



บทที่ 5

## การวิเคราะห์ผลที่ได้จากการสำรวจ

จากการศึกษา สำรวจ และเก็บข้อมูลจากงานที่ใช้คอมพิวเตอร์ ในร้านค้าต่าง ๆ ภายในประเทศในบทก่อนนั้น ในที่นี้จะสรุปผลที่ได้จากการสำรวจ ทุกด้านของหน่วยงานทั้งของราชการ รัฐวิสาหกิจ และธุรกิจเอกชนรวมกัน แล้วจึงจะวิเคราะห์ผลที่ได้จากการสำรวจต่อไป

### 5.1 การสรุปผลจากการสำรวจ

#### 5.1.1 ด้านความปลอดภัย ความถูกต้อง และความลับเฉพาะใน ด้านคอมพิวเตอร์

##### 5.1.1.1 ระบบความปลอดภัยของเครื่องจักรอุปกรณ์ ระบบ โปรแกรม และแฟ้มข้อมูล ได้จัดทำดังนี้

#### 1. เตรียมระบบการป้องกันความเสียหายไว้ล่วงหน้า

##### ก. ด้านเครื่องจักรอุปกรณ์

- โดยทำความเข้าใจระหว่างงานในหลายหน่วยงาน ที่มีเครื่องคอมพิวเตอร์ด้วยกันว่า ถ้าเครื่องคอมพิวเตอร์ของหน่วยงานของสมาชิก ใดซักเครื่องก็สามารถให้บริการคอมพิวเตอร์ของสมาชิกที่ใดซักเครื่องได้

- โดยทำความเข้าใจกับบริษัทผู้ขายเครื่องคอมพิวเตอร์ ให้ให้บริการที่บริษัทใดกรณที่คอมพิวเตอร์ในหน่วยงานนั้นเสีย

- เตรียมเครื่องจักรอุปกรณ์ไว้ 2 ชุด เอาไว้ที่ทำงานเดียวกัน ซึ่งกรณีที่เกิดเครื่องเสีย ก็จะสามารถใช้อีกเครื่องได้ แต่ถ้า เกิดภัยอื่น ๆ เช่น ไฟไหม้ ก็ไม่สามารถป้องกันได้

ข. การระบบโปรแกรม

– โดยเก็บโปรแกรมระบบอีกชุดไว้ในเทปแม่เหล็ก หรือ  
จานแม่เหล็ก โดยอาจเก็บไว้ที่ทำงานหรือนอกที่ทำงาน

ค. การข้อมูล

– โดยการคัดลอกข้อมูลเป็นระยะ ๆ ในกรณีข้อมูลที่  
สำคัญเท่านั้น เช่น ข้อมูลทางการเงิน

2. เตรียมหาวิธีการทำให้ระบบกลับคืนมาใหม่เมื่อเกิดความ  
เสียหายแล้ว

ก. การเครื่องจักรอุปกรณ์

- โดยใช้วิธีการ back up ที่เตรียมไว้แล้ว
- โดยการขอให้ช่างซ่อมให้เสร็จในกรณีงานไม่เร่งด่วน

ข. การระบบโปรแกรม

- โดยใช้วิธีการ back up ที่เตรียมไว้แล้ว
- โดยการคัดลอกจากกระดาษพิมพ์ต่อเนื่องในกรณี

ของโปรแกรมที่ใช้ปฏิบัติงานเสียหาย

– โดยการคัดลอกจากหน่วยงานหรือบริษัทที่ใช้ระบบ  
การทำงานเดียวกันในกรณีของโปรแกรมระบบ หรือโปรแกรมสำเร็จรูปที่ใช้เสียหาย

ค. การข้อมูล

- โดยใช้วิธีการ back up ที่เตรียมไว้แล้ว

– ดูจากรายละเอียดประกอบการทำงานและตรวจสอบ  
ย้อนรอยไปยังเอกสารเบื้องต้นใด ซึ่งหน่วยงานส่วนมากโดยเฉพาะราชการจะมี  
ข้อมูลชุดเดียวเท่านั้นที่ใช้ปฏิบัติงาน และจากการทำงานของหน่วยงานเหล่านี้พบว่า  
ยังไม่เคยที่เพิ่มข้อมูลจะเกิดความเสียหายมากเนื่องจากการประมวลผล

