# การบริหารความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการ กรณีศึกษาโรงพยาบาลแห่งหนึ่ง

นาย เนติ จินดามาตย์



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมอุตสาหการ ภาควิชาวิศวกรรมอุตสาหการ
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2550

# RISK MANAGEMENT FOR COMPUTER AND INTERNET USING IN ENTERPRISE CASE STUDY OF A HOSPITAL

Mr. Nati Chindamat



A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Engineering Program in Industrial Engineering

Department of Industrial Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2007

| | |
|---|---|
| หัวข้อวิทยานิพนธ์ | การบริหารความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการ กรณีศึกษาโรงพยาบาลแห่งหนึ่ง |
| โดย | นายเนติ จินดามาตย์ |
| สาขาวิชา | วิศวกรรมอุตสาหการ |
| อาจารย์ที่ปรึกษา | รองศาสตราจารย์ ดร.วันชัย ริจิรวนิช |

---

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้วิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร. ดิเรก ลาวัณย์ศิริ)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร. ปารเมศ ชุติมา)

..... อาจารย์ที่ปรึกษา
(รองศาสตราจารย์ ดร. วันชัย ริจิรวนิช)

..... กรรมการ
(รองศาสตราจารย์ จีรพัฒน์ เงาประเสริฐวงศ์)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ สุทัศน์ รัตนเกื้อกังวาน)

เนติ จินดามาตย์ : การบริหารความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการ กรณีศึกษาโรงพยาบาลแห่งหนึ่ง (RISK MANAGEMENT FOR COMPUTER AND INTERNET USING IN ENTERPRISE CASE STUDY OF A HOSPITAL) อ.ที่ปรึกษา: รศ.ดร. วันชัย ริจิรวนิช , 203 หน้า

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาลักษณะและผลกระทบของความเสี่ยงที่เกิดขึ้นจากการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการและสร้างแผนบริหารความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการกรณีศึกษา โดยการวิจัยครั้งนี้ได้ทำการวิจัยในโรงพยาบาลขนาดใหญ่

ขั้นตอนการวิจัยเริ่มจากการศึกษาระบบงานของโรงพยาบาลทั้งหมดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และอินเตอร์เน็ต จากนั้นจึงทำการระบุความเสี่ยงและประเมินความเสี่ยงโดยใช้ค่า RPN (Risk Priority Number) จากนั้นจึงทำการสร้างแผนจัดการความเสี่ยงซึ่งในขั้นตอนนี้ได้นำเอาวิธีการวิเคราะห์แขนงความบกพร่องมาช่วยในการวิเคราะห์หาสาเหตุพื้นฐานของการเกิดความเสี่ยง และขั้นตอนสุดท้ายคือการติดตามผลของแผนจัดการความเสี่ยงโดยใช้วิธีการประเมินความเสี่ยงแบบคาดหมาย

การวิจัยพบว่าความเสี่ยงที่เกิดขึ้นจากการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการกรณีศึกษาส่วนใหญ่มีสาเหตุมาจากปัจจัยภายในและส่วนใหญ่เกิดจากการใช้งานของบุคลากร ส่วนแผนจัดการความเสี่ยงที่สร้างขึ้นนั้นจากการติดตามผลพบว่าสามารถทำให้ระดับของความเสี่ยงที่อยู่ในระดับที่ยอมรับไม่ได้ลดลงอยู่ในระดับที่ยอมรับได้และแผนจัดการความเสี่ยงที่ได้สร้างขึ้นนั้น สามารถนำไปประยุกต์ใช้ในสถานประกอบการอื่นๆได้อีกด้วย



ภาควิชา วิศวกรรมอุตสาหการ ลายมือชื่อนิสิต เนติ จินดามาตย์

สาขาวิชา วิศวกรรมอุตสาหการ ลายมือชื่ออาจารย์ที่ปรึกษา

ปีการศึกษา 2550

## 4870678921 : MAJOR INDUSTRIAL ENGINEERING

KEY WORD : RISK MANAGEMENT / COMPUTER AND INTERNET

NATI CHINDAMAT : RISK MANAGEMENT FOR COMPUTER AND INTERNET USING IN ENTERPRISE CASE STUDY OF A HOSPITAL. THESIS ADVISOR : ASSOC. PROF. VANCHAI RIJIRAVANICH, Ph.D, 203 pp

The Objectives of this research is to study characteristics and impacts of risks from using computers and internets in enterprises, in order to develop risk management plan of using these technologies in studied enterprises. A big-scaled hospital was chosen as studied enterprises.

The first step of this research was studying every work activities related with computers and internet usages, after that, risks of these technologies were indicated and assessed by using RPN (Risk Priority Number). The second step of this research was developing risk management plan. In this step, causes and roots of risks were considered by FTA (Fault Tree Analysis). And the last step of the research was following up the results of developed risk management plan by expected risk assessment method.

Research results indicated that risks from using computers and internet in studied hospital mainly caused by internal factors, and mostly from personnel's usability. Outcomes after the implement shown that risk management plan developed from this research improved unacceptable risk level to acceptable level. The developed risk management plan also could be apply in other enterprises.



Department .. INDUSTRIAL ENGINEERRING ... Student ' s signature .....

Concentration ..... INDUSTRIAL ENGINEERRING Advisor ' s signature .....

Academic year ..... 2007

# กิตติกรรมประกาศ

วิทยานิพนธ์เล่มนี้สำเร็จลุล่วงไปได้ด้วยดี ผู้วิจัยต้องขอขอบพระคุณ รศ.ดร.วันชัย ริจิรวนิช อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่กรุณาให้คำปรึกษาแนะนำแนวทางในการทำวิจัยและเสียสละเวลาตรวจแก้ไขข้อผิดพลาดต่างๆที่เกิดขึ้น และต้องขอขอบพระคุณ รศ.ดร.ปารเมศ ชุติมา, รศ.จิรพัฒน์ เงาประเสริฐวงศ์ และ ผศ.สุทัศน์ รัตนเกื้อกังวาน ที่ได้กรุณาให้คำแนะนำที่เป็นประโยชน์ในการทำวิจัยในครั้งนี้

ขอขอบพระคุณท่านผู้อำนวยการโรงพยาบาลจุฬาลงกรณ์ ที่ให้ความกรุณาอนุญาตให้เก็บข้อมูลและทำวิจัยภายในโรงพยาบาลจุฬาลงกรณ์ และต้องขอขอบพระคุณบุคลากรในฝ่ายงานต่างๆของโรงพยาบาลจุฬาลงกรณ์ที่กรุณาให้ความร่วมมือในการอนุเคราะห์ข้อมูลต่างๆในการทำวิจัย

ขอบใจเพื่อนๆ ทุกคน ที่ได้ให้คำแนะนำและคอยช่วยเหลือในด้านต่างๆที่จำเป็นในการทำวิจัยครั้งนี้ รวมทั้งกำลังใจที่มีให้กัน

และที่จะขาดเสียมิได้ผู้วิจัยต้องขอกราบขอบพระคุณ คุณพ่อวิโรจน์ จินดามาตย์ ผู้ที่ได้ล่วงลับไปแล้ว และ คุณแม่จินดา จินดามาตย์ ที่ได้อบรมสั่งสอนและดูแลลูกคนนี้ด้วยดีเสมอมา และขอขอบคุณ พี่เสาและพี่รัตน์ พี่สาวทั้งสองคนที่คอยดูแลและได้ให้คำแนะนำต่างๆเป็นอย่างดี

# สารบัญ

หน้า

หน้า

หน้า

# สารบัญตาราง

หน้า

หน้า

หน้า

หน้า

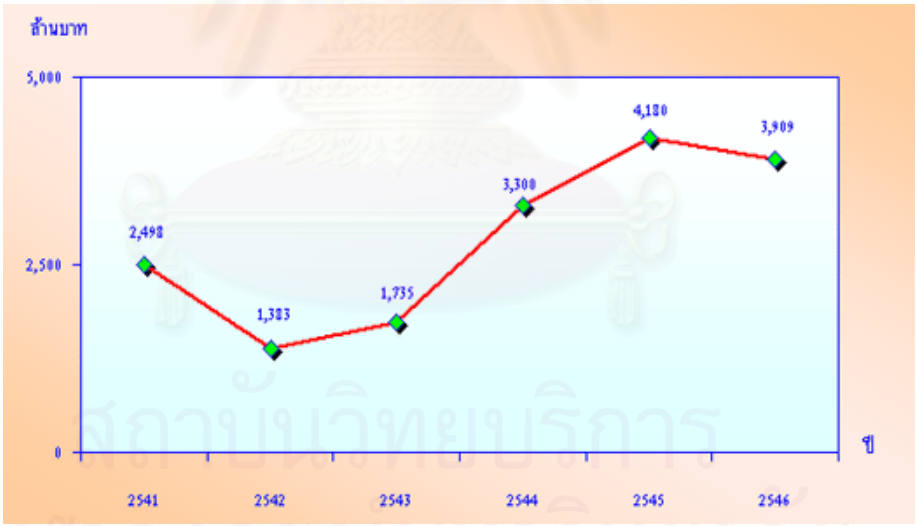
# สารบัญภาพ

หน้า

หน้า

# บทที่1
# บทนำ

ในปัจจุบัน เทคโนโลยีสารสนเทศมีบทบาทอย่างมากในการดำเนินงานหรือการทำกิจกรรมด้านต่างๆในหลายๆวงการ ส่งผลให้ประเทศที่เจริญแล้ว ยิ่งก้าวหน้าไปอย่างรวดเร็วมาก ทำให้ความเหลื่อมล้ำของการพัฒนาเศรษฐกิจและสังคมมีมากขึ้นตามลำดับ ประเทศไทยเองก็อยู่ในระหว่างการปรับตัวเพื่อนำความรู้และเทคโนโลยีมาเป็นพื้นฐานสำคัญในการพัฒนาประเทศ เพื่อให้สามารถยกระดับความสามารถในการแข่งขันได้ในสังคมแห่งภูมิปัญญา และการเรียนรู้ (Knowledge based economy) แม้ว่าในช่วงวิกฤติเศรษฐกิจที่ผ่านมานั้น เศรษฐกิจไทยมีแนวโน้มชะลอตัวลงทำให้เป็นข้อจำกัดในการพัฒนาในเรื่องนี้ แต่รัฐบาลได้ให้ความสำคัญกับการพัฒนาเทคโนโลยีและการสื่อสารเป็นอย่างมาก เห็นได้จากงบประมาณด้านเทคโนโลยีสารสนเทศของภาครัฐในปี พ.ศ. 2541-2546 มีแนวโน้มที่เพิ่มขึ้น ดังรูปที่ 1.1




รูปที่ 1.1 งบประมาณด้านเทคโนโลยีสารสนเทศของภาครัฐ (ฮาร์ดแวร์และซอฟต์แวร์)

ที่มา : Thailand ICT indicators, NECTEC

หมายเหตุ : ไม่รวมงบประมาณด้านการอบรมเทคโนโลยีสารสนเทศ

ซึ่งในปี พ.ศ.2545 รัฐบาลไทยได้จัดตั้งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร หรือกระทรวงไอซีทีขึ้น เมื่อวันที่ 3 ตุลาคม พ.ศ.2545 เพื่อสร้างความแข็งแกร่งให้กับภาครัฐและเอกชน

ทางด้านเทคโนโลยีสารสนเทศและการสื่อสารอีกทั้งยังเป็นการยกระดับคุณภาพชีวิตของประชาชนชาวไทยทางด้านการรับรู้ข้อมูลข่าวสาร พร้อมกันนี้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้กำหนดยุทธศาสตร์การพัฒนาในแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย พ.ศ. 2545 - 2549 ไว้ดังนี้

1) พัฒนาอุตสาหกรรม ICT เพื่อให้เป็นผู้นำในภูมิภาค
2) ใช้ ICT เพื่อยกระดับคุณภาพชีวิตของคนไทยและสังคมไทย
3) ปฏิรูปและการสร้างศักยภาพการวิจัยและพัฒนา ICT
4) ยกระดับศักยภาพพื้นฐานของสังคมไทยเพื่อการแข่งขันในอนาคต
5) พัฒนาศักยภาพของผู้ประกอบการ เพื่อมุ่งขยายตลาดต่างประเทศ
6) ส่งเสริมผู้ประกอบการขนาดกลางและขนาดย่อมให้ใช้ ICT
7) นำ ICT มาใช้ประโยชน์ในการบริหารและการให้บริการของภาครัฐ

