

# 22

---

**การตรวจสอบระบบการควบคุม**

## การตรวจสอบระบบการควบคุม

### 1. การตรวจสอบทั่วไป

#### 1.1 วัตถุประสงค์และขอบเขตของการตรวจสอบ

ผู้ตรวจสอบจะต้องใช้วิธีการตรวจสอบที่เหมาะสม เพื่อให้ได้หลักฐานและความมั่นใจว่าธนาคารพาณิชย์ได้ปฏิบัติตามระบบการควบคุมภายในอย่างเหมาะสมและต่อเนื่องตลอดงวดการบัญชีที่ตรวจสอบ การตรวจสอบเช่นนี้เรียกว่า การตรวจสอบระบบการควบคุม (Functional Tests หรือ Compliance Tests หรือ Procedural Tests)

โดยปกติผู้ตรวจสอบจะทำการตรวจสอบระบบการควบคุมภายหลังจากที่ประเมินคำตอบจากแบบสอบถามแล้วว่าสามารถให้ความเชื่อถือต่อระบบการควบคุมนั้นได้ ทั้งนี้เพื่อลดขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Tests) ลง อย่างไรก็ตามผู้ตรวจสอบอาจไม่ทำการตรวจสอบระบบการควบคุมก็ได้ หากพิจารณาเห็นว่า การขยายขอบเขตการตรวจสอบความถูกต้องของรายการทางการเงินจะช่วยให้คำตอบหรือยืนยันการปฏิบัติตามระบบการควบคุมภายในได้ด้วยเป็นอย่างดี

ผู้ตรวจสอบมักจะเข้มงวดและเชื่อถือการปฏิบัติตามระเบียบข้อบังคับ หรือความมีกฎเกณฑ์การควบคุม (Disciplines) มากกว่าการควบคุมขั้นพื้นฐาน (Basic Controls) เพราะหากธนาคารมีระเบียบข้อบังคับการควบคุมภายในใช้อยู่ ก็เป็นหลักประกันประการหนึ่งว่าธนาคารได้เอาใจใส่เข้มงวดการควบคุมภายใน ผู้ตรวจสอบจึงควรให้ความสนใจและตรวจสอบกฎเกณฑ์การควบคุมเป็นอันดับแรก

#### 1.2 การจัดทำเอกสารประกอบการตรวจสอบ

ผู้ตรวจสอบจะต้องทำบันทึกการตรวจสอบเพื่อรวบรวมและพิจารณาการปฏิบัติตามระบบการควบคุมของธนาคาร ขั้นตอนและบันทึกการตรวจสอบระบบการควบคุม อย่างน้อยควรจะมีดังนี้

- 1) รายละเอียดวิธีการตรวจสอบ
- 2) การอ้างอิงแสดงความสัมพันธ์ระหว่างการตรวจสอบแต่ละขั้นกับคำถามในแบบสอบถาม เพื่อความมั่นใจว่าได้ตรวจสอบระบบการควบคุมครบถ้วนและได้ตรวจสอบตรงต่อการควบคุม
- 3) กำหนดระดับการตรวจสอบ
- 4) ช่วงเวลาของข้อมูลที่ทำกรตรวจสอบ
- 5) หลักฐานที่ได้ตรวจสอบ
- 6) รายละเอียดของข้อขัดข้อง (Breakdown) หรือข้อนำสังเกตที่พบระหว่างการตรวจสอบและสาเหตุ
- 7) วันที่ตรวจสอบแล้วเสร็จแต่ละขั้นตอน และลายมือชื่อผู้ตรวจสอบ

กระดาดำทำกรสำหรับบันทึกการตรวจสอบระบบการควบคุมมีรายละเอียดปรากฏตามแผนภาพที่ 22.1 ส่วนวิธีการตรวจสอบที่เป็นมาตรฐานสำหรับการตรวจสอบระบบการควบคุมปรากฏตามภาคผนวก ก.

### 1.3 ประเภทการตรวจสอบ

การตรวจสอบระบบการควบคุมประกอบด้วยกรตรวจสอบ 2 ประเภทร่วมกัน ดังนี้

#### 1.3.1 การตรวจสอบหลักฐาน (Examination of Evidence)

คือ การตรวจสอบการบันทึกการรายการ เอกสาร และรายงานกระทบยอดว่าได้ปฏิบัติตามระเบียบข้อบังคับ หรือมีการควบคุมที่ดีหรือไม่ เช่น มีการลงนามกำกับรายการและเอกสารที่สำคัญโดยผู้มีอำนาจหน้าจ็อย่างครบถ้วน

แผ่นที่ \_\_\_\_\_  
จากจำนวน \_\_\_\_\_

กระดาดำทำกร  
บันทึกการตรวจสอบระบบการควบคุม

ธนาคาร \_\_\_\_\_  
การตรวจสอบเพียงวันที่ \_\_\_\_\_

การควบคุม \_\_\_\_\_

Ref. แบบ สอบถาม	รายละเอียดการตรวจสอบ หรือ เหตุผลที่ไม่ตรวจสอบ	ระดับ การ ตรวจสอบ (ร้อยละ)	ช่วงเวลา ของข้อมูล ที่ตรวจสอบ	หลักฐาน การตรวจสอบ (Ref. กระดาดำ ทำกร)	ข้อสังเกต	ผู้ตรวจสอบ และวันที่ ตรวจสอบ

แผนภาพที่ 22.1 กระดาดำทำกร "บันทึกการตรวจสอบระบบการควบคุม"

### 1.3.2 การสอบทานการปฏิบัติงาน (Reperformance)

คือ การทดสอบปฏิบัติงานซ้ำรอยของพนักงานธนาคาร เช่น คำนวณวิเคราะห์และกระทบยอด เป็นต้น หากพบข้อผิดพลาดหรือข้อบกพร่องจากการสอบทานการปฏิบัติงาน ผู้ตรวจสอบก็ไม่อาจให้ความเชื่อถือต่อการตรวจสอบหลักฐานที่ปฏิบัติไปแล้วได้

การควบคุมใดที่ผู้ตรวจสอบไม่อาจใช้วิธีการตรวจสอบโดยการตรวจสอบหลักฐาน และสอบทานการปฏิบัติงานได้ ผู้ตรวจสอบอาจใช้วิธีการสอบถามหรือสังเกตการณ์การปฏิบัติงานจริง (Observation) อย่างไรก็ตามวิธีการนี้มีข้อบกพร่อง เพราะไม่อาจวางใจได้ว่าในช่วงเวลาอื่นนอกเหนือจากเวลาที่สังเกตการณ์ ได้มีการปฏิบัติตามระบบการควบคุม หรือมีการควบคุมที่ดีหรือไม่ กรณีเช่นนี้ผู้ตรวจสอบอาจใช้วิธีขอคำยืนยันจากธนาคารก็ได้

## 2. การตรวจสอบในระบบคอมพิวเตอร์

### 2.1 ลักษณะของการตรวจสอบ

การตรวจสอบระบบการควบคุมในระบบคอมพิวเตอร์ มีวัตถุประสงค์เช่นเดียวกับการตรวจสอบในระบบเดิมที่มีได้ใช้คอมพิวเตอร์ แต่โดยที่การควบคุมในระบบคอมพิวเตอร์มีความแตกต่างไปจากเดิม เทคนิคและขอบเขตการตรวจสอบระบบการควบคุมจึงแตกต่างกันด้วย

ก่อนที่จะตัดสินใจตรวจสอบระบบการควบคุมในระบบคอมพิวเตอร์ ผู้ตรวจสอบพึงระลึกว่ามีวิธีการตรวจสอบอย่างอื่นอย่างน้อย 2 วิธี ซึ่งผู้ตรวจสอบอาจเลือกวิธีใดวิธีหนึ่งมาใช้ก็ได้ และได้ผลการตรวจสอบระบบการควบคุมอย่างมีประสิทธิภาพด้วยเช่นกัน หรือไม่จำเป็นต้องตรวจสอบระบบการควบคุมก็ได้ คือ

1) การใช้โปรแกรมคอมพิวเตอร์ (Computer Program) ช่วยในการตรวจสอบ ทบทวน และแยกประเภทข้อมูลที่ประมวลผลจำนวนมาก การใช้โปรแกรมคอมพิวเตอร์ช่วยตรวจสอบ เป็นการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) ที่มีประสิทธิภาพมากเช่นกัน

2) การเพิ่มระดับและขยายการทดสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) แทนการตรวจสอบระบบการควบคุมในเรื่องของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ผู้ตรวจสอบอาจจำกัดการตรวจสอบความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ได้ โดยการเพิ่มการตรวจสอบระบบและตัวโปรแกรม หรือเมื่อได้พิจารณาแล้วว่าได้มีการควบคุมทางด้านผู้ใช้ (User Controls) อย่างได้ผล

