เอกสารอ้างอิง

1. Hemphill, Charles F. Jr, and Hemphill, John M. Security Procedures for Computer Systems. Illinois: Dow Jones - Irwin, Inc., 1973.
2. Martin, Jome. Security Accuracy and Privacy in Computer Systems. New Jersey: Prentice - Hall, Inc., 1973.
3. Tassel, Van Dennis. Computer Security Management. New Jersey: Prentice - Hall, Inc., 1972.
4. Hoffman, Lance J. Modern Methods for Computer Security and Privacy. New Jersey: Prentice - Hall, Inc., 1977.
5. วิชิต อมรวิรัตนสกุล. "การตรวจสอบความถูกต้องของข้อมูลคอมพิวเตอร์." ใน **คอมพิวเตอร์สาร** หน้า 25 - 29 กรุงเทพมหานคร สมาคมคอมพิวเตอร์แห่งประเทศไทย, กรกฎาคม 2521.
6. วรนุช ตรีทิพยบุตร และ สหัส ตรีทิพยบุตร. ระบบบันทึกข้อมูล. กรุงเทพมหานคร : สำนักงานสถิติแห่งชาติ, ตุลาคม 2521.
7. Katzan, Harry, Jr. Computer Data Security. New York: Van Nostrand Reinhold Company, 1973.
8. เสนิส อคุลยพันธ์ พันเอก. "ปัญหาในการจัดตั้งหน่วยคอมพิวเตอร์." ในคอมพิวเตอร์สาร. หน้า 4 - 12. กรุงเทพมหานคร: สมาคมคอมพิวเตอร์แห่งประเทศไทย, เมษายน 2518.
9. Yearsley, R. B., and Graham, G.M.R. Handbook of Computer Management. Gower Press Limited, 1973.
10. กฤษณพันธุ์ สุพรรณโรจน์. คอมพิวเตอร์และแวดวงธุรกิจ. พิมพ์ครั้งที่ 2. กรุงเทพมหานคร : สำนักพิมพ์แพร่พิทยา, 2520.

11. Davis, Gordon B. Management Information Systems: Conceptual Foundations, Structure and Development New York: McGraw - Hill, Inc., 1974.

12. Walker, Bruce J., and Blake, Ian F. Computer Security and Protection Structures. Stroudsburg: Dowden, Hutchingon and Ross, Inc., 1977.

13. Hamilton Peter. Computer Security. Philadelphia: Auerbach Publishers Inc., 1973.

ภาคผนวก

ภาคผนวก ก.

แบบสอบถามการประเมินผลการควบคุมภายใน
ของศูนย์คอมพิวเตอร์

วันที่ .....เดือน.....ปี.....

รายละเอียดขั้นต้น

หน่วยงาน .....

ระบบที่ใช้ .....

— Hardware

CPU แบบ ..... จำนวน ..... Capacity ..... อื่น ๆ .....
เช่าหรือซื้อ ..... ราคาต่อหน่วย .....เงื่อนไ.....
ประวัติการใช้โดยย่อ .....

I/O Devices

— Input 1. แบบ ..... จำนวน .....Speed .....อื่น ๆ .....เช่าหรือซื้อ.....ราคาต่อหน่วย...
2. แบบ ..... จำนวน .....Speed .....อื่น ๆ .....เช่าหรือซื้อ.....ราคาต่อหน่วย...
3. แบบ ..... จำนวน .....Speed .....อื่น ๆ .....เช่นหรือซื้อ.....ราคาต่อหน่วย...

– Output 1 แบบ ..... จำนวน ..... Speed ..... อื่น ๆ .....เช่าหรือซื้อ...ราคาต่อหน่วย...

2 แบบ ..... จำนวน ..... Speed ..... อื่น ๆ .....เช่าหรือซื้อ...ราคาต่อหน่วย...

อื่น ๆ 1 แบบ ..... จำนวน ..... Speed ..... อื่น ๆ .....เช่าหรือซื้อ...ราคาต่อหน่วย...

2 แบบ ..... จำนวน ..... Speed ..... อื่น ๆ .....เช่าหรือซื้อ...ราคาต่อหน่วย...

– Software

ประวัติการวางระบบงานและ Application Program โดยสรุป .....

.....

..... ภาษาคอมพิวเตอร์ที่ใช้ .....

มีการใช้โปรแกรมสำเร็จรูป หรือไม่ถ้าใช้แสดงรายละเอียด .....

.....

บริการอื่น ๆ ที่ได้จาก บริษัทผู้ขายคอมพิวเตอร์/หน่วยงานคอมพิวเตอร์ที่ให้บริการ .....

.....

รายละเอียดงานที่ทำ

เริ่มโครงการเมื่อ ..... เหตุที่พิจารณาใช้ .....

.....

ประวัติการใช้งาน .....

.....

.....

.....

.....

.....

.....

.....

