บทที่ 3

ระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะที่เกี่ยวกับคอมพิวเตอร์

ดังได้กล่าวมาแล้วว่า จุดประสงค์ของการนำเอาคอมพิวเตอร์มาช่วยงานก็ต้องการให้ได้ข้อมูลที่ถูกต้อง เพื่อจะนำระบบข้อมูลที่ถูกต้องนี้มาช่วยในการวางแผนและการควบคุม การวิเคราะห์ตัดสินใจ การกำหนดแนวนโยบายหรืองานอื่น ๆ ที่ทำในหน้าที่ ระบบข้อมูลที่ถูกต้องจะต้องอาศัยระบบความปลอดภัย ความถูกต้องและความลับเฉพาะทั้งด้านตัวระบบคอมพิวเตอร์เอง ด้านลักษณะต่าง ๆ ภายนอกที่เกี่ยวข้องและสถานที่ใช้ปฏิบัติงาน รวมทั้งด้านการจัดการควบคุมงานในด้านบริหารตลอดจนเจ้าหน้าที่ที่ปฏิบัติงาน ซึ่งแต่ละด้านจะต้องใช้เทคนิค แนวทางต่าง ๆ และวิธีปฏิบัติแตกต่างกันไป แล้วแต่ความเหมาะสมกับลักษณะของงานที่ทำ หน่วยงานคอมพิวเตอร์ ระบบเครื่องที่ใช้ งบประมาณที่มีอยู่ ฯลฯ เป็นต้น

3.1 ระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะในด้านระบบคอมพิวเตอร์

ระบบด้านนี้เป็นชั้น (layer) ในสุดคือเป็นชั้นที่ใกล้อยู่ในตัวเครื่องคอมพิวเตอร์ ชั้นนี้จะต้องทำให้ดีที่สุดและเป็นชั้นที่สำคัญกว่าชั้นอื่น ๆ ซึ่งชั้นรอบนอกออกไปจะช่วยเสริมระบบนี้ให้มั่นคงเท่านั้น ถึงแม้การวางระบบชั้นนอก ๆ จะดีที่สุด แต่ในตัวระบบคอมพิวเตอร์เองไม่ดี การประมวลผลข้อมูลนั้นก็จะไม่ดี ดังนั้น จะต้องระมัดระวังการออกแบบในส่วนนี้ให้ดีที่สุด

องค์ประกอบของระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการประมวลผลข้อมูลได้แก่

- เครื่องจักรอุปกรณ์ (Hardware) เช่น CPU, Peripheral ได้แก่ หน่วยรับและส่งข้อมูลทั้งหมด ยกเว้น CPU และ Data Preparation ได้แก่ เทปแม่เหล็ก จานแม่เหล็ก บัตร และอุปกรณ์ปลายทาง เป็นต้น

– ระบบโปรแกรม (Software) เช่น ระบบควบคุมและการปฏิบัติงาน (Operation System) Package และโปรแกรมทั้งหลายที่ใช้ในการปฏิบัติงานตลอดจนภาษาที่ใช้ เป็นต้น

– ข้อมูล (File and data) เช่น ข้อมูลธรรมดา (Conventional File) ฐานข้อมูล (Data base) เป็นต้น

ในที่นี้จะกล่าวถึงด้านข้อมูลเป็นส่วนใหญ่ ส่วนด้านเครื่องจักรอุปกรณ์และระบบโปรแกรมในที่นี้จะกล่าวถึงเพียงเล็กน้อย เพราะด้านเครื่องจักรอุปกรณ์นั้นปกติผู้สร้าง ผู้ออกแบบระบบก็จะมีระบบการตรวจสอบภายในตัวของมันเองอยู่แล้ว ถ้าเกิดข้อผิดพลาด ความไม่ถูกต้องก็จะสามารถแก้ไขได้ ส่วนด้านระบบโปรแกรมก็เช่นเดียวกัน

3.1.1 <u>ระบบความปลอดภัยที่สร้างขึ้นในโปรแกรมระบบ</u> เนื่องจากปัจจุบันในหลายประเทศการดำรงชีวิตของมนุษย์กำลังเคลื่อนเข้าสู่ยุคที่ทุกย่างก้าวของชีวิตจำเป็นต้องใช้คอมพิวเตอร์ มนุษย์ทุกอาชีพจะต้องใช้คลังข้อมูล บางประเทศได้มีการสำรวจเพื่อวางแผนควบคุมข่ายคอมพิวเตอร์แห่งชาติขึ้น ในด้านธุรกิจและการลงทุนของเอกชน เช่น บริษัทโทรคมนาคม บริษัทผู้ผลิตคอมพิวเตอร์และบริษัทอื่นที่เกี่ยวข้อง ได้มีการวางแผนงานเกี่ยวกับการบริการคอมพิวเตอร์ เช่น การใช้เช่าอุปกรณ์ติดต่อ (เหมือนกับการให้เช่าโทรศัพท์) และการคิดค่าเช่าตามเวลาที่ใช้คอมพิวเตอร์ อุปกรณ์รับ – ส่งข้อมูลรวมทั้งโทรศัพท์แบบกดปุ่ม โทรพิมพ์ และอุปกรณ์ปลายทางคอมพิวเตอร์พิเศษอื่น ๆ ตลอดจนขายบริการ การให้บริการด้านเวลาที่ใช้คอมพิวเตอร์ และข่าวสารที่ต้องการโดยใช้อุปกรณ์ปลายทางเรียกข่าวสารนั้น

การวางแผนเกี่ยวกับการแบ่งเวลาเพื่อใช้คอมพิวเตอร์เป็นสาธารณประโยชน์ได้มีการเริ่มใช้หลายปีและได้รับความสำเร็จเป็นอย่างดี ซึ่งก้าวต่อไปของแผนงานก็คือการปรับปรุงเครื่องคอมพิวเตอร์ขนาดใหญ่ เชื่อกันว่าอีกไม่นานนัก การใช้งานคอมพิวเตอร์จะถึงจุดวิกฤตคือเมื่อคอมพิวเตอร์เป็นที่ยอมรับของคนทั่วไปจนต้องมีการผลิตออกขายเป็นอุตสาหกรรม และเมื่อถึงตอนนี้วิทยาการเกี่ยวกับคอมพิวเตอร์จะต้องเจริญขึ้นอย่างมาก ระบบคอมพิวเตอร์ต่าง ๆ จะเจริญก้าวหน้า จะมีการเพิ่มจำนวนขึ้น

อย่างรวดเร็ว และมีการเชื่อมโยงระหว่างกัน ข่ายคอมพิวเตอร์จะแผ่กระจายไปทั่วประเทศ การใช้คอมพิวเตอร์จะขยายไปในสาขาของงานต่าง ๆ มากมาย เราจะเห็นผู้ใช้ในสาขาต่าง ๆเหล่านี้เพิ่มโปรแกรมและข้อมูลต่าง ๆ ลงในแฟ้มข้อมูลที่ใช้เพื่อสาธารณะ จะมีการเขียนโปรแกรมขายให้แก่บริษัทคอมพิวเตอร์ จะได้โปรแกรมที่ดีและก้าวหน้าจำนวนมาก

เป็นที่คาดหมายกันว่าประเทศไทยต่อไปจะมีความก้าวหน้าครั้งสำคัญเกิดขึ้นในด้านการพัฒนานำเอาคอมพิวเตอร์ระบบ Real - time มาใช้กันอย่างแพร่หลาย อาจจะมีการตั้งบริษัทคอมพิวเตอร์ที่เปิดให้บริการแบบ Time sharing ซึ่งขายบริการด้านเวลาที่ใช้คอมพิวเตอร์และข่าวสารต่าง ๆ โดยใช้รหัสลับ หรือคำผ่าน (Password) และอุปกรณ์ปลายทาง หรืออาจจะมีการตั้งศูนย์คอมพิวเตอร์แห่งชาติขึ้น จะทำให้ระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะของระบบคอมพิวเตอร์มีบทบาทมากยิ่งขึ้น ซึ่งหน่วยงานต่าง ๆ และบุคคลทั้งหลายสามารถจะใช้ประโยชน์จากการสื่อสารข้อมูลจากระบบเหล่านี้ เช่น

ก. ทางราชการ ใช้ในการคำนวณโครงการ การเก็บและค้นหาข้อมูลอย่างมีประสิทธิภาพ เป็นต้น

ข. ธนาคาร ใช้ในการจัดทำธุรกิจด้านการเงิน ทำให้สดวกต่อลูกค้าในการเบิกเงินตามสาขาต่าง ๆ การจ่ายเงิน การโอนเงินหลาย ๆ อย่างจะทำได้โดยไม่ต้องใช้เงินสดหรือเช็ค ลูกค้าของธนาคารจะต้องมีวิธีการบางอย่างที่แสดงตนให้เครื่องอุปกรณ์ปลายทางรู้ว่าตนเป็นใคร คอมพิวเตอร์ก็จะทำตามขั้นตอนทุกอย่าง เป็นต้น

ค. นักวิทยาศาสตร์และวิศวกร ใช้ในการออกแบบโครงสร้างอาคารและการเก็บข้อมูล เป็นต้น

ง. วงการธุรกิจและอุตสาหกรรม ที่ใช้คอมพิวเตอร์ในการควบคุมวัสดุขั้นตอนการผลิต และช่วยในการตัดสินใจของผู้บริหาร เป็นต้น

จ. นักเรียนและนักศึกษา อาจใช้เครื่องโทรศัพท์แบบกดปุ่มให้คอมพิวเตอร์สอนวิชาต่าง ๆ ได้ หรือให้ตอบปัญหาต่าง ๆ โดยให้คำตอบเป็นเสียงพูดผ่านหูฟังของโทรศัพท์ได้ ฯลฯ

โดยทั่วไปคอมพิวเตอร์ระบบ Real – time นั้น คอมพิวเตอร์จะถูกโปรแกรมเอาไว้และการเข้าถึงคอมพิวเตอร์เพื่อเรียกใช้คอมพิวเตอร์นั้นสามารถทำได้โดยโทรศัพท์ หมายเลขโทรศัพท์นี้จะไม่ปรากฏอยู่ในสมุดโทรศัพท์และถือเป็นความลับสุดยอด เฉพาะผู้มีอำนาจเท่านั้นที่จะรู้หมายเลขนี้ การติดต่อกับคอมพิวเตอร์นั้น ขั้นแรกหมุนหมายเลขโทรศัพท์เรียกคอมพิวเตอร์ จากนั้นก็ให้รหัสคำผ่านเพื่อแสดงให้คอมพิวเตอร์ทราบว่าเป็นบุคคลที่มีสิทธิจะใช้มัน เมื่อคอมพิวเตอร์ตรวจสอบแล้วว่าถูกต้อง จึงจะเริ่มรอรับคำสั่งที่จะป้อนให้กับมัน ถ้าบังเอิญบุคคลภายนอกไปพบหมายเลขโทรศัพท์นี้เข้าและสามารถให้คำผ่านที่ถูกต้องได้ คอมพิวเตอร์ก็จะทำงานให้เหมือนกัน

การติดต่อนี้ซึ่งผู้ใช้หมุนโทรศัพท์ต่อไปยังศูนย์รวมข้อมูลและคอมพิวเตอร์โดยใช้โปรแกรมหรือข้อมูลเฉพาะที่กำหนดไว้ให้นั้นจะทำให้การปฏิบัติงานสดวกง่ายขึ้นโดยผู้ที่ใช้บริการของคอมพิวเตอร์อาจจะได้มีการเก็บข้อมูลของตนเป็นเอกเทศไว้ที่ศูนย์คอมพิวเตอร์จะต้องจัดให้มีแฟ้มข้อมูลสำหรับระบบ On – line สำหรับข้อมูลแต่ละชนิดและมีวิธีการค้นหาแฟ้มข้อมูลแต่ละชนิดโดยวิธีอัตโนมัติ เช่น แฟ้มข้อมูลทางการค้าและเศรษฐกิจจะถูกซักถามเพื่อการวางแผนทางธุรกิจ เอกชนผู้ลงทุนจะตรวจสอบสมมุติฐานของตนเพื่อพิจารณาว่าจะสามารถทำเงินได้อย่างไรในตลาดหุ้นที่ผ่านมา เป็นต้น

จากที่กล่าวมาแล้วจะเห็นว่าระบบ Real – time เป็นระบบที่ผู้ใช้หลายรายเก็บข้อมูลในระบบคอมพิวเตอร์เดียวกัน แฟ้มข้อมูลบางวันอาจใช้รวมกัน แฟ้มข้อมูลบางอันอาจเป็นความลับของผู้ใช้แต่ละราย การกำหนดให้ผู้ใช้แต่ละรายสามารถเข้าถึงเฉพาะแฟ้มข้อมูลที่ตนมีสิทธิ์ใช้โดยไม่อาจล่วงเลยไปถึงแฟ้มข้อมูลที่เป็นความลับของผู้อื่นเป็นสิ่งที่ต้องระมัดระวังอย่างมาก ตลอดจนการขโมยข่าวสารของผู้อื่นก็ต้องมีการเข้มงวดอย่างจริงจัง ในที่นี้จะเป็นเฉพาะความปลอดภัยในระบบ Real – time มากกว่าระบบประมวลผลเป็นชุด ๆ เพราะระบบนี้ง่ายต่อการควบคุม

จากการที่มีการขยายขอบเขตของการใช้เพิ่มขึ้น ดังนั้นจะมีระบบความปลอดภัยที่สร้างขึ้นในระบบโปรแกรมหลักเพื่อเป็นระบบที่ควบคุมการปฏิบัติงาน ได้แก่

ก. วิธีการตรวจหาผู้ใช้ (Identification the user)

ข. ระดับของการให้สิทธิการใช้ (Level of Authorization)

ค. การบันทึกรายการต่าง ๆ ที่เกิดขึ้น (Logging or Journaling)

ก. <u>วิธีการตรวจหาผู้ใช้</u> ในระบบ Real - time มักจะมีวิธีให้ผู้ใดก็ตามที่จะใช้เครื่องแสดงตนว่าผู้นั้นเป็นใคร และมีสิทธิในการใช้เครื่องเพียงใด เพื่อควบคุมให้เฉพาะผู้มีสิทธิเท่านั้นซึ่งจะสามารถใช้เครื่องวิธีการตรวจหามีหลาย ๆ แบบ เช่น

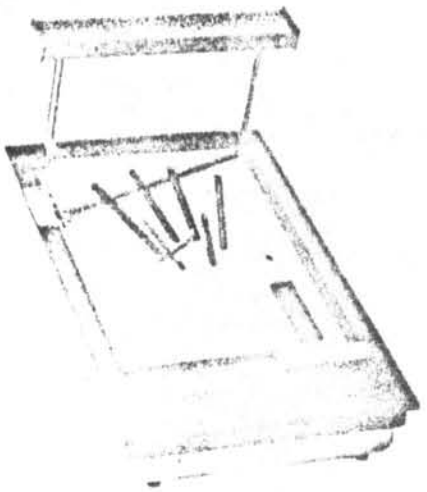
1. ตรวจสอบหาลักษณะเฉพาะบางอย่างของผู้ใช้ ได้แก่ลายมือ เสียงพูด วิธีการนี้ยังใช้น้อยมาก และเสียค่าใช้จ่ายสูง ปัจจุบันยังอยู่ในระหว่างการวิจัย ในที่นี้จะไม่กล่าวถึง

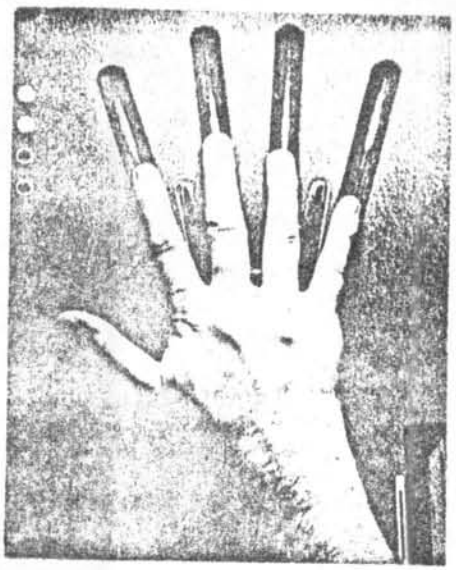
2. ตรวจสอบคำผ่านของผู้ใช้ โดยผู้ใช้แจ้งคำผ่านเฉพาะของตนเองเข้าเครื่องก่อนที่จะเข้าถึงแฟ้มข้อมูลใด ๆ ที่ต้องการ วิธีนี้เสียค่าใช้จ่ายน้อยมาก ในที่นี้จะใช้วิธีนี้เป็นส่วนใหญ่

3. ตรวจสอบจากสิ่งของต่าง ๆ เช่น แผ่นเหรียญ บัตรเครดิต กุญแจ เป็นต้น โดยหย่อนอุปกรณ์เหล่านี้ลงในอุปกรณ์ที่รับข้อมูลเฉพาะของมัน บนอุปกรณ์เหล่านี้จะบรรจุรหัส รายละเอียดที่ใช้เฉพาะเจาของแต่ละบุคคล บางทีอุปกรณ์ปลายทางบางระบบหลายใช้วิธีตรวจหาผู้ใช้หลายวิธีปนกัน เช่น ระบบล็อคด้วยกุญแจที่มีรหัสและระบบใช้บัตรรหัส เป็นต้น ปกติระบบเหล่านี้จะมีรายละเอียดที่อยู่บนอุปกรณ์ที่เรียกใช้เป็นข้อความความลับ ดังนั้น ผู้ใช้ต้องระวังไม่ให้ผู้อื่นเห็น หรือลืมทิ้งไว้ที่ตำแหน่งอุปกรณ์ปลายทางนั้น

วิธีการตรวจหาผู้ใช้แสดงดังรูป 3.1 ถึง 3.5

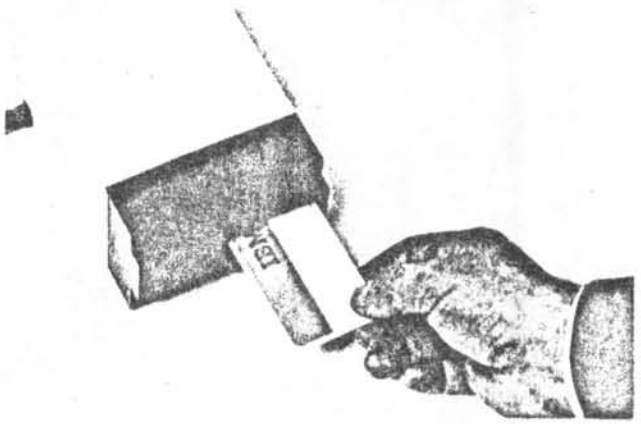
ข. <u>ระดับของการให้สิทธิการใช้</u> ในระบบ Real - time หลังจากที่ผู้ใช้ได้เรียกใช้คอมพิวเตอร์แล้ว ปัญหาต่อไปก็คือว่า โปรแกรมอะไรที่ผู้ใช้สามารถใช้ได้ และแฟ้มข้อมูลอะไรที่ผู้ใช้มีสิทธิใช้ จะเห็นว่าถ้ากรณีที่ผู้ใช้ใช้งานเฉพาะโปรแกรมของเขาและใช้ข้อมูลของเขาแล้ว ระบบความปลอดภัยก็จำเป็นที่ต้องจำกัดเฉพาะการใช้ข้อมูล





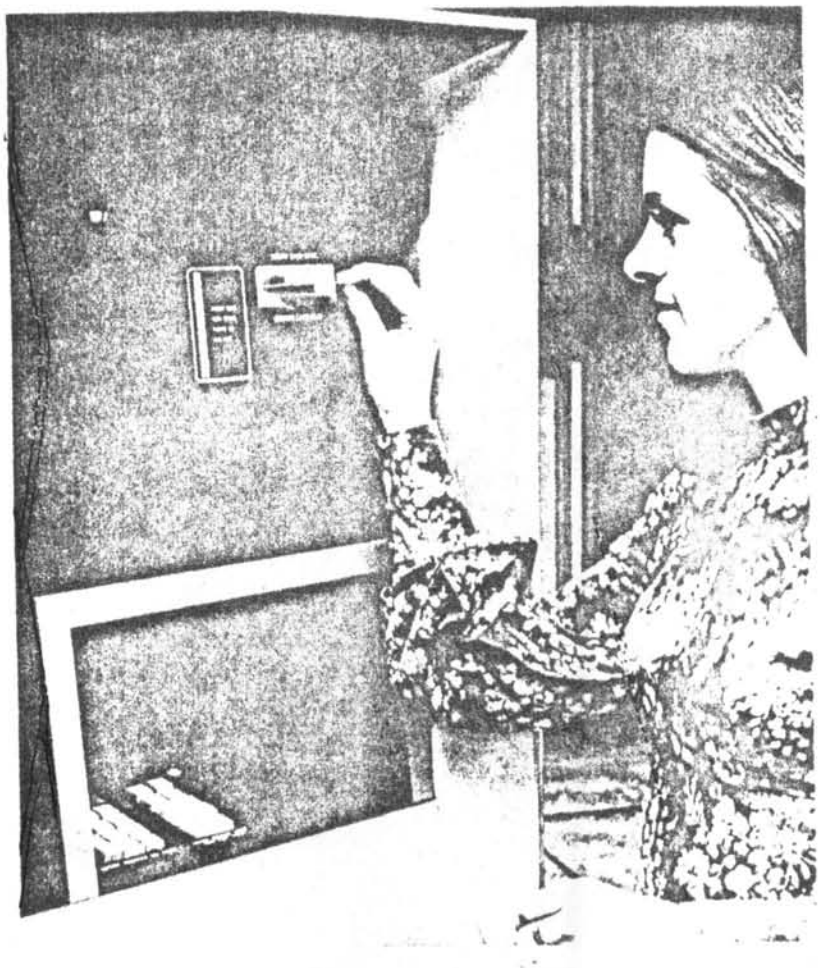
รูป 3.1 การตรวจลักษณะบางอย่างของผู้ใช้ เช่น ลายมือ

รูป 3.2 การตรวจบัตรเครดิตของผู้ใช้ในร้านขายของ

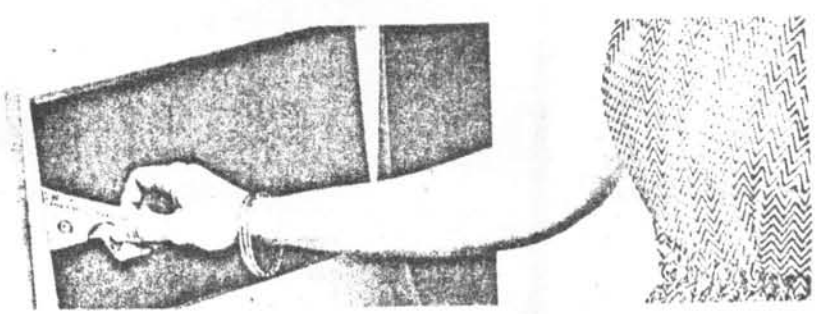


รูป 3.3 การตรวจบัตรของผู้ใช้โดยผ่านเครื่องอ่านบัตร

รูป 3.4 การตรวจบัตรของผู้ใช้เพื่อติดต่อข้อมูล

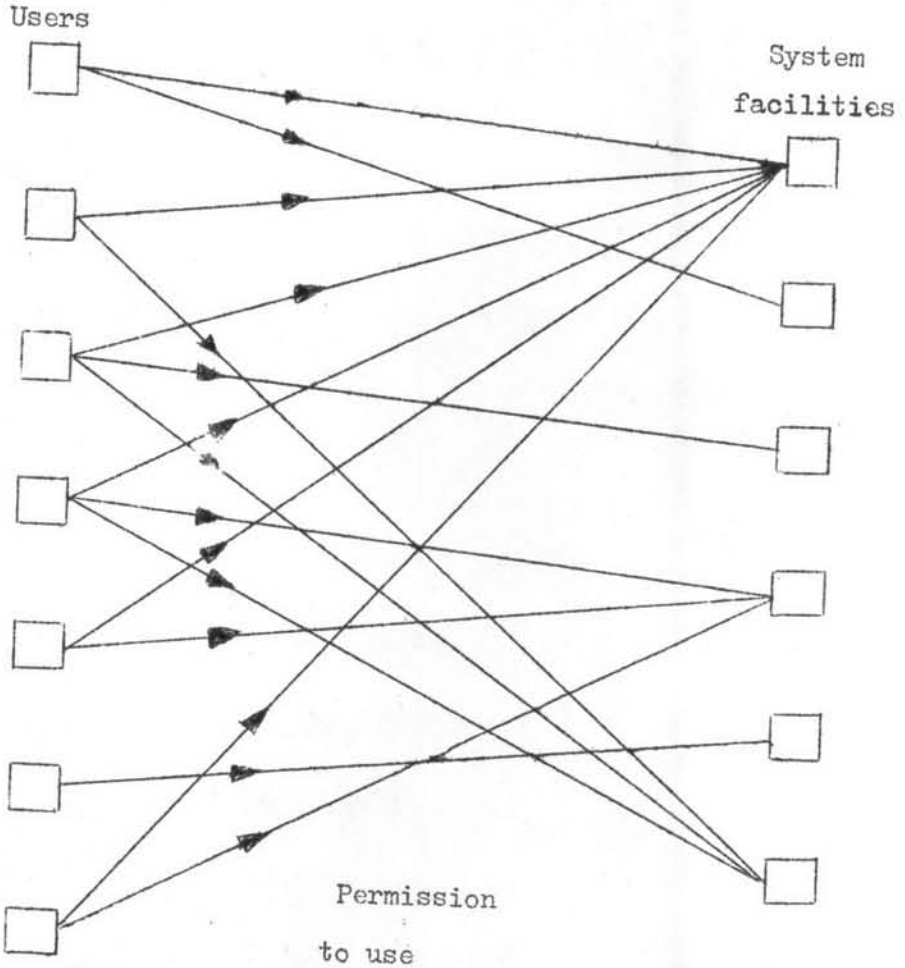


รูป 3.5 การตรวจบัตรของผู้ใช้ในกรณีถอนเงินจากธนาคาร



ของเขาก็พอ แต่สำหรับกรณีนี้โปรแกรมและแฟ้มข้อมูลถูกใช้โดยผู้ใช้หลายคน ระดับของการให้สิทธิการใช้มีความจำเป็นที่จะต้องนำมาพิจารณาซึ่งขึ้นกับรายละเอียดที่ผู้ใช้กำหนดขึ้นมาเพื่อเรียกให้เครื่องทำงาน

เมื่อโปรแกรมถูกใช้ร่วมกัน ผู้ใช้แต่ละคนจะถูกกำหนดให้ขึ้นกับระดับของการให้สิทธิการใช้ ซึ่งจะหาว่าโปรแกรมอะไรที่เขาสามารถใช้ได้ หรือเขาสามารถจะเปลี่ยนแปลงหรือแก้ไขโปรแกรมได้ในระดับไหนตามความต้องการของเขา การมีสิทธิใช้ของผู้ใช้แต่ละคนจะแสดงได้ด้วยตารางการให้สิทธิการใช้ (Authorization tables) ตามรูป 3.6

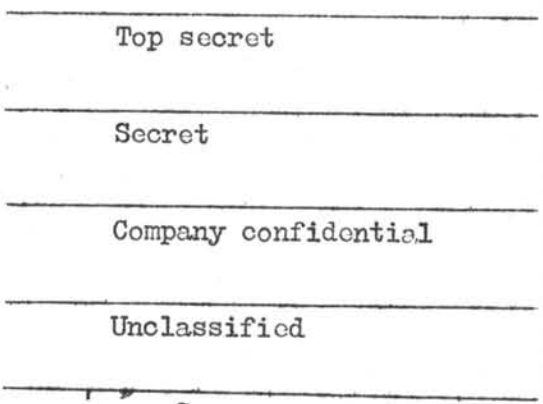


รูป 3.6 ตารางแสดงการให้สิทธิการใช้ข้อมูลหรือโปรแกรม

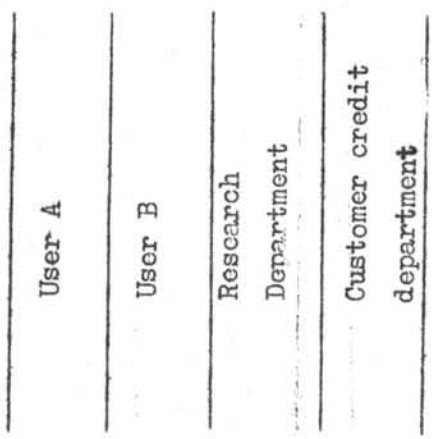
ระบบของการให้สิทธิการใช้ (Authorization system)แบ่ง 2 พวก คือ

1. Stratification ได้แก่ข้อมูลที่แบ่งตามแนวราบ คือแบ่งเป็นระดับ (Level) เช่น ข่าวสารที่ลับที่สุด ลับ ฯลฯ ตามรูป 3.7

2. Compartmentalization ได้แก่ข้อมูลที่แบ่งตามแนวดิ่ง คือแบ่งเป็นประเภท (Category) เช่น ข่าวสารประเภทนี้ใช้ได้เฉพาะผู้ใช้ A หรือใช้ได้เฉพาะหน่วยงานวิจัย ฯลฯ ตามรูป 3.8

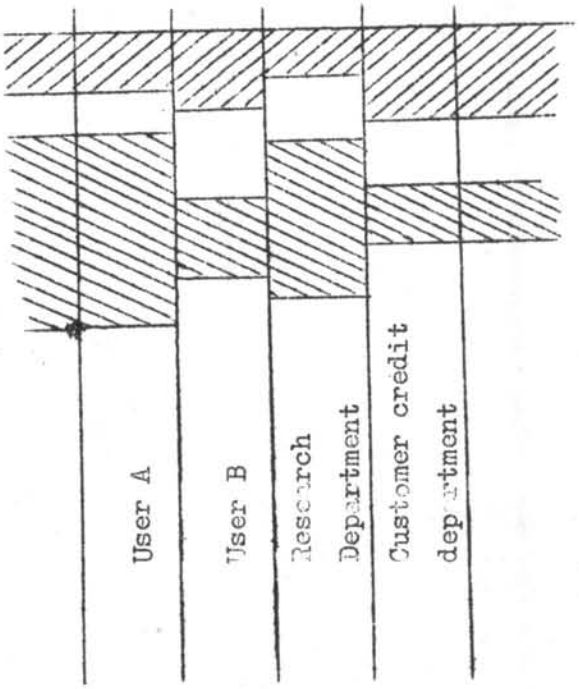


รูป 3.7 การแบ่งข้อมูลโดยแยกตามระดับ



รูป 3.8 การแบ่งข้อมูลโดยแยกตามประเภท

ในระบบงานจริง ๆ มักจะเอาทั้ง 2 ระบบ มารวมกันได้ตามรูป 3.9



รูป 3.9 โครงสร้างของการให้สิทธิการใช้ข้อมูล

ระดับการให้สิทธิการใช้ของผู้ใช้แต่ละคน ปกติจะเกิดขึ้นเมื่อผู้ใช้ให้สัญญาณ อาจโดยวิธีใช้คำผ่าน หรือรหัสชนิดอื่น ผ่านไปยังตารางที่มีรายละเอียดเกี่ยวกับระดับการให้สิทธิการใช้แก่ผู้ใช้ ก่อนที่ผู้ใช้เรียกใช้แล้วจึงจะได้รายละเอียดที่ตนต้องการ เครื่อง (ในที่นี้ก็คือโปรแกรม) ก็จะตรวจว่าถูกต้องหรือไม่ ถ้าถูกต้องจึงจะยอมให้ใช้ ปกติระดับการให้สิทธิการใช้จะแสดงด้วยตารางที่เรียกว่า ตารางแสดงการให้สิทธิการใช้แก่ผู้ใช้ (User's authorization table) ซึ่งประกอบด้วยรายละเอียด เช่น

- โปรแกรมที่ผู้ใช้มีสิทธิใช้
- ข้อมูลที่ผู้ใช้จะเรียกใช้ได้ (Read)
- ข้อมูลที่ผู้ใช้สามารถแก้ไขได้ (Modify)
- ชนิดของข้อมูลที่ผู้ใช้สามารถนำเข้าไปแก้ไข
- ประเภทของข้อมูลที่ผู้ใช้จะเรียกใช้ได้
- ประเภทของข้อมูลที่ผู้ใช้จะแก้ไขได้ เป็นต้น

ตารางที่แสดงรูปแบบการให้สิทธิการใช้ (Authorization matrix) เป็นหัวใจของระบบความปลอดภัยซึ่งจะแสดงรายละเอียดถึงผู้ใช้คนใดที่มีสิทธิใช้ในระดับไหน ได้รับข่าวสารอะไร โดยมีจำนวน Bits ในแต่ละข่าวสารเป็นตัวกำหนด เช่น ถ้าใช้ 2 Bits

- ถ้า 2 Bits ที่มีค่า = 01 ผู้ใช้มีสิทธิ 'READ' ข้อมูลนี้
- ถ้า 2 Bits ที่มีค่า = 10 ผู้ใช้มีสิทธิ 'WRITE' ข้อมูลนี้
- ถ้า 2 Bits ที่มีค่า = 11 ผู้ใช้มีสิทธิ 'READ and WRITE' ข้อมูลนี้
- ถ้า 2 Bits ที่มีค่า = 00 ผู้ใช้ไม่มีสิทธิในข้อมูลนี้เลย

ตัวอย่างตามตาราง 3.1 (4) ผู้ใช้ฝ่าย Personnel มีสิทธิที่จะเรียกข้อมูลในด้าน Employee address มาใช้ (READ) และในขณะเดียวกันก็มีสิทธิแก้ไขข้อมูลในด้าน Employee address (WRITE) เช่น กรณีลูกจ้างย้ายที่อยู่ เป็นต้น

นอกจากนี้ตารางแสดงถึงรูปแบบการให้สิทธิการใช้อาจอยู่ในรูปอื่น ๆ ได้หลายแบบ เช่น ทางด้านแถวราบจะแสดงถึงกลุ่มของผู้ใช้ และทางด้านแถวดิ่งแสดงถึงประเภทข้อมูลที่จะได้รับ โดยมีรหัสที่ใช้เรียก (request code) คลุมอีกชั้น ดังตาราง 3.2

ในการที่ผู้ใช้เรียกใช้ข้อมูลครั้งหนึ่ง ๆ นั้น จะต้องใช้ตารางที่แสดงถึงการให้สิทธิการใช้หลายตารางพร้อมกันโดยจะมีจำนวน Bit ใด Bit หนึ่งเป็นตัวชี้ (Pointers) เพื่อเชื่อมโยงระหว่างตารางเหล่านั้น ดังตาราง 3.4 โดยทั่วไปข้อมูลที่แสดงถึงรายละเอียดของตารางที่แสดงถึงการให้สิทธิการใช้จะเก็บไว้ในแฟ้มข้อมูลที่อยู่ในรูปรหัสทั้งหมด

ตารางที่แสดงการให้สิทธิการใช้แสดงได้อีกแบบ ตามตาราง 3.3

ตาราง 3.1 รูปแบบการใช้หลักการใช้ข้อมูล

Data Items / Terminal Locations	Employee Name	Employee Address	Employee ID Number	Employee Social Security Number	Employee Skills Profile	Employee Salary History	Employee Vehicle Information	Corporation Sales Projections	Prices of Parts
Personnel	11	11	11	10	11	11	00	00	00
Parking	00	00	00	00	00	00	11	00	00
Treasurer	01	00	01	01	00	11	00	00	00
Marketing	00	00	00	00	01	00	00	11	01
Purchasing	00	00	00	00	00	00	00	00	11
Research	00	00	01	00	01	00	00	00	01

ตาราง 3.2 รูปแบบการให้สิทธิการใช้ข้อมูลที่มีรหัสที่ใช้เรียก

REQUEST CODE / USER GROUP	CCUD COURT UPDATE DOCKET	CDAP DISTRICT ATTY ADD PERSON	CDAT DISTRICT ATTY ADD TRANSACT.	CDOC DISTRICT ATTY QUERY CHARGES	CDOP DISTRICT ATTY QUERY PERSON	CDUC DISTRICT ATTY UPDATE CHARGES	CDUP DISTRICT ATTY UPDATE PERSON	CBLE PUB. DEF. LIST REFERRALS	CFQH PUB. DEF. QUERY HISTORY	CIAC IN-CUSTODY ADD CUSTODY	CICT COMMITMENT DATES CALCULATOR	CILP IN-CUSTODY POPULATION COUNT	CILT IN-CUSTODY TO BE RELEASED	CIQC IN-CUSTODY QUERY COMMIT	CIUC IN-CUSTODY UPDATE CUSTODY	CPAA PERSON ADD AKA	CPAP PERSON ADD PERSON	CPOC PERSON QUERY CASE	CPQD PERSON QUERY DETAIL	CPQH PERSON QUERY HISTORY	CPQN PERSON QUERY NAME	CPOS PERSON QUERY SUMMARY	CPSE PERSON SEAL EVENT	CPSP PERSON SEAL PERSON	HELP DATA ELEMENT ASSIST	CALO ADULT PROBATION LIST COURT OUTCOMES (PROBATIONERS)	CBAE BOOKING ADD ENROUTE	CBAW BOOKING ADD WARRANT	CBLA BOOKING LIST BY ARR. AGY.	CBLE BOOKING LIST ENTIRE COUNTY	CBPP BOOKING PRINT PACKET	CBQB BOOKING QUERY BOOKING	CBQC BOOKING QUERY CHARGES	CBUB BOOKING UPDATE BOOKING	CBUC BOOKING UPDATE CHARGES	CCAC COURT ADD COMPLAINT	CCLB SUPERIOR COURT CALENDAR	CCLP COURT LIST PRISONER	CCQC COURT QUERY COMPLAINT	CCQD COURT QUERY DOCKET
Booking	X									X						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Central Identification Bureau	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Court	X	X	X	X	X	X	X	X		X					X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
District Attorney	X	X	X	X	X	X	X	X		X					X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Police	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Sheriff	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Public Defender	X	X	X	X	X	X	X	X	X	X					X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Probation	X	X	X	X	X	X	X	X		X					X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

ตาราง 3.3 ตารางแสดงการให้สิทธิการใช้แบบง่าย ๆ

MAN NUMBER	SECURITY CODE	160 AUTHORIZATION BITS

Identification number Such as Social security number or Corporate personnel number

one bit for each transaction type.

The authorization bits could be encoded with two bits per user for each transaction type, as follows:

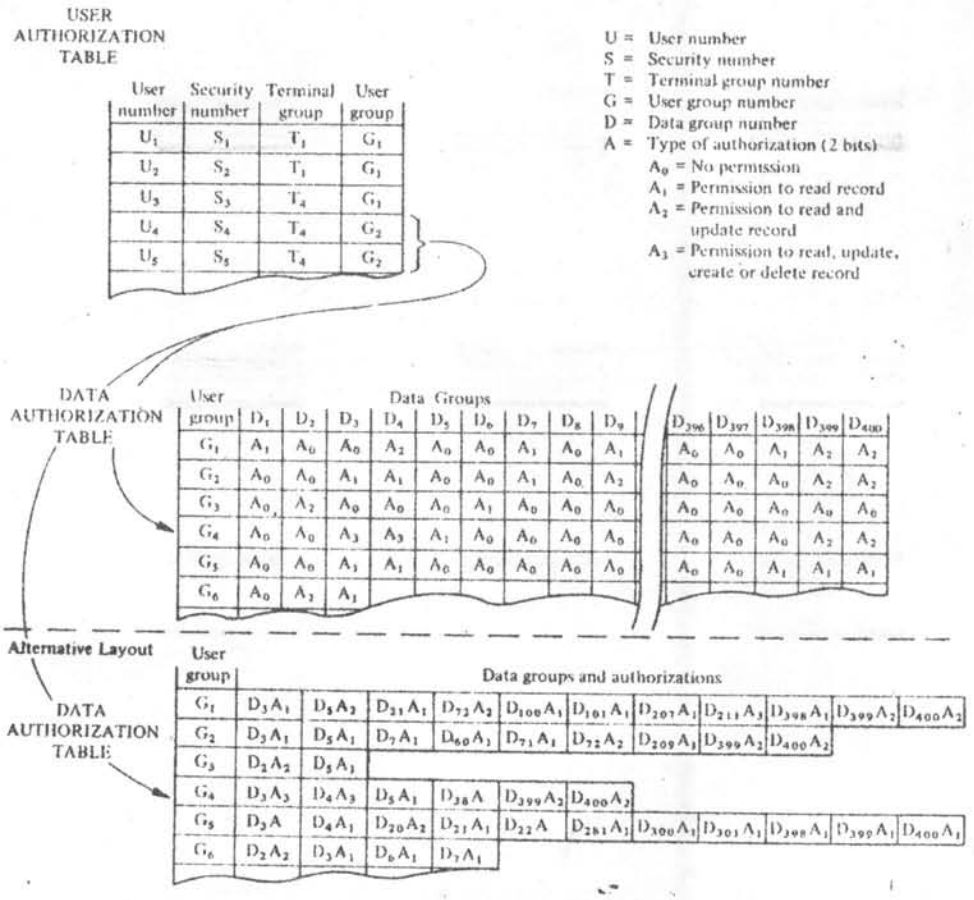
00 = No permission

01 = Permission to read records

10 = Authorization to modify records but no capability, hence permission granted to read but not write

11 = Permission to read and write records

ตาราง 3.4 ตารางการให้สิทธิการใช้โดยพิจารณาจาก user groups และ data groups



ค. <u>การบันทึกรายการต่าง ๆ ที่เกิดขึ้น</u> เป็นเทคนิคอันหนึ่งที่จะบันทึกรายละเอียดของการกระทำเกี่ยวกับด้านความปลอดภัยที่เป็นส่วนสำคัญส่วนหนึ่งในการทำให้เกิดระบบความปลอดภัย ความถูกต้อง และควบคุมลับเฉพาะในระบบประมวลผลแบบ On - line ส่วนระบบ Off - line ใช้ไม่มากนัก เหตุที่ต้องมีการบันทึกรายการต่าง ๆ ที่เกิดขึ้น เพราะเหตุดังนี้

1. ช่วยในการทำงานของผู้ตรวจสอบระบบ (auditor) เพื่อสามารถตรวจสอบข้อผิดพลาดได้ โดยดูข้อมูลที่เกิดขึ้นย้อนหลังได้

2. ช่วยในการทำให้ระบบข้อมูลกลับคืนใหม่ได้ ในกรณีที่พบว่ามีการแก้ไขเปลี่ยนแปลง (Update) หรือ การตัดทิ้ง (Delete) นั้นไม่ถูกต้อง

3. ช่วยในการสืบหาสาเหตุที่ทำให้ข้อมูลแต่ละระเบียน (Record) เกิดผิดพลาดโดยย้อนกลับไปดูใหม่

4. ช่วยทำให้แฟ้มข้อมูลกลับคืนสู่สภาพปกติในกรณีที่แฟ้มข้อมูลถูกทำลาย

5. ช่วยตรวจสอบแฟ้มข้อมูลให้ถูกต้องเมื่อพบว่าโปรแกรมที่ใช้ทำงานนั้นมีข้อผิดพลาดเกิดขึ้น ซึ่งเป็นผลเสียต่อข้อมูล

6. เป็นเครื่องวัดการทำงานที่ผิดพลาด โดยเฉพาะเรื่องที่สำคัญ ๆ ที่มีผลต่อระบบความปลอดภัย

7. เพื่อช่วยตรวจแก้ระบบให้กลับคืนสู่สภาพปกติในกรณีที่ระบบเกิดข้อผิดพลาดขึ้นมา

8. ช่วยในการปรับปรุงระบบการทำงานของคอมพิวเตอร์ เพราะรายการที่บันทึกไว้นี้สามารถใช้ในการปรับให้เข้ากับระบบ เนื่องจากรายการบันทึกนี้จะให้รายละเอียดที่ทำให้ทราบว่าอุปกรณ์ที่ใช้ทำงาน (system facility) ทั้งหลายว่าอันไหนใช้บ่อยแค่ไหน โดยเราอาจ sort ตามโปรแกรมที่ใช้บ่อย ๆ ก็จะทราบว่ารายละเอียดการใช้ของ compiler, statistical package, library program ฯลฯ จากการปรับปรุงอันนี้จะทำให้ระบบการทำงานมีประสิทธิภาพยิ่งขึ้น

9. ช่วยวิเคราะห์ในด้านผู้ใช้ว่า ผู้ใช้คนไหนเรียกใช้มาก หรือใช้ข้อมูลอันไหนมากหรือคนไหนที่ใช้น้อย เพื่อจะสามารถเปลี่ยนแปลงระดับชั้นของการให้สิทธิการใช้

เสียใหม่ให้เหมาะสม เพื่อประสิทธิภาพของการทำงาน

ฯลฯ

ชนิดของข้อมูลที่ต้องมีการบันทึกรายการต่าง ๆ ที่เกิดขึ้น มีหลายประเภท คือ

ก. รายการของข้อมูลที่เข้ามาประจำ (Transaction log)

ข. รายละเอียดของการทำงานของแฟ้มข้อมูล (File action log)

ค. การบันทึกรายการการกระทำที่เกิดการผิดพลาดที่มีผลต่อระบบความปลอดภัย

ง. การบันทึกของการตรวจแก้ไขแฟ้มข้อมูลให้ถูกต้อง

จ. การบันทึกการเปลี่ยนแปลงของรายการต่าง ๆ ที่ได้เกิดขึ้นแล้ว

ประเภท Transaction log และ File - action log มีความสำคัญมากที่สุด แต่ละชนิดของ Logging จะต้องบันทึกรายละเอียดเก็บไว้ ตัวอย่าง เช่น

Transaction log ประกอบด้วย

- Incoming enquiry transaction
- Incoming update transaction
- Transaction type
- Transaction number
- Origination terminal
- Originating operator
- Time and date
- Response to enquiry transaction
- Response to update transaction
- Indication that response was received correctly

- Procedural violations on input
- Record of start and end of file reconstruction
- Note of completion of update

File - action log ประกอบด้วย

- Transaction number
- Time and date
- Address of items updated
- Contents of items before they are updated
- Note of completion of update
- List of programs used for update
- Full contents of and records deleted
- Details of any indexes opened or closed
- Procedural violations deleted during update or processing
- Contents of items corrected, before correction
- Contents of items corrected, after correction
- Contents of items after they are updated
- Full contents of and records delet i
- Indication of start and end of a correction run

ฯลฯ เป็นต้น

การบันทึกรายละเอียดรายการต่าง ๆ ที่เกิดขึ้นจะต้องพิมพ์เป็นรายงานออกมา เพื่อช่วยในการหาข้อผิดพลาดที่เกิดขึ้น ซึ่งจะมีรายละเอียดของการบันทึกมากน้อยเพียงใด ต้องให้เพียงพอที่เจ้าหน้าที่ตรวจสอบด้านความปลอดภัยและเจ้าหน้าที่ตรวจสอบใช้ประกอบการทำงานได้ ตัวอย่างอย่างหนึ่งของการบันทึกรายละเอียดรายการต่าง ๆ ของงานทางด้านบัญชี เช่น ตาราง 3.5

ตาราง 3.5 ตัวอย่างของการบันทึกรายละเอียดของการกระทำที่เกิดขึ้น

```
Entry
Type Time     Termin l   User                Event
-------------------------------------------------------------------------
 01  10:13:58           CLEMENTS JOBTEST1XXXA7 STARTED
 02  10:13:59           CLEMENTS STEP FTN OF JOB TEST1XXXA7 STARTED
 81  10:14:06  TAS NOOP SME LOGIN,SMEDLEY NOOP
 03  10:14:08           HUBEAT C STEP COMPTS OF JOB STAIXXXXA4 ENDED
                                 RESOURCES USED: Cp=2.257   IO=4.423
                                       CORE =50  DISK =125 TERMINAL=0.000
                                       ACCTG UNITS CHARGES=137.386
 04  10:14:10           HUBERI C JOB STATXXXXA4 ENDED
                                 RESOURCES USED: Cp= 5.037 IO=5.521
                                       CORE=50  DISK=175   TERMINAL=0.000
                                       ACCTG UNITS CHARGED=189.630
 82  10:14:57  1A5 NOOP SME ACCOUNT = 0427
 74  10:15:02  1A2 JONES TO EXECUTE CIRCUIT (PROPRIETARY PROGRAM)
 01  10:15:02           JONES TO JOB % CIRCUTYAS STARTED
 02  10:15:03           JONES TO STEP % CIRC1 OF JOB %CIRCUIT STARTED
**************************************************************************
* 93  10:15:11  1A5 NOOP SME INCORRECT PASSWORD W2X3Y                      *
**************************************************************************
 01  10:15:20           JACINSKI JOB DEBUGXXXA9 STARTED
 02  10:15:21           JACINSKI STEP ASM OF JOB DEBUGXXXA9 STARTED
 89  10:15:33 203  FARMER L LOGOUT, LINDA FARMER
 83  10:15:55 1A5  NOOP SME CORRECT PASSWORD GIVEN
 03  10:16:14           HUBERT C STEP FTN OF JOB TEST1XXXA7 ENDED
                                 RESOURCES USED: CP=0.342   IO=2.575
                                       CORE=60  DISK=75   TERMINAL=0.000
                                       ACCTG UNITS CHARGED=63.986
 02  10:16:18           HUBERT C STEP LOAD OF JOB TEST1XXXA7 STARTED
 75  10:19:02 1A5  NOOP SME CHANGE MADE TO SENSITIVE DATA:
                           FILE PAYROLL RECORD JONES,FIELD SALARY
                           NEW FIELD VALUE: 20000
 81  10:19:03 203  HUBERT C LOGIN CAROL HUBERT
```

ค่าใช้จ่ายในการทำการบันทึกรายละเอียดรายการต่าง ๆ

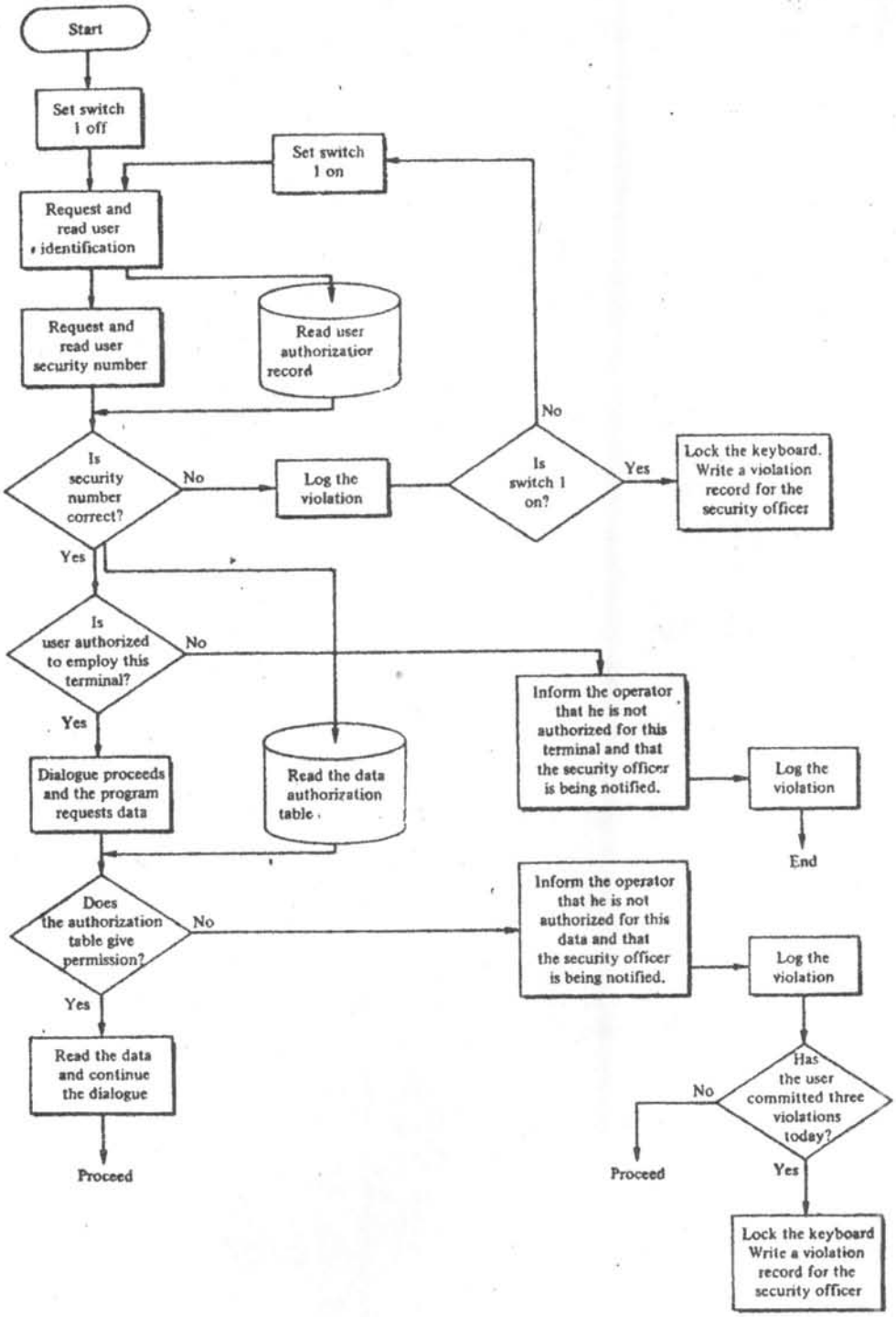
ปัจจุบันยังไม่ทราบว่าการบันทึกรายละเอียดของรายการการกระทำต่าง ๆ นี้จะใช้เครื่องจักรอุปกรณ์ช่วยได้หรือไม่ ซึ่ง Weissman ได้เสนอแนวความคิดว่าน่าจะทำได้ แต่ปัจจุบันการบันทึกเหล่านี้ใช้ระบบโปรแกรมในการปฏิบัติงาน ซึ่งจะต้องเพิ่มระบบโปรแกรมลงไป และอุปกรณ์รับข้อมูล เช่น Diskette เป็นต้น เพื่อใช้บันทึกรายการต่าง ๆ รายละเอียดของการบันทึกเหล่านี้อาจเข้ารหัสไว้เพื่อความปลอดภัย ในกรณีที่รายการนั้นมีความสำคัญมาก แต่ถ้าวางระบบความปลอดภัยอย่างเพียงพอกับอุปกรณ์บันทึกข้อมูลเหล่านี้ ข้อมูลที่บันทึกรายการต่าง ๆ ก็ไม่จำเป็นต้องเข้ารหัสก็ได้ แต่รายละเอียดของการบันทึกเหล่านี้ก็ไม่ควรจะใช้ในการทำงานประจำวันปกติ เมื่อระบบเกิดเสียหายหรือเกิดความผิดพลาดใด ๆ ก็จะไม่เกิดผลเสียต่อรายละเอียดใน Log ค่าใช้จ่ายโดยทั่วไปในการทำ Log ได้แก่ค่าใช้จ่ายด้าน

- ระบบโปรแกรม
- อุปกรณ์รับข้อมูล
- การเข้ารหัส เป็นต้น

ตัวอย่างที่แสดงถึงระบบการประมวลผลแบบ Real - time ที่วางระบบความปลอดภัยแล้ว ดูรูป 3.10 [2] ซึ่ง

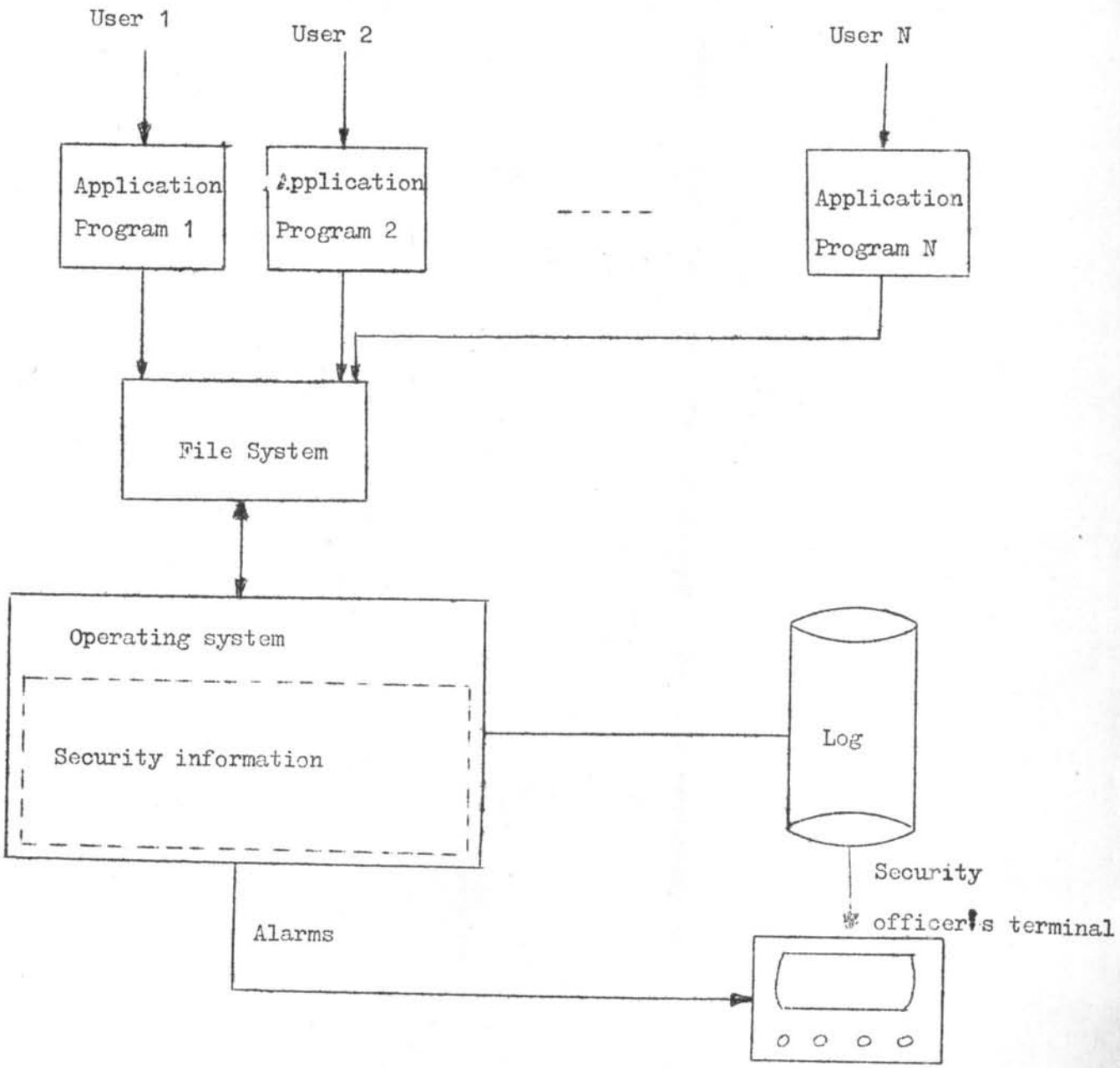
- keyboard ถูก lock ไว้
- ถ้าผู้ใช้เรียกคอมพิวเตอร์ใช้รหัสที่เรียกผิด 2 ครั้ง จะมีการบันทึกการกระทำลงบนแฟ้มข้อมูลอย่างหนึ่ง เพื่อที่จะนำไปตรวจสอบ

