชอบของส่วนตรวจสอบเทคโนโลยีสารสนเทศ ซึ่งจากองค์กรที่นำมาเป็นกรณีศึกษา นี้ หน้าที่ความรับผิดชอบอื่นที่ผู้วิจัยเห็นว่าควรมีการศึกษาเพิ่มเติมเป็นงานวิจัยต่อเนื่อง ได้แก่ การจัดหา / จัดจ้างบริษัทภายนอก (Outsource) เพื่อพัฒนาโปรแกรมระบบงาน, การตรวจสอบการปฏิบัติงานของหน่วยงานเทคโนโลยีสารสนเทศ เป็นต้น