งานที่ทำในปัจจุบัน

งานที่ทำเรียงตามลำดับ Priority สูง – ต่ำ	1	เอกสารเบื้องต้นที่ใช้	2	ประโยชน์ที่ได้รับหรือรายงานที่ได้	3	4	5	6	ผลเสียที่อาจเกิดขึ้นเมื่องานคั่งค้างหรือผิดพลาด	7

1 ช่วงระยะของงานตลอดเวลา (A) ทุกวัน(D) ทุกสัปดาห์ (W) ทุกเดือน(M) หรือทุกปี (Y)

2 การเตรียมเอกสารเบื้องต้นเสร็จทันตามกำหนดกี่เปอร์เซ็นต์

3 ชั่วโมงทำงานที่ต้องใช้

4 เปอร์เซ็นต์ของงานที่ทำโดยเครื่องคอมพิวเตอร์ของตนเอง (ส่วนที่เหลือเป็นเปอร์เซ็นต์ของงานที่ทำโดยเครื่องภายนอก) / เปอร์เซ็นต์ของงานที่ทำโดยบริการคอมพิวเตอร์ภายนอกทั้งหมด

5 เปอร์เซ็นต์ของงานคั่งค้าง

6 เปอร์เซ็นต์ของงานผิดพลาดโดยประมาณ

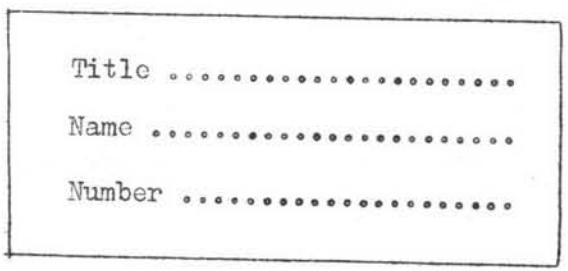
7 หมายเหตุและ Software Available for Audit Use

ในขณะนี้ชั่วโมงการใช้งานทั้งสิ้นเท่าใด ..... ความสามารถของระบบที่ใช้อยู่พอเพียงหรือไม่ ..... ถ้าไม่พอเพียงได้ดำเนินการแก้ไขอย่างไรและมีปัญหาอะไร .....
.....
.....

งานที่คาดว่าจะทำในอนาคต .....
.....
.....

โครงการปรับปรุงระยะยาว .....
.....
.....

Organization Chart



ประเมินอัตรากำลัง

อัตรากำลังในปัจจุบัน

ตำแหน่งหรือหน้าที่	จำนวน	ทำงานประจำหรือชั่วคราว	ชม.ทำงานต่อสัปดาห์	คุณวุฒิและประสบการณ์	หมายเหตุ

โครงการฝึกอบรม

เคยจัดมาแล้ว .....

กำลังจัด .....

จะจัดในอนาคต .....

อัตรากำลังในขณะนี้พอเพียงหรือไม่ถ้าไม่พอเพราะเหตุใด .....

ขาดแคลนในด้านใดบ้าง .....แก้ไขอย่างไร.....

มีโครงการระยะยาวอย่างไร .....

แบบสอบถามประเมินผลการควบคุมภายในทั่วไป

รายการคำถาม

คำถามทั่วไป

1. Standby arrangement

ก. มีการวางแผนตระเตรียมการใช้เครื่องคอมพิวเตอร์สำรองเมื่อ เครื่องที่ใช้อยู่ในปัจจุบันเกิดขัดข้องหรือไม่ อย่างใด

ข. ถ้ามีการวางแผน เคยทดลองการใช้โปรแกรมและ Computer File ที่ใช้กับเครื่องคอมพิวเตอร์สำรองหรือไม่

ก. ถ้าไม่มีการวางแผนใช้เครื่องสำรองมีมาตรการอะไรที่พิจารณาใช้ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้อยู่เกิดขัดข้องเป็นเวลานานติดต่อกัน

2. ได้มีการทำประกันอัคคีภัยและภัยอย่างอื่นหรือไม่ อย่างใด มีขอบเขตความคุ้มครองเพียงใด

3. ในระยะใดที่ผู้ตรวจสอบภายนอกหรือผู้ตรวจสอบภายในมีส่วนร่วมในการวางระบบคอมพิวเตอร์

ก. Feasible Stndy

ข. ร่างระบบที่จะใช้

ค. Detailed Specification

ง. Program Testing

จ. ในระยะแรกของการใช้งาน

ฉ. หลังจากเริ่มใช้งานไปแล้วนานพอสมควร

ช. ไม่เคยมีส่วนร่วมเลย

4. ถ้าผู้ตรวจและผู้ตรวจภายในมีส่วนร่วมในการวางระบบการมีส่วนร่วมนั้นเป็นเพียงผิวเผินหรือมากพอที่จะเชื่อถือได้ว่า

ก. มีการวางระบบควบคุมอย่างพอเพียง

ข. มีการรักษา Andit Trail ไว้อย่างเพียงพอ

ค. มีการใช้ประโยชน์จากเครื่องคอมพิวเตอร์อย่างเต็มที่

5. ก่อนจะใช้ระบบคอมพิวเตอร์หรือเปลี่ยนระบบการใช้ เคยมีการประมาณค่าใช้จ่ายหรือไม่ ถ้ามีใครเป็นคนประมาณและในทางปฏิบัติจริง ๆ นั้นเป็นไปตามที่ประมาณไว้หรือไม่

6. มีการเฉลี่ยค่าใช้จ่าย ในการใช้ระบบคอมพิวเตอร์ไปยังแผนกต่าง ๆ ซึ่งเป็นผู้ใช้หรือได้ใช้ประโยชน์หรือไม่ อย่างใด

<u>การควบคุมด้านการจัดองค์การ</u>

1. มีการแบ่งแยกขอบเขตความรับผิดชอบในระหว่างหน้าที่ต่อไปนี้อย่างชัดเจนหรือไม่ (รวมทั้งการแบ่งแยกผู้ทำหน้าที่ควบคุมตรวจตรา)