### 3. ระบบความปลอดภัยที่สร้างขึ้นในโปรแกรมระบบ

- โดยการบันทึกรายการต่าง ๆ ที่เกิดขึ้นในรูปแบบของโปรแกรม Job Accounting System เท่านั้น ซึ่งเป็นโปรแกรมที่จะบอกถึงรายละเอียดของการทำงานของเครื่อง เวลาที่ใช้ในการทำงาน ชื่อเจ้าของงาน เป็นต้น โปรแกรมอันนี้ได้จากบริษัทผู้ขายเครื่องคอมพิวเตอร์
- โดยการติดตั้งระบบการบันทึกรายการต่าง ๆ ที่เกิดขึ้นอย่างสมบูรณ์ ซึ่งกำลังอยู่ในระหว่างดำเนินการ

#### 5.1.1.2 ระบบความถูกต้องของข้อมูล

1. ตรวจสอบโดยวิธีการประมวลผลแบบ on - line ซึ่งอาจเป็นระบบ on - line ที่เครื่องอุปกรณ์ปลายทางอยู่ที่เดียว หรืออยู่คนละที่กับเครื่องคอมพิวเตอร์ก็ได้ ซึ่งจะใช้วิธีการตรวจสอบควบตามจอที่วิบนอุปกรณ์ปลายทางนั้น ถ้าผิดก็แก้ไขทันทีในทุกระเบียงจอที่เป็นไปไคของแต่ละงานที่แตกต่างกัน แล้วจึงตรวจสอบด้วยวิธีประมวลผลเป็นชุดข้อมูลอีกครั้งหนึ่ง
2. ตรวจสอบโดยวิธีการประมวลผลเป็นชุดข้อมูล ทุกหน่วยงานมีการตรวจสอบอย่างมีเสมอ โดยจะเลือกวิธีการตรวจสอบให้เหมาะสมกับประเภทของงาน

#### 5.1.1.3 ระบบความลับเฉพาะของข้อมูล

ใช้วิธีการเข้ารหัสแบบธรรมดาเท่านั้น นอกจากรายการที่สำคัญบางอัน เช่น งานคานธนาการ จึงใช้วิธีใช้ตัวเลขตรวจสอบ

#### 5.1.2 คานความปลอดภัยของสถานที่ทำการ และสิ่งต่าง ๆ ภายนอกเครื่อง ใค้จัดทำดังนี้

##### 5.1.2.1 คานความปลอดภัยของสถานที่ทำการ

### 1. การเลือกตำแหน่งที่ตั้งของตึกคอมพิวเตอร์

เกือบทุกหน่วยงานที่มีเครื่องคอมพิวเตอร์ไม่ได้เลือกตำแหน่งที่ตั้งของตึกคอมพิวเตอร์ ทั้ง ๆ ที่การพิจารณาในด้านระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะในระบบคอมพิวเตอร์นี้จะต้องพิจารณาเป็นอันดับแรกก่อนการติดตั้งเครื่องคอมพิวเตอร์ ตามข้อเท็จจริงปัจจุบันหน่วยงานใดต้องการติดตั้งระบบเครื่องคอมพิวเตอร์หรือใช้บริการเครื่องคอมพิวเตอร์จากแหล่งอื่น ก็ต้องขออนุมัติจากคณะกรรมการพิจารณากำหนดนโยบายและการบริหารงานคอมพิวเตอร์ของรัฐ ถ้าได้รับอนุมัติแล้วจึงจะดำเนินการได้ และหน่วยงานที่ขออนุมัติไปนั้นก็ให้นำเครื่องคอมพิวเตอร์ไว้ที่หน่วยงานเดิมของตน และเมื่อพิจารณาขอบเขตการนำคอมพิวเตอร์มาใช้งานในระดับปัจจุบันก็ไม่เป็นการเสียหายแต่อย่างใด

### 2. ตึกคอมพิวเตอร์และห้องคอมพิวเตอร์

- ในด้านตึกคอมพิวเตอร์นั้น หน่วยงานราชการและรัฐวิสาหกิจส่วนมากไม่มีงบประมาณในค่านี้นั้น ส่วนเอกชนทำได้เพราะการขออนุมัติงบประมาณทำได้สะดวกกว่า