ฯลฯ

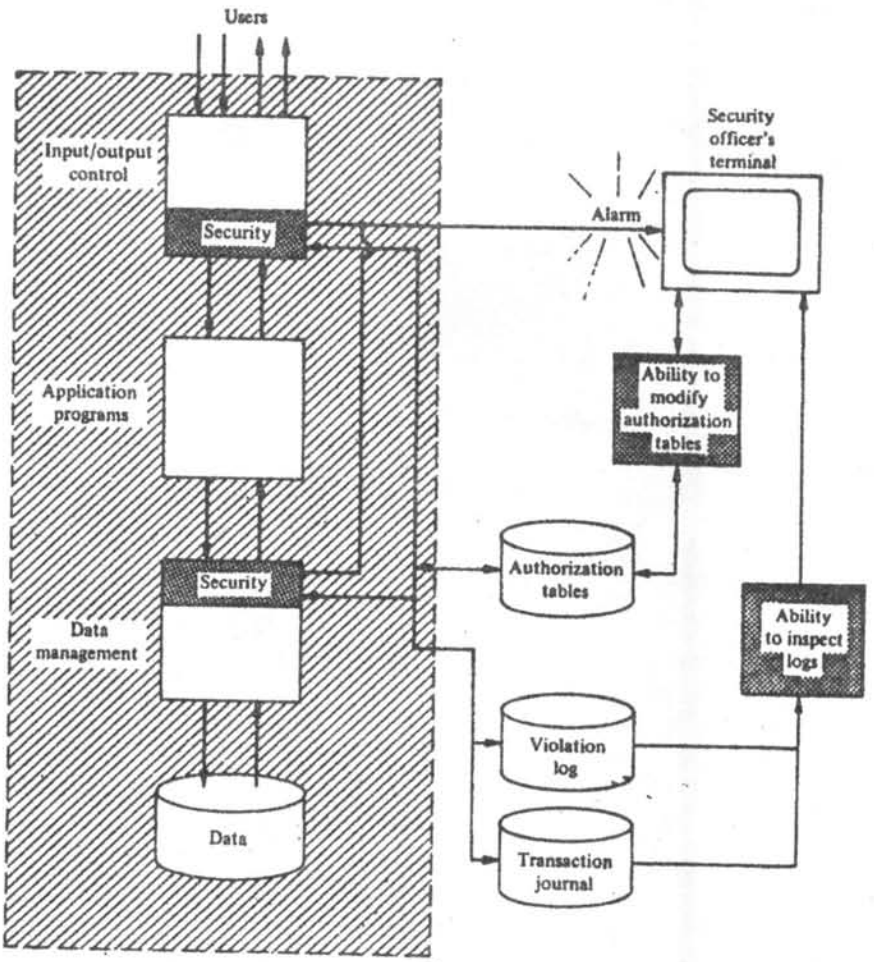


รูป 3.10 การประมวลผลข้อมูลแบบ Real – time ที่วางระบบความปลอดภัยแล้ว

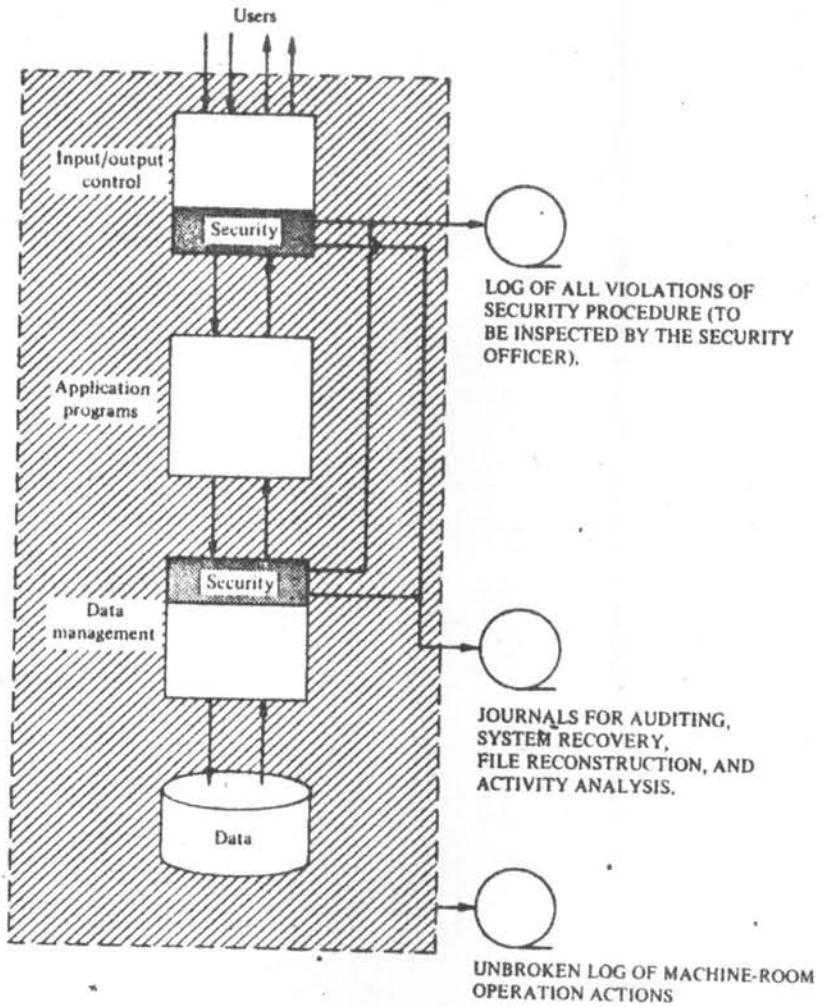
จากที่กล่าวมาแล้วทั้งหมด จะสรุประบบการทำงานของผู้ใช้แต่ละคน ในระบบ Real - time ที่ผ่านระบบควบคุมการปฏิบัติงานที่เป็นโปรแกรมหลัก ซึ่งสร้างระบบปลอดภัยไว้แล้ว รายละเอียดที่เกี่ยวข้องดูจากรูป 3.11 ถึง 3.13



รูป 3.11 การควบคุมระบบโปรแกรมภายในระบบการควบคุมการปฏิบัติงาน



รูป 3.12 ระบบความปลอดภัยที่จัดทำขึ้นในกรณีการปฏิบัติงานที่เกิดขึ้นในขณะนั้น พร้อมทั้งบันทึกรายการที่เกิดขึ้นทันที



รูป 3.13 การตรวจงานของผู้ใช้ที่เข้ามาในระบบที่จัดระบบความปลอดภัยแล้ว พร้อมทั้งบันทึกรายละเอียดที่เกิดขึ้น

3.4.2 เทคนิคที่ทำให้ข้อมูลกลับคืนมาใหม่เมื่อเกิดความเสียหาย ได้แก่

ก. กรณีการประมวลผลแบบ Batch Processing System แสดงแบบดังรูป 3.14

ข. กรณีการประมวลผลแบบ In - line system แสดงไดดังรูป3.15

ค. กรณีการประมวลผลแบบ Real - time system แสดงไดดังรูป 3.16

3.4.3 การตรวจสอบความถูกต้องของข้อมูล ระบบประมวลผลด้วยคอมพิวเตอร์มีองค์ประกอบใหญ่ ๆ 4 ส่วน คือ ระบบงาน โปรแกรม ข้อมูล และคอมพิวเตอร์ ในด้านข้อมูลมักจะมีผู้ให้ความสนใจน้อยที่สุด ส่วนทั้ง 3 ด้าน ได้มีการศึกษาค้นคว้าจนมีเทคนิคใหม่ ๆ เกิดขึ้นมาก แต่เราต้องไม่ลืมว่าในการปฏิบัติงานจริง ๆ หากข้อมูลไม่ได้รับการจัดการที่ถูกต้อง แม้ว่าการวางระบบงาน การเขียนโปรแกรม และระบบควบคุมการปฏิบัติงานจะมีประสิทธิภาพเพียงใดก็ไม่อาจที่จะให้ผลงานที่ดีออกมาได้ ดังมีคติพจน์ที่ว่า " Garbage in garbage out " (GIGO) รายละเอียดที่จะกล่าวถึงต่อไปนี้เป็นวิธีการตรวจสอบความถูกต้องข้อมูลที่ใช้กันแพร่หลาย ซึ่งผู้ใช้จะเลือกใช้ตามความต้องการและความเหมาะสมของงานต่อไป

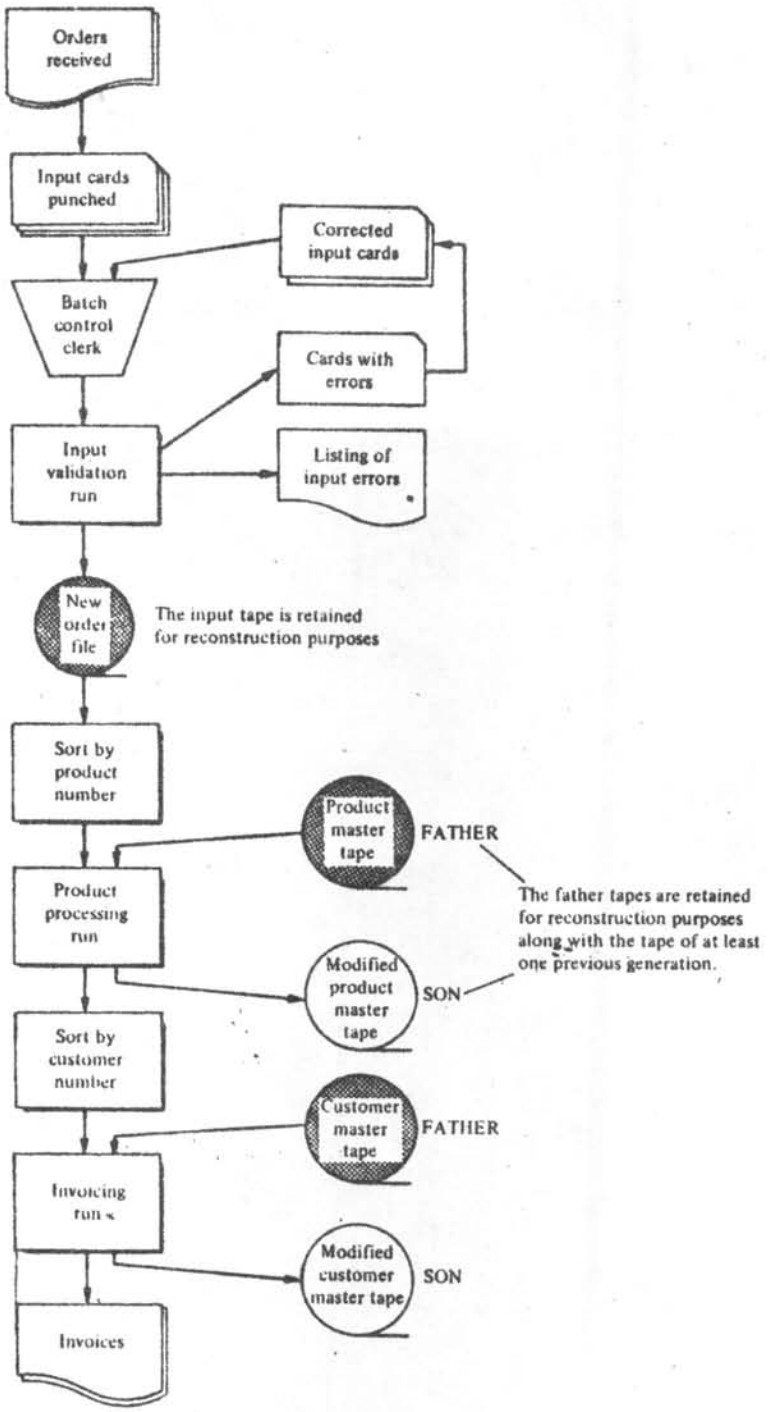
สาเหตุของความผิดในข้อมูล อาจผิดเนื่องจากสาเหตุดังนี้

1. ผิดมาจากต้นฉบับ เช่น ข้อความในแบบสอบถามหรือเอกสารเดิมไม่ถูกต้อง

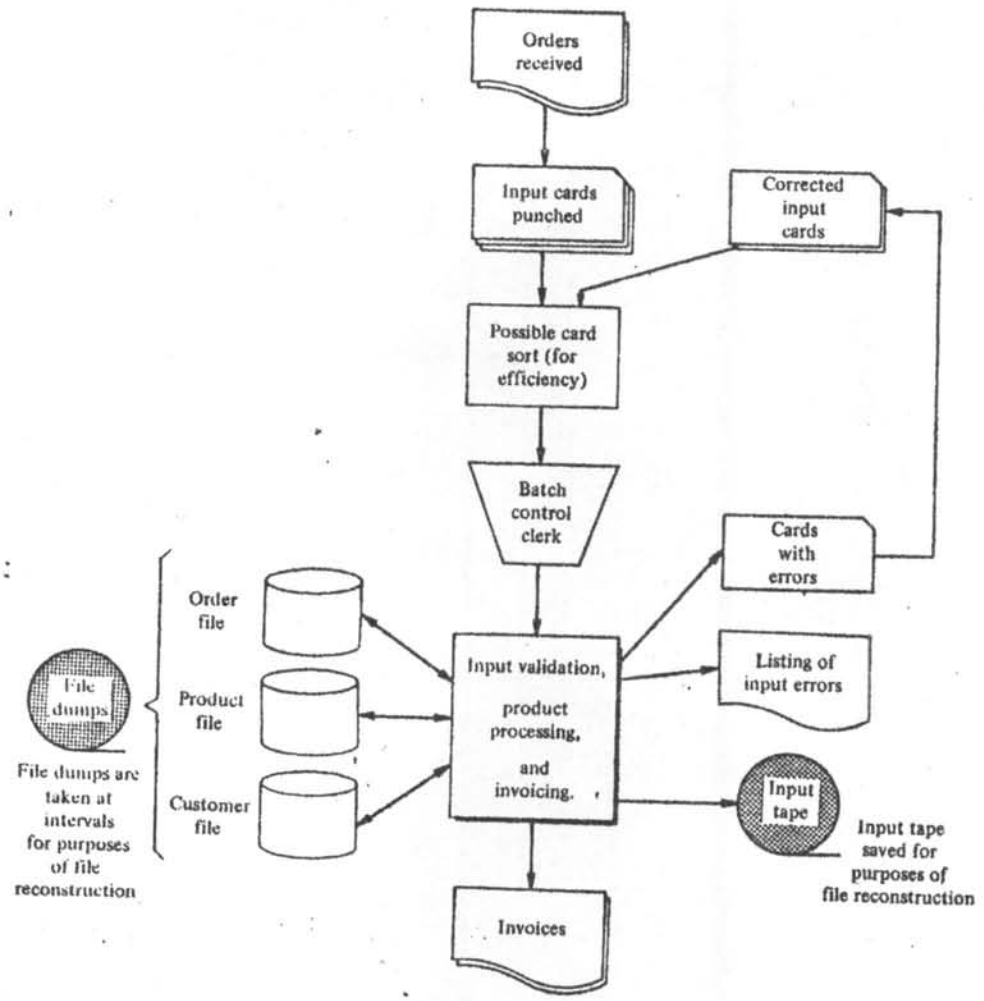
2. บันทึกข้อมูลผิด เช่น ข้อความในต้นฉบับถูก แต่พนักงานลงรหัสหรือพนักงานเจาะบัตรทำผิด

3. ความผิดพลาดจากการทำงาน เช่น หยิบเทปข้อมูลผิดม้วนเมื่อป้อนงานเข้าคอมพิวเตอร์

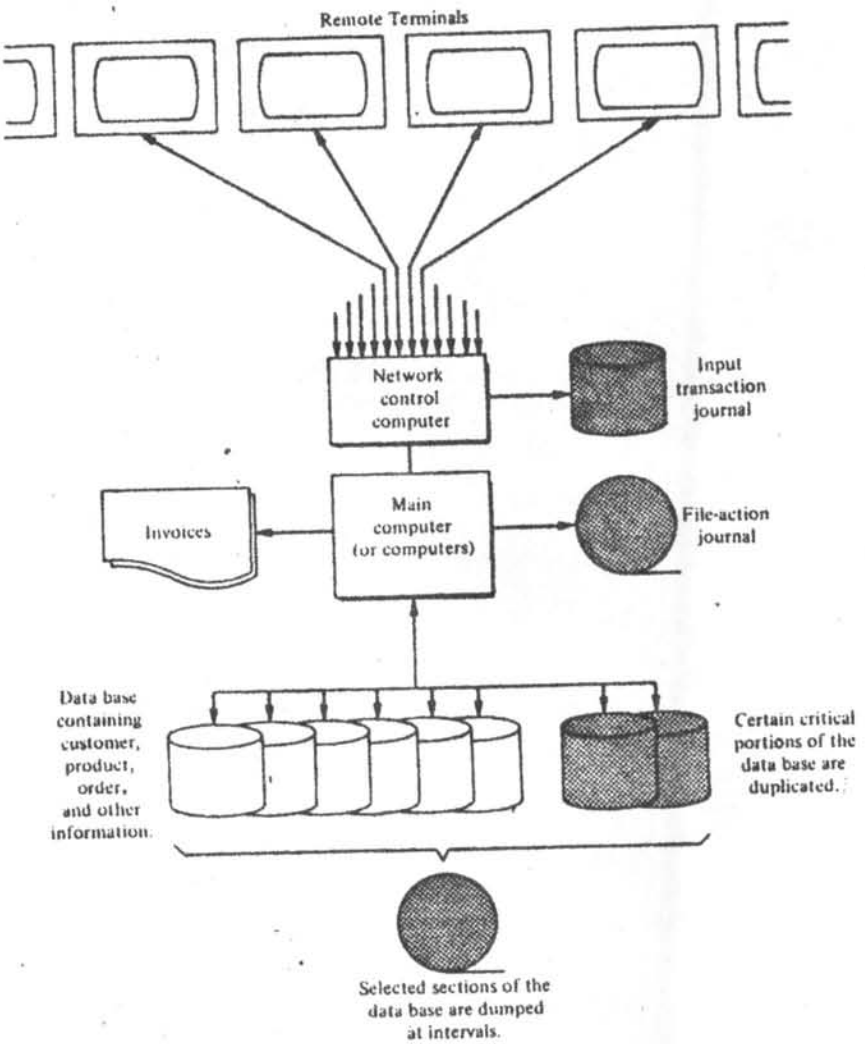
การแบ่งประเภทของงานตามความเสียหายอันเกิดจากข้อมูลผิด แบ่งได้ 3 ประเภท



รูป 3.14 การทำให้ข้อมูลกลับคืนมาใหม่เมื่อเกิดความเสียหายในกรณีการประมวลผลแบบ Batch processing system



รูป 3.15 การทำให้ข้อมูลกลับคืนมาใหม่เมื่อเกิดความเสียหายในกรณีการประมวลผลแบบ In - line system



รูป 3.16 การทำให้ข้อมูลกลับคืนมาใหม่เมื่อเกิดความเสียหายในกรณี
การประมวลผลแบบ Real - time system

1. งานที่ยอมให้ข้อมูลผิดไม่ได้เลย เช่น

- งานตรวจข้อสอบคัดเลือกนักศึกษาเข้ามหาวิทยาลัย
- งานทำบัญชีเงินฝากของลูกค้าธนาคาร
- ข้อมูลส่วนบุคคล ซึ่งเจ้าหน้าที่บ้านเมืองอาจใช้อ้างอิงหรือนำไปใช้

2. งานที่จะยอมให้ข้อมูลผิดพลาดได้บ้าง เช่น

- งานประมวลผลข้อมูลสถิติ
- Data transmission ซึ่งรับ – ส่งข้อความเป็นภาษาคำพูดธรรมดา เช่น โทรเลข เป็นต้น

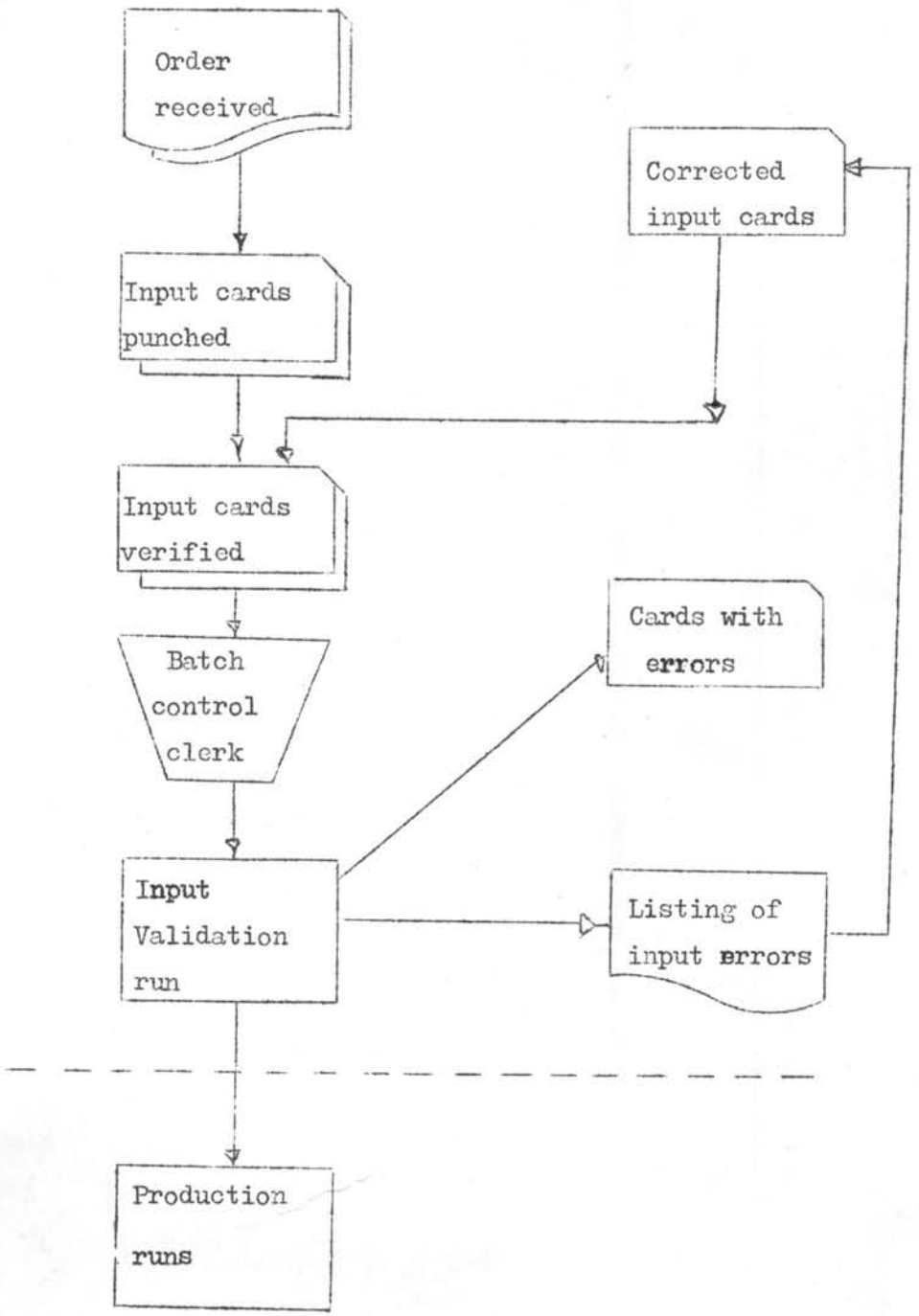
3. งานซึ่งโปรแกรมจะหยุดทำงานเมื่อข้อมูลผิด เช่น

- Multiple punched ในบัตรข้อมูลบางตัว คอมพิวเตอร์จะไม่ยอมรับ
- Data records มีความยาวน้อยกว่าที่ระบุไว้ในโปรแกรม

ขั้นตอนการตรวจสอบความถูกต้องของข้อมูล แสดงได้ดังรูป 3.17

<u>เทคนิคในการตรวจสอบความถูกต้องของข้อมูล</u> (5)

ความถูกต้องร้อยเปอร์เซนต์ของข้อมูล ย่อมเป็นสิ่งที่ผู้ทำงานประมวลผลด้วยคอมพิวเตอร์ทุกคนปรารถนา แต่ในความจริงอาจจะทำไม่ได้ หรือจะทำได้ก็ต้องลงทุนทั้งเวลา คน และค่าใช้จ่ายไม่คุ้มกับผลที่ได้รับ การเลือกใช้เทคนิคการตรวจสอบความถูกต้องของข้อมูลให้เหมาะสมกับงานเป็นความรับผิดชอบของผู้วิเคราะห์ระบบงาน โดยพิจารณาจากแหล่งความผิดของข้อมูลและความร้ายแรงของความเสียหายอันอาจเกิดกับงาน เทคนิคที่สำคัญมีดังต่อไปนี้



รูป 3.17 ขั้นตอนการตรวจสอบความถูกต้องของข้อมูล

1. การตรวจสอบด้วยตา โดยพิมพ์ข้อมูลเบื้องต้นทั้งหมดออกมาทางกระดาษพิมพ์แล้วตรวจดูด้วยตา ซึ่งเหมาะกับงานประมวลผลที่มีข้อมูลไม่มาก รายละเอียดของข้อมูลไม่ยุ่งยากนัก และไม่เป็นงานที่ต้องทำเป็นประจำ

2. Possible code check เป็นการใช้โปรแกรมคอมพิวเตอร์ตรวจสอบแต่ละเขต (field) ของข้อมูลให้แน่ใจว่ามีค่าอยู่ในช่วงที่กำหนดให้ ได้แก่

- Valid code : ตรวจรหัสของข้อมูลแต่ละชนิดย่อมมีจำกัด เช่น เพศมี 1 และ 2 เท่านั้น
- Valid character: การตรวจสอบแต่ละเขตที่เจาะในบัตรย่อมมีการกำหนดว่าเป็นตัวเลขหรือตัวอักษร
- Valid field size, sign and position : ถ้าข้อมูลเบื้องต้นใดมีข้อกำหนดแน่นอน เช่น กำหนดว่าหมายเลขรหัสส่วนใดจะต้องมีจำนวนกี่หลัก มีรูปแบบอย่างไร มีเครื่องหมายกำกับบวกหรือลบ โปรแกรมที่วางไว้จะทดสอบว่าเป็นไปตามข้อกำหนดหรือไม่
- Sequence test : ในการปฏิบัติข้อมูลโดยประมวลผลเป็นชุด ๆ โดยมากจะจัดข้อมูลเบื้องต้นที่นำเข้าเครื่องเรียงตามลำดับ เช่น ในด้านบัญชีเงินเดือน ระเบียน จะเรียงกันตามหมายเลขพนักงานอยู่แล้ว ดังนั้นจึงเป็นการง่ายที่จะวางโปรแกรมให้ทำการตรวจหาระเบียนที่ไม่เรียงตามลำดับหมายเลขหรือระเบียนที่สูญหายไป
- Limit or reasonable test : เป็นการทดสอบโดยตั้งสมมุติฐานว่าข้อมูลเบื้องต้นหรือผลลัพธ์ควรจะอยู่ในขอบเขตที่จำกัด เช่น เงินเดือนเสมียนควรไม่ต่ำกว่า 1,000 บาท และไม่เกิน 2,500 บาท ถ้าข้อมูลเบื้องต้นหรือผลลัพธ์ที่ได้จากการคำนวณผิดจากข้อจำกัดนี้ แสดงว่ามีข้อผิดพลาดเกิดขึ้น

จะต้องแก้ไข แม้การทดสอบแบบนี้จะไม่เป็นการยืนยันว่าข้อมูลหรือผลลัพธ์ถูกต้อง แต่อย่างน้อยที่สุดก็เป็นการยืนยันว่าไม่มีรายการใดผิดพลาดเกินกว่าข้อจำกัดที่วางไว้

3. Consistency (or Relationship) check บางครั้งข้อมูลที่ผิดอาจมีค่าตกอยู่ในช่วงที่เป็นไปได้ จึงไม่สามารถตรวจพบได้โดยใช้วิธีก่อน ในกรณีนี้จะใช้ความสัมพันธ์ระหว่างแต่ละช่วงรายการของข้อมูลตั้งแต่สองรายการขึ้นไปเป็นหลักเกณฑ์ในการตรวจความผิดของข้อมูล เช่น ช่วงรายการอายุของเด็ก 10 ปี และช่วงรายการจำนวนบุตรถ้ามีตัวเลข แสดงว่าผิด

4. Structural check เป็นการใช้โปรแกรมคอมพิวเตอร์ตรวจ "โครงสร้าง" หรือความครบถ้วนของข้อมูลเบื้องต้น เช่น ระเบียนของครอบครัวที่มีสมาชิก 4 คน จะมีระเบียน 2 ประเภท คือ

- Household record มีรายละเอียดทั่วไปของครอบครัว และมี 1 รายการที่บอกจำนวนสมาชิกในครอบครัว
- Member records บรรจุข้อมูลของสมาชิกในครอบครัว โดย 1 ระเบียนต่อ 1 คน

จะตรวจสอบความครบถ้วนด้วยโปรแกรมดังนี้ ตรวจสอบว่าภายใน 1 ครอบครัวต้องมี Household record 1 ใบ จำนวน Member records ต้องเท่ากับค่าของรายการที่บอกจำนวนสมาชิกในครอบครัวของบัตร Household record และหมายเลขสมาชิกในครอบครัวต้องไม่ซ้ำกัน

5. Validation against disk file or table ในกรณีที่รหัสข้อมูลมีเป็นจำนวนมาก และมีการเปลี่ยนแปลง เพิ่มเติม หรือตัดออกอยู่ตลอดเวลา (อาจเรียกรหัสข้อมูลประเภทนี้ว่า Dynamic data code) เช่น

- หมายเลขลูกค้าธนาคาร
- รหัสวิชาที่เปิดสอนในแต่ละภาคการศึกษา

– รหัสจังหวัด อำเภอ ตำบล

ฯลฯ

รหัสเหล่านี้ควรเก็บบันทึกไว้ในแฟ้มข้อมูลที่เป็นจานแม่เหล็กหรือเทปแม่เหล็ก การตรวจสอบข้อมูลในระเบียนข้อมูลเข้า ทำได้โดยค้นหาว่ารหัสข้อมูลนั้น ๆ มีอยู่ในแฟ้มข้อมูลหรือไม่ ถ้าไม่มีก็หมายความว่าเป็นข้อมูลที่ผิด รหัสในลักษณะดังกล่าวมักไม่เป็นช่วงที่ต่อเนื่องกัน หรือมีมากช่วงเกินไป และมักไม่มีความสัมพันธ์กับช่วงรายการข้อมูลอื่น ๆ จึงไม่สามารถตรวจสอบโดยทำ Possible code check หรือ Consistency check ง่าย ๆ ไว้ในโปรแกรม ส่วนการเก็บรหัสไว้ในแฟ้มข้อมูลที่เป็นจานแม่เหล็ก มีข้อดีคือ เมื่อจำเป็นต้องมีการเปลี่ยนแปลง เพิ่มเติมรหัสจะไม่ทระทบกระเทือนโปรแกรม เพราะไม่ได้ระบุรหัสที่เป็นไปได้ไว้ในโปรแกรมอย่างตายตัวเหมือนวิธีอื่น ๆ ที่กล่าวมาแล้วข้างต้น กรณีถ้ามีรหัสมีจำนวนไม่มากเกินไปนัก อาจให้โปรแกรมอ่านเข้ามาไว้ในหน่วยความจำ ทำการตรวจสอบในลักษณะ Table lookup ซึ่งจะทำงานได้เร็วกว่าการค้นหาในจานแม่เหล็ก

6. ตัวเลขตรวจสอบ (Self – checking digit or check digit)

การตรวจสอบข้อมูลที่จัดเป็น Dynamic data code ด้วยวิธีเปรียบเทียบรหัสในจานแม่เหล็กนั้น หากรหัสที่ผิดแต่บังเอิญเป็นรหัสที่เป็นไปได้ และมีอยู่ในจานแม่เหล็ก ความผิดลักษณะนี้ก็ไม่อาจตรวจพบด้วยวิธีดังกล่าว ซึ่งจะตรวจสอบความผิดลักษณะนี้ได้โดยเพิ่มตัวเลขพิเศษอีกตัวหนึ่งต่อท้ายเข้าไปในรหัสข้อมูล ตัวเลขที่เพิ่มเข้าไปเรียกว่าตัวเลขตรวจสอบ ซึ่งค่าของตัวเลขตรวจสอบขึ้นกับค่าของตัวเลขอื่น ๆ ในรหัสข้อมูล เมื่อตัวเลขตัวใดตัวหนึ่งเปลี่ยนแปลงไป จะมีผลทำให้ตัวเลขตรวจสอบที่ถูกต้องเปลี่ยนแปลงไปด้วย การกำหนดตัวเลขตรวจสอบทำได้หลายวิธีแตกต่างกันไป เช่น Identification number เป็น 57648 จะหาตัวเลขตรวจสอบตามหลักเกณฑ์ที่กำหนดดังนี้

– เอาตัวเลขในตำแหน่งเลขคี่คูณด้วย 2

5×2 , 6×2 ,และ 8×2 ได้ 10, 12 และ16

- บวกตัวเลขแต่ละตัวรวมตัวเลขเดิมที่ไม่มีการทูณ

  1 + 0 + 7 + 1 + 2 + 4 + 1 + 6 = 22

- ลบผลบวกที่ได้จากเลขจำนวนเต็มลงท้ายด้วยศูนย์ที่มีค่ามากกว่าค่าผลบวกนี้น้อยที่สุด ก็คือ 30

  30 - 22 = 8

- ได้ตัวเลขตรวจสอบ = 8 เขียน Identification number นี้ใหม่ได้ 576488

ข้อควรระวังเมื่อใช้ตัวเลขตรวจสอบก็คือ บางรหัสที่ต่างกันถ้าใช้บางวิธีจะให้ค่าตัวเลขตรวจสอบเท่ากัน เช่น 57846 และ 54678 ได้ตัวเลขตรวจสอบเป็น 8 จะแก้ไขได้โดยอาจใช้วิธีตัวเลขตรวจสอบหลาย ๆ วิธีพร้อมกันก็ได้

7. <u>เตรียมข้อมูล 2 ชุดและเปรียบเทียบความแตกต่าง</u> วิธีนี้ใช้พนักงาน 2 ชุด ทำงานทุกขั้นตอนในการเตรียมข้อมูลซ้ำกัน คือ

- ทำบรรณาธิกรณ์ด้วยคน 2 ชุด
- ลงรหัสในเอกสาร 2 ชุด และทำโดยพนักงาน 2 ชุด
- บันทึกข้อมูล 2 ชุด จากเอกสารคนละชุด

และให้โปรแกรมคอมพิวเตอร์เปรียบเทียบข้อมูลทั้ง 2 ชุด หากรายละเอียดของข้อมูลเดียวกันในข้อมูล 2 ชุด ไม่เหมือนกัน ก็แสดงว่ามีข้อผิดพลาดในข้อมูลชุดใดชุดหนึ่ง หากรายละเอียดของข้อมูลเข้าในข้อมูลทั้ง 2 ชุดเหมือนกันก็อนุโลมว่าข้อมูลถูกต้อง เพราะโอกาสที่พนักงานทั้งสองชุดซึ่งทำงานอิสระต่อกันจะทำผิดเหมือนกันมีน้อยมาก

8. <u>การตรวจสอบโดยการใช้การตรวจทาน</u> เมื่อรวบรวมข้อมูลได้แล้วเจาะบัตรข้อมูลลงในบัตร จะทำการตรวจสอบข้อผิดพลาดได้โดยการตรวจทานบัตรที่เจาะแล้ว โดยใช้พนักงานเจาะบัตรกับพนักงานตรวจทานบัตรเป็นคนละกลุ่ม แต่ใช้ข้อมูลเริ่มต้นเดียวกัน ถ้าหากการตรวจทานบัตรพบข้อผิดพลาดก็ต้องทำการแก้ไขเจาะใหม่ให้ถูกต้องตรงกับข้อมูลเริ่มต้น

9. ยอดรวมของชุดข้อมูล (Batch total) การตรวจสอบความถูกต้องโดยการตรวจทางบัตร (ในกรณีที่ใช้บัตรเป็นส่วนนำข้อมูลเข้า) ยังไม่ได้ผลที่ดีถึง 100 % ควรใช้วิธีการควบคุมชุดของข้อมูล (Batch control) ควบคู่ไปด้วย และวิธีนี้เหมาะกับการประมวลผลในเมืองไทย ซึ่งมักจะทำเป็นระบบการประมวลผลเป็นชุด ๆ กล่าวคือข้อมูลจะถูกรวบรวมเป็นชุดไว้รอประมวลผลพร้อมกัน วิธีการควบคุมชุดของข้อมูลได้แก่การเลือกเอาเขต (Field) ที่สำคัญ ๆ จากเอกสารซึ่งจะต้องมีการควบคุมให้ได้ความถูกต้อง 100 % เช่น ตัวเลขที่เป็นจำนวนเงิน เป็นต้น ซึ่งอาจมีเขตเดียวหรือหลาย ๆ เขต ตัวเลขดังกล่าวในเอกสารชุดหนึ่ง ๆ ถูกบวกเข้าด้วยกัน และเรียกผลบวกของแต่ละเขตนี้ว่า ยอดรวมของชุดข้อมูล ตัวเหล่านี้จะมีคนทำแล้วเขียนลงในใบคุมยอด (Batch total slip) ซึ่งตัวเลขจากใบคุมยอดจะถูกป้อนเข้าเครื่องคอมพิวเตอร์ด้วย โปรแกรมคอมพิวเตอร์จะบวกรายการดังกล่าวของข้อมูลทุกวันที่เกี่ยวข้องและเปรียบเทียบกับตัวเลขที่มาจากใบคุมยอด ถ้าไม่เท่ากันแสดงว่ามีข้อผิดพลาด ในแต่ละครั้ง อาจกำหนดให้มีการควบคุมชุดของข้อมูลมากกว่าหนึ่งรายการก็ได้ เช่น มียอดรวมของจำนวนเงินหลายรายการ ยอดรวมของปริมาณสินค้า ฯลฯ เป็นต้น

ข้อที่ควรพิจารณาว่างานใดควรมีการตรวจสอบความถูกต้องเพียงใด ผู้วิเคราะห์ระบบจะต้องตัดสินเอง และใช้วิธีใด ๆ ขึ้นกับปัจจัยต่าง ๆ ดังนี้

ก. ขนาดสำคัญของข้อมูล

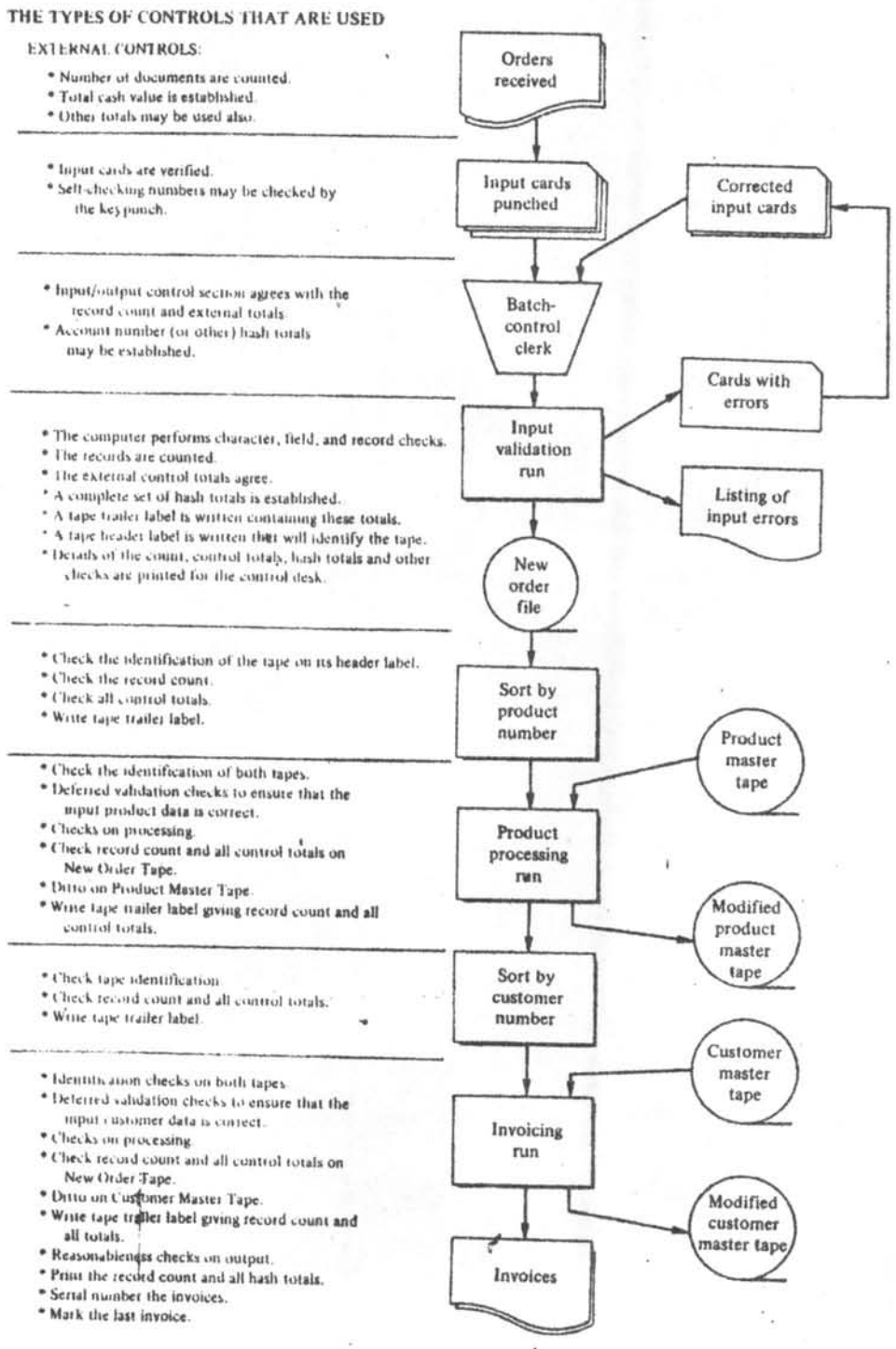
ข. ปริมาณของข้อมูล

ค. ความรีบด่วนของงาน

ง. กำลังคน และเวลาเครื่องคอมพิวเตอร์ที่มี

จ. ลักษณะของงานว่าเป็นงานที่ทำเพียงครั้งเดียวหรือทำเป็นประจำ หรือทำเป็นครั้งคราว เป็นต้น

ตัวอย่างของการควบคุมการประมวลผลแบบเป็นชุดข้อมูลแสดงได้ดังรูป 3.19



รูป 3.18 การควบคุมการประมวลผลแบบเป็นชุดข้อมูล

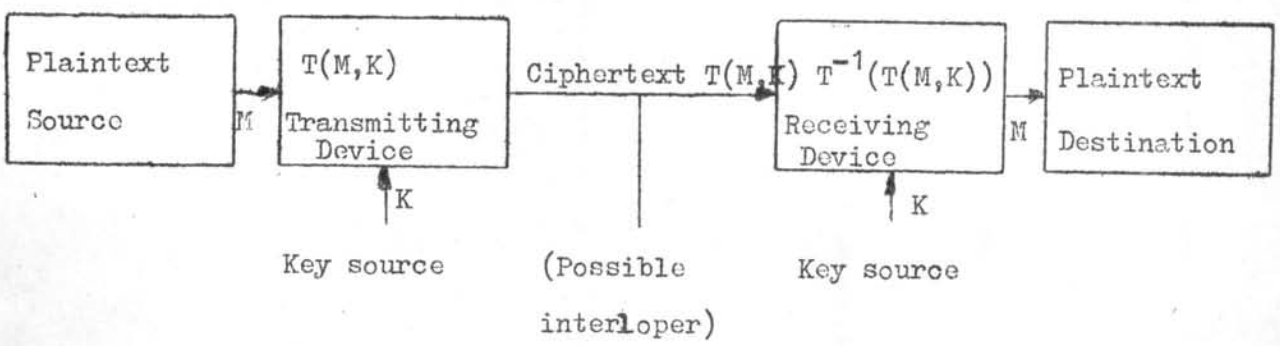
3.1.4 ระบบความลับเฉพาะของข้อมูลโดยการใช้รหัสเฉพาะ ระบบคอมพิวเตอร์สมัยใหม่ที่เป็นเครื่องขนาดใหญ่ วิธีการที่คอมพิวเตอร์จะทำงานให้เรามีหลายแบบ วิธีหนึ่งก็คือ ผู้ใช้อยู่ที่ห่างไกลจากที่ตั้งของคอมพิวเตอร์และเรียกใช้คอมพิวเตอร์โดยขบวนการโทรคมนาคม เช่น ผ่านทางสายโทรศัพท์ ดังรูป 3.19 โดยผู้ใช้เองต้องมีอุปกรณ์ปลายทาง ปกติผู้ใช้จะติดต่อคอมพิวเตอร์ทางสายโทรศัพท์โดยขั้นแรกหมุนหมายเลขโทรศัพท์ (ที่เป็นความลับไม่ให้คนอื่นทราบได้) เรียกคอมพิวเตอร์ จากนั้นก็ให้คำผ่านเพื่อแสดงให้คอมพิวเตอร์ทราบว่าเป็นบุคคลที่มีสิทธิจะใช้ เมื่อคอมพิวเตอร์ตรวจสอบแล้วว่าถูกต้อง จึงจะเริ่มรอรับคำสั่งที่จะป้อนให้กับมัน และอีกอย่างหนึ่ง ก็คือ การใช้สายโทรศัพท์ต้องมีการเคาะเป็นรหัส ซึ่งสามารถใช้กับเทคนิคของการแสดงด้วยอักษรลับได้ เทคนิคนี้สามารถให้ความปลอดภัยของข้อมูลได้ ซึ่งควรใช้ในกรณีที่ข้อมูลที่มีความสำคัญมาก ๆ จึงจะคุ้มเพราะค่าใช้จ่ายสูงมาก และสาเหตุอีกอย่างหนึ่งที่ต้องเก็บข้อมูลในแฟ้มข้อมูลหรือส่งข้อมูลโดยวิธีการโทรคมนาคมเป็นรหัสก็เพราะในปัจจุบันคอมพิวเตอร์ได้นำมาใช้กับงานมากด้านขึ้น ซึ่งการเก็บรวบรวมข้อมูลก็มากขึ้นตามไปด้วย เพื่อให้หลาย ๆ หน่วยงานที่เกี่ยวข้องเรียกใช้ข้อมูลรวมนั้นได้ ซึ่งจะต้องมีปัญหาด้านการระมัดระวังความปลอดภัยของข้อมูลตามมา

ระบบของการแสดงตัวหนังสือด้วยรหัสที่เป็นอักษรลับ แสดงได้ดังรูป 3.20 (4)

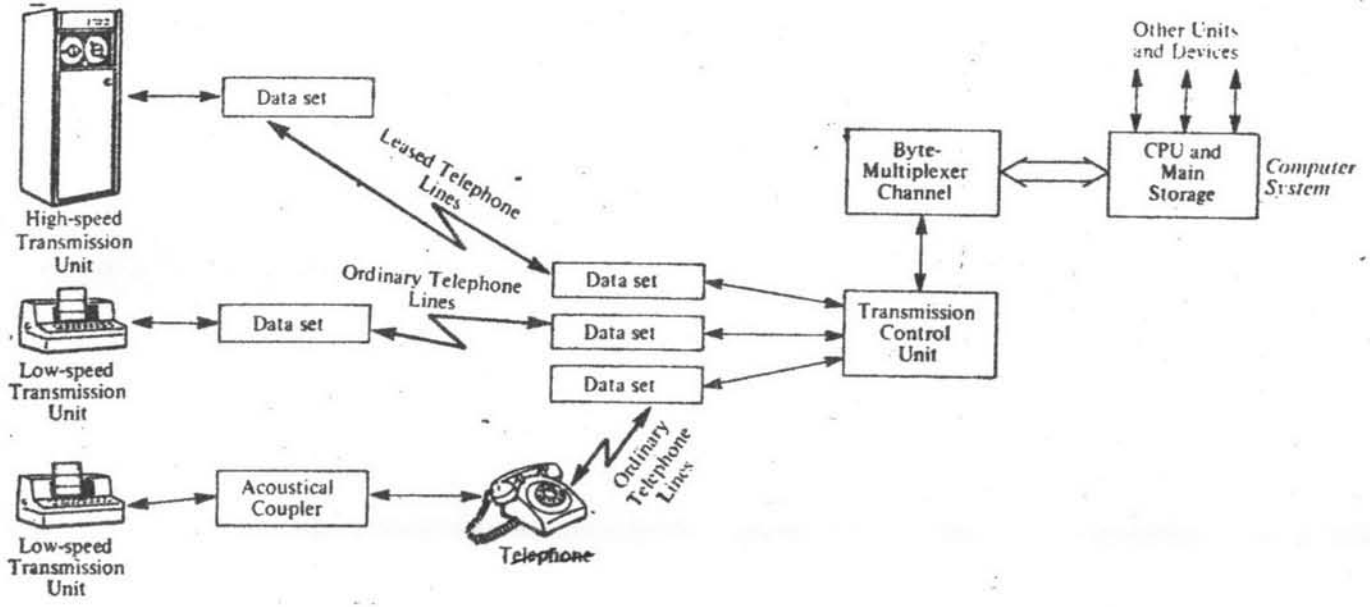
โดยที่ M คือ ข่าวสารที่ต้องการเข้ารหัส (Plaintext message)

K คือ เงื่อนไขสำหรับไขรหัส (Key)

E คือ ข่าวสารที่ผ่านการเข้ารหัสแล้ว (Ciphertext message)



รูป 3.20 ระบบการเข้ารหัสเฉพาะข้อมูล



รูป 3.19 ระบบการติดต่อสื่อสารของข้อมูล

นอกจากนี้การเข้ารหัสแสดงได้ดังรูป 3.21 ถึงรูป 3.23

วิธีการลับเฉพาะที่ใช้วิธีให้รหัสข่าวสาร (Privacy transformation) จะใช้เทคนิคที่เรียกว่า การแสดงตัวหนังสือที่เขียนด้วยรหัส (Cryptographic technique) ตัวหนังสือที่เขียนด้วยรหัสนี้ปกติจะใช้ในข้อมูลที่ส่งโดยวิธีการโทรคมนาคม และข้อมูลที่เก็บไว้เป็นแฟ้มข้อมูลแล้วอาจเป็นเทปแม่เหล็ก หรือจานแม่เหล็ก เป็นต้น จุดประสงค์ที่ใช้วิธีการนี้ก็คือ ถ้าในกรณีข้อมูลที่ส่งโดยวิธีการโทรคมนาคมก็เพื่อป้องกันการขโมยต่อสายโทรศัพท์เพื่อลอบฟังการติดต่อข่าวสารกัน โดยข่าวสารที่จะส่งไปทางสายโทรศัพท์นั้นก่อนส่งก็เปลี่ยนรูปใหม่โดยเข้ารหัสก่อน แล้วถอดรหัสออกเมื่อถึงปลายทางแล้ว เพื่อป้องกันข่าวสารรั่วไหล ส่วนในกรณีข้อมูลที่เก็บในแฟ้มข้อมูลก็เพื่อป้องกันเหตุร้ายที่เกิดขึ้นจากอุบัติเหตุหรือจากการเจตนาทำ เช่น การลักขโมยข้อมูล ทั้งสองกรณีอาจจะใช้วิธีการของรหัสเฉพาะอย่างใดอย่างหนึ่ง

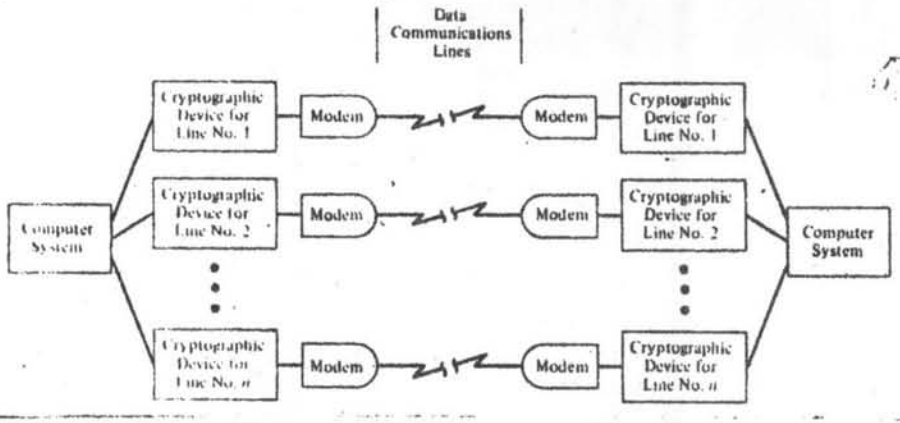
วิธีการลับเฉพาะที่ใช้วิธีให้รหัสข่าวสารนี้เป็นขบวนการที่สามารถเปลี่ยนตัวอักษรกลับไปกลับมาโดยวิธีการเฉพาะอย่างหนึ่ง ซึ่งแบ่งออกเป็น 3 พวกใหญ่ ๆ คือ (7)

ก. วิธีการสับเปลี่ยนที่กันของตัวอักษร (Transposition cipher systems)

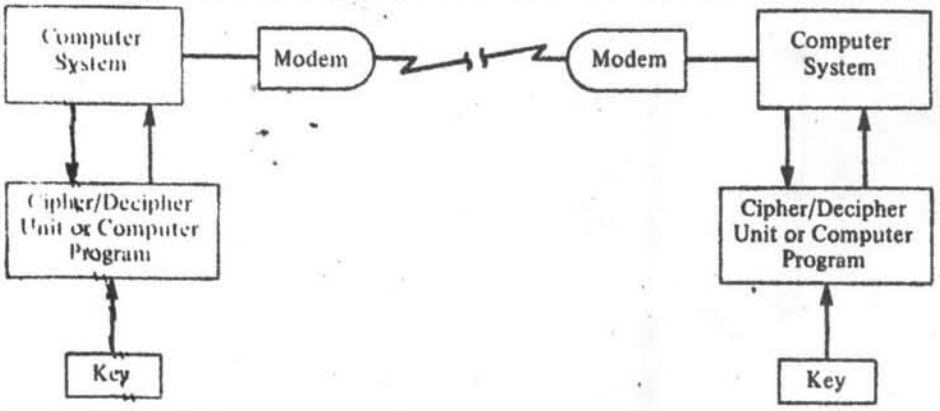
ข. วิธีการแทนที่ตัวอักษร (Substitution cipher systems)

ค. วิธีการโดยการคำนวณ (Hybrid and computational cipher systems)

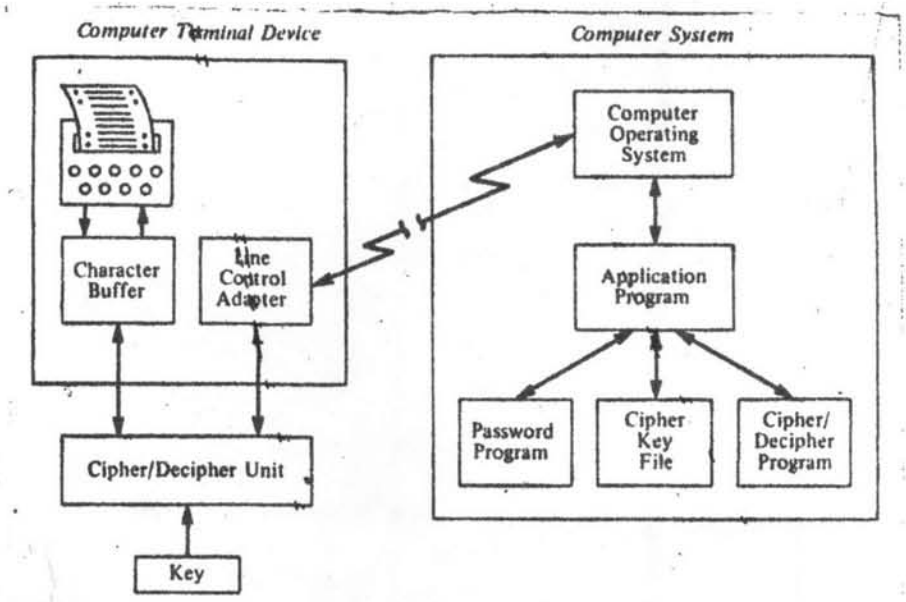
เนื่องจากการแสดงตัวหนังสือที่เขียนด้วยรหัสเป็นขบวนการที่เปลี่ยนภาษาที่เข้าใจได้ให้เป็นภาษาที่อ่านไม่เข้าใจ และในขณะเดียวกันก็จะเปลี่ยนภาษาที่อ่านไม่เข้าใจให้เป็นภาษาที่เข้าใจแบบเดิม ข่าวสารที่เข้าใจได้นี้เรียกว่า Plain text หรือ Clear text และข่าวสารที่อยู่ในรูปรหัสแล้วเรียก Cipher text หรือ Cytogram จะกล่าวถึงรายละเอียดต่อไป



รูป 3.21 การเข้ารหัสของข้อมูลที่ส่งมาจากที่ห่างไกลโดยแยกอุปกรณ์ในการเข้ารหัส/ถอดรหัสของแต่ละข้อมูล



รูป 3.22 การเข้ารหัสของข้อมูลที่ส่งมาจากที่ห่างไกลโดยใช้อุปกรณ์ในการเข้ารหัส/ถอดรหัสร่วมกันของแต่ละข้อมูล



รูป 3.23 การเข้ารหัสของข้อมูลที่ส่งมาจากที่ห่างไกลโดยใช้อุปกรณ์เข้ารหัส/ถอดรหัสติดเข้ากับอุปกรณ์ปลายทางและตัวระบบคอมพิวเตอร์

ก. วิธีการสับเปลี่ยนที่กันของตัวอักษร เป็นวิธีการที่ตัวอักษรในข่าวสารจะถูกจัดใหม่ตามวิธีการเฉพาะอย่างหนึ่ง วิธีนี้ไม่ค่อยทันสมัยแต่ก็ง่ายและสะดวกที่จะนำไปใช้

ตัวอย่างของวิธีนี้ซึ่งนิยมใช้มากที่สุดในจำพวกของวิธีการสับเปลี่ยนที่กันของตัวเอักษรก็คือ นำข้อความที่ต้องการจะเข้ารหัสจะเขียนไปตามแถวที่ 1,2, ... เรื่อย ๆ จนครบโดยมีตัวอักษรของคำไขรหัส (Key or Keyword) เป็นตัวกำหนดจำนวนแถวตั้ง และข่าวสารที่เข้ารหัสแล้วจะเลือกตามแถวตั้งของตัวอักษรซึ่งข่าวสารที่เข้ารหัสเรียงกันจากภาษาอังกฤษ เช่น

- Plain text : ALPINE CONTRACT CANCELLED STOP BID
- Key word : DIRECTOR
-

D I R E C T O R
2 4 6 3 1 8 5 7
A L P I N E C O
N T R A C T C A
N C E L L E D S
T O P B I D

- Cipher text : NCLIA NNTIA LBLTC OCCDP REPOA SETED

ข. วิธีการแทนที่ตัวอักษร วิธีการนี้ตัวอักษรหรือกลุ่มตัวอักษรจะถูกแทนที่ด้วยตัวอักษรหรือกลุ่มตัวอักษรตัวต่อตัวกับที่อ้างอิงไว้

ตัวอย่างของวิธีนี้ก็คือ การเข้ารหัสโดยจะกำหนด Plain alphabet และ cipher alphabet มาให้ เช่น

Plain alphabet : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher alphabet : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

ถ้า Plain text : CANCEL ALPINE CONTRACT

จะได้ Cipher text : FDQFH ODOSL QHFRQ WUDFW

ค. วิธีการโดยการคำนวณ ตัวอักษรในข่าวสารจะเปลี่ยนแปลงใหม่โดยใช้วิธีการทางคณิตศาสตร์ ซึ่งจะมีเงื่อนไขรหัสเฉพาะอย่างหนึ่ง

ตัวอย่างของวิธีนี้ก็คือ การใช้เทคนิคของวิธีการ Substitution และ Transposition รวมกัน ซึ่งทำได้หลายแบบ เช่น

Plain text : SELL SHORT BEFORE THURS

กำหนดคำไขรหัส คือ PUBLISHER ในรูปแมทริก 5 x 5 โดย

	1	2	3	4	5
1	P	U	B	L	I/J
2	S	H	E	R	A
3	C	D	F	G	R
4	M	N	O	Q	T
5	V	W	X	Y	Z

จะได้

SELL SHORT BEFORE THURS

2211 22424 123422 42122

1344 12345 333343 52241

เขียนรวมกันจากแถวบนก่อนและย้อนกลับไปดูคำไขรหัสในแมทริก จะได้

22 11 22 42 41 23 42 24 21 22 13 44 12 34 53

H P H N M E N R S H B Q U G X

33 34 35 22 41

F G K H M

Cipher text : HPHNM ENRSH BQUGX FGKHM

การเข้ารหัสข่าวสารด้วยเครื่องจักรอุปกรณ์

ในอนาคตคาดว่าการเข้ารหัสข่าวสาร ณ อุปกรณ์ปลายทาง จะต้องใช้เครื่องจักรอุปกรณ์มากกว่าระบบโปรแกรม ส่วนการเข้ารหัสข่าวสาร ณ ศูนย์คอมพิวเตอร์ใหญ่ ถ้าไม่ใช้ระบบโปรแกรมก็ใช้เครื่องจักรอุปกรณ์ และปัจจุบันนี้ยังใช้เฉพาะระบบโปรแกรมอยู่ ซึ่งการใช้เครื่องจักรอุปกรณ์ช่วยนี้จะทำให้หมดปัญหาในการป้องกันความปลอดภัยในด้านเจ้าหน้าที่เขียนโปรแกรมที่ทุจริตลงไป ซึ่งการเข้ารหัสที่ซับซ้อนก็จะป้องกันได้มากยิ่งขึ้น ซึ่งขบวนการถอดรหัสข่าวสารนั้นขั้นตอนของมันก็จะเป็นส่วนกลับ (Reverse) ของการเข้ารหัสข่าวสาร ส่วนอุปกรณ์รับ – ส่งข้อมูลก็จะต้องประกอบด้วยวงจร (Circuit) ที่สามารถบอกความแตกต่างระหว่างข่าวสารก่อนเข้ารหัสและข่าวสารที่ได้เข้ารหัสแล้ว เป็นต้น