## 2.2 เทคนิคการตรวจสอบ

เทคนิคการตรวจสอบจะแยกกล่าวตามหัวข้อการควบคุมต่อไปนี้

- กฎเกณฑ์การควบคุม (Disciplines)
- การควบคุมทางด้านผู้ใช้ (User Controls)
- การควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls)
- การควบคุมโดยขั้นตอนการทำงานของโปรแกรม (Programmed Procedures)

### 2.2.1 การตรวจสอบกฎเกณฑ์การควบคุม

โดยที่กล่าวมาแล้วในบทที่ 3 ว่ากฎเกณฑ์การควบคุมประกอบด้วย การกำกับ (Supervisory Controls) การแบ่งแยกหน้าที่ (Segregation of Duties) และการควบคุมทรัพย์สิน (Custodial Controls) การตรวจสอบระบบการควบคุมทั้ง 3 แบบทำได้ดังนี้

#### 1) การกำกับ

การตรวจสอบว่าได้มีการกำกับ (Supervisory Controls) ใช้อยู่หรือไม่ วิธีที่สำคัญคือตรวจสอบจากหลักฐาน (Examination of Evidence) ได้แก่ การตรวจสอบการลงนามของผู้มีหน้าที่กำกับ เช่น ในการควบคุมทางด้านผู้ใช้ ได้มีการสอบสวนและลงลายมือชื่อกำกับรายการที่เครื่องไม่ยอมรับ (Rejection Reports) หรือรายการที่มีข้อสังเกตผิดปกติ (Exception Reports) หรือไม่ หรือการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ได้มีการลงลายมือชื่อโดยผู้มีอำนาจในแบบฟอร์มขอแก้ไขโปรแกรม (Program Change Form) หรือไม่ นอกจากนั้นยังตรวจสอบได้จากหลักฐานบันทึกโต้ตอบภายใน ซึ่งอาจจะระบุวิธีการหรือการอนุมัติให้ทำลายหรือยกเลิกรายการบันทึกหรือเอกสารที่ผิดพลาดหรือไม่น่าพอใจ ในกรณีให้เห็นสมควรผู้ตรวจสอบควรขอตรวจสอบเอกสารหลักฐานต่าง ๆ ที่ผ่านมือผู้มีอำนาจหน้าที่กำกับว่าครบถ้วนเพียงพอหรือไม่ เช่น ในการทดสอบโปรแกรมได้ส่งรายละเอียดของข้อมูลตัวอย่างที่ทำการทดสอบกับผลของการทดสอบให้ผู้มีอำนาจหน้าที่กำกับตรวจสอบโดยครบถ้วนหรือไม่ ผู้ตรวจสอบควรเข้าไปสังเกตการณ์วิธีการควบคุมรายการหรือข้อมูลขณะประมวลผล และการจัดทำรายงานต่าง ๆ ในขณะใดขณะหนึ่งด้วย

การตรวจสอบการกำกับโดยใช้วิธีสอบทานการปฏิบัติงาน (Reperformance) อาจไม่ ได้ผลเต็มที่นัก หรือไม่อาจทำได้เนื่องจากผู้ตรวจสอบไม่อาจที่จะรู้หรือไม่มีความสามารถในการควบคุมแบบนี้ หรือ อาจเป็นเพราะการกำกับบางอย่างขึ้นอยู่กับการตัดสินใจของผู้มีอำนาจหน้าที่กำกับ จึงไม่ปรากฏหลักฐานให้สอบ ทานการปฏิบัติงานได้

การตรวจสอบการกำกับควรใช้ข้อมูลเดียวกันกับการตรวจสอบการควบคุมแบบอื่น ๆ เพราะจะให้ประสิทธิภาพในการตรวจสอบเป็นอย่างมาก ข้อบกพร่องที่พบจากการตรวจสอบการควบคุมอื่น ๆ ใน ข้อมูลหรือหลักฐานการตรวจสอบเดียวกัน จะยืนยันให้เห็นว่าการกำกับไม่มีประสิทธิภาพเพียงพอ

## 2) การแบ่งแยกหน้าที่และการควบคุมทรัพย์สิน

การตรวจสอบการแบ่งแยกหน้าที่และการควบคุมทรัพย์สิน ทำได้โดยการตรวจสอบลายมือชื่อและการลงนามกำกับในเอกสารและรายการ ตลอดจนใช้วิธีสังเกตการณ์และขอคำยืนยันยอด โดยปกติแล้วไม่อาจใช้วิธีการสอบทานการปฏิบัติงานเพื่อตรวจสอบการควบคุมทั้ง 2 ประเภทได้อย่างได้ผล

ตัวอย่างการตรวจสอบการควบคุมทางด้านผู้ใช้ (User Controls) ได้แก่ การตรวจสอบการลงนามและลายมือชื่อกำกับรายงานการกระทบยอดและรายงานข้อผิดพลาด เพื่อพิสูจน์ว่าผู้ที่ทำหน้าที่ควบคุมทางด้านผู้ใช้มิใช่บุคคลเดียวกันกับผู้ปฏิบัติการคอมพิวเตอร์ ผู้ตรวจสอบควรพิสูจน์การแบ่งแยกหน้าที่ทั้งในด้านการออกแบบระบบงาน การจัดทำโปรแกรม และการปฏิบัติการคอมพิวเตอร์ ผู้ตรวจสอบควรเข้าไปสังเกตการณ์การปฏิบัติงานในแผนกต่าง ๆ ที่เกี่ยวข้อง เพื่อตรวจสอบว่าได้มีการปฏิบัติงานโดยอิสระจากกันจริง

ในการควบคุมทรัพย์สินซึ่งเป็นส่วนหนึ่งของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ผู้ตรวจสอบจะต้องตรวจสอบดูว่าระเบียบคำสั่งที่ใช้บังคับแก่พนักงานผู้เกี่ยวข้องมีความเหมาะสมเพียงใด และควรเข้าไปสังเกตการณ์มาตรการรักษาความปลอดภัยว่าได้มีการปฏิบัติตามหรือไม่ นอกจากนั้นควรตรวจสอบบุคคลผู้ปฏิบัติหน้าที่ว่าตรงกับคำสั่งแต่งตั้งหรือไม่ โดยเฉพาะอย่างยิ่งในส่วนของการแบ่งแยกหน้าที่ เช่น ระหว่างผู้พัฒนาระบบงานกับผู้รักษาระบบงาน ผู้ปฏิบัติการคอมพิวเตอร์กับผู้เก็บรักษาแฟ้มข้อมูล เป็นต้น ผู้ตรวจสอบควรตรวจสอบผังการจัดองค์การ (Organization Charts) ของศูนย์คอมพิวเตอร์ และรายละเอียดตำแหน่งงาน (Job Description) เพื่อพิสูจน์ว่าได้มีการแบ่งแยกหน้าที่อย่างชัดเจนทั้งในระหว่างการปฏิบัติงานปกติ และการปฏิบัติงานนอกเวลาทำการ นอกจากนั้นควรพิสูจน์ข้อเท็จจริงดังกล่าวโดยการเข้าไปสังเกตการณ์ศูนย์คอมพิวเตอร์และห้องปฏิบัติการขณะใดขณะหนึ่งด้วย และควรตรวจสอบตารางการปฏิบัติงาน (Work Schedules) รายงานเวลาใช้คอมพิวเตอร์ (Time Report) รายละเอียดการปฏิบัติงานของผู้ปฏิบัติการคอมพิวเตอร์ที่พิมพ์โดยเครื่อง (Operator Logs) ตลอดจนเอกสารอื่น ๆ ในลักษณะที่กล่าวเพื่อตรวจสอบว่าการปฏิบัติงานจริงสอดคล้องกับวิธีการที่กำหนดไว้

### 2.2.2 การตรวจสอบการควบคุมทางด้านผู้ใช้

การตรวจสอบระบบการควบคุมทางด้านผู้ใช้ โดยปกติสามารถใช้ได้ทั้งวิธีตรวจสอบหลักฐานและวิธีสอบทานการปฏิบัติงาน ผู้ตรวจสอบจะไม่ประสบปัญหายุ่งยากในการตรวจสอบด้านนี้สัก เพราะเอกสารหลักฐานเกี่ยวกับการควบคุมสามารถมองเห็นได้ อย่างไรก็ตามการตรวจสอบการปฏิบัติงานที่มีปริมาณสูงนั้น หากใช้วิธีสอบทานการปฏิบัติงานก็ไม่สู้จะเหมาะสม