- ในด้านห้องคอมพิวเตอร์ หน่วยงานคอมพิวเตอร์ทั้งหลายจะมีห้องคอมพิวเตอร์ที่ถูกต้อง ทั้งนี้ เพราะทางบริษัทผู้ขายหรือให้เช่าเครื่องจะบริการในส่วนใหญ่ ๆ ที่จำเป็น

- เกือบทุกหน่วยงานทั้งของราชการ รัฐวิสาหกิจ และเอกชนจะมีแต่ละห้องที่โซทำงานของผู้วิเคราะห์ระบบ ผู้เขียนโปรแกรม ผู้ดูแลแฟ้มข้อมูล หรือตำแหน่งอื่นเหล่านั้นไม่มีความสัมพันธ์กัน จะใช้ห้องที่ว่างอยู่หรืออาจอยู่คนละตึก

### 3. การควบคุมการเช่าออกภายในตึกคอมพิวเตอร์

หน่วยงานราชการ รัฐวิสาหกิจ เกือบทุกแห่งมีระเบียบการควบคุมการเช่าออกภายในตึกคอมพิวเตอร์โดยมียามรักษาการณ์ข้างนอกตึก

ที่เป็นที่ตั้งของเครื่องคอมพิวเตอร์อย่างไม่เข้มงวดเท่ากับของเอกชน เพราะส่วนใหญ่ใช้การรู้จัก ความคุ้นเคย ก็จะอนุญาตให้เข้าได้โดยไม่ต้องมีบัตรขออนุญาตแสดง

#### 4. ระเบียบวิธีปฏิบัติภายในห้องคอมพิวเตอร์

- ทุกหน่วยงานใ้คว่างระเบียบไว้ โดยเฉพาะหน่วยงานเอกชนจะเคร่งครัดมาก มีการตรวจสอบทุกชั้นตอน ส่วนมากห้องนี้จะเข้าได้เฉพาะเจ้าหน้าที่ควบคุมเครื่องเท่านั้น แต่หน่วยราชการบางแห่งที่ให้บริการภายนอกก็จะให้เจ้าของงานนำงานไปประมวลผลตัวเอง
- หน่วยงานหลายแห่ง ในห้องเครื่องคอมพิวเตอร์จะวางของที่ไม่ใช่ซึ่งไม่จำเป็น เช่น เทปแม่เหล็กที่ยังไม่ได้ใช้ กระดาษพิมพ์ต่อเนื่อง และบัตรเจาะรู ซึ่งอาจเป็นเหตุให้เกิดไฟไหม้ หรืออาจเกิดอันตรายต่อเทปแม่เหล็กเหล่านี้ถ้าบังเอิญมีบุคคลใดที่สามารถเข้ามาในห้องนี้ได้ และนำเอาแม่เหล็กเข้ามาโดยตั้งใจหรือไม่ตั้งใจ ก็จะทำให้เทปแม่เหล็กเสียหายได้

#### 5. ความปลอดภัยของห้องพัก

เกือบทุกหน่วยงานที่มีเครื่องคอมพิวเตอร์จะไม่มีห้องพักสำหรับยามรักษาการณ์ที่จะตรวจดูความปลอดภัยในอาคาร ทั้งนี้ เพราะศูนย์คอมพิวเตอร์ในประเทศไทยไม่เป็นศูนย์ขนาดใหญ่ การประมวลผลข้อมูลก็ไม่ใช่เป็นความลับมาก ดังนั้น ส่วนมากจะมีเฉพาะยามรักษาการณ์บริเวณทางเข้าเท่านั้น

##### 5.1.2.2 สิ่งต่าง ๆ ภายนอกเครื่อง

1. การป้องกันการบุกรุกของผู้ที่เข้ามายังห้อง

คอมพิวเตอร์

เกือบทุกหน่วยงานใช้วิธีออกระเบียบปฏิบัติ โดยห้ามบุคคลที่ไม่เกี่ยวข้องหรือไม่เป็นผู้ควบคุมเครื่องเข้ามายังห้องคอมพิวเตอร์ และไม่ได้ติดตั้งเครื่องมือที่ให้อภัยเมื่อมีภัยโดยไม่ต้องมีคนควบคุม