ข้อควรคำนึงถึงอีกอย่างหนึ่งก็คือ ในการออกแบบระบบใด ๆ จะต้องมีข้อผิดพลาดเกิดขึ้นได้เสมอ จะต้องมีการทดสอบอย่างดีทั้งขบวนการ (Mechanisms) ของการเข้ารหัสและถอดรหัส ซึ่งการออกแบบระบบการแสดงตัวหนังสือด้วยรหัสลับเฉพาะนี้ควรจะเป็นแบบที่ธรรมดาที่สุดเท่าที่จะทำได้ เพราะโดยทั่วไประบบการแสดงตัวหนังสือด้วยรหัสลับเฉพาะนี้ก็ป้องกันผู้บุกรุกได้มากพอ ผู้ออกแบบระบบควรจะจำข้อเท็จจริงไว้สักอย่างหนึ่ง คือ

Cryptography + Loose discipline = Chaos

จะเห็นได้ว่าการติดต่อสื่อสารข้อมูลจากที่ห่างไกลนั้น ระบบความปลอดภัยของข้อมูลมีความสำคัญมาก ซึ่งมีปัจจัยที่เกี่ยวข้องซึ่งควรพิจารณา ได้แก่

– ชนิดของระบบการสื่อสารข้อมูล ซึ่งอาจเป็นการสื่อสารระหว่างคอมพิวเตอร์กับคอมพิวเตอร์ ดังรูป 3.22 หรือ
– วิธีการเข้ารหัสของข้อมูล อาจใช้ระบบเครื่องจักรอุปกรณ์หรือระบบโปรแกรม
– วิธีการส่งข้อมูลหรือการกำหนดรหัส
– ข้อกำหนดการให้สิทธิการใช้และคำผ่าน
– เวลาและค่าใช้จ่ายที่ใช้ทั้งหมด เป็นต้น

3.2 ระบบความปลอดภัยในด้านสถานที่ทำการ และลักษณะต่าง ๆ ภายนอกที่เกี่ยวข้อง

หลังจากได้วางระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะในตัวคอมพิวเตอร์เองแล้ว ซึ่งเป็นชั้นในสุด ถัดมาก็ต้องวางระบบความปลอดภัยในนั้นถัดออกมาอีกเพื่อควบคุมในด้านสิ่งแวดล้อมภายนอกที่เกี่ยวข้องกับระบบคอมพิวเตอร์ให้รัดกุมกว่าเดิม จะพิจารณาได้ดังนี้

3.2.1 การกำหนดเขตพื้นที่ ลักษณะจำเพาะ และลักษณะทางเดินของงาน มีหลายกรณีที่เกี่ยวข้อง ดังนี้

ก. ตำแหน่งที่ตั้งของตึกคอมพิวเตอร์ จะต้องเตรียมก่อนที่จะติดตั้งเครื่อง ที่ตั้งของตึกควรอยู่ในทำเลที่ปลอดภัยและห่างไกลจากเหตุร้ายต่าง ๆ บริเวณพื้นที่ที่ไม่ควรเลือกเป็นสถานที่ตั้ง ได้แก่ บริเวณที่อยู่ใกล้ป่าที่มีไฟไหม้บ่อย ๆ บริเวณที่ได้รับความสั่นสะเทือนมาก มักถูกรบกวนจากเรดาร์และกำลังงานสูงทางอีเล็คโทรนิคอยู่เสมอ ไม่ควรตั้งอยู่ใกล้กับโรงงานอุตสาหกรรมหนัก ทางรถไฟ บริเวณอื่น ๆ ที่เต็มไปด้วยฝุ่น ไอน้ำ ควัน เสียงรบกวน และบริเวณที่เกิดจลาจลบ่อย ๆ เป็นต้น ความจริงคอมพิวเตอร์ควรจะอยู่ในอาคารที่แยกต่างหาก ควรเป็นตึกที่ทำงานทุกอย่างที่เกี่ยวกับคอมพิวเตอร์โดยเฉพาะอย่างเดียว เพื่อที่จะได้จัดระบบการป้องกันความปลอดภัย ระบบการทำงาน การให้ความคุ้มกันแก่คอมพิวเตอร์ได้อย่างเต็มที่ และตึกนี้ควรจะอยู่ไกลจากตึกอื่น ๆ ด้วย ไม่ควรจะอยู่ติดตึกอื่น ๆ เกินไป เพื่อป้องกันผู้บุกรุกเข้ามาในตึกและป้องกันเหตุร้ายจากไฟไหม้ รอบ ๆ ตัวตึกไม่ควรจะให้มีรั้วต้นไม้เตี้ย ๆ หรือต้นไม้ใหญ่น้อยทั้งหลาย เพราะจะเป็นที่อาศัย กำบัง ในกรณีที่จะมีผู้บุกรุกเข้ามาในตึกคอมพิวเตอร์ ตึกคอมพิวเตอร์ควรเป็นอาคารที่ได้จัดระบบความปลอดภัยด้านไฟไหม้แล้ว (ire - proof building) แต่ถ้าทำไม่ได้ก็ให้คอมพิวเตอร์อยู่ในส่วนหนึ่งส่วนใดของอาคารซึ่งอาคารนี้ก็ได้จัดระบบความปลอดภัยด้านไฟไหม้แล้ว อาคารที่จะเอาคอมพิวเตอร์ไปตั้งไว้นี้ควรจะเลือกอาคารที่คิดว่าโอกาสที่จะเกิดไฟไหม้ น้ำท่วม หรือเหตุร้ายอื่น ๆ จากอาคารที่เชื่อมติดต่อกันหรืออาคารที่อยู่ใกล้ ๆ เป็นต้น

นอกจากนี้ปัจจัยอีกประการหนึ่งในการเลือกสถานที่ที่ตั้งก็คือ ทัศนคติของหน่วยงานที่มีต่อการติดตั้งเครื่องคอมพิวเตอร์ เช่น บางบริษัทอาจต้องการลงทุน เพื่อแสดงให้ประชาชนเห็นความเจริญก้าวหน้าของตนในกรณีนี้ ควรจะได้จัดสร้างสถานที่ให้ตั้งอยู่ ณ ที่ที่ประชาชนส่วนมากผ่านไปมา สามารถมองเห็นได้โดยง่าย ดังนั้น รอบ ๆ ฝาผนังภายนอกห้องเครื่องคอมพิวเตอร์ทั้งหมดหรือบางส่วนจึงควรจัดสร้างด้วยกระจกโปร่งแสง นอกจากนั้นอาจจำเป็นต้องใช้เครื่องตกแต่งที่สวยงาม เช่น สีสรรของห้อง โต๊ะเก้าอี้ทำงานอย่างดี และเครื่องมือเครื่องใช้ที่ทันสมัย เป็นต้น อีกประการหนึ่งในการเลือกสถานที่ตั้งควรจะได้ทำการศึกษาความเหมาะสมในเรื่องต่าง ๆ ไว้ด้วย ดังนี้ คือ ความสามารถที่จะได้รับการบริการที่จำเป็น ได้แก่ เป็นสถานที่ที่สามารถได้รับสิ่งอำนวยความสะดวกจากองค์การอื่น ๆ ที่อยู่ใกล้เคียง เกี่ยวกับเรื่องกำลังงานไฟฟ้า การประปา การสุขาภิบาล การรักษาความปลอดภัย การป้องกันอัคคีภัย การบริการเกี่ยวกับการติดต่อสื่อสาร ความสดวกในการขนส่ง เป็นต้น นอกจากนี้ควรจะศึกษาพิจารณาถึงลักษณะภูมิประเทศด้วยว่า ถ้าเป็นบริเวณพื้นที่ที่มีอุณหภูมิสูง ความชื้นมาก มีกฎกรบกวนจากแผ่นดินไหว หรือมีพายุพัดแรงอยู่เสมอ ควรนำปัจจัยเหล่านี้มาพิจารณาในการก่อสร้างสถานที่ตั้งให้มีความแข็งแรงมั่นคงเป็นพิเศษ ทำการสร้างระบบเครื่องปรับอากาศให้ดี จัดการควบคุมเรื่องฝุ่นละอองให้เข้มงวด และป้องกันมิให้น้ำท่วมเข้าในสถานที่ตั้งได้

ข. <u>ตึกคอมพิวเตอร์และห้องคอมพิวเตอร์</u> เนื่องจากบริเวณที่ตั้งตึกคอมพิวเตอร์เป็นบริเวณสำคัญ เพราะมีทั้งห้องคอมพิวเตอร์ แฟ้มข้อมูล บริเวณที่เตรียมข้อมูล รวมทั้งอุปกรณ์ประกอบอื่น ๆ เช่น ระบบการติดตั้งไฟฟ้า เครื่องปรับอากาศภายในตัวตึก ดังนั้นปัจจัยที่ควรจะนำมาพิจารณาในการวางแผนก่อสร้างสามารถนำไปใช้ได้ทั้งการดัดแปลงสถานที่ที่อยู่เดิมหรือเป็นการสร้างอาคารขึ้นใหม่ ซึ่งส่วนมากได้แก่เรื่องต่าง ๆ ดังต่อไปนี้คือ การจัดแผนผังบริเวณสถานที่ของหน่วยคอมพิวเตอร์ การพิจารณาออกแบบทางสถาปัตยกรรม เช่น เกี่ยวกับพื้นห้อง ฝาผนังและฝากั้นห้อง เพดานห้อง

ประตู หน้าต่าง ทางนำเครื่องมือเข้า บันได ลิฟต์ วัสดุป้องกันความร้อนและเก็บเสียง และการทาสี เป็นต้น นอกนั้นก็เป็นเรื่องที่เกี่ยวกับข้อพึงประสงค์ต่าง ๆ ที่สำคัญในการติดตั้งเครื่องปรับอากาศ การวางท่อระบายน้ำ การจัดระบบไฟฟ้า การให้แสงสว่าง และการติดต่อสื่อสาร

โดยทั่วไปการจัดสถานที่สำหรับหน่วยคอมพิวเตอร์นั้นจะพิจารณาเกี่ยวกับเรื่องต่าง ๆ ดังต่อไปนี้คือ ขนาดที่ว่างของบริเวณพื้นที่ที่ต้องการ โครงแบบของระบบเครื่องคอมพิวเตอร์ที่จะนำมาติดตั้ง จำนวนเจ้าหน้าที่ทั้งหมด ขนาดของส่วนต่าง ๆ ภายในหน่วยคอมพิวเตอร์ สำหรับหลักฐานที่ใช้ในการวางแผนผังบริเวณการติดตั้งโครงแบบของระบบเครื่องคอมพิวเตอร์นั้น บริษัทผู้ผลิตจะมีเอกสารแสดงรายละเอียดเกี่ยวกับขนาด น้ำหนัก ความต้องการเกี่ยวกับกำลังงานไฟฟ้า ที่เชื่อมต่อทางสาย ความยาวสายเคบิล และพื้นที่ที่ต้องการในการปฏิบัติงานของตัวเครื่องจักรกลต่าง ๆ สามารถติดต่อขอความสนับสนุนเอกสารต่าง ๆ ดังกล่าวนี้ได้โดยตรงจากบริษัทผู้ผลิต

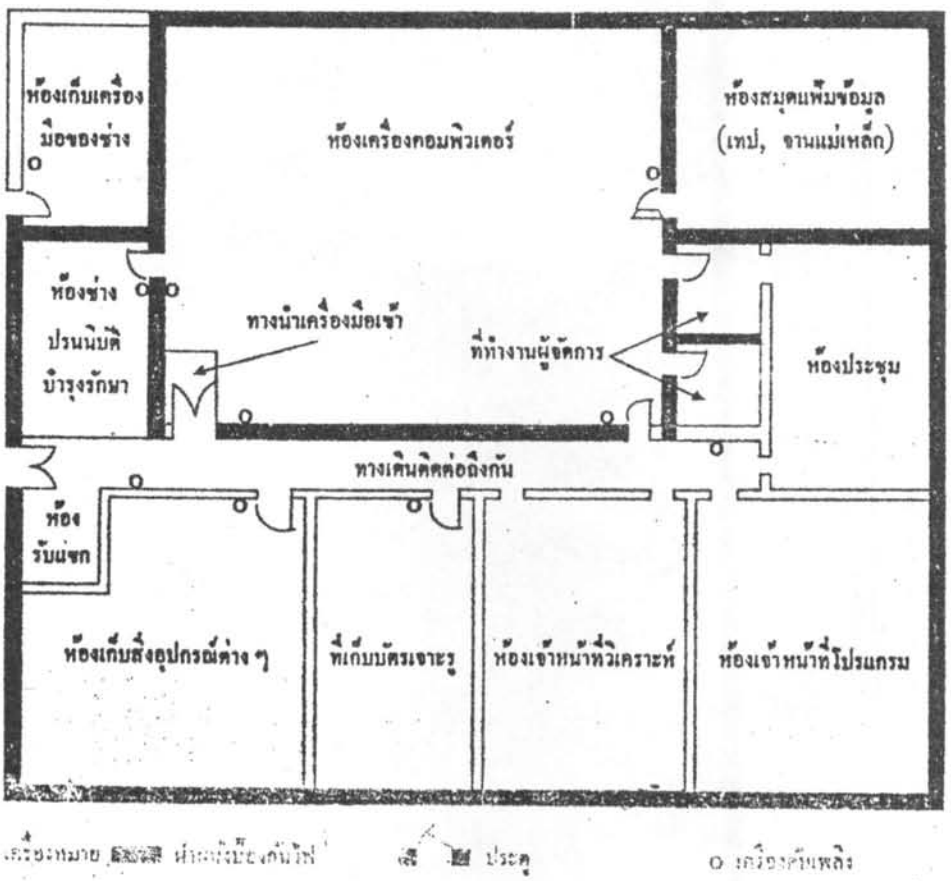
จากการที่บริเวณหน่วยงานคอมพิวเตอร์เป็นบริเวณสำคัญก็ต้องควบคุมเป็นพิเศษ ซึ่ง IBM's "The Consideration of Physical Security in a Computer Environment" ได้แนะนำว่า ผนังตึกควรจะทำคล้ายกระจกเป็นช่วง ๆ สี่เหลี่ยม เพราะอาคารแบบนี้สามารถดูแลได้ง่ายกว่าเพราะมองเห็น ส่วนผนังตึก พื้น พื้นที่ยกขึ้นสูง เพดานและประตูควรใช้วัสดุที่กันไฟได้ และผนังตึกก็ใช้วัสดุที่ไม่ให้เกิดเสียงสะท้อน ตึกคอมพิวเตอร์ควรจะมีทางเข้าทางเดียว โดยการจัดระบบการป้องกันความปลอดภัยแบบ Lock และมียามรักษาการณ์ (Guards) ด้วย ประตูที่ใช้สำหรับเหตุฉุกเฉินหรือใช้กรณีพิเศษ เช่น ใช้ขนเครื่องมือเครื่องใช้ ควรจะเปิดได้เฉพาะด้านในเท่านั้น ตึกคอมพิวเตอร์ที่ปลอดภัยไม่ควรมีหน้าต่าง

ตัวอย่างลักษณะของตึกคอมพิวเตอร์ที่ดีมี 2 แบบ ดังนี้

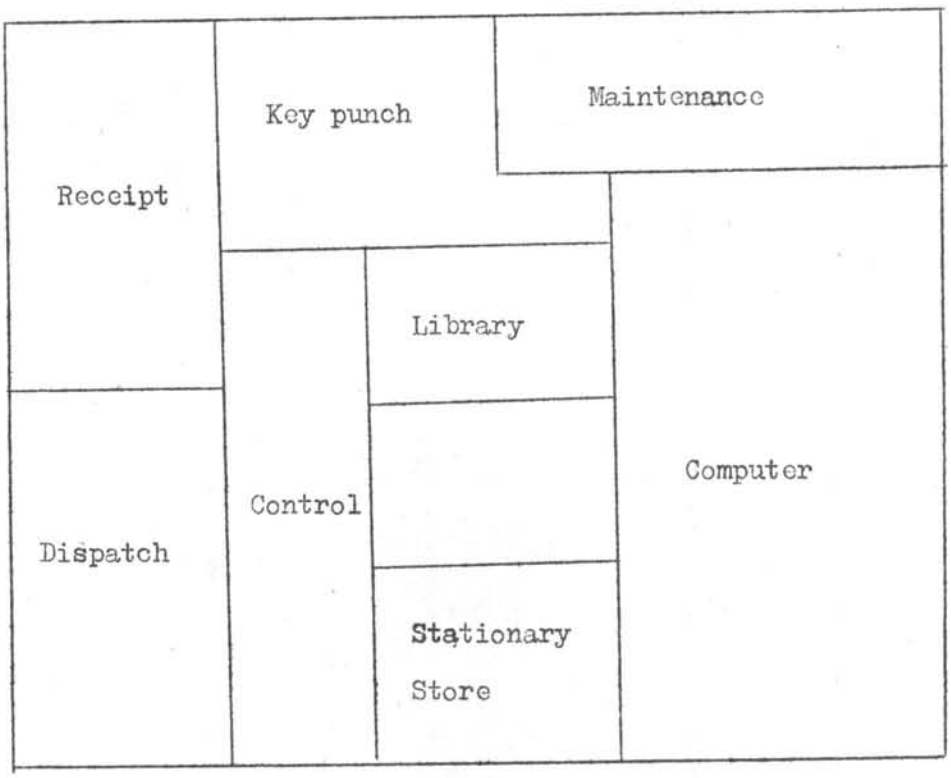
แบบที่ 1 (8) ตามรูป 3.24 การจัดบริเวณสถานที่ต่าง ๆ แบบหนึ่งของหน่วยคอมพิวเตอร์ ซึ่งประกอบด้วยห้องคอมพิวเตอร์ ที่ทำงานของผู้จัดการ ช่างบำรุงรักษา เจ้าหน้าที่โปรแกรม เจ้าหน้าที่วิเคราะห์ระบบ และห้องเจาะบัตร สำหรับเตรียมข้อมูล สำหรับห้องประชุม ห้องรับแขก และที่เก็บสิ่งอุปกรณ์ ควรจัดพื้นที่ให้มีอย่างเพียงพอ ที่เก็บสิ่งอุปกรณ์ได้แก่ ห้องเก็บแฟ้มข้อมูล เช่นบัตรเจาะรู เทป แม่เหล็ก จานแม่เหล็ก เป็นต้น และห้องเก็บเครื่องมือช่าง ห้องสุขาชายหญิง เป็นต้น

ตามปกติขนาดของห้องเครื่องคอมพิวเตอร์ จะมีอัตราส่วนกว้างยาวประมาณ 1:1.5 หรือ 1:2 การวางเครื่องจักรต่าง ๆ ภายในห้องเครื่องคอมพิวเตอร์ควรให้หัวหน้าเจ้าหน้าที่ประจำเครื่องสามารถมองเห็นการทำงานของเครื่องจักรต่าง ๆ ได้ทั่วถึง ห้องแฟ้มข้อมูลควรอยู่ชิดติดกันหรืออยู่ภายในห้องเครื่องคอมพิวเตอร์ ส่วนห้องทำงานสำหรับเจ้าหน้าที่โปรแกรมและเจ้าหน้าที่วิเคราะห์ระบบก็ควรอยู่ติดกัน ห้องของผู้จัดการควรอยู่ใกล้กับบริเวณห้องเจ้าหน้าที่โปรแกรมและเจ้าหน้าที่วิเคราะห์ระบบ ส่วนห้องรับแขกควรตั้งอยู่ใกล้ทางเข้าสำนักงาน ช่างบำรุงรักษาส่วนมากจะต้องการพื้นที่ประมาณ 15 % ของห้องเก็บเครื่องมือ ห้องสมุดแฟ้มข้อมูลขนาดกว้างตาม 24 + 36 ฟุต สามารถเก็บเทปแม่เหล็กได้ประมาณ 10,000 ม้วน เครื่องควบคุมความชื้น และอุณหภูมิควรจัดให้อยู่ในห้องเครื่องคอมพิวเตอร์ ห้องเก็บสิ่งอุปกรณ์ต่าง ๆ ควรมีขนาดใหญ่พอที่จะเก็บสิ่งของต่าง ๆ ได้เป็นจำนวนมาก โดยทั่วไปจะมีขนาดประมาณ 1,200 ลูกบาศก์ฟุต

แบบที่ 2 ตามรูป 3.25 แสดงถึงการจัดห้องคอมพิวเตอร์อีกแบบหนึ่ง ซึ่งจะพิจารณาในด้านการจัดให้มีประสิทธิภาพมากที่สุดด้วย



รูป 3.24 แผนผังการจัดบริเวณต่าง ๆ ของหน่วยงานคอมพิวเตอร์



รูป 3.25 การจัดห้องคอมพิวเตอร์

การจัดห้องคอมพิวเตอร์แบบนี้มีประโยชน์ดังนี้

– ช่วยการทำงานของผู้บริหารด้านคอมพิวเตอร์ในการที่จะเริ่มต้นทบทวนการทำงานทั้งหลายที่อยู่ภายใต้ความรับผิดชอบของเขา ซึ่งเขามีหน้าที่จะต้องตรวจสอบสถานที่ตั้ง สถานที่ทำงานของหน่วยงานต่าง ๆ ที่เกี่ยวกับคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของเขา ตามในรูปนี้ว่าอยู่ในขอบเขตบริเวณที่ถูกต้องหรือไม่

– ช่วยในการทำงานทั้งส่วนรวม เพราะจะทำให้เกิดลักษณะทางเดินของงานเป็นไปอย่างมีแบบแผน เพื่อสดวกในการควบคุม ซึ่งอันนี้บางครั้งอาจจะมีการเปลี่ยนแปลงลักษณะของแต่ละหน่วยงานย่อย เพื่อให้เข้ากับลักษณะของงานที่จะทำให้งานมีประสิทธิภาพ เจ้าหน้าที่ทำงานสดวก ถึงแม้บางครั้งอาจจะต้องใช้จ่ายเงินเพิ่มขึ้นเพื่อการนี้อีกก็ตาม ก็ต้องยอมเสียเงิน เพื่อจะให้ได้ลักษณะทางเดินของงานที่ดี ซึ่งจะเป็นผลตามมา คือ การจัดระบบความปลอดภัยก็สดวก ง่ายต่อการควบคุม เป็นต้น

ค. <u>การควบคุมการเข้าออกภายในตึกคอมพิวเตอร์</u> ดังได้กล่าวมาแล้วว่าห้องเครื่องคอมพิวเตอร์ที่มีควรจะแยกเอาไว้ในตึกคอมพิวเตอร์ต่างหาก เพราะสดวกในการควบคุมการเข้าออกของคน และห้องเครื่องคอมพิวเตอร์ก็ควรจะอยู่ตรงกลางของตึก ทั้งนี้ก็เพื่อจะควบคุมการเข้าออกได้ง่ายเช่นกัน เนื่องจาก

– ผู้เข้าออกในบริเวณที่ทำงานด้านคอมพิวเตอร์ได้ก็ได้แก่ ยามรักษาการณ์ ผู้ที่มาเยี่ยมเยือนซึ่งได้รับอนุญาตให้เข้าได้ หรือผู้ร่วมงานทุกคนที่เกี่ยวข้องเท่านั้น บุคคลเหล่านี้จะสามารถควบคุมการเข้าออกได้ และยังป้องกันเหตุร้ายอื่น ๆ เช่น ไฟไหม้ ลอบวางเพลิง ทำลายข้อมูลโดยอำนาจแม่เหล็กที่แอบเอาติดตัวเข้าไป เป็นต้น และการควบคุมการเข้าออกของตึกจะต้องสร้างระบบความปลอดภัยโดยใช้วิธีการต่าง ๆ กัน เช่น

1 สัญญาณดักจับขโมย
2 สัญญาณแจ้งไฟไหม้
3 สัญญาณดักจับคลื่นแม่เหล็กไฟฟ้า
4 สัญญาณดักจับความสั่นสะเทือนของคลื่น
ฯลฯ

เครื่องมือเหล่านี้จะต่อเข้ากับที่ ๆ เหมาะสมกันที่แต่ละแห่งซึ่งพร้อมจะให้สัญญาณได้เมื่อเกิดเหตุร้าย

– ในอาคารศูนย์คอมพิวเตอร์ผู้ที่ได้รับอนุญาตให้เข้าได้ในแต่ละบริเวณจะเป็น บุคคลหลายประเภท หลายระดับ การใช้รหัสสัญญาณของแต่ละบุคคลเมื่อเข้าออกในแต่ละบริเวณก็ต่างกัน ซึ่งหน่วยงานองค์การใดที่มีคอมพิวเตอร์ ไม่จำเป็นต้องสร้างระบบความปลอดภัยทั้งหลายเหมือนกันหมด ย่อมขึ้นกับลักษณะความสำคัญของงาน งบประมาณที่ได้รับ ฯลฯ เป็นต้น ตัวอย่างดูจากรูป 3.26

ง. <u>ระเบียบวิธีปฏิบัติภายในห้องคอมพิวเตอร์</u> เช่น

– จะต้องห้ามสูบบุหรี่ รับประทานอาหาร ดื่มน้ำ น้ำชากาแฟ ให้ห้องเครื่องเพื่อไม่ให้เครื่องมืออุปกรณ์ทั้งหลายรวมทั้งเทปแม่เหล็ก จานแม่เหล็ก สกปรก กรณีสูบบุหรี่บางแห่งอาจอนุญาต ซึ่งจะต้องระมัดระวังความปลอดภัยมากขึ้นกว่าเดิม

– ห้องเครื่องคอมพิวเตอร์ควรจะทำความสะอาดบ่อย ๆ พื้นห้องไม่ควรเช็ดถูด้วยขี้ฝุ้ง ห้องนี้ควรจะสะอาดที่สุดเท่าที่จะทำได้

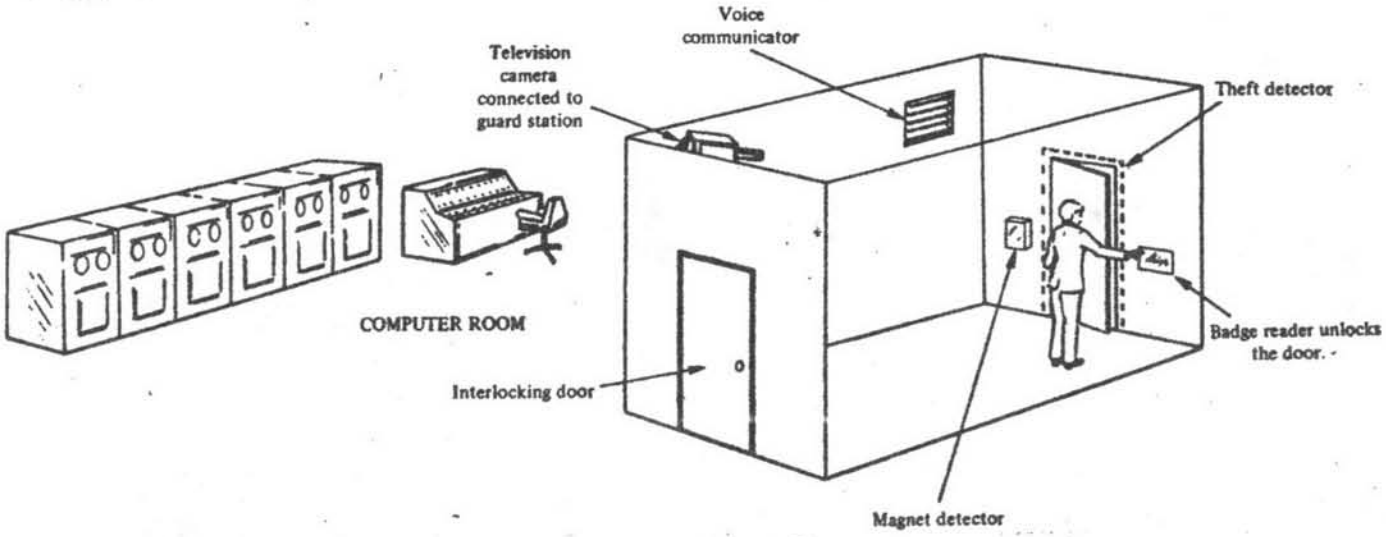
– เจ้าหน้าที่ที่ปฏิบัติงานเกี่ยวกับเครื่องควรจะล้างมือทุกครั้งก่อนเข้ามาทำงานในห้องนี้โดยเฉพาะหลังจากรับประทานอาหารมาแล้ว

– ถ้าเป็นไปได้ห้องเครื่องควรจะมีเครื่องกรองฝุ่นเพราะป้องกันความสกปรกของฝุ่นละอองที่เข้ามาในห้อง

– ภายในห้องเครื่องควรจะนำเอากระดาษพิมพ์ บัตร ที่ไม่จำเป็นออกไปไว้ข้างนอกเพื่อป้องกันเหตุร้ายจากไฟไหม้ เพราะสิ่งเหล่านี้เป็นเชื้อเพลิงอย่างดี แต่ถึงแม้เทปแม่เหล็ก จานแม่เหล็ก ไม่เป็นเชื้อเพลิงก็ตามก็ไม่ควรเก็บไว้ในห้องเครื่อง เพราะต้องการความปลอดภัยของข้อมูลด้วย

– เฟอร์นิเจอร์ทั้งหลายไม่ควรเอามาไว้ในห้องเครื่อง

– ที่ทิ้งกระดาษใช้แล้วควรจะหมั่นตรวจตราและนำไปทิ้งบ่อย ๆ



รูป 3.26 ระบบการควบคุมการเข้ามาสู่ห้องคอมพิวเตอร์

– อุปกรณ์กันน้ำ (Waterproof) ที่จะใช้เมื่อเกิดไฟไหม้เพื่อคลุมป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ กรณีที่ใช้เครื่องดับเพลิงชนิดที่พ่นน้ำออกมาเมื่อเกิดเพลิงไหม้ อุปกรณ์กันน้ำเหล่านี้ควรจะจัดไว้ในที่หยิบง่าย เก็บไว้เป็นสัดส่วนที่สามารถหยิบได้อย่างรวดเร็ว

– กรณีใช้คอมพิวเตอร์หลายเครื่อง อุปกรณ์ของข้อมูลเข้าข้อมูลออกหลายอัน ถ้าเป็นไปได้ควรจะแยกห้องกันไม่ควรเก็บไว้ในห้องเดียวกัน เพื่อป้องกันการถูกทำลายด้วยเหตุร้ายต่าง ๆ และการจัดระบบความปลอดภัยก็จะทำสดวกขึ้น

จ. <u>ความปลอดภัยของห้องพัก</u> ส่วนมากบริเวณที่จะเข้ามายังตึกคอมพิวเตอร์มักจะสร้างห้องพักก่อนเป็นทางผ่านที่จะเข้าไปยังห้องคอมพิวเตอร์หรือตึกคอมพิวเตอร์ ห้องพักนี้ควรจะกว้างพอสำหรับคน 1 – 2 คนอยู่ได้ และเป็นห้องหนึ่งแยกเป็นอิสระต่างหาก คล้าย ๆ กับเป็นประตูที่จะเข้ามายังตึกคอมพิวเตอร์หรือห้องเครื่อง ภายในห้องนี้ต้องมีระบบการควบคุมการเข้าออกของคนโดยติดตั้งทีวีเพื่อแสดงให้เห็นภาพแต่ละบริเวณในตึกคอมพิวเตอร์หรือห้องคอมพิวเตอร์ และมียามคอยดูแลหน้าทีวี ลักษณะดังรูป 3.27

3.2.2 <u>แนวทางในการป้องกันสิ่งอื่น ๆ ภายนอกเครื่องคอมพิวเตอร์</u>

การสร้างระบบการป้องกันภายนอกเครื่องจะช่วยเสริมสร้างระบบความปลอดภัยให้มากขึ้น การป้องกันนี้นอกจากจะเกี่ยวข้องกับบริเวณที่สำคัญที่สุดของศูนย์คอมพิวเตอร์ เช่น ห้องเครื่องคอมพิวเตอร์ ห้องสมุดแฟ้มข้อมูลแล้วยังเกี่ยวข้องกับทุก ๆ ระบบงานที่เกี่ยวข้องกับคอมพิวเตอร์ เช่น ดังนี้ (ตามรูป 3.28)

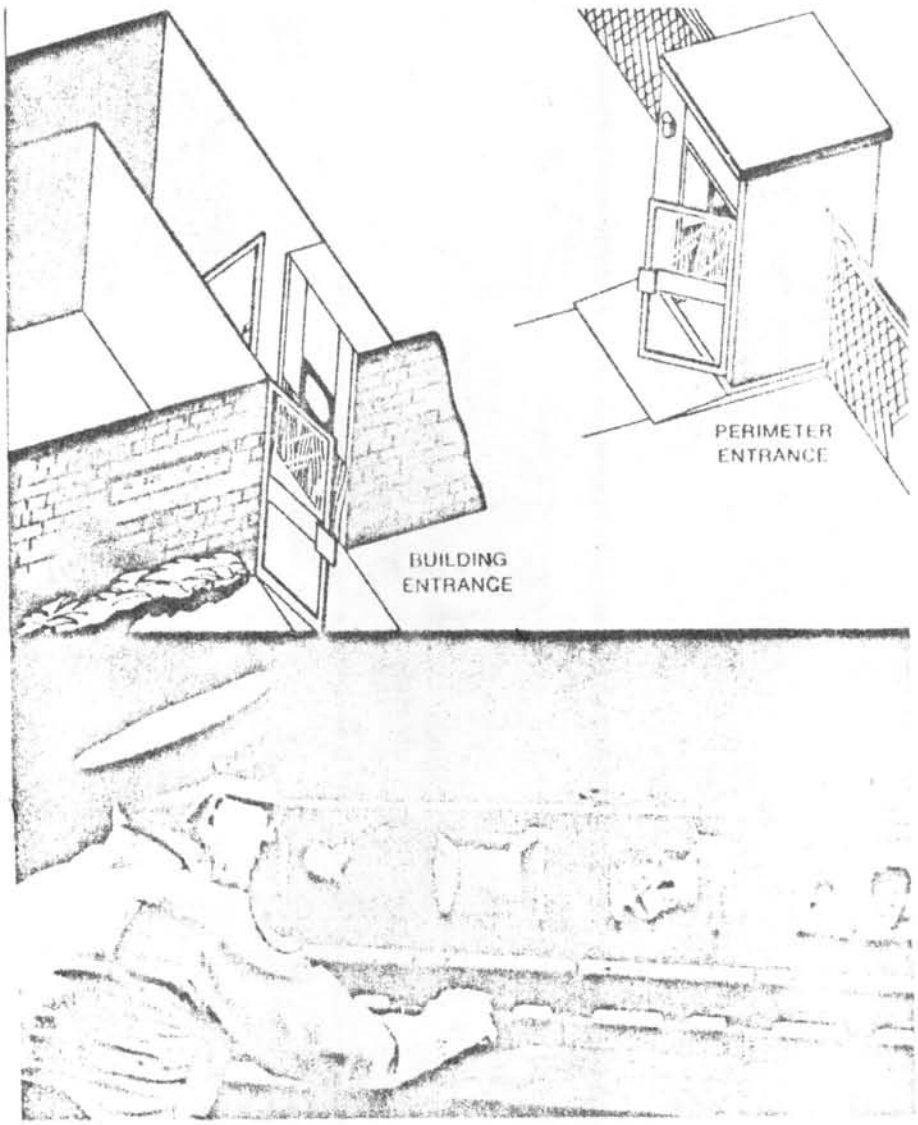
– Programming

– Program maintenance

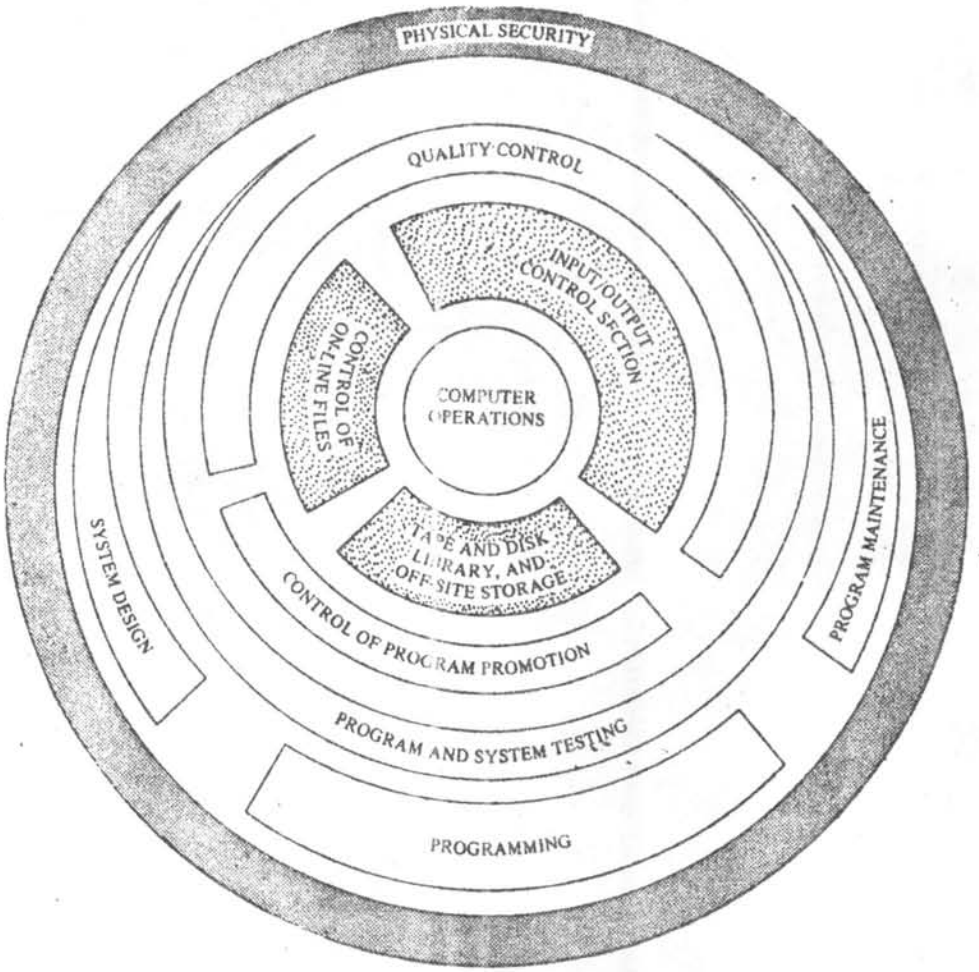
– Progran and System testing

– Control of progran promotion

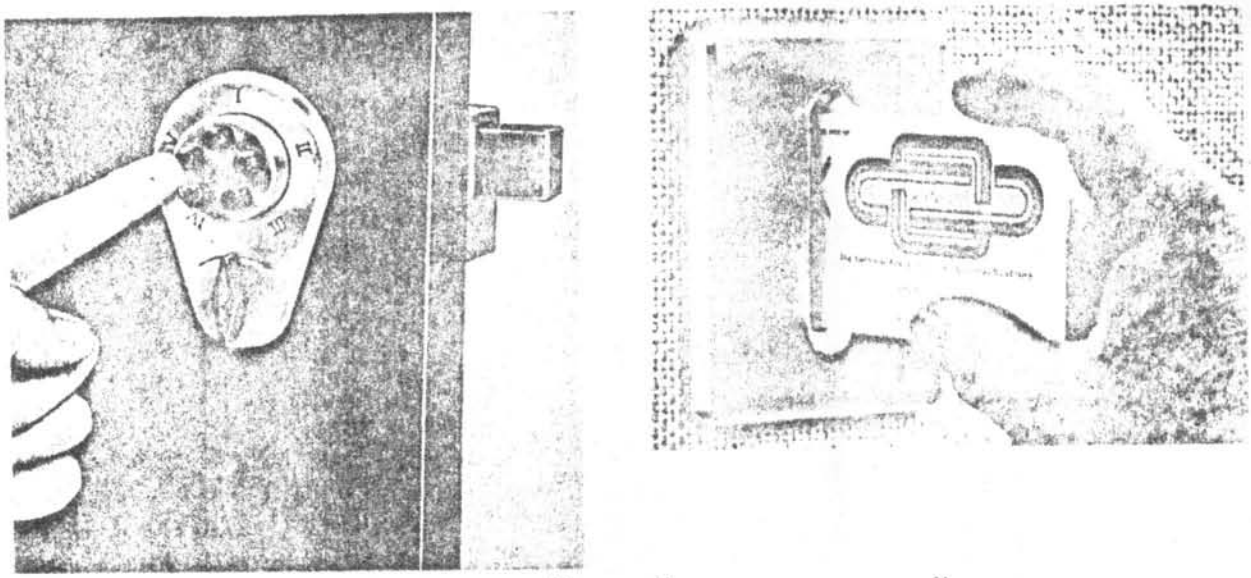
– Quality control



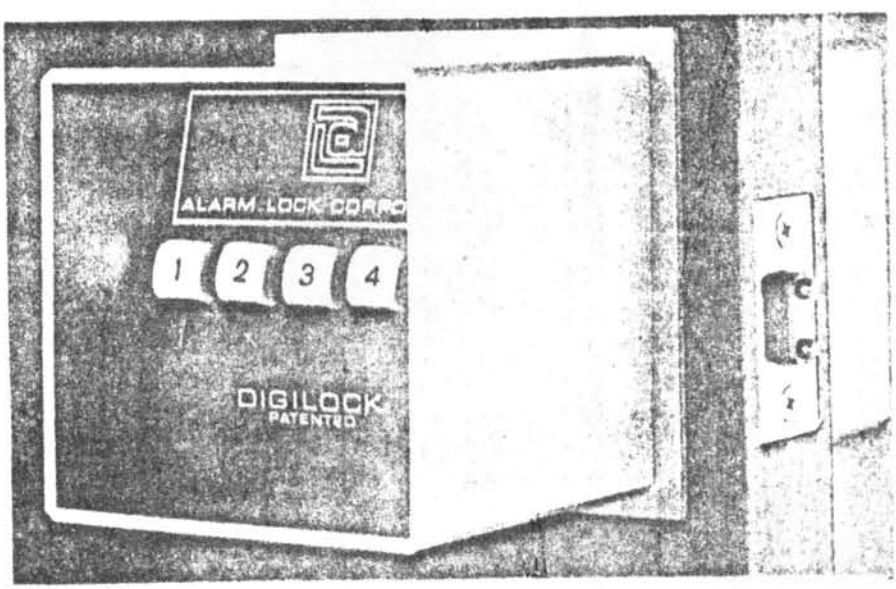
รูป 3.27 ระบบความปลอดภัยของห้องพัก



รูป 3.28 ระบบความปลอดภัยที่จำเป็นในทุก ๆ ด้าน ที่เกี่ยวข้องกับการประมวลผลข้อมูล



รูป 3.29 การควบคุมการเข้าไปในห้องคอมพิวเตอร์โดยใช้ระบบล็อค



- Tape and disk library and off - line storage
- Input/Output control section
- Control of on - line file

เหตุรายต่าง ๆ ที่อาจเกิดขึ้นได้ในส่วนที่เกี่ยวข้องกับคอมพิวเตอร์ได้แก่

- ไฟ อาจเป็นการลอบวางเพลิง หรือไฟไหม้เอง เป็นต้น
- มีผู้บุกรุก บุกรุกเพื่อทำลาย ลักขโมย เป็นต้น
- ความหายนะอื่น ๆ เช่น เหตุเนื่องจากแม่เหล็ก น้ำ เป็นต้น

ก. <u>การป้องกันการบุกรุกของผู้ที่เข้ามายังห้องคอมพิวเตอร์</u> สามารถทำได้ ๓ ชั้น คือ ชั้นนอกสุด ชั้นกลาง ชั้นในสุด

1. <u>ชั้นนอกสุด</u> มีเครื่องกั้นเป็นแนวรอบอาณาเขตของศูนย์คอมพิวเตอร์ เช่น ทำเป็นกำแพง รั้ว เป็นต้น ปกติแต่ละหน่วยงานมักจะไม่ป้องกันชั้นนี้ จะทำต่อเมื่อแยกอาณาเขตของศูนย์คอมพิวเตอร์ออกไปจากที่ห่างไกลอีกต่างหาก

2. <u>ชั้นกลาง</u> เป็นชั้นถัดเข้ามาข้างในโดยทำผนังตึก หน้าต่างและประตู ที่ติดระบบล็อค ตามรูป 3.29 ทั้ง ๆ ที่บางครั้งขโมยมักจะไม่เข้าทางหน้าต่าง ประตู เพราะเขาคิดว่าจะต้องมีการติดสัญญาณป้องกันภัยไว้ ถึงแม้บางครั้งหน้าต่าง ประตูจะเปิดทิ้งไว้ก็ตาม ปกติอาคารศูนย์คอมพิวเตอร์ก็เข้าได้ทางลิฟต์ที่เปิด หลังคาบางแห่งที่ไม่สูงเกินไปหรืออาจเจาะเข้าทางที่ติดเครื่องปรับอากาศก็ได้ หรือเจาะเข้าทางผนังตึก กรณีที่ผนังตึกบาง เพราะที่เหล่านี้ปกติจะไม่ติดสัญญาณอะไรไว้ ดังนั้นศูนย์คอมพิวเตอร์อาจจะมีทั้งยามรักษาการณ์ (Guards) และยามที่เดินตรวจตรา (Patrols) รอบ ๆ บริเวณนั้นก็ได้ ทั้ง ๆ ที่ศูนย์คอมพิวเตอร์บางแห่งอาจจะมีทางเข้าไปในตึกได้ทางเดียวก็ตาม และในขณะเดียวกันในหน่วยงานที่มีความสำคัญมากข้อมูลและโปรแกรมก็ควร

จะเก็บไว้ในที่กันขโมยได้ อันนี้จะกล่าวรายละเอียดตอนต่อไป ข้อที่จำเป็นอีกอย่างหนึ่ง ก็คือ ผู้ดูแล (Receptionist) และผู้ควบคุมเครื่อง ควรจะรู้ว่าควรจะทำอะไร เมื่อมีคนแปลกหน้าบุกรุกเข้ามา ควรจะถามเขาและคิดว่าควรจะเชื่อหรือไม่ ที่เขาพูด เพราะบางครั้งคนแปลกหน้านั้นแอบเข้ามาในศูนย์และมีความประสงค์ร้ายต่อศูนย์ก็ได้

นอกจากนี้ยามรักษาการณ์ก็มีความสำคัญมาก ควรจะจัดเครื่องมือเครื่องใช้ ในการทำงานของเขาให้อย่างดี เช่น ทีวี ต้องใช้การได้เสมอ เป็นต้น สำหรับคุณสมบัติ ของยามรักษาการณ์ก็จำเป็นต้องเป็นคนที่มีความสังเกตเป็นพิเศษ มีไหวพริบดี พิจารณา เหตุการณ์เฉพาะหน้าได้ดี เพราะบางทีขโมยต้องการเข้ามาในศูนย์อาจจะโกหกบอกว่า เป็นเจ้าหน้าที่ หรือผู้จัดการใหญ่ก็ได้ ซึ่งอันนี้บริษัทใหญ่ ๆ ควรจะมีการฝึกอบรมและ แนะนำตัวเองแก่ยามรักษาการณ์ ตลอดจนสิ่งน่ารู้ทั้งหลายโดยเจ้าหน้าที่ในหน่วยรักษา ความปลอดภัยของบริษัทเอง หรือฝึกอบรมบริษัทข้างนอก เป็นต้น

ข. <u>ชนิดของเครื่องมือที่ใช้ในสัญญาณเมื่อมีภัย</u> ปัจจุบันมีมากมายหลายชนิด และได้มีผู้คนคิดเรื่อย ๆ ผู้สนใจติดตามจากวารสารได้ ทุกชนิดที่ได้ผลดีขึ้น และได้มีผู้คนคิด ขึ้น มีประโยชน์แต่ละด้านต่างกัน จะต้องเลือกใช้เฉพาะที่จำเป็น มีประโยชน์ คุ้มค่า กับเงินและงานที่ลงทุนไป ไม่จำเป็นต้องใช้ทุกอย่างเพราะบางชนิดแพงมาก เครื่องมือ ที่ใช้ให้สัญญาณเมื่อมีภัยที่จำเป็น ได้แก่

๑. อุปกรณ์ที่ให้สัญญาณเมื่อเกิดไฟไหม้ (Fire detector)
แบ่งเป็น ๒ แบบ

- ชนิดที่ให้สัญญาณเมื่อได้รับความร้อน (Heat detector)
- ชนิดที่สัญญาณเมื่อได้รับควัน (Smoke detector)

รายละเอียดจะกล่าวตอนต่อไป

2. อุปกรณ์ที่ให้สัญญาณเมื่อได้รับอำนาจแม่เหล็ก (Magnet detector) ใช้ป้องกันข้อมูลในเทปแม่เหล็ก จานแม่เหล็ก เพราะอำนาจแม่เหล็กสามารถจะทำลายข้อมูลบนเทปแม่เหล็ก และจานแม่เหล็กได้ภายในช่วงรัศมีต่าง ๆ กันแล้วแต่ประสิทธิภาพของแม่เหล็ก เพื่อป้องกันผู้บุกรุกเข้ามาทำลายข้อมูล หรือแซกที่มาเยี่ยมเยือนศูนย์คอมพิวเตอร์ ดงอาจพอใส่กระเป๋าไว้ ดังนั้นจะต้องติดตั้งอุปกรณ์ที่ให้สัญญาณเมื่อได้รับอำนาจแม่เหล็กในช่วงรัศมีต่างกันไว้ สัญญาณนี้จะเป็นแบบไหนก็แล้วแต่บริษัทผู้ผลิต

3. บัตรที่มีรหัส ใช้กรณีเมื่อผ่านเข้าประตู จะต้องหย่อนบัตรนี้ลงในเครื่องมืออ่านบัตรก่อน บนบัตรจะมีรหัสเมื่อใช้รหัสที่ถูกต้องก็สามารถผ่านเข้าประตูไปได้ ซึ่งป้องกันผู้บุกรุกเข้าไปโดยไม่ได้รับอนุญาต รหัสบนบัตรมักจะใช้เลข ๑๐ ตัว หรือจะหาวิธีคิดขึ้นเองก็ได้ รหัสนี้จะได้มาโดยวิธีการลับเฉพาะ (Cryptographic procedure) ในกรณียามลาดตระเวนที่ตรวจตราทั้งศูนย์คอมพิวเตอร์ก็ใช้วิธีนี้ด้วย

4. ทีวี (Closed - circuit television) ใช้ช่วยในบริเวณที่ต้องการโดยจะต่อเชื่อมโยงมายังห้องที่มียามรักษาการณ์เพื่อทราบการเคลื่อนไหวแต่ละอาณาบริเวณ ภายในศูนย์คอมพิวเตอร์ได้

5. อุปกรณ์ที่ให้สัญญาณเมื่อได้รับเสียง (Detection of sound and vibration) จะใช้ไมโครโฟนช่วยโดยติดไมโครโฟนไว้ในบริเวณใดบริเวณหนึ่งและต่อโยงไปยังห้องที่มียามรักษาการณ์ เมื่อได้รับเสียงไมโครโฟนดังโดยอัตโนมัติ ปกติจะติดไว้ที่ผนังอาคารมักใช้ในกรณีการต่อสายโทรศัพท์เพื่อลอบฟังการสนทนา

6. เครื่องดักจับชนิด อาจติดที่ประตูหรือที่เก็บข้อมูลทั้งเทปแม่เหล็กและจานแม่เหล็ก เมื่อมีผู้บุกรุกเข้ามาทางประตูเครื่องนี้ก็จะให้สัญญาณดังขึ้น หรือเป็นสัญญาณแบบอื่นก็ได้แล้วแต่บริษัทผู้ผลิต

นอกจากนี้ควรจะพิจารณาส่วนประกอบอื่น ๆ ที่เกี่ยวข้องด้วย เช่น สถานที่อยู่ที่ตั้งของส่วนราชการ ได้แก่ โรงพยาบาล สถานีตำรวจ ฯลฯ หรือเบอร์โทรศัพท์ภายใน

แต่ละเบอร์ภายในศูนย์เองต้องมีไฟพร้อมเพื่อสะดวกในการติดต่อเมื่อเกิดภัย เป็นต้น

ตัวอย่างของระบบความปลอดภัยแบบหนึ่ง ดูจากรูป 3.28

3. ชั้นในสุด เป็นชั้นที่ใกล้ชิดกับเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบการทำงานมากที่สุด หน่วยงานส่วนมากมักจะไม่สนใจความปลอดภัยในชั้นนี้มากนัก ทั้ง ๆ ที่ระบบความปลอดภัยของชั้นในสุดนี้สำคัญมาก พิจารณาได้ 4 แบบ คือ

ก. ตู้นิรภัย (Safes and cabinets)
ข. ที่ ๆ สร้างขึ้นและวางระบบความปลอดภัย (Vaults)
ค. ห้องที่เก็บอุปกรณ์ทั้งหลาย (Record storage rooms)
ง. บริเวณที่ทำงาน (Closed area)

ก. ตู้นิรภัย ปกติจะเป็นแบบทั้งกันขโมยและกันไฟ และป้องกันการถูกโจรกรรมด้วย ผู้ใช้จะต้องเลือกใช้เอง บริษัทที่ผลิตที่มีชื่อเสียงในอเมริกาได้แก่ U.S. Safe Manufacturers 'National Association' จะผลิตทั้งชนิดกันไฟและกันขโมย ผู้สนใจศึกษารายละเอียดได้ต่อไป แต่อย่าลืมว่าเมื่อใช้ตู้นิรภัยแล้ว กุญแจที่ใช้เปิดก็ไม่ควรแขวนไว้ที่เปิดเผยโดยเข้าใจว่าจะหยิบง่าย เพราะถ้าผู้บุกรุกได้เข้ามาถึงชั้นในสุดนี้ได้ก็จะสามารถเอากุญแจเปิดตู้นิรภัยได้

ข. Vaults หมายถึงที่ที่หนึ่งที่ถูกสร้างขึ้นมาอย่างถาวร และเคลื่อนย้ายไปไหนไม่ได้ เพื่อเก็บอุปกรณ์ข้อมูลทั้งหลาย ที่ ๆ สร้างขึ้นนี้ต้องวางระบบความปลอดภัยไว้ด้วยทั้งผนัง พื้น หลังคา ประตู วัสดุที่จะใช้สร้าง และการวางระบบความปลอดภัยจะใช้อย่างไร ระดับไหน จะเป็นชนิดทั้งกันขโมยและกันไฟหรือแบบใดแบบหนึ่งก็ต้องพิจารณาตามความเหมาะสม นอกจากนี้ทางสมาคม Mational Fire Protection Association ของอเมริกาได้แนะนำว่าความจุของแต่ละ Vaults ไม่ควรจะมากกว่า 5,000 ลูกบาศก์ฟุต

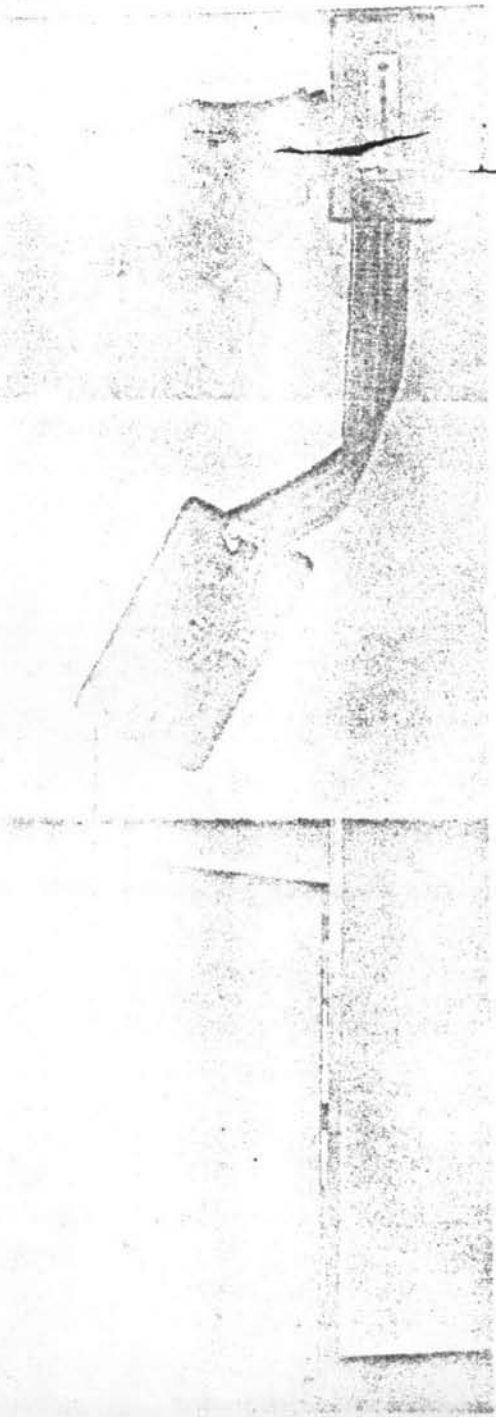
ก. Record storage rooms เป็นบริเวณที่สร้างขึ้นมาเพื่อป้องกันความปลอดภัยเช่นกัน แต่จะมีขนาดใหญ่กว่า Vault เนื่องจากบริเวณที่สร้างขึ้นนี้มีบริเวณกว้าง ดังนั้น การป้องกันภัยจากไฟ น้ำ ขโมย ฯลฯ จึงมีน้อยกว่า Vault ในกรณีที่ต้องการเก็บข้อมูลรายการที่สำคัญมากก็ควรจะเก็บไว้ใน Vault ก่อนแล้วอาจจะเก็บซ้อนไว้ใน Record storage room อีกทีก็ได้ ภายในบริเวณที่สร้างขึ้นนี้ควรจะมีระบบการป้องกันไฟไหม้โดยใช้อุปกรณ์ดับเพลิงชนิดพ่นน้ำออกมาแบบอัตโนมัติหรือชนิดที่พ่นเป็นแก๊สออกมา และบริเวณข้างนอกใกล้ ๆ กับห้องที่สร้างขึ้นนี้ควรจะมีอุปกรณ์กันไฟอีกชั้นหนึ่ง ความจุของห้องที่สร้างขึ้นจะมีความจุเท่าไรก็ได้ แต่ก็ไม่ควรจะมากกว่า 65,000 ลูกบาศก์ฟุต โดยให้เก็บเฉพาะข้อมูล

ง. Closed area เช่นบริเวณที่ทำงานเกี่ยวกับด้านคอมพิวเตอร์ ห้องคอมพิวเตอร์ เป็นต้น บริเวณนี้ควรมีทางเข้าทางเดียว มียาม หรือผู้ดูแลเฝ้าตลอดเวลาที่มีการทำงาน ทางออกปกติจะใช้เป็นแบบ 'Panic bar' คือใช้เป็นทางออกเข้าไม่ได้ ทางเข้าอาจจะใช้ระบบ 'A card lock' คือหย่อนบัตรลงไปตรงข้างหน้าประตู ถ้าบัตรถูกต้องประตูก็จะเปิดให้เข้าได้ โดยบัตรนี้จะเป็นแบบเฉพาะ หรือจะใช้ 'A code bey' ตามรูป 3.30 ซึ่งแตกต่างกันไปสำหรับแต่ละคนเพราะการอนุญาตให้เข้าได้ในแต่ละห้อง ให้เข้าได้ในคนหลายระดับ

ทั้ง 4 แบบ ที่กล่าวมาข้างต้นจะต้องมีสัญญาณเตือนภัยเสมอ และการพิจารณาวัสดุต่าง ๆ ที่เกี่ยวข้องว่าจะเกิดความเสียหายอย่างไรบ้างเมื่อเกิดไฟไหม้ตามอุณหภูมิที่สูงขึ้น ดูรูป 3.31

การป้องกันไฟไหม้ เนื่องจากไฟไหม้เป็นเหตุอีกอย่างหนึ่งที่เกี่ยวข้องกับศูนย์คอมพิวเตอร์ ซึ่งอาจเกิดขึ้นโดยอุบัติเหตุหรือเกิดขึ้นเองตามธรรมชาติ หรืออาจเกิดโดยการลอบวางเพลิงจากผู้ที่บุกรุกเข้าไป ผู้บริหารจะต้องสนใจเอาใจใส่ในการป้องกันเหตุร้ายจากไฟเป็นอันดับแรก เนื่องจากไฟไหม้เป็นภัยที่ร้ายแรงมาก มันจะไม่เกิดความเสียหายเฉพาะบริเวณที่เกิดไฟไหม้เท่านั้น มันจะลุกลามไปทั้งศูนย์คอมพิวเตอร์ มีข้อที่ควรคำนึงถึงอีกอย่างหนึ่งก็คือว่า เหตุร้ายที่เกิดจากไฟไหม้นี้