### 2.2.3 การตรวจสอบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์

ผู้ตรวจสอบจะต้องตรวจสอบระบบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ซึ่งปกติจะเป็นการตรวจสอบด้วยมือ (Manually) และสุ่มตัวอย่างทดสอบการทำงานของโปรแกรมระบบคอมพิวเตอร์ (System Software Procedures) ผู้ตรวจสอบจะต้องเลือกและตัดสินใจว่าจะเลือกใช้โปรแกรมระบบโปรแกรมใด และจำนวนมากน้อยเพียงไร เพื่อทำการทดสอบและยืนยันการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ โดยเฉพาะการควบคุมการพัฒนาและใช้โปรแกรมระบบและการรักษาความปลอดภัยแก่โปรแกรมระบบ

การตรวจสอบระบบการควบคุมในส่วนของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์โดยการตรวจสอบด้วยมือ ได้แก่ การตรวจสอบหลักฐานการสอบทานการปฏิบัติงานและการสังเกตการณ์ การตรวจสอบส่วนใหญ่คล้ายคลึงกับการตรวจสอบทางด้านผู้ใช้ ได้แก่ การตรวจสอบจากรายงานคอมพิวเตอร์ และการตรวจสอบบางด้านจะคล้ายคลึงกับการตรวจสอบในระบบที่มีได้ใช้คอมพิวเตอร์ เช่น การตรวจสอบการควบคุมการแก้ไขเปลี่ยนแปลงโปรแกรม เป็นต้น การตรวจสอบหลักฐานเป็นการตรวจสอบที่สำคัญ เพราะไม่อาจใช้วิธีการสอบทานการปฏิบัติงานได้เสมอไป ฉะนั้นผู้ตรวจสอบจึงควรตรวจสอบเอกสารประกอบระบบงาน (System Descriptions) และคู่มือปฏิบัติการคอมพิวเตอร์ (Operating Instructions) อย่างถี่ถ้วนถึงความเพียงพอและความสมบูรณ์ของเอกสารดังกล่าว

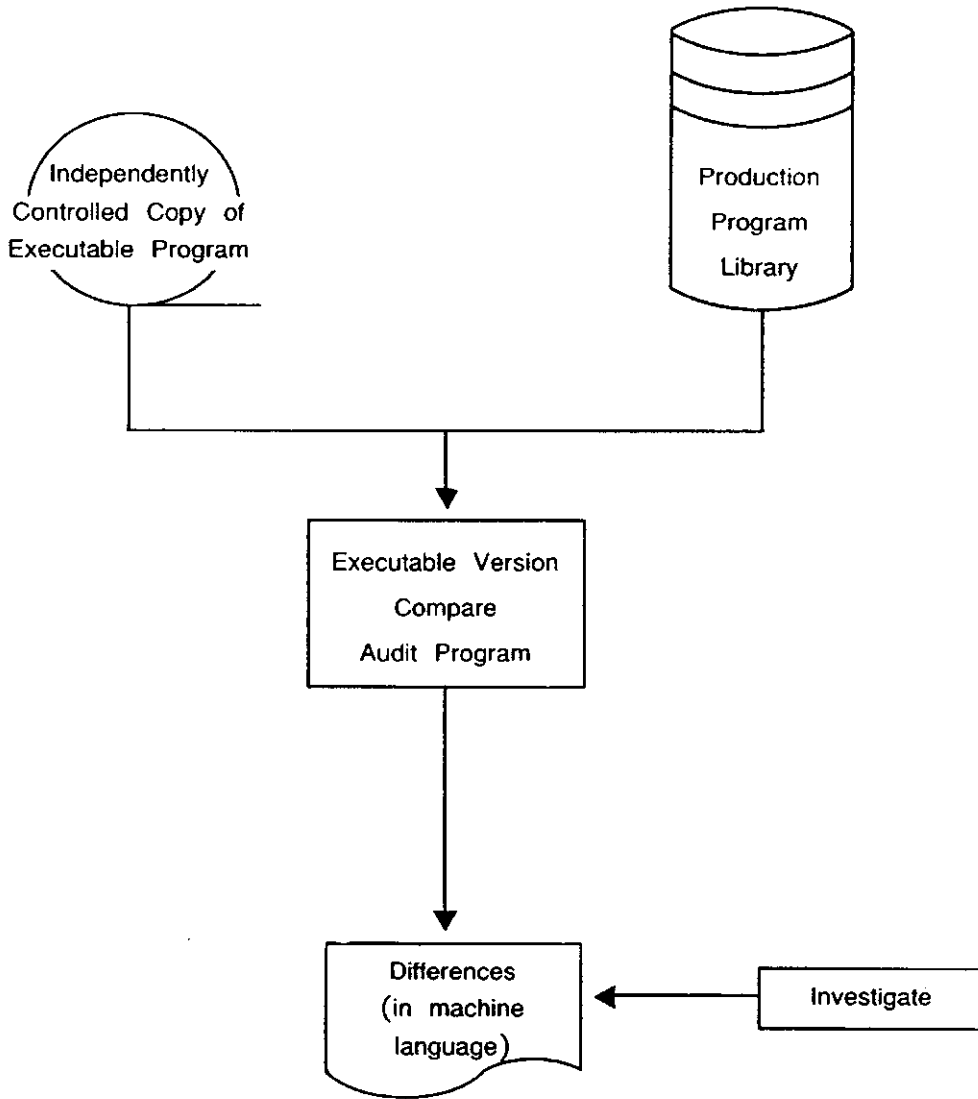
การตรวจสอบโปรแกรมของระบบมีวิธีการตรวจสอบที่สามารถนำมาใช้ได้หลายวิธี ขึ้นอยู่กับลักษณะของการปฏิบัติงานที่จะตรวจสอบ ตัวอย่าง เช่น การตรวจสอบ Cataloguing Procedures ก็อาจใช้ข้อมูลตัวอย่างทดสอบ (Audit Test Data) หรือใช้วิธีวิเคราะห์รหัสโปรแกรม (Program Code Analysis) เพื่อพิสูจน์ว่าโปรแกรมใหม่ ๆ หรือโปรแกรมที่แก้ไขใหม่ได้ Catalogued เป็นที่เรียบร้อยและน่าพอใจหรือไม่ นอกจากนี้ที่กล่าวแล้วยังอาจพัฒนาโปรแกรมคอมพิวเตอร์ (Computer Program) ขึ้นมาช่วยในการตรวจสอบโปรแกรมของระบบได้ ดังนี้

- 1) โปรแกรมที่ใช้ตรวจสอบว่าได้มีการเปลี่ยนแปลงแก้ไขโปรแกรมของระบบโดยได้รับอนุญาต หรือโดยถูกต้องหรือไม่ ทั้งนี้โดยการนำโปรแกรมของระบบที่ใช้ปฏิบัติงานขณะนั้นมาเปรียบเทียบกับโปรแกรมสำเนาที่เก็บไว้ภายใต้การควบคุมอย่างอิสระ แล้วรายงานข้อแตกต่างที่เกิดขึ้น (แผนภาพที่ 22.2 และ 22.3)
- 2) โปรแกรมที่ใช้วิเคราะห์และรายงานข้อมูลที่เก็บไว้ใน System Log ซึ่งผู้ตรวจสอบจะนำมาเปรียบเทียบกับรายงานที่ธนาคารพาณิชย์จัดทำเพื่อหาข้อแตกต่างได้ (แผนภาพที่ 22.4)