ก. ผู้วางระบบงานและผู้เตรียมโปรแกรม

ข. ผู้ตระเตรียมข้อมูล

ค. ผู้ควบคุมเครื่อง

ง. ผู้เก็บรักษาวัสดุข้อมูลและโปรแกรม

จ. ผู้ควบคุมการปฏิบัติงาน

มีการกำหนดหน้าที่ความรับผิดชอบเป็นลายลักษณ์อักษรหรือไม่

2. มีการวางระเบียบดังต่อไปนี้หรือไม่

ก. ห้ามมิให้ผู้เตรียมโปรแกรมใช้ Computer File หรือโปรแกรมที่ยังใช้งานอยู่ทำการปฏิบัติข้อมูลจริง ๆ ยกเว้นการใช้เพื่อทดสอบเป็นครั้งคราวซึ่งต้องอยู่ในความควบคุมของบุคคลที่เป็นอิสระจากผู้เตรียมโปรแกรมนั้น

ข. มีการวางระเบียบควบคุมให้ผู้มีหน้าที่เกี่ยวข้องเท่านั้นที่อาจใช้ในการเปลี่ยนแปลงหรือพิมพ์รายงานจากข้อมูลใน Computer File

ค. จำกัดงานการเตรียมข้อมูลเบื้องต้นที่จะใช้ปฏิบัติข้อมูลให้เป็นงานของผู้มีหน้าที่โดยแท้จริงเท่านั้น

ง. ผู้ที่มีหน้าที่ในการปฏิบัติข้อมูลหรือผู้ควบคุมเครื่องถูกห้ามมิให้เป็นผู้เก็บรักษาหรือล่วงรู้ข้อมูลเอกสารทางการเงิน

จ. ห้ามมิให้ผู้เตรียมโปรแกรมและผู้ควบคุมเครื่องแก้ไข Input Data ได้เอง

ฉ. เฉพาะผู้ควบคุมเครื่องเท่านั้นที่ได้รับอนุญาตให้ควบคุมเครื่องคอมพิวเตอร์ในขณะใช้งาน

ช. กำหนดให้มีผู้ควบคุมเครื่องอย่างน้อยสองคนขึ้นไปทำการปฏิบัติหน้าที่ในช่วงใดช่วงหนึ่งและมีการสับเปลี่ยนหน้าที่เป็นครั้งคราวหรือไม่

ซ. แบบฟอร์มเอกสารบางประเภทที่ต้องระมัดระวังเป็นพิเศษ เช่น เช็คเปล่าที่จะใช้พิมพ์รายการจ่ายเงินของพนักงานได้ถูกเก็บรักษาโดยบุคคลที่เป็นอิสระจากผู้ควบคุมเครื่องหรือไม่

ฌ. จำกัดให้เพียงผู้เก็บรักษาวัสดุข้อมูลที่สามารถเข้าไปยังห้องเก็บ File และโปรแกรม

ด. ผู้เก็บรักษาวัสดุข้อมูลต้องเป็นผู้มีอิสระในการปฏิบัติงานและไม่มีหน้าที่

8. ศูนย์คอมพิวเตอร์เป็นอิสระจากหน่วยงานอื่นที่ศูนย์ทำการปฏิบัติข้อมูลหรือไม่

4. พนักงานในศูนย์คอมพิวเตอร์มีหน้าที่ในหน่วยงานอื่นในขณะเดียวกันหรือไม่

5. มีการแต่งตั้งคณะกรรมการประสานงานการใช้คอมพิวเตอร์หรือไม่ มีการประชุมประสานงานกันบ่อยเพียงใด

6. มีการแต่งตั้งผู้มีหน้าที่ตรวจสอบภายในหรือไม่ ถ้ามีการแต่งตั้งได้ทำหน้าที่อะไรบ้าง

ก. ควบคุมการรับ Input

ข. ควบคุมการแจกจ่าย Output

ค. ควบคุมรายการผิดพลาด ติดตามตรวจสอบว่าได้มีการรายงานความผิดพลาดที่เกิดขึ้นทุกรายการให้มีการนำส่งไปแก้ไขและมีการ Reprocess

ง. ตรวจสอบ Console Error Listing และอื่น ๆ

7. ผู้ตรวจสอบภายในได้ดำเนินการตรวจสอบในระดับใด

ก. Review หรือ **Audit**

ข. ควบคุมเป็นประจำโดยใกล้ชิดแบบ Day - to - day Control

8. ผู้ตรวจสอบภายในมีความรู้ในระบบคอมพิวเตอร์ดีเพียงใด

<u>การควบคุมด้านการทำเอกสารรายละเอียดประกอบระบบงาน</u>

1. มีการเตรียมเอกสารดังต่อไปนี้บ้างหรือไม่

ก. Organization Chart

ข. Process Flow Chart

ค. Program Run Book

ง. รายละเอียดประกอบ File

2. ใครบ้างมีหน้าที่รับผิดชอบในการจัดทำรายละเอียดประกอบระบบงาน

ก. ควบคุมให้มีการตระเตรียมอย่างถูกต้อง

ข. มีการแก้ไขให้ทันต่อการเปลี่ยนแปลง

ค. ตรวจทานให้เป็นไปตามมาตรฐานผลของการปฏิบัติหน้าที่เป็นไปอย่างน่าพอใจหรือไม่

3. มีการกำหนดมาตรฐานที่ใช้ในเอกสารเหล่านี้บ้างหรือไม่

ก. การสำรวจขั้นต้น

ข. การร่างระบบ

ค. การทำ feasibility Study

ง. การจัดทำโปรแกรมและรายการแก้ไข

4. ใครเป็นผู้รับผิดชอบในการควบคุมให้มีการใช้มาตรฐานเดียวกันโดยตลอด มีวิธีการอย่างใด