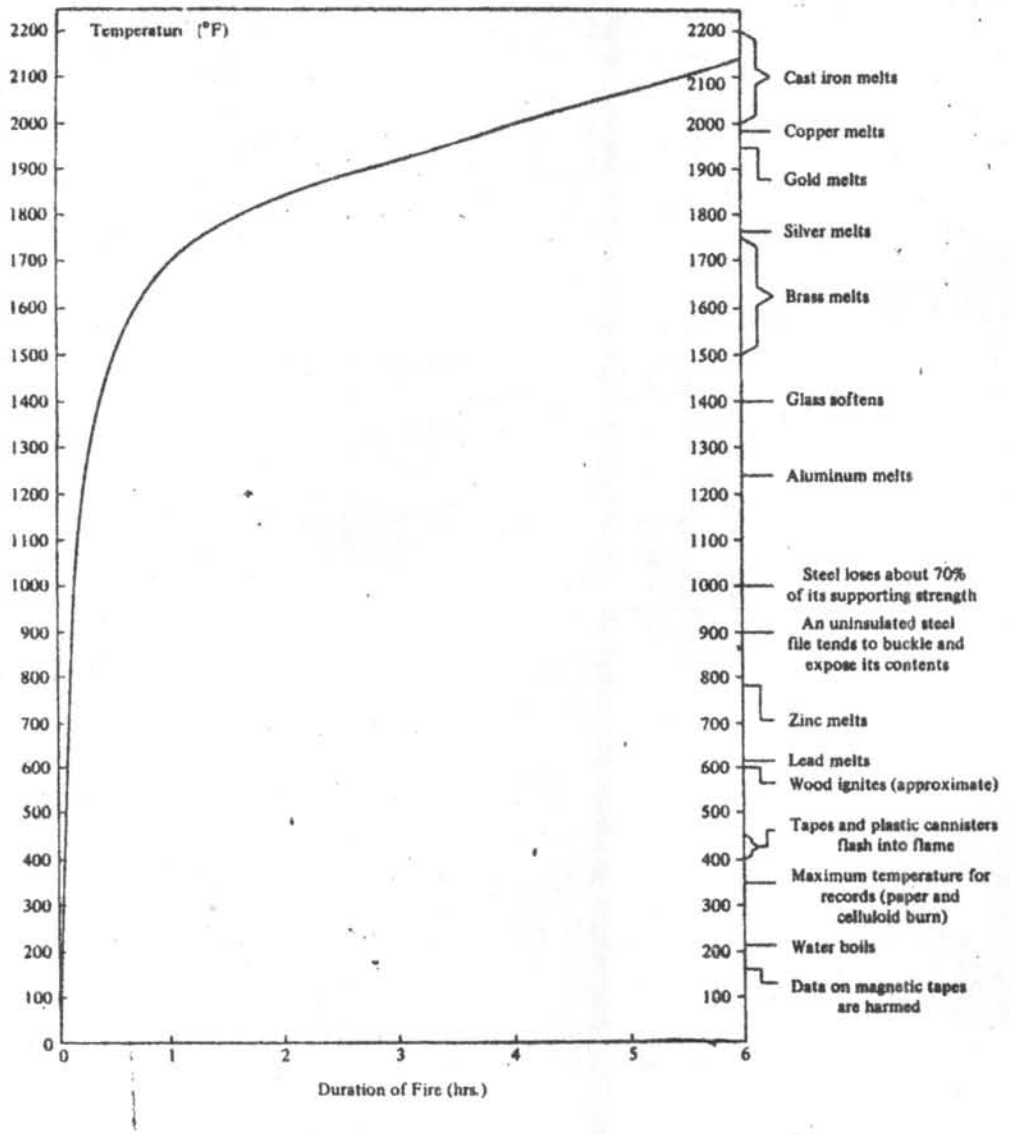
รูป 3.30 ระบบการทำงานโดยการใช้ a coded key system



only this key

tells this unit

to open this door



รูป 3.31 รูปกราฟแสดงถึงผลของวัสดุต่าง ๆ ที่จะเกิดขึ้นในระหว่างที่เกิดไฟไหม้

ย่อมจะมีขึ้นได้ เป็นไปได้ที่โอกาสจะเกิดไฟไหม้ไม่มีเลย ดังนั้นเราต้องพยายามให้มันมีโอกาสเกิดขึ้นน้อยที่สุด ควรจะพิจารณาในส่วนที่เกี่ยวข้อง ดังนี้

1. การเลือกทำเลที่ตั้งของศูนย์คอมพิวเตอร์ การป้องกันไฟไหม้ควรจะพิจารณาตั้งแต่เริ่มนำเครื่องคอมพิวเตอร์เข้ามาติดตั้งแล้ว **ต้องพิจารณา** ภายนอก ภายในที่ทำการศูนย์ทั้งหมด

2. การติดตั้งเครื่องปรับอากาศและอุปกรณ์อื่น ๆ ต้องเลือกใช้ให้พอเหมาะ

3. อุปกรณ์เครื่องมือเครื่องใช้ไม่วางไว้ในตำแหน่งที่อาจจะเกิดไฟไหม้ได้ เช่น กระดาษพิมพ์ผลลัพธ์ต้องไม่นำไปวางใกล้ที่ ๆ เครื่องร้อน

4. อุปกรณ์ช่วยในการดับเพลิงวางไว้ในที่ ๆ เห็นได้ชัดเจน และต้องฝึกอบรมเจ้าหน้าที่ที่ทำงานซึ่งเกี่ยวของกับสถานที่นั้น ๆ อยู่เสมอ เพื่อความคล่องตัวและกันลืม

5. อุปกรณ์ป้องกันไฟไหม้ ต้องติดตั้งในที่พอเหมาะ

6. เครื่องเตือนสัญญาณเมื่อเกิดไฟไหม้ควรจะเป็นแบบที่ให้สัญญาณภายในห้องที่เกิดไฟไหม้ และเชื่อมโยงสัญญาณให้ไปเกิดยังบริเวณที่เกี่ยวข้อง เพื่อให้ผู้เกี่ยวข้องสามารถรู้และช่วยกันระงับได้

7. ทุก ๆ คนที่เกี่ยวข้องในศูนย์คอมพิวเตอร์จะต้องรู้และจำวิธีปฏิบัติเมื่อเกิดสัญญาณของแต่ละเครื่องมือว่าจะต้องทำอย่างไรบ้าง เพื่อจะได้ปฏิบัติได้ถูกต้อง

8. การวางระบบความปลอดภัยในศูนย์คอมพิวเตอร์นี้ จะต้องนึกถึงความปลอดภัยของเจ้าหน้าที่ในหน่วยงานนั้นด้วย เพราะวิธีการบางอย่างอาจเป็นอันตรายต่อคน เช่น ก๊าซคาร์บอนไดออกไซด์ช่วยดับไฟ อาจจะถูกคนต้องมีวิธีป้องกันอีก

9. ข้อมูลที่สำคัญ ต้องเก็บไว้ในอุปกรณ์ที่กันไฟได้

10. ข้อมูลทั้งหลายต้องเก็บไว้นอกห้องเครื่องคอมพิวเตอร์

11. ข้อมูลที่นำไปใช้ทั้งกรณีใช้สร้างแฟ้มข้อมูลใหม่จะต้องมีหลักฐานเก็บไว้อีกชุด

12. การใช้อุปกรณ์ประกอบอื่น ๆ กับคอมพิวเตอร์ จะต้องเตรียมวิธีการป้องกันไว้เพื่อป้องกันการถูกทำลาย เช่น ข้อมูลในเทปแม่เหล็กถูกทำลาย

13. ควรจะมีการประกันภัย ทั้งศูนย์คอมพิวเตอร์หรือเครื่องมือประกอบอื่น ๆ

ฯลฯ

อุปกรณ์ดับเพลิง แบ่งได้เป็น

1. อุปกรณ์ดับเพลิงชนิดใช้คนช่วย (Hand - operated extinguishers)
2. อุปกรณ์ดับเพลิงชนิดอัตโนมัติ (Automatic extinguishers)

1. อุปกรณ์ดับเพลิงชนิดใช้คนช่วย

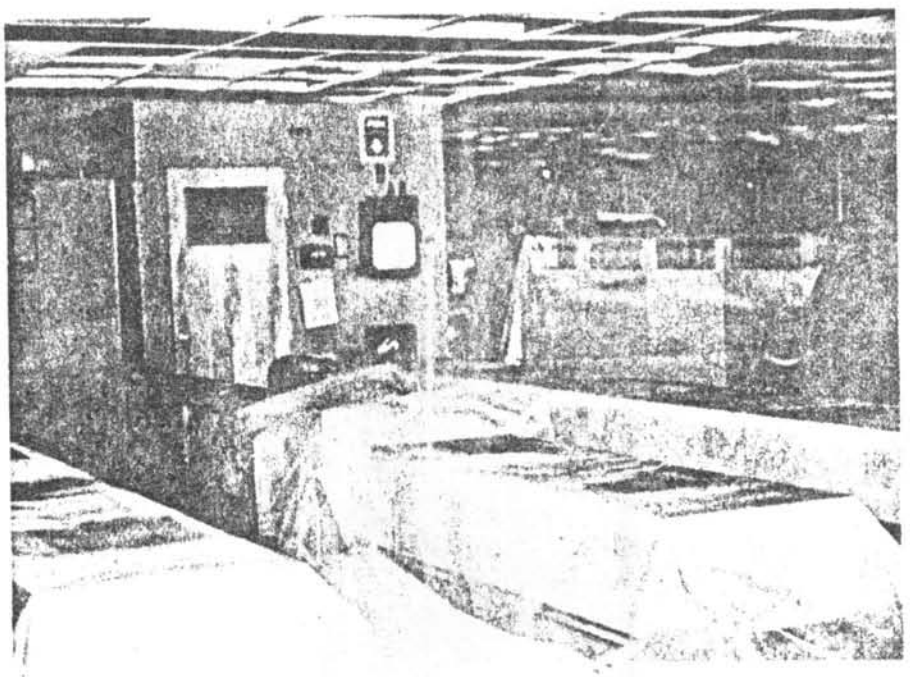
- อาจจะใช้กาซคาร์บอนไดออกไซด์ ซึ่งใช้กรณีเมื่อเกิดไฟไหม้อุปกรณ์ไฟฟ้า
- อาจจะใช้กรดโซดา เมื่อเกิดไฟไหม้กระดาษ

นอกจากนี้อุปกรณ์ดับเพลิงควรจะมีรายละเอียดบอกชัดเจน เช่น ใช้เมื่ออะไรไหม้ จะต้องมีการตรวจสอบอุปกรณ์ดับเพลิงเสมอว่าใช้เหลืออีกมากไหม ต้องทบทวนวิธีการปฏิบัติในการใช้บ่อย ๆ เพื่อกันลืม

2. อุปกรณ์ดับเพลิงชนิดอัตโนมัติ ซึ่งไม่ต้องใช้คนช่วย ที่นิยมใช้กันทั่วไปมี 3 แบบ คือ

ก. Sprinkers ประกอบด้วยน้ำช่วยในการดับเพลิง เมื่อเกิดไฟไหม้จะมีสัญญาณไปเตือนอุปกรณ์อันนี้ซึ่งอยู่บนเพดานห้องเครื่อง และอุปกรณ์ดับเพลิงนี้จะพ่นน้ำออกมาจนไฟดับแล้วจึงจะหยุด ห้องคอมพิวเตอร์ระบบนี้ ซึ่งนิยมใช้มาก เพราะปลอดภัยแก่คนด้วย แต่มีข้อเสียคือทำความเสียหายแก่เครื่องจักร ซึ่งอาจตัดสัญญาณเตือนภัยก่อน เพื่อคนที่ได้ยินจะได้ใช้พลาสติกคลุมก่อน ดังรูป 3.22

ข. แก๊สคาร์บอนไดออกไซด์ ใช้ดับเพลิง และแก๊สนี้มีคุณสมบัติคือไม่มีกลิ่น ไม่มีสี และมีอันตรายต่อชีวิต เมื่อใช้อุปกรณ์ดับเพลิงชนิดนี้เมื่อเกิดไฟไหม้ในห้องใดบุคคลที่ทำงานในห้องนั้นจะต้องรีบออกจากห้องอย่างรวดเร็ว มีการป้องกันอย่างง่าย ๆ



รูป 3.32 การใช้พลาสติกปกคลุมเครื่องจักรในกรณีที่ใช้อุปกรณ์ดับเพลิงชนิดที่ใช้น้ำ

เมื่อมีความจำเป็นที่ต้องเข้าไปในห้องเกิดเพลิงไหม้ก็ควรจะเตรียมอุปกรณ์ช่วยในการหายใจติดตัวแต่ละคน

ค. Halon เป็นก๊าซที่มีอันตรายต่อคนเหมือนกัน แต่น้อยกว่าคาร์บอนไดออกไซด์ แต่ก๊าซนี้บางชนิดก็อันตรายมาก ซึ่งอันนี้จะมีกลิ่นเหม็นอย่างแรง คนจะทนไม่ได้ต้องรีบออกจากห้องทันที เมื่อก๊าซนี้ถูกพ่นออกมาจากอุปกรณ์ดับเพลิง

อุปกรณ์ที่ให้สัญญาณเมื่อมีไฟไหม้ (Fire detectors) ปกติจะต้องใช้ควบคู่ไปกับอุปกรณ์ดับเพลิงอัตโนมัติทั้ง 3 แบบ ซึ่งเมื่อเกิดไฟไหม้ขึ้น อุปกรณ์นี้จะให้สัญญาณไปทั่วบริเวณที่ได้ติดตั้งระบบนี้ไปถึง แล้วอุปกรณ์ดับเพลิงอัตโนมัติทั้งหลายที่ติดตั้งก็จะทำงานทันที ในกรณีศูนย์คอมพิวเตอร์ขนาดเล็กและงานก็ไม่สำคัญมากนักก็อาจจะติดตั้งเฉพาะอุปกรณ์ที่ให้สัญญาณเมื่อมีไฟไหม้ก็เพียงพอ เพราะเมื่อให้สัญญาณแล้ว คนก็จะมาดับเพลิงทันทีโดยใช้เครื่องดับเพลิงชนิดที่ใช้คนช่วย และอุปกรณ์ดับเพลิงที่ใช้ก๊าซนี้มีราคาแพง ส่วนที่ใช้น้ำบางทีเกิดความเสียหาย แต่น้ำก็ทำความเสียหายให้น้อยกว่าไฟไหม้ เหล่านี้เกินความจำเป็นที่จะใช้ และอีกกรณีหนึ่งก็คือโอกาสที่จะเกิดไฟไหม้ขณะที่เครื่องคอมพิวเตอร์ทำงานจะมีมากกว่าตอนเครื่องหยุดทำงาน เช่น เวลากลางคืน เวลาที่เครื่องทำงานนั้นมักจะมีอย่างน้อยที่สุดก็เจ้าหน้าที่ควบคุมเครื่องประจำอยู่ แต่ศูนย์คอมพิวเตอร์ใหญ่ ๆ การทำงานทั้งหลายจะเป็นแบบอัตโนมัติมากกว่า คนอยู่ประจำก็ไม่มากควรจะติดตั้งทั้งอุปกรณ์ที่ให้สัญญาณเมื่อเกิดไฟไหม้ และอุปกรณ์ดับเพลิง

อุปกรณ์ที่ให้สัญญาณเมื่อมีไฟไหม้ ที่ใช้กันมี 2 แบบ

ชนิดที่ให้สัญญาณเมื่อได้รับควัน (Smoke detector)

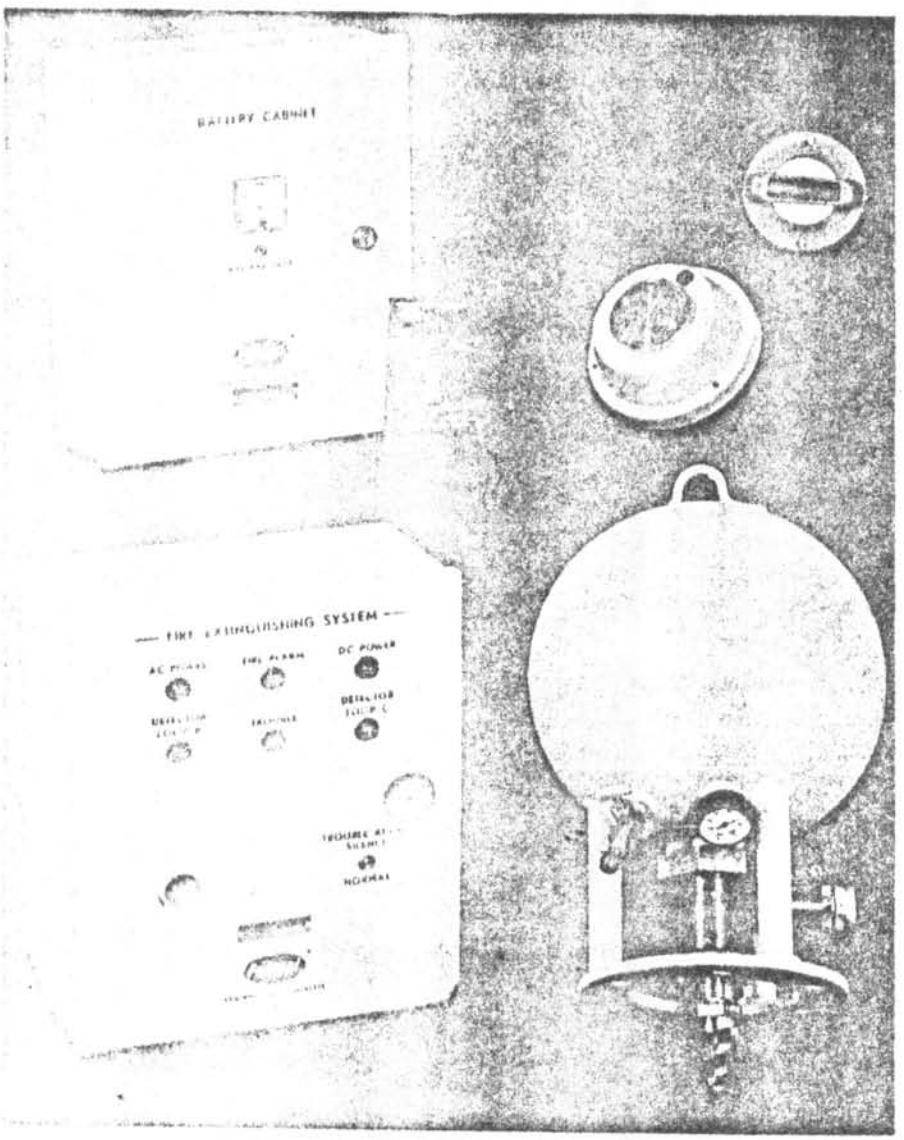
ชนิดที่ให้สัญญาณเมื่อได้รับความร้อน (Heat detector)

1. <u>อุปกรณ์ที่ให้สัญญาณไฟไหม้เมื่อได้รับความร้อน</u> จะให้สัญญาณต่อเมื่อมีความร้อนเกิดขึ้น เนื่องจากคอมพิวเตอร์ประกอบด้วยอุปกรณ์ทางไฟฟ้า ซึ่งจะมีความร้อนเกิดขึ้นเสมอ และอุปกรณ์ที่ให้สัญญาณนี้จะติดตั้งเป็นแห่ง ๆ ถ้าติดใกล้กับอุปกรณ์ไฟฟ้าอันใดอันหนึ่งแล้วความร้อนที่เกิดขึ้นถึงจุดหนึ่ง อุปกรณ์ที่ให้สัญญาณเมื่อได้รับความร้อนก็จะส่งสัญญาณออกมาทันที แต่ถ้าติดไกลจากตำแหน่งที่เกิดไฟไหม้จริง ๆ ความร้อนเนื่องจากไฟไหม้ที่เกิดขึ้นกว่าจะไปถึงอุปกรณ์ที่ให้สัญญาณก็ช้า และปกติในห้องคอมพิวเตอร์จะต้องมีเครื่องปรับอากาศ ช่วยปรับอุณหภูมิในห้องให้คงที่ ถ้าติดอุปกรณ์ที่ให้สัญญาณเมื่อได้รับความร้อนเชื่อมกับอุปกรณ์ดับเพลิงอัตโนมัติ เช่น ใช้น้ำแล้วกว่าอุปกรณ์ดับเพลิงจะทำงานได้ก็อาจเกิดความเสียหายมากแล้วก็ได้ วิธีนี้จึงไม่ค่อยนิยมใช้กัน มักจะใช้คนช่วยดับเพลิงมากกว่า

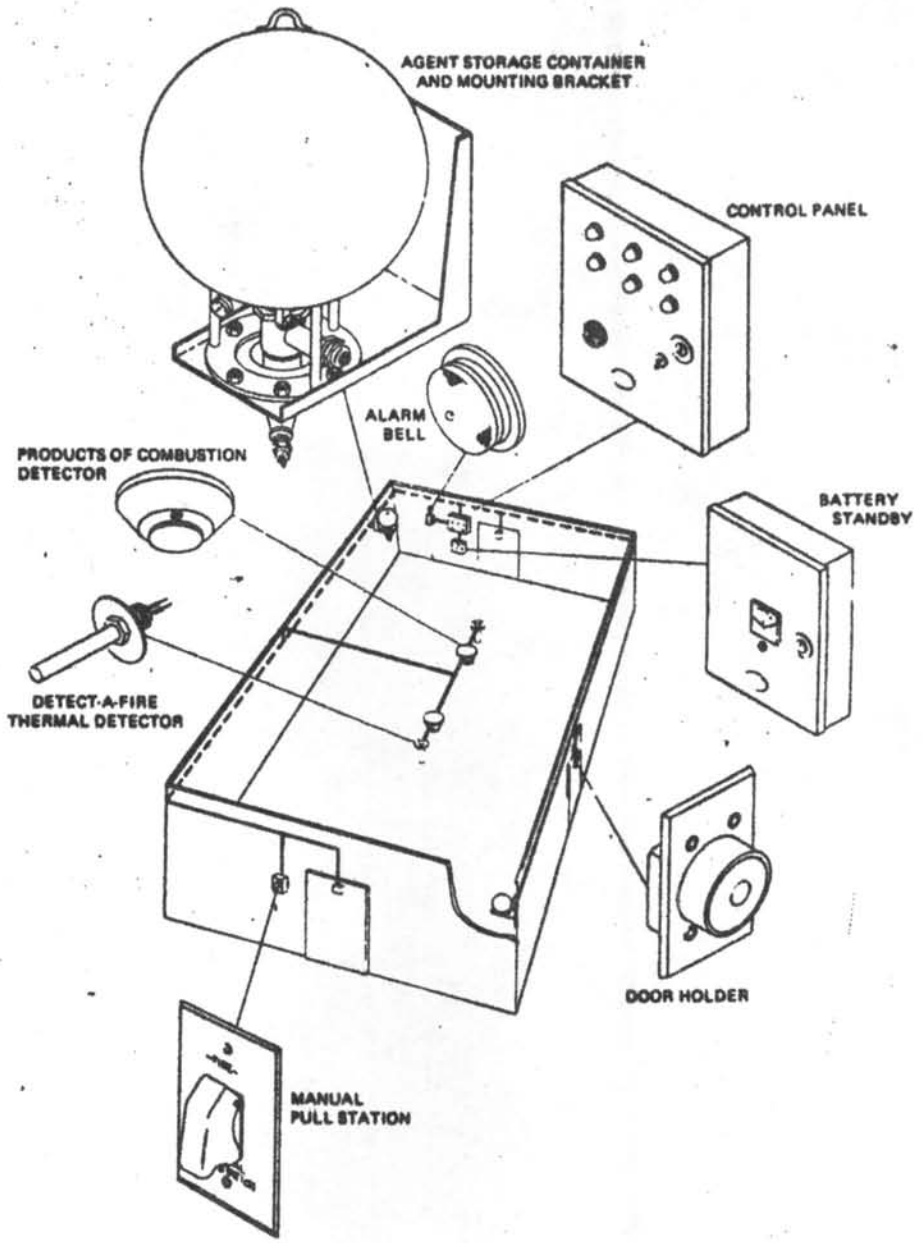
2. <u>อุปกรณ์ที่ให้สัญญาณไฟไหม้เมื่อได้รับควัน</u> แบบนี้รับความรู้สึกต่อการเกิดไฟไหม้ได้เร็วกว่า ถ้าไฟไหม้จะมีควัน แบบนี้มีหลายระดับ แล้วแต่เราตั้งระดับของควันที่จะได้รับ แต่มีข้อเสียคือถ้าในห้องมีควันจากเหตุอื่น เช่น สูบบุหรี่ อุปกรณ์นี้จะให้สัญญาณทันที ดังนั้นต้องห้ามสูบบุหรี่ในห้องนี้ สัญญาณที่อุปกรณ์เหล่านี้จะเป็นแบบไหนก็แล้วแต่บริษัทผู้ผลิต ซึ่งเราเลือกใช้ได้ตามความเหมาะสม เช่น

- จะมีเสียงดังเตือนผู้ควบคุมเครื่องให้ระวัง ให้เตรียมพร้อม เช่น ในกรณีที่ตั้งระดับอุปกรณ์ที่ให้สัญญาณนี้ในระดับ "ต่ำ"
- ขณะมีเสียงเตือนอาจจะมีแสงไปทั่วบริเวณที่เกิดเหตุด้วย
- จะให้สัญญาณเสียงเตือนไปยังตำแหน่งอื่น ๆ ที่เกี่ยวข้อง เช่น ห้องยามรักษาการณ์ ห้องผู้จัดการใหญ่ เป็นต้น

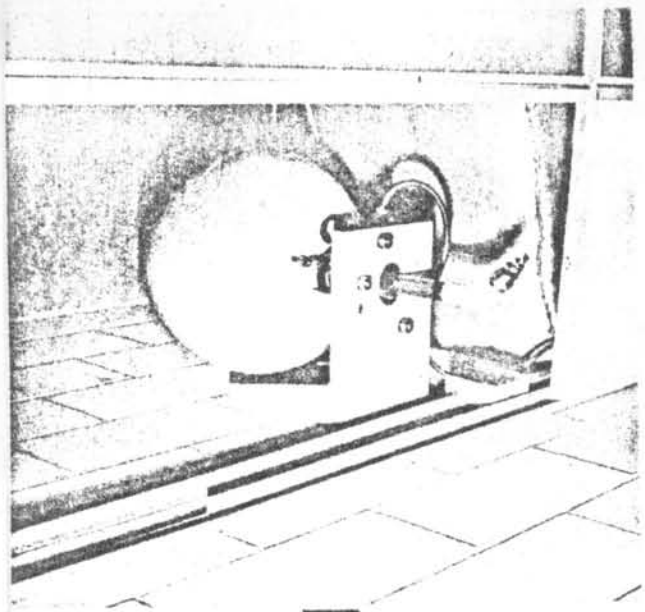
ตัวอย่างการติดตั้งอุปกรณ์เหล่านี้ ดูจากรูป 3.33 ถึงรูป 3.35

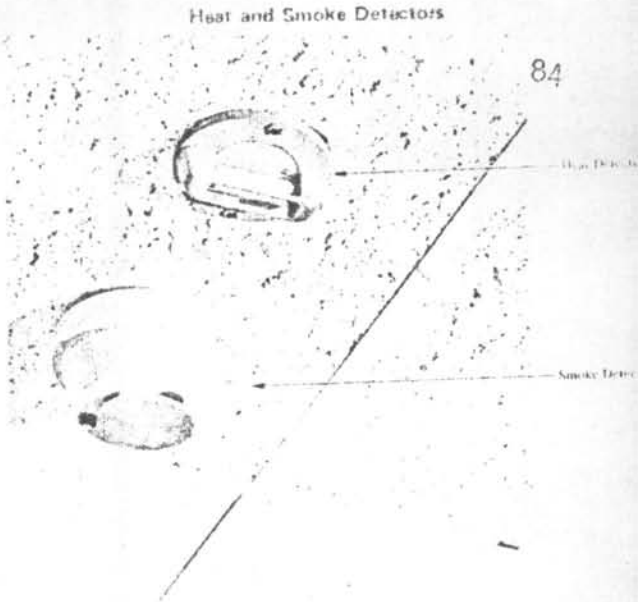


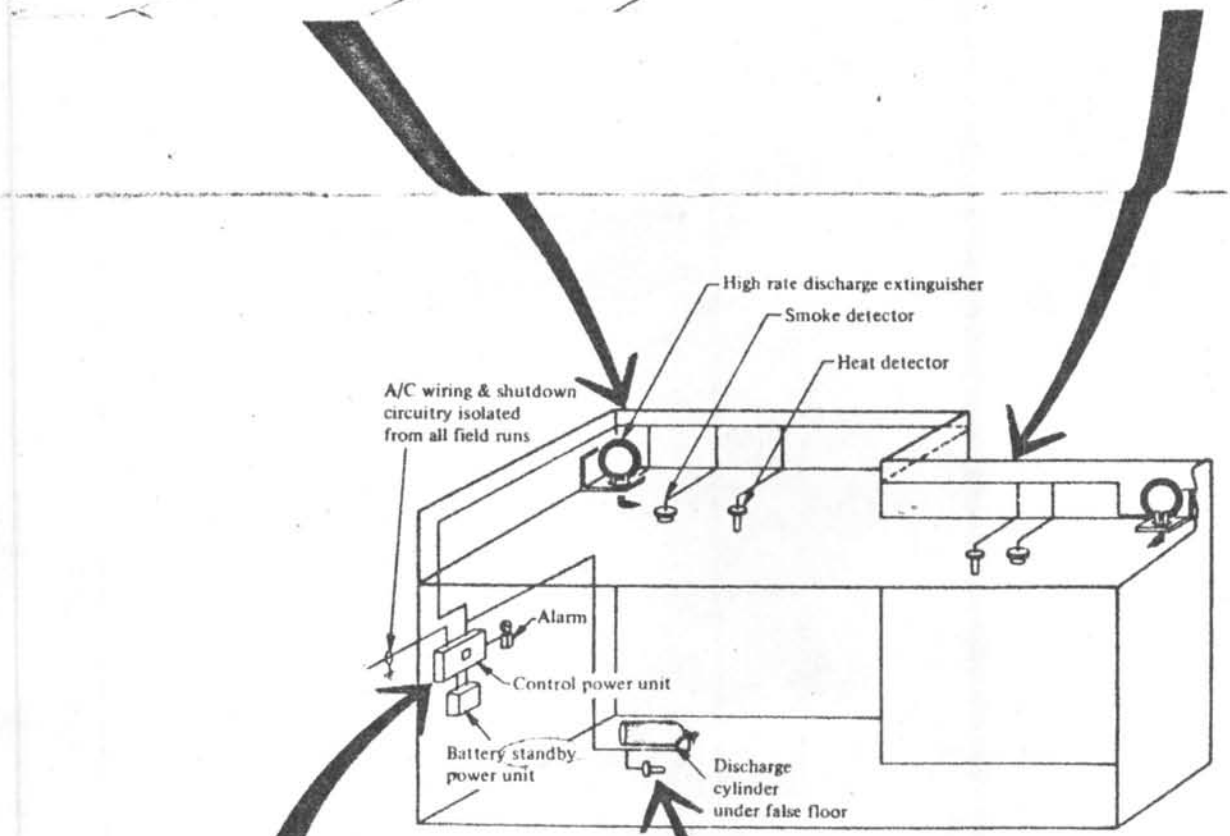
รูป 3.33 อุปกรณ์ดับเพลิงอัตโนมัติที่ใช้แก๊สฮาลอน

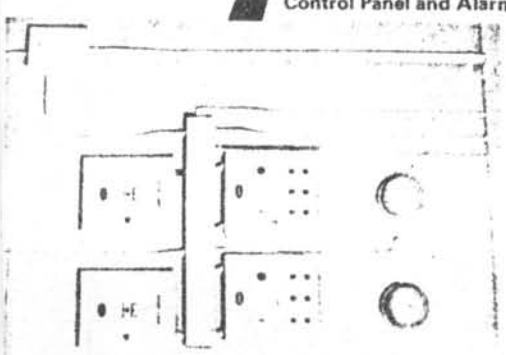


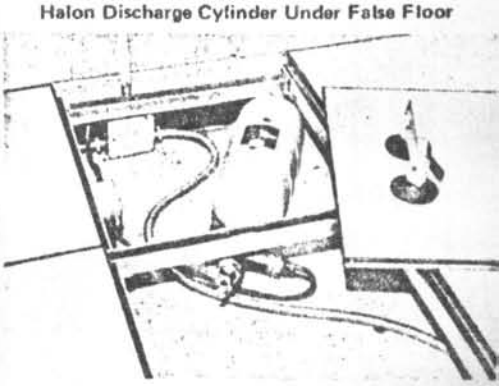
รูป 3.34 ตำแหน่งที่ติดตั้งอุปกรณ์ที่ให้สัญญาณเมื่อเกิดเพลิงไหม้











รูป 3.35 ตำแหน่งที่ติดตั้งอุปกรณ์ดับเพลิงและอุปกรณ์ที่ใช้ตรวจจับเมื่อมีไฟไหม้

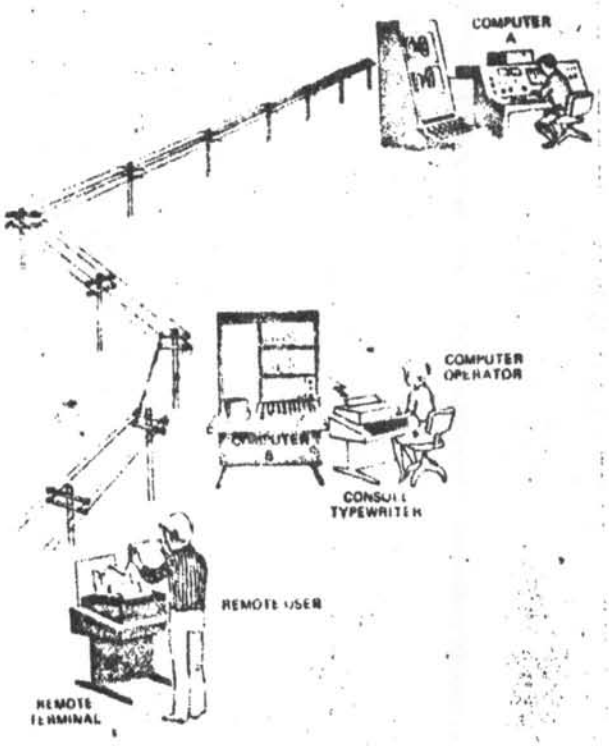
นอกจากนี้ทางศูนย์คอมพิวเตอร์อาจจะออกคำสั่งให้ทุกคนทำตาม และวิธีปฏิบัติในด้านความปลอดภัยจากไฟไหม้ ติดประกาศให้เห็นชัดเจน จัดให้มีการอบรมอธิบายให้พนักงานทุกคนในด้านความปลอดภัยโดยเฉพาะ ทางศูนย์อาจจะหาผู้เชี่ยวชาญเกี่ยวกับความปลอดภัยไว้แนะนำ ตรวจตรา ความบกพร่องของหน่วยงานในด้านการป้องกันไฟไหม้ ฯลฯ เป็นต้น

3.2.3 การป้องกันการชโมยต่อสายโทรศัพท์

ก่อนอื่นจะกล่าวถึงการรับส่งข้อมูลจากที่ห่างไกลคอมพิวเตอร์อย่างคร่าว ๆ ดูรูป 3.36

การติดต่อสื่อสารของข้อมูล การติดต่อรับส่งข้อความหรือข่าวสารในระบบโทรคมนาคม ปัจจุบันนี้อาจแบ่งได้ตามลักษณะของข่าวสาร เป็น ประเภทใหญ่ ๆ คือ ข้อความหรือข่าวสารที่เป็น Analog ซึ่งได้แก่การติดต่อพูดจนกันทางโทรศัพท์ ทางวิทยุ หรือทางโทรทัศน์ เป็นต้น ข่าวสารประเภทนี้ เป็นข่าวสารที่บุคคลผู้ติดต่อสามารถรับทราบเข้าใจโดยทันที เมื่อได้ยินหรือได้เห็นข่าวสารนั้น ๆ ข่าวสารอีกประเภทหนึ่งคือข่าวสารที่เป็น Digital ซึ่งเป็นข่าวสารที่กำหนดไว้เป็นรหัสแน่นอนอย่างใดอย่างหนึ่ง และตามปกติผู้ใช้ไม่สามารถจะทราบหรือเข้าใจความหมายในทันทีทันใดที่ได้เห็น หรือได้เห็นข่าวสารนั้น ๆ

อาจกล่าวได้อีกอย่างหนึ่งว่า การติดต่อโดยใช้สัญญาณที่เป็นอนาลอกนั้นส่วนใหญ่ก็คือการติดต่อระหว่างคนต่อคนด้วยกัน ซึ่งต้องการจะได้ยิน ได้เห็นและเข้าใจเรื่องราวต่าง ๆ โดยทันที การติดต่อสื่อสารโดยใช้สัญญาณที่ข้อมูลหรือดิจิทอลนั้นส่วนใหญ่ก็เป็นการติดต่ออุปกรณ์เครื่องบางชนิด เพื่อถ่ายทอดข้อมูลบางอย่างระหว่างกัน การติดต่อสื่อสารของข้อมูลนี้ นับวันแต่จะมีความสำคัญและแพร่หลายมากขึ้น อันเนื่องมาจากการหาวิธีการใช้ประโยชน์จากคอมพิวเตอร์ต่าง ๆ ได้กว้างขวางยิ่งขึ้น ประกอบกับการขยายตัวและความก้าวหน้าในกิจการโทรคมนาคม ซึ่งทั้งสองประเภทนี้มีส่วนช่วยเสริมซึ่งกันและกัน ในการดำเนินการธุรกิจและกิจการอื่น ๆ แทบทุกประการให้เจริญ



รูป 3.36 การประมวลผลของข้อมูลโดยที่อุปกรณ์ข้อมูลเข้า/ข้อมูลออก อยู่ในที่ตั้งห่างไกลจากเครื่องคอมพิวเตอร์

ก้าวหน้า ทั้งนี้ เป็นไปโดยสะดวกรวดเร็วและประหยัดยิ่งขึ้นด้วย

ในงานด้านโทรคมนาคมของทุก ๆ ประเทศ เนื่องจากข่ายโทรศัพท์ของประเทศนั้น ๆ เกิดขึ้นมาก่อนความต้องการในการรับส่งสัญญาณข้อมูล ดังนั้น ก็ย่อมเป็นของแน่นอนว่า การริเริ่มและพัฒนากิจการรับ – ส่งข้อมูลนี้ ก็ควรอาศัยระบบและข่ายโทรศัพท์ที่มีอยู่แล้วเป็นหลัก ผู้เช่าโทรศัพท์ที่กระจัดกระจายกันอยู่ตามที่ต่าง ๆ นั้น ก็ย่อมต้องมีคู่สายของตนเองต่อไปยังชุมสายโทรศัพท์ และต่อเชื่อมโยงกับผู้อื่นได้ ข่ายโทรศัพท์ดังกล่าวเป็นระบบที่สร้างไว้แล้ว และลงทุนไปแล้วเป็นจำนวนเงินไม่น้อย ก็ย่อมสมควรที่จะนำมาใช้สำหรับการสื่อสารของข้อมูลด้วย ในทำนองเดียวกันข่ายโทรศัพท์ทางไกล หรือข่าวโทรคมนาคมทั้งภายในประเทศและระหว่างประเทศที่สร้างขึ้นมาแล้วนั้น ก็ย่อมสมควรจะนำมาใช้เพื่อการติดต่อสื่อสารสำหรับข้อมูลด้วยเช่นกัน ทั้งนี้ เพื่อความประหยัดและความสะดวกหลายประการที่จะได้รับ

ในระยะแรกที่มีการใช้คอมพิวเตอร์ในวงการธุรกิจ แทบจะกล่าวได้ว่าไม่มีระบบการรับส่งข้อมูลเลย จะมีบ้างก็เพียงเป็นการทดลองเท่านั้น ต่อมาความต้องการใช้ระบบรับส่งข้อมูลเพิ่มขึ้นอย่างมาก แต่ก็ยังมีปัญหาบางประการ เนื่องจากอุปกรณ์ต่าง ๆ ที่ใช้ในงานโทรคมนาคมนั้นได้ออกแบบขึ้นสำหรับการรับส่งสัญญาณเสียงพูด และโทรทัศน์ มิได้ออกแบบมาสำหรับการรับส่งข้อมูลของคอมพิวเตอร์ จึงจำเป็นต้องมีการปรับปรุง ดัดแปลง อุปกรณ์บางอย่าง ซึ่งทำให้ระบบโทรคมนาคมที่มีอยู่นั้น สามารถใช้ในงานรับส่งข้อมูลได้ ต่อไปในอนาคตจะมีการพัฒนาระบบการรับส่งข้อมูลเพิ่มขึ้นอย่างมาก ซึ่งในด้านการขยายตัวของระบบหรืออุปกรณ์ในงานโทรคมนาคมเองมีส่วนช่วยมาก ดังนั้น ระบบความปลอดภัยในด้านการสื่อสารข้อมูลนี้จึงเป็นสิ่งสำคัญ ที่ผู้บริหารควรจะนึกถึงเป็นอันดับแรก

วิธีการเกิดการขโมยต่อสายโทรศัพท์ การรับส่งข้อมูล (Data transmission) จากที่ห่างไกล ซึ่งอาศัยสายนี้จะต้องมีการป้องกันการขโมยต่อสายโทรศัพท์ ซึ่งอาจจะเกิดขึ้นได้ 2 กรณี

1. Active wiretapping

2. Passive wiretapping

1. Active wiretapping หมายถึงการที่ผู้บุกรุกขโมยฟังสัญญาณ และในขณะเดียวกันก็เปลี่ยนแปลงข้อมูลเดิมและส่งสัญญาของเขาไปตามสายโทรศัพท์นั้นแทน กรณีนี้ผู้บุกรุกจะต้องมีอุปกรณ์ปลายทางและโมเด็มที่เหมาะสมกับชนิดของการรับส่งข้อมูลผ่านสายโทรศัพท์นั้น แต่ผู้บุกรุกก็ไม่สามารถขโมยข้อมูลจากฐานข้อมูลนั้น เพราะถูกควบคุมโดยวิธีการ การให้สิทธิการใช้ และการล็อคแฟ้มข้อมูล นอกจากข้อมูลที่ผ่านมาทางสายโทรศัพท์แล้ว Active wiretapping นี้ส่วนมากจะเกิดขึ้นได้ในกรณีของ Man-machine conversation เท่านั้น โดยผู้บุกรุกจะส่งสัญญาณของตนเองไปแทนในช่องที่ไม่มีการโต้ตอบระหว่างคนและเครื่อง คือช่วงหมดประโยคหนึ่ง จะหยุดสักครู่หนึ่งเพื่อรอสัญญาณ เวลานี้ผู้บุกรุกจะรับส่งสัญญาณของเขาไปยังคอมพิวเตอร์ และคอมพิวเตอร์จะรับได้ทันทีและเขาสามารถจะตัดสัญญาณของผู้ใช้ที่ใช้อยู่ก่อนแล้วทันที และต่อไปผู้บุกรุกจะส่งข้อความให้คอมพิวเตอร์ โดยใช้ชื่อของผู้ใช้คนเดิมนั้น คอมพิวเตอร์ก็จะรับได้ อย่างไรก็ดีวิธีการ Active wiretapping นี้ ผู้บุกรุกจะต้องมีความรู้ทางเทคนิคหลาย ๆ อย่างเป็นอย่างดี และต้องมีความรู้อย่างกว้างขวาง และเฉลียวฉลาดมากด้วย โดยทั่วไปแล้ว Aotive wiretapping ผู้บุกรุกทำได้ยากมาก ในทางปฏิบัติจะไม่มีโอกาสเกิดขึ้นเลย ดังนั้นในที่นี้จะไม่กล่าวถึง

2. Passive wiretapping หมายถึงการที่ผู้บุกรุกขโมยฟังสัญญาณที่ส่งมาตามสายโทรศัพท์เท่านั้น ไม่เปลี่ยนแปลงข้อมูลหรือส่งสัญญาณของตนเองไป ผู้บุกรุกหรือผู้ลอบฟังอาจใช้เทปบันทึก โดยบันทึกสัญญาณที่ผ่าน Communication line และนำข้อมูลนั้นมาสร้างใหม่ (Reconstruct) โดยต่อเข้ากับอุปกรณ์ปลายทางและโมเด็มที่เหมาะสมเพื่อแปลงสัญญาณรายังอุปกรณ์ปลายทาง อุปกรณ์ปลายทางจะพิมพ์ข้อความนั้นออกมา

ผู้ที่ลอบต่อสายโทรศัพท์เพื่อฟังข่าวสาร จะฟังได้นานจนกว่าเขาจะได้รู้ข้อมูลที่เขาต้องการ การขโมยต่อสายโทรศัพท์จะต้องใช้เทคนิคมากมายหลายอย่างช่วย

กรณีที่ทราบรหัสลับเฉพาะเพื่อที่จะเรียกข้อมูล ผู้ลอบฟังจะสามารถเปลี่ยนรหัสการให้สิทธิการใช้ในระบบได้ และยังสามารถเรียกใช้ข้อมูลจากฐานข้อมูลได้ แต่ข้อสำคัญผู้ลอบฟังจะต้องใช้ความรู้ความสามารถทางเทคนิคอย่างมาก

วิธีการป้องกันการขโมยข่าวสารทางโทรศัพท์ทำได้ 2 แบบ คือ

1. ใช้เทคนิคช่วย เช่น

ก. ใช้วิธีการเข้ารหัสลับเฉพาะ

ข. ใช้ระเบียบวิธีปฏิบัติในด้านการควบคุม Teleprocessing ซึ่งวิธีนี้จะใช้ในกรณี Active wiretapping. ซึ่งค่อนข้างจะทำได้ยากคือจะใช้วิธีตรวจหาอุปกรณ์ปลายทาง

2. ไม่ใช้เทคนิคช่วย เป็นวิธีป้องกันลักษณะต่าง ๆ ภายนอก ซึ่งจะได้กล่าวต่อไป

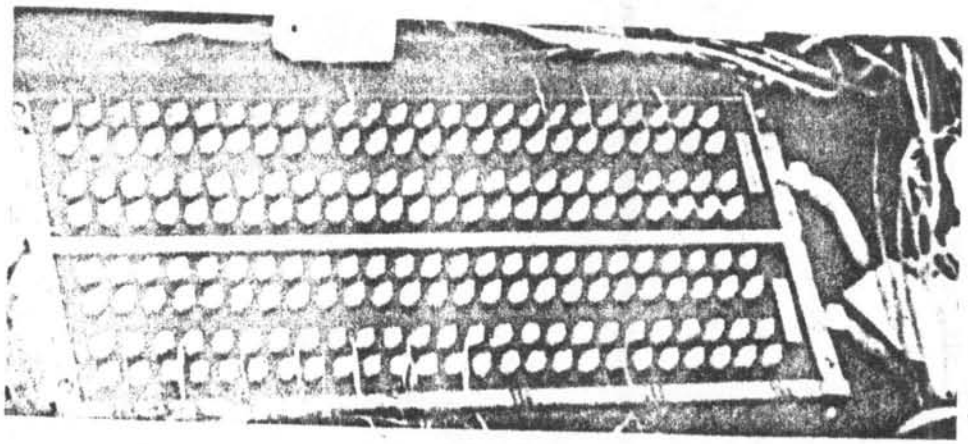
การลอบต่อสายโทรศัพท์นี้อาจทำได้ทั้ง : -

1. การลอบต่อสายโทรศัพท์สาธารณะ (Tapping public lines)

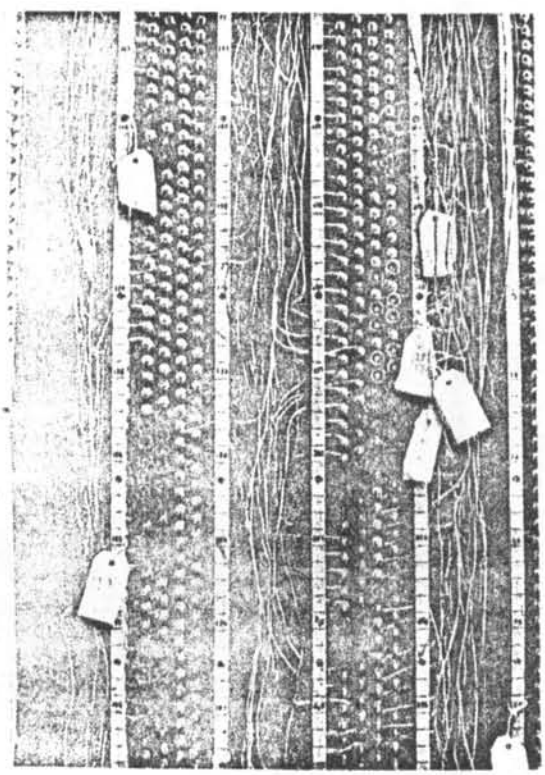
2. การลอบต่อสายโทรศัพท์ ณ ตำแหน่งผู้ใช้ (Tapping on the user's premises) ดูจากรูป 3.37

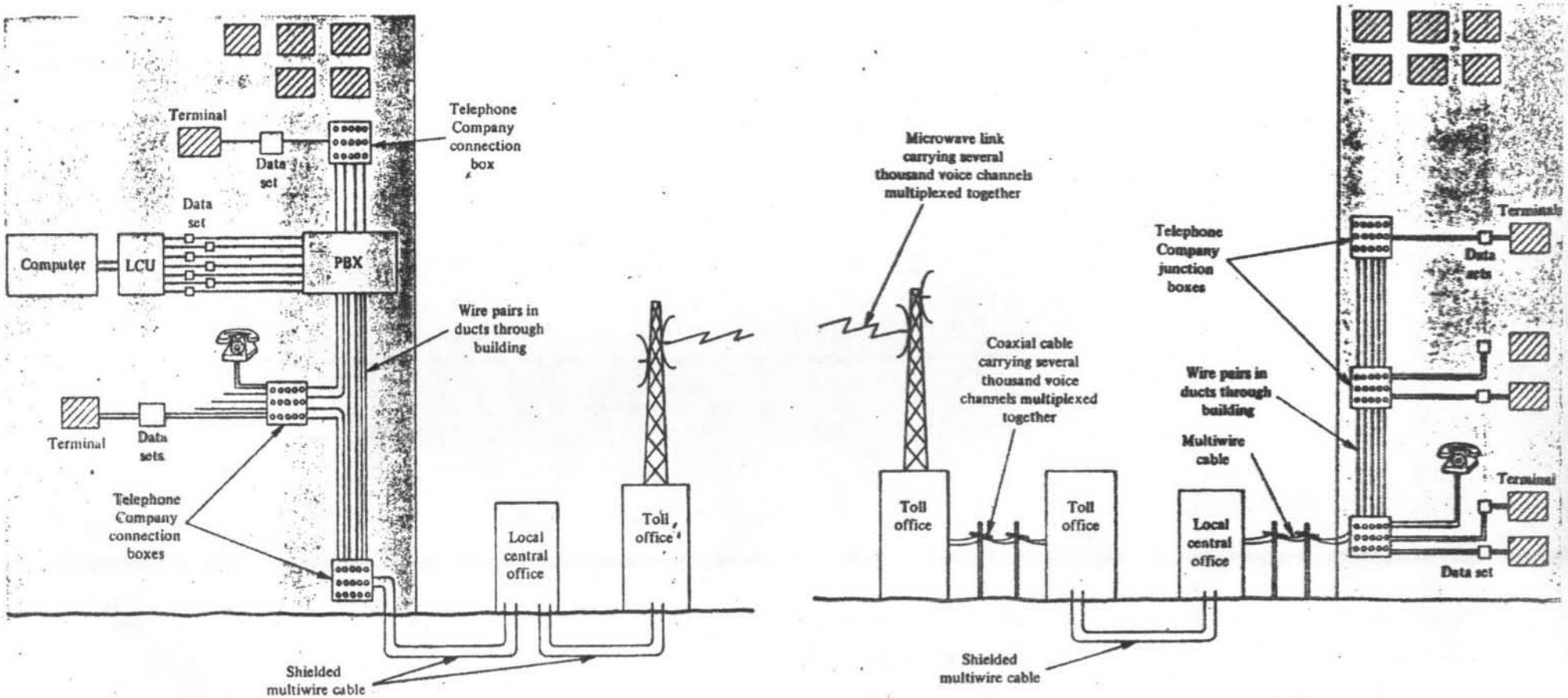
ช่ายสายการสื่อสารโทรคมนาคมที่ต่อระหว่างคอมพิวเตอร์ในตึกหนึ่งไปยังอุปกรณ์ปลายทางที่อยู่อีกตึก แสดงได้ดังรูป 3.38

1. <u>การลอบต่อสายโทรศัพท์สาธารณะ</u> การลอบต่อสายโทรศัพท์แบบนี้ทำได้สำเร็จยากมาก เนื่องจากแต่ละตึกก็อาจมีสายโทรศัพท์ต่อออกไปข้างนอกตึกออกไปยังถนน ซึ่งก็จะมีมากมายหลายสาย ผู้บุกรุกไม่สามารถจะทราบได้เลยว่าคู่สายอันไหนของใคร เขาจะรู้ได้ต่อเมื่อเขาได้รับคู่มือ (Cable book) ที่จะบอกรายละเอียดทางด้าน Telephone company engineer พร้อมทั้งคู่สายโทรศัพท์ (Pair of wires) ที่แต่ละแห่งใช้ กรณีนี้ถ้าผู้บุกรุกไม่สมรู้ร่วมคิดกับคนทำงานในบริษัทนี้ก็จะไม่ทราบได้ และเขายังจะต้องมีความรู้ทางด้านเทคนิคอย่างดีด้วย



รูป 3.37 สายโทรศัพท์ที่อาจถูกลักลอบต่อเพื่อลอบฟังการสนทนา ซึ่งเฉิดขึ้นได้ง่าย ณ ตำแหน่งผู้ใช้





รูป 3.38 ข่ายสายการสื่อสารโทรคมนาคมที่ต่อระหว่างคอมพิวเตอร์ในตึกหนึ่งไปยังอุปกรณ์ปลายทางที่อยู่อีกตึก

ปกติแล้วสายเคเบิลจากที่ห่างไกลจะต้องผ่าน Telephone company local central office ณ ตำแหน่งนี้ เส้นลวด (wire) จะถูกต่อกับสายคู่เช่า (Leased line) ซึ่งเป็นการยากมากที่จะเกิดการลักลอบต่อสายโทรศัพท์ ณ ตำแหน่งนี้ ถ้าไม่เกิดการสมรู้ร่วมคิดกับคนทำงานใน Telephone company จะไม่มีทางทำได้เลย ดังนั้นจึงมีความปลอดภัย ณ ตำแหน่งนี้

2. <u>การลอบต่อสายโทรศัพท์ ณ ตำแหน่งผู้ใช้</u> เนื่องจากเคเบิลที่ต่อมาจาก Local central office แล้วต่อมายัง Telephone company connection box ซึ่งอยู่ภายในตึกคู่สายมากมายจะถูกแยกและเชื่อมกับ Terminal screw ซึ่งเห็นได้ชัดเจนจากกล่อง (Box) อันนี้ เพียงคู่สายโทรศัพท์คู่เดียวจะผ่านเข้าไปยังห้องที่มีอุปกรณ์ปลายทาง ถ้าในตึกนั้น ๆมีอุปกรณ์ปลายทางหลายอัน ก็จะใช้กล่องนี้หลายอันกล่องที่ต่อไปยังอุปกรณ์ปลายทางโดยตรง ผู้บุกรุกจะทราบได้ทันทีว่าเป็นของใคร ก็สามารถจะลอบต่อได้อย่างง่ายดาย สำหรับ PBX (Private branch exchange) ที่ต่อมาจากคอมพิวเตอร์โดยตรง ก็จะมีเส้นลวดเห็นได้ชัดเจน ผู้บุกรุกก็สามารถลอบต่อได้โดยใช้เทคนิคบางอย่างช่วย จากนั้นเขาก็สามารถลอบฟังข่าวสารจากที่ห่างไกลได้อย่างสะดวกและปลอดภัย ภายในสำนักงานหลายแห่งที่ PBX ไม่ล็อค สำหรับ Telephone company connection box การลอบต่อก็ทำได้สะดวก ทั้ง ๆ ที่ภายในตึกอาจมีหลายหน่วยงานที่ใช้ Terminal box รวมที่ต่อมาจาก Local central office จะมีมากมายก็ตาม ผู้ลอบต่อสามารถจะรู้ได้ทันทีว่า เส้นลวดในกล่องนั้นเป็นของหน่วยงานไหน เพราะตามปกติจะทำสัญญาณ เช่น สีต่าง ๆ ให้เห็นชัดเจน

วิธีการป้องกันการลอบต่อสายโทรศัพท์โดยไม่ใช้เทคนิคอะไรเพียงแต่ให้ Telephone company connection boxes และPBX ทุก ๆ อันนั้นล็อคเสียโดยอาจเก็บไว้ในห้องหรือตู้เล็ก ๆ ก็ได้ และล็อคห้องหรือตู้เล็ก ๆ นั้น หรือถ้าจะให้ดีอาจติดสัญญาณกันขโมย เมื่อตู้ถูกเปิดออกและสัญญาณถูกส่งผ่านสายโทรศัพท์ สัญญาณจะดัง โดยทั่วไปถ้าผู้ใช้สามารถทำระบบการป้องกันความปลอดภัยในด้านนี้ภายในตึกของเขาแล้ว การลอบต่อสายโทรศัพท์ทำได้ยากมาก

นอกจากที่กล่าวมาแล้ว ก็มีวิธีการอีกหลายแบบที่ทำให้ผู้บุกรุกสามารถรู้รายละเอียดบางอย่างที่เขาต้องการได้ เช่น

– เศษกระดาษ ถังสำหรับทิ้งเศษกระดาษในห้องคอมพิวเตอร์นั้น มีรายละเอียดหลายอย่างที่น่าสนใจมาก ซึ่งจะมีทั้งกระดาษคาร์บอนของรายการที่พิมพ์ รวมทั้งข้อมูลที่สำคัญ ข้อมูลที่คัดลงมาจากแฟ้มข้อมูล รายละเอียดที่พิมพ์มาจากกระดาษพิมพ์ต่อเนื่อง ถังเหล่านั้นปกติแล้ว เจ้าหน้าที่เขียนโปรแกรมจะต้องมีเพื่อทิ้งเศษกระดาษ ปกติเขาจะเขียนรายละเอียดไว้มาก พร้อมทั้งวิธีปฏิบัติ นอกจากนี้ก็มีวิธีการจัดแฟ้มข้อมูล โปรแกรมที่เขียนสำหรับใช้งานเหล่านั้นบางครั้งเขาอาจจะเขียนคำผ่านหรือรหัสที่ให้สิทธิการใช้ข้อมูลลงไป ผู้สนใจอาจเก็บรายละเอียดเหล่านี้ที่เขาเอามาทิ้งทุก ๆ วัน หรืออาจจะขอซื้อขยะจากผู้ที่เก็บขยะก็ได้ ผู้ที่สนใจก็จะสามารถรวบรวมศึกษารายละเอียดเหล่านี้ได้ วิธีป้องกันอย่างง่าย ๆ ก็คือใช้ถังขยะที่มีฝาปิด และ Lock ไว้ด้วย และมีช่องหย่อนกระดาษลงไปทุก ๆ วัน ขยะที่จะเอามาทิ้งต้องทำลายก่อน

– Visual Eavesdropping รหัสลับจะเรียนรู้ได้โดยการเฝ้าดูจากจอภาพ หรือกระดาษพิมพ์ต่อเนื่อง ผู้ที่ออกแบบระบบในด้านนี้ควรจะไม่ให้มีการพิมพ์รหัสบนกระดาษพิมพ์ หรือออกทางจอทีวี โดยปกติรหัสเหล่านี้จะออกมาทางอุปกรณ์ปลายทาง กรณีนี้ผู้บุกรุกอาจสังเกตการทำงานของผู้ควบคุมเครื่องขณะกดปุ่ม เพื่อให้รหัสซึ่งเรื่องนี้ผู้ควบคุมเครื่อง ณ อุปกรณ์ปลายทางควรจะระมัดระวังและมีความรอบคอบมาก ๆ ในด้านรหัสลับแก่ผู้ที่เฝ้าดู โดยเฉพาะผู้ที่มาเยี่ยมเยือนเป็นบางครั้ง นอกจากนี้ในปัจจุบันกล้อง Telescope มีประสิทธิภาพดีมาก ดังนั้นอุปกรณ์ปลายทางไม่ต้องวางไว้ใกล้หน้าต่าง เพราะอาจส่องดูได้