## 2.. การป้องกันไฟไหม้

- หน่วยงานคอมพิวเตอร์เกือบทุกแห่งใช้อุปกรณ์

ดับเพลิงชนิดที่ใช่มนุษย์

- ส่วนมากไม่ติดตั้งอุปกรณ์ดับเพลิงอัตโนมัติ

เลย เพราะแพงมาก และไม่ติดตั้งอุปกรณ์ที่ให้อภัยเมื่อมีไฟไหม้

## 3.. การส่งข้อมูลทางสายโทรศัพท์

ไม่ได้พิจารณา เนื่องจากขอบเขตการนำ

คอมพิวเตอร์มาใช้ในประเทศไทยยังไม่มาก

## 4. การรับข่าวสารโดยวิธีอื่น

งานนี้ไม่ได้พิจารณาเพราะระดับข้อมูลของการ

ทำงานไม่เป็นความลับมาก

5.1.3 ด้านการควบคุมงานในด้านการบริหารรวมทั้งเจ้าหน้าที่ปฏิบัติการ  
ได้จัดทำดังนี้

### 5.1.3.1 ด้านทั่วไป

หน่วยงานส่วนมากไม่ได้พิจารณาในด้านตัวบุคคลที่จะมีผลต่อความปลอดภัยของระบบงาน นอกจากบางแห่งสืบประวัติของบุคคลที่เข้ามาทำงานตามระเบียบทั่วไปของทั้งองค์การเท่านั้น

### 5.1.3.2 ด้านการควบคุมภายใน

- ทุกหน่วยงานจัดระเบียบวิธีปฏิบัติในค่านเหล่านี้

คือ การควบคุมข้อมูลเบื้องต้น การควบคุมระหว่างประมวลผล การควบคุมผลลัพธ์ และการควบคุมการทำเอกสารรายละเอียดประกอบ

- ส่วนการควบคุมด้านการปฏิบัติงาน เช่น ควบคุมการเปลี่ยนแปลงโปรแกรมที่ไซ ควบคุมแฟ้มข้อมูล ควบคุมรักษาความปลอดภัยของข้อมูลและโปรแกรมที่ไซ ควบคุมการเข้าสู่สถานที่ตั้งเครื่องคอมพิวเตอร์ และควบคุมการใช้การแก้ไขระหว่างการปฏิบัติงาน เป็นต้น หน่วยงานส่วนมากไม่ค่อยพิจารณาในด้านนี้

- สำหรับการจัดองค์การของหน่วยงานของศูนย์คอมพิวเตอร์นั้น หน่วยงานเอกชนส่วนมากจะแยกออกเป็นอิสระมีฐานะเท่ากับหน่วยงานอื่น ๆ ในองค์กรนั้น ส่วนของราชการและรัฐวิสาหกิจ ถ้าหน่วยงานคอมพิวเตอร์ขององค์กรนั้นเป็นหน่วยงานขนาดเล็กก็จะเป็นหน่วยงานที่ขึ้นกับแผนกบัญชีหรือการเงิน

- ส่วนการควบคุมคุณภาพของงานที่ได้นั้น หน่วยงานส่วนมากไม่ค่อยมีการวิเคราะห์เพื่อทำเป็นสถิติต่อไป

### 5.1.3.3 คานงงบประมาณ

- ในด้านความปลอดภัย หน่วยงานของราชการจะใ้คางงบประมาณเพียงครั้งเดียวเฉพาะตอนติดตั้งเครื่องคอมพิวเตอร์ ซึ่งส่วนมากก็จะไม่ใ้คางงบประมาณเพื่อในคานนี้เลย ส่วนของเอกชนจะใ้คางงบประมาณเรื่อย ๆ ตามที่ขอไปตามเหตุผล ซึ่งส่วนมากก็คักคางตามความจำเป็นตามระดับความสำคัญของงานเท่านั้น

- ในด้านความถูกต้อง จะใ้คางงบประมาณเฉพาะการประมวลผลข้อมูล ซึ่งขึ้นกับปฏิบัติการว่าคองการในระดับใด

- คานความลับเฉพาะ หน่วยงานส่วนมากไม่จัดสรรเฉพาะในคานนี้ เพราะระดับงานในเมืองไทยไม่มีความลับมากเกินไป