และจากยุทธศาสตร์การพัฒนาแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทยทั้งเจ็ดข้อนี้ โดยเฉพาะข้อที่ 6) ที่ระบุเอาไว้ว่า “ ส่งเสริมผู้ประกอบการขนาดกลางและขนาดย่อมให้ใช้ ICT ” ส่งผลให้สถานประกอบการในประเทศไทยมีการนำเอาเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานหรือทำกิจกรรมต่างๆในสถานประกอบการมากขึ้น โดยอ้างอิงจากผลการสำรวจของสำนักงานสถิติแห่งชาติ ซึ่งได้ทำการสำรวจการใช้คอมพิวเตอร์และการใช้อินเตอร์เน็ตในสถานประกอบการที่ตั้งอยู่ในกรุงเทพมหานครและเขตเทศบาลทั่วราชอาณาจักรในปี พ.ศ. 2547-2549 โดยสถานประกอบการ ณ ที่นี้ หมายถึง สถานประกอบการที่มีคนทำงานตั้งแต่ 1 คนขึ้นไป(ไม่นับรวมแผงลอย) ซึ่งมีการประกอบกิจกรรมดังต่อไปนี้

1.) ธุรกิจและบริการ
2.) การผลิต
3.) การก่อสร้าง
4.) การขนส่งทางบกและตัวแทนธุรกิจการท่องเที่ยว
5.) โรงพยาบาล

ซึ่งผลการสำรวจที่ได้มีดังต่อไปนี้

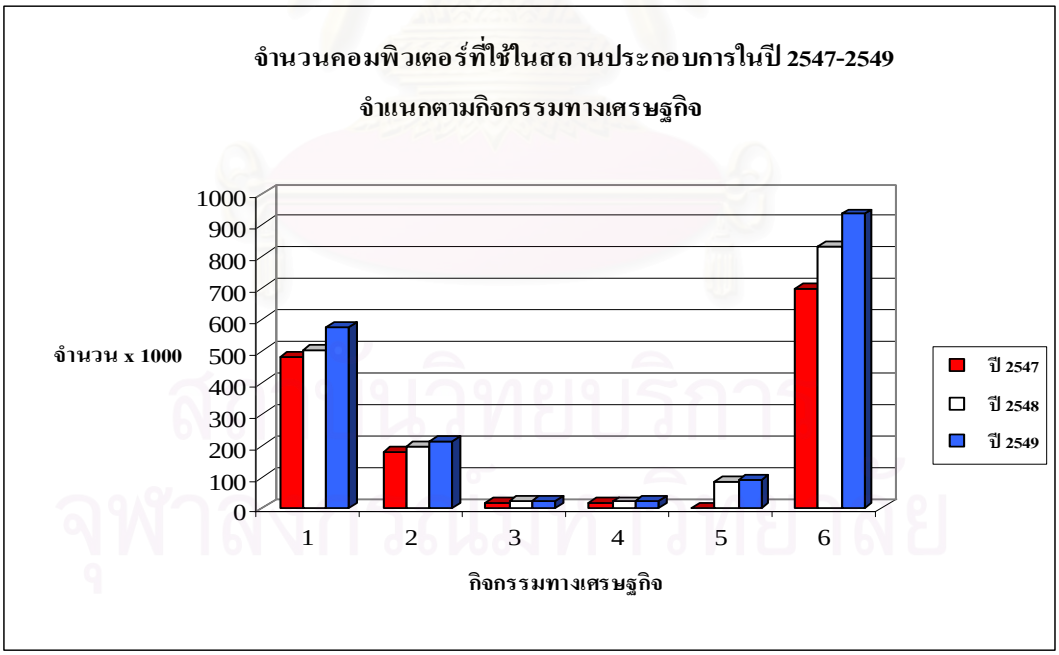
ตารางที่ 1.1 จำนวนคอมพิวเตอร์ที่ใช้ในสถานประกอบการในปี 2547-2549 จำแนกตามกิจกรรมทางเศรษฐกิจ

หน่วย : 1000

| กิจกรรมทางเศรษฐกิจ | ปี 2547 | ปี 2548 | ปี 2549 |
|---|---|---|---|
| 1. ธุรกิจและบริการ | 481.1 | 502.8 | 574.5 |
| 2. การผลิต | 179.1 | 197.1 | 215.3 |
| 3. การก่อสร้าง | 20.9 | 23.5 | 26.2 |
| 4. การขนส่งทางบกและตัวแทนธุรกิจการท่องเที่ยว | 18.0 | 21.8 | 24.7 |
| 5. โรงพยาบาล | - | 86.4 | 93.4 |
| 6. รวม | 699.2 | 831.6 | 934.1 |

ที่มา : การสำรวจข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. 2547-2549 สำนักงานสถิติแห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

หมายเหตุ : ปี 2547 การสำรวจไม่คุ้มรวมกิจกรรมด้านโรงพยาบาล




รูปที่ 1.2 จำนวนคอมพิวเตอร์ที่ใช้ในสถานประกอบการในปี 2547-2549 จำแนกตามกิจกรรมทางเศรษฐกิจ

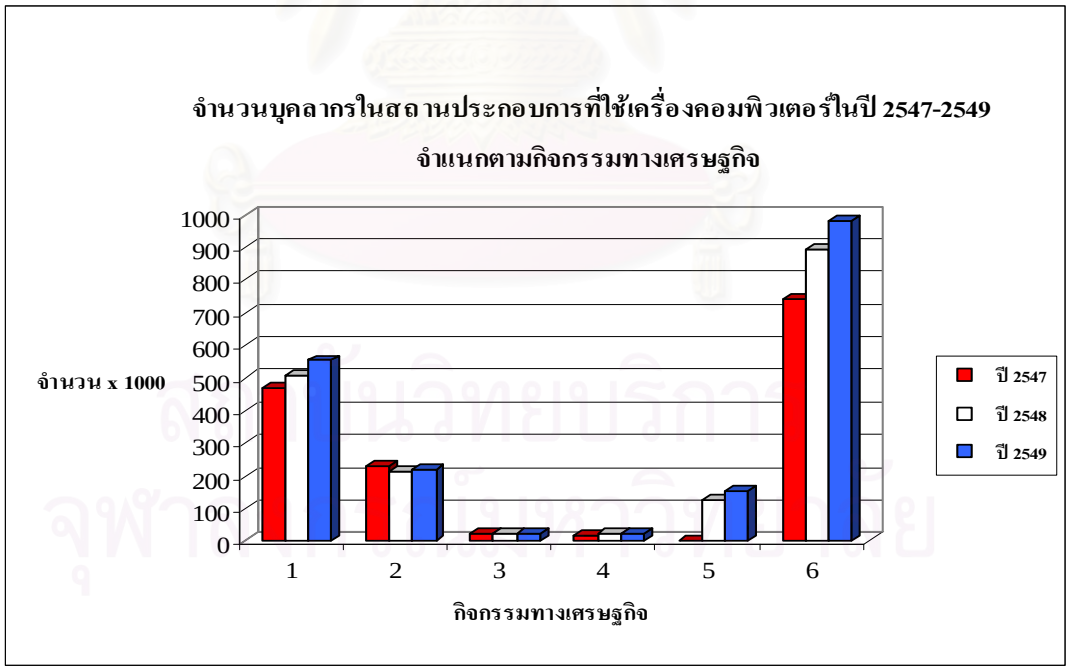
ตารางที่ 1.2 บุคลากรที่ใช้เครื่องคอมพิวเตอร์ในปี 2547-2549 จำแนกตามกิจกรรมทางเศรษฐกิจ

หน่วย : 1000

| กิจกรรมทางเศรษฐกิจ | ปี 2547 | ปี 2548 | ปี 2549 |
|---|---|---|---|
| 1. ธุรกิจและบริการ | 470.5 | 507.8 | 554.4 |
| 2. การผลิต | 231.8 | 212.4 | 219.6 |
| 3. การก่อสร้าง | 21.8 | 25.7 | 25.6 |
| 4. การขนส่งทางบกและตัวแทนธุรกิจการท่องเที่ยว | 17.2 | 23.0 | 23.9 |
| 5. โรงพยาบาล | - | 127.9 | 156.6 |
| 6. รวม | 741.3 | 896.8 | 980.2 |

ที่มา : การสำรวจข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. 2547-2549 สำนักงานสถิติแห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

หมายเหตุ : ปี 2547 การสำรวจไม่คุ้มรวมกิจกรรมด้านโรงพยาบาล



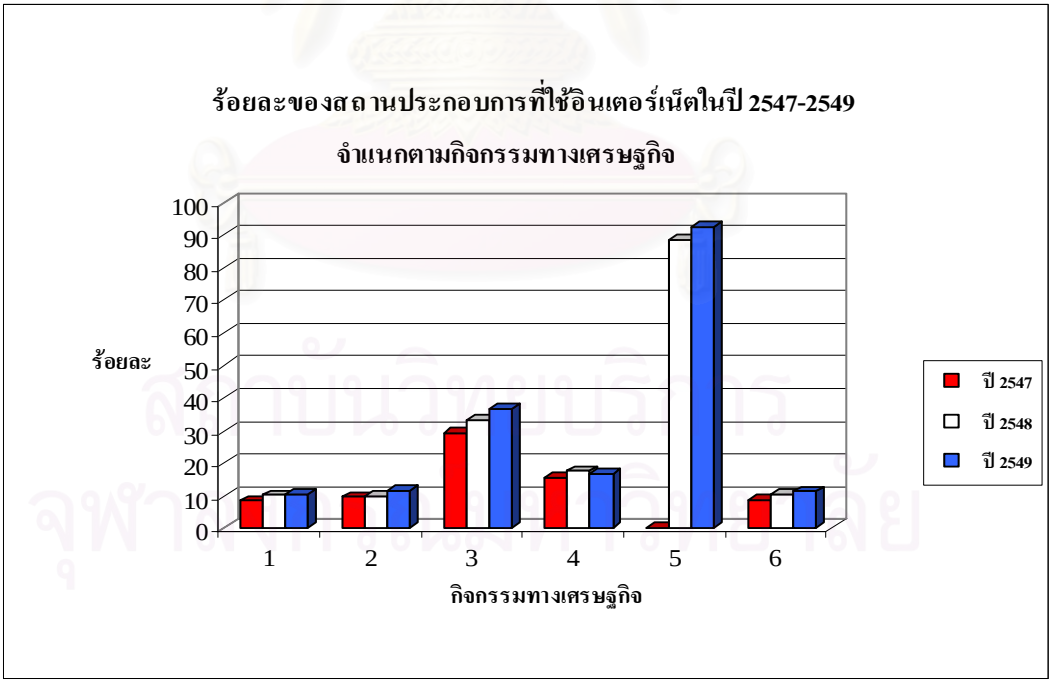

รูปที่ 1.3บุคลากรที่ใช้เครื่องคอมพิวเตอร์ในปี 2547-2549 จำแนกตามกิจกรรมทางเศรษฐกิจ

ตารางที่ 1.3 ร้อยละของสถานประกอบการที่ใช้อินเทอร์เน็ต ปี 2547-2549 จำแนกตามกิจกรรมทางเศรษฐกิจ

| กิจกรรมทางเศรษฐกิจ | ปี 2547 | ปี 2548 | ปี 2549 |
|---|---|---|---|
| 1. ธุรกิจและบริการ | 8.5 | 10.2 | 10.6 |
| 2. การผลิต | 9.6 | 10.1 | 11.8 |
| 3. การก่อสร้าง | 29.3 | 33.1 | 36.6 |
| 4. การขนส่งทางบกและตัวแทนธุรกิจการท่องเที่ยว | 15.4 | 17.6 | 16.9 |
| 5. โรงพยาบาล | - | 88.5 | 92.6 |
| 6. รวม | 9.0 | 10.7 | 11.3 |

ที่มา : การสำรวจข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. 2547-2549 สำนักงานสถิติแห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

หมายเหตุ : ปี 2547 การสำรวจไม่คุ้มรวมกิจกรรมด้านโรงพยาบาล




รูปที่ 1.4 ร้อยละของสถานประกอบการที่ใช้อินเทอร์เน็ต ปี 2547-2549 จำแนกตามกิจกรรมทางเศรษฐกิจ

จากผลการสำรวจแสดงให้เห็นเป็นรูปธรรมว่าการนำเอาเทคโนโลยีสารสนเทศมาใช้ในสถานประกอบการในปี พ.ศ.2547-2549 นั้นมีแนวโน้มเพิ่มขึ้นทุกปี เห็นได้จากจำนวนคอมพิวเตอร์และจำนวนบุคลากรที่ใช้คอมพิวเตอร์ รวมไปถึงการใช้อินเตอร์เน็ตในสถานประกอบการมีแนวโน้มเพิ่มขึ้นทุกปี แต่อย่างไรก็ตามการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการในประเทศไทยยังเป็นเรื่องที่ใหม่มาก เห็นได้จากรัฐบาลพึ่งเริ่มมีการสนับสนุนในเรื่องของเทคโนโลยีสารสนเทศอย่างจริงจังในปี พ.ศ. 2545 โดยการตั้งกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารขึ้นมา และได้กำหนดยุทธศาสตร์การพัฒนาในแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทยขึ้นในปี พ.ศ.2545 หรือเมื่อประมาณ 4 ปีที่ผ่านมา ดังนั้นการนำเอาเทคโนโลยีสารสนเทศมาใช้ในสถานประกอบการจึงมีปัญหาและอุปสรรคต่างๆเกิดขึ้น โดยอ้างอิงข้อมูลจากผลการสำรวจของสำนักงานสถิติแห่งชาติ ในหัวข้อเรื่องร้อยละของสถานประกอบการ จำแนกตามปัญหาและอุปสรรคในการใช้เทคโนโลยีสารสนเทศในสถานประกอบการ ในปี พ.ศ.2547 และ พ.ศ.2548 ซึ่งผลการสำรวจมีดังต่อไปนี้