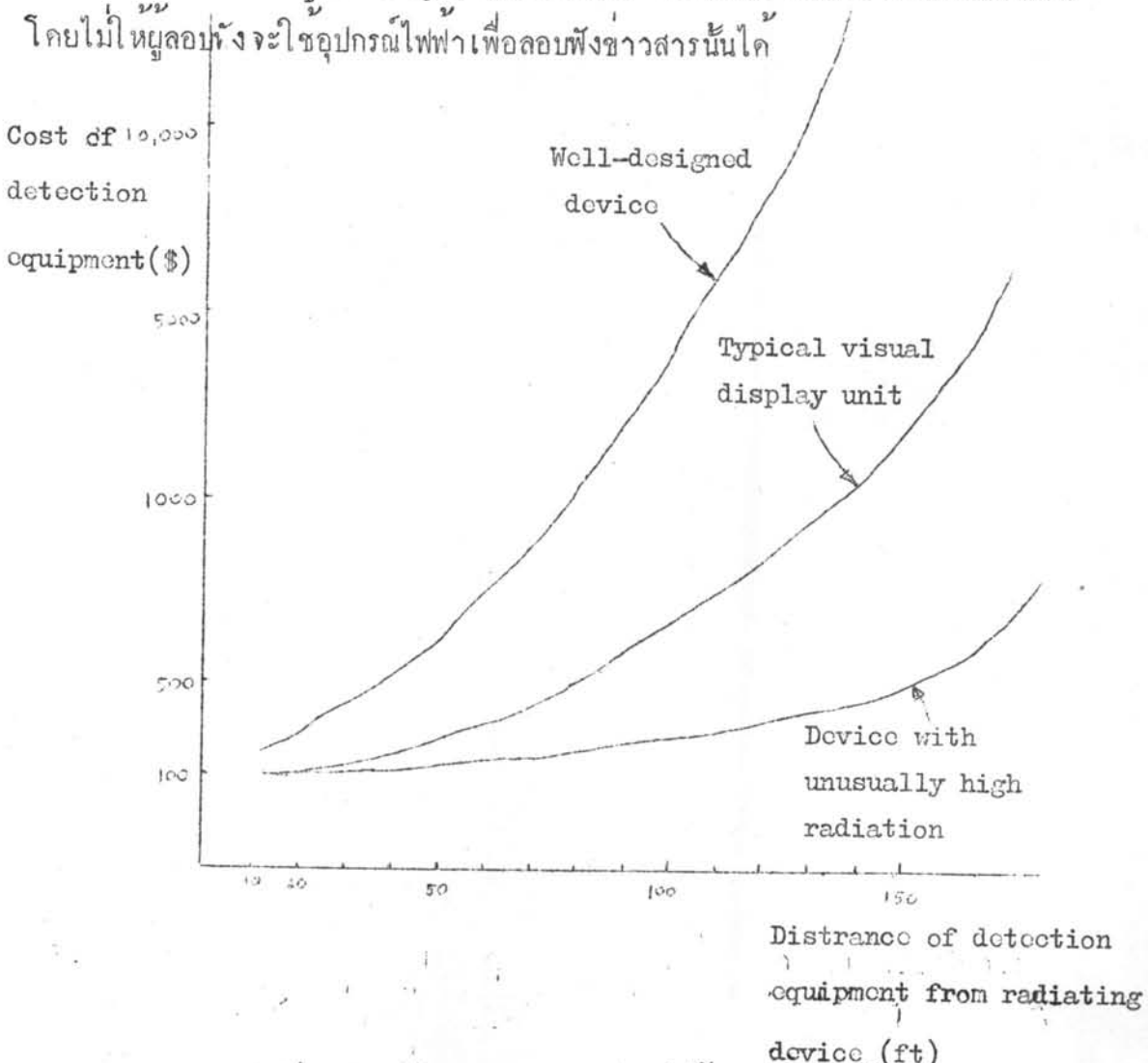
– Cameras กล้องถ่ายรูปอาจจะถูกซ่อนไว้ในบริเวณใดบริเวณหนึ่งก็ได้ หรืออาจนำกล้องถ่ายรูปติดตัวเข้าไป ผู้ที่รับผิดชอบด้านระบบความปลอดภัยจะต้องนึกถึงเรื่องนี้ด้วย และต้องรู้ว่าปัจจุบันกล้องถ่ายรูปมีขนาดเล็กมาก ซึ่งมีประสิทธิภาพสูง สามารถถ่ายภาพได้ในระยะไกล ๆ

– Bugging devices เป็นเครื่องมือที่เล็กมาก โดยอาจซ่อนไว้ตามใต้โต๊ะ หลังรูปภาพ ฯลฯ เครื่องมือนี้สามารถจะบันทึกข้อความที่ได้ยิน เครื่องนี้ประกอบด้วยไมโครโฟนที่เล็กมาก, Recorder ซึ่งล็อคไว้ด้วย ผู้ใช้จะใช้เครื่องนี้ก็ตั้งเครื่องไว้ เครื่องนี้สามารถบอกเสียงที่ได้ยินด้วยว่าเป็นเสียงอะไร เช่น คำสั่งพิมพ์กระดาษพิมพ์หรือเสียงเจาะบัตร ซึ่งวิธีนี้อาจจะขโมยข้อมูลได้ง่ายมาก ดังนั้น เพื่อความปลอดภัยควรจะมีเครื่องมือที่ช่วยในการค้นหา Bugging device นี้อีกที

– อุปกรณ์ทางไฟฟ้าที่ใช้ในการลอบฟัง (Electronic eavesdropping) รูปแบบอย่างหนึ่งของการลอบฟังข่าวสาร ก็คือการบันทึกการกระจายอำนาจแม่เหล็กไฟฟ้าของเสียง (Electro. agnetic radiation) จากอุปกรณ์ทางไฟฟ้า (Electronic devices) เครื่องจักรส่วนมาก เช่น คอมพิวเตอร์ อุปกรณ์ปลายทาง และโมเด็ม จะเกิดมีการกระจายของเสียงซึ่งสามารถรับได้ในระยะหนึ่ง ผู้ลอบฟังที่มีอุปกรณ์ทางไฟฟ้าที่ใช้ในการลอบฟังก็จะลอบฟังข่าวสารต่าง ๆ ได้

ความจริงการลอบฟังสัญญาณแม่เหล็กไฟฟ้าของเสียงนี้ยุ่งยากมาก เนื่องจากสัญญาณจะปนกันยุ่ง ไม่สมบูรณ์ ไม่ชัดเจน เทคนิคต่าง ๆ ก็ต้องใช้มากขึ้นเพื่อใช้ในการลอบฟังสัญญาณเหล่านี้ ปกติผู้ออกแบบอุปกรณ์ปลายทางจะไม่คิดถึงการกระจายของเสียงเลย อุปกรณ์บางชนิดที่ผลิตขึ้นมาจึงมีการกระจายของเสียงในอัตราที่สูงมาก ผู้ผลิตบางรายก็ทราบถึงปัญหาในด้านนี้ดี แต่ถ้าอุปกรณ์ทั้งหลายถูกสร้างขึ้นมาในระบบที่การกระจายของเสียงถูกกำจัดหมดแล้ว อุปกรณ์เหล่านี้จะมีราคาแพงเกินไป ผู้ใช้จะมีวิธี ป้องกันปัญหานี้ได้โดยเขาควรจะหลีกเลี่ยงการใช้อุปกรณ์ปลายทางที่มีอัตราการกระจายของเสียงต่ำ ตำแหน่งที่จะเอาอุปกรณ์ปลายทางไว้ภายในตึกก็ควรเลือกตรงใจกลางของตึกมากกว่าที่จะเอาไว้ข้างนอก โดยเฉพาะอุปกรณ์ปลายทางที่ใช้กับงานที่สำคัญจะต้องระมัดระวังตำแหน่งที่จะเอาอุปกรณ์ปลายทางนี้ไว้เป็นพิเศษ ซึ่งก็แล้วแต่หน่วยงานอีก

นอกจากนี้การกระจายอำนาจแม่เหล็กไฟฟ้า ยังสามารถกระจายผ่าน Conductor เช่น Water pipe, Power line และโลหะที่มีอยู่ในตึกการป้องกันการลอบฟังการกระจายอำนาจแม่เหล็กไฟฟ้าของเสียง อาจทำได้โดยการเคลื่อนย้ายอุปกรณ์ปลายทางไปยังด้านอื่น ๆ ที่เหมาะสมของห้อง หรือสร้างที่กำบังไฟฟ้า หรือใช้เทคนิคอื่น ๆ ที่เกี่ยวข้อง เป็นต้น ในอนาคตในด้านการติดตั้งเครื่องคอมพิวเตอร์ไว้ ณ ตำแหน่งใด จะต้องให้ผู้เชี่ยวชาญทางด้านนี้เพื่อกำจัดการกระจายอำนาจแม่เหล็กไฟฟ้าโดยไม่ให้ผู้ลอบฟังจะใช้อุปกรณ์ไฟฟ้าเพื่อลอบฟังข่าวสารนั้นได้



รูป 3.39 อุปกรณ์ต่าง ๆ เช่น อุปกรณ์ปลายทางที่ได้ออกแบบเพื่อป้องกันการแผ่รังสี ค่าใช้จ่ายที่ป้องกันการแผ่รังสีของคลื่นแม่เหล็กไฟฟ้าจะสูงขึ้นตามระยะทางที่เกิดการลักลอบฟังนั้น (upper curve)

3.3 ระบบการควบคุมงานในด้านบริหาร รวมทั้งเจ้าหน้าที่ปฏิบัติงาน

เป็นชั้นถัดออกมาข้างนอกหลังจากได้วางระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะในตัวคอมพิวเตอร์ และการวางระบบความปลอดภัยในด้านสถานที่ทำการ ตลอดจนสักษณะต่าง ๆ ภายนอกที่เกี่ยวข้อง ทั้ง 3 ด้านจะต้องทำไปพร้อม ๆ กัน จะขาดด้านใดด้านหนึ่งไม่ได้ เพราะแต่ละด้านจะช่วยเสริมกันและกัน จะพิจารณาได้ดังนี้

3.3.1 ด้านทั่วไป

ก. บุคคลที่เกี่ยวข้องกับระบบและวิธีการควบคุม หน่วยงานใด ๆ ที่นำเอาคอมพิวเตอร์มาช่วยในการทำงานตั้งแต่เริ่มตั้งเครื่อง ทดสอบเครื่อง จนเครื่องใช้ทำงานได้ และในขณะเดียวกันก็จะวางระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะไปพร้อม ๆ กัน เทคนิค แนวทางและวิธีการต่าง ๆ ที่ใช้ในการนี้ตั้งแต่เริ่มต้นจนสามารถผ่านการประมวลผลข้อมูล และนำข้อมูลนั้นไปใช้งานทั้งทางตรงและทางอ้อม "คน" เท่านั้นที่ทราบรายละเอียดทุกอย่างทั้งข้อผิดพลาด ข้อปรับปรุง และจุดอ่อนของงานเป็นต้น บุคคลเหล่านี้จะมีหลายฝ่ายทั้งผู้ที่เกี่ยวข้องโดยตรง และบุคคลภายนอกที่ต้องการเข้ามาบุกรุก ฯลฯ ซึ่ง "คน" เหล่านี้จะเป็นผู้ที่รักษาระบบให้ทำงานได้ต่อไปอย่างดี หรือทำลายระบบเพื่อจุดประสงค์อย่างใดอย่างหนึ่งได้ ควรจะได้พิจารณาดังนี้

บุคคลที่มีผลต่อระบบความปลอดภัยโดยตรง ระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะที่ได้วางไว้ทั้งในด้านตัวระบบคอมพิวเตอร์เอง หรือด้านลักษณะต่าง ๆ ภายนอกเครื่อง รวมทั้งสถานที่ปฏิบัติงาน ปัญหาต่าง ๆ ทั้งด้านเหตุร้ายที่เกิดขึ้นโดยอุบัติเหตุ หรือเกิดขึ้นโดยการจงใจให้เกิด บุคคลที่เกี่ยวข้องโดยตรงนี้มีความสำคัญมาก เพราะเป็นผู้เกี่ยวข้องทั้งในด้านการวางระบบและใช้เครื่องคอมพิวเตอร์โดยตรง ย่อมจะรู้วิธีการทั้งหลายเป็นอย่างดี บุคคลเหล่านี้ได้แก่

1. บุคคลภายนอกศูนย์คอมพิวเตอร์ที่บังเอิญได้รู้รายละเอียดต่าง ๆ ในศูนย์คอมพิวเตอร์ เช่น ผู้บุกรุกที่ต้องการจะมาทำลาย

2. วิศวกร รวมทั้งวิศวกรที่ทำงานเกี่ยวกับตัวเครื่องคอมพิวเตอร์ และวิศวกรที่ทำงานในด้านอุปกรณ์ เครื่องมือเครื่องใช้ประกอบอื่น ๆ

3. เจ้าหน้าที่เขียนโปรแกรม รวมทั้งเจ้าหน้าที่เขียนโปรแกรมเฉพาะงานใดงานหนึ่ง และเจ้าหน้าที่เขียนโปรแกรมในด้านระบบเครื่อง

4. เจ้าหน้าที่ที่ปฏิบัติงานในห้องเครื่องคอมพิวเตอร์

5. เจ้าหน้าที่ที่ดูแลรักษาข้อมูลทุกอย่าง

6. เจ้าหน้าที่ออกแบบลักษณะข้อมูลที่ใช้

7. เจ้าหน้าที่ที่ทำงานเกี่ยวกับด้านความปลอดภัยโดยตรง

8. ผู้ออกแบบระบบงาน

9. ผู้บริหารในหน่วยงานประมวลผลข้อมูล

<u>บุคคลที่จะช่วยป้องกันและรับผิดชอบในการปฏิบัติงานเพื่อให้เกิดความปลอดภัย</u> จะต้องระมัดระวังความปลอดภัยในส่วนที่เกี่ยวข้องอยู่ตลอดเวลาโดยเริ่มตั้งแต่การปฏิบัติงานแต่ละอย่างในแต่ละวัน เพราะความเสียหายทั้งหลายจะเกิดเมื่อไรก็ได้ ผู้ที่เกี่ยวข้องทุกคนจะต้องรับผิดชอบร่วมกัน ซึ่งได้แก่

1. ผู้บริหารงานในหน่วยงานประมวลผลข้อมูล จะต้องดูแลเอาใจใส่การทำงานของทุกคนอย่างเข้มงวด เนื่องจากทุกคนที่ทำงานในศูนย์ประมวลผลต่างก็มีหน้าที่ประจำของตนเองว่าทำอะไร เมื่อทุกคนทำงานในหน้าที่อย่างถูกต้อง ทำตามวิธีการทุกอย่างก็จะทำให้เกิดระบบความปลอดภัยทั้งศูนย์ได้เป็นอย่างดี

2. ผู้บริหารในด้านระบบความปลอดภัยโดยเฉพาะ ตำแหน่งนี้ถ้าเป็นหน่วยงานเล็ก ๆ อาจจะเป็นคนเดียวกับผู้บริหารศูนย์คอมพิวเตอร์ก็ได้ แต่ในศูนย์คอมพิวเตอร์ใหญ่ ๆ และงานที่ทำมีความสำคัญมากตำแหน่งนี้ควรจะมี ซึ่งโดยหน้าที่จะมีหน้าที่ดังนี้

–ตรวจงานที่ทำไปของแต่ละวันในด้านที่เกี่ยวข้องกับระบบความปลอดภัยของเจ้าหน้าที่ที่ทำงานด้านความปลอดภัยโดยเปรียบเทียบกับมาตรฐานที่วางไว้ว่าแตกต่างไปมากน้อยเพียงไร จะต้องแก้ไขหรือไม่

–งานที่เกี่ยวกับระบบ On – line เขาจะรับผิดชอบในรายละเอียดคำผ่าน (Passwords or Security code) ที่ใช้ในการเรียกโปรแกรม ข้อมูล พร้อมรายละเอียดอื่น ๆ ที่เกี่ยวข้อง

–จะตรวจรายละเอียดของการปฏิบัติงานของเจ้าหน้าที่เครื่อง (Console operator's log) ข้อมูลทุกอย่างเกี่ยวกับระบบ รายงานบันทึกของยามรักษาการณ์ รายละเอียดของงานล่วงเวลาที่ทำ และรายละเอียดอื่น ๆ ที่เกี่ยวข้องกับระบบความปลอดภัย

–จะกำหนดรายละเอียดของระบบความปลอดภัยที่จะต้องใช้ภายในศูนย์คอมพิวเตอร์ทุกอย่าง พร้อมทั้งหาเทคนิคใหม่ ๆ มาใช้เพื่อให้งานด้านระบบความปลอดภัยมีประสิทธิภาพยิ่งขึ้น

3. เจ้าหน้าที่รักษาความปลอดภัยเฉพาะแห่ง ในกรณีงานระบบ On – line จะต้องมีอุปกรณ์ปลายทางหลายแห่ง แต่ละแห่งจะต้องมีเจ้าหน้าที่รักษาความปลอดภัย ซึ่งอาจจะเป็นคน ๆ เดียวกับผู้บริหารแต่ละแห่งย่อยนั้นก็ได้ เจ้าหน้าที่รักษาความปลอดภัยเฉพาะแห่งนี้จะต้องปฏิบัติตามคำสั่งของเจ้าหน้าที่รักษาความปลอดภัยที่ศูนย์กลางใหญ่

4. ผู้รับผิดชอบแฟ้มข้อมูล จะต้องรับผิดชอบความปลอดภัยของข้อมูลทั้งหมด ส่วนในกรณีงานระบบ On – line จะรับผิดชอบในการอนุญาตให้บุคคลใดใช้ข้อมูลนั้น ๆ และสร้างแฟ้มข้อมูลขึ้นใหม่เมื่อแฟ้มข้อมูลถูกทำลาย สรุปแล้ว ก็คือ

จะต้องรับผิดชอบทั้งด้านความถูกต้องและความปลอดภัยของแฟ้มข้อมูล

5. ผู้จัดการของหน่วยงาน รับผิดชอบในการทำงานของเขาที่จะมีผลต่อระบบความปลอดภัยพร้อมทั้งดูการปฏิบัติงานของคนภายใต้บังคับบัญชาอย่างเข้มงวด

6. ผู้ตรวจสอบ อาจใช้เทคนิควิธีการตรวจสอบระบบความปลอดภัยและการกำหนดระยะเวลาในการตรวจสอบตามความเหมาะสม ผู้ตรวจสอบทำงานคล้าย ๆ กับผู้บริหารในด้านระบบความปลอดภัยก็คือ จะต้องรายงานความบกพร่อง ณ จุดต่าง ๆ ที่ควรแก้ไขแก่ผู้ออกแบบระบบความปลอดภัย

7. เจ้าหน้าที่ทุก ๆ คน (All staff) ทุก ๆ คนที่เกี่ยวข้องในศูนย์คอมพิวเตอร์จะต้องช่วยกันทำงาน สอดส่องดูแล แก้ไขข้อบกพร่อง ระมัดระวังในงานทุกด้านภายในศูนย์ เพราะว่าระบบความปลอดภัย ความถูกต้องและความลับเฉพาะที่ดีจะมีความสัมพันธ์และเกี่ยวข้องซึ่งกันและกันจะขาดด้านใดด้านหนึ่งไม่ได้ ดังนั้น จะต้องได้รับความร่วมมือ ความรับผิดชอบของทุก ๆ คนที่เกี่ยวข้อง ดังคำกล่าวที่ว่า "Security is everyone ' s responsibility"

ข้อปฏิบัติเกี่ยวกับระบบความปลอดภัยที่ควรพิจารณาในด้านที่เกี่ยวกับบุคคล "คน" มีส่วนสำคัญอย่างมากต่อระบบ เนื่องจากคนเป็นผู้วางระบบ ซึ่งการทำงานในระบบจะดีก็ขึ้นกับคนทั้งนั้น ดังนั้นจะต้องคำนึงถึงสิ่งแวดล้อมที่เกี่ยวกับตัวบุคคลตลอดจนในด้านจิตใจเป็นสำคัญ เช่น

1. ให้ทุกคนที่เกี่ยวข้องในระบบความปลอดภัยเข้าใจในรายละเอียดต่าง ๆ เป็นอย่างดี อาจทำโดยการอบรม ให้เข้าใจอย่างมีเหตุผลว่า แต่ละระบบที่วางไว้แต่ละด้าน เช่น ความปลอดภัยของเครื่องจักรอุปกรณ์ ระบบโปรแกรมและข้อมูล ความปลอดภัยของสถานที่ทำการ ตลอดจนสิ่งต่าง ๆ ภายนอกที่เกี่ยวข้อง และการจัดระบบการควบคุมงานในด้านบริหาร รวมทั้งเจ้าหน้าที่ที่ปฏิบัติงาน ซึ่งจะให้เข้าใจว่าระบบเหล่านี้

วางไว้ทำไปเพื่ออะไร มีความสำคัญอย่างไร ถ้าบกพร่องจะเกิดความเสียหายแก่หน่วยงานอย่างไรให้ทุกคนได้รับรู้ไว้ ซึ่งจะทำให้แต่ละคนมีความรู้สึกว่าตนเองมีส่วนร่วมและมีความสำคัญต่อระบบความปลอดภัย จะทำให้ช่วยสอดส่องดูแลทุกอย่าง

2. ผู้บริหารจะต้องชี้แจงให้ลูกน้องเห็นความสำคัญของระบบความปลอดภัยอย่างจริงจัง ชี้ให้เห็นว่าทุก ๆ ส่วนในระบบมีความสำคัญทั้งนั้น ซึ่งจะมีผลต่อระบบความปลอดภัยรวม และทุกขั้นตอนของการทำงานไม่ควรบกพร่อง

3. ผู้บริหารจะต้องดูแล เอาใจใส่การทำงานของลูกน้องโดยหมั่นตรวจตราการทำงานอยู่เสมอ ถ้าลูกน้องบกพร่องควรจะชี้แจงให้เข้าใจและให้ทุก ๆ คนที่ทำงานเข้าใจไว้ว่าที่ผู้บริหารทำแบบนี้ไม่ใช่จะจับผิดการทำงานหรือเข้มงวดเกินไป จะต้องเข้าใจว่าปกติแล้วระบบความปลอดภัยนี้คนส่วนมากมักจะไม่ค่อยเห็นความสำคัญ จะสืบเสียต่อเมื่อเกิดความเสียหายเกิดขึ้นแล้วก็จะนึกได้จึงจะแก้ไข ซึ่งบางครั้งก็เกิดความเสียหายมากจนแก้ไขไม่ได้แล้ว ดังนั้นควรจะป้องกันไว้ตลอดเวลาดีกว่า

4. การปกครอง การบริหารงาน แนวนโยบายทั้งหลายจะต้องถูกต้องเป็นธรรมที่ทุกคนยอมรับ ซึ่งผู้บริหารงานตามสายงานโดยตรงมีหน้าที่รับผิดชอบเพื่อไม่ให้เกิดมีปัญหาด้านความไม่ชอบธรรมเกิดขึ้น ซึ่งจะทำให้ผู้ร่วมงานไม่พอใจเตรียมออกงานบ่อย ๆ และอาจนำเอกสารสำคัญ ความลับต่าง ๆ ไปเผยแพร่ได้ ซึ่งเป็นผลเสียต่อหน่วยงาน ต้องพยายามให้ผู้ร่วมงานร่วมทำงานตลอดไป

5. ผู้บริหารงานจะต้องพยายามศึกษา เข้าใจในลูกน้องของตนเองทั้งด้านนิสัย พื้นเพ ความรู้ ฯลฯ เพื่อใช้ประกอบในการทำงานพร้อมทั้งจะต้องจัดงานให้เหมาะสมไม่ให้มีความเหลื่อมล้ำกันมาก จัดคนให้เหมาะสมกับลำดับความสำคัญ ลักษณะงาน ฯลฯ

6. ผู้บริหารจะต้องสนใจเป็นพิเศษ เมื่อลูกน้องออกจากงานว่า สาเหตุ

ที่แท้จริงเป็นอะไร จะได้แก้ไข เพราะการที่ลูกน้องออกงานบ่อย ๆ ย่อมมีผลต่อระบบความปลอดภัยของหน่วยงานได้

7. ควรจะควบคุม ดูแลเป็นพิเศษสำหรับผู้ที่มาช่วยงานเป็นครั้งคราว ที่ไม่ได้เป็นพนักงานประจำของหน่วยงาน รายละเอียดทั้งหลายในด้านระบบความปลอดภัยของหน่วยงาน กฎเกณฑ์ต่าง ๆ ไม่ควรให้เห็นโดยเฉพาะเรื่องที่สำคัญห้ามเด็ดขาดเพื่อป้องกันความลับรั่วไหล บุคคลประเภทนี้ถ้าเลี่ยงได้ก็ควรจะเลี่ยง ควรเอาพนักงานในหน่วยงานของตนเองดีกว่า

8. ต้องศึกษาจากหน่วยงานอื่น ๆ ที่เกิดความผิดพลาดในระบบความปลอดภัยมาแล้ว เพื่อนำมาเป็นแนวทางในหน่วยงานของตนเอง

นอกจากนี้แต่ละหน่วยงานอาจจะมีข้อปลีกย่อยเพิ่มเติมได้อีกตามความเหมาะสม

ข. <u>ความรับผิดชอบต่อระบบความปลอดภัยในด้านต่าง ๆ ที่วางไว้</u> ในหน่วยงานใด ๆ เพื่อให้เกิดความปลอดภัย ความถูกต้อง และความลับเฉพาะต่อระบบนั้น จะต้องมีเทคนิคหลายอย่างพร้อมทั้งกำหนดวิธีการปฏิบัติให้แน่ชัด ซึ่งจะต้องกำหนดความรับผิดชอบแต่ละส่วนที่เกี่ยวข้องดังนี้

ก. ความรับผิดชอบทั้งศูนย์คอมพิวเตอร์ ผู้บริหารระดับสูงจะต้องรับผิดชอบ จะต้องเข้าใจหลักการในระบบความปลอดภัยที่ใช้ตลอดจนการทำงานของเจ้าหน้าที่ที่เกี่ยวข้องในระบบนี้ และจะต้องรับผิดชอบทั้งศูนย์คอมพิวเตอร์ จะต้องเข้าใจระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะที่สร้างขึ้นในศูนย์คอมพิวเตอร์นั้นทั้ง 3 ชั้น คือ

- ในด้านตัวระบบคอมพิวเตอร์
- ในด้านสถานที่ทำการและลักษณะต่าง ๆ ภายนอกที่เกี่ยวข้อง
- ในด้านการควบคุมงานด้านบริหารรวมทั้งเจ้าหน้าที่ที่ปฏิบัติงาน

ข. ความรับผิดชอบในด้านเทคนิคที่ใช้ในการวางระบบ จะมีผู้วิเคราะห์ระบบรับผิดชอบ ในแต่ละส่วนที่ได้วางระบบไว้ ทั้งด้านเครื่องจักรอุปกรณ์ ระบบโปรแกรม และข้อมูล ได้แก่

1. การควบคุมความถูกต้องในการประมวลผลข้อมูลทั้งระบบประมวลผลเป็นชุดข้อมูล และระบบประมวลผลที่เกิดขึ้นทันที

2. การควบคุมความปลอดภัยและความลับเฉพาะ เช่น เทคนิคการแสดงตัวหนังสือด้วยรหัส การควบคุมการใช้แฟ้มข้อมูล การใช้ระบบให้สัญญาณเมื่อมีเหตุร้าย การสร้างระบบความปลอดภัยในระบบโปรแกรมด้านปฏิบัติงาน วิธีการทำให้ข้อมูลกลับคืนหลังจากข้อมูลเดิมเสียหาย การควบคุมการใช้รหัสในการประมวลผลข้อมูล ฯลฯ เป็นต้น

3. ความรับผิดชอบในด้านระเบียบวิธีปฏิบัติที่ใช้ จะต้องมีผู้บริหารหน่วยงานประมวลผลข้อมูลรับผิดชอบ ให้ทุกคนในศูนย์คอมพิวเตอร์ปฏิบัติตามระเบียบวิธีที่วางไว้อย่างเคร่งครัด เช่น

- ระเบียบปฏิบัติ ในห้องเครื่องคอมพิวเตอร์
- ระเบียบปฏิบัติในการใช้ห้องสมุดข้อมูล
- ระเบียบการควบคุมงานในหน่วยงาน Input/output section ฯลฯ

4. ความรับผิดชอบในด้านโปรแกรมตลอดจนเจ้าหน้าที่เขียนโปรแกรมจะมีผู้บริหารในงานด้านโปรแกรมรับผิดชอบ เพื่อ

- ป้องกันไม่ให้เอาโปรแกรมไปใช้หรือแก้ไขโดยไม่ได้รับอนุญาต
- ควบคุมป้องกันไม่ให้มีการแก้ไขเปลี่ยนแปลงรายละเอียดประกอบโปรแกรม (Documentation) และเก็บรักษา

– ควบคุมวิธีปฏิบัติในการทดสอบโปรแกรม

5. ความรับผิดชอบในด้านระบบความปลอดภัยในด้านสถานที่ทำการและลักษณะต่าง ๆ ภายนอกเครื่อง จะมีผู้เชี่ยวชาญในแต่ละด้านรับผิดชอบร่วมกัน งานด้านนี้ได้แก่

– การป้องกันไฟไหม้
– การติดตั้งสัญญาณ การป้องกันเหตุร้ายจากการบุกรุก
– ด้านการระมัดระวังการขโมยต่อสายโทรศัพท์เพื่อฟังการสนทนา (Wiretapping) รวมทั้งการลอบฟัง (Eavesdropping)
– จัดหาติดตามข่าวคราวอุปกรณ์ป้องกันระบบความปลอดภัยที่ทันสมัยเพื่อนำมาใช้

6. ความรับผิดชอบในด้านบริหาร จะมีผู้บริหารศูนย์คอมพิวเตอร์รับผิดชอบ โดยจะต้องกำหนดความรับผิดชอบ อำนาจของบุคคลที่เกี่ยวข้องในศูนย์คอมพิวเตอร์ในหน้าที่ของงานด้านต่าง ๆ ที่กล่าวมาแล้ว ตลอดจนควบคุมกำหนดลำดับชั้นของการได้รับอนุญาตให้ใช้โปรแกรม ข้อมูลรายละเอียดประกอบโปรแกรม ซึ่งแตกต่างกันในแต่ละระดับของบุคคล และวิธีการทำให้ระบบกลับคืนเหมือนเดิมในกรณีที่มีความเสียหายเกิดขึ้น

7. ผู้ตรวจสอบ เพื่อตรวจสอบการทำงาน ผลงาน แผนงานที่ใช้ทุกขั้นตอนทุก ๆ ส่วนอาจนำเทคนิคบางอย่างมาใช้เพื่อการนี้ และอาจเตรียมข้อตรวจสอบ (Checklists) เพื่อใช้ในการตรวจสอบต่อไป

3.3.2 <u>การจัดสรรงบประมาณที่ใช้เพื่อวางแผนในระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะ</u> (Absolute security) ดังได้กล่าวมาแล้วว่าระบบความปลอดภัยอย่างแท้จริงนั้น ไม่สามารถกระทำได้ จึงไม่มีวิธีที่ดีใด ๆ จะสามารถ

ป้องกันได้ วิธีที่ได้กล่าวมาแล้วจะสามารถป้องกันอันตรายที่จะเกิดแก่ระบบคอมพิวเตอร์หรือข้อมูลให้มีโอกาส (Probability) เกิดขึ้นน้อยที่สุดเท่านั้น ความปลอดภัยที่อยู่ในระดับสูงจะต้องใช้เงินมาก ซึ่งผู้บริหารจะต้องพิจารณาก่อนว่าความปลอดภัยระดับไหนที่จะต้องใช้แก่หน่วยงานของตน ควรพิจารณาดังนี้

ก. ค่าใช้จ่ายในการกำจัดข้อผิดพลาด (Cost of error correction) ตามที่ได้กล่าวมาแล้วว่า ในการประมวลผลข้อมูลเพื่อให้ได้ข้อมูลที่ถูกต้อง กำจัดข้อผิดพลาดทั้งหลายก่อน ซึ่งได้แก่

1. ความผิดพลาดเนื่องจากเครื่องจักรอุปกรณ์
2. ความผิดพลาดเนื่องจากระบบโปรแกรมที่ช่วยการทำงานของระบบเครื่อง
3. ความผิดพลาดเนื่องจากระบบโปรแกรมใช้งาน
4. ความผิดพลาดจากเจ้าหน้าที่ปฏิบัติงานด้านเครื่อง
5. ความผิดพลาดจากข้อมูลเข้า
6. การออกแบบระบบโปรแกรมที่ไม่ดี เป็นต้น

การที่จะกำหนดค่าใช้จ่ายว่าเป็นเท่าไร เพื่อใช้ในการกำจัดข้อผิดพลาดแต่ละส่วนนั้น ก็ขึ้นกับลักษณะของงานด้วย เช่น ในระบบประมวลผลข้อมูลเป็นชุด ๆ ก็จะเสียค่าใช้จ่ายน้อยกว่าระบบประมวลผลที่เกิดขึ้นทันที เป็นต้น ในการประมวลผลแต่ละครั้งค่าใช้จ่ายที่จะเสียจะรวมถึงค่าใช้จ่ายด้าน

- การเขียนโปรแกรม
- เวลาตรวจสอบแก้ไขโปรแกรม

ฯลฯ

ข. ค่าใช้จ่ายในการสูญเสียข้อมูล (Cost of losing data)
ก่อนอื่นจะต้องรู้คุณค่าของข้อมูล (Value of data) ว่าข้อมูลทุกชนิดระดับความสำคัญต่างกัน ข้อมูลบางอย่างไม่ต้องเสียค่าใช้จ่ายในการป้องกัน แต่บางอย่างมีความสำคัญมากและจำเป็นมากต่อกิจการ ถ้าข้อมูลนี้หายหรือถูกทำลายจะทำความเสียหายอย่างร้ายแรงมากแก่กิจการ ข้อมูลประเภทนี้ต้องเสียค่าใช้จ่ายในการป้องกันมาก

เมื่อทราบคุณค่าของข้อมูลแล้วจะต้องประมาณดูว่าข้อมูลแต่ละประเภทนั้น ถ้าถูกทำลาย ถูกแก้ไข ถูกลักไป เราจะต้องเสียค่าใช้จ่ายมากน้อยแค่ไหนในการทำให้ข้อมูลกลับเข้าสู่สภาพเดิม

หลังจากได้ทราบคุณค่าของข้อมูลแต่ละพวกพร้อมทั้งค่าใช้จ่ายที่จะใช้ในการควบคุมระบบแล้ว ก็ต้องทำงบประมาณเพื่องานนี้ต่อไป ซึ่งงบประมาณไม่ควรเกิน 5 % ของงบประมาณของหน่วยประมวลผลข้อมูลทั้งหมด นอกจากนี้จะต้องคำนึงถึงว่าระดับของค่าใช้จ่ายจะต้องสัมพันธ์กันกับระดับของความไม่มั่นคง (Degree of vulnerability) ของศูนย์คอมพิวเตอร์และคุณค่าของข้อมูล ถ้าผลของความเสียหายหรือการถูกทำลายมีค่าสูงก็ต้องยอมเสียค่าใช้จ่ายเพื่อป้องกันไม่ให้เหตุการณ์ไม่ดีเกิดขึ้น ในทุกหน่วยงานใด ๆ ระดับความสำคัญของข้อมูลแต่ละพวกจะต่างกัน จะมีข้อมูลประเภทหนึ่งบางอย่างที่มีความสำคัญ และจำเป็นที่สุดต่อกิจการ ถ้าข้อมูลนี้หายหรือไม่ถูกต้องจะมีผลเสียหายมาก ขณะเดียวกันข้อมูลบางอย่างมีความสำคัญรองลงไป ถ้าหายหรือไม่ถูกต้องก็ไม่เป็นไร ทั้งสองพวกค่าใช้จ่ายที่ใช้ในการป้องกันก็ต่างกัน ส่วนระดับความไม่มั่นคงของศูนย์จะเกี่ยวข้องกับข้อมูลด้วย เช่น ข้อมูลไม่ถูกต้อง แฟ้มข้อมูลถูกทำลายหรือหาย ศูนย์คอมพิวเตอร์ถูกลอบวางเพลิงหรือถูกบุกรุกทำลาย เป็นต้น เหตุการณ์เหล่านี้จะต้องเสียค่าใช้จ่ายในการป้องกันทั้งนั้น ซึ่งเป็นหน้าที่ของหน่วยงานประมวลผลข้อมูลที่จะให้มีโอกาสเกิดน้อยที่สุด นอกจากนี้ จะต้องพิจารณาสิ่งแวดล้อม (Likelihood) ของเหตุการณ์เหล่านี้ เช่น โอกาสที่จะเกิดการก่อวินาศกรรมต่อศูนย์คอมพิวเตอร์นั้น ๆ หรือโอกาสที่จะเกิดไฟไหม้ หรือโอกาสที่จะเกิดการยักยอก ฯลฯ เป็นต้น ถ้าพิจารณาแล้วเห็นว่า

โอกาสที่จะเกิดเหตุการณ์เหล่านี้ต่ำมาก เช่น ศูนย์คอมพิวเตอร์ที่ไม่มีความสำคัญมากนักและข้อมูลที่ใช้ก็ไม่สำคัญ แบบนี้ค่าใช้จ่ายในการป้องกันทั้งศูนย์คอมพิวเตอร์ก็ต่ำ อาจจะมีแต่เพียงยามรักษาการณ์ก็พอ

งบประมาณที่ใช้ในระบบนั้น ควรจะใช้จ่ายให้มีประสิทธิภาพมากที่สุด บางศูนย์คอมพิวเตอร์อาจต้องการใช้งบประมาณในด้านระบบความถูกต้องมากกว่าระบบความปลอดภัยก็ได้ ซึ่งมีเทคนิคต่าง ๆ มาก เทคนิคทั้งหลายเหล่านั้นในศูนย์คอมพิวเตอร์ใด ๆ ไม่จำเป็นต้องนำมาใช้ให้ครบทั้งหมด ต้องเลือกเทคนิคที่คิดว่าจะให้คุณค่าและเหมาะสมต่อศูนย์เองและดูงบประมาณที่มีอยู่ด้วย เพื่อจัดระบบให้เหมาะสมด้วย ตัวอย่างเช่น ศูนย์คอมพิวเตอร์บางแห่งวางระบบด้านความปลอดภัยอย่างดี อาจจะมียามรักษาการณ์พร้อมทั้งทีวีและอุปกรณ์ติดต่อแจ้งภัยทั่วทั้งศูนย์คอมพิวเตอร์ และติดระบบการป้องกันภัยเป็นระบบให้สัญญาณที่ประตู ซึ่งทั้งหมดนี้ค่าใช้จ่ายสูง แต่ในขณะเดียวกันภายในห้องคอมพิวเตอร์จริง ๆ ไม่ได้วางระบบความปลอดภัยไว้เลย ระบบการควบคุมข้อมูล วิธีการทำให้ระบบกลับคืนใหม่ ฯลฯ ก็ไม่ได้ทำ จะเห็นว่าการวางระบบความปลอดภัยในศูนย์คอมพิวเตอร์แบบนี้ก็ไม่เกิดประโยชน์ และเสียค่าใช้จ่ายด้วย

เนื่องจากงบประมาณที่ใช้ในระบบความปลอดภัยไม่ควรเกิน 5 % ของงบประมาณทั้งหมดของหน่วยประมวลผลข้อมูล ซึ่งงบประมาณส่วนนี้แยกได้ดังนี้

- ไม่เกิน 5 % สำหรับงานด้านโปรแกรมที่ใช้ระบบ
- ไม่เกิน 40 % สำหรับควบคุมด้านความถูกต้อง
- ไม่เกิน 10 % สำหรับด้านการประมวลผลหรือเวลาใช้เครื่องควบคุมระบบความปลอดภัย ความถูกต้อง
- ส่วนที่เหลือก็แล้วแต่ความเหมาะสม

3.3.3 <u>การควบคุมภายในหน่วยงานคอมพิวเตอร์</u>[10] เนื่องจากการประมวลผลข้อมูลนั้นงานทุกชนิดจะต้องผ่านเข้าสู่จุดศูนย์กลาง คือผ่านเข้าสู่การประมวลผลโดยเครื่องคอมพิวเตอร์ ซึ่งเป็นการรวมงานในหน้าที่ต่าง ๆ เข้ามาอยู่

ในที่แห่งเดียวกัน ถ้ามิได้มีการกำหนดวิธีการควบคุมให้รัดกุมทั้งภายในภายนอกแผนกประมวลผลข้อมูลแล้ว ก็อาจจะก่อให้เกิดความผิดพลาดหรือการทุจริตเกิดขึ้นได้ ดังนั้น จึงจำต้องคำนึงถึงการจัดระบบการทำงานตลอดจนวิธีการควบคุมความถูกต้องให้รัดกุม เพื่อให้เกิดความแน่ใจว่าไม่มีข้อมูลสูญหายไป หรืออาจนำมาประมวลผลซ้ำอีก หรืออาจนำมาแก้ไขเปลี่ยนแปลงซ้ำอีก นอกจากนั้นยังป้องกันการยักยอก ซึ่งสิ่งนี้จะเกี่ยวโยงไปถึงการเขียนโปรแกรมและผู้เขียนโปรแกรมที่อาจจะแก้ไขโปรแกรมได้ การควบคุมภายในนี้จะต้องมีการวางแผนล่วงหน้าเพื่อจะได้คลุมทุก ๆ ด้าน เพราะมิเช่นนั้นแล้วผลดีที่ได้รับจากประสิทธิภาพของเครื่องคอมพิวเตอร์ก็อาจจะถูกลบล้างไป ซึ่งจะนำผลเสียหายมาสู่หน่วยงานเป็นส่วนรวมได้ในที่สุด

ความจำเป็นที่ต้องมีการควบคุมภายในอย่างใกล้ชิด ในระบบงานที่ไม่ใช้คอมพิวเตอร์งานได้ถูกแบ่งแยกปฏิบัติโดยแผนกต่าง ๆ และมีพนักงานจำนวนมากรับผิดชอบในแต่ละส่วนของงาน ตัวอย่างเช่น ในบริษัทแห่งหนึ่งเมื่อได้รับใบสั่งซื้อจากลูกค้า การอนุมัติให้เครดิตแก่ลูกค้าจะกระทำโดยแผนกหนึ่ง การออกบิลเรียกเก็บเงินทำโดยอีกแผนกหนึ่ง และการรับชำระหนี้ตลอดจนการออกใบเสร็จรับเงินก็จะแบ่งแยกกระทำโดยแผนกที่ไม่เกี่ยวกัน จะเห็นว่าโครงสร้างของระบบงานได้แบ่งแยกกันระหว่างผู้รับใบสั่งซื้อ ผู้อนุมัติ ผู้ดำเนินการขาย ผู้รับชำระหนี้และผู้ออกใบเสร็จ การแบ่งแยกหน้าที่กันเช่นนี้ทำให้ยากที่จะเกิดการทุจริต เนื่องจากบุคคลหลายคนจากแผนกงานที่ต่างกันจะต้องร่วมทุจริตด้วยกันจึงจะทำได้สำเร็จ นอกจากนี้ แต่ละแผนกยังสามารถทดสอบความถูกต้องกับแผนกอื่นโดยวิธีการสอบยันอีกด้วย ทำให้ง่ายแก่การตรวจสอบ

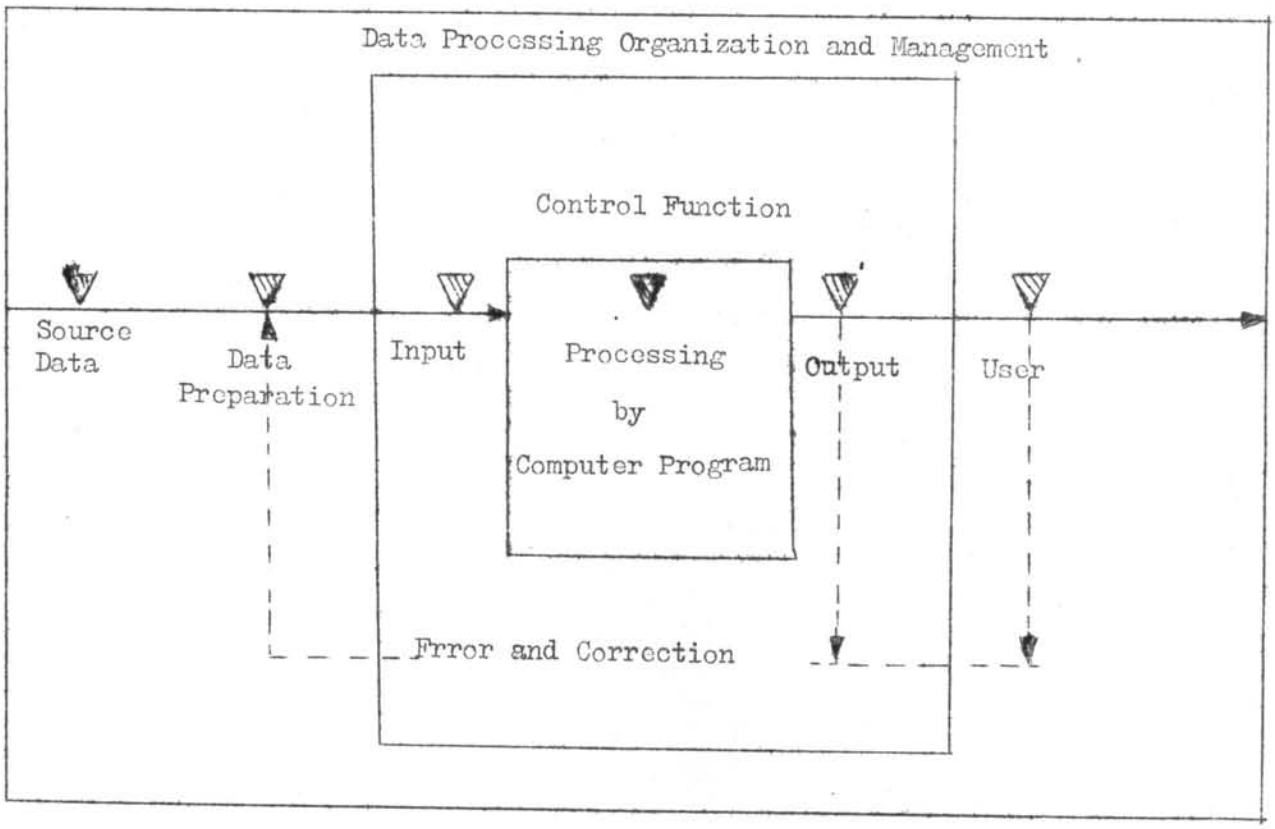
เมื่อใช้คอมพิวเตอร์ข้อมูลต่าง ๆ มักจะถูกรวบรวมไว้ในที่แห่งเดียว และขั้นตอนการปฏิบัติงานมักจะถูกรวบรัดให้สั้นเข้าเพื่อความสะดวกในการใช้เครื่อง แผนกคอมพิวเตอร์อาจจะปฏิบัติขั้นตอนทั้งหมดในการรับใบสั่งซื้อ ออกใบเก็บเงิน และปฏิบัติงานด้านบัญชี จะเห็นได้ว่า การรวบรวมระบบงานให้อยู่ในหน่วยงานน้อยหน่วยมีผลเท่ากับการลดความเข้มแข็งของระบบควบคุม เหตุนี้จึงจำเป็นต้องให้มีการควบคุมภายในอย่างใกล้ชิดเป็นพิเศษ ในต่างประเทศในปัจจุบันนี้มักจะนิยม

ให้ผู้ตรวจสอบหรือผู้เชี่ยวชาญในด้านการควบคุมภายในมีส่วนร่วมในการวางระบบตั้งแต่ขั้นผู้ออกแบบระบบ ทั้งนี้เพื่อป้องกันแก้ไขจุดอ่อนของระบบและวางจุดควบคุม (Control points) ที่เหมาะสมตั้งแต่เริ่มงานนั้น ดังรูป 3.39

การทุจริตทางด้านคอมพิวเตอร์มักเกิดจากวงใน ผู้เชี่ยวชาญในด้านการป้องกันทุจริตจึงแนะนำว่า ควรจะวางมาตรการในด้านการควบคุมภายในอย่างใกล้ชิด โดยเฉพาะการตรวจสอบระบบงานและผู้ใช้สำหรับในต่างประเทศนั้น การทุจริตโดยอาศัยเครื่องคอมพิวเตอร์กำลังได้รับการกล่าวถึงอย่างแพร่หลาย และการทุจริตมักเกิดขึ้นในหน่วยงานที่เร่งรีบเปลี่ยนระบบการใช้บุคคลมาเป็นระบบใช้คอมพิวเตอร์ โดยไม่ได้ศึกษาวางแผนให้รัดกุมเพราะเชื่อว่าระบบคอมพิวเตอร์เป็นระบบที่ทำงานทุกอย่างโดยไม่ผิดพลาด ผลของความเชื่อเช่นนี้ทำให้มีการนำเอาระบบคอมพิวเตอร์มาใช้โดยไม่วางระบบควบคุมที่มีประสิทธิภาพควบคู่ไปด้วย และสาเหตุอีกประการหนึ่งก็คือผู้บริหารชั้นสูงตลอดจนพนักงานทั่วไปมักขาดความรู้ความเข้าใจในระบบคอมพิวเตอร์อย่างแท้จริง เหตุนี้จึงมักมอบหมายความรับผิดชอบทั้งหมดในการควบคุมศูนย์คอมพิวเตอร์ให้ผู้เตรียมโปรแกรม ผู้ควบคุมเครื่องหรือคนภายนอก ฯลฯ เพียงไม่กี่คน ซึ่งเป็นสาเหตุให้การทุจริตเกิดขึ้นโดยง่าย การใช้คอมพิวเตอร์โดยไม่ควบคุมให้รัดกุมย่อมเป็นการเสี่ยงภัยอย่างมาก ภัยเหล่านี้ได้เกิดขึ้นแล้ว เช่น

1. การทุจริตทางด้านการเงินและการค้า
2. การทำให้คอมพิวเตอร์บิดเบือนข้อเท็จจริงของรายงานเพื่อผลประโยชน์ในทางมิชอบ
3. การเสี่ยงต่อการสูญหายของข้อมูล
4. การเสี่ยงต่อการถูกเปิดเผยความลับ

1. <u>การทุจริตทางด้านการเงินและการค้า</u> ปัจจุบันเฉพาะในสหรัฐอเมริกาเพียงแห่งเดียวเงินนับร้อยล้านดอลล่าร์ได้ถูกยักยอกโดยใช้ระบบคอมพิวเตอร์เป็นเครื่องช่วย ความสูญเสียนี้ประมาณกันว่ามากกว่าเสียหายอันเกิดจากการถูกโจรกรรมทั้งสิ้น



รูป 3.39 จุดสำคัญที่ต้องการการควบคุมเป็นพิเศษ(11)

จากการสำรวจปรากฏว่าคุณสมบัติในระบบการทำงานของคอมพิวเตอร์เองและระเบียบปฏิบัติงานที่วางไว้ไม่ดีพอ มีส่วนช่วยให้การทุจริตเกิดขึ้นอย่างมากมายต่อการตรวจสอบยิ่งกว่าระบบงานแบบเดิมที่ใช้บุคคลเป็นผู้ปฏิบัติงาน วิธีพื้นฐานที่ผู้ทุจริตใช้ในการฉ้อโกงประกอบไปด้วย

ก. <u>การดัดแปลงแก้ไขข้อมูลเบื้องต้น</u> เป็นวิธีที่ใช้กันอย่างแพร่หลายและทำได้ง่ายเพราะข้อมูลที่ได้รับการแก้ไขเพื่อผลในการทุจริตจะดูไม่แตกต่างไปจากข้อมูลปกติเลย ถ้าระเบียบควบคุมด้านข้อมูลเบื้องต้นไม่ดีพอแล้วการทุจริตจะเกิดขึ้นโดยง่าย ตัวอย่าง เช่น

รองประธานของ New York Brokerage House ได้ยักยอกเงินของบริษัทกว่า $ 250,000 ในช่วงเวลา 5 ปี โดยการแก้ไขข้อมูลเบื้องต้น นอกจากนี้วิธีทุจริตยังประกอบไปด้วยกรรมวิธีซับซ้อนในการเขียนโปรแกรมให้เพิ่มยอดในบัญชีเงินค่าหุ้นส่วนตัวของตนเองและภรรยา ในขณะเดียวกันก็ลดยอดรายได้ดอกเบี้ยของบริษัทในจำนวนที่เท่ากัน

ธนาคารแห่งหนึ่งในบอสตันได้จัดเตรียมบัตรคอมพิวเตอร์ที่ใช้เป็นแบบฟอร์มใบนำส่งเงินฝากใบแทนไว้ในห้องโถงสำหรับลูกค้าที่ลืมนำแบบฟอร์มใบนำส่งเงินฝากเฉพาะตนซึ่งพิมพ์หมายเลข MICR ประจำบัญชีรายตัวได้ใช้แบบฟอร์มใบแทนนี้ไปพลาง ๆ ก่อน แบบฟอร์มใบแทนที่ไม่ได้พิมพ์หมายเลข MICR นี้เมื่อนำเข้าเครื่องอ่านจะถูกแยกออกมาโดยเครื่องเพื่อนำไปเข้าบัญชีด้วยมือในภายหลัง เมื่อได้ศึกษากรรมวิธีปฏิบัติข้อมูลโดยแจ้งชัดผู้ทุจริตได้แอบเอาแบบฟอร์มใบนำส่งเงินฝากซึ่งได้พิมพ์หมายเลข MICR บัญชีของตนมาเปลี่ยนไว้แทนแบบฟอร์มใบนำส่งเงินฝากใบแทนนั้น ตลอดทั้งวันลูกค้าธนาคารซึ่งลืมนำแบบฟอร์มใบนำส่งเงินฝากเฉพาะตนมาได้ใช้แบบฟอร์มที่ผู้ทุจริตเตรียมไว้โดยไม่รู้ตัว หลังจากรอให้มีการหักล้างบัญชีกันเรียบร้อยแล้วผู้ทุจริตได้ถอนเงินในบัญชีออกจนหมดสิ้น แล้วหลบหนีไป

ข. <u>การดัดแปลงแก้ไขโปรแกรม</u> โดยปกติจะทำได้ยากกว่าการดัดแปลงข้อมูลเบื้องต้น เนื่องจากการเขียนโปรแกรมโดยตัวของมันเองเป็นของยาก

แก่การเข้าใจ อย่างไรก็ตาม ด้วยเหตุที่โปรแกรมเป็นของที่ซับซ้อน ดังนั้น ผู้บริหารชั้นสูงจึงไม่ควบคุมโดยใกล้ชิดและมอบความไว้วางใจให้แก่ผู้เขียนโปรแกรมรับผิดชอบทั้งหมด เหตุนี้การทุจริตทางด้านการแก้ไขโปรแกรมจึงมักเกิดขึ้นเสมอ ตัวอย่าง เช่น

โปรแกรมเมอร์คนหนึ่งของ National City Bank แห่ง Miniapolis ได้รับมอบหมายให้ออกแบบโปรแกรม Check Handling Systems ซึ่งเขามีบัญชีเงินฝากกระแสรายวันอยู่ ไม่เพียงแต่ออกแบบโปรแกรมสำหรับประมวลผลเช็คเพียงอย่างเดียวในตอนกลางของโปรแกรมอันสลับซับซ้อนนี้ เขายังได้ถือโอกาสแทรกโปรแกรมส่วนพิเศษซึ่งสั่งให้ระบบคอมพิวเตอร์มองข้ามเช็คส่วนตัว ซึ่งเขาเบิกเงินเกินบัญชีทั้งสิ้น ด้วยเหตุนี้เขาจึงมีเงินใช้อย่างฟุ่มเฟือยไม่ขาดมือเป็นเวลาหลายเดือน จนกระทั่งวันหนึ่งระบบคอมพิวเตอร์เกิดขัดข้องจึงต้องทำการประมวลผลเช็คด้วยมือ จึงเป็นเหตุให้ความลับของเขาถูกเปิดเผยเพราะเสมียนคนหนึ่งสังเกตพบการทุจริต

การใช้เครื่องคอมพิวเตอร์ร่วมการทุจริตโดยการใช้ความรู้เขียนโปรแกรมให้คอมพิวเตอร์ทำตามที่ต้องการอีกตัวอย่างหนึ่งได้แก่ สมุหบัญชีของบริษัทแห่งหนึ่งในแคลิฟอร์เนียยักยอกเงินมากกว่าหนึ่งล้านดอลล่าร์จากบริษัทโดยเขียนโปรแกรมให้เครื่องลงรายการค่าวัตถุดิบมากกว่าที่จ่ายจริงและโอนเงินส่วนเกินไปเข้าบัญชีของบริษัทหุ่นที่ตั้งขึ้น

ก. <u>การสร้างข้อมูลปลอม</u> โดยมากมักจะทำร่วมกับการดัดแปลงแก้ไขข้อมูลที่มีอยู่แล้ว หรือการแก้ไขโปรแกรมประกอบไปด้วยพร้อมกัน ตัวอย่าง เช่น

เมื่อเร็ว ๆ นี้ เจ้าหน้าที่ตำรวจในนิวเจอซี่ได้จับกุมรองประธานของ Trenton Bank พร้อมกับพนักงานศูนย์คอมพิวเตอร์ชั้นผู้ใหญ่ เนื่องจากจับได้ว่าทุจริตเงิน 128,000 ดอลล่าร์ โดยการสร้างข้อมูลปลอมและแก้ไขโปรแกรมยักยอกเงินจากลูกค้าในบัญชีที่ไม่เคลื่อนไหวเป็นเวลานาน

นอกจากนี้ยังมีพนักงานแผนกคอมพิวเตอร์ของ Human Resources Administration ในนิวยอร์คได้ร่วมกันวางโปรแกรมให้คอมพิวเตอร์พิมพ์เช็คเงินเดือนปลอมเป็นเงินกว่าสองล้านดอลล่าร์ในช่วงเวลา 1 ปี

2. <u>การทำให้คอมพิวเตอร์บิดเบือนข้อเท็จจริงของรายงานเพื่อผลประโยชน์ในทางมิชอบ</u> เช่น ผู้อำนวยการพยายามบิดเบือนข้อเท็จจริงของรายการ/เงินซึ่งเตรียมโดยระบบคอมพิวเตอร์เพื่อที่จะแสดงฐานะของบริษัทดีกว่าความเป็นจริง แสดงรายการทรัพย์สินสูงกว่าความเป็นจริง หรือแสดงรายการหนี้สินต่ำกว่าความเป็นจริง ตัวอย่าง เช่น

ในปี 2515 บริษัทประกันภัยแห่งหนึ่งต้องการเพิ่มราคา Equity Stock จึงป้อนข้อมูลโดยยอกย้อนว่ามีผู้ถือกรมธรรม์ของบริษัทกว่า 97,000 กรมธรรม์ ในขณะที่ความจริงมีน้อยกว่า 3,300 กรมธรรม์เท่านั้น

3. <u>การเสี่ยงต่อการสูญหายของข้อมูล</u> การเก็บรักษาบัตรเจาะ เทปแม่เหล็ก และจานแม่เหล็ก โดยไม่ระมัดระวังอาจเป็นเหตุให้ข้อมูลถูกทำลายได้โดยง่าย สิ่งที่เป็นอันตรายต่อข้อมูลเป็นอย่างยิ่งก็คือ อัคคีภัย วินาศภัย และความเผลอเรอ เป็นต้น

อัคคีภัยเป็นภัยร้ายแรงที่สุดที่คุกคามศูนย์คอมพิวเตอร์ ในห้องคอมพิวเตอร์โดยมากมักจะเต็มไปด้วยวัตถุไวไฟ เช่น บัตรเจาะ และเทปแม่เหล็ก อันทำมาจากพลาสติกซึ่งเมื่อเกิดเพลิงไหม้ย่อมยากที่จะดับ อุปกรณ์ประเภทสายไฟและกล่องบรรจุเทปพลาสติก เมื่อไหม้ไฟจะทำให้เกิดควันพิษ ซึ่งเป็นอันตรายต่อพนักงานผู้ทำการดับเป็นอย่างยิ่ง ตัวเครื่องคอมพิวเตอร์ตลอดจนอุปกรณ์ต่าง ๆ อาจมีสัญญาประกันคุ้มภัยและสามารถนำมาเปลี่ยนได้ในเวลาอันรวดเร็ว อย่างไรก็ตาม การสร้างข้อมูลขึ้นใหม่แทนข้อมูลที่สูญเสียไป นอกจากจะต้องใช้เวลานานแล้ว บางครั้งยังไม่อาจกระทำได้อีกด้วย โดยปกติเมื่อเปรียบเทียบกันระหว่างหน่วยงานที่ใช้คอมพิวเตอร์และหน่วยงานทั่วไปที่ไม่ใช้ อัคคีภัยจะเป็นอันตรายต่อข้อมูล