### 5.1.3.4 คานตรวจสอบ

- หน่วยงานคอมพิวเตอร์ส่วนมากยังไม่ใ้คางการตรวจสอบทุกคานของระบบคอมพิวเตอร์อย่างสมบูรณ์ ทำเฉพาะในระดับ

ผู้ตรวจสอบงานค่านับบัญชีและการเงินของธนาคารเท่านั้น ซึ่งเจ้าหน้าที่อาจรู้หรือไม่รู้เรื่องเกี่ยวกับคอมพิวเตอร์ก็ได้ ในกรณีที่ไม่มีการตรวจสอบ ควรเป็นหน้าที่ของเจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวกับคอมพิวเตอร์ในหน่วยงานนั้น ช่วยดูแล

## 5.2 การวิเคราะห์ผล

### 5.2.1 ภัยที่อาจเกิดขึ้น ได้แก่

#### 1. เกิดโดยทั่วไป เช่น

- ไฟไหม้
- ความหายนะอื่น ๆ เช่น การบุกรุกทำลาย การจลาจล

เป็นต้น

#### 2. เกิดโดยความประมาทของคน เช่น

- ความผิดพลาดในการเจาะบัตร
- ความผิดพลาดของผู้ส่งข้อมูลเข้า ณ อุปกรณ์ปลายทาง
- ความผิดพลาดของเจ้าหน้าที่ผู้ควบคุมเครื่อง
- การหยิบเทปแม่เหล็กผิดความ
- โปรแกรมที่เขียนมาจากการบอกกล่าวเงื่อนไข

ที่เข้าใจผิด

- เกิดอุบัติเหตุในระหว่างการทดสอบโปรแกรม

#### 3. เกิดขึ้นโดยความผิดพลาดของเครื่องจักรและโปรแกรม เช่น

- เครื่องคอมพิวเตอร์ที่ล้าสมัย
- แฟ้มข้อมูลเสียหายเนื่องจากการประมวลผล
- เทปแม่เหล็กเสียหายเป็นบางส่วน เนื่องจากโปรแกรม

#### 4. เกิดโดยการประสงคร้ายจากคน เช่น

- โดยการลักขโมยข้อมูล เช่น ข้อมูลของบริษัทคู่แข่งชั้น
- โดยการขโมย
- โดยการตั้งใจทำลาย



- โดยการบังเอิญ เช่น มีอุปกรณ์แม่เหล็ก
- ผิดพลาดโดยไม่ตั้งใจทำให้เทปแม่เหล็กถูกลบไป
- โดยผู้ควบคุมเครื่องที่มีเจตนาร้าย
- โดยผู้เขียนโปรแกรมที่มีเจตนาร้าย
- โดยเจ้าหน้าที่เก็บรักษาแฟ้มข้อมูลที่มีเจตนาร้าย
- โดยผู้ควบคุมเครื่อง ณ อุปกรณ์ปลายทางที่มีเจตนาร้าย
- โดยผู้ใช้ที่มีเจตนาร้าย

### 5.2.2 เหตุที่ทำให้เกิดความผิดพลาดในระบบคอมพิวเตอร์ ได้แก่

1. ความผิดพลาดจากเครื่องอุปกรณ์ โดยปกติเครื่องคอมพิวเตอร์มีระบบตรวจเช็คตัวมันเองอยู่แล้ว
2. ความผิดพลาดจากระบบโปรแกรม ป้องกันโดย
  - ใช้โปรแกรมที่มีคุณภาพดี
  - ไม่เปลี่ยนระบบใหม่ ๆ บ่อย
  - มีการทดสอบทุกเงื่อนไขที่เป็นไปได้โดยละเอียด
3. ความผิดพลาดของโปรแกรมที่ใส่แต่ละงาน ป้องกันโดย
  - ทดสอบโปรแกรมอย่างละเอียด
  - ควบคุมการทำงานของโปรแกรมไม่ให้มีการทุจริตได้ในกรณีงานสำคัญ
    - ควบคุมโปรแกรมที่แยกเขียนเป็นส่วน ๆ เหล่านั้น
4. ความผิดพลาดจากผู้ควบคุมเครื่อง ป้องกันโดย
  - กำหนดระเบียบวิธีปฏิบัติให้ชัดเจนเพื่อให้ผู้ควบคุมเครื่องเข้าใจอย่างชัดเจนแจ่มแจ้งทุกขั้นตอนและไม่เข้าใจผิดได้
  - กำหนดการทดสอบในตัวโปรแกรมเพื่อไม่ให้ผู้ควบคุมเครื่องหยิบแฟ้มข้อมูลผิด