<u>การควบคุมด้านการปฏิบัติงาน</u>

1. มีการจัดทำคู่มือการปฏิบัติงานมาตรฐานสำหรับงานต่อไปนี้หรือไม่
   - ก. ผู้วิเคราะห์ระบบ
   - ข. ผู้เตรียมโปรแกรม
   - ค. ผู้ควบคุมเครื่อง
   - ง. ผู้เก็บรักษาวัสดุข้อมูลและโปรแกรม
   - จ. ผู้เตรียมข้อมูล
   - ฉ. เจ้าหน้าที่รักษาความปลอดภัย
   - ช. หน่วยงานที่ใช้
   - ฌ. ผู้มีหน้าที่ควบคุมและหน่วยตรวจสอบภายใน
2. ใครบ้างที่มีหน้าที่รับผิดชอบในการ
   - ก. ควบคุมให้มีการตระเตรียมอย่างถูกต้อง
   - ข. ทำการแก้ไขให้ทันต่อการเปลี่ยนแปลง
   - ค. ตรวจทานให้เป็นไปตามมาตรฐาน

ผลการปฏิบัติงานเป็นไปอย่างน่าพอใจหรือไม่

<u>การควบคุมด้านโปรแกรม</u>

1. มีการเตรียมเอกสารต่อไปนี้เพื่อประกอบโดยครบถ้วนหรือไม่
   - _ Problem Statement
   - _ System Flow Chart
   - _ Record Layouts

- Program Flow Chart
- Program Listing
- Test Data
- Operator Instruction
- Summary of Controls
- Approval and Change Record

2. ใครบ้างที่มีหน้าที่รับผิดชอบใน การ
   ก. ควบคุมให้มีการตระเตรียมอย่างถูกต้อง
   ข. ทำการแก้ไขให้ทันต่อการเปลี่ยนแปลง
   ค. ตรวจทานให้เป็นไปตามมาตรฐาน
3. ใครบ้างที่มีอำนาจสั่งการให้ทำการเปลี่ยนแปลง
   ก. ระบบงาน
   ข. โปรแกรม

มีการวางระเบียบเป็นลายลักษณ์อักษรกำหนดโดยชัดแจ้งหรือไม่

4. รายการเปลี่ยนแปลงทุกครั้งมีการอนุมัติและทำรายละเอียดประกอบเป็นการถาวรทุกครั้งหรือไม่

5. ก่อนที่จะนำโปรแกรมที่เปลี่ยนแปลงไปใช้การจริง ๆ มีการขออนุมัติจากผู้มีหน้าที่ต่อไปนี้หรือไม่
   ก. ผู้อำนวยการศูนย์คอมพิวเตอร์
   ข. หน่วยงานผู้ใช้
   ค. ผู้ตรวจสอบภายใน

6. ถ้ามีการทดสอบโปรแกรมที่แก้ไขก่อนใช้งานจริง ๆ การทดสอบประกอบไปด้วยเทคนิคใดบ้าง
   ก. Test Data
   ข. Parallel Running
   ค. Pilot Running

7. ถ้ามีการใช้ Test Datd

ก. มีการตระเตรียมการทดสอบโดยหน่วยงานที่อิสระจากหน่วยงานที่ทำการเปลี่ยนแปลงแก้ไขหรือไม่

8. มีการวางระเบียบในด้านการตรวจสอบโปรแกรมที่ผ่านการเปลี่ยนแปลงโดยชัดแจ้งหรือไม่

9. ผู้ตรวจสอบภายในมีส่วนร่วมในการตระเตรียม Test Dats หรือไม่ มีการเตรียม Test Data โดยแง่มุมของผู้ตรวจสอบบ้างหรือไม่

<u>การควบคุม Master Files</u>

1. มีการวางระเบียบกำหนดผู้มีอำนาจสั่งการ Update Master File โดยชัดแจ้ง

2. หลังจาก Update มีการตรวจสอบรายการใน Master File กระทบยอดกับเอกสารเบื้องต้นอีกครั้งหรือไม่

3. ในการตระเตรียมการ Update Master File

ก. มีการขออนุมัติก่อนหรือไม่?

ข. ใครับการตรวจสอบโดยหน่วยงานใดบ้าง

- หน่วยงานตรวจสอบ
- หน่วยงานผู้ใช้

4. มีการพิสูจน์ความถูกต้องของยอดรวมในMaster File เป็นครั้งคราวหรือไม่ เช่น ตรวจสอบกลับโดยการตรวจนับของจริง การขอใบยืนยันยอมจากลูกหนี้

ก. ทำอย่างไร

ข. บ่อยเพียงใด

ค. โดยใคร

การควบคุมรักษาความปลอดภัยของข้อมูลและโปรแกรมที่ใช้

1. มีการวางระบบป้องกันอัคคีภัยหรือไม่ มีวิธีป้องกันอย่างใดบ้าง และระบบป้องกันเชื่อถือได้เพียงใด

2. มีการตระเตรียมระบบขนย้ายข้อมูลในกรณีที่เกิดอัคคีภัยหรือไม่ มีการซักซ้อมเป็นครั้งคราวหรือไม่

3. มีการแต่งตั้งผู้รับผิดชอบรักษาวัสดุข้อมูลและโปรแกรมหรือไม่ ถ้าไม่ ใครรับผิดชอบหน้าที่นี้

4. ผู้รับผิดชอบรักษาวัสดุข้อมูลและโปรแกรมปฏิบัติหน้าที่ตลอดเวลาหรือไม่

- ในระหว่างเวลาปกติ
- ในระหว่างการปฏิบัติล่วงเวลา
- ในระหว่างวันหยุด

5. มีการเก็บโปรแกรมและ File ทั้งสิ้นที่ใช้ในห้องเก็บโดยครบถ้วนหรือไม่ ถ้าไม่เก็บในห้องได้นำไปรักษาไว้ ณ ที่ใดอย่างไร