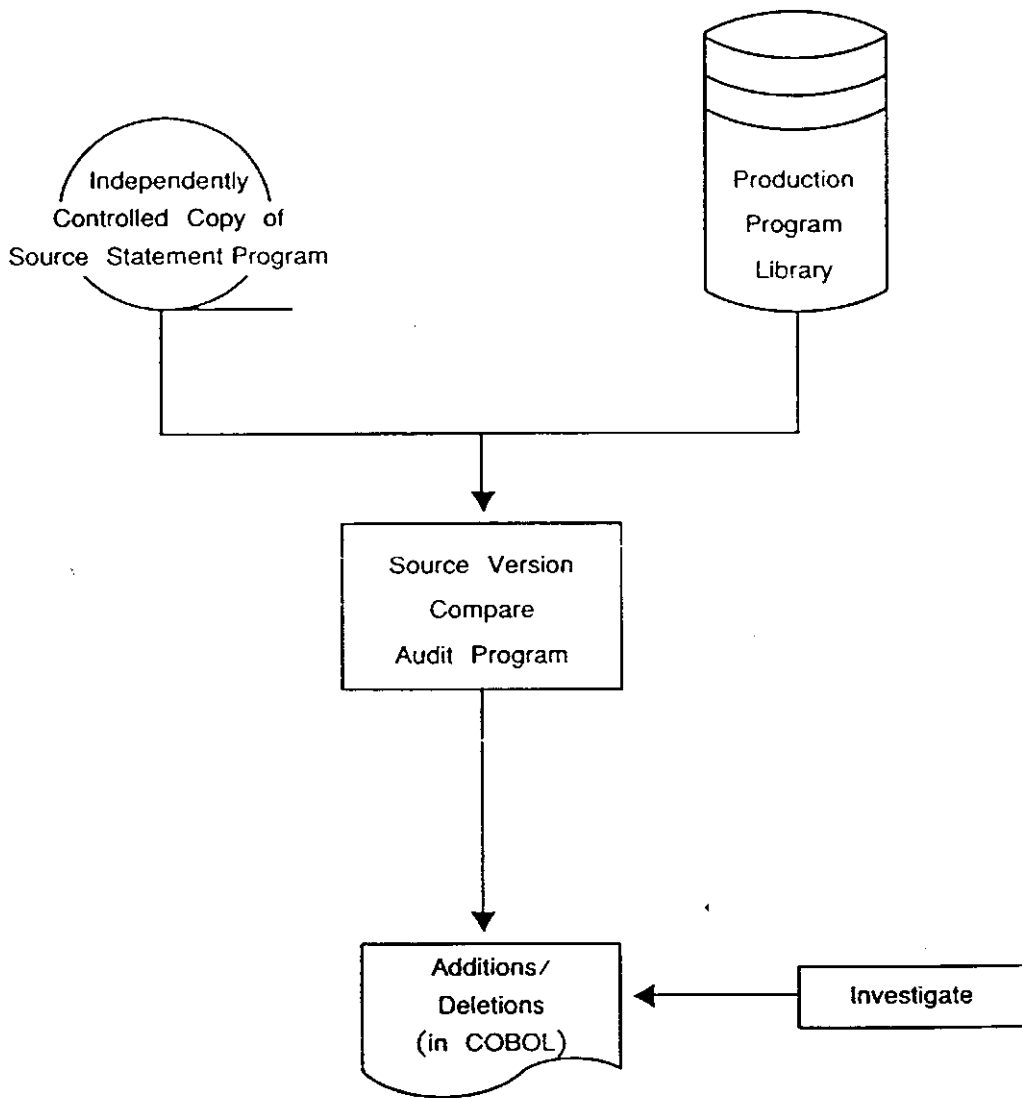
การทดสอบโปรแกรมของระบบที่ใช้ในการคุ้มครองรหัสลับเฉพาะผู้มีหน้าที่ในการปฏิบัติการ (Password Protection) อาจทำได้โดยผู้ตรวจสอบทดลองใช้รหัสลับที่มีได้รับอนุญาตผ่านเข้าไปทางเครื่องเทอร์มินอล อย่างไรก็ตามก่อนที่จะใช้เทคนิคใด ๆ ผู้ตรวจสอบพึงระมัดระวังผลกระทบที่มีต่อการประมวลผลด้วย

#### 2.2.4 การตรวจสอบขั้นตอนการทำงานของโปรแกรม

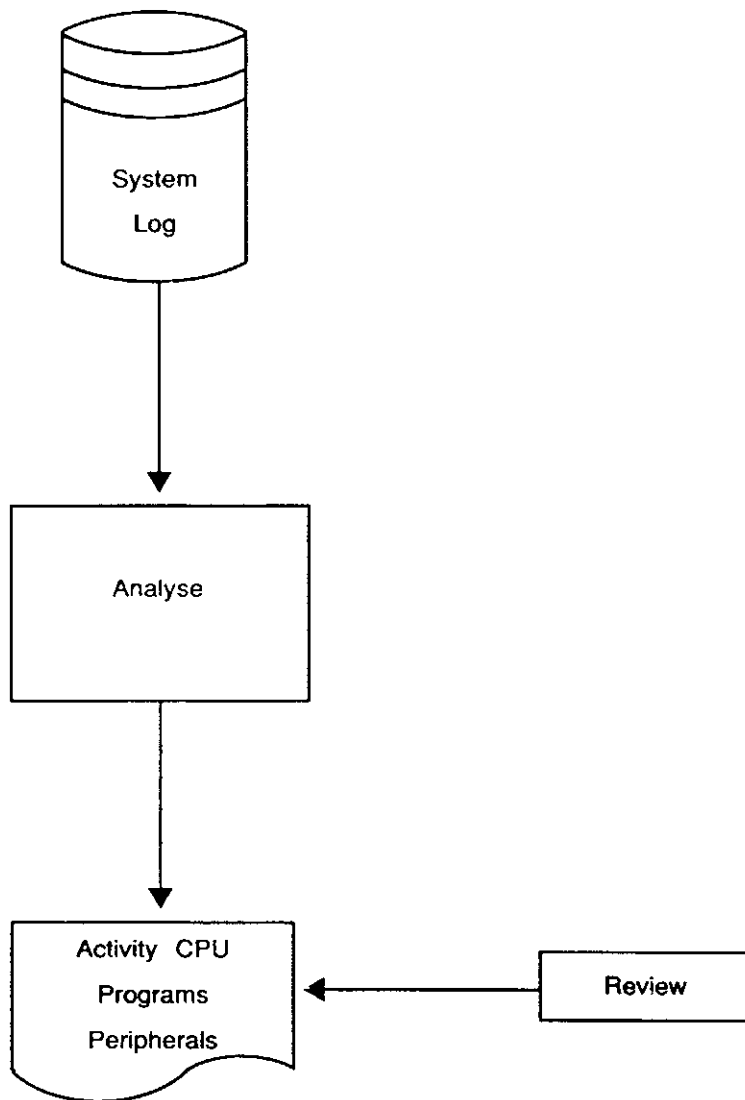
ในขณะที่ผู้ตรวจสอบดำเนินการตรวจสอบระบบการควบคุมในด้านการควบคุมการพัฒนาและใช้ระบบงาน (Implementation Controls) โดยวิธีสอบทานการปฏิบัติงาน (Reperformance) นั้น ก็เท่ากับเป็นการตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ด้วยส่วนหนึ่ง นอกจากนั้นการตรวจสอบขั้นตอนการทำงานของโปรแกรมายังแทรกอยู่ส่วนหนึ่งของการตรวจสอบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ นั่นคือ การตรวจสอบว่าได้มีการจัดสร้างและใช้ขั้นตอนของโปรแกรมอย่างเหมาะสม และโดยต่อเนื่อง อย่างไรก็ตามผู้ตรวจสอบก็ควรที่จะตรวจสอบขั้นตอนการทำงานของโปรแกรมโดยเฉพาะด้วยเพื่อความสมบูรณ์ของการตรวจสอบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ และเพื่อให้ได้หลักฐานว่าได้มีการควบคุมดังกล่าวโดยต่อเนื่อง



แผนภาพที่ 22.2 การตรวจสอบโปรแกรมปฏิบัติงาน (Executable Program)



แผนภาพที่ 22.3 การตรวจสอบโปรแกรมจากต้นฉบับ (Source Statement Programs)



แผนภาพที่ 22.4 การวิเคราะห์ System Log

การตรวจสอบขั้นตอนการทำงานของโปรแกรม ปกติจะใช้วิธีสอบทานการปฏิบัติงาน เพราะเป็นการยากหรือไม่เหมาะสมที่จะตรวจสอบจากหลักฐาน อย่างไรก็ตามหลักฐานบางอย่าง เช่น รายงานข้อผิดพลาดจากรายการที่ประมวลผลก็อาจใช้เป็นหลักฐานเบื้องต้นยืนยันว่าการควบคุมโดยขั้นตอนการปฏิบัติงานของโปรแกรมได้มีใช้อยู่ และโดยต่อเนื่องหรือไม่ การตรวจสอบจากหลักฐานนี้ปกติจะกระทำเป็นส่วนหนึ่งของการตรวจสอบการควบคุมทางด้านผู้ใช้ (User Controls)

เทคนิคสำคัญของการตรวจสอบขั้นตอนการทำงานของโปรแกรม ประกอบด้วย การทดสอบด้วยมือ (Manual Tests) การใช้ข้อมูลตัวอย่างตรวจสอบ (Audit Test Data) การวิเคราะห์รหัสโปรแกรม (Program Code Analysis) และการใช้โปรแกรมตรวจสอบ (Computer Audit Programs) การเลือกที่จะใช้เทคนิคใดก็ตามขึ้นอยู่กับว่าจะมีหลักฐานที่มองเห็นได้ให้ตรวจสอบหรือไม่