ในหน่วยงานที่ใช้คอมพิวเตอร์มากกว่า ทั้งนี้เพราะในหน่วยงานที่ใช้บุคคลปฏิบัติงานข้อมูลจะกระจายอยู่เป็นบริเวณกว้างทั้งมีสำเนาและความจำส่วนบุคคลเป็นระบบ Back up โดยอัตโนมัติ แต่ในหน่วยงานที่ใช้คอมพิวเตอร์ ข้อมูลต่าง ๆ จะถูกรวบรวมไว้ในที่แห่งเดียว ดังนั้นหน่วยงานใดไม่มีระบบ Back up ที่ดีพอแล้วย่อมอยู่ในภาวะที่เสี่ยงภัยอย่างมาก

ส่วนอันตรายจากวินาศภัยนั้นจะเห็นได้จากในช่วงเวลา 15 เดือน ซึ่งสิ้นสุดเมื่อกันยายน ค.ศ. 1970 เฉพาะในสหรัฐอเมริกาแห่งเดียวมีการวางระเบิดศูนย์คอมพิวเตอร์ถึง 4,330 ครั้ง ทำให้คนตายกว่า 40 คนและบาดเจ็บกว่า 380 คน

นอกจากนี้เมื่อเร็ว ๆ นี้ บริษัท Dow Chemical ได้ถูกโจมตีโดยพวกจลาจลผิว พวกก่อการจลาจลได้แอบเข้าไปในห้องคอมพิวเตอร์ และใช้แท่งแม่เหล็กเล็ก ๆ ลบข้อมูลในเทปแม่เหล็ก 1,000 ม้วน ทั้งยังแอบซ่อนแท่งแม่เหล็กไว้ในที่ต่าง ๆ ทั่วห้อง แท่งแม่เหล็กเป็นเครื่องมือที่แพร่หลายที่สุด ในการใช้ทำลายข้อมูล เพียงแต่นำมาใกล้เทปแม่เหล็กข้อมูลที่บรรจุอยู่จะถูกทำลายหมดสิ้น

ตัวอย่างของการสูญหายของข้อมูลที่เกิดจากความเผลอเรออีกแห่งหนึ่งเกิดขึ้นในธนาคารแห่งหนึ่งในสหรัฐอเมริกา พนักงานคุมเครื่องได้ลบบัญชีเงินฝากเมื่อเรียกของลูกค้าโดยบังเอิญในขณะที่ใช้ไฟฉายชนิดเหน็บกระเป๋าเสื้อส่องตรวจแฟ้มข้อมูลที่เป็นจานแม่เหล็กโดยไม่ทราบว่าด้านหนึ่งของไฟฉายนั้น มีสภาพเป็นแม่เหล็กซึ่งจะทำการลบข้อมูลทุกชนิดขณะที่มันเคลื่อนผ่าน

ตัวอย่างอีกอย่างหนึ่งได้แก่ การทุจริตโดยการแอบขโมยข้อมูลที่เก็บรักษาในระบบคอมพิวเตอร์โดยบุคคลภายนอก เช่น เมื่อเดือนมิถุนายน 2519 อดีตพนักงานของบริษัทเอกชนซึ่งรับเหมาออกแบบโปรแกรมให้ Federal Energy Administration แห่งสหรัฐอเมริกาได้ถูกจับในข้อหาจารกรรมความลับสุดยอดของ FEA

. การเสี่ยงต่อการถูกเปิดเผยความลับ บุคคลภายนอกบางคนอาจต้องการที่จะทราบข้อมูลลับ ซึ่งเก็บรักษาไว้ในระบบคอมพิวเตอร์ เช่น ข้อมูลเกี่ยวกับรายละเอียดกรรมวิธีการผลิตสินค้า รายงานการค้นคว้า ตลอดจนโปรแกรมซึ่งได้พัฒนาไว้สำหรับงานพิเศษ การล้วงความลับจากระบบคอมพิวเตอร์อาจทำได้โดยวิธีง่าย ๆ เช่น

– ติดสินบนบุคคลผู้ควบคุมเครื่องคอมพิวเตอร์ให้ Copy รายการจากแฟ้มข้อมูลหลัก ซึ่งอาจทำสำเร็จภายในเวลาไม่กี่นาทีโดยไม่ทิ้งร่องรอยใด ๆ ไว้เลย

– เก็บกระดาษคัดลอกจากเครื่องพิมพ์กระดาษต่อเนื่อง หรือเอกสารอื่น ๆ ที่ใช้แล้ว

– ใช้วิธีขโมยต่อสายโทรศัพท์เพื่อฟังการสนทนา ดักจับข้อมูลที่ส่งผ่านระบบสาย เช่นในระบบ On - line

– ใช้เครื่องอี.. ทรนิค ซึ่งสามารถตรวจจับการแผ่รังสีของคลื่นแม่เหล็กไฟฟ้า ซึ่งเกิดจากอุปกรณ์คอมพิวเตอร์ และเปลี่ยน Radiator ให้กลับมาอยู่ในรูปซึ่งอ่านได้ (ในการสาธิตครั้งหนึ่งในสหรัฐอเมริกา เครื่องรับและเครื่องพิมพ์ได้ถูกซ่อนไว้ในรถบรรทุก ซึ่งนำมาจอดซุ่มอยู่ใกล้ศูนย์คอมพิวเตอร์ที่ไม่ได้ติดตั้งระบบป้องกันการแผ่รังสี ผลปรากฏว่าข้อมูลทั้งสิ้นที่พิมพ์ลงในศูนย์คอมพิวเตอร์ได้ถูกคัดลอกโดยเครื่องพิมพ์ที่ซ่อนไว้ในรถบรรทุกในขณะเดียวกัน)

เทคนิคอื่น ๆ ในการฉ้อโกงยังประกอบไปด้วยการทำโปรแกรมให้หักเงินจำนวนเล็กน้อยเพียงเศษสตางค์จากบัญชีย่อยซึ่งมีจำนวนนับพันบัญชี เช่น บัญชีเงินฝากรายตัวของลูกค้าธนาคาร หรือบัญชีหักภาษี ณ ที่จ่ายของพนักงานแล้วโอนเงินนั้นมาเข้าบัญชีเงินฝากร้างค้าหุ้นที่ตั้งขึ้น เป็นต้น

ตัวอย่างที่กล่าวมาเป็นเพียงส่วนน้อยของกรรมวิธีที่ใช้เท่านั้น เนื่องจากบริษัทที่เกี่ยวข้องกับการทุจริตมักจะพยายามรักษาภาพพจน์ของตนต่อสาธารณะชน ข้อมูลและรายละเอียดการทุจริตจึงมักถูกปกปิดหรือมีคำแถลงแต่เพียงสั้น ๆ เท่านั้น

จากตัวอย่างที่กล่าวมาเป็นเพียงหนึ่งในหลายพันกรณีซึ่งเกิดขึ้นในขณะนี้ ดังที่ Terry Knoepp หัวหน้าอัยการแห่งสหรัฐอเมริกาขนานนามว่า "อาชญากรรมแห่งปี ค.ศ. 1980 การทุจริตโดยใช้เครื่องคอมพิวเตอร์" อาชญากรแผนใหม่ใช้ความรู้ความชำนาญในด้านคอมพิวเตอร์ประกอบการทุจริต ซึ่งทำความเสียหายให้ธนาคาร บริษัทเอกชนและรัฐบาลเท่าที่เปิดเผยเป็นเงินนับ $ 100 ล้านต่อปี นอกจากนั้นยังประมาณกันว่า 85 % ของการทุจริตโดยคอมพิวเตอร์ ยังดำเนินต่อไปโดยไม่อาจตรวจพบหรือไม่ได้รับการเปิดเผย และจากหนังสือ 'Crime by Computer' ของ Standford Research Institute รายงานว่ายอดเงินจากการทุจริตตกประมาณปีละกว่า 300 ล้านดอลล่าร์ ด้วยเหตุดังกล่าวบริษัทผู้ผลิตคอมพิวเตอร์ ผู้ตรวจบัญชี และนักกฎหมายจึงได้รีบเร่งที่จะหาทางป้องกันอาชญากรรมแผนใหม่นี้ เมื่อต้นเดือนสิงหาคม 2519 คณะผู้แทนกรมอัยการแห่งสหรัฐอเมริกาได้ร่วมประชุมหารือกัน ณ มหาวิทยาลัยแคลิฟอร์เนียเพื่อจะวางลู่ทางที่มีประสิทธิภาพอย่างเพียงพอเพื่อป้องกันการทุจริตที่จะเกิดขึ้น

ถึงแม้ว่าการใช้ระบบคอมพิวเตอร์จะก่อให้เกิดจุดอ่อนในระบบควบคุม ระบบป้องกันภัย และระบบรักษาความลับได้ง่ายดังได้กล่าวมาแล้ว ถ้าคิดโดยนัยตรงข้าม หากวางระบบแก้ข้อบกพร่องให้เหมาะสมผู้ใช้กลับสามารถจะแสวงหาผลประโยชน์จากคุณสมบัติของคอมพิวเตอร์มาเสริมสร้างระบบควบคุมให้รัดกุมยิ่งกว่าในระบบใด ๆ ทั้งสิ้น เพราะ

– ความสามารถของเครื่องคอมพิวเตอร์ที่อาจจะปฏิบัติตามนโยบายและขั้นตอนที่วางไว้อย่างเที่ยงตรงและสม่ำเสมอ

– ถ้ามีการควบคุมอย่างเหมาะสมการที่จะเปลี่ยนแปลงหรือแก้ไขข้อมูลในทางฉ้อโกงย่อมทำได้ยาก

– เมื่อป้อนข้อมูลที่ถูกต้องและโปรแกรมที่ใช้ไม่ผิดพลาด คอมพิวเตอร์ย่อมเหนือกว่าในด้านการให้ผลลัพธ์ที่ถูกต้อง แม่นยำ เป็นต้น

ดังได้กล่าวมาแล้วว่า การทุจริตทางด้านคอมพิวเตอร์มักเกิดจากวงในผู้เชี่ยวชาญในด้านการป้องกันทุจริตจึงแนะนำว่า ควรจะวางมาตรการในด้านการควบคุมภายในหน่วยงานคอมพิวเตอร์อย่างใกล้ชิด ซึ่งได้แก่

1. การควบคุมข้อมูลเบื้องต้น
2. การควบคุมระหว่างประมวลผล
3. การควบคุมผลลัพธ์
4. การควบคุมคุณภาพของงาน
5. การควบคุมทางด้านการจัดองค์การของหน่วยงาน
6. การควบคุมด้านการทำเอกสารรายละเอียดประกอบ
7. การควบคุมด้านการปฏิบัติงาน
8. การควบคุมในกรณีที่ใช้บริการคอมพิวเตอร์ภายนอก

1. การควบคุมข้อมูลเบื้องต้น โดยปกติข้อมูลดิบเบื้องต้นจะเป็นจุดอ่อนของระบบคอมพิวเตอร์ ซึ่งควรได้รับการสนใจเป็นพิเศษ การทดสอบความถูกต้องของระบบงานหรือโปรแกรมอาจจะกระทำนาน ๆ ครั้งหนึ่ง แต่ปัญหาเกี่ยวกับข้อมูลเบื้องต้นจะต้องได้รับการตรวจสอบอย่างสม่ำเสมอ ไม่ว่าระบบคอมพิวเตอร์หรือโปรแกรมที่วางไว้จะดีเพียงใดก็ตาม ถ้าข้อมลเบื้องต้นไม่ถูกต้องตั้งแต่แรกแล้วผลลัพธ์ย่อมไม่มีทางถูกต้องไปได้ รายการควบคุมทางด้านข้อมูลเบื้องต้นนี้ถือเป็นหัวใจสำคัญของระบบคอมพิวเตอร์ จะสังเกตได้ว่าระบบคอมพิวเตอร์ขององค์การใดจะประสบผลสำเร็จหรือล้มเหลวก็มักมีผลเกี่ยวเนื่องมาจากข้อมูลเบื้องต้นเป็นส่วนใหญ่ ซึ่งอาจสรุปได้ว่าข้อมูลเบื้องต้นอาจผิดพลาดได้ง่ายด้วยเหตุ 5 ประการ คือ

1. อาจได้รับการบันทึกมาผิดตั้งแต่จุดเริ่มต้น
2. อาจได้รับการถ่ายทอดเป็นข้อมูลที่พร้อมจะเข้าเครื่องผิด (Machine Readable forms) ผิด
3. สูญหาย

4. ได้รับการประมวลผลไม่ถูกต้องเมื่ออ่านโดยเครื่องคอมพิวเตอร์

5. ถูกแก้ไขเพื่อผลในการทุจริต

เนื่องจากข้อมูลเบื้องต้นที่จะนำมาประมวลผลนั้นส่วนใหญ่จะมาจากแผนกที่ต้องการใช้ข้อมูล ซึ่งตามปกติข้อมูลเบื้องต้นเหล่านี้จะจัดเตรียม โดยเฉพาะผู้ใช้ข้อมูลและอาจเกิดข้อผิดพลาดขึ้นได้จากแผนกดังกล่าว โดยที่ข้อผิดพลาดเหล่านี้จะไม่สามารถตรวจพบได้ในระหว่างประมวลผลดังนั้นการควบคุมข้อมูลเบื้องต้นจึงเป็นสิ่งสำคัญยิ่ง และจุดที่จะเกิดข้อผิดพลาดซึ่งจะต้องระมัดระวังเป็นพิเศษ คือ

– จุดที่ข้อมูลเบื้องต้นก่อกำเนิดขึ้น และถูกแปลงเป็นข้อมูลที่พร้อมที่จะป้อนเข้าเครื่อง

– จุดที่ข้อมูลถูกป้อนเข้าเครื่อง

– จุดที่ข้อมูลถูกนำไปใช้หรือส่งต่อภายในหน่วยงาน

ฉะนั้น เพื่อให้บรรลุถึงความถูกต้องแม่นยำของข้อมูล จึงต้องจัดระบบของการควบคุมข้อมูลตามจุดต่าง ๆ ที่อาจเกิดข้อผิดพลาดดังกล่าว โดยปกติหน่วยงานที่เกี่ยวข้องกันกับการควบคุมข้อมูลเบื้องต้นจะประกอบด้วย 3 หน่วยงาน คือ

1. แผนกที่ใช้ข้อมูล (User Department)

2. ส่วนควบคุม (Control Section)

3. ส่วนจัดเตรียมข้อมูล (Input Prepartion Section)

1. แผนกที่ใช้ข้อมูล การวางระบบการควบคุมภายในแผนกนี้ควรทำดังนี้

– เหตุการณ์ทุกชนิดที่เกิดขึ้นจะต้องบันทึกลงในเอกสารเบื้องต้นทันที

– เอกสารเบื้องต้นเหล่านี้ควรจะลงรหัสไว้อย่างถูกต้องทันที

– กำหนดวิธีการควบคุมยอดรวม และนับจำนวนเอกสารเพื่อให้รู้ว่าข้อมูลแต่ละชุดมีเอกสารกี่ใบ ซึ่งวิธีดังกล่าวควรบันทึกไว้ในคู่มือการปฏิบัติงาน

– เอกสารทุกประเภทควรจะจัดส่งไปยังแผนกประมวลผลข้อมูลตามตารางเวลาที่กำหนดไว้ และควรจะทำการตรวจสอบเอกสารเหล่านี้ก่อนที่จะส่งไปยังแผนกประมวลผลข้อมูล

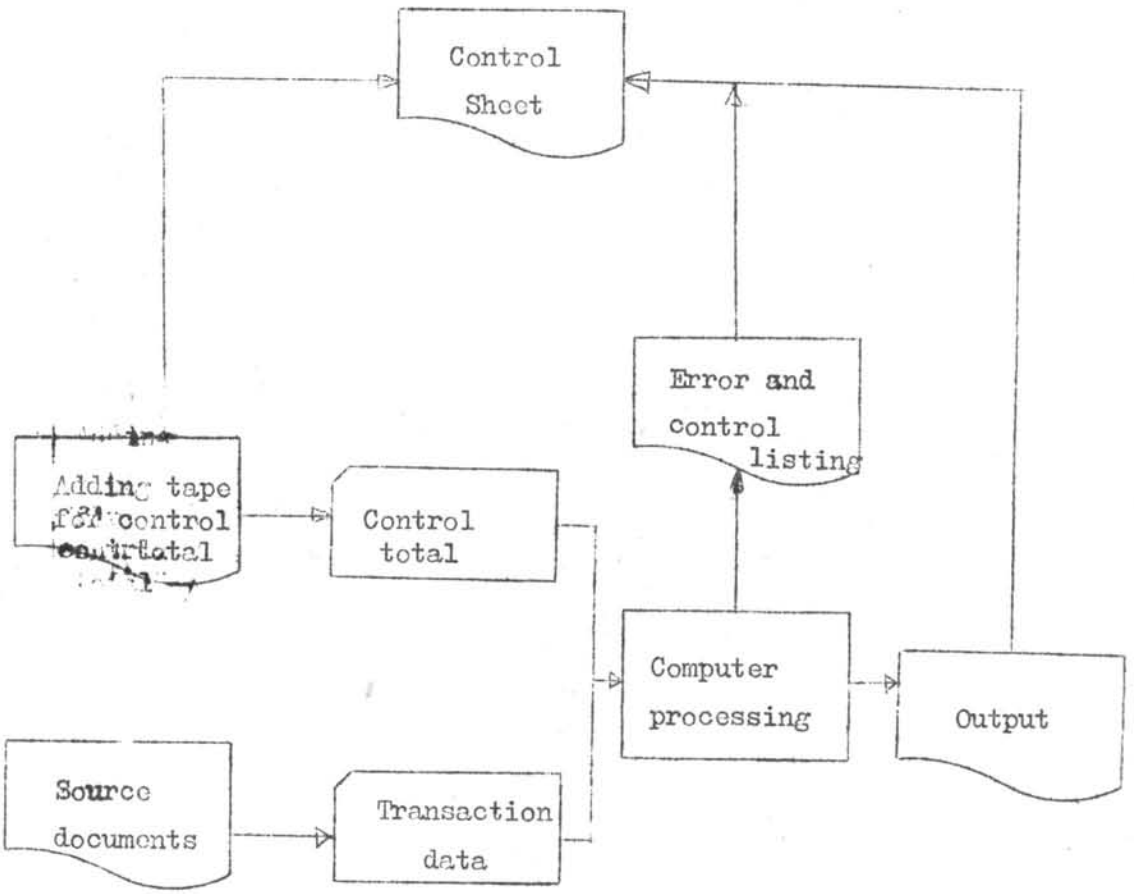
นอกจากนี้ก็ควรจะได้มีการจัดวางระบบการควบคุมข้อมูลแต่ละชุดขึ้นในแผนกที่ใช้ข้อมูล เพื่อให้แน่ใจว่าข้อมูลทั้งหมดได้ถูกนำมาประมวลผลโดยครบถ้วน แต่ถ้าการขาดความบกพร่องของเอกสารบางชนิดไม่เป็นที่เสียหายแล้ว ก็ไม่จำเป็นต้องวางวิธีการควบคุมวิธีนี้แต่อย่างใด เพราะจะทำให้เสียเวลาและค่าใช้จ่ายมากขึ้น สำหรับระบบคอมพิวเตอร์ที่ส่งข้อมูลทางที่ห่างไกลนั้น ระบบควบคุมแต่ละชุดข้อมูลนั้นจะไม่สามารถนำมาใช้ได้ ก็ควรที่จะวางระบบการควบคุมเกี่ยวกับอุปกรณ์การอ่านและการส่งข้อมูลเพื่อป้องกันมิให้ใช้อุปกรณ์ดังกล่าวโดยมิได้รับอนุมัติ และสิ่งที่ต้องระมัดระวังเป็นพิเศษคือ การป้องกันมิให้ข้อมูลบางส่วนถูกบิดเบือนหรือสูญหายในระหว่างการส่งข้อมูลโดยเครื่องมือดังกล่าว ซึ่งเป็นเรื่องทางเทคนิคเฉพาะ

สำหรับการใช้จำนวนคุมยอดหรือการควบคุมยอดรวมนั้นเป็นวิธีที่ใช้กันอย่างแพร่หลายในการทดสอบว่า ข้อมูลเบื้องต้นที่แยกเป็นหมวดหรือประเภทได้รับการประมวลผลข้อมูลครบถ้วนหรือไม่ วิธีการประกอบด้วย การรวมยอดของข้อมูลเบื้องต้นเสียครั้งหนึ่งก่อนจะนำไปประมวลผลข้อมูล จากนั้นจึงทำการรวมยอดซ้ำอีกครั้งขณะทำการประมวลผลข้อมูลเพื่อจะได้เทียบยอดว่าถูกต้องตรงกันหรือไม่ ที่ได้กล่าวมาแล้วข้างต้น ตัวอย่างได้แก่ จำนวนลูกหนี้ทั้งสิ้นได้รับการรวมยอดโดยใช้เครื่องคิดเลขครั้งหนึ่งก่อนที่จะนำไปเจาะบัตร การรวมยอดในลักษณะเดียวกันจะกระทำอีกครั้งหนึ่งเมื่อทำการประมวลข้อมูลเพื่อทดสอบว่ายอดรวมตรงกันหรือไม่ ขั้นตอนการทำงานแสดงได้ดังรูป 3.4 วิธีการคุมยอดที่นิยมใช้กันประกอบด้วย

- Financial total คือยอดรวมทางด้านการเงิน เช่น รวมยอดขาย รวมยอดมูลค่าพัสดุ เป็นต้น

- Hash total คือการรวมยอดสิ่งใดสิ่งหนึ่งเพื่อผลในการควบคุมเท่านั้น เช่น ทดสอบว่าจำนวนรวมของรายการพัสดุก่อนที่จะนำไปประมวลผลข้อมูลตรงกันกับจำนวนรวมที่ได้จากการประมวลผลข้อมูล

- Document หรือ Record count เป็นการนับจำนวนเพื่อทดสอบว่าเอกสารหรือบัตรเจาะทุกรายการถูกนำมาประมวลผลโดยครบถ้วนหรือไม่ เช่น



รูป 3.40 ขั้นตอนของวิธีกุมยอด

นับจำนวนบัตรเจาะขึ้นำมาเข้าเครื่องเปรียบเทียบกับบัตรเจาะที่เสร็จจากการประมวลผลข้อมูลแล้ว หรือจำนวนรายการที่อ่านได้จากเทปแม่เหล็กเปรียบเทียบกับจำนวนเอกสารเบื้องต้น

นอกจากนี้มีสิ่งที่ควรคำนึงถึงเพิ่มเติมในการควบคุมข้อมูลเบื้องต้น คือ

ก. ควรให้ลำดับหมายเลขของเอกสารกำกับไว้ทุกรายการ เพื่อให้สะดวกในการค้นหามาใช้ภายหลัง

ข. เอกสารที่สำคัญทุกรายการควรจะได้มีการลงชื่อกำกับโดยผู้มีอำนาจก่อนจะนำไปประมวลผล

ค. กำหนดวิธีการป้องกันการเคลื่อนย้าย แก้ไข หรือแทรกข้อมูลเบื้องต้นเข้ามาในระหว่านำไปประมวลผลโดยมิได้รับอนุมัติ ตัวอย่างดูรูป 3.41 และรูป3.42

2. ส่วนควบคุม ส่วนนี้ควรจะทำการตรวจสอบเอกสารเบื้องต้นทุกชนิดที่ได้รับจากแผนกที่ใช้ข้อมูลว่าได้รับอย่างครบถ้วน และมีการอนุมัติถูกต้องหรือไม่ นอกจากนี้การจะกระทำหน้าที่เพิ่มเติมดังนี้

ก. บันทึกการได้รับเอกสารหรือชุดข้อมูล และกำหนดวิธีควบคุมยอดรวมลงในทะเบียนควบคุม

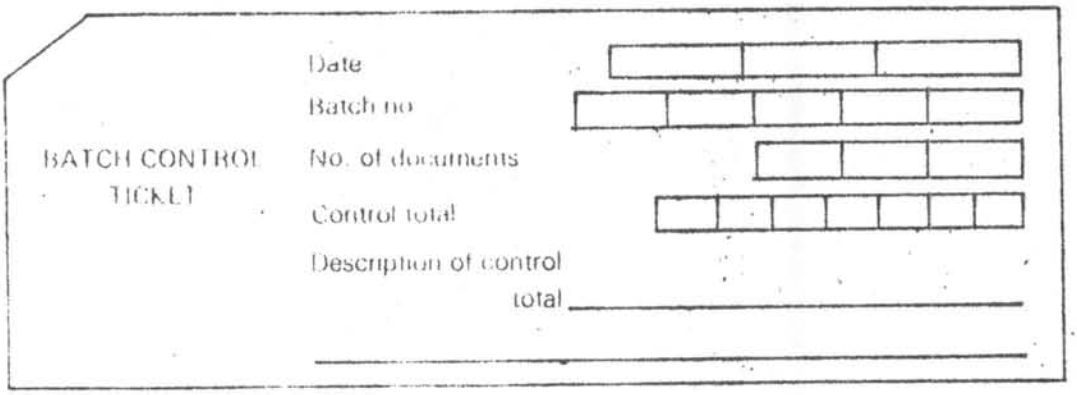
ข. ปรับปรุงแผนการดำเนินงานหรือทะเบียนบันทึกต่าง ๆ ให้ทันต่อเหตุการณ์เพื่อให้แน่ใจว่า เอกสารทุกชนิดได้รับไว้โดยถูกต้องเมื่อถึงกำหนดเวลา

นอกจากนี้วิธีการควบคุมข้อมูลเบื้องต้นยังรวมถึงการให้รหัสแก่เอกสารเบื้องต้นก่อนที่จะนำไปประมวลผล เพื่อให้แน่ใจว่า

– เอกสารเบื้องต้นได้ส่งไปถึงแผนกจัดเตรียมข้อมูล เพื่อเปลี่ยนเป็นข้อมูลที่พร้อมจะป้อนเข้าเครื่องอย่างครบถ้วน

– ข้อมูลที่พร้อมจะป้อนเข้าเครื่องได้ส่งไปยังห้องเครื่อง เพื่อประมวลผลอย่างครบถ้วน

– เอกสารที่นำไปแปลงเป็นข้อมูลที่พร้อมจะป้อนเข้าเครื่อง จะต้องเป็นเอกสารที่ผ่านการอนุมัติอย่างถูกต้องเท่านั้น



รูป 3.41 บัตรเจาะซึ่งใช้เป็นบัตรควบคุมชุดข้อมูล

Batch no.	To
Date	Form
No. of documents	Form Numbered To
Control Totals	

รูป 3.42 บัตรควบคุมชุดข้อมูล ซึ่งใช้คุมเอกสารเบื้องต้น

– เอกสารที่นำไปแบ่งเป็นข้อมูลที่พร้อมจะป้อนเข้าเครื่อง จะต้องเป็นเอกสารที่ผ่านการอนุมัติอย่างถูกต้องเท่านั้น

– ข้อมูลเบื้องต้นจะไม่นำไปประมวลผลซ้ำ

3. ส่วนจัดเตรียมข้อมูล จุดประสงค์ของการมี ส่วน จัดเตรียมข้อมูลก็เพื่อแปลงข้อมูลจากเอกสารเบื้องต้นไปเป็นข้อมูลที่พร้อมจะป้อนเข้าเครื่องให้เกิดข้อผิดพลาดน้อยที่สุด ซึ่งวิธีการควบคุมดังกล่าวนี้จะแตกต่างกันในแต่ละแบบ แต่โดยปกติแล้วจะประกอบด้วยสิ่งต่อไปนี้ คือ

ก. การแบ่งแยกหน้าที่ระหว่างการเจาะบัตรข้อมูล และการตรวจทานบัตรข้อมูล

ข. จัดให้มีการจัดเก็บเอกสารเบื้องต้นและข้อมูลเบื้องต้นอย่างระมัดระวัง

ค. กำหนดวิธีการบันทึกและตรวจสอบข้อผิดพลาดโดยให้สามารถตรวจสอบได้ภายในขั้นตอนต่าง ๆ ของการตรวจสอบ และกำหนดวิธีควบคุมการแก้ไขข้อผิดพลาดนั้น ๆ ด้วย

ง. กำหนดวิธีควบคุมของการเจาะบัตรข้อมูล และการตรวจทานบัตรข้อมูลที่ได้เจาะแล้ว

หลังจากข้อมูลเบื้องต้นพร้อมที่จะป้อนเข้าเครื่องได้แล้ว ก็ควรที่จะกำหนดวิธีการควบคุมข้อมูลเหล่านี้อีกชั้นหนึ่ง เช่น การควบคุมยอดรวมต่าง ๆ ซึ่งโดยปกติแล้วจะกระทำโดยแผนกควบคุม เพื่อที่จะให้แน่ใจว่าไม่มีชุดข้อมูลใดสูญหาย

อนึ่ง โดยปกติเครื่องคอมพิวเตอร์จะทำการประมวลผลข้อมูลโดยไม่หยุดแม้จะพบที่ผิด ทั้งนี้ เพราะการ Restart นั้นเสียเวลาและค่าใช้จ่ายมาก ถ้าใช้การประมวลผลแบบเป็นชุด ความผิดพลาดที่พบอาจจะพิมพ์แจ้งไว้ใน Console Printer หรือในเครื่องพิมพ์ที่ได้กำหนดไว้ มาตรการควบคุมการแก้ไขข้อผิดพลาดย่อมแตกต่างกันไปตามสภาพของงาน อย่างไรก็ตาม การอนุญาตให้ผู้ควบคุมเครื่องดำเนินการแก้ข้อผิดพลาดด้วยตนเองตามลำพัง แม้เป็นกรณีเล็กน้อยย่อมถือได้ว่าเป็นวิธีปฏิบัติ

ที่ไม่เหมาะตามหลักการควบคุม วิธีปฏิบัติที่นิยมกันคือ เมื่อพบข้อผิดก็จะนำมารวมกันไว้ในแฟ้มเพื่อรอการวินิจฉัย และส่งคืนไปยังผู้เตรียมข้อมูลเบื้องต้นที่เกี่ยวข้องเพื่อให้ดำเนินการแก้ไข แล้วส่งกลับเข้ามาประมวลผลข้อมูลใหม่ ควรมีระเบียบปฏิบัติที่ถนอนรัดกุมในการติดตามรายการแก้ไขข้อผิดพลาดเพื่อให้แน่ใจได้ว่าได้มีการแก้ไขข้อผิดพลาดทุกรายการโดยครบถ้วนในเวลาอันสมควร

2. การควบคุมระหว่างประมวลผล (Processing Controls) การวางระบบการควบคุมในแผนกประมวลข้อมูลนั้นแตกต่างจากระบบการควบคุมโดยทั่วไปในแผนกที่ใช้ข้อมูล เพราะวิธีการควบคุมส่วนใหญ่ในแผนกประมวลข้อมูลจะกำหนดไว้ในตัวโปรแกรมคอมพิวเตอร์ นอกจากนี้ข้อผิดพลาดบางชนิดจะตรวจพบได้ก็โดยใช้เครื่องคอมพิวเตอร์เท่านั้น ซึ่งวิธีการควบคุมในระหว่างประมวลผลจะประกอบด้วยขั้นตอนดังนี้

ก. การบรรณาธิกรณ์ (Editing)

ข. การบรรณาธิกรณ์ก่อนเข้าเครื่องคอมพิวเตอร์ (Pre-Computer Editing)

ค. กำหนดวิธีตรวจสอบในตัวโปรแกรม (Program Checks)

ง. กำหนดจุดทดสอบ (Check Points)

ก. การบรรณาธิกรณ์ วิธีการที่สำคัญที่สุดอย่างหนึ่งของการใช้ระบบคอมพิวเตอร์ก็คือ วิธีการบรรณาธิกรณ์หรือทดสอบข้อมูล วิธีบรรณาธิกรณ์คือวิธีการที่กำหนดขึ้นภายในโปรแกรมเพื่อที่จะให้มั่นใจว่าข้อมูลที่นำมาประมวลผลนั้นเป็นข้อมูลที่ถูกต้อง และเพื่อป้องกันความผิดพลาดที่อาจเกิดขึ้นจากความบกพร่องของตัวโปรแกรม ซึ่งวิธีบรรณาธิกรณ์อาจจะเป็นวิธีที่จะกระทำภายในหรือภายนอก วิธีภายในก็คือวิธีตรวจสอบที่สร้างขึ้นภายในตัวโปรแกรม ส่วนวิธีภายนอกจะกระทำโดยการเปรียบเทียบข้อมูลที่ต้องการบรรณาธิกรณ์กับแฟ้มบันทึกข้อมูลภายนอก เช่น แฟ้มข้อมูลหลักของตารางเลขที่แยกประเภททั่วไป หรือเลขที่ของแผนกต่าง ๆ เป็นต้น ซึ่งวิธีการดังกล่าวนี้สามารถจะกระทำในขั้นตอนต่าง ๆ ของการทดสอบข้อมูล ถึงแม้ว่าการกระทำดังกล่าวโดยปกติจะกระทำโดยแผนกควบคุมในระหว่างตรวจสอบข้อมูลเบื้องต้นก็ตาม แต่ก็สามารถกระทำในขั้นตอนหลังจากแปลงข้อมูลจากข้อมูลเบื้องต้น

เป็นข้อมูลที่พร้อมจะป้อนเข้าเครื่องแล้ว ซึ่งวิธีบรรณาธิกรณ์ดังกล่าวจะมีประโยชน์และช่วยลดข้อผิดพลาดที่อาจเกิดขึ้นได้คือ

– ป้องกันแฟ้มข้อมูลหลักมิให้เกิดความเสียหายโดยการรวมข้อมูลที่ไม่ถูกต้องเข้าไว้

– ลดเวลาที่จะต้องใช้ในการตรวจสอบและแก้ไขผลลัพธ์ที่ได้ในภายหลัง

– ลดเวลาที่จะต้องใช้ในการประมวลผลใหม่ ถ้าหากเกิดข้อผิดพลาดขึ้นภายหลัง

วิธีบรรณาธิกรณ์นี้เป็นหน้าที่ของแผนกควบคุมเพื่อป้องกันข้อผิดพลาดที่อาจเกิดขึ้นได้และหลังจากบรรณาธิกรณ์แล้วรายงานที่ได้รับการแก้ไขให้ถูกต้องก็จะเก็บบันทึกไว้ในอุปกรณ์บันทึกข้อมูลเพื่อที่จะนำไปประมวลผลในขั้นต่อไป

ข. <u>การบรรณาธิกรณ์ข้อมูลก่อนเข้าเครื่องคอมพิวเตอร์</u> ต้องทำดังนี้

– ตรวจนับจำนวนบัตรที่จะนำไปประมวลผล

– ตรวจสอบข้อมูลที่อยู่ในรูปของข้อมูลที่พร้อมจะนำไปเข้าเครื่องว่าถูกต้องหรือไม่

– ตรวจสอบการเรียงลำดับของบัตรข้อมูลก่อนที่จะนำไปประมวลผล

– กำหนดและทดสอบวิธีการควบคุมยอดรวมของข้อมูลเบื้องต้น

โดยปกติจะใช้อุปกรณ์ชนิดต่าง ๆ ที่สามารถทำการทดสอบข้อมูลเหล่านั้นได้

ค. <u>กำหนดวิธีตรวจสอบในตัวโปรแกรม</u> ซึ่งจะประกอบด้วยสิ่งต่อไปนี้คือ

– สร้างระบบการควบคุมยอดรวมในขณะประมวลผล โดยการเปรียบเทียบกับข้อมูลทั้งหมดที่มีอยู่ เพื่อที่จะป้องกันข้อมูลสูญหาย ตัวอย่าง เช่น รวมยอดรายการที่นำมาประมวลผล (การตรวจนับจำนวนรายการ) การควบคุมยอดรวมของข้อมูลแต่ละชนิด ยอดรวมของจำนวนหน่วยหรือจำนวนเงินในรูปแบบต่าง ๆ เป็นต้น

– สร้างวิธีควบคุมยอดรวมของข้อมูลขึ้นใหม่ในระหว่างการประมวลผล เพื่อที่จะนำไปทดสอบความถูกต้องของการประมวลผลในขั้นต่อไป

– กำหนดวิธีการทดสอบข้อมูลให้อยู่ในขอบเขตที่กำหนดไว้ เพื่อที่จะทดสอบว่า ข้อมูลที่อยู่ในระหว่างประมวลผลนั้นอยู่ในขอบเขตที่ยอมรับหรือไม่ เช่น ค่าแรงรายสัปดาห์ที่จ่ายให้แก่คนงานแต่ละคนจะต้องไม่เกินกว่า 1,000 บาท เป็นต้น รายละเอียดอื่น ๆ ที่เกี่ยวข้องได้กล่าวมาแล้วในตอนต้น

สำหรับการทดสอบยอดรวมของข้อมูลเบื้องต้นกับผลลัพธ์ที่ได้อาจจะกระทำในระหว่างประมวลผลโดยให้พิมพ์ยอดรวมออกมาทางเครื่องพิมพ์ หรือจะกระทำเมื่อเสร็จสิ้นการประมวลชุดหนึ่ง ๆ ก็ได้

ง. กำหนดจุดทดสอบ โดยปกติจุดทดสอบจะแทรกไว้ในโปรแกรมเพื่อจุดประสงค์ ดังนี้

– เป็นเครื่องชี้ให้เห็นว่าได้มีการกำหนดวิธีทดสอบความแม่นยำในแต่ละช่วงของการประมวลผล

– ถ้าเกิดข้อผิดพลาดขึ้นก็สามารถย้อนหลังกลับไปยังจุดทดสอบจุดก่อนเท่านั้นโดยไม่ต้องกลับไปตั้งต้นใหม่ทั้งหมด

นอกจากนี้การกำหนดวิธีการควบคุมยอดรวมก็อาจกระทำได้ในแต่ละช่วงของจุดทดสอบดังกล่าวได้

3. การควบคุมผลลัพธ์ (Output Controls) การวางระบบวิธีการควบคุมข้อมูลเบื้องต้นและวิธีการควบคุมข้อมูลในระหว่างประมวลผลนั้น ถ้าหากได้กระทำอย่างระมัดระวังแล้วก็จะให้ความมั่นใจได้ว่า ผลลัพธ์ที่ได้จะถูกต้อง ดังนั้น จุดที่จะเกิดข้อผิดพลาดในช่วงนี้อันควรกระทำการควบคุมอย่างระมัดระวังก็คือ วิธีการจัดส่งผลลัพธ์ไปยังบุคคลที่ได้รับอนุมัติให้เป็นผู้รับรายงานต่าง ๆ ซึ่งควรจะได้มีการบันทึกการจัดส่งเอกสารโดยทำเป็นใบปะหน้าแนบไปกับรายงานนั้น ๆ โดยเฉพาะอย่างยิ่งหากเป็นรายงานที่เป็นความลับ นอกจากนี้แล้วก็ควรจะมีการตรวจสอบผลลัพธ์ที่ได้ว่า

ถูกต้องหรือไม่ โดยปกติจะกระทำทั้งภายในแผนกประมวลข้อมูลและแผนกที่ใช้ข้อมูลเหล่านั้น ซึ่งหน่วยงานที่เกี่ยวข้องกับการควบคุมและตรวจสอบผลลัพธ์นี้จะประกอบด้วย 2 หน่วยงาน คือ

ก. ส่วนควบคุม

ข. แผนกที่ใช้ข้อมูล

ก. ส่วนควบคุม ผลลัพธ์ที่พิมพ์ออกมาจากเครื่องคอมพิวเตอร์จะส่งต่อไปยังส่วนควบคุม ซึ่งมีหน้าที่รับผิดชอบดังต่อไปนี้

– ตรวจผลลัพธ์ที่ได้ว่าถูกต้องเหมาะสมหรือไม่ เช่น ใบกำกับสินค้าได้พิมพ์ออกมาครบถ้วนถูกต้องหรือไม่ เป็นต้น

– ทำการตรวจสอบความถูกต้องของผลลัพธ์ โดยการสุ่มตัวอย่างเป็นระยะตามหลักวิชาโดยสม่ำเสมอ

– ตรวจสอบยอดรวมกับวิธีควบคุมยอดรวมที่กำหนดไว้แต่แรก

– ตรวจสอบว่าข้อข้องใจต่าง ๆ ที่ติดค้างอยู่นั้นได้รับการอธิบายจนเป็นที่พอใจแล้ว

– ตรวจสอบรายงานข้อผิดพลาดต่าง ๆ ที่จัดทำขึ้น และทำการควบคุมการแก้ไขข้อผิดพลาดนั้น ๆ

– ส่งมอบผลลัพธ์ที่เหมาะสมไปยังแผนกต่าง ๆ ที่ต้องการใช้หลังจากเสร็จสิ้นการตรวจสอบแล้ว

นอกจากนี้สิ่งที่จะต้องคำนึงถึงเป็นกรณีพิเศษที่เกี่ยวข้องกับการควบคุมผลลัพธ์ก็คือ

– การควบคุมข้อมูลที่เป็นความลับ เช่น เงินเดือน หรือรายงานผลของการดำเนินงาน เป็นต้น

– การตรวจสอบรายงานที่เกี่ยวกับข้อยกเว้นต่าง ๆ เพื่อให้แน่ใจว่า

ก. ข้อยกเว้นต่าง ๆ ทั้งหมดได้รับการพิมพ์ออกมาจากเครื่องคอมพิวเตอร์

ข. รายงานข้อยกเว้นทั้งหลายที่พิมพ์ออกมาได้จัดส่งไปยังผู้ที่เกี่ยวข้องกับข้อยกเว้นนั้น ๆ อย่างถูกต้อง

– การตรวจสอบว่าข้อผิดพลาดต่าง ๆ ที่เกิดขึ้นนั้นได้รับการแก้ไขในระยะเวลาที่เหมาะสม ตลอดจนได้กำหนดวิธีการเพื่อที่จะป้องกันข้อผิดพลาดเหล่านั้นมิให้เกิดขึ้นอีกต่อไป

– เอกสารหรือผลลัพธ์บางประเภทควรมีระเบียบควบคุมอย่างรัดกุมเป็นพิเศษ เช่น มีการลงหมายเลขลวงหน้าและมีทะเบียนคุม เช่น เช็คเปล่าที่ใช้พิมพ์รายการในบัญชีจ่ายเงินเดือน เป็นต้น

ข. แผนกที่ใช้ข้อมูล หลังจากที่ได้เสร็จสิ้นงานของส่วนควบคุมโดยได้จัดส่งผลลัพธ์ไปยังแผนกต่าง ๆ ที่เกี่ยวข้องแล้ว แผนกที่ใช้ข้อมูลก็จะทำการควบคุมและตรวจสอบข้อมูลเหล่านั้นเพื่อป้องกันข้อผิดพลาดที่อาจเกิดขึ้นได้ดังนี้

– ข้อผิดพลาดที่เกิดขึ้นจากการละเมิดระเบียบข้อบังคับที่กำหนดขึ้นภายในแผนกที่ใช้ข้อมูลเอง เช่น ยอดรวมบัญชีขายที่เกินกว่าวงเงินที่จะให้สินเชื่อเป็นต้น

– ข้อผิดพลาดที่มิได้เกิดขึ้นอันเนื่องมาจากแผนกที่ใช้ข้อมูล แต่อาจจะเป็นผลที่เกิดขึ้นในระหว่างการประมวลผล

โดยปกติถ้าหากว่าผลลัพธ์ที่ได้ไม่ตรงกับผลที่ใช้ในการควบคุมจากภายนอกควรจะถูกค้นพบโดยส่วนควบคุม แต่อย่างไรก็ตามอาจจะมีข้อผิดพลาดบางชนิดที่มิได้ถูกค้นพบ เช่น ยอดรวมย่อยภายในยอดรวมใหญ่ของรายงานบางชนิดอาจจะไม่ถูกต้อง แต่ยอดรวมใหญ่นั้นถูกต้อง นอกจากนี้ยังมีข้อมูลบางชนิดที่จะเป็นเครื่องชี้ให้เห็นถึงจุดอ่อนของระบบการควบคุมที่อยู่ภายนอกแผนกประมวลผล ตัวอย่าง เช่น ความผิดพลาดของตัวเลขด้านต้นทุน อาจจะเกิดจากความไม่มีประสิทธิภาพของการบันทึกชั่วโมงแรงงาน หรือข้อโต้แย้งที่ได้รับจากลูกค้าในการส่งใบแจ้งหนี้ ซึ่งอาจจะเป็นเพราะมีการทำงานผิดพลาดขึ้นในแผนกรับคำสั่งซื้อ เป็นต้น ดังนั้น เมื่อเหตุการณ์ดังกล่าวเกิดขึ้นก็ควรจะค้นหาสาเหตุที่เกิดข้อผิดพลาดอย่างแท้จริงเพื่อที่จะได้ทำการกำจัดสาเหตุดังกล่าวนั้นเสีย

4. การควบคุมคุณภาพของงาน (Quality Control) จุดมุ่งหมายก็เพื่อควบคุมคุณภาพของงานเพื่อให้เกิดความถูกต้องทั้งก่อนและหลังการประมวลผล ตลอดจนแก้ไขข้อผิดพลาดที่เกิดขึ้นให้มีน้อยที่สุด วิธีการควบคุมที่ควรทำประกอบไปด้วย

ก. เก็บรวบรวมรายละเอียดข้อผิดพลาดทุกอย่างที่เกิดขึ้น เช่น สาเหตุที่เกิด ชนิดของความผิดพลาดที่เกิด ปริมาณของความผิดพลาดที่เกิด ฯลฯ เป็นต้น นอกจากนี้อาจเก็บรายละเอียดทางด้านเครื่องเสีย การทำงานของผู้ควบคุมเครื่อง ตลอดจนปัญหาต่าง ๆ ที่เกิดขึ้น

ข. หน่วยงานบางแห่งอาจนำรายละเอียดเหล่านี้เก็บไว้ในแฟ้มข้อมูลเพื่อเปรียบเทียบต่อไป โดยเขียนโปรแกรมเพื่อวิเคราะห์รายละเอียดเหล่านี้จะสามารถทำให้ทราบสถิติของความผิดพลาดที่เกิดขึ้นได้ตามต้องการ

ค. จากรายงานที่ได้ออกมาทำให้นำมาปรับปรุงข้อบกพร่องในแต่ละด้านได้ ก่อนที่จะเกิดความเสียหายมากขึ้นกว่าเดิมจนเกิดความเสียหายทั้งหน่วยงานได้ เช่น จัดให้มีการฝึกอบรมผู้ควบคุมเครื่องเพิ่มขึ้นกรณีเกิดความผิดพลาดบ่อย ๆ

ง. กรณีงานในด้าน On - line การควบคุมคุณภาพมีความสำคัญเป็นอย่างมากซึ่งแฟ้มข้อมูลจะถูกแก้ไขเปลี่ยนแปลงให้ทันสมัยตลอดเวลาจากเครื่องอุปกรณ์ปลายทางจะทำให้เกิดข้อผิดพลาดได้น้อยลง ถ้ามีการควบคุมที่เหมาะสม

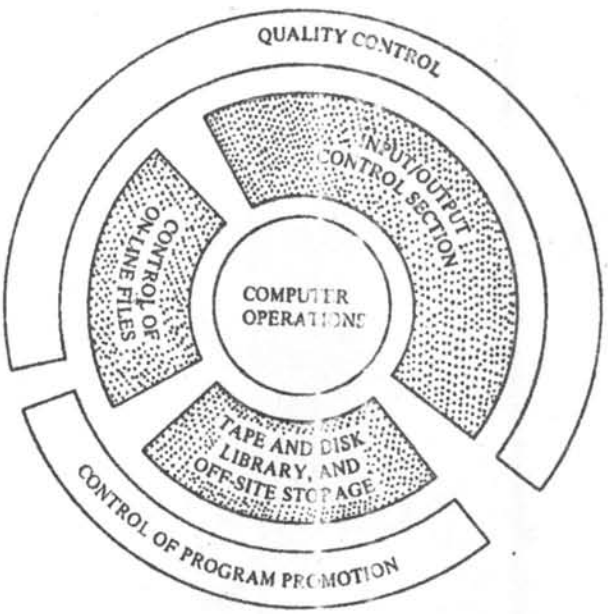
จากที่ได้กล่าวมาแล้วจะเห็นว่า การควบคุมคุณภาพนี้เป็นส่วนประกอบที่สำคัญส่วนหนึ่งของการทำงานด้วยคอมพิวเตอร์ ตามรูป 3.03

5. การควบคุมทางด้านการจัดองค์การของหน่วยงาน เป็นการควบคุมเพื่อให้แน่ใจว่ามีการแยกหน้าที่กันอย่างเหมาะสมในองค์การและในศูนย์คอมพิวเตอร์เอง ถึงแม้ว่าโครงสร้างขององค์การจะแตกต่างกันเนื่องจากสภาพแวดล้อม แต่อย่างน้อยระบบสายการบังคับบัญชาและความรับผิดชอบของผู้ปฏิบัติงานจะต้องได้รับการกำหนดโดยชัดแจ้งถึงการแบ่งแยกกันระหว่าง

ก. ผู้มีอำนาจหน้าที่ในการปฏิบัติงาน

ข. ผู้บันทึกข้อมูลของการปฏิบัติงาน

ค. ผู้เก็บรักษาทรัพย์สิน



รูป 3.43 การควบคุมการทำงานด้วยคอมพิวเตอร์

เนื่องจากการนำระบบคอมพิวเตอร์มาใช้ในการปฏิบัติงานมักก่อให้เกิด

– Centralization เหตุที่ทำให้เกิดการ Centralization ประการหนึ่งก็คือราคาของเครื่องคอมพิวเตอร์และอุปกรณ์ประกอบมักจะสูงมาก ทำให้ต้องพยายามนำงานมารวมทำกันในที่แห่งเดียวเพื่อผลในการประหยัด ประกอบกับความก้าวหน้าในระบบการสื่อสารข้อมูลทำให้การ Centralization ของข้อมูลเป็นไปอย่างสะดวก

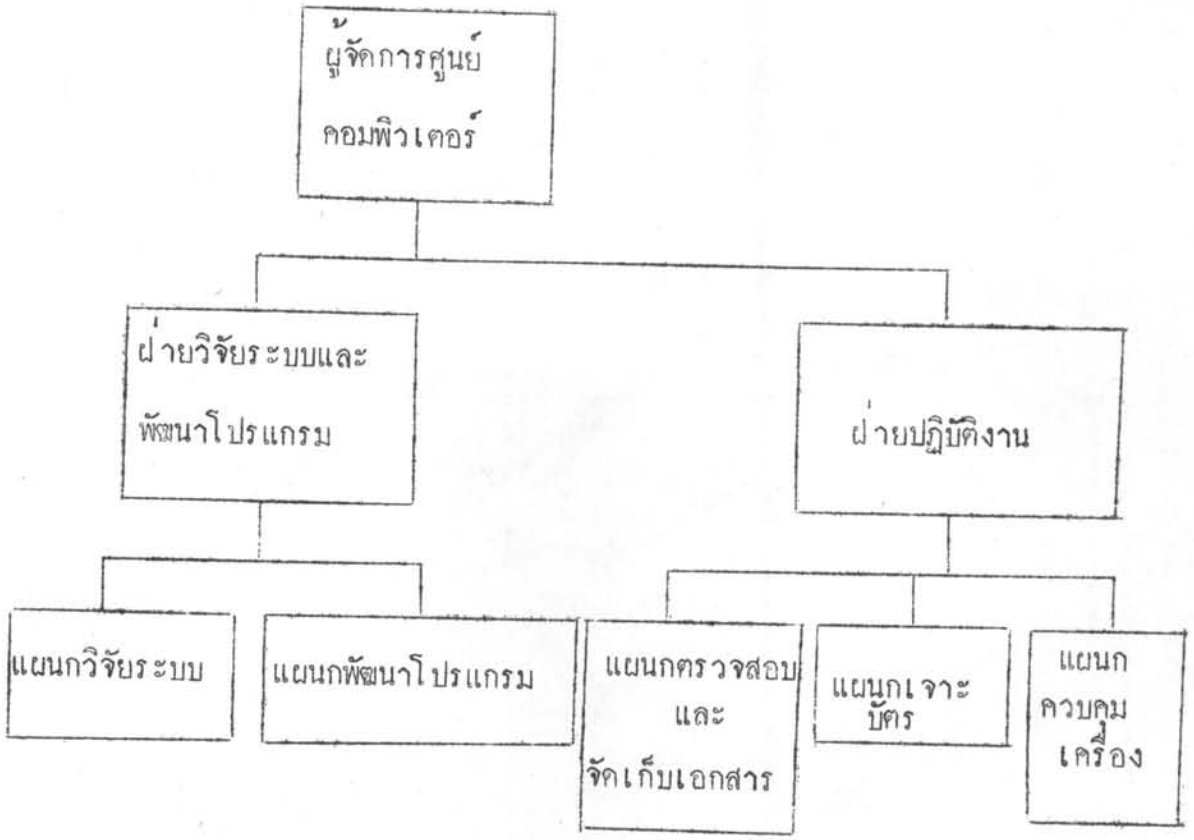
– Concentration ผลของการ Concentration ทำให้สามารถลดขั้นตอนของการทำงานไปได้มาก งานหลายอย่างอาจนำมารวมทำเป็นงานเดียว

ทั้งการ Centralization และการ Concentration บางครั้งอาจทำให้ระบบการแบ่งแยกหน้าที่และระบบสอบยันเป็นไปอย่างลำบากหรือไม่ชัดแจ้ง เมื่อพิจารณาองค์การโดยส่วนรวมจะเห็นได้ว่าหน้าที่ของศูนย์คอมพิวเตอร์ก็คือหน้าที่ในการบันทึกข้อมูลผลการปฏิบัติงาน ดังนั้น ศูนย์คอมพิวเตอร์จะต้องไม่มีส่วนร่วมในการปฏิบัติงานโดยตรง เช่น เมื่อมีหน้าที่ออกใบเก็บเงินจากลูกค้า และบันทึกการรับเงินอยู่แล้วก็ไม่ควรมีหน้าที่ในการรับชำระเงินจากลูกค้าหรือออกใบรับเงินเสียเอง นอกจากนี้ศูนย์คอมพิวเตอร์จะต้องไม่มีหน้าที่ในการควบคุมทรัพย์สินไม่ว่าโดยทางตรงหรือทางอ้อม เช่น เมื่อมีหน้าที่บันทึกรายการทรัพย์สินในคลังพัสดุก็ไม่ควรมีหน้าที่ในการควบคุมคลังวัสดุเสียเอง

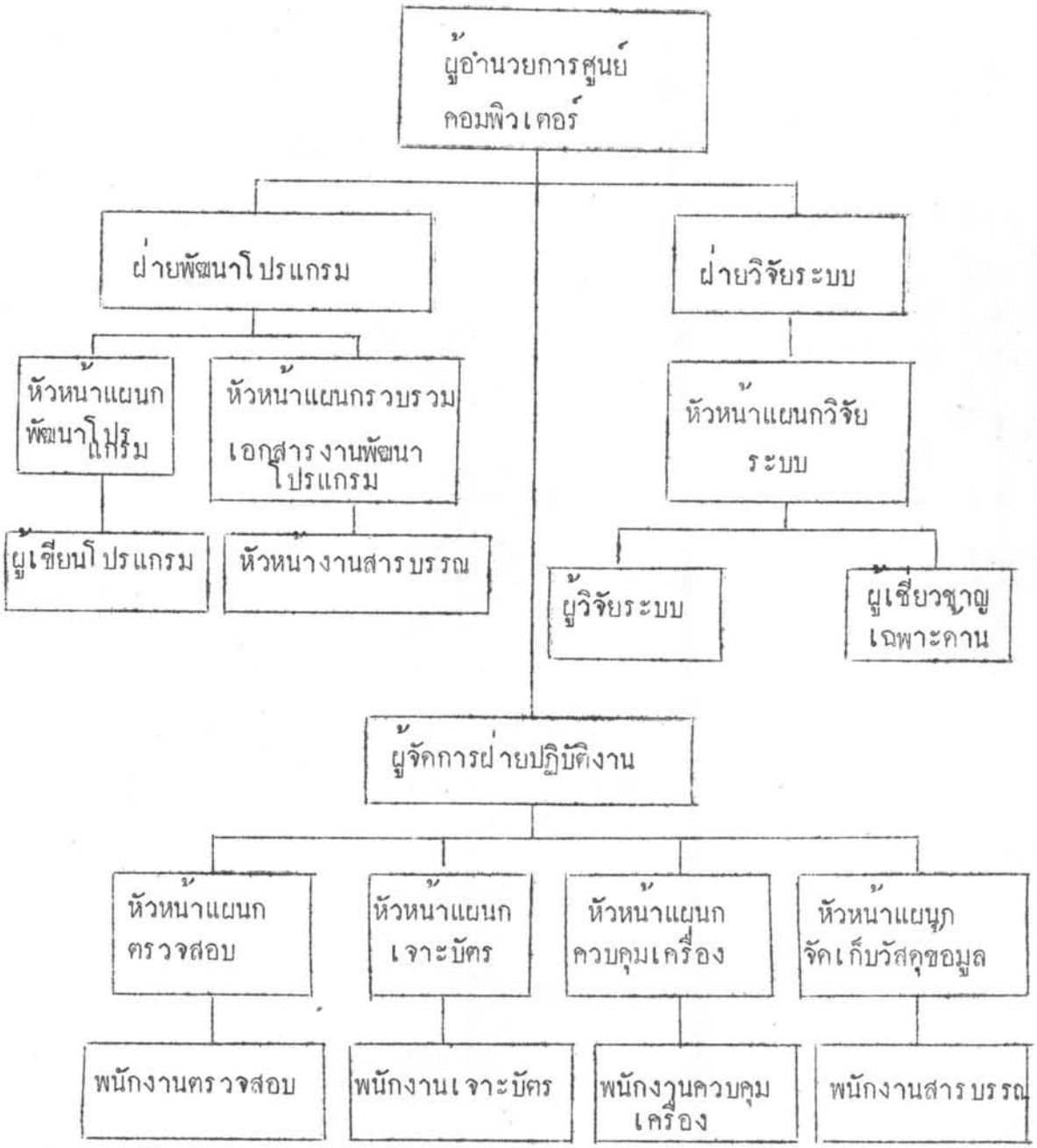
ในด้านการจัดระบบงานภายในศูนย์คอมพิวเตอร์เองนั้น เพื่อที่จะให้โครงสร้างควบคุมซึ่งกันและกัน หน้าที่เหล่านี้ควรแบ่งแยกกันโดยเด็ดขาด

– ผู้มีหน้าที่วางระบบหรือผู้เขียนโปรแกรม
– ผู้ทำหน้าที่ควบคุมเครื่อง
– ผู้ทำหน้าที่ Librarian รักษาข้อมูลและโปรแกรมที่ใช้ ตัวอย่างของการจัดหน่วยงานภายในศูนย์คอมพิวเตอร์ แสดงไดดังรูป 3.44 และรูป 3.45

เหตุผลในการกำหนดเช่นนี้ก็เพื่อที่จะ



รูป 3.44 แผนภูมิการจัดองค์การสำหรับศูนย์คอมพิวเตอร์ขนาดเล็ก



รูป 3.45 แผนภูมิการจัดองค์การสำหรับศูนย์คอมพิวเตอร์ขนาดใหญ่

– ให้มีการสอบทานมิให้ผู้ใดทำการเปลี่ยนแปลงระบบหรือขั้นตอนการทำงานตลอดจนข้อมูลเพื่อผลในการทุจริตโดยง่าย