ตารางที่ 1.4 ร้อยละของสถานประกอบการจำแนกตามปัญหาและอุปสรรคที่พบมากในการนำเอาเทคโนโลยีสารสนเทศมาใช้ในสถานประกอบการในปี พ.ศ.2547

| ปัญหา / กิจกรรมทางเศรษฐกิจ | กิจกรรมที่ 1 | กิจกรรมที่ 2 | กิจกรรมที่ 3 | กิจกรรมที่ 4 |
|---|---|---|---|---|
| ค่าใช้จ่ายสูงเกินไป | 23.3 | 22.6 | 34.2 | 25.2 |
| เทคโนโลยีเปลี่ยนแปลงเร็วเกินไป | 23.4 | 22.1 | 35.7 | 23.9 |
| ลูกจ้างไม่มีทักษะในการใช้งาน/มีความลังเลที่จะใช้ | 18.4 | 17.4 | 33.0 | 17.6 |
| คัดเลือกลูกจ้างที่มีคุณสมบัติเหมาะสมยาก | 17.2 | 15.8 | 29.8 | 16.0 |
| ค่าใช้จ่ายในการเชื่อมต่ออินเตอร์เน็ตสูงเกินไป | 15.8 | 14.0 | 25.5 | 17.3 |
| เทคโนโลยีมีความซับซ้อนเกินไป | 15.6 | 14.1 | 27.5 | 16.9 |
| ปัญหาเรื่องความปลอดภัย | 13.6 | 12.5 | 28.2 | 15.8 |
| การรับส่งข้อมูลช้าเกินไปหรือไม่แน่นอน | 12.5 | 11.5 | 26.4 | 14.8 |
| พนักงานสูญเสียเวลากับการใช้เว็บไซท์ที่ไม่เกี่ยวข้อง | 10.0 | 9.1 | 20.6 | 11.3 |

ตารางที่ 1.4 ร้อยละของสถานประกอบการ จำแนกตามปัญหาและอุปสรรคที่พบมากในการนำเอาเทคโนโลยีสารสนเทศมาใช้ในสถานประกอบการ ในปี พ.ศ.2547 (ต่อ)

| ปัญหา / กิจกรรมทางเศรษฐกิจ | กิจกรรมที่ 1 | กิจกรรมที่ 2 | กิจกรรมที่ 3 | กิจกรรมที่ 4 |
|---|---|---|---|---|
| สินค้าและบริการไม่เหมาะสมกับการขายทาง internet | 9.1 | 8.0 | 12.0 | 8.6 |
| ลูกค้ายังไม่พร้อมที่จะใช้อีคอมเมิร์ซ | 6.7 | 5.6 | 9.6 | 7.5 |
| ค่าใช้จ่ายในการพัฒนาและบำรุงเว็บไซท์สูงเกินไป | 6.3 | 5.4 | 9.8 | 6.7 |
| ค่าใช้จ่ายในการพัฒนาและบำรุงรักษาอีคอมเมิร์ซสูงไป | 5.7 | 4.7 | 8.6 | 6.2 |
| ปัญหาเรื่องความปลอดภัยของการชำระเงินค่าสินค้า | 5.6 | 4.5 | 7.9 | 5.7 |
| ความไม่แน่นอนเกี่ยวกับสัญญาข้อตกลงในการส่งสินค้าและการรับประกัน | 5.3 | 4.4 | 7.2 | 5.1 |
| ปัญหาเรื่องการจัดส่งสินค้า | 5.1 | 4.2 | 7.2 | 4.9 |
| กฎหมายหรือระเบียบเกี่ยวกับอีคอมเมิร์ซ | 4.6 | 3.9 | 6.4 | 4.6 |

หมายเหตุ 1. ธุรกิจและบริการ 2. การผลิต 3. การก่อสร้าง 4. การขนส่งทางบกและตัวแทนธุรกิจการท่องเที่ยว

ที่มา : การสำรวจข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. 2547 สำนักงานสถิติแห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ตารางที่ 1.5 ร้อยละของสถานประกอบการจำแนกตามปัญหาและอุปสรรคที่พบมากในการนำเอาเทคโนโลยีสารสนเทศมาใช้ในสถานประกอบการในปี พ.ศ.2548

| ปัญหา / กิจกรรมทางเศรษฐกิจ | กิจกรรมที่ 1 | กิจกรรมที่ 2 | กิจกรรมที่ 3 | กิจกรรมที่ 4 | กิจกรรมที่ 5 |
|---|---|---|---|---|---|
| ค่าใช้จ่ายสูงเกินไป | 10.1 | 9.0 | 11.6 | 8.2 | 28.4 |
| เทคโนโลยีเปลี่ยนแปลงเร็วเกินไป | 10.0 | 8.5 | 14.6 | 7.7 | 26.5 |
| ลูกจ้างไม่มีทักษะในการใช้งาน/มีความลังเลที่จะใช้ | 8.0 | 7.0 | 10.7 | 5.7 | 33.1 |
| คัดเลือกลูกจ้างที่มีคุณสมบัติเหมาะสมยาก | 7.1 | 6.2 | 10.4 | 5.0 | 30.6 |
| ค่าใช้จ่ายในการเชื่อมต่ออินเตอร์เน็ตสูงเกินไป | 7.1 | 5.4 | 8.4 | 7.3 | 22.7 |
| เทคโนโลยีมีความซับซ้อนเกินไป | 6.7 | 5.2 | 9.2 | 6.8 | 18.6 |
| ปัญหาเรื่องความปลอดภัย | 5.7 | 5.1 | 11.2 | 7.4 | 40.1 |
| การรับส่งข้อมูลช้าเกินไปหรือไม่แน่นอน | 5.1 | 4.0 | 10.1 | 6.0 | 33.1 |

ตารางที่ 1.5 ร้อยละของสถานประกอบการจำแนกตามปัญหาและอุปสรรคที่พบมากในการนำเอาเทคโนโลยีสารสนเทศมาใช้ในสถานประกอบการในปี พ.ศ.2548 (ต่อ)

| ปัญหา / กิจกรรมทางเศรษฐกิจ | กิจกรรมที่ 1 | กิจกรรมที่ 2 | กิจกรรมที่ 3 | กิจกรรมที่ 4 | กิจกรรมที่ 5 |
|---|---|---|---|---|---|
| พนักงานสูญเสียเวลากับการใช้เว็บไซท์ที่ไม่เกี่ยวข้อง | 3.6 | 3.0 | 6.9 | 4.4 | 22.2 |
| สินค้าและบริการไม่เหมาะสมกับการขายทาง internet | 4.1 | 3.4 | 6.1 | 2.6 | 8.7 |
| ลูกค้ายังไม่พร้อมที่จะใช้อีคอมเมิร์ซ | 3.2 | 2.5 | 5.4 | 2.8 | 10.5 |
| ค่าใช้จ่ายในการพัฒนาและบำรุงเว็บไซท์สูงเกินไป | 3.0 | 2.4 | 5.3 | 3.3 | 9.5 |
| ค่าใช้จ่ายในการพัฒนาและบำรุงรักษาอีคอมเมิร์ซสูงไป | 3.0 | 2.4 | 4.9 | 3.1 | 9.8 |
| ปัญหาเรื่องความปลอดภัยของการชำระเงินค่าสินค้า | 2.9 | 2.5 | 4.5 | 2.3 | 9.3 |
| ความไม่แน่นอนเกี่ยวกับสัญญาข้อตกลงในการส่งสินค้าและการรับประกัน | 2.8 | 2.3 | 4.4 | 2.4 | 8.9 |
| ปัญหาเรื่องการจัดส่งสินค้า | 2.5 | 2.0 | 4.4 | 2.0 | 6.9 |
| กฎหมายหรือระเบียบเกี่ยวกับอีคอมเมิร์ซ | 2.2 | 1.9 | 4.1 | 2.3 | 9.2 |

หมายเหตุ 1. ธุรกิจและบริการ 2. การผลิต 3. การก่อสร้าง 4. การขนส่งทางบกและตัวแทนธุรกิจการท่องเที่ยว 5. โรงพยาบาล

ที่มา : การสำรวจข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. 2548 สำนักงานสถิติแห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

**1.1 ความสำคัญของงานวิจัย**

การที่รัฐบาลได้จัดตั้งกระทรวงเทคโนโลยีสารสนเทศขึ้นมาในปี พ.ศ.2545 และกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้กำหนดยุทธศาสตร์การพัฒนาในแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย พ.ศ. 2545-2549 ขึ้นมาเจ็ดข้อ โดยมีอยู่ข้อหนึ่งได้ระบุเอาไว้ว่า ส่งเสริมให้ผู้ประกอบการขนาดกลางและขนาดย่อมนำเอาเทคโนโลยีสารสนเทศมาใช้ในสถานประกอบการ ส่งผลให้สถานประกอบการต่างๆนำเอาเทคโนโลยีสารสนเทศมาใช้ในสถานประกอบการเพิ่มขึ้นทุกปี เห็นได้จากการสำรวจของสำนักงานสถิติแห่งชาติ ในเรื่องของ จำนวนคอมพิวเตอร์ จำนวนบุคลากรที่ใช้คอมพิวเตอร์ และร้อยละของการใช้อินเตอร์เน็ต ในสถานประกอบการในปี 2547-2549 ซึ่งมีแนวโน้มเพิ่มขึ้นทุกปี

ซึ่งการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการนั้นช่วยเพิ่มศักยภาพในการทำงานด้านต่างๆให้กับสถานประกอบการเป็นอย่างมาก เช่น การเชื่อมโยงระบบสารสนเทศของสำนักงาน การทำธุรกรรมทางการเงิน ช่องทางการติดต่อสื่อสารโฆษณาประชาสัมพันธ์ การซื้อ/ขายสินค้า ติดตามความเคลื่อนไหวของตลาด รับ-ส่งข้อมูลทางอีเมล์ ค้นหาข้อมูล ติดต่อสอบถามข้อมูล รับคำสั่งซื้อสินค้าทางเว็บไซท์ ให้บริการหลังการขาย รับและ/หรือชำระเงิน

แต่การนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการนั้น ก็นำมาซึ่งความเสี่ยงในการเกิดปัญหาต่างๆมากมาย ซึ่งสำนักงานสถิติแห่งชาติก็ได้ทำการสำรวจปัญหาที่เกิดขึ้นในการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการเช่นกัน ซึ่งผลการสำรวจก็แสดงให้เห็นว่ายังมีปัญหาที่เกิดขึ้นอยู่มากในการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการ ซึ่งปัญหาที่เกิดขึ้นนั้นอาจจะยังไม่เกิดขึ้นกับทุกๆสถานประกอบการ แต่ก็ถือเป็นความเสี่ยงที่อาจจะเกิดขึ้นได้กับสถานประกอบการเช่นกันในอนาคตหากผู้ประกอบการไม่มีการบริหารจัดการที่ดี

เครื่องมือหนึ่งที่สามารถที่จะนำมาบริหารจัดการในเรื่องนี้ คือ “การบริหารจัดการความเสี่ยง” นั่นเอง ซึ่งหากพิจารณาข้อมูลจากการสำรวจของสำนักงานสถิติแห่งชาติในเรื่อง ปัญหาและอุปสรรคที่พบมากในการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการ สามารถสรุปปัญหาความเสี่ยงที่อาจจะเกิดขึ้นในการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการ ซึ่งเป็นปัญหาความเสี่ยงที่ผู้ประกอบการมีความจำเป็นอย่างยิ่งที่ต้องบริหารจัดการความเสี่ยงกับปัญหาความเสี่ยงเหล่านั้น โดยปัญหาความเสี่ยงต่างๆเหล่านั้นประกอบด้วย ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านเทคโนโลยี ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ ความเสี่ยงด้านกฎหมาย และความเสี่ยงด้านอื่นๆ โดยมีรายละเอียดคร่าวๆดังต่อไปนี้

**1.) ความเสี่ยงด้านบุคลากร**

บุคลากรนับเป็นปัจจัยที่สำคัญสำหรับทุกๆขั้นตอนในการทำงานอยู่แล้วดังนั้นในการนำคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการย่อมต้องมีความเสี่ยงอันเนื่องมาจากบุคลากรผู้ใช้งานคอมพิวเตอร์และอินเตอร์เน็ต เช่น บุคลากรขาดทักษะในการใช้งาน มีความลังเลที่จะใช้งาน บุคลากรสูญเสียเวลาไปกับการใช้เว็บไซท์ที่ไม่เกี่ยวข้อง หรือแม้แต่ความลำบากในการคัดเลือกคุณสมบัติที่เหมาะสมของบุคลากรใหม่ๆเข้ามาทำงานในตำแหน่งที่ต้องมีการใช้งานคอมพิวเตอร์และอินเตอร์เน็ต เป็นต้น