### 1) การขาดหลักฐานที่มองเห็นได้

โดยปกติรายงานที่คอมพิวเตอร์พิมพ์ออกมาให้มันจะไม่มีรายละเอียด ซึ่งเป็นลักษณะอย่างหนึ่งของการประมวลผลด้วยคอมพิวเตอร์ ด้วยเหตุที่ขาดรายละเอียดหรือขาดรายงานบางอย่างไป ผู้ตรวจสอบจึงไม่อาจใช้วิธีการตรวจสอบหลักฐานในการตรวจสอบขั้นตอนการทำงานของโปรแกรมได้ ความยุ่งยากที่เกิดขึ้นมี 2 แบบ คือ แบบแรก คอมพิวเตอร์อาจจะพิมพ์ยอดรวมและยอดประกอบยอดรวม แต่มิได้ให้รายละเอียดประกอบส่วนแบบที่ 2 หลักฐานที่ได้ไม่แน่ชัดเพียงพอ เช่น กรณีที่คอมพิวเตอร์พิมพ์รายงานที่มีข้อสังเกต (Exception Reports) หรือรายงานเกี่ยวกับรายการที่เครื่องไม่ยอมรับ (Rejected Items) ผู้ตรวจสอบไม่อาจเชื่อมั่นได้ว่ารายการที่มีข้อสังเกตหรือที่คอมพิวเตอร์ไม่ยอมรับได้พิมพ์ออกมาโดยครบถ้วนหรือไม่ ข้อยุ่งยากทั้ง 2 แบบนี้เรียกว่า การตรวจสอบร่องรอยการตรวจสอบ อย่างไรก็ตามการขาดร่องรอยการตรวจสอบมิได้หมายความว่ามีความหมายว่ามิชอบหรือในระบบการควบคุม ผู้ตรวจสอบจำเป็นต้องเปลี่ยนแปลงเทคนิคการตรวจสอบให้สอดคล้องกับร่องรอยการตรวจสอบที่ขาดหายไปด้วย

### 2) การทดสอบด้วยมือ (Manual Tests)

การตรวจสอบขั้นตอนการทำงานของโปรแกรมโดยการทดสอบด้วยมือ สามารถทำได้ในกรณีที่หลักฐานมีปรากฏอย่างครบถ้วน เช่น รายการบัญชี (Statements) ของลูกหนี้ ได้แสดงรายละเอียดความเคลื่อนไหวทุกรายการ ซึ่งสามารถทำให้ทดสอบการผ่านบัญชีได้ เป็นต้น การทดสอบยังอาจทำได้โดยปฏิบัติงานด้วยมือซ้ำกับการทำงานด้วยขั้นตอนการทำงานของโปรแกรมแล้วเปรียบเทียบผลลัพธ์ที่ได้

ในกรณีที่หลักฐานมีปรากฏไม่ครบถ้วน ผู้ตรวจสอบสามารถที่จะสร้างหลักฐานเพื่อการตรวจสอบได้ด้วยวิธีต่อไปนี้

- ก. นำข้อมูลที่ประมวลผลแล้วมารวบรวมปรับปรุงใหม่ให้อยู่ในสภาพเดียวกับขณะที่ใช้ขั้นตอนการทำงานของโปรแกรมทำการประมวลผล
- ข. รวบรวมและตรวจสอบจากข้อมูลปัจจุบันก่อนที่จะทำการประมวลผลด้วยคอมพิวเตอร์ ตัวอย่าง เช่น ทดสอบยอดรวมของ Batches เป็นต้น

- ค. เลือกข้อมูลจำนวนหนึ่งจากข้อมูลทั้งหมดมาทำการประมวลผลด้วยมือต่างหาก แล้วเปรียบเทียบกับผลที่ได้จากการประมวลผลด้วยคอมพิวเตอร์
- ง. เลือกทดสอบเงื่อนไขของขั้นตอนการทำงานของโปรแกรม ซึ่งหากมีประสิทธิภาพเพียงพอและมีความเหมาะสมแล้ว จะรายงานข้อผิดพลาดที่ตรงตามเงื่อนไขนั้นออกมา เช่น ดึงเอกสารบางอย่างไว้ไม่ส่งเข้าไปประมวลผล หรือแก้ตัวเลขให้ผิดพลาด เป็นต้น ซึ่งขั้นตอนการทำงานของโปรแกรมหากล่าวจะต้องรายงานข้อผิดพลาดออกมา
- จ. ขอให้คอมพิวเตอร์พิมพ์รายงานพิเศษให้ในกรณีที่ไม่มีหลักฐานที่มองเห็นได้เลย และไม่สามารถใช้วิธีสร้างหลักฐานเพื่อการตรวจสอบอย่างใดอย่างหนึ่งได้ การทดสอบด้วยมือก็ไม่สามารถทำได้ จึงควรเปลี่ยนไปใช้วิธีการตรวจสอบอย่างอื่นแทน

### 3) การสร้างข้อมูลตัวอย่างทดสอบ (Audit Test Data)

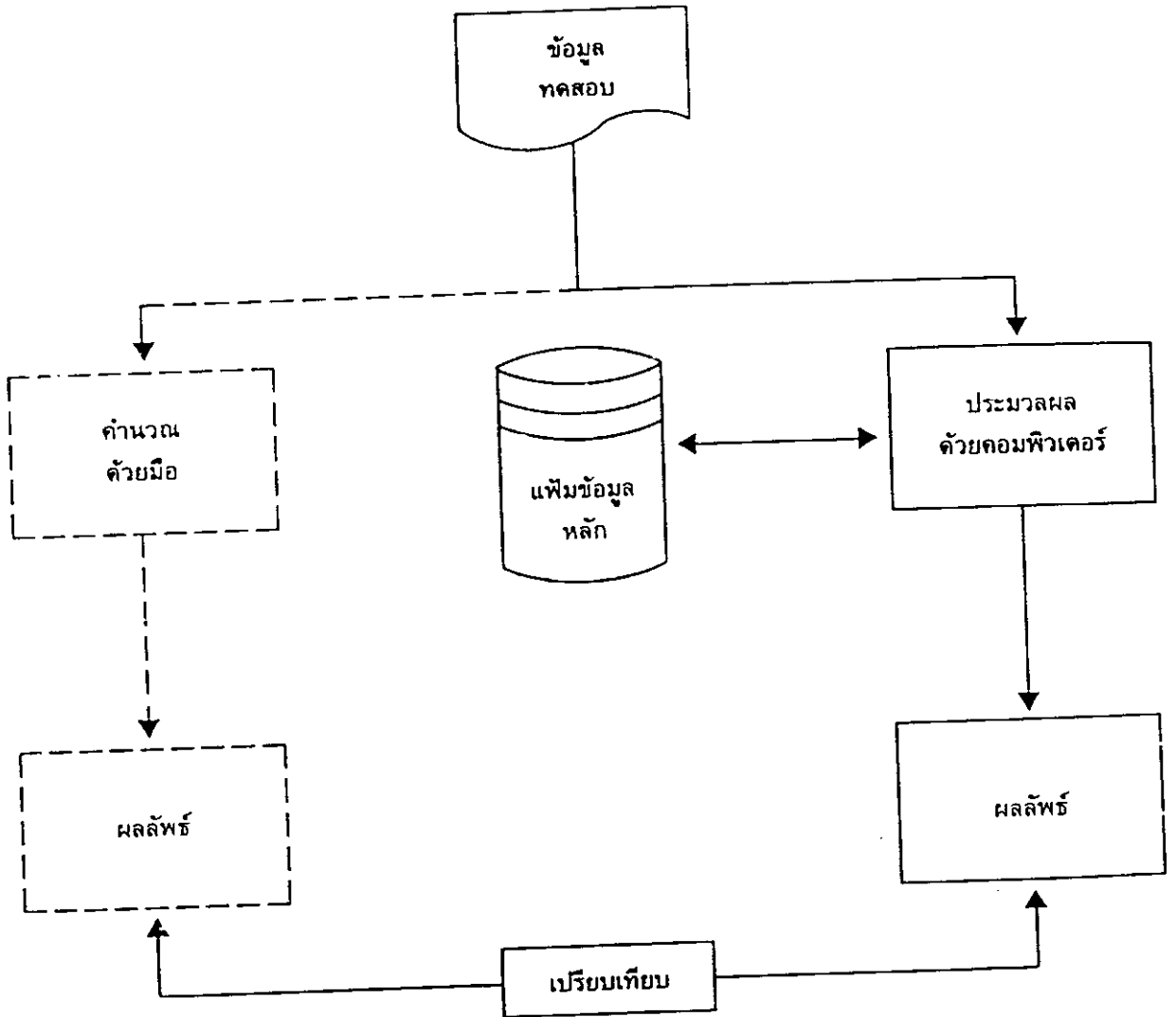
เป็นวิธีการสร้างข้อมูลขึ้นมาชุดหนึ่ง แล้วคำนวณผลลัพธ์ที่ได้ไว้ล่วงหน้า หลังจากนั้นส่งข้อมูลตัวอย่างดังกล่าวไปทดสอบกับขั้นตอนการทำงานของโปรแกรมเปรียบเทียบผลลัพธ์ที่ได้จากคอมพิวเตอร์กับผลลัพธ์ที่ทราบล่วงหน้านั้น เทคนิคนี้มีความเหมาะสมมากในกรณีที่ไม่มีหลักฐานที่มองเห็นได้ให้ตรวจสอบเลย และการทดสอบด้วยมือไม่ได้ผล