6. ถ้ามีการเก็บในห้องที่ปิดกุญแจเมื่อผู้รักษาวัสดุข้อมูลไม่อยู่อะไรจะเกิดขึ้นเมื่อต้องการใช้ File ที่เก็บในห้องนั้น

7. จากการสังเกตพบว่ามีการวางวัสดุข้อมูลกระจัดกระจายโดยปราศจากผู้ดูแลหรือไม่

8. มีการทำทะเบียนควบคุม File และโปรแกรมหรือไม่ มีการบันทึกการยืมและส่งคืนผู้ทำหน้าที่เก็บรักษาโดยครบถ้วนหรือไม่

9. มีการตรวจสอบความถูกต้องครบถ้วนของทะเบียนนี้เป็นครั้งคราวหรือไม่ ใครเป็นผู้ตรวจสอบ

10. มีระเบียบห้ามมิให้ผู้เตรียมโปรแกรมยุ่งเกี่ยวกับ File และโปรแกรมที่ใช้ยกเว้นได้รับอนุญาตหรือไม่

11. มีการวางระบบ Back - up อย่างใดหรือไม่มีระเบียบการอย่างไรมีการแยกข้อมูลตามความสำคัญหรือไม่

ก. มีการป้องกันข้อมูลที่เก็บรักษาในเทปแม่เหล็กโดยระบบ Back up ใดบ้างหรือไม่

ข. มีการDumping ข้อมูลที่เก็บรักษาในแผ่นจานแม่เหล็กลงในเทปแม่เหล็กเป็นครั้งคราวในช่วงเวลาที่เหมาะสมหรือไม่

ค. ข้อมูลที่เก็บรักษาในรูปแบบอื่นได้รับการป้องกันรักษาอย่างไร

ง. มีระบบ Off - site Storage หรือไม่

12. ระบบรักษาความปลอดภัยของข้อมูลเชื่อถือได้เพียงใดในกรณีที่

ก. เกิดอุบัติเหตุ File สูญหาย หรือ File ถูกทำลาย

ข. มีการลับลอบนำ File หรือโปรแกรมไปใช้โดยไม่ได้รับอนุญาต

13. มีการนำสอบระบบ Back up เป็นครั้งคราวหรือไม่

<u>การควบคุมการเข้าสู่สถานที่ตั้งคอมพิวเตอร์</u>

1. มีการแต่งตั้งเจ้าหน้าที่รักษาความปลอดภัยหรือไม่ ถ้ามีทำหน้าที่อะไรบ้าง

ก. ควบคุมการเข้าออกในศูนย์คอมพิวเตอร์และ Terminal

ข. ควบคุมการผ่านเข้าออกในห้องเก็บข้อมูล Terminal ถ้าไม่มีการแต่งตั้งเจ้าหน้าที่รักษาความปลอดภัยมีมาตรการอย่างอื่นที่ใช้อย่างใด

2. เจ้าหน้าที่รักษาความปลอดภัยมีหน้าที่อื่นใดที่เกี่ยวกับศูนย์คอมพิวเตอร์หรือหน่วยงานอื่นหรือไม่

3. มีมาตรการอะไรบ้างในการควบคุมการใช้ terminal เพื่อป้องกัน

ก. การใช้ terminal โดยผู้ไม่มีอำนาจหน้าที่

ข. การใช้ terminalที่ผู้ใช้นั้นไม่มีสิทธิใช้

ค. ถ้ามีการส่งข้อมูลไปตามสายมีมาตรการป้องกันความลับหรือป้องกันการสูญหายของข้อมูลอย่างไร

4. ถ้ามีการใช้ password

ก. มีวิธีการกำหนดบันทึกและเปลี่ยนแปลง password อย่างไร มีมาตรการควบคุมอย่างไร

ข. มีการป้องกันมิให้มีการปลอมแปลง password อย่างไร

5. ถ้าใช้ระบบควบคุมอย่างอื่นระบุโดยละเอียด

6. เมื่อผู้มีอำนาจหน้าที่ต้องการใช้ File ซึ่งปกปิดที่มีสิทธิ์ใช้ มีขั้นตอนการขอใช้อย่างใด

7. มีการตรวจสอบหาร่องรอยการใช้ File โดยไม่ได้รับอนุญาตเป็นครั้งคราวบ้างหรือไม่

<u>การควบคุมด้านการใช้เครื่องคอมพิวเตอร์</u>

1. มีการกำหนดระเบียบการต่อไปนี้หรือไม่

ก. ขอบเขตหน้าที่และความรับผิดชอบของผู้ควบคุมเครื่องแต่ละคน

ข. การสับเปลี่ยนหน้าที่

ค. มาตรการที่จะปฏิบัติเมื่อมีรายการ program halt โดยไม่คาดหมายมาก่อน

2. มีมาตรการป้องกันการใช้เครื่องปฏิบัติงานที่ไม่ได้รับการมอบหมายอย่างไร และการควบคุมนี้มีผลตลอดเวลาหรือไม่ โดยเฉพาะอย่างยิ่งในระหว่างเวลากลางคืนและวันหยุด

3. มีการทำหมายกำหนดการล่วงหน้าแสดงงานที่จะทำหรือไม่ ถ้ามีใครเป็นผู้จัดทำ ถ้าไม่มีได้กำหนดวิธีการควบคุมอย่างไดหรือไม่