**2.) ความเสี่ยงด้านเทคโนโลยี**

ความเสี่ยงด้านเทคโนโลยีนั้นนับเป็นประเด็นที่สำคัญมากประเด็นหนึ่งในการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการซึ่งผู้ประกอบการจะมองข้ามไม่ได้สำหรับความเสี่ยงด้านเทคโนโลยี เช่น เทคโนโลยีมีความเปลี่ยนแปลงเร็วเกินไป เทคโนโลยีมีความซับซ้อนเกินไป หรือแม้แต่ภัยคุกคามต่างๆด้านเทคโนโลยี เช่น ไวรัสคอมพิวเตอร์ เป็นต้น ซึ่งผู้ประกอบการมีความจำเป็นอย่างยิ่งที่จะต้องมีการวางแผนเตรียมที่จะรับมือกับความเสี่ยงด้านเทคโนโลยีที่อาจจะเกิดขึ้นจากการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการ

**3.) ความเสี่ยงด้านข้อมูล**

การนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการนั้นวัตถุประสงค์หลักในการนำเอามาใช้คือการนำมาจัดการกับข้อมูลต่างๆที่เกี่ยวข้องกับการดำเนินงานของสถานประกอบการนั้นๆ ดังนั้นความเสี่ยงด้านข้อมูลจึงนับเป็นความเสี่ยงอีกด้านหนึ่งที่จะละเลยไม่ได้และต้องให้ความสำคัญกับมัน สำหรับความเสี่ยงด้านข้อมูลนั้นก็มีอยู่หลายรูปแบบด้วยกัน เช่น ความผิดพลาดคลาดเคลื่อนของข้อมูล ไม่มีการอัพเดทข้อมูล ถ่ายโอนข้อมูลไม่ได้ ข้อมูลสูญหาย เป็นต้น

**4.) ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์**

ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์จัดว่าเป็นความเสี่ยงอีกด้านหนึ่งที่จะมองข้ามไม่ได้ในการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการเพราะฮาร์ดแวร์และซอฟท์แวร์ ถือว่าเป็นองค์ประกอบที่สำคัญมากในการใช้งานคอมพิวเตอร์และอินเตอร์เน็ต สำหรับความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ก็มีอยู่หลายรูปแบบ เช่น เลือกฮาร์ดแวร์และซอฟท์แวร์ไม่เหมาะสมกับการใช้งาน ความบกพร่องของฮาร์ดแวร์และซอฟท์แวร์ ค่าใช้จ่ายด้านการบำรุงรักษาฮาร์ดแวร์สูง ซอฟท์แวร์ใช้งานยาก เป็นต้น

**5.) ความเสี่ยงด้านกฎหมาย**

เนื่องจากการนำคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการนั้นยังเป็นเรื่องที่ค่อนข้างใหม่สำหรับสถานประกอบการในประเทศไทย จะเห็นได้จากในปัจจุบัน(พ.ศ.2549) ประเทศไทยมีกฎหมายที่มารองรับเกี่ยวกับการใช้คอมพิวเตอร์และอินเตอร์เน็ตเพียงหนึ่งฉบับคือ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และอยู่ในระหว่างยกร่างอีกหนึ่งฉบับคือ ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งยังไม่มีผลบังคับใช้ ดังนั้นจึงมีความเป็นไปได้สูงว่ากฎหมายที่มีผลบังใช้อยู่นั้นอาจจะยังไม่ครอบคลุม หรือคุ้มครองในทุกเรื่อง

เกี่ยวกับการใช้งานคอมพิวเตอร์และอินเตอร์เน็ต เนื่องจากเป็นกฎหมายเก่าที่ออกมาหลายปีแล้ว ดังนั้น ผู้ประกอบการต้องมีการศึกษากฎหมายให้ดีเพื่อป้องกันปัญหาความเสี่ยงด้านกฎหมายที่อาจจะเกิดขึ้น นอกจากนี้ยังมีความเสี่ยงด้านกฎหมายอีกลักษณะหนึ่งคือ การที่สถานประกอบการทำผิดกฎหมายเสียเอง เช่น การละเมิดลิขสิทธิ์ด้านซอฟท์แวร์โดยไม่เจตนา เป็นต้น

**6.) ความเสี่ยงด้านอื่นๆ**

นอกจากปัญหาความเสี่ยงด้านต่างๆที่ได้กล่าวมาแล้ว การนำคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการยังมีความเสี่ยงด้านอื่นๆอีกหลายๆด้าน เช่น ลูกค้ายังไม่พร้อมที่จะใช้บริการ การรับส่งข้อมูลที่ไม่แน่นอน ระบบอินเตอร์เน็ตล่ม เป็นต้น ซึ่งปัญหาความเสี่ยงด้านอื่นๆเหล่านี้ก็เป็นสิ่งที่ผู้ประกอบการจะละเลยไม่ได้เช่นกัน ดังนั้นหากสถานประกอบการต่างๆมีการบริหารความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการ ก็จะช่วยป้องกันหรือลดความเสี่ยงที่อาจจะเกิดขึ้น ซึ่งจะส่งผลให้การนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการเกิดประโยชน์สูงสุด รวมทั้งลดความสูญเสียต่างๆที่อาจจะเกิดขึ้นกับสถานประกอบการในการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการอีกด้วย

## 1.2 วัตถุประสงค์ของการวิจัย

วัตถุประสงค์ของการวิจัยมีดังต่อไปนี้

(1) เพื่อศึกษาลักษณะและผลกระทบของความเสี่ยงที่เกิดขึ้นจากการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการ
(2) สร้างแผนบริหารความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการกรณีศึกษา

## 1.3 ขั้นตอนการดำเนินงานวิจัย

ขั้นตอนในการดำเนินงานวิจัยมีดังต่อไปนี้

(1) ศึกษาทฤษฎี บทความและงานวิจัยที่เกี่ยวข้อง
(2) ค้นคว้าและศึกษาข้อมูลการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการ

(3) ติดต่อสถานประกอบการเพื่อศึกษาและสร้างแผนบริหารความเสี่ยง

(4) ศึกษาขั้นตอนการดำเนินงานในสถานประกอบการพร้อมทั้งระบุขั้นตอนการดำเนินงานที่เกี่ยวข้องกับคอมพิวเตอร์และอินเตอร์เน็ต

(5) ทำการระบุความเสี่ยงและประเมินความเสี่ยงในด้านของความรุนแรงของความเสี่ยง (Severity; S) โอกาสในการเกิดความเสี่ยง(Occurrence; O) และความสามารถในการตรวจจับความ เสี่ยง(Detection; D) เพื่อจัดระดับความเสี่ยงตามค่าตัวเลขความวิกฤต Risk Priority Number หรือ ค่า RPN

(6) สร้างแผนบริหารความเสี่ยงตามระดับความเสี่ยงโดยนำวิธีการวิเคราะห์แขนงความบกพร่อง (Fault Tree Analysis ; FTA) มาประยุกต์ใช้

(7) นำเสนอแผนบริหารความเสี่ยงให้ผู้ที่เกี่ยวข้องทำการประเมินแก้ไขตามความเหมาะสม

(8) ติดตามผลของแผนบริหารความเสี่ยงโดยใช้การประเมินความเสี่ยงแบบคาดหมาย (Expected) เพื่อเปรียบเทียบค่า RPN ของความเสี่ยงก่อนและหลังจากมีแผนบริหารจัดการความเสี่ยง

(9) สรุปผลการศึกษาวิจัย

(10) จัดทำรูปเล่มวิทยานิพนธ์

**1.4 ขอบเขตของการวิจัย**

ขอบเขตของการศึกษามีดังนี้

(1) การจัดทำแผนบริหารความเสี่ยงจะครอบคลุมการดำเนินงานในสถานประกอบการกรณีศึกษาเฉพาะช่วงเวลาที่ทำการศึกษาวิจัยเท่านั้น

(2) การติดตามผลของแผนบริหารความเสี่ยงจะใช้การประเมินความเสี่ยงแบบคาดหมาย (Expected) เพื่อเปรียบเทียบค่า RPN ของความเสี่ยงก่อนและหลังจากมีแผนบริหารความเสี่ยง

**1.5 ประโยชน์ที่ได้รับ**

ประโยชน์ที่คาดว่าจะได้รับมีดังนี้

(1) มีความรู้ความเข้าใจในลักษณะและผลกระทบของความเสี่ยงที่เกิดขึ้นของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการ

(2) ได้แผนบริหารความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการกรณีศึกษา เพื่อใช้ในสถานประกอบการกรณีศึกษา

(3) เป็นแนวทางในการทำแผนบริหารความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการของสถานประกอบการอื่นๆ

# บทที่ 2
# ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในการศึกษาทฤษฎีที่เกี่ยวข้อง มีการศึกษาทฤษฎีด้านการบริหารความเสี่ยง และทฤษฎีด้านการวิเคราะห์แขนงความบกพร่อง (Fault Tree Analysis; FTA)

## 2.1 การบริหารความเสี่ยง

### 2.1.1 ความหมายและคำจำกัดความต่างๆของการบริหารความเสี่ยง

ความเสี่ยง(Risk) หมายถึง เหตุการณ์ที่ไม่แน่นอนที่อาจเกิดขึ้นในอนาคต แล้วส่งผลกระทบในแง่ลบ หรือ ขัดขวางการบรรลุวัตถุประสงค์ (คู่มือการบริหารความเสี่ยง การไฟฟ้านครหลวง, 2547)

ปัจจัยเสี่ยง(Risk Factor) หมายถึง สาเหตุหรือปัจจัยทั้งภายในและภายนอก ซึ่งสามารถก่อให้เกิดความเสี่ยงขึ้นได้ (คู่มือการบริหารความเสี่ยง การไฟฟ้านครหลวง, 2547)

การระบุความเสี่ยง(Risk Identification) หมายถึง การจะกำหนดว่าเหตุการณ์ใดเป็นความเสี่ยง โดยพิจารณาจากวัตถุประสงค์ที่ตั้งไว้เป็นหลัก (ธารชุดา อมรเพชรกุล, 2546)

การประเมินความเสี่ยง (Risk Assessment ) หมายถึง กระบวนการที่ใช้ในการระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยงหรือการบริหารความเสี่ยง (นพ.โสภณ เมฆธน, กรมอนามัย)

ระดับความเสี่ยง(Risk Score) หมายถึง ความสมดุลระหว่างความเสี่ยงและการควบคุมสามารถพิจารณาจากการประเมินความเสี่ยง และจุดตัดความเสี่ยง (Risk Cut Off) ประกอบการพิจารณาระดับผลกระทบ (Impact Score) และระดับโอกาสในการเกิด (Likelihood Score) (คู่มือการบริหารความเสี่ยง การไฟฟ้านครหลวง, 2547)

การบริหารความเสี่ยง(Risk Management) หมายถึง การกำหนดแนวทางและกระบวนการในการบ่งชี้ วิเคราะห์ ประเมิน จัดการ และติดตามความเสี่ยงที่เกี่ยวข้องกับกิจกรรม หน่วยงาน หรือกระบวนการ

ดำเนินงานขององค์กร รวมทั้งการกำหนดวิธีการในการบริหารและควบคุมความเสี่ยงให้อยู่ในระดับที่ผู้บริหารยอมรับได้ (คู่มือการบริหารความเสี่ยง การไฟฟ้านครหลวง, 2547)

**2.1.2 ขั้นตอนการบริหารความเสี่ยง**

ขั้นตอนการบริหารความเสี่ยงหลัก ๆ มี 5 ขั้นตอนดังต่อไปนี้

**ขั้นตอนที่ 1** การกำหนดวัตถุประสงค์ของการดำเนินงาน (Understand Objectives)

การกำหนดวัตถุประสงค์ของการดำเนินงานจะช่วยให้เข้าใจสภาพการดำเนินงานของสถานประกอบการ สามารถระบุและกำหนดขอบเขตของสิ่งที่ส่งผลกระทบต่อสถานประกอบการ ทั้งที่มาจากปัจจัยภายนอกและปัจจัยภายในซึ่งปัจจัยต่างๆเหล่านี้จะช่วยให้สถานประกอบการสามารถกำหนดวัตถุประสงค์การดำเนินงานได้อย่างชัดเจนและเป็นไปในทิศทางเดียวกัน

**ขั้นตอนที่ 2** การระบุความเสี่ยง (Risk Identification)

การระบุความเสี่ยง คือ การระบุและจัดกลุ่มประเด็นความเสี่ยง ตามสาเหตุที่ทำให้ความเสี่ยงนั้นเกิดขึ้น ซึ่งขั้นตอนการระบุความเสี่ยงมีดังนี้