– สามารถควบคุมมิให้ผู้ไม่มีหน้าที่เกี่ยวข้องมาดำเนินการใช้คอมพิวเตอร์

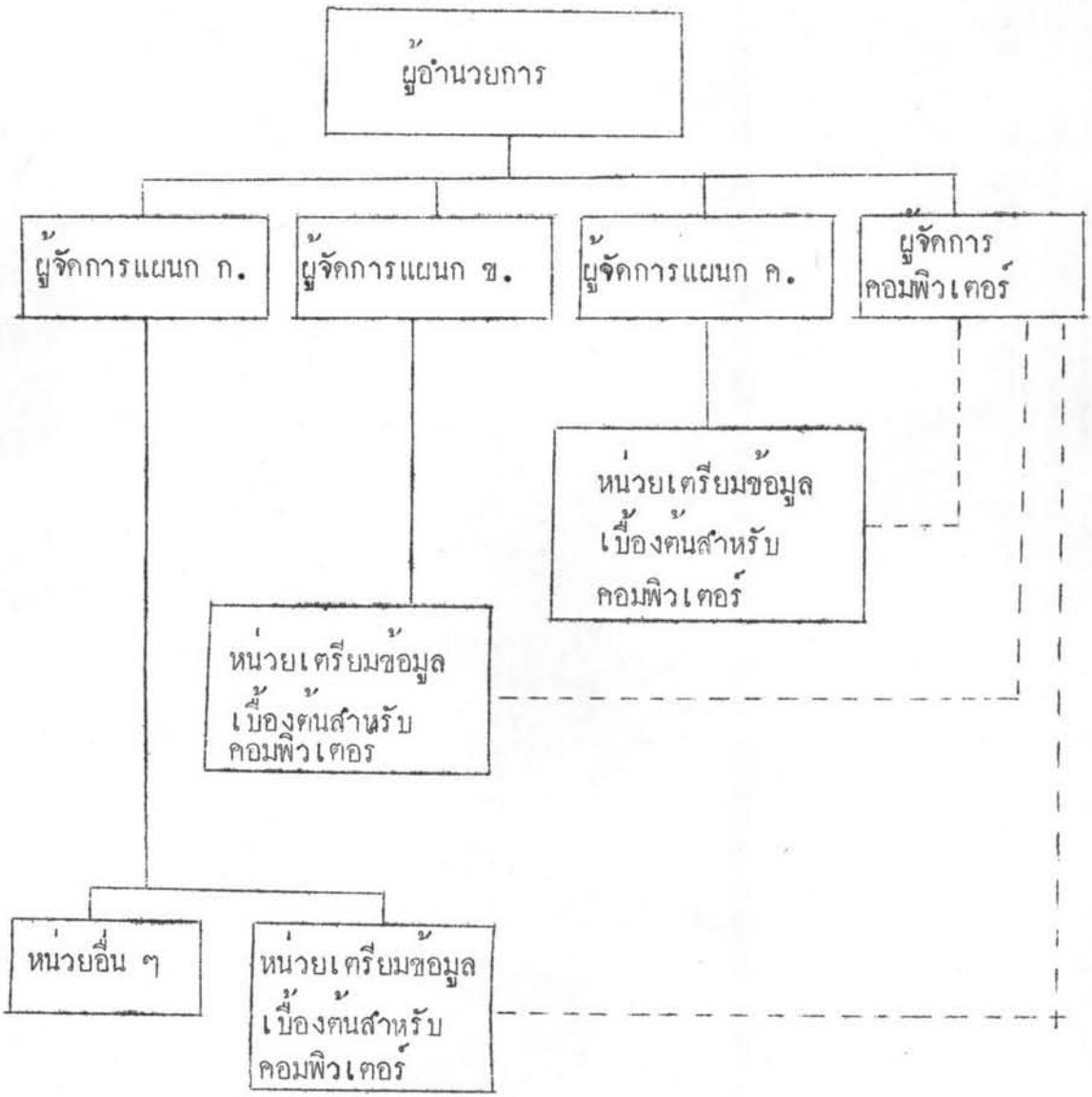
– เพิ่มพูนประสิทธิภาพในการปฏิบัติงานให้มีความชำนาญพิเศษเฉพาะด้าน ทั้งนี้เพราะสภาวะการทำงานแต่ละประเภทที่กล่าวมาแล้วแตกต่างกันอย่างมาก

โดยปกติมักนิยมจัดตั้งศูนย์คอมพิวเตอร์เป็นหน่วยงานอิสระในระดับอย่างน้อยเท่ากับหน่วยงานที่ส่งข้อมูลมาปฏิบัติ การจัดตั้งเป็นหน่วยงานอิสระเช่นนี้ ช่วยให้ศูนย์คอมพิวเตอร์มีประสิทธิภาพและอำนาจเต็มที่ในการปฏิเสธไม่ยอมประมวลผลข้อมูลที่ไม่ผ่านการตระเตรียมมาโดยถูกต้องตามระเบียบที่วางไว้ ตามรูป 3.46 นอกจากนี้บุคคลใดก็ตามที่มีหน้าที่ทั้งการประมวลผลข้อมูลและมีหน้าที่ใช้ผลที่ได้ในขณะเดียวกัน ย่อมแสดงถึงการขัดแย้งกันในหน้าที่รับผิดชอบ และไม่แน่ใจจนเกิดความสงสัยในความถูกต้องของการปฏิบัติงาน ในสหรัฐอเมริกาปัจจุบันมีเพียงหน่วยงานเล็ก ๆ เท่านั้นที่ยังยอมให้ผู้ควบคุมบัญชีเงินเดือนหรือผู้ควบคุมกลังพัสดุเป็นผู้อำนวยการศูนย์คอมพิวเตอร์ด้วยพร้อมกัน นอกจากนี้โดยปกติมักนิยมจัดตั้งคณะกรรมการประสานงานการใช้คอมพิวเตอร์โดยประกอบไปด้วยผู้อำนวยการศูนย์คอมพิวเตอร์ ผู้อำนวยการหน่วยงานที่เกี่ยวข้องในการประมวลข้อมูล ฯลฯ เป็นต้น การจัดให้มีคณะกรรมการประสานงานก็เพื่อให้มีการประชุมแลกเปลี่ยนความคิดเห็นและประสานความต้องการซึ่งกันและกัน

6. <u>การควบคุมด้านการทำเอกสารรายละเอียดประกอบ</u> โดยเหตุที่ระบบการใช้คอมพิวเตอร์ในการปฏิบัติงานมักยุ่งยากซับซ้อน ดังนั้น การทำเอกสารรายละเอียดประกอบระบบงานจึงเป็นสิ่งจำเป็นอย่างยิ่ง เอกสารรายละเอียดจะแสดงถึงการแจกแจงระบบและขั้นตอนการปฏิบัติงาน ทั้งนี้เพื่อ

– เป็นเครื่องช่วยให้ผู้บริหารเข้าใจจุดมุ่งหมาย ระบบงานหลักและการควบคุมของศูนย์คอมพิวเตอร์

– ช่วยให้ผู้มีหน้าที่วิเคราะห์ระบบงาน ผู้เขียนโปรแกรม ตลอดจนผู้ควบคุมเครื่องมีสิ่งอ้างอิงในการศึกษาวิจัยระบบงานและสามารถวางแนวการปรับปรุงงานที่ทำอยู่ในปัจจุบันโดยง่าย



รูป 3.46 ความสัมพันธ์ระหว่างหน่วยเตรียมข้อมูลเบื้องต้นสำหรับคอมพิวเตอร์ในแผนกต่าง ๆ กับศูนย์คอมพิวเตอร์

– ช่วยให้ผู้ตรวจสอบทั้งภายในภายนอกเข้าใจระบบงานที่กระทำ
– ช่วยในการวางมาตรฐานการทำงาน เป็นต้น

<u>เอกสารประกอบการวางระบบงานของศูนย์คอมพิวเตอร์</u> สิ่งสำคัญที่สุดของการควบคุมด้านการวางระบบงานก็คือ ต้องจัดให้มีการทำเอกสารรายละเอียดประกอบการวางระบบโดยครบถ้วน เอกสารที่จัดทำไว้อย่างละเอียดย่อมสามารถใช้เป็นพื้นฐานในการประเมินผลและวิจัยระบบงาน ถ้าปราศจากเอกสารประกอบและผังการทำงานแล้ว ผู้บริหารและผู้ตรวจสอบอาจไม่ทราบหรือมองข้ามจุดอ่อนที่แฝงอยู่หรือไม่อาจดัดแปลงผังงานให้เหมาะสมได้ทันตามที่ต้องการ นอกจากนี้ก็มีปรากฏอยู่เสมอที่ผู้บริหารชั้นสูงไม่เข้าใจหน้าที่ของศูนย์คอมพิวเตอร์โดยชัดแจ้งและโดยนัยกลับกันผู้ทำงานในศูนย์คอมพิวเตอร์ก็ไม่เข้าใจหรือไม่ระวังนโยบายที่ผู้บริหารชั้นสูงวางไว้ การทำเอกสารประกอบควรจะทำตั้งแต่ขั้นการศึกษาระบบ เอกสารเหล่านี้ต้องได้รับการตรวจทานและอนุมัติโดยผู้บริหารหรือหัวหน้าแผนกที่เกี่ยวข้องเพื่อตรวจทานว่าการวางระบบงานหรือการแก้ไขเป็นไปตามนโยบายที่วางไว้หรือไม่ จากที่กล่าวมานี้จะเห็นว่า หน่วยงานที่ไม่มีเอกสารประกอบย่อมแสดงถึงระบบควบคุมภายในที่อ่อนแอและการไม่เอาใจใส่ของผู้บริหารตั้งแต่เบื้องต้น ดังนั้นจุดแรกของการควบคุมทางด้านการวางระบบงานในศูนย์คอมพิวเตอร์ก็คือ ต้องมอบหมายให้มีผู้รับผิดชอบในการตระเตรียมเอกสารรายละเอียดประกอบงานเท่าที่จำเป็น เช่น จัดให้มีแผนภูมิขององค์การและรายละเอียดของขั้นตอนงานที่ทำ เป็นต้น

<u>เอกสารประกอบโปรแกรมที่ใช้</u> เช่นเดียวกับการควบคุมด้านการวางระบบงาน รายละเอียดทุกขั้นพร้อมทั้งสำเนาเอกสารประกอบควรรวบรวมเก็บเป็นแฟ้มเฉพาะโปรแกรมหนึ่ง ๆ รายละเอียดของเอกสารประกอบควรรวมถึงนโยบายการใช้โปรแกรม บุคคลใดบ้างที่มีสิทธิใช้ รายการทดสอบรายการเปลี่ยนแปลงแก้ไข และประเภทของข้อมูลที่เกี่ยวข้อง การทำเอกสารประกอบโปรแกรมโดยละเอียด นอกจากจะช่วยให้สามารถตรวจสอบโปรแกรมโดยสะดวกแล้ว ยังเป็นการง่ายที่ผู้อื่นจะรับช่วงงานต่อจากผู้เขียนโปรแกรมคนปัจจุบันถ้าหากมีความจำเป็นต้องมีการเปลี่ยนแปลง

เอกสารประกอบโปรแกรมที่ใช้ควรจะมีรายละเอียดซึ่งแสดงถึง

- จุดประสงค์ของโปรแกรม
- แผนผังการทำงานประกอบโปรแกรม
- รายละเอียดที่พิมพ์ออกมาของโปรแกรม
- คำสั่งในการปฏิบัติงาน
- เอกสารประกอบการทดสอบโปรแกรม
- ตัวอย่างของรายงานที่ได้จากโปรแกรม

เอกสารประกอบแฟ้มข้อมูลที่ใช้เช่นเดียวกับเอกสารรายละเอียดประกอบโปรแกรม เอกสารประกอบแฟ้มข้อมูลที่ใช้ควรจะแสดงถึง

- ชื่อและหมายเลขของแฟ้มข้อมูล
- ผู้มีอำนาจหน้าที่ในการใช้แฟ้มข้อมูล
- ช่วงการแก้ไขเปลี่ยนแปลงข้อมูล
- การเก็บรักษา
- ขนาดของแฟ้มข้อมูล
- ถ้าเป็นแฟ้มข้อมูลที่เป็นจานแม่เหล็ก หรือวัสดุข้อมูลประเภท Random Access อื่น ๆ ควรมีรายละเอียดของวันที่จะถ่ายทอดข้อมูลลงในวัสดุข้อมูลอื่นเช่นเดียวกับเทปแม่เหล็กเพื่อเป็นการ Back up
- ทำอย่างไรจึงจะสามารถสร้างแฟ้มข้อมูลขึ้นใหม่ในกรณีที่เกิดความเสียหาย การที่ให้วางมาตรการไว้ตั้งแต่เริ่มต้นก็เพื่อเป็นการทบทวนระบบ Back up ว่ามีจุดบกพร่องหรือไม่
- จะเก็บรักษาแฟ้มข้อมูลอย่างไร

7. <u>การควบคุมด้านการปฏิบัติงาน</u> จุดมุ่งหมายก็เพื่อตรวจสอบการปฏิบัติงานว่าสามารถเชื่อถือได้เพียงใด ในด้านความถูกต้อง และการรักษาความปลอดภัยของข้อมูลโดยเน้นถึงการทำงานทั่วไปของศูนย์คอมพิวเตอร์ เครื่องมือเบื้องต้นที่ใช้ก็คือการจัดทำคู่มือมาตรฐานการปฏิบัติงาน ซึ่งจะรวมคำอธิบายถึงระเบียบ

ปฏิบัติในการดำเนินงานประจำวันโดยละเอียด มาตรฐานการทำงาน มาตรฐานในการใช้เครื่องมือประกอบ ซึ่งจะต้องใช้อุปกรณ์อะไรบาง จะต้องใช้อุปกรณ์อะไรบาง จะต้องใช้ข้อมูลอะไรบ้างในการทำงาน เมื่องานเสร็จแล้วจะแจกจ่ายผลงานอย่างไร และจะปฏิบัติอย่างไรเมื่อมีข้อขัดข้องจากการปฏิบัติงานตามปกติ การควบคุมด้านการปฏิบัติงานต้องทำหลายด้าน ดังนี้

ก. ควบคุมการเปลี่ยนแปลงโปรแกรมที่ใช้

ข. ควบคุมแฟ้มข้อมูล

ค. ควบคุมรักษาความปลอดภัยของข้อมูลและโปรแกรมที่ใช้

ง. ควบคุมการเข้าสู่สถานที่ตั้งเครื่องคอมพิวเตอร์

จ. ควบคุมการใช้ การแก้ไขระหว่างการปฏิบัติงาน (Console Intervention)

ก. <u>ควบคุมการเปลี่ยนแปลงโปรแกรมที่ใช้</u> ผลของความเจริญเติบโตขององค์การย่อมทำให้ต้องปรับปรุงโปรแกรมที่ใช้ให้เหมาะสมกับสถานการณ์อยู่เสมอ ข้อสำคัญคือต้องวางระเบียบปฏิบัติ (Procedure) ให้รัดกุมเพื่อป้องกันการเปลี่ยนแปลงโปรแกรมเพื่อผลในการทุจริต มีระเบียบปฏิบัติหลายประการที่ควรนำมาใช้ เช่น

1. ต้องเขียนอธิบายความมุ่งหมายในการเปลี่ยนแปลงโดยชัดเจน และต้องได้รับอนุมัติในหลักการจากผู้รับผิดชอบ การเปลี่ยนแปลงหลักต้องได้รับความเห็นชอบจากผู้ออกแบบระบบ และคณะกรรมการเสียก่อน การเปลี่ยนแปลงย่อยอาจต้องการเพียงความเห็นชอบจากผู้จัดการศูนย์และหน่วยงานผู้ใช้ที่เกี่ยวข้องเท่านั้น การเขียนคำอธิบายความมุ่งหมายของการเปลี่ยนแปลงเป็นลายลักษณ์อักษรจะช่วยป้องกันการเข้าใจผิดและเป็นการแสดงถึงประวัติของโปรแกรมด้วย

2. การทำการเปลี่ยนแปลงแก้ไขควรอยู่ในความรับผิดชอบของผู้วิเคราะห์ระบบและผู้เตรียมโปรแกรมเท่านั้น ผู้มีหน้าที่ทางด้านควบคุมเครื่องไม่ควรเกี่ยวข้องโดยเด็ดขาด การแบ่งแยกเช่นนี้ก็เพื่อป้องกันมิให้ผู้ควบคุมเครื่องรู้รายละเอียดของโปรแกรมแล้วใช้การแก้ไขระหว่างการทำงานของเครื่องเพื่อทุจริต อนึ่ง บางแห่ง

ยินยอมให้ผู้ควบคุมเครื่องมีอำนาจในการแก้ไขโปรแกรมเล็ก ๆ น้อย ๆ ได้เอง การอนุญาตเช่นนั้นยากแก่การควบคุมให้อยู่ในขอบเขตและก่อให้เกิดปัญหาในการรักษาเอกสารรายละเอียดให้ทันสมัยอยู่เสมอ

3. นอกจากจะต้องทำรายละเอียดการเปลี่ยนแปลงแล้ว โปรแกรมที่เปลี่ยนแปลงแก้ไขจะต้องได้รับการทดสอบโดยหน่วยงานอิสระไม่เกี่ยวข้องกับหน่วยงานที่ทำการเปลี่ยนแปลง การควบคุมให้มีการทดสอบโปรแกรมอย่างเหมาะสมเป็นช่วงงานที่สำคัญยิ่งในการพัฒนาระบบงาน การทดสอบโปรแกรมควรจะประกอบด้วยขั้นตอนดังต่อไปนี้

– มาตรการที่จะใช้ในการทดสอบจะต้องกำหนดโดยชัดแจ้งและควรจะง่ายต่อการเข้าใจ

– นอกจากทดสอบโปรแกรมกับข้อมูลที่ใช้เป็นปกติแล้ว การทดสอบข้อมูลควรรวมถึงข้อมูลที่ออกแบบพิเศษสำหรับทดสอบว่าระบบควบคุมความถูกต้องและมีปฏิกิริยาตอบสนองต่อข้อมูลที่ผิดปกติอย่างไร เช่น ปฏิกิริยาที่มีต่อข้อมูลที่ไม่สมบูรณ์และข้อมูลที่ผ่านการปฏิบัติขั้นตอน เป็นต้น

– จำนวนข้อมูลที่นำมาทดสอบควรจะมีจำนวนมากพอสมควร โดยปกติการทดสอบควรจะทำร่วมกับโปรแกรมอื่นเป็นชุดจนสุดสิ้นขบวนการของการทำงานเป็นการจำลองภาวะการปฏิบัติงานจริง ๆ การประเมินผลต้องรวมถึงอิทธิพลของการเปลี่ยนแปลงที่มีต่อแต่ละขั้นตอนของการทำงานด้วย

– ในขั้นสุดท้ายการทดสอบควรจะกระทำกับการปฏิบัติงานจริง ๆ และควรจะกระทำโดยมีให้ผู้เตรียมโปรแกรมมีส่วนร่วมเพื่อทดสอบว่าสามารถนำมาใช้โดยอิสระปราศจากการช่วยเหลือของผู้เตรียมโปรแกรม หรือไม่

4. หลังจากเสร็จสิ้นการเปลี่ยนแปลงและการทดสอบแล้วจะต้องบันทึกรายการในทะเบียนคุมการเปลี่ยนแปลง ควรจะมีการวางระเบียบโดยเคร่งครัดให้ผู้ควบคุมเครื่องจะใช้แต่โปรแกรมที่ผ่านขั้นตอนการสร้างและการเปลี่ยนแปลงโดยถูกต้องครบถ้วนเท่านั้น

REQUEST FOR PROGRAM CHANGE

To Date

Description of service being requested

Date desired

Requested by	Name	Title	Phone
	Dept.		

Space below for data-processing use only

Program name Program No.

Change approved by Date

Estimated starting date	Documentation	By	Date
Estimated completion date	1. Source deck corrected 2. New program listing 3. New program tested 4. Results approved 5. Flow charts corrected 6. Other manuals changed 7. Operating instr. changed 8. Old listing destroyed 9. Old object deck destroved 10. Accepted by librarian		
Assigned to:			
Program change No.			
___ Patched ___ Recompiled			
Released to operations_____ By	Distribution: Original to Data Processing Decond copy returned to department by Data Processing Third copy retained by department for follow-up		
Department notified_____ By			
Effective date of change			

รูป 3.47 แบบฟอร์มการขอเปลี่ยนแปลงแก้ไขโปรแกรม

5. เอกสารที่เกี่ยวกับการเปลี่ยนแปลงทั้งหมดต้องเก็บรักษารวมไว้ในแฟ้มเอกสารประกอบโปรแกรม

นอกจากนี้ เพื่อให้การปฏิบัติงานเป็นมาตรฐานเดียวกันสิ่งที่ควรจัดทำคือคู่มือเกี่ยวกับโปรแกรมซึ่งแสดงถึงนโยบาย ระเบียบขั้นตอนการปฏิบัติงานและเทคนิคที่ใช้เป็นมาตรฐาน การจัดทำคู่มือจะช่วยประสานความร่วมมือระหว่างหน่วยงานต่าง ๆ ที่ใช้โปรแกรม และช่วยป้องกันการทำงานซ้ำซ้อนหรือการขัดแย้งอีกด้วย นอกจากนี้อาจจะเพิ่มรายละเอียดเฉพาะบางอย่าง สำหรับงานบางอย่าง เช่น ด้านบัญชี องค์การบางแห่งอาจวางนโยบายที่จะเลื่อนการแก้ไขเล็ก ๆ น้อย ๆ ไว้จนสิ้นสุดรอบบัญชีหนึ่ง ๆ ทั้งนี้ เพื่อให้วิธีการประมวลผลข้อมูลเป็นไปโดยคงที่สม่ำเสมอตลอดรอบปีบัญชี เป็นต้น

ดังได้กล่าวมาแล้วว่า ทุกหน่วยงานจะต้องมีการแก้ไขเปลี่ยนแปลงโปรแกรมในภายหลัง ซึ่งแบบฟอร์มของการอนุมัติการแก้ไขเปลี่ยนแปลงโปรแกรมควรจะมีข้อความที่สำคัญ ๆ ดังนี้ ตัวอย่างของแบบฟอร์ม แสดงได้ดังรูป 3.47

ก. วันที่ของการเปลี่ยนแปลง

ข. เหตุผลของการเปลี่ยนแปลง

ค. การอนุมัติการเปลี่ยนแปลงเบื้องต้น

ง. การอนุมัติวิธีการเปลี่ยนแปลง ฯลฯ เป็นต้น

แบบฟอร์มในการบันทึกการเปลี่ยนแ. โปรแกรมนี้ควรจะเก็บรวบรวมไว้เพื่อที่จะปรับปรุงให้เอกสารที่เกี่ยวข้องทันสมัยอยู่ เ อ เพราะจะทำให้ไม่ต้องแก้ไขเอกสารต่าง ๆ ตลอดจนผังทางเดินของงานใหม่ทั้งหมด เนื่องจากการเขียนโปรแกรมหรือผังทางเดินของงานในแต่ละครั้งนั้นจะสิ้นเปลืองเวลามาก นอกจากนี้ยังเป็นการป้องกันมิให้มีการแก้ไขเปลี่ยนแปลงโปรแกรมโดยมิได้ผ่านการอนุมัติโดยถูกต้องอีกด้วย การป้องกันการแก้ไขโปรแกรมนั้นกระทำได้โดยการเก็บโปรแกรมไว้ในสถานที่เก็บอย่างเหมาะสม โดยที่การนำโปรแกรมไปใช้แต่ละครั้งจะต้องทำการบันทึกลงในสมุดทะเบียนซึ่งจะบันทึกเวลาที่นำไปใช้และเวลาที่นำกลับเข้ามาเก็บ นอกจากนี้ยังอาจกระทำได้

โดยนำสำเนาโปรแกรมไปเก็บไว้ในที่ปลอดภัยอีกแห่งหนึ่งและจะนำสำเนาโปรแกรมไปเปรียบเทียบกับโปรแกรมที่ใช้อยู่จริงเป็นครั้งคราวโดยมิให้รู้ตัว เพื่อที่จะตรวจสอบดูว่ามีการเปลี่ยนแปลงที่มิได้รับการอนุมัติเกิดขึ้นหรือไม่

ข. ควบคุมแฟ้มข้อมูล นั้นปกติจะกระทำในขณะปรับปรุงแฟ้มข้อมูลเพื่อให้ทันเวลา หรืออาจเรียกว่าการดูแลรักษาแฟ้มข้อมูลซึ่งกระทำเช่นเดียวกับวิธีการควบคุมในขณะประมวลผล โดยอาจแบ่งวิธีการควบคุมออกเป็น 2 ประเภท คือ

1. การดูแลรักษาข้อมูลหลัก
2. การดูแลรักษาข้อมูลย่อย

1. การดูแลรักษาข้อมูลหลัก การวางระบบควบคุมเกี่ยวกับการแก้ไขข้อมูลหลักในแฟ้มข้อมูลหลักไว้แล้ว ก็เพื่อที่จะให้แน่ใจว่าไม่มีการเปลี่ยนแปลงข้อมูลต่าง ๆ ในแฟ้มดังกล่าวโดยมิได้รับการอนุมัติ เพราะข้อมูลหลักนั้นเป็นข้อมูลที่ใช้สำหรับอ้างอิงอันมีผลกระทบกระเทือนต่อข้อมูลที่บันทึกอยู่ในแฟ้มข้อมูลทั้งหมด ถ้าหากมีการเปลี่ยนแปลง เช่น ราคาขายของสินค้า หรืออัตราค่าแรง เป็นต้น ซึ่งการควบคุมประกอบด้วยวิธีดังต่อไปนี้ คือ

– ให้พิมพ์ข้อมูลที่บันทึกไว้ออกมาเป็นระยะ ๆ เพื่อที่จะตรวจสอบกับข้อมูลที่จัดเตรียมด้วยมือ

– กำหนดวิธีการควบคุมยอดรวมต่างหาก เพื่อที่จะทำการทดสอบเป็นระยะ ๆ กับยอดรวมสะสมต่าง ๆ ในแฟ้มข้อมูลที่เกี่ยวข้อง

– กำหนดวิธีการเพื่อทดสอบยอดรวม ในโปรแกรมคอมพิวเตอร์ที่เกี่ยวข้อง เป็นต้น

2. การดูแลรักษาข้อมูลย่อย ความสำคัญของการควบคุมข้อมูลย่อยประเภทต่าง ๆ จะขึ้นอยู่กับความสำคัญของรายการนั้น ๆ เพราะข้อมูลย่อยเป็นข้อมูลเฉพาะตัวไม่เกี่ยวเนื่องหรือกระทบกระเทือนต่อข้อมูลอื่น ๆ ดังเช่นข้อมูลหลัก เช่น การดูแลรักษาแฟ้มข้อมูลของบัญชีแยกประเภทค่าขาย หรือบัญชีแยกประเภทสินค้าคงเหลือ

ย่อมมีความสำคัญทางด้านบัญชีแฟ้มข้อมูลเกี่ยวกับการวิเคราะห์การขาย เป็นต้น และมากกว่า
โดยปกติจะใช้วิธีการควบคุมยอดรวมเพื่อควบคุมยอดรวมของบัญชีต่าง ๆ ที่อยู่ในแฟ้มข้อมูลเหล่านั้น ซึ่งวิธีการควบคุมก็กระทำเช่นเดียวกับการดูแลรักษาข้อมูลหลัก เช่น ทำการตรวจสอบตัวเลขยอดรวมของบัญชีคุมยอด กับยอดรวมของข้อมูลต่าง ๆ ที่อยู่ในแฟ้มข้อมูลที่เกี่ยวข้องว่าตรงกันหรือไม่ นอกจากการควบคุมยอดรวมดังกล่าวแล้ว ก็อาจทำการทดสอบยอดรวมแต่ละรายการซึ่งจะใช้วิธีนี้หรือไม่นั้นก็ขึ้นอยู่กับขอบเขตของการควบคุมที่กระทำในระหว่างการประมวลผลว่ามีมากน้อยเพียงใด โดยที่การควบคุมและการทดสอบยอดรวมของแต่ละรายการจะกระทำด้วยวิธีการทดสอบที่ใช้กันอยู่เดิม เช่น การเปรียบเทียบยอดของเจ้าหนี้แต่ละรายกับใบแจ้งหนี้ หรือการเปรียบเทียบยอดของสินค้าคงเหลือกับยอดของสินค้าที่ตรวจนับได้ เป็นต้น นอกจากนี้ก็ควรกำหนดวิธีควบคุมในขณะที่ประมวลผลการแก้ไขปรับปรุงแฟ้มข้อมูล เพื่อให้เกิดความถูกต้องแม่นยำดังต่อไปนี้

– ตรวจสอบการเรียงลำดับของรายการที่บันทึกในแฟ้มข้อมูล

– นับจำนวนรายการที่บันทึกไว้ เช่น จำนวนของคนงานจากแฟ้มการจ่ายค่าแรง

– ทดสอบยอดรวมเฉพาะอย่างของข้อมูลบางประเภท เช่น การเรียงลำดับเลขที่ของลูกค้าแต่ละกลุ่ม เป็นต้น

– ทดสอบยอดรวมที่เป็นจำนวนเงินหรือจำนวนหน่วย เช่น ยอดรวมของบัญชีขายที่เป็นจำนวนเงิน หรือรายการของสินค้าคงเหลือเป็นจำนวนหน่วย เป็นต้น

การทดสอบยอดรวมต่าง ๆ ดังกล่าวควรจะให้พิมพ์ผลที่ได้ออกมาด้วย หลังจากที่ประมวลผลครั้งหนึ่ง ๆ เพื่อให้แผนกควบคุมทำการกระทบยอด และสำเนาของผลลัพธ์ที่พิมพ์ออกมานี้อาจจะส่งไปยังแผนกที่ใช้ข้อมูลเพื่อที่จะตรวจสอบกับยอดรวมที่บันทึกไว้ของแผนกนั้น ๆ เช่น ยอดรวมของบัญชีขายควรจะตรงยอดรวมของบัญชีคุมยอดในแผนกบัญชี เป็นต้น

ค. <u>ควบคุมรักษาความปลอดภัยของข้อมูลและโปรแกรมที่ใช้</u> เพื่อจุดประสงค์ดังนี้ คือ

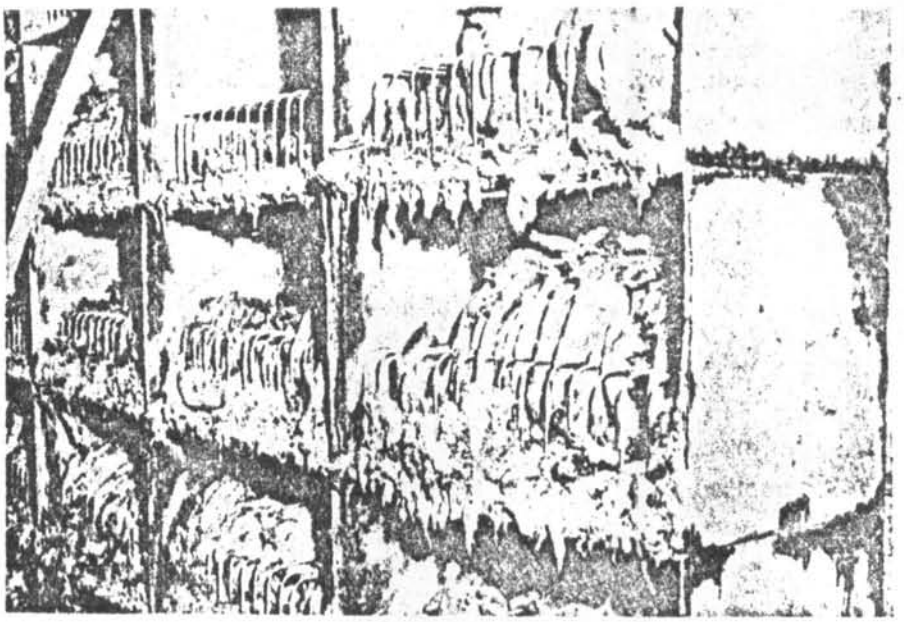
1. เพื่อป้องกันมิให้มีการแก้ไขโดยมิได้รับอนุมัติ

2. เพื่อมิให้แฟ้มข้อมูลและโปรแกรมได้รับความเสียหายจากอัคคีภัย หรือจากสิ่งรบกวนอื่น ๆ เช่น จากสนามแม่เหล็ก เป็นต้น

การควบคุมรักษาความปลอดภัยของข้อมูลและโปรแกรมที่ใช้ควรพิจารณาดังนี้

– ภัยสำคัญของข้อมูลตลอดจนโปรแกรมที่ใช้ก็คืออัคคีภัย มีรายละเอียดที่น่าสนใจในประการหนึ่งเกี่ยวกับม้วนเทปแม่เหล็ก กล่าวคือ ตามปกตินำจะไม่เป็นอันตรายต่อข้อมูลที่บรรจุในเทป ถ้าไม่ทำให้ม้วนเทปเปียกน้ำหรือเก็บไว้ในที่ชื้น เป็นเวลานานจนเกิดออกไซด์ ม้วนเทปแม่เหล็กที่เก็บไว้ในตู้เก็บจะสามารถทนอุณหภูมิสูงถึง 250 องศาฟาเรนไฮท์ในเวลานานพอสมควร โดยไม่เกิดการเสื่อมเสียไป แม้อุณหภูมิจะสูงถึง 300 องศาฟาเรนไฮท์ก็ยังคงนำมาเข้าเครื่องอ่านได้ อย่างไรก็ตาม มีข้อน่าสังเกตว่า ถ้านำทั้งความร้อนและความชื้นมารวมกันก็จะเป็นอันตรายอย่างยิ่ง ตามรูป 3.48 ม้วนเทปแม่เหล็กอาจจะสูญเสียข้อมูลที่บรรจุอยู่ถ้านำมาเก็บไว้ในที่ซึ่งมีอุณหภูมิสูงเพียง 130 องศาฟาเรนไฮท์ แต่ความชื้น 85 % (ซึ่งเป็นสภาวะที่มักเกิดในตัวถังรถยนต์ซึ่งปิดทึบไว้ในวันที่มีอากาศร้อน) มีศูนย์คอมพิวเตอร์หลายแห่งติดตั้งอุปกรณ์ป้องกันอัคคีภัยชนิดที่จะพ่นละอองน้ำออกมาดับไฟโดยอัตโนมัติในทันทีที่อุณหภูมิถึงขีดที่ตั้งไว้ เช่น เมื่ออุณหภูมิสูง 165 องศาฟาเรนไฮท์ ผลคืออาจทำให้ข้อมูลที่บรรจุในเทปแม่เหล็กถูกทำลายโดยง่าย ดังนั้น จึงจำเป็นที่จะต้องดูแลระบบป้องกันอัคคีภัยโดยละเอียด เพราะบางระบบนั้นนอกจากจะทำงานไม่ได้ผลแล้วยังเป็นอันตรายต่อตัวเครื่องคอมพิวเตอร์และข้อมูลที่เก็บรักษาไว้เสียยิ่งกว่าตัวอัคคีภัยเอง

วิธีลดความเสี่ยงภัยจากการสูญเสียข้อมูลที่ปฏิบัติทั่วไปคือ การจัดให้มีระบบ Back up สำหรับโปรแกรมและแฟ้มข้อมูลที่พิจารณาว่ามีความสำคัญโดยนำไปเก็บรักษาแยกจากจุดที่ตั้งศูนย์คอมพิวเตอร์หรือที่เรียกว่าระ Off – Site Storage ทั้งนี้ก็เพื่อให้มีข้อมูลเหลือพอที่จะสร้างข้อมูลใหม่ได้ในกรณีที่เกิดอัคคีภัย ณ จุดใดจุดหนึ่ง



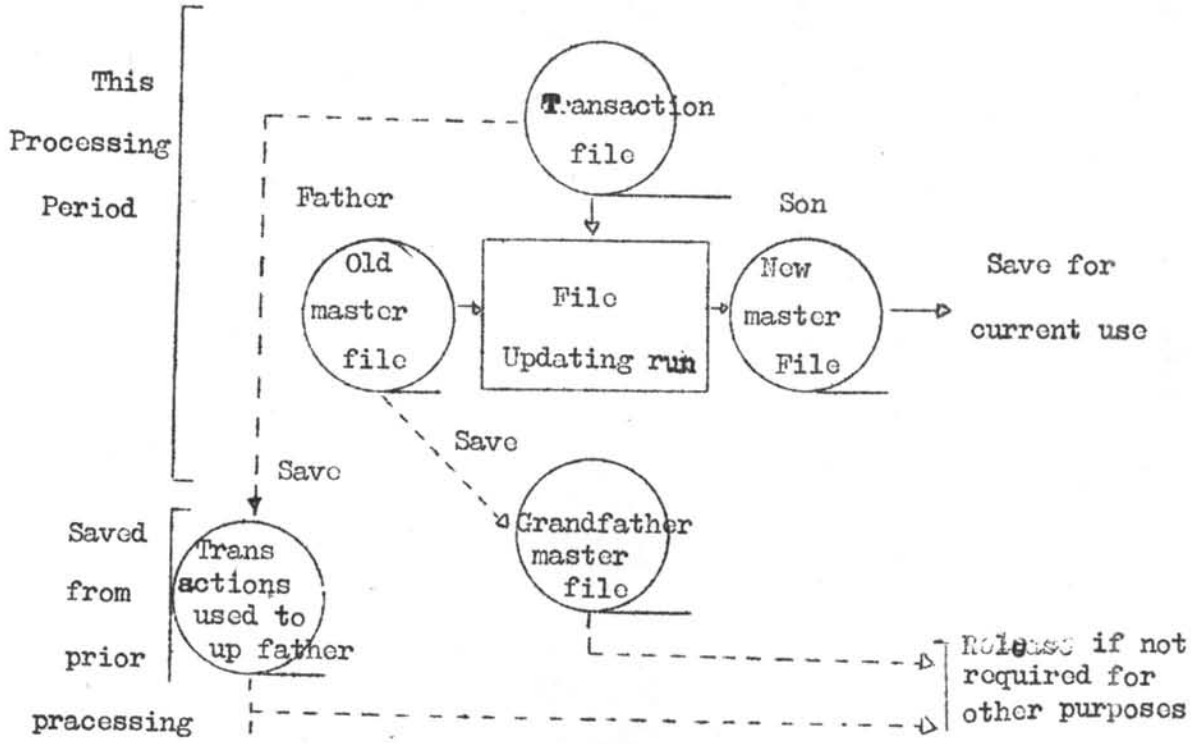
รูป 3.48 สภาพแม่เหล็กที่ถูกทำลายโดยความร้อนและน้ำ

ข้อสำคัญที่ต้องระวังคือจะต้องแยกออกโดยชัดแจ้งว่า ข้อมูลใดบ้างมีความสำคัญต้องรับการเก็บรักษาเป็นพิเศษ มีศูนย์คอมพิวเตอร์เป็นจำนวนมากที่เก็บรักษา ข้อมูลประเภทหนึ่งเป็นอย่างดี แต่ไม่สนใจข้อมูลอีกประเภทหนึ่งที่มีความสำคัญพอกัน ตัวอย่างการBack up ดังรูป3.49

– วิธีลดความเสี่ยงภัยจากการสูญเสียข้อมูลที่ปฏิบัติทั่วไปคือ การจัดให้มีระบบ Back up สำหรับโปรแกรมและแฟ้มข้อมูลที่พิจารณาว่ามีความสำคัญ โดยนำไปเก็บรักษาแยกจากจุดที่ตั้งศูนย์คอมพิวเตอร์หรือที่เรียกว่าระบบOff – Site ;

ทั้งนี้ก็เพื่อให้มีข้อมูลเหลือพอที่จะสร้างข้อมูลใหม่ได้ในกรณีที่เกิดอัคคีภัย ณ จุดใดจุดหนึ่ง ข้อสำคัญที่ต้องระวังคือจะต้องแยกออกโดยชัดแจ้งว่าข้อมูลใดบ้างมีความสำคัญต้องรับการเก็บรักษาเป็นพิเศษ มีศูนย์คอมพิวเตอร์เป็นจำนวนมากที่เก็บรักษาข้อมูลประเภทหนึ่งเป็นอย่างดี แต่ไม่สนใจข้อมูลอีกประเภทที่มีความสำคัญพอกัน

– แฟ้มข้อมูลอาจถูกทำลายได้โดยอำนาจของสนามแม่เหล็ก ตามลักษณะของแท่งแม่เหล็ก ตามรูป 3.50 ซึ่งเป็นการยากที่จะตรวจบุคคลที่ผ่านเข้าไปยังศูนย์คอมพิวเตอร์ว่าใดมีแท่งแม่เหล็กซุกซ่อนโดยเจตนาหรือไม่เจตนาก็ตาม วิธีป้องกันง่าย ๆ ที่ใช้กันอยู่ทั่วไปก็คือ การควบคุมเก็บรักษาม้วนเทปแม่เหล็กและวัสดุข้อมูลอื่น ๆ อย่างเข้มงวดกวดขัน อย่างน้อยที่สุดจะต้องมีบุคคลที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบ เช่น เจ้าหน้าที่ดูแลแฟ้มข้อมูลอยู่ดูแลประจำตลอดเวลาที่นำเทปและวัสดุข้อมูลออกมาใช้ มีหลายแห่งที่มีผู้รับผิดชอบแต่เพียงในนามหรือดูแลเฉพาะตอนนำออกใช้เท่านั้น เคยมีผู้เข้าชมศูนย์คอมพิวเตอร์ของบริษัทประกันภัยแห่งหนึ่งได้แอบหยิบม้วนเทปที่วางทิ้งกระจัดกระจายทั่วห้องกลับบ้านเพื่อเป็นที่ระลึกกว่าที่บริษัทจะสำรวจพบและทำการสอบสวนติดตามคืนได้ก็ต้องเสียค่าใช้จ่ายและเวลาอย่างมากมาย ตัวอย่างที่เกิดขึ้นอีกอย่างได้แก่ ในปี ค.ศ. 1970 บริษัทใน Cleveland มลรัฐโอไฮโอได้ไล่พนักงานผู้หนึ่งออกจากงาน ในตอนบ่ายหลังจากที่ทุกคนในบริษัทออกไปรับประทานอาหาร พนักงานผู้นั้นได้แอบเข้าไปในห้องเก็บม้วนเทปแม่เหล็กและทำลายข้อมูลสำคัญจนหมดสิ้นด้วยแท่งแม่เหล็กขนาดเล็กที่ซ่อนในอุ้งมือ ในชั่วเวลาไม่กี่นาทีเทปสำคัญ ๆ ได้ถูกลบจนหมด บริษัทต้องจ้างผู้เชี่ยวชาญพิเศษมาทำการสร้างข้อมูลทดแทน ทั้งนี้ต้องใช้เวลา



รูป 3.49 ระบบการ Back up

Magnet	Approximate Magnetic Field (gauss)	
	At Pole Edges	At Stated Distance
1. Flashlight magnet (5/8" X 1-1/2"; 16 ga.)	800	45 @ 1/2 inch
2. Small dipole disc (1/4 oz) (1/2" dia. X1/4")	800	15 @ 1/2 inch
3. Small horseshoe (2 oz) (1-1/2" X1"X5/16")	1100	10 @ 1 inch
4. Small rod (1/4 oz) (1/4"X1-1/4")	800	290 @ 1/8 inch
5. Rod (1-3/4 oz) (1/2"X2")	850	390 @ 1/16 inch 90 @ 1/2 inch
6. Ferrite ring (8 oz) (4" dia., X3/8", 1-1/2" conter hole	1000	100 @ 3/8 inch 95 @ 1 inch
7. Large U magnet (4 oz) (1"X3/8"X1")	2000	1900 @ 1/8 inch 280 @ 1/2 inch
8. Magnetron magnet (6 lb) (6-3/4" X3-7/8", 1-1/2" air gap)	3000	1800 @ 1/8 inch 680 @ 1/2 inch 420 @ 1/4 inch

รูป 3.50 สนามแม่เหล็กของแท่งแม่เหล็กขนาดต่าง ๆ กัน (ซึ่งโดยทั่วไปสนามแม่เหล็กมีค่า 400-500 gauss ก็ทำให้แผ่นแม่เหล็กดูดกันได้)

ใช้เงินจำนวนมหาศาลและเกือบจะต้องเลิกล้มกิจการ ต้องไม่ลืมว่าข้อมูลบางประเภทนั้นไม่อาจสร้างขึ้นมาทดแทนได้เลย

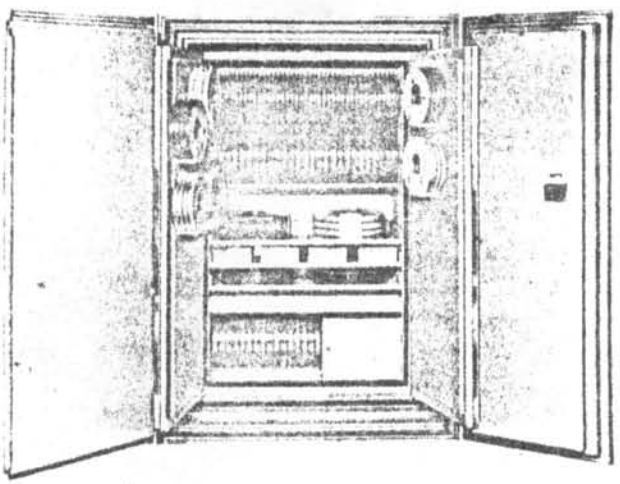
– ห้องเก็บเทปแม่เหล็กและวัสดุข้อมูลอื่น ๆ ควรจัดให้เป็นสัดส่วนดังรูป 3.51 รูป 3.52 มีเจ้าหน้าที่ดูแลแฟ้มข้อมูลควบคุม มีการทำบันทึกรายการต่าง ๆ ที่เกิดขึ้นบนเทปลงรายละเอียด เช่น รายละเอียดการยืม การส่งคืนและบุคคลที่เกี่ยวข้อง การผ่านเข้าออกยังห้องเก็บข้อมูลนี้ต้องมีการควบคุมอย่างเคร่งครัด ทุกคนที่จะเข้าไปยังห้องนี้แม้แต่พนักงานทำความสะอาดต้องได้รับอนุญาตทุกครั้ง ในกรณีพิเศษใด ๆ ถ้าบุคคลอื่นที่นอกเหนือจากเจ้าหน้าที่ดูแลแฟ้มข้อมูลได้รับอนุญาตให้เข้าไปในห้องเก็บเทปแม่เหล็กจะต้องแน่ใจว่าผู้เข้าไปไม่ได้นำวัตถุที่มีคุณสมบัติทางแม่เหล็กติดตัวไปด้วยไม่ว่าจะโดยเจตนาหรือไม่เจตนาก็ตามและต้องได้รับการดูแลอย่างใกล้ชิดตลอดเวลาที่อยู่ในห้องนั้น

– ในต่างประเทศปัจจุบันระบบการรักษาความลับของข้อมูลในคอมพิวเตอร์กำลังได้รับความสนใจพัฒนาอย่างเร่งรีบเพราะการจารกรรมความลับได้เพิ่มจำนวนอย่างมากมาย การนำเอาระบบโทรคมนาคม , On – Line System, Time – Sharing และ Remote Terminal มาใช้อย่างกว้างขวางทำให้ต้องพิจารณาปัญหาในด้านรักษาความลับของข้อมูลเป็นพิเศษ ข้อมูลใด ๆ ที่ส่งไปตามสายย่อมง่ายต่อการจารกรรมโดยบุคคลภายนอก ได้มีการทำระบบส่งข้อมูลเป็นรหัสตามที่ได้กล่าวมาแล้วข้างต้นเพื่อให้การจารกรรมข้อมูลเป็นไปอย่างลำบากขึ้น แต่ทั้งนี้ก็ต้องเสียค่าใช้จ่ายสูงมาก ซึ่งระบบรักษาความปลอดภัยที่ใช้กันทั่วไปส่วนมากใช้ระบบคำไขรหัส หรือเลขรหัสคำผ่านเพราะง่ายต่อการใช้และเสียค่าใช้จ่ายไม่แพง อย่างไรก็ตาม การใช้ระบบดังกล่าวคำไขรหัส และเลขรหัสคำผ่าน อาจรั่วไหลได้ง่าย ดังนั้นจึงควรเปลี่ยนแปลงรหัสที่ใช้อยู่เสมอในช่วงเวลาที่เหมาะสม

– มีหน่วยงานหลายแห่งที่มีระบบรักษาความลับอย่างซับซ้อน แต่ไม่ได้วางวิธีปฏิบัติในการรักษาความลับขั้นพื้นฐาน เช่น ระเบียบการปฏิบัติในการเก็บเอกสารเบื้องต้นที่บรรจุข้อมูลซึ่งเป็นความลับ หรือระเบียบวิธีการทำลายกระดาษคาร์บอน

– ข้อควรระวังอีกอย่างหนึ่งก็คือไม่ว่าระบบรักษาความปลอดภัยจะวางไว้อย่างรัดกุมเพียงใดก็ตาม พนักงานที่ขาดความรับผิดชอบอาจละเลยไม่ปฏิบัติตาม

รูป 3.51 ห้องเก็บเทปแม่เหล็ก

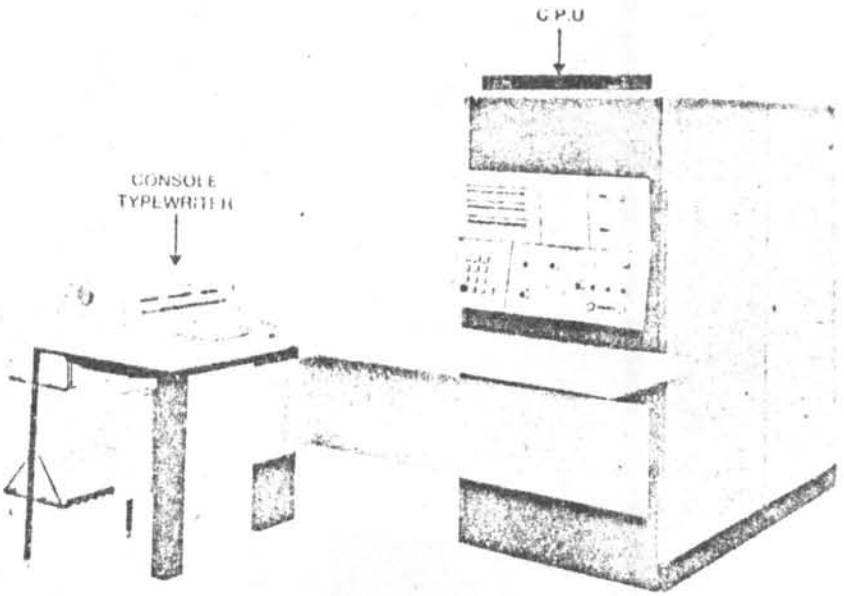


รูป 3.52 ตู้เก็บเทปแม่แหล็ก

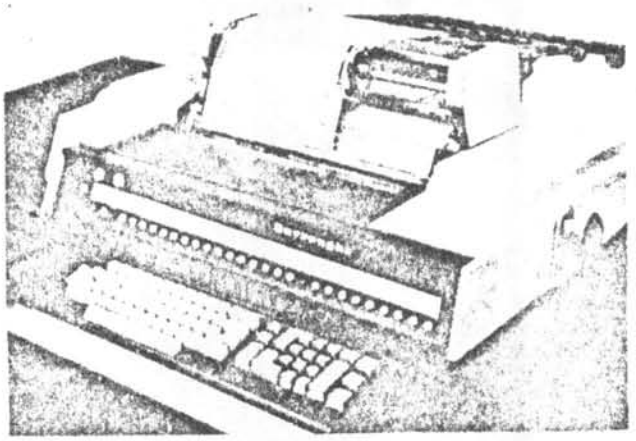
ดังนั้น จึงควรที่จะคัดเลือกพนักงานที่จะปฏิบัติงานในศูนย์คอมพิวเตอร์อย่างถี่ถ้วน พนักงานทุกคนควรได้รับการฝึกให้ปฏิบัติตามกฎเกณฑ์ที่วางไว้จนเป็นนิสัย และต้องจัดให้มีการตรวจตราเป็นระยะเพื่อให้แน่ใจว่าระเบียบที่วางไว้ได้รับการยึดถือปฏิบัติอย่างสม่ำเสมอ บุคคลโดยทั่วไปมักมีแนวโน้มที่ไม่สนใจเครื่องมือหรือระเบียบรักษาความปลอดภัยใด ๆ ที่พิจารณาเห็นว่าเข้มงวดแต่ไม่มีประโยชน์ต่อตนโดยตรง

ง. <u>การควบคุมการเข้าไปในสถานที่ตั้งเครื่องคอมพิวเตอร์</u> ถ้าไม่ควบคุมโดยใกล้ชิดย่อมเปิดโอกาสให้สามารถทำการเปลี่ยนแปลงข้อมูลและโปรแกรมเพื่อผลในการทุจริตได้ง่าย ในศูนย์คอมพิวเตอร์ที่มีการควบคุมอย่างเคร่งครัดนั้น เจ้าหน้าที่ที่ทำงานในศูนย์ ฯ ได้รับการกำหนดให้ติดเครื่องหมายที่มีสีต่าง ๆ กัน และกำหนดว่าผู้ติดเครื่องหมายสีหนึ่ง ๆ จะอยู่ในเขตใดของศูนย์ ฯ ได้บ้าง ทั้งนี้เพื่อป้องกันการทุจริต หรือการก้าวก่ายหน้าที่ เช่น ป้องกันมิให้ผู้เตรียมโปรแกรมมาดำเนินการใช้เครื่องคอมพิวเตอร์เสียเอง ถ้าเป็นไปได้ควรวางระเบียบให้ใช้ระบบ Buddy Systems กล่าวคือ กำหนดไว้ว่าห้ามมิให้ผู้ใดอยู่ในศูนย์คอมพิวเตอร์ในช่วงเวลาใดเวลาหนึ่งเพียงคนเดียว รายละเอียดอื่น ๆ ที่เกี่ยวข้องการควบคุมการเข้าไปในสถานที่ตั้งเครื่องคอมพิวเตอร์ได้กล่าวมาแล้วตอนต้น

จ. <u>การควบคุมการใช้วิธีการแก้ไขระหว่างการทำงานของเครื่องบนปุ่มที่อยู่บนแผนหน้าปัทม์ของเครื่องคอมพิวเตอร์</u> ตามรูป 3.53 ซึ่งผู้ควบคุมเครื่องสามารถที่จะหยุดการปฏิบัติงาน ปกติของเครื่องคอมพิวเตอร์ชั่วคราวแล้วใช้ระบบควบคุมการทำงานจากภายนอกโดยผ่านคอนโซล ดังนั้น จึงเป็นไปได้ที่ผู้ควบคุมเครื่องสามารถละเว้นมิให้เครื่องคอมพิวเตอร์ทำงานตามโปรแกรมในบางโอกาส ด้วยเหตุนี้จึงจำเป็นต้องแบ่งแยกหน้าที่กันโดยเด็ดขาด ระหว่างผู้ควบคุมเครื่องและผู้เตรียมโปรแกรม ผู้ควบคุมเครื่องไม่ควรมีส่วนทราบโปรแกรมที่เขียนเป็นภาษาชั้นสูง เช่น ฟอร์แทรน, โคบอล, พีแอล/วัน , และอาร์พีจี เป็นต้น ถ้าจำเป็นควรให้ทราบเฉพาะโปรแกรมภาษาเครื่องเท่านั้น ดังนั้น ข้อมูลที่นำเข้าเครื่องก็เช่นกัน ผู้ควบคุมเครื่องไม่ควรมีส่วนในการเตรียมข้อมูลที่จะนำเข้าเครื่องและไม่ควรทราบข้อมูลในรูปของข้อมูลเบื้องต้น เช่น ถ้าข้อมูลเบื้องต้นเป็นบัตรเจาะก็ไม่ควรพิมพ์ข้อความหรือตัวเลขไว้ตอนส่วนบน



รูป 3.53 ลักษณะการพิมพ์ข้อมูลออกทางคอนโซล



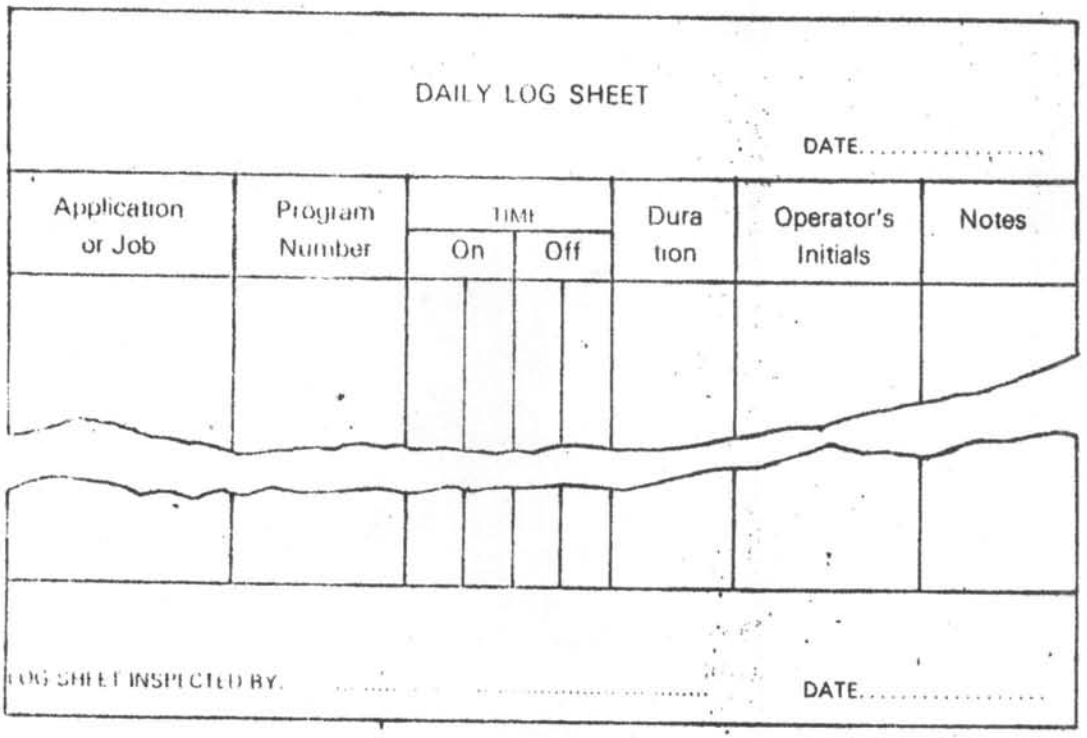
ของบัตร ทั้งนี้ก็เพื่อป้องกันมิให้ผู้ควบคุมเครื่องรู้รายละเอียดของโปรแกรมและข้อมูลที่ใช้แล้วโดยใช้วิธีการแก้ไขระหว่างการทำงานของเครื่องคอมพิวเตอร์ เพื่อผลในการทุจริต ซึ่งการควบคุมมิให้มีการแก้ไขระหว่างการทำงาน เครื่องคอมพิวเตอร์โดยไม่จำเป็นหรือทำโดยไม่ได้รับมอบหมายจากผู้มีอำนาจรับผิดชอบ วิธีที่ใช้กันก็คือ

– เครื่องพิมพ์ที่คอนโซลควรจะพิมพ์รายการการแก้ไขระหว่างการทำงานของเครื่องคอมพิวเตอร์ที่เกิดขึ้นทุกรายการ เช่น รายการผิดพลาด และ Restart เป็นต้น

– ตามปกติเครื่องพิมพ์ที่คอนโซลควรจะพิมพ์เวลากำกับไว้ด้วยทุกครั้ง ดังนั้นจึงรู้ได้ว่าในระยะเวลาใดเครื่องได้ทำอะไรบ้าง ถ้าใช้ความสังเกตผู้ตรวจสอบก็อาจทราบได้ว่าช่วงเวลาที่เครื่องทำงานสำหรับรายการหนึ่ง ๆ เป็นไปตามปกติหรือไม่ ถ้านานผิดปกติก็อาจเป็นไปได้ว่ามีสิ่งผิดปกติเกิดขึ้น การแก้ไขระหว่างการทำงานของเครื่องโดยใช้คนนำนั้นมักช้า ดังนั้น จึงทำให้เวลาที่ใช้เครื่องคอมพิวเตอร์นานเกินควร

– การบันทึกรายการที่เกิดขึ้น ตามรูป 3.54 ซึ่งมีประโยชน์ในการป้องกันการทุจริตดังกล่าวมาแล้ว ยังช่วยป้องกันการรั่วไหลในการใช้เครื่องด้วย ซึ่งในสหรัฐอเมริกามีการตรวจพบว่าพนักงานของหน่วยงานที่เกี่ยวข้องจำนวนมากได้แอบใช้เครื่องคอมพิวเตอร์ทำงานให้เอกชนเพื่อหารายได้พิเศษ

– กระดาษที่ใช้กับเครื่องพิมพ์ที่คอนโซลนี้ควรจะมีหมายเลขลำดับล่วงหน้ากำกับและได้รับการตรวจจากผู้มีหน้าที่รับผิดชอบในเวลาที่เหมาะสม สำหรับรายการประเภทที่สำคัญนั้นอาจจัดให้เครื่องพิมพ์ประจำคอนโซลอยู่แยกออกไปจากห้องคอมพิวเตอร์ เช่น จัดไว้ในห้องปิดกุญแจ ถ้าไม่อาจทำได้อย่างน้อยกระดาษพิมพ์คอนโซลควรเป็นกระดาษแบบสองตอนคือส่วนที่เป็นกระดาษธรรมดาและกระดาษคาร์บอน การจัดให้กระดาษคาร์บอนแยกไปเข้าที่เก็บล็อคในเครื่องทันทีที่เสร็จสิ้นการพิมพ์เป็นวิธีป้องกันง่าย ๆ วิธีหนึ่งที่แทบจะไม่ต้องเสียค่าใช้จ่ายเพิ่มขึ้นเลย