- บันทึกรายละเอียดการทำงานของผู้ควบคุมเครื่อง  
และตรวจสอบบ่อย ๆ

- มีการฝึกหัด และทดสอบการทำงานของผู้ควบคุม  
เครื่องเป็นครั้งคราว

#### 5. ข้อมูลเบื้องต้น ป้องกันโดย

- ให้มีการตรวจทานบัตร

- ใช้วิธีควบคุมชุดข้อมูล

- ตรวจเช็คข้อมูลโดยการกวาดหา ( Scanning ) ข้อมูล

เช่น ตรวจสอบข้อมูลแต่ละชุด หรือหายอกรวมของรายการใดรายการหนึ่ง  
เป็นคน

ที่เกิดขึ้น

- ควบคุมคุณภาพของงาน โดยทำเป็นสถิติข้อผิดพลาด

#### 6. ระบบโปรแกรมออกแบบไม่ผิดพลาด ป้องกันโดย

- เลือกผู้วิเคราะห์ระบบที่มีความสามารถสูง

#### 5.2.3 ความเสียหายที่อาจเกิดขึ้นแก่แฟ้มข้อมูล ได้แก่

##### 1. ความผิดพลาดจากการเจาะบัตร ป้องกันโดย

- ใช้วิธีตรวจทานบัตร

- ใช้วิธีตรวจความถูกต้องของข้อมูล

##### 2. ความผิดพลาดจากโปรแกรม ป้องกันโดย

- ทดสอบโปรแกรมอย่างละเอียด

##### 3. อุบัติเหตุที่เกิดขึ้นระหว่างทดสอบโปรแกรม

- ไม่ควรใช้แฟ้มข้อมูลจริง เพื่อทดสอบ ควรคัดลอก

แฟ้มข้อมูลไว้ออน

##### 4. ใช้แฟ้มข้อมูลฝึก ป้องกันโดย

- วางระเบียบวิธีปฏิบัติแก่เจ้าหน้าที่ผู้เก็บรักษาแฟ้มข้อมูล

อย่างชัดเจนและเข้มงวด

- ตรวจสอบ Label ของแฟ้มข้อมูลก่อนทุกครั้ง
- 5. ความผิดพลาดจากผู้ควบคุมเครื่อง ป้องกันโดย
  - มีการฝึกหัดผู้ควบคุมเครื่องอย่างถี่
  - ออกระเบียบวิธีปฏิบัติอย่างชัดเจน เพื่อไม่ให้

ควบคุมเครื่องเข้าใจผิดได้

- 6. แฟ้มข้อมูลไม่ค้ ป้องกันโดย
  - ใช้เทปแม่เหล็กหรือจานแม่เหล็กที่มีคุณภาพดี
- 7. การขโมยแฟ้มข้อมูล ป้องกันโดย
  - เก็บในที่ที่ล็อคได้ และอาจมีสัญญาณเตือนภัยเมื่อมี

คนขโมย

- กวดขันการทำงานของเจ้าหน้าที่ดูแลแฟ้มข้อมูล

- 8. การรั่วข้อมูล ป้องกันโดย
  - กวดขันเลขหมายที่ให้ไว้กับเบอร์แฟ้มข้อมูล
  - กวดขันการทำงานของยูเซียนโปรแกรมในขณะทดสอบ

โปรแกรม ไม่อนุญาตให้ยูเซียนโปรแกรมเข้าไปควบคุมการทำงานของเครื่องคอมพิวเตอร์ และโปรแกรมที่สำคัญไม่ควรให้ยูเซียนโปรแกรมรู้อย่างละเอียดคนเกี่ยวข้องหมดตลอดโปรแกรม

- แยกการทำงานของยูเซียนโปรแกรมและผู้ควบคุม

เครื่องออกจากกันโดยเด็ดขาด

- ควบคุมข้อมูลเข้า
- ควบคุมระหว่างประมวลผล
- ควบคุมการทำงานในห้องคอมพิวเตอร์
- ควบคุมรายละเอียดเอกสารประกอบ
- ควบคุมการจัดการในก้านบริหาร
- ควรวิธีวิธีการตรวจสอบเป็นบางครั้ง
- ควบคุมการปฏิบัติงานของเจ้าหน้าที่ในหน่วยงานเพื่อ