1. พิจารณาว่าในการดำเนินงานมีกิจกรรมหรือกระบวนการใดบ้างที่เกี่ยวข้องกับวัตถุประสงค์ของการดำเนินงานในแต่ละข้อ

2. พิจารณาว่าในแต่ละกิจกรรมหรือกระบวนการนั้น มีปัจจัยหรือเหตุการณ์ใดบ้างที่จะส่งผลให้สถานประกอบการไม่สามารถดำเนินการตามกิจกรรมนั้นๆได้ โดยให้พิจารณาถึงความเป็นไปได้ทุกๆรูปแบบหรือพิจารณาความเสี่ยงทุกประเภทให้ครอบคลุมมากที่สุด

3. ทำการระบุความเสี่ยง (Risk Identification) ที่ได้เพื่อนำมาเป็นข้อมูลในการประเมินความเสี่ยงต่อไป

**ขั้นตอนที่ 3** การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง มีวัตถุประสงค์เพื่อวิเคราะห์และประเมินค่าของความเสี่ยงแต่ละข้อแล้วจึงนำมาทำการจัดระดับค่า RPN ตามคะแนนที่ได้ โดยมีปัจจัยที่นำมาพิจารณา 3 ปัจจัย คือ

ก. ความรุนแรงของความเสี่ยง (Severity; S)

ตารางที่ 2.1 การกำหนดระดับความรุนแรงของความเสี่ยง (S)

| ระดับคะแนน | ความรุนแรง | ความหมาย |
|---|---|---|
| 1 | น้อยมาก | ■ เสียเวลาการทำงานน้อยมาก<br>■ ส่งผลกระทบต่อผู้ป่วยน้อยมาก |
| 2 | น้อย | ■ เสียเวลาการทำงานน้อย<br>■ ส่งผลกระทบต่อผู้ป่วยน้อย |
| 3 | ปานกลาง | ■ เสียเวลาการทำงานปานกลาง<br>■ ส่งผลกระทบต่อผู้ป่วยปานกลาง |
| 4 | มาก | ■ เสียเวลาการทำงานมาก<br>■ ส่งผลกระทบต่อผู้ป่วยมาก |
| 5 | มากที่สุด | ■ เสียเวลาการทำงานมากที่สุด<br>■ ส่งผลกระทบต่อผู้ป่วยมากที่สุด<br>■ ขัดต่อกฎหมาย |

ข. โอกาสในการเกิดความเสี่ยง (Occurrence; O)

ตารางที่ 2.2 การกำหนดระดับโอกาสในการเกิดความเสี่ยง (O)

| ระดับคะแนน | โอกาสเกิด | ความหมาย |
|---|---|---|
| 1 | น้อยมาก | ■ เกิดได้เฉพาะสถานการณ์ผิดปกติ : ทุกปี |
| 2 | น้อย | ■ สามารถเกิดขึ้นได้น้อยครั้ง : ทุก 6 เดือน |
| 3 | ปานกลาง | ■ อาจเกิดขึ้นได้บ้าง บางโอกาส : ทุกเดือน |
| 4 | มาก | ■ เกิดขึ้นได้เป็นปกติมักเกิดซ้ำบ่อยๆ : ทุกสัปดาห์ |
| 5 | มากที่สุด | ■ ไม่สามารถหลีกเลี่ยงได้ มีโอกาสเกิดสูงมาก : ทุกวัน |

ค. ความสามารถในการตรวจพบความเสี่ยง (Detection; D)

ตารางที่ 2.3 การกำหนดระดับความสามารถในการตรวจพบความเสี่ยง (D)

| ระดับคะแนน | ประสิทธิภาพ | ความหมาย |
|---|---|---|
| 1 | สูงที่สุด | ▪ สามารถตรวจพบได้แน่นอนเป็นส่วนใหญ่/มีการควบคุมที่ดีมาก |
| 2 | สูง | ▪ มีโอกาสสูงในการตรวจพบ/มีการควบคุมที่ดี |
| 3 | ปานกลาง | ▪ อาจตรวจพบได้ในบางครั้ง/มีการควบคุมปานกลาง |
| 4 | ต่ำ | ▪ มีโอกาสตรวจพบน้อยมาก/มีการควบคุมที่ไม่ค่อยดี |
| 5 | ต่ำมาก | ▪ ไม่สามารถตรวจพบได้เลย/ไม่มีการควบคุม |

จากนั้นจะนำคะแนนทั้ง 3 ส่วนมาคูณกัน ได้ค่าที่เรียกว่า ตัวเลขความเสี่ยงชี้นำหรือความวิกฤต (Risk Priority Number) หรือ RPN โดยความเสี่ยงที่มีค่า RPN สูง หมายถึง ความเสี่ยงที่มีความรุนแรงสูง มีโอกาสเกิดได้บ่อยครั้ง และ ระบบในปัจจุบันตรวจพบได้ยาก จึงควรเร่งจัดการป้องกันแก้ไขก่อน ในทางตรงกันข้าม ความเสี่ยงที่มีค่า RPN ต่ำ จะ หมายถึงว่า ความเสี่ยงนั้น ๆ ก่อให้เกิดความเสียหายน้อย มีโอกาสเกิดได้ไม่บ่อย และ สามารถตรวจพบได้ดีอยู่แล้ว

**ขั้นตอนที่ 4** การจัดการความเสี่ยง (Response to Risks)

การจัดการความเสี่ยง เป็นการกำหนดแนวทางที่เหมาะสมเพื่อจัดการต่อความเสี่ยงที่ไม่สามารถยอมรับได้ สามารถจำแนกออกได้เป็น 4 แนวทาง ดังนี้

ก. Take – การยอมรับความเสี่ยง (Risk Acceptance)

คือ การยอมรับให้มีความเสี่ยงนั้นๆปรากฏอยู่ เนื่องจากค่าใช้จ่ายในการจัดการหรือสร้างระบบการควบคุม มีมูลค่าสูงกว่าผลลัพธ์ที่ได้จากการแก้ไขความเสียหายที่อาจเกิดขึ้น อย่างไรก็ตาม เราก็ควรมีมาตรการในการจัดการเพื่อให้สามารถติดตามและดูแลความเสี่ยงนั้นๆ

ข. Treat – การลด/ควบคุมความเสี่ยง (Risk Reduction/Control)

คือ การออกแบบระบบการควบคุมภายใน การแก้ไขปรับปรุงในด้านองค์กร, ทิศทางขององค์กร, การปฏิบัติงาน และ การติดตามตรวจสอบ เพื่อป้องกันหรือจำกัดผลกระทบและโอกาสที่จะเกิดเหตุการณ์ความเสียหาย

ค. Terminate – การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)

เป็นการหลีกเลี่ยงหยุด หรือเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น การหยุดทำกิจกรรมนั้นๆ การปรับเปลี่ยนรูปแบบการดำเนินการหรือระบบต่างๆเป็นต้น

ง. Transfer – การกระจาย/โอนความเสี่ยง (Risk Sharing/Spreading)

คือ การกระจายความเสี่ยงในสินทรัพย์ หรือกระบวนการต่างๆเพื่อลดความสูญเสีย เช่น การทำประกันความเสียหายที่อาจจะเกิดขึ้น ได้แก่ การประกันภัย, การจ้างบุคคลภายนอก (Outsource) ซึ่งเป็นการถ่ายโอนความเสี่ยงไปยังบริษัทประกันและบริษัทภายนอก, การทำสำเนาเอกสารหลายๆชุด และการกระจายที่เก็บทรัพย์สินค่า เป็นต้น

**ขั้นตอนที่ 5** การติดตามผล (Monitoring)

ผู้รับผิดชอบด้านการบริหารความเสี่ยงจะทำหน้าที่ติดตามและประเมินผลการจัดการความเสี่ยงอย่างสม่ำเสมอ โดยทำการทบทวนปัจจัยเสี่ยงและนโยบายที่เกี่ยวข้อง ที่อาจเปลี่ยนแปลงไป เพื่อทบทวนว่าระดับความเสี่ยงที่เหลืออยู่ อยู่ในระดับที่ยอมรับได้หรือไม่ และทำการสรุปผลติดตามเป็นลายลักษณ์อักษร พร้อมทั้งส่งรายงานผลให้ฝ่ายบริหารรับทราบ ในกรณีที่มีการปรับปรุงเพิ่มเติมมาตรการจัดการความเสี่ยง ควรแจ้งให้ผู้บริหารที่รับผิดชอบทราบทุกครั้ง และในกรณีที่พบว่าระดับความเสี่ยงเพิ่มสูงขึ้น ควรมีการเสนอแผนจัดการความเสี่ยงและรายงานให้ผู้บริหารเพื่อพิจารณาอย่างเร่งด่วน

## 2.2 การวิเคราะห์แขนงความบกพร่อง (Fault Tree Analysis; FTA)

Fault Tree Analysis หรือ FTA นี้ มีผู้เรียกเป็นภาษาไทยหลายชื่อ เช่น การวิเคราะห์แขนงความบกพร่อง หรือ แผนภูมิต้นไม้ (Tree Diagrams) เป็นการวิเคราะห์หาสาเหตุของอันตรายอุบัติเหตุ ความบกพร่องต่างๆ ที่เกี่ยวข้องกับงาน วิธีการทำงาน และกระบวนการผลิตอย่างเป็นระบบ แสดงให้เห็นถึงความเกี่ยวโยงที่จะนำไปสู่เหตุการณ์ที่ไม่ต้องการให้เกิดขึ้น เพื่อจะได้นำข้อมูลที่ได้มาหามาตรฐานในการควบคุมและป้องกันต่อไป

FTA จะช่วยในการหาโอกาสการเกิดเหตุการณ์ที่ไม่คาดคิด ว่ามีโอกาสมากหรือน้อยเพียงใด โดยอาศัยหลักพีชคณิตและตรรกะ (Boolean Algebra / Logic) หรือ Matrix และข้อมูลเกี่ยวกับอัตราการล้มเหลวในการทำงานเป็นพื้นฐานในการคำนวณ โดยผู้วิเคราะห์จะต้องมีความรู้ความเข้าใจในเทคนิค

และสัญลักษณ์ต่าง ๆ รวมทั้งขั้นตอนในการวิเคราะห์เป็นอย่างดีจึงจะทำให้สามารถวิเคราะห์ได้อย่างถูกต้อง

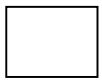
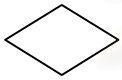
### 2.2.1 ประวัติความเป็นมาของ FTA

FTA ถูกคิดค้นขึ้นโดย H.A. Watson แห่ง Bell Telephone Laboratories ในปี 1962เพื่อวิเคราะห์ Minute-man Launch Control System ต่อมา North American Space Industrial ได้พัฒนา FTA ต่อไปจนกระทั่งเป็นที่รู้จักแพร่หลายว่าเป็นวิธีการในการวิเคราะห์ความน่าเชื่อถือของผลิตภัณฑ์

### 2.2.2 สัญลักษณ์ที่ใช้ในการวิเคราะห์ FTA

FTA เป็นการวิเคราะห์เหตุการณ์ด้วยแผนผัง ซึ่งจะใช้สัญลักษณ์รูปภาพต่าง ๆแทนเหตุการณ์และความเชื่อมโยงของแต่ละเหตุการณ์เข้าด้วยกัน สัญลักษณ์ที่ใช้แบ่งได้เป็น 2 ประเภทใหญ่ ๆ คือ สัญลักษณ์ที่ใช้กับเหตุการณ์ (Event Symbol) และสัญลักษณ์ที่ใช้แสดงความเป็นเหตุเป็นผลกัน (Logic Gate) รูปร่างและความหมายของสัญลักษณ์ต่าง ๆ ทั้ง 2 ประเภท แสดงได้ดังตารางที่ 2.4