รูป 3.54 แบบฟอร์มการบันทึกรายการที่เกิดขึ้นในแต่ละวัน

โดยทั่วไปนั้นผู้เขียนโปรแกรมจะเป็นผู้กำหนดเกี่ยวกับลำดับขั้นของการใช้เครื่องคอมพิวเตอร์ในการประมวลผลครั้งหนึ่ง ๆ ซึ่งลำดับขั้นต่าง ๆ ที่กำหนดขึ้นนั้นจะประกอบด้วยสิ่งต่อไปนี้

ก. อุปกรณ์บันทึกข้อมูลเบื้องต้น

ข. อุปกรณ์บันทึกข้อมูลอื่น ๆ

ค. วิธีปฏิบัติเกี่ยวกับตัวโปรแกรม และการปฏิบัติในกรณีที่เครื่องหยุดโดยไม่ทราบล่วงหน้า

ง. กำหนดวิธีปฏิบัติก่อนที่จะถึงจุดทดสอบในตัวโปรแกรม

จ. ประมาณระยะเวลาที่จะใช้ในการประมวลผลตามปกติครั้งหนึ่ง ๆ

เอกสารที่จัดทำขึ้นดังกล่าวข้างต้นนี้จะเป็นเครื่องช่วยทั้งในด้านการเดินเครื่องคอมพิวเตอร์ และการจัดเตรียมในบันทึกเวลาการใช้เครื่อง โดยที่ในบันทึกเวลานี้จะเก็บรักษาไว้โดยผู้ควบคุมเครื่องเพื่อที่จะให้หัวหน้าฝ่ายควบคุมเครื่องได้ใช้ในการเปรียบเทียบเวลาที่ใช้จริงกับเวลาที่ใช้ในครั้งก่อน ๆ และเวลาที่ประมาณไว้ ซึ่งในบันทึกเวลาประจำวันนี้จะช่วยให้ฝ่ายจัดการหรือผู้บริหารได้ทราบถึงประสิทธิภาพในการทำงานของแผนกดังกล่าว เพื่อที่จะหาทางแก้ไขและในเดียวกันก็เป็นมาตรการในการควบคุมการใช้เครื่องคอมพิวเตอร์ด้วย เช่น

– ทำให้ทราบถึงเวลาที่ใช้ไปในงานที่สูญเปล่า เช่น การเริ่มต้นใหม่หรือเวลาที่ใช้ไปในการทดสอบ เป็นต้น

– ทำให้ทราบถึงการใช้เครื่องที่มิได้ผ่านการอนุมัติ

– ทำให้ทราบถึงผลประโยชน์ที่ได้รับจากการใช้เครื่องนอกเวลาโดยหน่วยงานหรือบุคคลอื่น หากว่ามีการใช้เครื่องในกรณีดังกล่าว

8. <u>การควบคุมในกรณีที่ใช้บริการคอมพิวเตอร์ภายนอก</u> ตามปกติถ้าระบบคอมพิวเตอร์เกิดขัดข้องหรือมีงานที่จะปฏิบัติมากเกินกำลังของเครื่อง ในทางปฏิบัติ มักนิยมเลื่อนรายการปฏิบัติข้อมูลงานที่ไม่สำคัญออกไปก่อนมากกว่าที่จะนำงาน

ไปปฏิบัติกับเครื่องคอมพิวเตอร์ภายนอกทั้งนี้เพราะยากลำบากในการควบคุมป้องกันการสูญหายของข้อมูล อย่างไรก็ตาม ถ้ามีความจำเป็นไม่อาจหลีกเลี่ยงได้ก็ควรพิจารณาใช้ระบบควบคุมเช่นเดียวกับหน่วยงานที่ไม่มีเครื่องคอมพิวเตอร์เป็นของตนเองจำเป็นต้องใช้บริการคอมพิวเตอร์จากหน่วยงานอื่น ระบบควบคุมเหล่านี้ ได้แก่

– มีการกำหนดขอบเขตความรับผิดชอบระหว่างทั้งสองฝ่ายโดยแน่ชัดว่าใครจะเป็นผู้รับผิดชอบในกรณีเกิดความสูญเสียหรือสูญหายของข้อมูลโดยประการต่าง ๆ

– ศึกษาระบบคอมพิวเตอร์ของศูนย์ภายนอกอย่างถี่ถ้วนว่าอาจใช้ระบบร่วมกันได้หรือไม่ ต้องดัดแปลงแก้ไขอะไรบ้าง

– ถ้าระบบที่จะใช้ผิดไปจากที่เคยจะต้องมีการตรวจสอบรายการของการเปลี่ยนแปลงแฟ้มข้อมูลอย่างถี่ถ้วน

– ควบคุมระบบการส่งข้อมูลอย่างใกล้ชิดเพื่อป้องกันการสูญหายหรือมีการแก้ไขโดยไม่ได้รับอนุญาต บางหน่วยงานอาจจะมีการบันทึกข้อมูลที่ส่งไปปฏิบัติภายนอกในไมโครฟิล์มเสียชั้นหนึ่งก่อนเพื่อเป็นการ Back up

– วางแผนปฏิบัติข้อมูลผิดปกติที่เครื่องคอมพิวเตอร์ไม่ยอมรับอย่างรัดกุมเพื่อแน่ใจว่ารายการผิดพลาดทุกรายการได้รับการแก้ไขและนำไปประมวลผลใหม่อีกครั้งทันตามกำหนดการ

– ควบคุมระบบการแจกจ่ายผลลัพธ์อย่างเคร่งครัดเพื่อแน่ใจได้ว่าได้ผลลัพธ์ทั้งสิ้นจากศูนย์คอมพิวเตอร์ภายนอกโดยครบถ้วน ไม่มีผลลัพธ์ตกค้างหรือรั่วไหล

– ทดสอบผลของการปฏิบัติข้อมูลโดยตรวจสอบอีกครั้งหนึ่ง

– ตรวจสอบระบบควบคุมที่วางไว้ในโปรแกรมว่าทำงานได้ผลหรือไม่ บางครั้งระบบที่วางไว้จะทำงานอย่างได้ผลในระบบหนึ่งแต่ทำงานไม่เต็มที่ในระบบซึ่งต่างกันออกไป

– ตรวจตราระบบ Back up เป็นพิเศษเพราะผู้ใช้ไม่อาจควบคุมระบบรักษาความปลอดภัยได้เต็มที่เมื่อส่งงานไปปฏิบัติภายนอก

3.3.4 การตรวจสอบเพื่อประเมินผลงาน โดยมีผู้ตรวจสอบที่เรียกว่า ผู้ตรวจสอบภายใน (Internal auditors) เป็นผู้ดำเนินงาน และทำเฉพาะในหน่วยงานประมวลผลข้อมูล ผู้ตรวจสอบที่มีเหล่านี้ต้องเป็นผู้มีประสบการณ์ในงานประเภทนี้อย่างดี เพราะเทคนิคที่ใช้ในการตรวจสอบบางอย่างจะเรียนรู้ได้จากประสบการณ์เท่านั้น และจากประสบการณ์ทำให้เขาประเมินผลงานได้อย่างรวดเร็ว ซึ่งย่อมจะดีกว่าตรวจตามเทคนิคที่ใช้หรือตรวจตามข้อทดสอบที่ใช้ ผู้ตรวจสอบประกอบด้วยผู้เชี่ยวชาญทางด้านเทคนิคด้านลักษณะการป้องกันภายนอกเครื่อง ฯลฯ ตลอดจนรูปถึงด้านจิตวิทยาของคนทำงาน กลุ่มผู้ตรวจสอบเหล่านี้จะเป็นหน่วยงานหนึ่ง หรือเป็นของฝ่ายตรวจสอบภายใน แต่จะต้องอยู่คนละฝ่ายประมวลผลข้อมูลคือไม่ให้เกี่ยวของกันเลย ไม่ให้มีคนใดคนหนึ่งทำงานในทั้งสองฝ่ายพร้อม ๆ กัน

การตรวจสอบจะตรวจทุก ๆ ด้านที่เกี่ยวข้อง ดังรูป 3.55

วิธีการในการตรวจสอบ เช่น

- General questioning ผู้ตรวจสอบจะตั้งคำถามถามทุกอย่างที่ต้องการจะรู้เท่านั้น ไปถามด้วยตนเอง

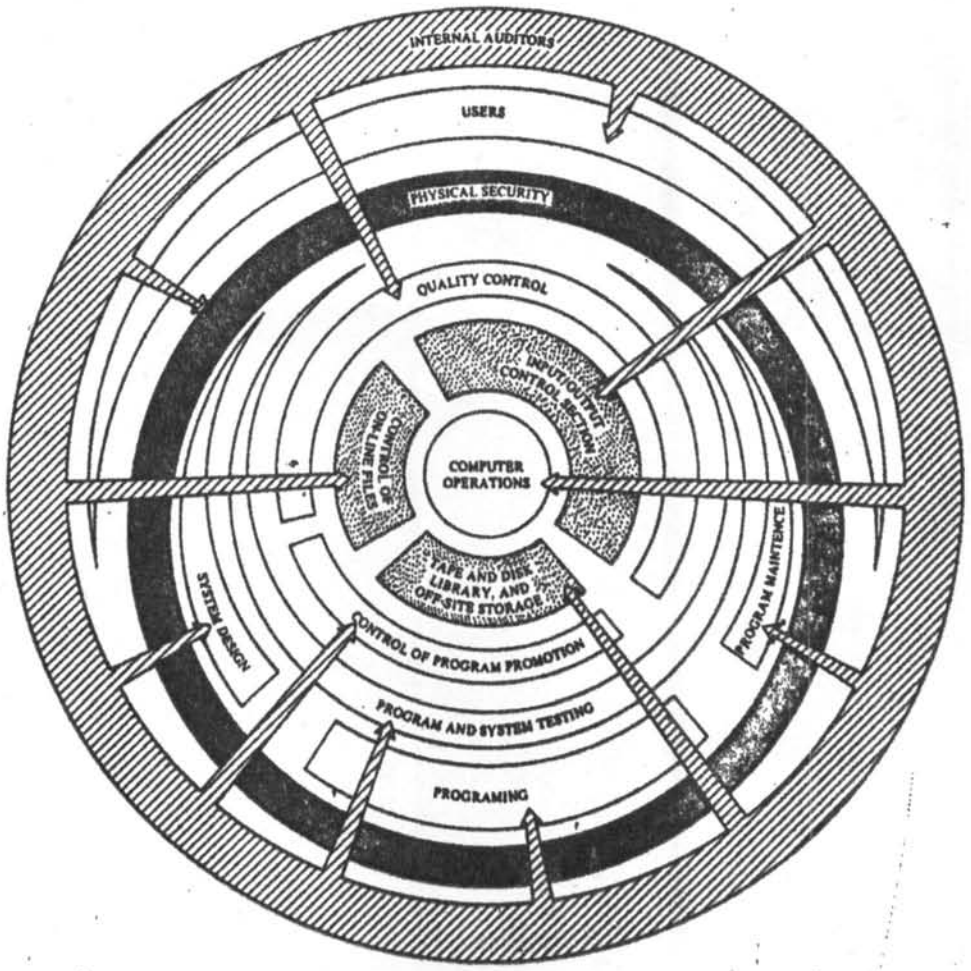
- Questions and clecklists ผู้ตรวจสอบจะมีข้อตรวจสอบเป็นรายละเอียดเอาไว้เพื่อกันลืม แล้วจึงจะตรวจสอบเป็นข้อ ๆ ตามรายละเอียด รายละเอียดของข้อตรวจสอบเหล่านี้แตกต่างกันไปแล้วแต่หน่วยงาน และข้อตรวจสอบอย่างนี้จะต้องถามคลุมทุก ๆ ด้านภายในศูนย์คอมพิวเตอร์หรือหน่วยประมวลผลข้อมูลนั้น

- Spot checks โดยจะตรวจสอบในช่วงใดช่วงหนึ่งของระบบ

- Sampling เลือกตัวอย่างบางส่วนนำมาตรวจสอบ

- Special program ใช้ในกรณีที่ไม่มีกระดาษพิมพ์ผลลัพธ์ออกมาให้เห็น จะมีการเขียนโปรแกรมขึ้นมาใหม่โดยเขียนภายนอกของหน่วยงานประมวลข้อมูล กรณีตรวจสอบวิธีนี้มักจะใช้ในระบบการประมวลผลทันที

- ฯลฯ



รูป 3.55 การตรวจสอบทุก ๆ ด้านที่เกี่ยวข้องกับคอมพิวเตอร์

การกำหนดระยะเวลาในการตรวจสอบระบบ มีหลายแบบ เช่น

- Daily monitoring ตรวจสอบทุก ๆ วัน เช่น ในกรณีตรวจรายการบันทึกการทำงานของเจ้าหน้าที่ควบคุมเครื่อง

- Spot checks จะตรวจสอบในช่วงเวลาใด ๆ ก็ได้ ใช้ได้ทั้งกรณีตรวจสอบการทำงานในห้องคอมพิวเตอร์ หน่วยงานของผู้ใช้ การตรวจสอบการทดสอบของโปรแกรม ฯลฯ เป็นต้น

- Periodic checks ตรวจสอบทุก ๆ ช่วงเวลาที่กำหนด

ฯลฯ

การดำเนินการตรวจสอบ เช่นเดียวกับการตรวจสอบทั่ว ๆ ไป เทคนิคพื้นฐานที่ต้องใช้คือการประเมินผลการควบคุมภายในของผู้รับตรวจเป็นอันดับแรก ทั้งนี้เพื่อนำผลมากำหนดวิธีการตรวจและประมาณงานที่จะทำการสุ่มสอบ

การประเมินผลการควบคุมภายใน ความมุ่งหมายของการประเมินผลการควบคุมภายในก็เพื่อให้ผู้ตรวจสอบสามารถมั่นใจได้ว่า มีการป้องกันความผิดพลาดอย่างรัดกุม หรือถ้าเกิดความผิดพลาดขึ้นในระบบก็ตรวจพบได้ในเวลารวดเร็ว ผลของการประเมินจะเป็นเครื่องชี้ว่าสามารถจะเชื่อถือหรือยืนยันความถูกต้องของรายงานที่มาจากการประมวลผลข้อมูลได้หรือไม่เพียงใด จุดที่ต้องเพ่งเล็งในการประเมินผลประกอบด้วย

ก. มีการแบ่งแยกหน้าที่และขอบเขตความรับผิดชอบของผู้ปฏิบัติงานโดยชัดแจ้ง และมีระเบียบยืนยันความถูกต้องที่เหมาะสม

ข. มีการวางระเบียบปฏิบัติในการควบคุมรัดกุมและสมเหตุสมผล

ค. มีการควบคุมให้ปฏิบัติตามระเบียบที่วางไว้อย่างสม่ำเสมอ ระเบียบใด ๆ จะมีค่าเพียงเศษกระดาษเปื้อนหมึกเท่านั้น ถ้าไม่มีการตรวจตราให้ปฏิบัติตามอย่างใกล้ชิด ระเบียบปฏิบัติในด้านต่อไปนี้ต้องได้รับการเพ่งเล็งควบคุมเป็นพิเศษ

- มีการเตรียมข้อมูลเบื้องต้นอย่างถูกต้อง
- ข้อมูลทุกรายการได้รับการปฏิบัติโดยปราศจากการละเว้นหรือเพิ่มเติม
- ขบวนการประมวลผลข้อมูลเป็นไปอย่างถูกต้องเหมาะสม
- ผลลัพธ์ได้รับการแจกจ่ายอย่างตรงเวลาไปยังผู้รับซึ่งมีหน้าที่รับผิดชอบเกี่ยวข้องเท่านั้น

ข้อมูลที่จะนำมาใช้ในการประเมินผลย่อมได้มาจากการสังเกตการณ์และสอบถาม การศึกษาผังงานและคู่มือการปฏิบัติงาน วิธีการดำเนินงานเพื่อที่จะได้ข้อมูลที่จำเป็นสำหรับบันทึกในกระดาษยอมแตกต่างกันตามวิธีการดำเนินงานของผู้ตรวจสอบแต่ละคน

ในทางปฏิบัติโดยทั่วไปการประเมินผลการควบคุมภายในอาจจะแบ่งออกเป็นสองภาคคือ

- ภาคแรกเป็นการประเมินผลการควบคุมโดยส่วนรวม
- ภาคที่สองเป็นการประเมินผลการควบคุมในด้านใดด้านหนึ่งโดยเฉพาะ

สำหรับการประเมินผลการควบคุมโดยส่วนรวมนั้น ผู้ตรวจสอบนิยมใช้การออกแบบสอบถามเพื่อใช้เป็นแบบสอบถาม ตัวอย่างของแบบสอบถามได้นำมาแสดงไว้ในภาคผนวก ซึ่งเป็นแบบสอบถามที่ออกแบบสำหรับการใช้ระบบคอมพิวเตอร์ในประเทศไทย โดยดัดแปลงจากคำถามหลักตามมาตรฐานของ Distric Audit แห่งประเทศอังกฤษ

ในด้านการประเมินผลการควบคุมภายในเฉพาะด้านนั้น เนื่องจากสภาวะและวิธีการทำงานแตกต่างกันอย่างมากจากที่แห่งหนึ่งไปยังอีกแห่งหนึ่ง ดังนั้น จึงไม่อาจจัดเตรียมแบบสอบถามที่เป็นมาตรฐานสากลโดยแท้จริงได้ ผู้ตรวจสอบต้องพิจารณาประเมินผลให้เหมาะสมกับงานแต่ละงานโดยใช้วิจารณญาณและประสบการณ์เป็นเครื่องประกอบ

ในการตรวจสอบระบบงานที่ใช้คอมพิวเตอร์อาจกล่าวได้ว่า งานประเมินผลการควบคุมภายในเป็นงานสำคัญที่สุด การทำงานโดยใช้บุคคลเป็นผู้ปฏิบัติและการใช้คอมพิวเตอร์มีข้อแตกต่างที่เด่นชัดอยู่ข้อหนึ่ง การใช้บุคคลเป็นผู้ปฏิบัติงานนั้นถึงจะมี

มาตรการควบคุมเข้มแข็งเพียงใดก็ตาม รายการผิดพลาดย่อมเกิดขึ้นได้เสมอ เช่น รายการคำนวณผิดพลาด เปรียบเทียบตัวเลขผิดเพราะเผลอเรอหลงลืม เป็นต้น ทั้งนี้เพราะธรรมชาติการทำงานของคนมีแนวโน้มที่จะผิดพลาดได้ง่ายอยู่แล้ว ในทางตรงข้ามการทำงานของระบบคอมพิวเตอร์นั้นโดยตัวของมันเองยากที่จะเกิดการผิดพลาด ถ้ามีการวางระบบการทำงานเป็นอย่างดี แล้วเครื่องคอมพิวเตอร์ย่อมตรวจผลการทำงานด้วยตัวของมันเองตลอดเวลา ดังนั้น ถ้ามีการควบคุมระบบการทำงานอย่างถูกต้องและใกล้ชิดโอกาสที่จะเกิดความผิดพลาดย่อมมีน้อยมาก เพราะฉะนั้น ถ้าผลของการประเมินผลการควบคุมภายในปรากฏเป็นที่น่าพอใจแล้ว ผู้ตรวจสอบย่อมวางใจในความถูกต้องของข้อมูลที่ทำการตรวจสอบได้มากกว่าที่ผ่านการใช้บุคคลปฏิบัติงานมากมาย เหตุนี้ผลของการประเมินผลการควบคุมภายในจึงมีอิทธิพลอย่างยิ่งต่อการกำหนดแนวทางวิธีการตรวจ และปริมาณงานที่จะทำการตรวจสอบ

หลังจากได้ศึกษาระบบการควบคุมภายในโดยละเอียดแล้ว ผู้ตรวจสอบย่อมเข้าใจถึงระบบงานที่จะตรวจ ขอบเขตและความมุ่งหมายของงานแต่ละชนิดที่ทำ ในการพิจารณาวางแนวและปริมาณงานที่จะทำการตรวจผู้ตรวจสอบต้องพิจารณาถึงปัจจัยต่อไปนี้ประกอบด้วย

ก. ความสำคัญของระบบคอมพิวเตอร์ที่มีต่องานของผู้รับตรวจเพื่อพิจารณาว่าจะเพ่งเล็งให้ความสำคัญต่อการตรวจสอบในด้านนี้เพียงใด

ข. ความบกพร่องในระบบการควบคุมและวิธีปฏิบัติที่มีอิทธิพลต่อแนวการตรวจสอบและทำการดัดแปลงแนวการตรวจสอบให้เหมาะสมกับสถานการณ์

<u>ประเภทของการดำเนินงานตรวจสอบ</u> โดยทั่วไปนิยมแบ่งออกเป็น 2 ประเภทใหญ่ คือ

1. Around the Computer

2. Through the Computer

1. Around the Computer โดยวิธีนี้ผู้ตรวจสอบมองข้ามระบบคอมพิวเตอร์ โดยถือเสมือนเป็น " Black Box" ผู้ตรวจสอบคัดเลือกรายการที่จะทำการตรวจสอบแล้วทดลองปฏิบัติงานด้วยตนเองตั้งแต่เป็นเอกสารเบื้องต้นจนสำเร็จเป็นงานสุดท้าย แล้วนำมาเปรียบเทียบกับผลงานที่ปฏิบัติโดยเครื่องคอมพิวเตอร์ จะเห็นได้ว่า โดยวิธีนี้การตรวจสอบจะกระทำโดยไม่คำนึงถึงว่าระบบงานที่ตรวจปฏิบัติจริง ๆ เป็นอย่างไร โดยถือหลักการว่า ถ้าสามารถพิสูจน์ได้ว่าเอกสารเบื้องต้นได้รับการเตรียมโดยถูกต้องและผลการปฏิบัติงานสะท้อนให้เห็นถึงการนำเอกสารเบื้องต้นนั้นมาใช้อย่างเหมาะสม ดังนั้น ก็อาจสรุปได้ว่า ขั้นตอนการปฏิบัติงานส่วนที่ทำโดยระบบคอมพิวเตอร์ถูกต้องด้วย

วิธีการตรวจสอบแบบ Around the Computer เป็นวิธีการที่ใช้กันอย่างแพร่หลายในระยะแรกด้วยเหตุผลหลายประการ คือ

ก. เป็นวิธีที่คล้ายกับการตรวจสอบปกติที่ผู้ตรวจสอบคุ้นเคยอยู่แล้ว

ข. ไม่จำเป็นต้องมีความรู้ทางเทคนิคในด้านระบบคอมพิวเตอร์

ค. ในระยะแรกของการใช้ระบบคอมพิวเตอร์ ความสามารถที่จะสอบย้อนกลับไปยังเอกสารขั้นต้น (Audit Trails) ยังไม่เปลี่ยนรูปแบบดังนั้นจึงยังอาจใช้วิธีตรวจสอบแบบเดิมได้สะดวก

อย่างไรก็ตาม เหตุผลที่สำคัญที่สุดและมักมิได้นำมาอ้างก็คือ ผู้ตรวจสอบจำนวนมากไม่พยายามที่จะเข้าใจระบบคอมพิวเตอร์

2. Through the Computer โดยวิธีนี้ผู้ตรวจสอบยึดถือหลักการว่า ถ้าเอกสารเบื้องต้นได้รับการเตรียมโดยถูกต้อง ระบบการควบคุมภายในเป็นไปอย่างเหมาะสม ดังนั้นถ้านำเอกสารเบื้องต้นมาประมวลผลข้อมูลอย่างถูกต้องก็ย่อมจะเชื่อได้ว่าผลของการประมวลผลข้อมูลย่อมจะถูกต้อง สมมุติฐานของวิธีนี้ก็คือผู้ตรวจสอบมั่นใจต่อความถูกต้อง ในการทำงานของระบบคอมพิวเตอร์

การตรวจสอบโดยวิธีนี้จะช่วยลดงานและประหยัดค่าใช้จ่ายในการตรวจสอบลงมากเพราะผู้ตรวจสอบไม่จำเป็นต้องประมวลผลข้อมูลใหม่ด้วยตนเองเป็นจำนวนมากเพื่อเปรียบเทียบกับผลการตรวจสอบด้วยวิธี Around the computer

การพิจารณาว่าจะใช้วิธี Through the Computer ได้หรือไม่นั้น ก่อนอื่นต้องพิจารณาว่าผลที่ได้รับจากการตรวจสอบการควบคุมภายในเป็นที่น่าพอใจ และงานที่ตรวจไม่เปลี่ยนแปลงระเบียบหรือขั้นตอนการทำงานบ่อยครั้งในช่วงที่ทำการตรวจ ถ้าศูนย์คอมพิวเตอร์นั้นไม่มีระบบการควบคุมภายในที่ดีหรือการปฏิบัติตามระเบียบที่วางไว้ไม่เคร่งครัดแล้วก็จะไม่มั่นใจในผลของการประมวลผลข้อมูลโดยคอมพิวเตอร์ได้ ซึ่งย่อมจำเป็นที่จะต้องกลับไปใช้วิธี Around the Computer ในการตรวจสอบ

อย่างไรก็ตาม เป็นที่น่าสังเกตว่า ความหมายของคำว่า Around the Computer และ Through the Computer ยังเป็นที่คลุมเครือสับสน การตีความหมายของคำทั้งสองยังไม่มีบรรทัดฐานแบ่งแยกที่แน่ชัด ผู้ตรวจสอบไม่ควรยึดถือหรือเน้นความสนใจกับวิธีใดวิธีหนึ่งโดยเฉพาะ แต่ควรใช้วิจารณญาณคัดเลือกเทคนิคที่เหมาะสมมาใช้กับงานแต่ละด้านมากกว่า ในปัจจุบันเป็นการยากที่จะใช้แต่เพียงวิธี Around the Computer หรือวิธี Through the Computer เพียงอย่างหนึ่งอย่างเดียว ปริมาณงานที่ต้องทำการตรวจสอบซึ่งเพิ่มขึ้นอย่างมากมายอันเป็นผลจากการใช้คอมพิวเตอร์ในการทำงาน ทำให้การตรวจแบบ Around the Computer เป็นไปโดยทั่วถึงได้ยากและต้องเสียค่าใช้จ่ายสูงมาก ในทางตรงข้ามการควบคุมที่ไม่เคร่งครัดและระเบียบการปฏิบัติงานที่เปลี่ยนแปลงอยู่เสมอก็ทำให้ไม่สามารถจะใช้วิธี Through the Computer ได้ในบางโอกาส อย่างไรก็ตาม ไม่ว่าจะนำวิธีใดมาใช้ในการดำเนินการตรวจสอบ ข้อที่ต้องระวังก็คือ ไม่ควรจะลดความสำคัญของงานประเมินผลการควบคุมภายใน ผู้ตรวจสอบต้องยอมรับความสำคัญและบทบาทของเครื่องมืออิเล็คโทรนิคส์เหล่านี้ และต้องต่อต้านความจริงของการตั้งสมมุติฐานที่คาดว่าถ้าข้อมูลเบื้องต้นได้รับการตรวจสอบว่าถูกต้องและผลลัพธ์ก็สามารถสอบยอนมายังเอกสารเบื้องต้นได้โดยง่าย ผู้ตรวจสอบอาจละเลยไม่สนใจสิ่งที่เกิดขึ้นในระบบคอมพิวเตอร์เลย จากประสบการณ์ที่ผ่านมาของผู้ตรวจสอบอาวุโสได้แนะนำว่า วิธีการตรวจสอบที่มีประสิทธิภาพมากที่สุด คือ การใช้วิธีทั้งสองร่วมกันตามความเหมาะสมของแต่ละงาน

เทคนิคที่ใช้ในการตรวจสอบ ได้แก่

1. การตรวจลืบหาข้อมูล (Tracing the Transaction)
2. ตรวจรายการข้อมูลที่ได้พิมพ์ออกมาจากแฟ้มข้อมูล (File Listing)
3. ตรวจสอบโปรแกรมคอมพิวเตอร์ (Review of Computer Program)
4. Minicompany
5. การประมวลผลใหม่ (Control Reprocessing)
6. การใช้โปรแกรมในการตรวจสอบ (Audit Software)
7. ใช้ข้อมูลทดสอบ (Test Data)

1. การตรวจสืบหาข้อมูล เป็นการตรวจสอบโดยการติดตามขั้นตอนการประมวลผลข้อมูลของงานใดงานหนึ่ง เช่น งานด้านการทำรายละเอียดลูกหนี้ ผู้ตรวจสอบจะติดตามการปฏิบัติงานตั้งแต่การเตรียมเอกสารเบื้องต้น ส่งเข้ามาประมวลผลยังศูนย์คอมพิวเตอร์ จนกระทั่งท้ายสุดสำเร็จเป็นผลลัพธ์ขั้นสุดท้าย ผู้ตรวจสอบประเมินผลการทำงานและตรวจสอบความถูกต้องของขบวนการประมวลผลเป็นระยะ ๆ โดยปกติการตรวจสอบแบบนี้มักทำควบคู่กันไปกับการประเมินผลการควบคุมภายในโดยเลือกรายการตัวอย่างที่จะติดตามขั้นตอนการปฏิบัติงาน ทั้งนี้ เพื่อให้สามารถเข้าใจระบบงานที่ผู้รับตรวจใช้ได้ดีขึ้น และสามารถเห็นภาพพจน์ของระบบการควบคุมจากการติดตามการปฏิบัติงานจริง ๆ อย่างไรก็ตาม การตรวจสอบโดยวิธีนี้เสียเวลาและค่าใช้จ่ายมาก ดังนั้น จึงไม่อาจทำอย่างกว้างขวาง นอกจากทำเป็นตัวอย่างเพียงสองสามรายการ

ในการใช้ระบบ Online Realtime System การแก้ไขเปลี่ยนแปลงแฟ้มข้อมูลหลักอาจทำโดยผ่านอุปกรณ์ปลายทาง ดังนั้นจึงอาจไม่มีรายละเอียดประกอบอันเดิม และการควบคุมชุดข้อมูลเช่น ระบบการประมวลผลแบบเป็นชุด อย่างไรก็ตาม การปล่อยให้ระบบดำเนินไปโดยไม่มีการตรวจสอบย้อนกลับไปยังเอกสารขั้นต้นอย่างพอเพียงย่อมแสดงถึงระบบที่เลวในด้านการออกแบบ ในทางปฏิบัตินั้นก่อนที่ข้อมูลเบื้องต้นใดที่ผ่านจากอุปกรณ์ปลายทางจะถูกส่งเข้าไปประมวลผลข้อมูลในแฟ้มข้อมูลหลัก ควรจะถูกบันทึก

ไว้ในเทป เมื่อสิ้นงวด เช่น สิ้นวันทำการ ข้อมูลเบื้องต้นทั้งหมดที่บันทึกไว้นั้น จะถูกนำมา Sort หรือจำแนกเป็นประเภทและจัดทำจำนวนคุมยอมแล้วนำไปกระทบยอดกับการเปลี่ยนแปลงของแฟ้มข้อมูลหลักอีกครั้งหนึ่ง รายละเอียดที่กล่าวมาแสดงได้ดังรูป 3.56 และรูป 3.57

2. ตรวจรายการข้อมูลที่ได้พิมพ์ออกมาจากแฟ้มข้อมูล ถ้าผู้ตรวจสอบต้องการทราบข้อมูลที่บรรจุอยู่ในแฟ้มข้อมูลได้ย่อมเป็นการง่ายที่จะขอให้ผู้รับตรวจข้อมูลออกมาจากแฟ้มข้อมูล โดยพิมพ์ถ่ายทอดข้อมูลจากแฟ้มข้อมูลให้อยู่ในรูปที่อ่านได้ การพิมพ์ข้อมูลออกมาจากแฟ้มข้อมูลนี้ถ้าทำในรูปที่ยังไม่ได้จัดรูปแบบที่อ่านได้ง่าย การที่จะอ่านข้อมูลที่ยังไม่ได้จัดรูปแบบนี้ได้ย่อมสะดวกผู้ตรวจสอบอาจขอรูปแบบ (Format) จากผู้รับตรวจแล้วใช้คิดสอบแบ่งรายการเป็นหมวดหมู่ตามความเหมาะสม

การดำเนินการตรวจสอบรายการของข้อมูลที่พิมพ์ออกมาจากแฟ้มข้อมูลนั้น ใช้หลักการเกี่ยวกับการปฏิบัติงานตามปกติ เช่น ใช้หลักการเกี่ยวกับการตรวจรายการในสมุดบัญชีย่อย การพิจารณารายการแต่ละรายการอาจเปิดเผยให้ทราบถึงรายการหรือรหัสบัญชีที่ผิดปกติ จำนวนเงินที่มากเกินความสมเหตุสมผล ฯลฯ

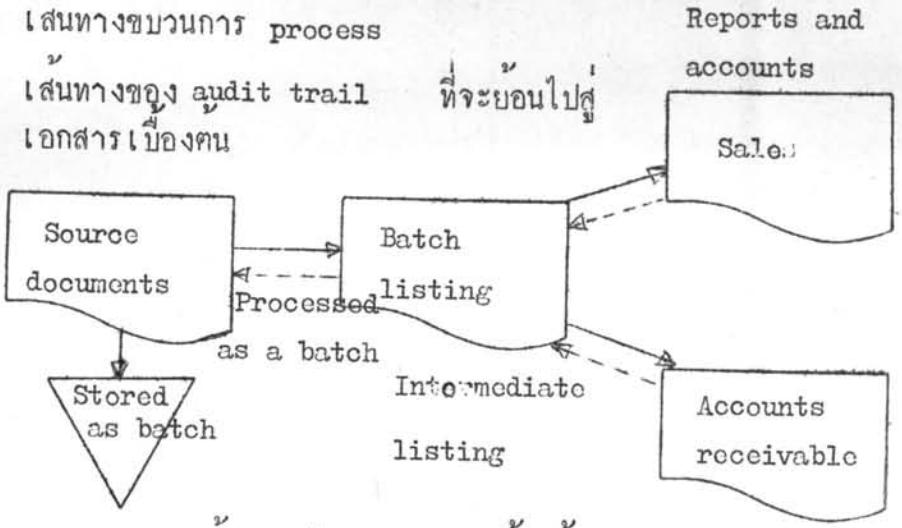
3. ตรวจสอบโปรแกรมคอมพิวเตอร์ เป็นการคัดลอกโปรแกรมที่ผู้รับตรวจใช้อยู่มาศึกษาว่าถูกต้องสมเหตุสมผลหรือไม่ กล่าวคือเป็นการตรวจสอบเพื่อค้นหาข้อผิดพลาดและจุดอ่อนของโปรแกรม

อย่างไรก็ตามในทางปฏิบัติการใช้วิธีการตรวจสอบโปรแกรมน้อยมากด้วยเหตุดังต่อไปนี้

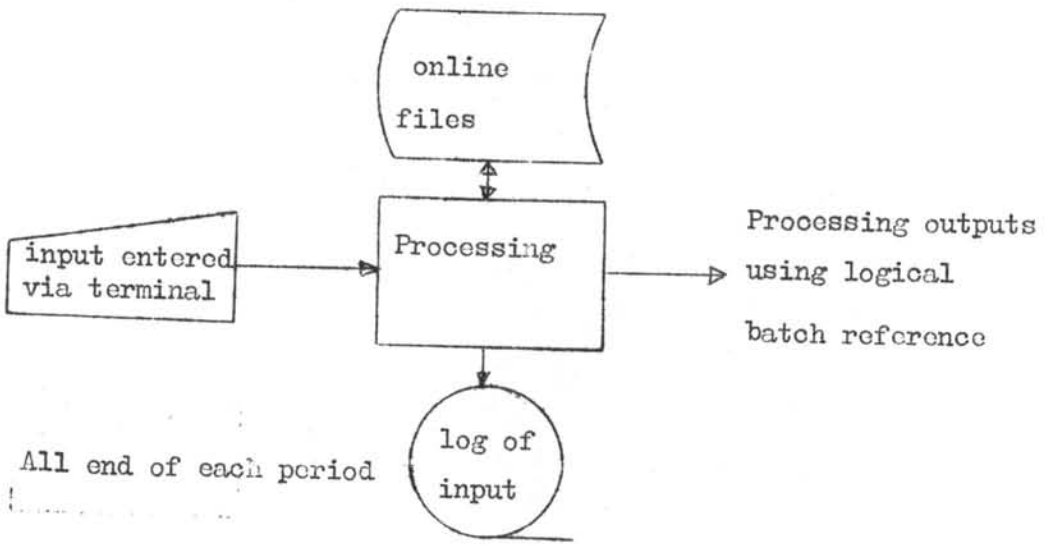
ก. ตามปกติการตรวจสอบโปรแกรมต้องใช้ความรู้และความชำนาญในด้านโปรแกรมมากกว่าการเขียนโปรแกรมเองตั้งแต่ต้น การที่จะติดตามรายละเอียดในโปรแกรมย่อย นับไม่ถ้วน ย่อมเป็นงานที่ยากลำบากอย่างยิ่ง ถึงแม้ผู้ตรวจและทีมงานจะเป็นผู้เชี่ยวชาญในด้านโปรแกรมก็ตาม แต่การตรวจสอบโปรแกรมจะต้องใช้เวลาและค่าใช้จ่ายเป็นอย่างมาก

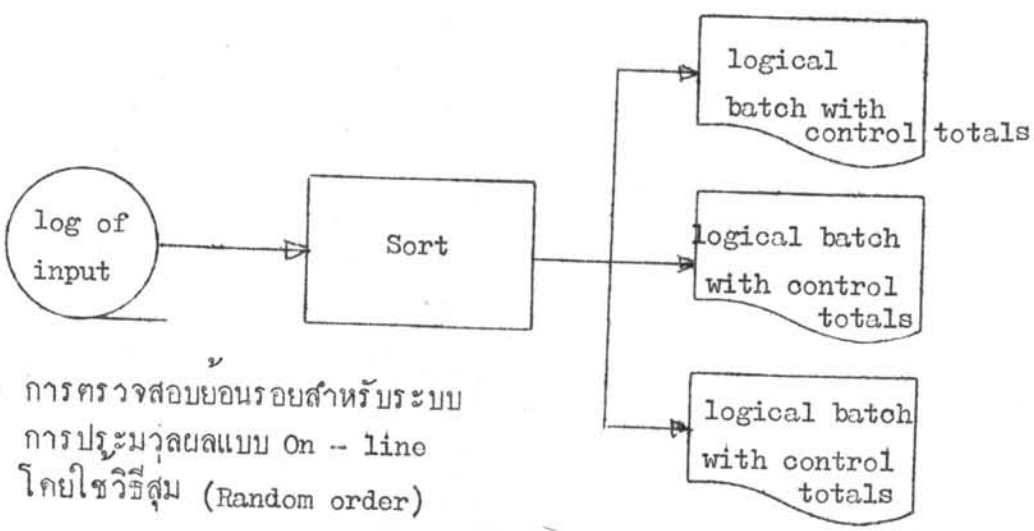
——— เส้นทางขบวนการ process

- - - - - เส้นทางของ audit trail ที่จะย้อนไปสู่เอกสารเบื้องต้น



รูป 3.56 การตรวจสอบย้อนรอยไปยังเอกสารเบื้องต้นสำหรับการประมวลผลข้อมูลแบบเป็นชุด





รูป 3.57 การตรวจสอบย้อนรอยสำหรับระบบการประมวลผลแบบ On – line โดยใช้วิธีสุ่ม (Random order)

ข. ในการตรวจวิเคราะห์โปรแกรมนั้นในทางปฏิบัติมักปรากฏว่า ผู้วิเคราะห์ข้ามจุดอ่อนเสียเอง ซึ่งการที่จะพัฒนาโปรแกรมให้อยู่ในขั้นใช้งานได้นั้น ต้องใช้เวลานานและทำการทดสอบนับครั้งไม่ถ้วน การวิเคราะห์ในช่วงเวลาสั้น ๆ จึงไม่อาจมองแง่มุมต่าง ๆ ที่แฝงอยู่ได้ถี่ถ้วน

ค. โปรแกรมที่ใช้มักจะมีการเปลี่ยนแปลงแก้ไขตลอดเวลา ถ้าผู้ตรวจสอบดำเนินการตรวจสอบแบบกระจายงานเป็นระยะ เช่น ตลอดปีบัญชี การที่จะติดตามรายการเปลี่ยนแปลงซึ่งมีจำนวนมากทุกรายการ ย่อมเป็นไปได้ยากในทางปฏิบัติ

ด้วยเหตุดังกล่าวการที่จะตรวจสอบโปรแกรมในทางปฏิบัติจึงมักใช้วิธีตรวจสอบทางอ้อม คือการตรวจสอบควบคู่ไปกับการใช้วิธีการทดสอบข้อมูล ซึ่งจะได้อธิบายโดยละเอียดต่อไป

4. Minicompany เป็นวิธีการตรวจโดยสร้างระบบจำลองระบบที่ใช้อยู่จริง ๆ ตามปกติมักใช้เมื่อผู้รับตรวจใช้ระบบ Cnline real-Time System ซึ่งการทดสอบระบบการทำงานโดยตรงอาจกระทบกระเทือนการทำงานปกติ

5. การประมวลผลใหม่ โดยวิธีนี้ผู้ตรวจสอบเตรียมโปรแกรมที่จะใช้ในการประมวลผลข้อมูลในงานที่จะตรวจสอบเสียเองจากนั้นจึงนำไปประมวลผลข้อมูลกับแฟ้มข้อมูลหลักของงานที่จะตรวจสอบ ผลที่ได้รับจะนำมาเปรียบเทียบกับผลที่ได้จากการประมวลผลข้อมูลกับโปรแกรมของงานที่ตรวจสอบใช้อยู่จริง ๆ และถ้ามีข้อแตกต่างก็จะทำการวินิจฉัยข้อแตกต่างนั้น กล่าวคือ เป็นการทำงานซ้ำซ้อนกันกับการทำงานที่ตรวจสอบนั้น วิธีการตรวจสอบแบบนี้มักทำร่วมกับการใช้โปรแกรมสำเร็จรูปในการตรวจสอบ ซึ่งจะได้กล่าวถึงต่อไป

6. การใช้โปรแกรมในการตรวจสอบ เพื่อแบ่งเบางานผู้ตรวจสอบอาจใช้ความสามารถพิเศษของเครื่องคอมพิวเตอร์ที่สามารถทำงานได้อย่างรวดเร็วเที่ยงตรงและประหยัด ช่วยในงานตรวจสอบ ตัวอย่างของงานเหล่านี้ ได้แก่

– รวบรวมข้อมูลและทำการแยกประเภทตามที่ผู้ตรวจต้องการ เช่น ทำการแยกประเภทและอายุลูกหนี้เพื่อเป็นข้อมูลเบื้องต้นในการวิเคราะห์รายการลูกหนี้

– ตรวจสอบความถูกต้องของรายการแต่ละรายการในแฟ้มข้อมูลหลักของงานที่ตรวจ

– ใช้เครื่องคอมพิวเตอร์คัดเลือกและพิมพ์รายการยืนยันยอด เช่น ใช้เครื่องคอมพิวเตอร์ทำการคัดเลือกรายการลูกหนี้ตามมาตรการที่กำหนดในโปรแกรมที่วางไว้จากแฟ้มข้อมูลหลัก แล้วทำการพิมพ์รายการตามแบบฟอร์ม

– ใช้คอมพิวเตอร์คัดเลือกข้อมูลเพื่อทำการตรวจสอบตามระบบสุ่มตัวอย่างที่วางไว้

– เปรียบเทียบข้อมูลที่ได้จากการตรวจสอบของจริงกับข้อในแฟ้มข้อมูลหลักของงานที่ตรวจ เช่น เปรียบเทียบรายการตรวจนับพัสดุกับรายการพัสดุที่บันทึกในแฟ้มข้อมูลหลัก

โปรแกรมที่ใช้เพื่อการตรวจสอบอาจได้มาจากแหล่งต่าง ๆ ดังนี้

1. โปรแกรมของงานที่ตรวจใช้อยู่เป็นประจำมักจะมีรายการวิเคราะห์หลายประเภทซึ่งเป็นที่ต้องการทั้งด้านผู้รับตรวจและผู้ตรวจสอบ เช่น รายการวิเคราะห์อายุลูกหนี้ รายการวิเคราะห์ด้านสินค้าคงคลัง หรือรายการวิเคราะห์พัสดุล้าสมัย งานที่จะต้องตรวจมักมีโปรแกรมเหล่านี้อยู่แล้ว จึงเป็นการสะดวกที่ผู้ตรวจสอบจะขอใช้ ข้อสำคัญก็คือผู้ตรวจสอบต้องทำการตรวจสอบโปรแกรมเหล่านี้โดยถี่ถ้วนเสียก่อนว่าทำหน้าที่ตามที่ต้องการจริง ๆ และถูกต้อง

2. ผู้ตรวจสอบเตรียมโปรแกรมสำหรับใช้ในการตรวจสอบเอง ผู้ตรวจสอบที่มีความรู้ในด้านโปรแกรมดีพออาจจะทำการเขียนโปรแกรมด้วยตนเองหรืออาจขอความร่วมมือจากผู้เตรียมโปรแกรมของงานที่จะตรวจให้ช่วยเขียนตามข้อกำหนดของโปรแกรมที่ผู้ตรวจสอบกำหนด โดยปกติจะมีขั้นตอนพัฒนาโปรแกรมดังนี้

– ตัดสินใจเลือกจุดมุ่งหมายและแนวการตรวจสอบ

– ถ่ายทอดแนวการตรวจเป็นแผนผังการทำงานของระบบข้อกำหนดของโปรแกรม และแผนผังการทำงานของโปรแกรม

– ดำเนินการเขียนโปรแกรม

– ทดสอบโปรแกรม

3. ใช้โปรแกรมการตรวจสอบทั่ว ๆ ไป นับแต่ปี ค.ศ. 1960 เป็นต้นมา จำนวนการติดตั้งระบบคอมพิวเตอร์ในสหรัฐอเมริกาเพียงแห่งเดียวได้ทวีจำนวนเท่าตัวทุก ๆ 3 ปี ผู้ตรวจสอบจะพบว่างานตรวจสอบในส่วนที่เกี่ยวกับระบบคอมพิวเตอร์ได้เพิ่มขึ้นอย่างรวดเร็ว โดยเฉพาะงานตรวจสอบในระบบบัญชีที่ใช้คอมพิวเตอร์ช่วยปฏิบัติงาน ซึ่งผลกระทบกระเทือนของการใช้คอมพิวเตอร์ที่มีต่องานตรวจสอบอาจแยกออกเป็นส่วนสำคัญ 2 ส่วน คือ

ก. ก่อให้เกิดการเปลี่ยนแปลงในรูปแบบของการควบคุมภายในได้กล่าวมาแล้วในตอนต้น

ข. วิธีการที่ใช้ในการตรวจสอบเปลี่ยนไป และมีการนำคอมพิวเตอร์มาช่วยการปฏิบัติงานในด้านผู้ตรวจสอบ

โปรแกรมตรวจสอบสำเร็จรูป ชื่อ Haskins & Sell Auditape ได้นำออกใช้ครั้งแรกในปี ค.ศ. 1967 โดยออกแบบให้ใช้กับ IBM 1401 หรือ IBM System/360 จากนั้นการใช้โปรแกรมตรวจสอบสำเร็จรูปได้เป็นที่นิยมอย่างแพร่หลาย นอกจากที่บริษัทคอมพิวเตอร์ใหญ่ ๆ จะได้ออกแบบโปรแกรมตรวจสอบสำเร็จรูปเพื่อใช้งานเฉพาะตนแล้ว บริษัทขายบริการทางด้านระบบโปรแกรมหลายแห่งได้หันมาสนใจร่วมพัฒนาด้วย ในปี ค.ศ. 1971 มีโปรแกรมตรวจสอบสำเร็จรูปที่อาจหาได้ในท้องตลาดได้แก่

Firm	Software
1. Whinney Murray Ernst & Etnst 67 Chiswell Street London , E.C 1, England	ASK - 360
2. Alexander Grant & Co. One First National Plaza Chicago , Ill. 60670	AUDASSIST
3. Arthur Andersen & Co. 69 West Washington Street Chicago , Ill. 60670	AUDEX
4. S.D. Leidesdorf & Co. 125 Park Avenue New York , N.Y. 10017	AUDITALL
5. Haskins & Sells 1114 Avenue of the Americas New York , N.Y. 10036	AUDITAPE
6. Coopers & Lybrand 1251 Avenue of the Americas New York , N.Y. 10020	AUDITPAK
7. Computer Resources, Inc. Box 431 Wilton , Conn. 06897	AUDIT THRU
8. Ernst & Ernst 1300 Union Commerce Building Cleveland , Ohio 44115	AUTRONIC - 16

Firm	Software
9. Arthur Young & Company 277 Park Avenue New York , N.Y. 10017	Arthur Young & Company Audit / Management System
10. Computer Audit System, Inc. 725 Park Avenue East Orange, N.J. 07017	CARS
11. Price Waterhouse & Co. 1633 Broadway New York , N.Y. 10019	Computer File Analyzer
12. Information Science , Inc. New City Rockland County New York , N.Y. 10959	GRS
13. Cullinane Corporation One Boston Place Boston , Mass. 02108	EDP - Auditor
14. Republic Software Products 715 Park Avenue East Orange , N.J. 07017	MIRACL
15. Programming Methods , Inc. 51 Madison Avenue New York , N.Y.	SCORE
16. Touche Ross & Co. 1633 Broadway New York , N.Y. 10019	STRATA
17. Peat , Marwick , Mitchell & Co. 345 Park Avenue New York , N.Y. 10022	S/2170

จุดมุ่งหมายที่สำคัญของการใช้โปรแกรมตรวจสอบสำเร็จรูปก็คือ ช่วยให้ผู้ตรวจสอบซึ่งมีความรู้ในด้านคอมพิวเตอร์เพียงเล็กน้อยสามารถตรวจสอบระบบงานที่ใช้คอมพิวเตอร์ได้ ผู้ตรวจสอบเพียงแต่กรอบข้อความลงในข้อกำหนด แจ้งความประสงค์ที่จะใช้โปรแกรมตรวจสอบ รายการในข้อกำหนดจะแสดงถึงวิธีที่ผู้ตรวจสอบจะนำระบบโปรแกรมมาดัดแปลงให้เข้าความประสงค์และจะใช้เป็นเอกสารเบื้องต้นที่จะนำไปเข้าเครื่องคอมพิวเตอร์ จากนั้นรหัสในข้อกำหนดจะเชื่อมโยงโปรแกรมตรวจสอบส่วนต่าง ๆ เข้าเป็นโปรแกรมสำหรับใช้กับงานตรวจสอบที่ต้องการ

ตามปกติการฝึกงานเพียง 2-3 วันก่อนจะใช้โปรแกรมตรวจสอบสำเร็จรูปก็อาจจะพอเพียงสำหรับผู้ตรวจสอบที่มีความรู้ในด้านคอมพิวเตอร์ดีพอสมควร สำหรับผู้ที่ไม่มีพื้นความรู้ในด้านคอมพิวเตอร์มาก่อนเลย เวลาที่ใช้ในการฝึกอาจประมาณ 2 อาทิตย์ อย่างไรก็ตาม สำหรับผู้ที่มีพื้นฐานไม่ดีพอมักมีปัญหาเมื่อพบกับสถานการณ์ที่นอกเหนือจากเหตุการณ์ปกติ อนึ่ง โปรแกรมตรวจสอบสำเร็จรูปมีทั้งที่ออกแบบให้ใช้กับระบบคอมพิวเตอร์ใดโดยเฉพาะและที่สามารถใช้กับระบบทั่วไป ถ้าได้รับการออกแบบให้ใช้กับระบบคอมพิวเตอร์ใดโดยเฉพาะจะได้เปรียบในการใช้คุณสมบัติที่มีเด่นประจำของแต่ละระบบได้อย่างเต็มที่ ภาษาที่ใช้ก็อาจเป็นภาษาเครื่อง ทำให้สามารถทำงานได้รวดเร็วขึ้นและไม่ต้องใช้เนื้อที่ในหน่วยความจำมาก โปรแกรมการตรวจสอบสำเร็จรูปที่ออกแบบเพื่อใช้กับระบบคอมพิวเตอร์ทั่วไปส่วนมากจะใช้ภาษาชั้นสูง เช่น โคบอล ดังนั้นโปรแกรมประเภทนี้อาจจะใช้กับระบบคอมพิวเตอร์ใดก็ได้ที่มีตัวแปลของภาษาโคบอล โดยการแก้ไขเพียงเล็กน้อย อย่างไรก็ตาม ก็มีปัญหาใหญ่ประการหนึ่งก็คือ ทั้งผู้ตรวจสอบและผู้ออกแบบระบบ ต้องพยายามร่วมกันคิดค้นวิธีที่จะรักษา การตรวจสอบย้อนกลับไปยังเอกสารขั้นต้นไว้ให้พร้อมเสมอที่จะสอบย้อนไปสู่ต้นเรื่องในเวลาอันรวดเร็ว ในขณะเดียวกันการตรวจสอบย้อนกลับนี้ต้องมีรูปแบบที่ง่ายและไม่มีรายการประกอบมากเกินไป ซึ่งไม่เหมาะแก่การทำงานของเครื่องคอมพิวเตอร์ และเพื่อที่จะทำหน้าที่อย่างมีประสิทธิภาพจำเป็นอย่างยิ่งที่ผู้ตรวจสอบจะต้องมีความรู้และความเข้าใจในระบบคอมพิวเตอร์ดีพอสมควร

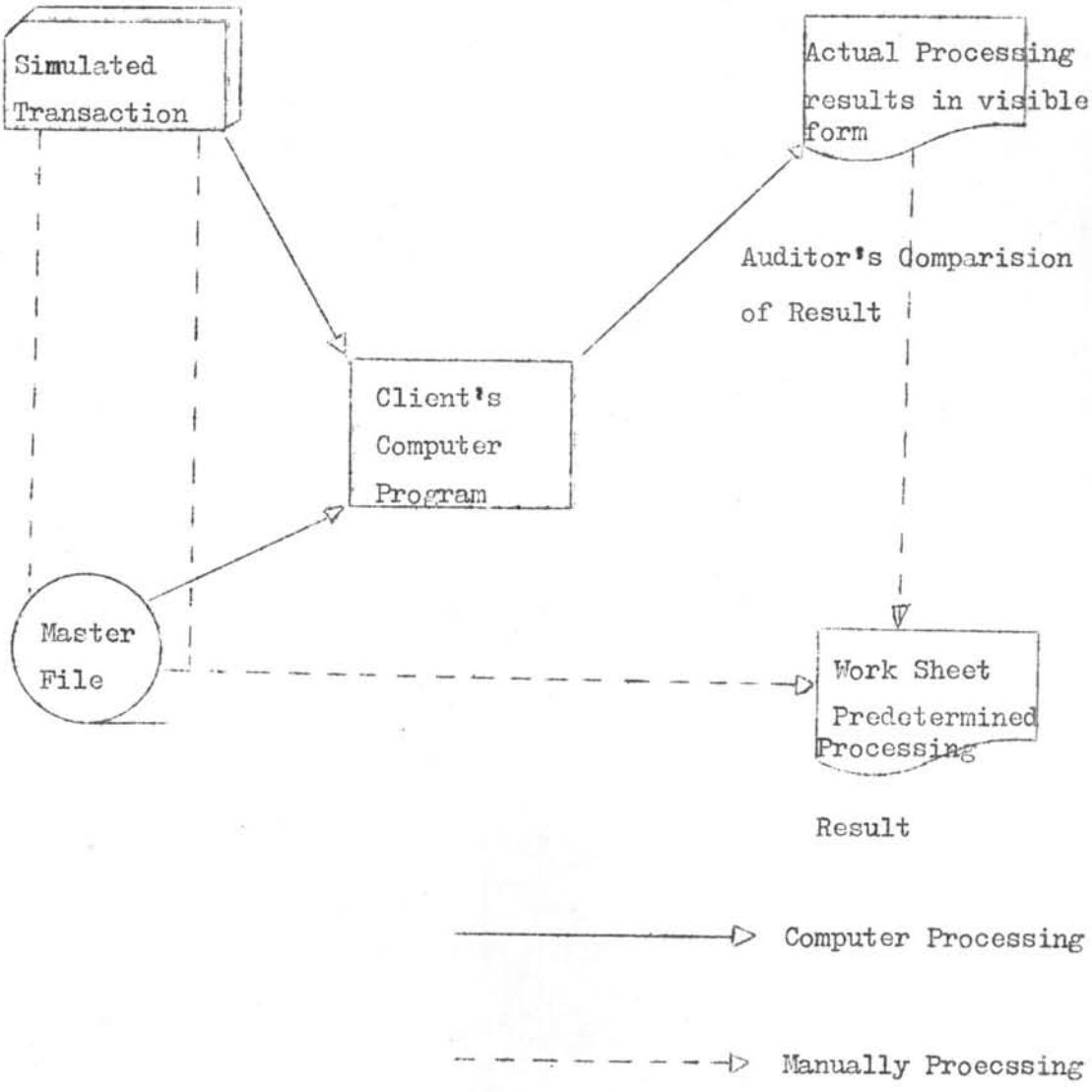
7. ใช้ข้อมูลทดสอบ เป็นการเตรียมข้อมูลเข้าหรือที่เรียกว่ากลุ่มข้อมูลทดสอบ (Test Deck) ซึ่งออกแบบให้จำลองรายการข้อมูลนำเข้าทุกประเภทเท่าที่อาจเป็นไปได้ กลุ่มข้อมูลทดสอบที่เตรียมนี้จะนำไปประมวลผลข้อมูลกับแฟ้มข้อมูลหลัก โดยใช้โปรแกรมซึ่งได้ใช้ปฏิบัติงานในขณะนั้นจริง ๆ ผลที่ได้รับจากการประมวลผลข้อมูลโดยคอมพิวเตอร์จะนำมาเปรียบเทียบกับผลการคำนวณที่เตรียมไว้ล่วงหน้าแล้ว จุดมุ่งหมายของการใช้ข้อมูลทดสอบก็เพื่อจะทดสอบว่าโปรแกรมที่จะใช้มีปฏิกิริยาต่อรายการข้อมูลนำเข้าแต่ละแบบอย่างไร ที่กล่าวมาแสดงได้ดังรูป 3.58

ผู้ตรวจสอบที่จะจัดเตรียมข้อมูลทดสอบได้จะต้องเป็นผู้เชี่ยวชาญในด้านตรรกของโปรแกรมพอสมควร การตรวจสอบโดยการใช้ข้อมูลทดสอบแต่ละครั้งอาจต้องใช้เวลาของเครื่องนาน จะสังเกตได้ว่าถึงแม้จะมีการแนะนำให้ใช้ข้อมูลทดสอบในฐานะที่เป็นเทคนิคเบื้องต้นในการตรวจสอบซึ่งใช้ระบบคอมพิวเตอร์แต่ในการปฏิบัติจริง ๆ นั้นการใช้ไม่แพร่หลายเท่าที่ควร เพราะความยากลำบากในการจัดเตรียมและเวลาที่ต้องใช้ในการทดสอบ ตามปกตินิยมใช้ข้อมูลทดสอบในกรณีต่อไปนี้

1. เมื่อส่วนสำคัญของระบบการควบคุมขึ้นอยู่กับการออกแบบโปรแกรมที่ใช้

2. มีช่องว่างระหว่างการตรวจสอบยอนไปหาเอกสารขั้นต้นจนยากหรือเป็นไปไม่ได้ที่จะติดตามขบวนการประมวลผลข้อมูลตั้งแต่ต้นจนสำเร็จเป็นผลลัพธ์ขั้นสุดท้าย ดังนั้นการที่จะรับรองความถูกต้องของผลลัพธ์ได้หรือไม่นั้นจึงขึ้นอยู่กับความถูกต้องของขบวนการประมวลผลข้อมูลและโปรแกรมที่ใช้เป็นสำคัญ การใช้วิธีการทดสอบข้อมูลเป็นวิธีง่ายในการที่จะพิสูจน์ความถูกต้องของขบวนการประมวลผลข้อมูลและโปรแกรมที่ใช้

3. ปริมาณข้อมูลที่จะทำการตรวจสอบมีมาก ดังนั้น การทดสอบความถูกต้องของขบวนการประมวลผลข้อมูลและโปรแกรมโดยใช้ข้อมูลทดสอบแล้วพิจารณาว่า จะให้ความเชื่อถือในขบวนการประมวลผลข้อมูลได้หรือไม่จึงเป็นวิธีที่ประหยัดและมีประสิทธิภาพมากกว่า



รูป 3.59 ขั้นตอนการตรวจสอบโดยการทดสอบข้อมูล