ไม่ให้สมรู้ร่วมคิดกัน เช่น ไม่ควรให้บุคคลที่เป็นญาติใกล้ชิดทำงานเดียวกันหรือ

ไม่ให้คนใดคนหนึ่งรับผิดชอบงานหลายอย่างในเวลาเดียวกัน หรือรับผิดชอบระบบงานทั้งหมดที่สำคัญแต่เพียงผู้เดียว

- ควบคุมการทำงานล่วงเวลา
- ตรวจสอบพื้นที่ ความประพฤติกของผูปฏิบัติงาน
- การจ้างผู้เชี่ยวชาญภายนอกควรมีคระวังเป็นพิเศษ

### 5.3 ปัญหาที่ไ้จากการสำรวจ

1. ด้านความปลอดภัยในคานสถานที่ทำการ เกือบทุกแห่งไม่คำนึงถึงมากนัก อย่างน้อยที่สุดควรติดตั้งอุปกรณ์ดับเพลิงชนิดที่ไซคนช่วย เพราะบางแห่งไม่มีอุปกรณ์ดับเพลิงเลย

2. ด้านความปลอดภัยของแฟ้มข้อมูล มีหลายหน่วยงานที่ไม่มีระเบียบวิธีปฏิบัติในคานการจัดเก็บอย่างชัดเจน โดยเฉพาะศูนย์คอมพิวเตอร์ที่ให้บริการภายนอกแก่หน่วยงานอื่น แฟ้มข้อมูลของผูไซจะเก็บไม่เรียบร้อย ซึ่งอาจเกิดความเสียหายโดยการเจตนาหรือไม่เจตนาได้

3. การสำรวจในคานความปลอดภัย ความถูกต้อง และความลับเฉพาะในคานระบบคอมพิวเตอร์นี้ ทำไม่ได้เต็มที่ทุกคาน ทุกหน่วยงาน เพราะข้อมูลเกี่ยวกับคานนี้จะเป็นความลับ ถ้าเปิดเผยแล้วจะเกิดความเสียหายอย่างร้ายแรงต่อหน่วยงานตนเองได้ อย่างไรก็ตาม ข้อมูลที่ไ้ก็พอเพียงที่จะศึกษาในคานนี้

4. คานงบประมาณที่ไ้ไม่มากพอที่จะจัดระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะในระบบคอมพิวเตอร์ให้สมบูรณ์ได้

5. เจ้าหน้าที่ที่ปฏิบัติงานของแต่ละตำแหน่งในหน่วยงานคอมพิวเตอร์ส่วนมากยังขาดแคลนมาก จึงทำให้ระบบเหล่านี้ไม่ไ้พอ

#### 5.4 สรุปจากการสำรวจ

1. ปัจจุบันขอบเขตการใช้งานด้วยคอมพิวเตอร์ไม่ใช่เทคนิคที่ซับซ้อนมากเกินไป ใช้เทคนิคเบื้องต้นอย่างง่าย ๆ และระดับข้อมูลก็ไม่สำคัญ และเป็นความลับมากนัก
2. ในอนาคตจะต้องมีการใช้เทคนิคในการทำงานเพิ่มมากขึ้น ดังนั้นควรพิจารณาคานระบบความปลอดภัย ความถูกต้อง และความลับเฉพาะในระบบคอมพิวเตอร์ก่อนเป็นอันดับแรก
3. การทำวิจัยครั้งนี้ทำในลักษณะผสมระหว่างการวิจัยเชิงเอกสาร (Documentary Research ) และการวิจัยเชิงสำรวจ (Survey Research) ดังนั้นข้อมูลที่ได้อาจจะมีการทดลองปฏิบัติเพื่อพิสูจน์ยืนยันให้แน่นอนอีก แต่คิดว่า การเสนอข้อมูลเหล่านี้จะเป็นการโน้มนำ กระตุ้นหรือท้าทายให้เกิดการศึกษา ค้นคว้า และพัฒนาความรู้ในกานระบบนี้ให้กว้างขวางยิ่งขึ้น