เทคนิคการใช้วิธีการสร้างข้อมูลตัวอย่างทดสอบปรากฏตามแผนภาพที่ 22.5

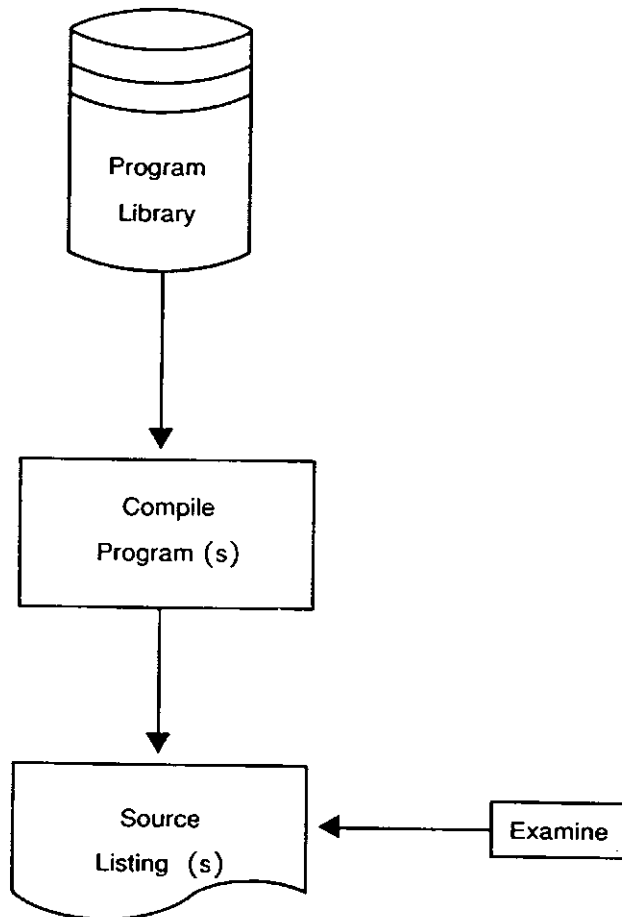
### 4) การวิเคราะห์รหัสโปรแกรม (Program Code Analysis)

หมายถึง การตรวจสอบโปรแกรมปฏิบัติการ (Operational Programs) จากโปรแกรมต้นฉบับที่คอมพิวเตอร์พิมพ์ออกมาให้ (Source Listing) เพื่อพิสูจน์ว่าขั้นตอนการทำงานของโปรแกรมที่เกี่ยวข้องได้ถูกใช้และให้รหัสอย่างถูกต้องหรือไม่ เทคนิคการตรวจสอบเช่นนี้ต้องการความรู้และทักษะทางด้านโปรแกรมอย่างสูง ผู้ตรวจสอบจะต้องตรวจสอบว่ารหัสที่ปรากฏในโปรแกรมต้นฉบับ (Source Listing) ไม่แตกต่างจากโปรแกรมปฏิบัติการที่ใช้ในการประมวลผลจริง เทคนิคการวิเคราะห์รหัสโปรแกรมปรากฏตามแผนภาพที่ 22.6





แผนภาพที่ 22.5 การสร้างข้อมูลตัวอย่างทดสอบ (Audit Test Data)



แผนภาพที่ 22.6 การวิเคราะห์รหัสโปรแกรม (Program Code Analysis)

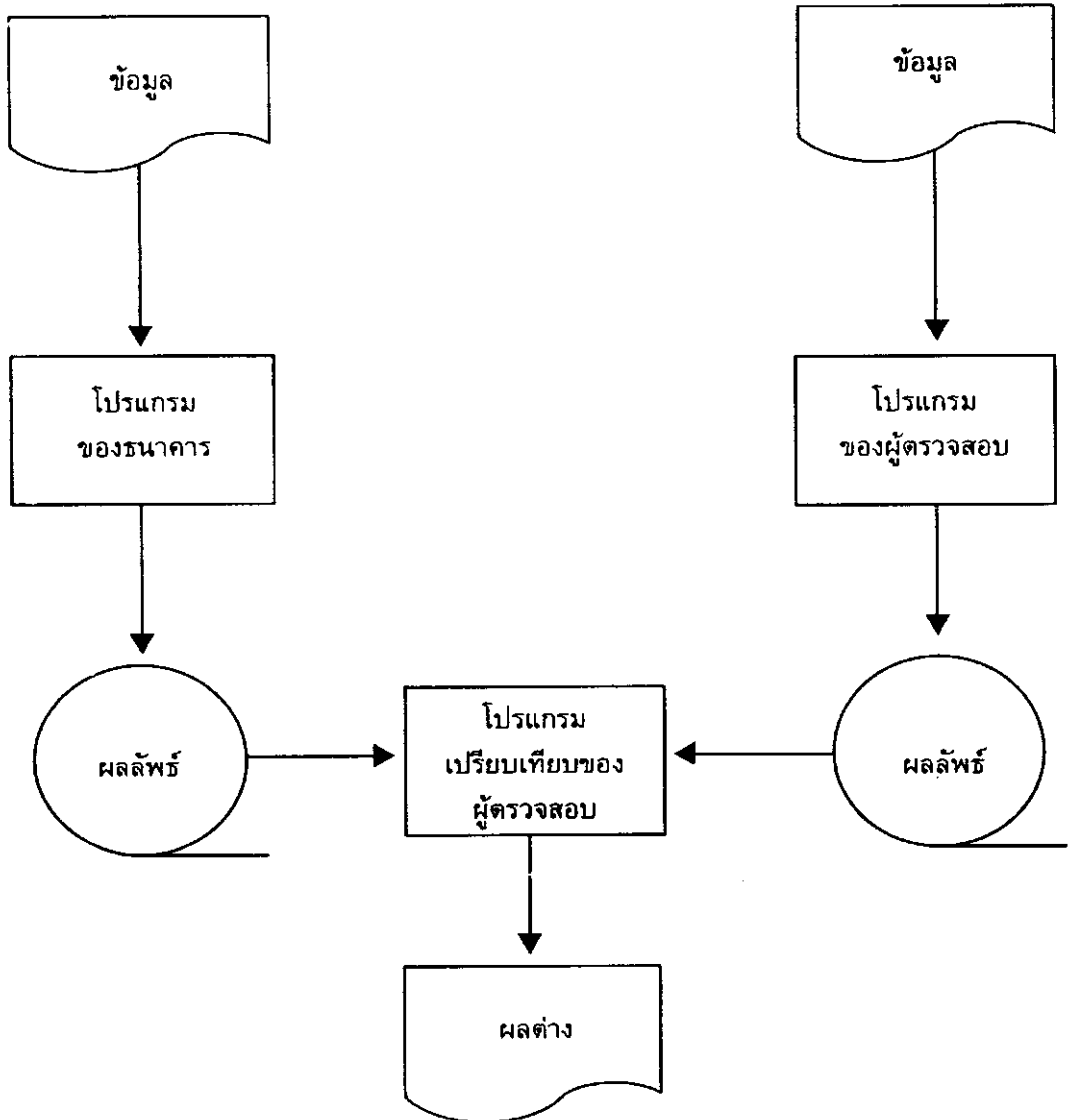
5) การตรวจสอบโดยใช้โปรแกรมคอมพิวเตอร์ (Computer Program)