ตารางที่ 2.4 สัญลักษณ์ที่ใช้ในการวิเคราะห์ Fault Tree Analysis (FTA)

| ประเภท | สัญลักษณ์ | ชื่อ | ความหมาย |
|---|---|---|---|
| Event Symbol |  | Fault Event | เหตุการณ์อยู่ระหว่างกลาง (Intermediate Event) เป็นเหตุการณ์ย่อยที่ส่งผลให้เหตุการณ์อื่นต่อไป ต้องถูกทำการวิเคราะห์ลงไปอีก |
| |  | Basic Event | เหตุการณ์ย่อยที่เกิดขึ้นได้ตามปกติเห็นได้ชัดเจนโดยไม่ต้องทำการวิเคราะห์หาสาเหตุต่อไป เป็นสาเหตุแรกของการเกิดความบกพร่องและจะอยู่ในส่วนล่างสุดของทุกๆ เหตุการณ์ |
| |  | Undeveloped Event | เหตุการณ์ย่อยที่ไม่มีข้อมูลเพียงพอ หรือยุ่งยากซับซ้อนหรือเป็นข้อมูลที่ไม่เกี่ยวข้องกับ Top Event จึงไม่วิเคราะห์ต่อไป แต่ถ้ามีข้อมูลเพิ่มเติมก็สามารถวิเคราะห์ต่อไปได้ |
| |  | House Event/ External Event | เหตุการณ์ภายนอกหรือปัจจัยภายนอกที่เป็นสาเหตุให้เกิดเหตุการณ์ต่างๆต้องพิจารณาว่าจะเกิดหรือไม่บางทีเรียกว่า Switch Event หรือ Normal Event |
| |  | Tree Transfer | ใช้เขียนเพื่ออ้างถึงเหตุการณ์หนึ่งซึ่งอยู่ในกิ่งก้านอื่นของแผนภูมิซึ่งเป็นเหตุการณ์ที่เหมือนกัน โดยไม่ต้องเขียนเหตุการณ์นั้นซ้ำอีก |
| Logic Gate |  | Or Gate | แสดงความสัมพันธ์ว่าเหตุการณ์หนึ่งจะเกิดขึ้นได้จะต้องมีสาเหตุมาจากสาเหตุใดสาเหตุหนึ่งของเหตุการณ์ย่อยหรือมากกว่านั้น |
| |  | And Gate | แสดงความสัมพันธ์ว่าเหตุการณ์หนึ่งจะเกิดขึ้นได้จะต้องมีสาเหตุมาจากเหตุการณ์ย่อยทุกๆเหตุการณ์เกิดขึ้นพร้อมกัน |
| |  | Inhibit Gate | แสดงกรณีที่เหตุการณ์ใดๆจะเกิดขึ้นได้ก็ต่อเมื่อมีเงื่อนไข (Condition) หรือข้อจำกัด (Restriction) หรือองค์ประกอบอื่นๆซึ่งจะเสริมให้เกิดเหตุการณ์นั้นๆ เช่น อุณหภูมิ ความดัน เป็นต้น |

**2.2.3 ขั้นตอนการวิเคราะห์ FTA**

การวิเคราะห์ FTA นั้นจะเริ่มจากการเขียนแผนผังลำดับการเกิดเหตุการณ์จนครบจากนั้นจะมีการคำนวณตัวเลขตามสูตรและข้อมูลที่มี หรือเขียนในรูป Matrix เพื่อหาโอกาสในการเกิดเหตุการณ์ แต่เนื่องจากในการวิจัยนี้จะใช้ FTA สำหรับการวิเคราะห์ต้นเหตุของปัญหาเท่านั้น จึงไม่ขอแสดงรายละเอียดในส่วนของวิธีคำนวณ สำหรับขั้นตอนการเขียนแผนผัง FTA นั้นมีดังต่อไปนี้

1. เลือกเหตุการณ์ที่เป็นอุบัติเหตุ ความบกพร่อง ความสูญเสียที่ต้องการวิเคราะห์เขียนอยู่บนสุดเป็น Top Event

2. พิจารณาโอกาสในการเกิดปัญหาดังกล่าว ซึ่งถ้าพบว่าเกิดขึ้นจากเหตุการณ์ย่อยเหตุการณ์ใดเหตุการณ์หนึ่งเท่านั้น ให้ใช้สัญลักษณ์ “Or Gate”

3. กรณีที่ต้องเกิดจากเหตุการณ์ย่อยหลายเหตุการณ์พร้อมกัน ให้ใช้สัญลักษณ์“And Gate”

4. ในระดับเหตุการณ์ย่อยดังกล่าว ก็อาจเกิดเหตุการณ์ย่อยลงไปอีก ซึ่งมีโอกาสเกิดขึ้นได้จากแต่ละเหตุการณ์ หรือเหตุการณ์ย่อยหลายเหตุการณ์พร้อมกันก็จะใช้สัญลักษณ์ “Or Gate” หรือ “And Gate” เชื่อมต่อลงไปแล้วแต่กรณี

5. ท้ายที่สุดเมื่อแตกเหตุการณ์ย่อยเช่นนี้ลงไปอีกก็จะพบว่า เหตุการณ์ย่อยระดับล่างสุดจะเป็น

- เหตุการณ์ที่เกิดเป็นปรกติทั่วไป (Basic Event)
- เหตุการณ์ที่วิเคราะห์ต่อไม่ได้ (Undeveloped Event)
- เหตุการณ์จากภายนอก (External Event) เช่น ปรากฏการณ์ธรรมชาติ

**2.2.4 ประโยชน์ของการวิเคราะห์ FTA**

ประโยชน์ของการวิเคราะห์แขนงความบกพร่อง มีดังต่อไปนี้

1. ใช้วิเคราะห์หาสาเหตุของปัญหาที่เกี่ยวกับงาน วิธีการทำงาน เครื่องจักร และกระบวนการผลิตได้ดี

2.ใช้ในการวางแผนป้องกันอุบัติเหตุเพราะจะทำให้ทราบสาเหตุและโอกาสในการเกิดล่วงหน้า

3. สามารถนำมาใช้ในการสอบสวนปัญหาและเหตุการณ์ที่สลับซับซ้อนได้

4. การวิเคราะห์จะแสดงความสัมพันธ์ของเหตุการณ์ต่าง ๆ ด้วยรูปภาพ ทำให้เห็นภาพได้อย่างชัดเจน และเข้าใจง่ายขึ้น

**2.3 งานวิจัยที่เกี่ยวข้อง**

การศึกษางานวิจัยที่เกี่ยวข้องมีดังต่อไปนี้

**วราพร อาสาพห์ประกิต (2547)**

งานวิจัยนี้ได้ทำการศึกษาและพัฒนาระบบบริหารความเสี่ยงของโครงการการให้คำปรึกษาและติดตั้งระบบสารสนเทศ โดยมีกระบวนการในการศึกษาดังนี้ ได้แก่ (1) การกำหนดและวางขอบเขตของโครงการ (2) การระบุความเสี่ยงภายในโครงการ (3) การค้นหาความเสี่ยงภายนอกโครงการ (4) การวิเคราะห์ปัจจัยเสี่ยง (5) การสร้างแผนจัดการความเสี่ยง และ (6) พัฒนาใบบันทึกข้อมูลความเสี่ยงเพื่อติดตามปัจจัยเสี่ยง จากการวิเคราะห์พบว่า มีความเสี่ยงภายใน 13 ปัจจัย และความเสี่ยงภายนอก 14 ปัจจัย ทุกปัจจัยจะถูกจัดลำดับและประเมินโดยผู้เชี่ยวชาญ ผู้บริหารโครงการ และผู้ปฏิบัติงานในโครงการ จากนั้นได้มีการนำเทคนิคการวิเคราะห์แขนงความบกพร่อง หรือ Fault Tree Analysis (FTA) มาใช้ในการสร้างแผนควบคุมความเสี่ยงของโครงการ

**สิริวรรธน์ ธรรมรัตน์ (2547)**

งานวิจัยนี้ได้ทำการศึกษาปัญหาการใช้โปรแกรมคอมพิวเตอร์สำเร็จรูปด้านการจัดการงานบำรุงรักษา โดยศึกษาจากโรงงานผลิตปลาทูน่ากระป๋องที่ใช้โปรแกรม SAP จากการศึกษาพบว่ามีปัญหาดังนี้ (1)พนักงานขาดความเข้าใจในระบบ SAP (2) วิธีการทำงานไม่เหมาะสม (3) จำนวนเครื่องคอมพิวเตอร์ที่สามารถใช้ SAP ได้ไม่เพียงพอ และ (4) ข้อมูลไม่ถูกต้อง ไม่ครบถ้วน เมื่อวิเคราะห์ปัญหาแล้วได้แก้ไขดังต่อไปนี้ (1) ฝึกอบรมในหัวข้อที่เกี่ยวข้องกับการใช้งานระบบ SAP ให้พนักงานทุกระดับ (2) ปรับปรุงขั้นตอนงานบำรุงรักษาเครื่องจักร (3) ปรับปรุงข้อมูลในระบบ SAP ให้ถูกต้อง (4) จัดวางเครื่องคอมพิวเตอร์ให้เหมาะกับปริมาณการใช้ และ (5) ดำเนินงานตามแนวทางที่ผู้บริหารแนะนำในส่วนสนับสนุน

**ฐิติรัตน์ พุทธิสารชัย (2544)**

งานวิจัยนี้ได้ทำการศึกษาพฤติกรรมการนำบริการระบบเครือข่ายอินเตอร์เน็ตมาใช้ในการทำงานของพนักงานบริษัทร่วมทุนในเขตกรุงเทพมหานคร โดยทำการศึกษา 2 ประเด็น คือ 1) ศึกษาถึงสถานภาพในปัจจุบันของปริมาณการใช้งานและประเภทหรือรูปแบบการใช้งานบริการระบบเครือข่ายอินเตอร์เน็ตของพนักงานในบริษัทร่วมทุน 2) ศึกษาถึงประโยชน์ที่ได้รับจากการนำบริการระบบเครือข่ายอินเตอร์เน็ตมาใช้ในการทำงาน โดยทำการศึกษาความแตกต่างด้านลักษณะทาง ประชากรและ

ระดับความรู้เกี่ยวกับอินเตอร์เน็ตของกลุ่มตัวอย่างจำนวน 400 คน เปรียบเทียบกับปริมาณการใช้งานและประโยชน์ที่ได้รับจากบริการระบบเครือข่ายอินเตอร์เน็ต รูปแบบของการวิจัยเป็นการวิจัยเชิงสำรวจ โดยใช้แบบสอบถามเป็นเครื่องมือในการเก็บข้อมูลจากกลุ่มตัวอย่าง และแบบสัมภาษณ์เพื่อประกอบการอภิปรายผลการวิจัย และจากผลการศึกษาพบว่า กลุ่มตัวอย่างมีความรู้เกี่ยวกับอินเตอร์เน็ตอยู่ในระดับสูง มีปริมาณการใช้งานในระดับต่ำ และได้รับประโยชน์จากอินเตอร์เน็ตในระดับปานกลาง นอกจากนี้ยังได้รับประโยชน์จากบริการระบบเครือข่ายอินเตอร์เน็ตในด้านอื่นๆ นอกเหนือจากในด้านการทำงานในระดับปานกลางเช่นกัน ผลการทดสอบสมมติฐานการวิจัยพบว่า 1. เพศที่ต่างกัน มีปริมาณการใช้งานระบบเครือข่ายอินเตอร์เน็ตแตกต่างกัน ส่วนอายุและระดับการศึกษาที่ต่างกัน มีปริมาณการใช้งานระบบเครือข่ายอินเตอร์เน็ตไม่แตกต่างกัน 2.ระดับความรู้เกี่ยวกับอินเตอร์เน็ตมีความสัมพันธ์เชิงบวกกับการได้รับประโยชน์จากบริการระบบเครือข่ายอินเตอร์เน็ตแต่ความสัมพันธ์ที่พบอยู่ในระดับต่ำ 3.เพศ อายุ และระดับการศึกษาที่ต่างกัน ได้รับประโยชน์จากบริการระบบเครือข่ายอินเตอร์เน็ตแตกต่างกัน

**ธนิต ธงทอง (2540)**

งานวิจัยนี้ได้ทำการศึกษา Information technology ในอุตสาหกรรมการก่อสร้างโดยใช้อินเตอร์เน็ต โดยมีวัตถุประสงค์คือ เพื่อพัฒนาอุตสาหกรรมการก่อสร้างด้วยการประยุกต์เทคโนโลยีด้านคอมพิวเตอร์ โดยนำเสนอรูปแบบการประยุกต์ใช้ Information Technology บนอินเตอรเนตในลักษณะที่ง่ายต่อการเข้าใจและการนำไปใช้งานเหมาะสมตามลักษณะของงานก่อสร้าง การวิจัยนี้ได้วิเคราะห์การดำเนินงานต่าง ๆ ขององค์กรที่อยู่ในอุตสาหกรรมการก่อสร้าง (องค์กรด้านการศึกษาวิจัย องค์กรธุรกิจ และสมาคม) เพื่อคัดเลือกกิจกรรมที่สามารถเพิ่มประสิทธิภาพของการดำเนินงานได้โดยใช้ระบบ Information Technology บนเครือข่ายอินเตอร์เน็ต รูปแบบของการประยุกต์ใช้ได้ถูกนำเสนอและทดลองปฏิบัติ ซึ่งพบว่าการเลือกกิจกรรมที่เหมาะสมและการประยุกต์ใช้ที่สอดคล้องกับการดำเนินงาน สามารถเพิ่มประสิทธิภาพการดำเนินงานขององค์กรในอุตสาหกรรมการก่อสร้างได้ ทั้งในเรื่องของเวลา ค่าใช้จ่าย และประโยชน์ที่ได้รับ การวิจัยได้นำเสนอรูปแบบและวิธีการประยุกต์เพื่อให้สามารถนำไปปฏิบัติได้ทันที รวมทั้งปัญหาอุปสรรค และแนะแนวทางแก้ไข