4. มีการควบคุมให้ปฏิบัติตามหมายกำหนดการที่เตรียมไว้อย่างใด ใครเป็นผู้ควบคุม

5. มีการทำ Program Opreating Instruction บ้างหรือไม่ มีรายการต่อไปนี้หรือไม่

ก. อุปกรณ์ Peripherals และ Core Storage ที่ต้องใช้

ข. Input และ Output File ที่ต้องใช้และจะได้จากการปฏิบัติข้อมูล

ค. Set - up Instructions

ง. ประมาณเวลาที่ใช้ในการปฏิบัติข้อมูลปกติ

6. มีการวางระเบียบให้ผู้ควบคุมเครื่องไม่ยอมรับการเปลี่ยนแปลง Program Operating Instrution ยกเว้นจะมีการสั่งเป็นลายลักษณ์อักษรและมีการอนุมัติถูกต้องหรือไม่

7. ถ้ามีการนำงานไปปฏิบัติโดยเครื่องคอมพิวเตอร์ภายนอก มีมาตรการควบคุมอย่างไร

8. มีการทำ Operator ' s logs หรือไม่ ถ้าทำ มีการบันทึกรายละเอียดรายการเหล่านี้หรือไม่

ก. การ Process งานปกติ

ข. รายการ Re - run

ค. เครื่องขัดข้อง

ง. การทดสอบโปรแกรม

จ. เวลาที่ว่างจากการใช้

9. มีการบันทึกคำอธิบายถึงการปฏิบัติข้อมูลที่ใช้เวลายาวนานผิดปกติหรือไม่

10. มีการตรวจสอบ Operator ' s log เป็นครั้งคราวหรือไม่ ถ้ามี ใครเป็นผู้ตรวจสอบ

11. มีการประเมินผลประสิทธิภาพในการใช้เครื่องคอมพิวเตอร์บ้างหรือไม่ ถ้ามี ใครเป็นผู้ทำและมีวิธีทำอย่างไร

12. มีการพิมพ์ Console log ใน Console Printer โดยอัตโนมัติหรือไม่

13. รายการ Operator Intervention ทุกรายการได้รับการบันทึกใน Console log โดยครบถ้วนหรือไม่ และมีการพิมพ์เวลากำกับไว้ด้วยหรือเปล่า

14. มีข้อมูลใดบ้างที่พิมพ์ใน Console log มีการลงหมายเลขลำดับล่วงหน้าในกระดาษพิมพ์หรือไม่

15. มีมาตรการอย่างใดในการป้องกันมิให้ผู้ควบคุมรายละเอียดของโปรแกรมและข้อมูลที่ใช้เกินกว่าความจำเป็นในการปฏิบัติหน้าที่จนอาจก่อให้เกิดการ Intervention การใช้เครื่องเพื่อผลในทางทุจริตได้

การควบคุมด้าน Input

1. มีการตรวจสอบเอกสารเบื้องต้นก่อนนำไปเจาะบัตรหรือไม่ และหลังจากเจาะบัตรแล้วมีการนำไป Verification อีกครั้งหรือไม่

2. มีการลงเลขลำดับล่วงหน้าในเอกสารเบื้องต้นที่จะใช้เป็น Input Data หรือไม่ ถ้ามีใช้ในประเภทใดบ้าง

3. มีการทำทะเบียนรับ – จ่าย เอกสารเบื้องต้นที่สำคัญหรือไม่

4. มีการปฏิบัติอย่างใดกับเอกสารเบื้องต้นที่ผ่านการเจาะบัตรแล้วเพื่อป้องกันมิให้นำกลับไปเจาะบัตรซ้ำอีก

5. มีการวางระบบควบคุมการเคลื่อนไหวของ Input Data อย่างใด

ก. จากหน่วยงานผู้ตระเตรียม Input ไปยังศูนย์คอมพิวเตอร์

ข. ในศูนย์คอมพิวเตอร์

ระบบการควบคุมนี้เพียงพอหรือไม่ เพื่อให้แน่ใจว่า

ก. มีการปฏิบัติข้อมูลที่ถูกต้องโดยครบถ้วน

ข. ละเว้นการปฏิบัติข้อมูลที่ผ่านการเตรียมโดยไม่ถูกต้อง

ค. ไม่มีการปฏิบัติข้อมูลรายการเดียวกันซ้ำซ้อน

6. มีการกำหนดมาตรฐานเอกสารเบื้องต้นที่เป็น Input เท่าที่สามารถจะทำได้หรือไม่

7. ตรวจดูรายละเอียดวิธีปฏิบัติงาน ว่า

ก. งานการเตรียม Input Data เป็นอิสระจากผู้ควบคุมเครื่องหรือไม่

ข. สามารถที่จะส่งข้อมูลมาปฏิบัติโดยวิธีใดที่อาจจะหลบหลีกการตรวจความถูกต้องหรือไม่

ค. มีการทำรายงานการตรวจสอบความถูกต้องของข้อมูลหรือไม่ ในรายงานนั้นมีการทำรายละเอียดการแก้ไขหรือไม่ มีการเก็บรักษาไว้ให้ผู้ตรวจสอบภายในตรวจตราหรือไม่

ง. มีการติดตามผลการแก้ไขข้อผิดพลาดในทุกกรณีหรือไม่ มีการควบคุมอย่างใดเพื่อให้แน่ใจว่า Input Data ที่ผิดได้รับการแก้ไขแล้วส่งกลับมา Re - process โดยไม่ชักช้า

8. มีการควบคุมทางด้านอื่น ๆ อย่างใดบ้าง

- Control
- Input Validity Test
- Seguence Test
- Limit or Reasonableness Test

9. มีการนำงานไปปฏิบัติยังศูนย์คอมพิวเตอร์ภายนอกหรือไม่ มีวิธีป้องกันการสูญหายของข้อมูลระหว่างการส่งผ่านอย่างใด