โดยปกติผู้ตรวจสอบจะสร้างโปรแกรมคอมพิวเตอร์ของผู้ตรวจสอบขึ้นมา เพื่อช่วยในการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) แต่ก็อาจสร้างโปรแกรมขึ้นมาเพื่อช่วยในการตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ซึ่งเรียกว่าการทดสอบโดยแบบจำลอง (Simulation) ด้วยก็ได้ โดยหลักพื้นฐานแล้วไม่มีความแตกต่างกันสำหรับการใช้โปรแกรมคอมพิวเตอร์ในการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) กับการตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ข้อแตกต่างที่สำคัญคือ ในการใช้โปรแกรมคอมพิวเตอร์เพื่อตรวจสอบขั้นตอนการทำงานของโปรแกรมของธนาคาร ซึ่งเป็นการทดสอบโดยแบบจำลองนั้นมีวัตถุประสงค์เพื่อตรวจสอบว่าโปรแกรมของธนาคารได้ประมวลผลโดยถูกต้องหรือไม่ โดยตรวจสอบตัวเลขหรือผลการคำนวณโปรแกรมของธนาคาร แต่ในกรณีที่สร้างโปรแกรมคอมพิวเตอร์เพื่อตรวจสอบความถูกต้องของรายการทางการเงิน โปรแกรมของผู้ตรวจสอบจะถูกใช้เพื่อสร้างและเตรียมข้อมูลจากแฟ้มข้อมูลต่าง ๆ ของธนาคารที่เกี่ยวข้อง เพื่อเป็นข้อมูลสำหรับการตรวจสอบต่อไป

ปัญหาในทางปฏิบัติของการใช้โปรแกรมของผู้ตรวจสอบเพื่อตรวจสอบขั้นตอนการทำงานของโปรแกรมของธนาคาร คือ การย่นย่อ (Short-out) โปรแกรมที่สลับบันทึกของธนาคารเพื่อตรวจสอบค่อนข้างยากลำบาก บางครั้งอาจทำให้ผู้ตรวจสอบได้รับตัวเลขที่แตกต่างไปจากการประมวลผลของธนาคาร และอาจต้องเสียเวลาในการแก้ไขโปรแกรมหรือเสียเวลาในการกระทบยอด ด้วยเหตุนี้เทคนิคการใช้โปรแกรมคอมพิวเตอร์เพื่อตรวจสอบขั้นตอนการทำงานของโปรแกรม จึงไม่อาจกล่าวได้ว่ามีประสิทธิภาพดีเสมอไป โดยเฉพาะเมื่อได้มีการทดสอบการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) แล้ว และเห็นว่าการควบคุมดังกล่าวเชื่อถือได้ เพียงแต่ให้มีการสอบทาน (Reperformance) ขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) เท่านั้นก็เพียงพอแล้ว อย่างไรก็ตามในบางส่วนที่ผู้ตรวจสอบไม่อาจจะเชื่อถือการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ได้ การใช้โปรแกรมของผู้ตรวจสอบเพื่อตรวจสอบขั้นตอนการทำงานของโปรแกรมก็เป็นทางเลือกที่ดี



เพื่อขยายขอบเขตของการตรวจสอบระบบการควบคุม (Functional Tests) ผู้ตรวจสอบอาจจะแทรกจุดทดสอบลงไปโปรแกรมตรวจสอบด้วย เช่น การตรวจสอบยอดคงเหลือของลูกหนี้แต่ละครั้ง ก่อนที่จะปล่อยเงินกู้ครั้งต่อไปมิให้เกินกว่าวงเงินในสัญญา ซึ่งจะช่วยป้องกันมิให้เกิดหนี้สูญรายใหญ่ขึ้น เป็นต้น การตรวจสอบดังกล่าว อาจช่วยให้เพิ่มข้อเสนอแนะที่ดีในการแก้ไขการปฏิบัติงานและระบบงานของธนาคาร อันเป็นคุณลักษณะอย่างหนึ่งของการตรวจสอบระบบปฏิบัติงานของธนาคาร (Operational Examination)



แผนภาพที่ 22.7 การทดสอบข้อมูลโดยใช้โปรแกรมจำลอง (Simulation)

## 2.3 ระดับการทดสอบ (Levels of Test)

การกำหนดกฎเกณฑ์ของระดับการทดสอบระบบการควบคุมให้เป็นมาตรฐานตายตัวลงไปเป็นสิ่งที่เป็นไปไม่ได้ ผู้ตรวจสอบจึงควรต้องพิจารณาเป็นกรณี ๆ ไป โดยขึ้นอยู่กับ การควบคุม (Basic Control or Discipline) ว่ามีอยู่มากหรือน้อยเพียงไร ซึ่งโดยทั่วไปแล้วถ้าระเบียบหรือการควบคุมมีอยู่มาก ปริมาณหรือระดับการทดสอบก็ควรจะต้องมากขึ้นด้วย และโดยปกติระดับของการตรวจสอบโดยวิธีสอบทานการปฏิบัติงาน (Reperformance) จะต่ำกว่าระดับการตรวจสอบหลักฐาน (Examination of Evidence) แนวทางในการกำหนดระดับการทดสอบของการควบคุม มีดังนี้

### 2.3.1 การตรวจสอบการควบคุมทางด้านผู้ใช้ (User Controls)

ปกติจะกำหนดระดับของการทดสอบเช่นเดียวกับการตรวจสอบในระบบที่มีได้ใช้คอมพิวเตอร์ที่มีการปฏิบัติการและการควบคุมที่เหมือนกัน

### 2.3.2 การตรวจสอบความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls)

#### 1) การควบคุมการใช้ระบบงาน (Implementation Controls)

ในกรณีที่ธนาคารพัฒนาระบบงานใหม่ ผู้ตรวจสอบจะต้องตรวจสอบด้วยว่าธนาคารได้มีระเบียบข้อบังคับเพื่อการควบคุมการใช้ระบบงานใหม่ (Disciplines) ที่มีประสิทธิภาพเพียงพอ และได้มีการปฏิบัติตามระเบียบนั้นอย่างเคร่งครัด ถ้าผลการตรวจสอบการปฏิบัติตามระเบียบเป็นที่พอใจ ผู้ตรวจสอบเพียงแต่ทดสอบการควบคุมพื้นฐาน (Basic Control) ของขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ของแต่ละระบบงานก็ย่อมเป็นการเพียงพอ ในการเลือกตัวอย่างทดสอบควรจะได้พิจารณาถึงความสำคัญของระบบงานและการประมวลผล โดยเฉพาะผลที่จะเกิดขึ้นหากระบบงานหรือการประมวลผลนั้นมีได้ดำเนินไปอย่างถูกต้อง

ระดับของการทดสอบการแก้ไขโปรแกรม (Program Changes) อาจเปรียบเทียบได้กับการตรวจสอบในระบบที่มีได้ใช้คอมพิวเตอร์ ซึ่งมีลักษณะของการควบคุมที่คล้ายคลึงกัน และวิธีการตรวจสอบก็คล้ายคลึงกันในทุก ๆ ระบบงาน อย่างไรก็ตามควรจะต้องตรวจสอบการเปลี่ยนแปลงแก้ไขโปรแกรมที่เกี่ยวข้องกับขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) มากกว่าการเปลี่ยนแปลงในสิ่งเล็ก ๆ น้อย ๆ ซึ่งมีผลกระทบเพียงด้านการปฏิบัติการ (Operational Effect) เท่านั้น เช่น การเปลี่ยนแปลงรูปแบบของรายงาน เป็นต้น

#### 2) การควบคุมและรักษาความปลอดภัยโปรแกรม ระบบปฏิบัติการ และเพิ่มข้อมูล

การควบคุมในขอบเขตนี้จำเป็นต้องปฏิบัติอยู่ตลอดเวลา ลักษณะเฉพาะของการควบคุมประเภทนี้คือ มิได้มีความสัมพันธ์กับปริมาณข้อมูลที่ประมวลผล แต่มีความสัมพันธ์กับปริมาณและการใช้โปรแกรมในการประมวลผล จึงควรเลือกระดับการทดสอบให้สัมพันธ์กับปริมาณและการใช้โปรแกรมด้วย

#### 3) โปรแกรมของระบบคอมพิวเตอร์ (System Software)

ลักษณะและขอบเขตของการทดสอบความเหมาะสมของโปรแกรมของระบบคอมพิวเตอร์

ขึ้นอยู่กับ การตัดสินใจวินิจฉัยของผู้ตรวจสอบ ปัจจัยที่ควรพิจารณาคือ ระดับความเชื่อถือได้ของการควบคุมการใช้งาน (Implementation Controls) และการรักษาความปลอดภัยต่อโปรแกรมของระบบ (Security of System Software) ตลอดจนผลที่มีต่อการตรวจสอบด้านอื่นๆ

### 2.3.3 การตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures)

ลักษณะและขอบเขตของการทดสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) เพิ่มเติม ขึ้นอยู่กับ การตัดสินใจวินิจฉัยของผู้ตรวจสอบเช่นกัน ปัจจัยที่ควรพิจารณามีดังนี้