**อรวรรณ ปิลันธน์โอวาท (2536)**

งานวิจัยนี้เป็นงานวิจัยเชิงคุณภาพ เพื่อศึกษาเกี่ยวกับเทคโนโลยีสารสนเทศและบทบาทในการพัฒนาสังคมไทย โดยได้ทำการเก็บรวบรวมข้อมูลจากการสัมภาษณ์เจาะลึกจากผู้บริหารในหน่วยราชการไทย กลุ่มผู้เกี่ยวข้องกับนโยบายการใช้คอมพิวเตอร์ของรัฐ ผู้อยู่ในแวดวงวิชาการและวิชาชีพทางด้านคอมพิวเตอร์รวมทั้งการรวบรวมข้อมูลจากเอกสารต่าง ๆ และผลการศึกษาพบว่า

1. สถานภาพการใช้เทคโนโลยีสารสนเทศของหน่วยราชการไทยนั้น หน่วยรายการไทยหลายแห่งมีคอมพิวเตอร์ใช้อย่างเพียงพอ และนิยมใช้คอมพิวเตอร์ขนาดเล็ก (Microcomputer) มากที่สุด ลักษณะการใช้งานเป็นการใช้งานทั่วไปเป็นหลัก โดยส่วนใหญ่เป็นการใช้ข้อมูลเพื่องานภายในหน่วยงาน การเชื่อมโยงระหว่างหน่วยงานมีน้อย ขาดศูนย์รวมข้อมูล มีความซ้ำซ้อนในการจัดเก็บข้อมูล

2. ผลการใช้เทคโนโลยีสารสนเทศ ผลการวิจัยสรุปได้ว่า เทคโนโลยีสารสนเทศให้ผลทางด้านบวกมากกว่าด้านลบ ไม่ว่าจะเป็นผลต่องานของหน่วยงาน และความสัมพันธ์ระหว่างบุคลากร สำหรับผลต่อการนำมาใช้เพื่อการพัฒนาประเทศยังคงอยู่ในระดับที่ไม่กว้างขวางมากนัก การให้บริการให้กับหน่วยงานภายนอกมีไม่มากนัก ส่วนใหญ่เป็นการพัฒนาภายในหน่วยงานเท่านั้น

3. ปัญหาและข้อจำกัดการใช้เทคโนโลยีสารสนเทศ ส่วนใหญ่เป็นปัญหาด้านความพร้อมและความชำนาญในการใช้เทคโนโลยีของบุคลากร นอกจากนี้หน่วยงานราชการส่วนใหญ่ยังขาดแคลนบุคลากรทางด้านนี้ การพิจารณาเลือกเทคโนโลยีมาใช้กับหน่วยงานมีขั้นตอนยุ่งยาก นอกจากนี้ยังมีปัญหาการจัดเก็บข้อมูลซึ่งยังคงไม่เป็นระบบเดียวกัน

4. แนวโน้มการใช้เทคโนโลยีสารสนเทศของหน่วยราชการไทยในอนาคต มีโครงการจะขยายการใช้มากขึ้นทั้งทางด้านจำนวน ระบบที่ใช้ การเพิ่มเครือข่ายและลักษณะการเชื่อมโยง และการให้บริการ แลกเปลี่ยนข้อมูลซึ่งกันและกัน

**ยุบล เบ็ญจรงค์กิจ (2534)**

งานวิจัยนี้ได้ทำการสำรวจการใช้เทคโนโลยีคอมพิวเตอร์ในสถาบันอุดมศึกษาของรัฐ เพื่อสำรวจปริมาณและประเภทของคอมพิวเตอร์ที่มีอยู่ในหน่วยงานปริมาณและประเภทของงานที่ใช้เครื่องคอมพิวเตอร์ช่วยในการปฏิบัติงาน รวมทั้งความต้องการในการใช้คอมพิวเตอร์และความพึงพอใจที่ได้รับจากการใช้เครื่องคอมพิวเตอร์ ซึ่งรวบรวมข้อมูลโดยใช้แบบสอบถามกับสถาบันอุดมศึกษาของรัฐบาลทั้งในเขตกรุงเทพมหานครและต่างจังหวัด รวม184 แห่ง ผลการวิจัยพบว่า

1. คณะและหน่วยงานต่างๆ ส่วนใหญ่มีเครื่องคอมพิวเตอร์ใช้ในการปฏิบัติงานเครื่องคอมพิวเตอร์ที่ใช้มากที่สุด คือ คอมพิวเตอร์ขนาดเล็ก (Micro computer) ซึ่งส่วนใหญ่ใช้เครื่องคอมพิวเตอร์ยี่ห้อ IBM

2. ปริมาณการใช้เครื่องคอมพิวเตอร์ในหน่วยงานต่างๆ ส่วนใหญ่อยู่ในระดับปานกลาง ประเภทของงานที่ใช้เครื่องคอมพิวเตอร์ช่วยในการปฏิบัติงานมากที่สุดคืองานจัดเตรียมเอกสาร และการให้บริการด้านฝึกอบรมแก่หน่วยราชการอื่นๆ

3. หน่วยงานต่างๆมีความพึงพอใจที่ได้รับจากการใช้เครื่องคอมพิวเตอร์มาก

4. หน่วยงานต่างๆ มีความต้องการใช้คอมพิวเตอร์ช่วยในการปฏิบัติงานมาก โดยเฉพาะอย่างยิ่งงานเก็บรวบรวมและจัดระบบฐานข้อมูล

# บทที่ 3

# ข้อมูลเบื้องต้นของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในโรงพยาบาลที่ทำการวิจัย

การศึกษาข้อมูลเบื้องต้นของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในโรงพยาบาลจุฬาลงกรณ์ ได้ศึกษาประวัติความเป็นมาของการใช้คอมพิวเตอร์และอินเตอร์เน็ตภายในโรงพยาบาล พันธกิจและวิสัยทัศน์ของฝ่ายเทคโนโลยีสารสนเทศ หน้าที่ความรับผิดชอบของฝ่ายเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ ฮาร์ดแวร์และซอฟท์แวร์ ระบบคอมพิวเตอร์ และซอฟท์แวร์ ที่โรงพยาบาลใช้อยู่ในปัจจุบัน และระบบงานในโรงพยาบาลที่ใช้คอมพิวเตอร์และอินเตอร์เน็ต

## 3.1 ประวัติความเป็นมาของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในโรงพยาบาล

สืบเนื่องจากโรงพยาบาลมีผู้ป่วยมารับบริการเพิ่มขึ้นทุกปี ดังนั้นในปี พ.ศ.2526 ทางโรงพยาบาลจึงได้มีนโยบายในการพัฒนาระบบคอมพิวเตอร์เพื่อที่จะนำมาใช้ในโรงพยาบาลเพื่อเพิ่มประสิทธิภาพในการให้บริการผู้ป่วยที่มารับบริการและเป็นการพัฒนางานของโรงพยาบาลในส่วนอื่นๆ ด้วยต่อมาทางผู้อำนวยการโรงพยาบาลจึงได้มีการจัดตั้งคณะกรรมการเฉพาะกิจขึ้นมาเพื่อที่จะรับผิดชอบในการศึกษาและเสนอแผนงานในการติดตั้งระบบคอมพิวเตอร์ในโรงพยาบาล ซึ่งคณะกรรมการชุดนี้ได้ทำการนำเสนอแผนการดำเนินงานการเพื่อติดตั้งระบบคอมพิวเตอร์กับทางโรงพยาบาล ในวันที่ 29 มิถุนายน พ.ศ.2530 สำหรับแผนงานที่นำเสนอมีดังต่อไปนี้ คือ ทำการจัดตั้งหน่วยคอมพิวเตอร์ และสรรหาบุคลากรมาปฏิบัติงาน รวมทั้งว่าจ้างบริษัทจากภายนอกให้เข้ามาดำเนินงานในการติดตั้งระบบคอมพิวเตอร์ ต่อมาเมื่อวันที่ 14 ธันวาคม พ.ศ.2531 ทางโรงพยาบาลก็ได้มีมติให้ดำการตามแผนงานที่คณะกรรมการนำเสนอมาและได้จัดตั้งหน่วยคอมพิวเตอร์ของโรงพยาบาลขึ้นมาในปี พ.ศ.2532 ให้เป็นหน่วยงานที่ขึ้นตรงกับผู้อำนวยการโรงพยาบาล และหน่วยคอมพิวเตอร์ของโรงพยาบาลก็ได้ดำเนินงานนับจากนั้นเป็นต้นมาจนถึงปัจจุบัน ซึ่งในปัจจุบันหน่วยคอมพิวเตอร์ของโรงพยาบาลได้เปลี่ยนมาเป็นฝ่ายเทคโนโลยีสารสนเทศ

**3.2 พันธกิจและวิสัยทัศน์ของฝ่ายเทคโนโลยีสารสนเทศ**

ฝ่ายเทคโนโลยีสารสนเทศของโรงพยาบาลได้มีการกำหนดพันธกิจและวิสัยทัศน์ในการปฏิบัติงานให้บริการด้านคอมพิวเตอร์และอินเตอร์เน็ตภายในโรงพยาบาล ดังต่อไปนี้

พันธกิจ คือ บริการระบบงานคอมพิวเตอร์ On-line ของโรงพยาบาลด้วยความสะดวก รวดเร็ว ถูกต้อง และปลอดภัย บริการข้อมูลเพื่อการบริหารและพัฒนา บริการข้อมูล เพื่อการศึกษาวิจัยทางการแพทย์ ดูแลความปลอดภัยและความถูกต้องของข้อมูล

วิสัยทัศน์ คือ บริการงานด้านคอมพิวเตอร์ทุกเวลา มุ่งมั่นพัฒนาด้วยศรัทธาเพื่อคนไข้

**3.3 หน้าที่ความรับผิดชอบของฝ่ายเทคโนโลยีสารสนเทศ**

จากพันธกิจและวิสัยทัศน์ที่ทางฝ่ายเทคโนโลยีสารสนเทศของโรงพยาบาลได้กำหนดไว้ในการปฏิบัติงานให้บริการด้านคอมพิวเตอร์และอินเตอร์เน็ตภายในโรงพยาบาล ฝ่ายเทคโนโลยีสารสนเทศจึงมีหน้าที่ความรับผิดชอบหลักเพื่อให้บรรลุตามพันธกิจและวิสัยทัศน์ที่ทางฝ่ายเทคโนโลยีสารสนเทศได้กำหนดไว้ดังต่อไปนี้

1. ให้บริการระบบคอมพิวเตอร์ On-line ของโรงพยาบาล ตลอด 24 ชั่วโมง
    - สำรวจจุดติดตั้งเครื่องคอมพิวเตอร์ เครื่องพิมพ์ และอุปกรณ์ต่อพ่วงต่างๆ
    - จัดเตรียมเครื่องคอมพิวเตอร์ เครื่องพิมพ์ และอุปกรณ์ต่อพ่วงสำรอง ให้เพียงพอต่อการใช้งาน
    - ติดตั้งเครื่องคอมพิวเตอร์ เครื่องพิมพ์ และอุปกรณ์ต่อพ่วงต่างๆ
    - วางระบบเครือข่ายคอมพิวเตอร์ในโรงพยาบาล
    - วิเคราะห์ ออกแบบ และพัฒนาโปรแกรม
    - บริการให้คำปรึกษา และแก้ไขปัญหาให้กับผู้ใช้ระบบคอมพิวเตอร์ On-line

2. รักษาความปลอดภัยของระบบคอมพิวเตอร์ โดยมีมาตรฐานการเข้าใช้งานของผู้ใช้ระบบคอมพิวเตอร์ On-line ในส่วนต่างๆ ดังนี้
    - ฮาร์ดแวร์ คือ อุปกรณ์ต่างๆที่ประกอบกันเป็นเครื่องคอมพิวเตอร์
    - เครือข่ายคอมพิวเตอร์

- ซอฟท์แวร์
  - ฐานข้อมูล
  - โปรแกรมที่ออกแบบเฉพาะงาน

3. พัฒนางานบริการและงานข้อมูลคอมพิวเตอร์ On-line ของโรงพยาบาล ดังต่อไปนี้
   - โครงการกำจัดข้อมูลขยะ (Dirty data)
   - โครงการปรับปรุงประสิทธิภาพ Hard disk ของเครื่องคอมพิวเตอร์ลูกข่าย (Client)
   - โครงการพัฒนาการรับแจ้งปัญหาจากผู้ใช้ระบบคอมพิวเตอร์ On-line และมีการนำระบบคอมพิวเตอร์มาใช้สำหรับงานบริการรับแจ้งปัญหา (Call center)