10. ศูนย์คอมพิวเตอร์รับงานจากภายนอกมาทำบ้างหรือไม่ ถ้ารับมีวิธีควบคุมอย่างไรมิให้ข้อมูลปนกับข้อมูลภายใน

11. ถ้ามีการส่งผ่าน Data ในระยะไกล (Telecomunication) มีวิธีการอย่างไรที่จะควบคุมให้ข้อมูลที่ส่งไม่มีการสูญหาย

Processing control

1. ถ้ามีรายการผิดพลาดเกิดขึ้นมีการบันทึกรายละเอียด การผิดพลาดตลอดจนการดำเนินการแก้ไขหรือไม่ และมีการตรวจสอบจากบุคคลที่เป็นอิสระจาก Operator หรือไม่

2. หากการใช้ Batch total ถ้าพบว่ายอดรวมที่ได้จากการปฏิบัติข้อมูลแตกต่างจากยอดรวมที่คำนวณก่อนล่วงหน้าจะดำเนินการแก้ไขอย่างใดก่อนที่จะทำการปฏิบัติข้อมูลต่อ

3. ถ้ามีคาดว่าระยะเวลาที่จะปฏิบัติข้อมูลงานใดงานหนึ่ง เกิน 30 นาที มีการเตรียมการอย่างใดในการ Restarting program ถ้าเกิดการ Interrupted เช่นกระแสไฟขัดข้อง

การควบคุมทางด้าน Output

1. มีการใช้มาตรการอะไรในการตรวจสอบผลของการปฏิบัติข้อมูล

2. ถ้ามีการใช้ control total ใครเป็นผู้ตรวจสอบว่ายอดที่ตระเตรียมเท่ากับยอดที่ได้รับจากการปฏิบัติข้อมูล ถ้าพบว่าไม่ตรงกัน มีมาตรการแก้ไขอย่างไรก่อนที่จะแจกจ่าย Output ไปยังผู้ใช้

3. ข้อมูลใน Output มีรายละเอียดเพียงพอที่จะสอบกลับไปยังเอกสารเบื้องต้นหรือไม่ และเพียงพอที่จะยืนยันความถูกต้องของ Control total หรือไม่ มีการเก็บรักษาเอกสารเบื้องต้นไว้ชั่วระยะหนึ่งจนกว่าจะแน่ใจว่า Output Output นั้นถูกต้องสมบูรณ์หรือไม่

4. ถา Output จากการปฏิบัติข้อมูลถูกส่งไปเป็น Input ของอีกขบวนการปฏิบัติข้อมูลหนึ่งโดยตรงมีการเก็บรักษา Audit trails ไว้โดยครบถ้วนหรือไม่ และยังคงรักษา Control totals หรือไม่

5. ใครเป็นผู้รับหรือเก็บ Output ก่อนที่จะทำการแจกจ่าย

6. มีมาตรการอย่างใดในการควบคุมการแจกจ่าย Output (โดยเฉพาะการแจกจ่าย Output ที่เป็นเช็ค เช่น เช็คเงินเดือน)

ก. มีการทำทะเบียนแจกจ่าย Output หรือไม่

ข. มีการทำหมายกำหนดการล่วงหน้าระบุจำนวน Copy ของ Output ที่ต้องการและรายชื่อผู้ควรได้รับ Output หรือไม่

ค. ผู้ใช้มารับ Output เอง มีการตรวจหลักฐานการขอรับหรือบัตรแสดงตนก่อนยินยอมให้รับ Output หรือไม่