1) ระดับความเชื่อถือได้ของการควบคุมความสมบูรณ์ถูกต้องในกระบวนการของคอมพิวเตอร์ (Integrity Controls) ถ้าผู้ตรวจสอบไม่อาจเชื่อถือต่อการควบคุมการใช้งาน (Implementation Controls) ผู้ตรวจสอบก็ต้องเพิ่มระดับการทดสอบขั้นตอนการทำงานของโปรแกรม โดยการเพิ่มจำนวนโปรแกรมที่ตรวจสอบ ถ้าผู้ตรวจสอบไม่อาจให้ความเชื่อถือต่อการรักษาความปลอดภัยโปรแกรม หรือการควบคุมการปฏิบัติการคอมพิวเตอร์ ผู้ตรวจสอบก็ควรพิจารณาขยายช่วงเวลาของข้อมูลที่ผ่านมาโปรแกรมที่ตรวจสอบให้มากยิ่งขึ้น

2) ขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) ที่เลือกทดสอบควรเป็นโปรแกรมที่มีผลกระทบต่อภัยสำคัญ (Material Effect) ของรายงานแสดงฐานะและการดำเนินงานของธนาคาร

3) ในการกำหนดระดับการทดสอบ ผู้ตรวจสอบควรพิจารณาลักษณะและขนาดของรายการที่ทำการประมวลผล และความเสียหายที่จะเกิดข้อผิดพลาดอันมีนัยสำคัญ (Material Error) ระบบเกี่ยวกับการจ่ายเงินบัญชีเงินสดและลูกหนี้ มักจะมีแนวโน้มที่เสี่ยงต่อการทุจริตอย่างมาก

4) ในระบบงานใดซึ่งผลลัพธ์จากการประมวลผลได้มีการสอบทานใหม่ทั้งหมดอีกครั้งหนึ่ง โอกาสที่จะเกิดข้อผิดพลาดเนื่องจากโปรแกรมย่อมน้อยกว่าระบบซึ่งผลลัพธ์จากการประมวลผลไม่อาจจะสอบทานใหม่ด้วยมือได้

### 2.3.4 ข้อควรพิจารณาอื่น

ข้อควรพิจารณาอื่นในการเลือกระดับการทดสอบ มีดังนี้

#### 1) ปฏิบัติการของผู้ตรวจสอบที่มีต่อข้อบกพร่องในการควบคุม

ผู้ตรวจสอบควรที่จะเลือกระดับการทดสอบได้เหมาะสมกับข้อบกพร่องของการควบคุมที่พบจากการประเมินระบบการควบคุมภายใน ตัวอย่างเช่น ในกรณีที่ขาดการควบคุมแบบกำกับ (Supervisory Controls) แต่พอจะสันนิษฐานได้ว่ามีการแบ่งแยกหน้าที่ (Segregation of Duties) อย่างเหมาะสม ผู้ตรวจสอบก็อาจเพิ่มระดับการตรวจสอบหลักฐาน (Examination of Evidence) เพื่อความมั่นใจว่าได้มีการปฏิบัติตามการควบคุมขั้นพื้นฐาน (Basic Controls) อย่างต่อเนื่องตลอดงวดการบัญชีที่ตรวจสอบ ในทางกลับกันในกรณีที่การแบ่งแยกหน้าที่ไม่เหมาะสม แต่มีการควบคุมแบบกำกับที่ดีพอผู้ตรวจสอบอาจเพิ่มระดับการสอบทานการปฏิบัติงาน (Reperformance) เพื่อความมั่นใจว่าได้มีการปฏิบัติตามการควบคุมขั้นพื้นฐาน (Basic Controls) โดยต่อเนื่องเช่นกัน

## 2) ความสำคัญของข้อผิดพลาดที่อาจเกิดขึ้น

ความล้มเหลว (Breakdown) หรือการขาดระบบควบคุมใด ๆ จะให้ผลที่แตกต่างกันแล้วแต่ลักษณะของการควบคุมนั้น ๆ ตัวอย่างเช่น การขาดการควบคุมข้อมูลถาวร (Standing Data) ย่อมจะมีความสำคัญว่าการขาดการควบคุมข้อมูลเคลื่อนไหว (Transaction Data) ฉะนั้นจึงควรจะใช้ระดับการทดสอบที่สูงกว่า หรือหากไม่มีการควบคุมความถูกต้องสมบูรณ์ครบถ้วน (Completeness) ย่อมจะมีความสำคัญมากกว่าการขาดการควบคุมด้านความถูกต้อง (Accuracy หรือ Validity) ของข้อมูลเคลื่อนไหวแต่ละข้อมูล ทั้งนี้เพราะรายการที่ควรจะรวมอยู่ในผลลัพธ์จากการประมวลผล แต่ขาดหายไปในระหว่างการประมวลผล ยากแก่การตรวจพบในระหว่างตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) ฉะนั้นระดับการทดสอบความถูกต้องสมบูรณ์จึงควรอยู่ในระดับสูงขณะที่ทำการตรวจสอบระบบการควบคุม (Functional Test)

## 3) ความสลับซับซ้อนของรายการบัญชีและประสบการณ์การตรวจสอบ

ถ้าข้อมูลที่น่าเข้าประมวลผลด้วยคอมพิวเตอร์มีหลายประเภท และมีความแตกต่างกันอย่างมาก หรือรายการหรือการคำนวณมีความสลับซับซ้อน ระดับการทดสอบก็ควรมีประสิทธิภาพพอที่จะครอบคลุมความแตกต่างกันในทุกแง่มุมได้ทั้งหมด ในทำนองเดียวกันถ้าจากการตรวจสอบที่ผ่านมาได้พบข้อบกพร่องจากการประมวลผลระดับของการทดสอบก็ควรจำเป็นต้องเพิ่มให้ครอบคลุมข้อบกพร่องทุกด้านที่เคยเกิดขึ้น

## 3. สรุป

ในระบบคอมพิวเตอร์วัตถุประสงค์ของการตรวจสอบระบบการควบคุม (Functional Tests) ยังคงเช่นเดียวกับการตรวจสอบในระบบที่มีได้ใช้คอมพิวเตอร์ คือ การหาหลักฐานว่าได้มีการปฏิบัติตามขบวนการการควบคุมภายในตามที่ระบุในแบบสอบถาม (Internal Control Questionnaire) หรือไม่ แต่ด้วยเหตุที่มีการเปลี่ยนแปลงการควบคุมในระบบคอมพิวเตอร์ เทคนิคและขอบเขตของการตรวจสอบจึงแตกต่างไปจากระบบธรรมดา

ก่อนที่จะตัดสินใจตรวจสอบระบบการควบคุม (Functional Tests) ผู้ตรวจสอบพึงระลึกว่าประสิทธิภาพการตรวจสอบในบางครั้งก็อาจจะดีกว่าก็ได้ หากเลือกวิธีการตรวจสอบอย่างใดอย่างหนึ่งซึ่งเป็นลักษณะเฉพาะของระบบคอมพิวเตอร์ คือ การใช้โปรแกรมคอมพิวเตอร์เพื่อตรวจสอบข้อมูลที่ประมวลผลจำนวนมาก ซึ่งเป็นวิธีการหนึ่งที่จะช่วยเพิ่มประสิทธิภาพของการตรวจสอบความถูกต้องของรายการทางการเงิน (Validation Procedures) อีกทางหนึ่งด้วย หรืออีกทางเลือกหนึ่งคือ เพิ่มการตรวจสอบขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) หรือตรวจสอบโปรแกรมของระบบ (System Softwares) โดยไม่จำเป็นต้องประเมินหรือตัดสินใจให้ความเชื่อถือการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (Integrity Controls)

การทดสอบการควบคุมทางด้านผู้ใช้ (User Controls) และการควบคุมความสมบูรณ์ถูกต้องในกระบวนการคอมพิวเตอร์ (Integrity Controls) ซึ่งกระทำด้วยมือ จะมีลักษณะเหมือนการตรวจสอบในระบบที่มีได้ใช้คอมพิวเตอร์ แต่การทดสอบความเหมาะสมของโปรแกรมของระบบ (System Software) และขั้นตอนการทำงานของโปรแกรม (Programmed Procedures) มักจะต้องใช้เทคนิคที่แตกต่างออกไป ซึ่งได้แก่ ทั้งการสร้างข้อมูลตัวอย่างทดสอบ (Audit Test Data) การวิเคราะห์รหัสโปรแกรม (Program Code Analysis) และการใช้โปรแกรมคอมพิวเตอร์ (Computer Programs)