ง. มีวิธีการทำลาย Output ที่มีใช้อย่างใดโดยเฉพาะรายการที่เป็นรายงานทางการเงิน

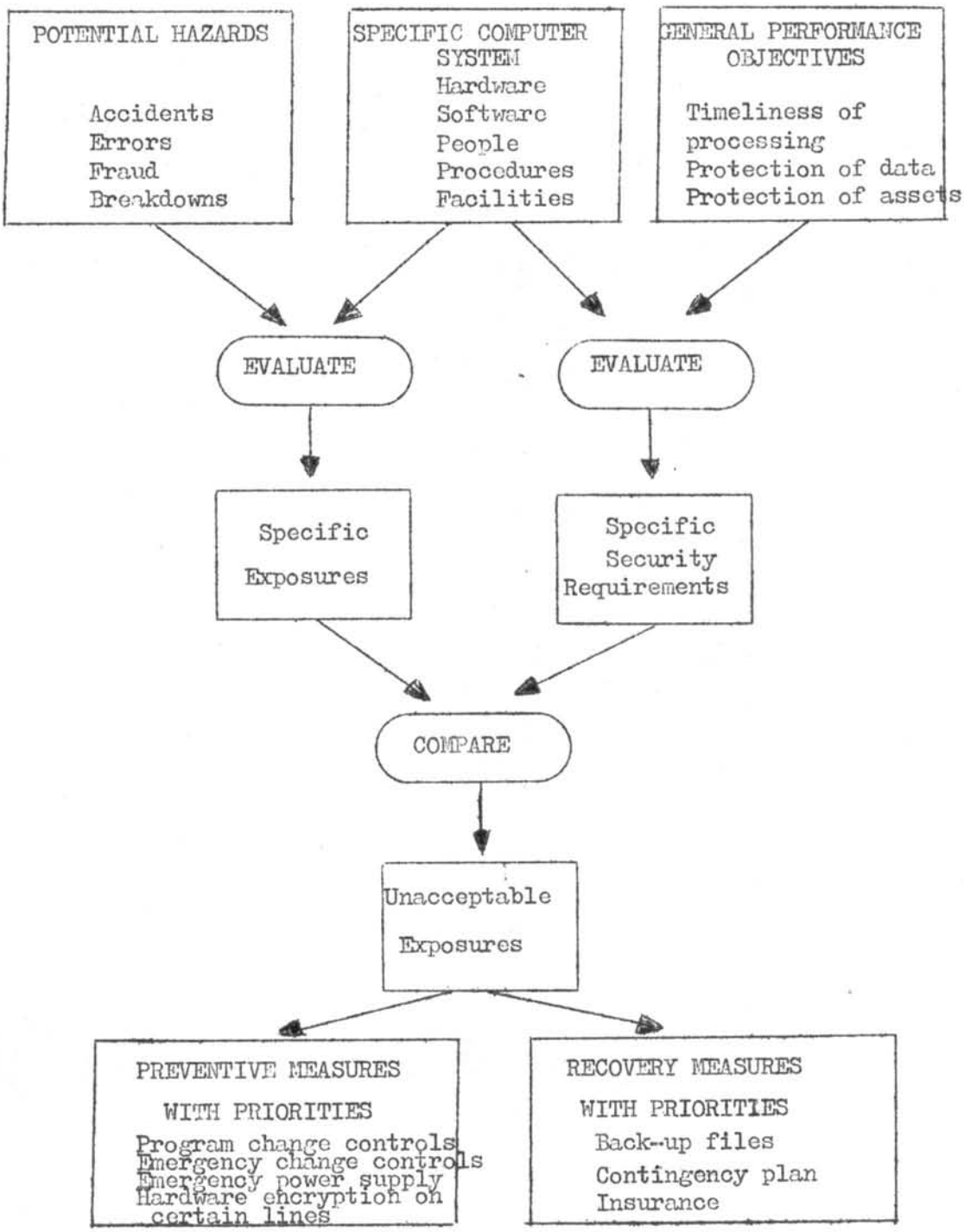
7. มีการควบคุมเอกสาร Output บางประเภท เช่น เช็คเปล่าที่จะใช้พิมพ์รายการจ่ายเงินเดือนหรือไม่ มีการลงเลขลำดับล่วงหน้าและทะเบียนควบคุมหรือไม่ มีการเก็บรักษาอย่างใด ใครเป็นผู้รับผิดชอบ

8. หน่วยตรวจสอบภายในได้ Sampling ความถูกต้องของ Output เป็นระยะตามหลักวิชาโดยสม่ำเสมอหรือไม่

9. มีการสอบถามผลการดำเนินงานกับแผนกอื่นหรือไม่

ภาคผนวก ข.

การวิเคราะห์ความเสี่ยงภัยของความปลอดภัยในระบบคอมพิวเตอร์



ภาคผนวก ค.

Summary of the United States
Fair Credit Reporting Act of 1971

Compilers of credit and "investigative" reports must:

Eliminate from their reports bankruptcies after 14 years and other adverse information after 7 years.

Keep record entries on employment up to date; confirm adverse interview information 3 months before reporting it.

Notify subject that report is being made; whenever employment or credit is denied on basis of report, subject must be advised of reporting agency must disclose "nature and substance" of material in file (but not file itself); must disclose sources of data; must reinvestigate item at subject's request; if agency does not correct item, must include subject's statement on it.

Maintain "reasonable procedures" to grant reports only to those with "reasonable interest."

Agency must not, without written consent of subject, furnish to government agency more than name, address, and place of employment of subject except when government has "legitimate business need."

ภาคผนวก ข.

Summary of the United States Federal Privacy Bill of 1973

Any government agency that maintains records on individuals must:

Notify individual that record exists.

Notify individual regarding all transfers of information in files.

Disclose information from such records only with consent of individual.

Record names and positions of all persons inspecting such records, and their reasons.

Permit individual to inspect records, make copies of them, and supplement them.

Remove erroneous or misleading information from individual's file.

Bill creates a Federal Privacy Board to hear complaints on any of above requirements.

Exceptions are made in case of national security and police files.

The President shall report to Congress each year on the number of records exempted in each agency.

ภาคผนวก ข.

Summary of the British
Data Surveillance Bill of 1969

Registrar

A Registrar shall be established to keep a register of all data banks (including those government, corporations, credit bureaus, private detective agencies, and any persons who sell information)

The register shall contain details of the data kept, the person responsible, the purpose for which they may be used and by whom.

Only data relevant to the stated purpose may be stored.

The register shall be open to inspection by the public and press.

Any person about whom data are stored shall receive a printout of that data and the purposes for which they are kept when the data bank is established.

Thereafter he may obtain a printout of the data, their purposes, and a listing of all receipients on payment of a fee.

Any person may apply for an order that data about him be removed on grounds that they are inaccurate, unfair, or out of date.

If data are found to be inaccurate, unfair, or out of date, all recipients will be notified.

Offences

It is a punishable offence.

not to accurately register a data bank.

to use the data for nonregistered purposes.

to allow access to persons other than those entered on the register.

to aid and abet the wrong use of the data.

Liability

The operator of a data bank is liable for damages when he permits inaccurate data to be supplied that can cause a person harm.

ประวัติการศึกษา

นางสาวทิพวัลย์ เชื้อชาว เกิดวันที่ 27 ตุลาคม พ.ศ. 2494 ที่จังหวัดเชียงใหม่ ได้รับปริญญาวิทยาศาสตรบัณฑิต (คณิตศาสตร์) จากคณะวิทยาศาสตร์ มหาวิทยาลัยเชียงใหม่ ในปี พ.ศ. 2515