**3.4 ระบบคอมพิวเตอร์ ฮาร์ดแวร์และซอฟท์แวร์ ที่โรงพยาบาลใช้อยู่ในปัจจุบัน**

โรงพยาบาลได้มีการนำเอาระบบคอมพิวเตอร์ HIS (Hospital Information System) มาใช้ในโรงพยาบาลเพื่อให้บริการระบบคอมพิวเตอร์ On-line ของโรงพยาบาลในการให้บริการผู้ใช้งานในโรงพยาบาล สำหรับโปรแกรมที่ใช้จะเป็นไปในลักษณะที่เขียนขึ้นมาตามการใช้งานจริง คือ ฝ่ายเทคโนโลยีสารสนเทศจะมีการสำรวจ วิเคราะห์ ออกแบบ และเขียนหรือพัฒนาโปรแกรมขึ้นใหม่ตามลักษณะการใช้งานจริงของงานนั้นๆที่ต้องใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำงาน ซึ่งปัจจุบันทางโรงพยาบาลมีจำนวนคอมพิวเตอร์ทั้งสิ้น 850 เครื่อง เครื่องพิมพ์ 650 เครื่อง โดยมีฮาร์ดแวร์และซอฟท์แวร์หลักที่ใช้งานอยู่ในปัจจุบันดังต่อไปนี้

ฮาร์ดแวร์ประกอบไปด้วย

- Machine IBM RS/6000 SP Width Node 5 Node
- Disk Storage Total 2.02 TB
- Tape Storage IBM 7337 Digital Linear
- Tape Library up to 15 tape Capacity 35 GB per tape 70 GB with Compression

ซอฟท์แวร์ประกอบไปด้วย

- OS AIX Version 4.3.3
- Database INFORMIX Version 7.31
- High Availability Version 4
- Storage Software Tivoli Version 5.1

- Application Tool Power Builder Version 7

โดยระบบคอมพิวเตอร์ที่ใช้อยู่ในโรงพยาบาล รวมไปถึงฮาร์ดแวร์ และซอฟท์แวร์ ต่างๆที่ใช้งานอยู่ในโรงพยาบาลทั้งหมดจะถูกกำหนดโดยฝ่ายเทคโนโลยีสารสนเทศของโรงพยาบาล ซึ่งอาจจะเปลี่ยนแปลงได้ตามความเหมาะสมในอนาคต

**3.5 ระบบงานในโรงพยาบาลที่ใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำงาน**

ระบบงานในโรงพยาบาลที่ต้องใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำงาน ประกอบไปด้วยสองส่วนหลักๆ คือ ส่วนที่หนึ่งคือระบบงานบริการผู้ป่วย ส่วนที่สองคือระบบงานการบริหารจัดการเรื่องทั่วๆไปในโรงพยาบาลที่ไม่เกี่ยวข้องกับผู้ป่วย หรือที่เรียกว่าระบบงาน Back Officeโดยระบบงานทั้งสองระบบมีรายละเอียดดังต่อไปนี้

1. ระบบงานบริการผู้ป่วย

นับได้ว่าเป็นงานหลักของทางโรงพยาบาลที่ต้องให้บริการกับผู้ป่วยหรือผู้มารับบริการในด้านต่างๆของทางโรงพยาบาล ซึ่งทางโรงพยาบาลที่ทำการวิจัยได้นำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในงานด้านต่างๆเกี่ยวกับระบบงานบริการผู้ป่วยดังต่อไปนี้

- งานเวชระเบียนผู้ป่วย
- งานจัดการหน้าห้องตรวจ
- งานลงวินิจฉัยโรคผู้ป่วย
- งานนัดผู้ป่วยนอก
- ระบบศูนย์บรรจุผู้ป่วยนอก/ใน
- งานห้องฉุกเฉิน
- งานคลินิกพิเศษนอกเวลา
- งานคลังยา
- งานเภสัชกรรมสนเทศ
- งานจ่ายยาผู้ป่วยนอก/ใน
- หน่วยผลิตยา
- งานประกันสุขภาพ

- ศูนย์โรคหัวใจ
- คลังเวชภัณฑ์
- งานจ่ายเวชภัณฑ์ผู้ป่วยนอก/ใน
- การเงินผู้ป่วยนอก/ใน
- สังคมสงเคราะห์
- เวชระเบียนและสถิติ
- งานระบบหอผู้ป่วย
- งานสรุป Discharge Summary
- งานห้องผ่าตัด/วิสัญญี
- งานโภชนวิทยา
- งานธนาคารเลือด

2. ระบบงาน Back Office

ระบบงาน Back Office เป็นระบบงานที่เป็นงานประเภทสนับสนุนงานหลัก กล่าวคือเป็นระบบงานที่สนับสนุนระบบงานบริการผู้ป่วยซึ่งจะไม่เกี่ยวข้องกับการบริการผู้ป่วยโดยตรง แต่จะเป็นระบบงานที่เกี่ยวกับการบริหารจัดการเรื่องทั่วๆไปภายในโรงพยาบาล ซึ่งทางโรงพยาบาลที่ทำการวิจัยได้นำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในงานด้านต่างๆเกี่ยวกับระบบงาน Back Office ดังต่อไปนี้

- ระบบจัดซื้อ/สัมภาระ
- ระบบงบประมาณ
- ระบบบัญชี
- ระบบเครื่องมือแพทย์
- ระบบบุคลากร
- ระบบเงินบริจาค
- ระบบรับแจ้งปัญหาจาก ผู้ใช้คอมพิวเตอร์

# บทที่ 4
# การระบุความเสี่ยง

ขั้นตอนการระบุความเสี่ยงนับเป็นขั้นตอนหนึ่งที่สำคัญมากในการบริหารความเสี่ยง เนื่องจากขั้นตอนการระบุความเสี่ยงนั้นเป็นขั้นตอนในการกำหนดว่าเหตุการณ์หรือสถานการณ์ใดบ้างที่จัดว่าเป็นความเสี่ยงในการดำเนินงานขององค์กร ดังนั้นการระบุความเสี่ยงจึงต้องมีการกำหนดขอบเขตในการระบุความเสี่ยงให้ชัดเจน เพราะหากการระบุความเสี่ยงนั้นไม่มีการกำหนดขอบเขตที่ชัดเจนก็จะทำให้การระบุความเสี่ยงนั้นเป็นไปอย่างไม่มีทิศทาง ไม่ตรงประเด็นที่ต้องการบริหารจัดการ ซึ่งจะส่งผลให้การบริหารความเสี่ยงนั้นไม่เกิดประโยชน์ใดๆเลยกับองค์กร อีกทั้งยังอาจทำให้องค์กรต้องสูญเสียทรัพยากรต่างๆขององค์กรโดยเปล่าประโยชน์อีกด้วย ซึ่งการกำหนดขอบเขตของการระบุความเสี่ยงนั้นสามารถทำได้โดยพิจารณาจากวัตถุประสงค์ของการบริหารความเสี่ยง

## 4.1 การกำหนดวัตถุประสงค์ของการบริหารความเสี่ยง

การกำหนดวัตถุประสงค์ของการบริหารความเสี่ยงนั้นสามารถทำได้โดยศึกษาและพิจารณาจากวัตถุประสงค์ของการดำเนินงานที่โรงพยาบาลได้ตั้งเอาไว้ในการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในโรงพยาบาล

### 4.1.1 การศึกษาวัตถุประสงค์ของการดำเนินงาน

การนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในโรงพยาบาลที่ทำการวิจัยนั้น ทางฝ่ายเทคโนโลยีสารสนเทศของโรงพยาบาลได้มีการกำหนดพันธกิจและวิสัยทัศน์ไว้อย่างชัดเจน ดังที่ได้กล่าวไว้แล้วในบทที่ 3 ในหัวข้อ 3.2 และจากการศึกษาพันธกิจและวิสัยทัศน์ที่ทางฝ่ายเทคโนโลยีสารสนเทศได้ตั้งเอาไว้ในการนำคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในโรงพยาบาล สามารถสรุปออกมาเป็นวัตถุประสงค์ของการดำเนินงานได้ดังต่อไปนี้ คือ “ระบบคอมพิวเตอร์ On-line ของโรงพยาบาลต้องพร้อมใช้งานตลอด 24 ชั่วโมง เพื่อให้บริการผู้ป่วยในด้านต่างๆ รวมไปถึงงานด้านอื่นๆในโรงพยาบาล ด้วยความรวดเร็ว ถูกต้องและปลอดภัย”

**4.1.2 วัตถุประสงค์ของการบริหารความเสี่ยง**

เมื่อทำการศึกษาและพิจารณาจากวัตถุประสงค์ของการดำเนินงาน สามารถกำหนดวัตถุประสงค์ของการบริหารความเสี่ยงได้ดังนี้ คือ การบริหารความเสี่ยงทางด้าน บุคลากร, เทคโนโลยี, ข้อมูล, ฮาร์ดแวร์และซอฟท์แวร์ และกฎหมาย

- ความเสี่ยงด้านบุคลากร

บุคลากรเป็นผู้ที่ต้องใช้งานคอมพิวเตอร์และอินเตอร์เน็ต ดังนั้นความผิดพลาดหรือความล่าช้าต่างๆอาจมีสาเหตุมาจากบุคลากรผู้ใช้งาน เช่น บุคลากรทำงานผิดพลาด บุคลากรขาดทักษะการใช้งาน เป็นต้น

- ความเสี่ยงด้านเทคโนโลยี

ความเสี่ยงด้านเทคโนโลยี เป็นอีกประเด็นหนึ่งที่อาจจะเป็นอุปสรรคในการดำเนินงานของการใช้คอมพิวเตอร์และอินเตอร์เน็ต เนื่องจากการใช้คอมพิวเตอร์และอินเตอร์เน็ตนั้นเกี่ยวข้องกับเทคโนโลยีโดยตรง ความเสี่ยงด้านเทคโนโลยีที่อาจเกิดขึ้นเช่น เทคโนโลยีเปลี่ยนแปลงเร็ว เทคโนโลยีมีความซับซ้อนเกินไป หรือแม้แต่ภัยคุกคามต่างๆด้านเทคโนโลยี เช่น ไวรัสคอมพิวเตอร์ เป็นต้น

- ความเสี่ยงด้านข้อมูล

ความเสี่ยงด้านข้อมูลนับว่ามีความสำคัญมาก เนื่องจากการนำคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในโรงพยาบาลนั้นวัตถุประสงค์หลัก คือ การนำมาจัดการข้อมูลต่างๆในโรงพยาบาลโดยเฉพาะข้อมูลด้านต่างๆของผู้ป่วย ดังนั้นหากเกิดความผิดพลาดของข้อมูลในด้านต่างๆ เช่น ข้อมูลสูญหาย ไม่มีการอัพเดทข้อมูล ฯลฯ ย่อมส่งผลต่อการให้บริการผู้ป่วยโดยตรง

- ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์

องค์ประกอบของคอมพิวเตอร์ก็คือฮาร์ดแวร์และซอฟท์แวร์ดังนั้นอุปสรรคของการใช้คอมพิวเตอร์และอินเตอร์เน็ตบ่อยครั้งมีสาเหตุมาจากฮาร์ดแวร์และซอฟท์แวร์ เช่น ความบกพร่องของฮาร์ดแวร์และซอฟท์แวร์ ซอฟท์แวร์ใช้งานยาก เป็นต้น

- ความเสี่ยงด้านกฎหมาย

ความเสี่ยงด้านกฎหมายอาจไม่เป็นอุปสรรคโดยตรงต่อการใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำงาน แต่ก็ไม่อาจละเลยได้ เนื่องจากการใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำงานนั้นอาจนำพาไปสู่การทำผิดกฎหมายได้โดยไม่เจตนา ซึ่งจะส่งผลเสียอย่างยิ่งต่อภาพลักษณ์ขององค์กร

**4.2 ขอบเขตและผู้มีส่วนเกี่ยวข้องในการระบุความเสี่ยง**

การที่จะพิจารณาว่าเหตุการณ์หรือสถานการณ์ใดบ้างที่จัดว่าเป็นความเสี่ยงในการดำเนินงานนั้นสามารถพิจารณาได้โดย หากเหตุการณ์หรือสถานการณ์นั้นเกิดขึ้นจะทำให้เกิดอุปสรรคในการดำเนินงานหรือทำให้ไม่สามารถบรรลุวัตถุประสงค์ของการดำเนินงานจะถือว่าเหตุการณ์หรือสถานการณ์นั้นเป็นความเสี่ยง โดยจะทำการระบุความเสี่ยงในด้านต่างๆตามวัตถุประสงค์ของการบริหารความเสี่ยง ได้แก่ ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านเทคโนโลยี ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ และความเสี่ยงด้านกฎหมาย

ระบบงานของทางโรงพยาบาลที่ทำการวิจัย มีระบบงานที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และอินเตอร์เน็ตแบ่งเป็นสองส่วนหลักๆ คือ ระบบงานบริการผู้ป่วยและระบบงาน Back Office ดังนั้นบุคลากรที่มีส่วนเกี่ยวข้องในการระบุความเสี่ยงจะต้องเป็นบุคลากรที่ปฏิบัติงานอยู่ในระบบงานบริการผู้ป่วย และระบบงานBack Office และต้องเป็นผู้ที่ใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำงานหรือมีส่วนรับผิดชอบในการใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำงาน โดยการระบุความเสี่ยงในครั้งนี้ใช้แบบสอบถามในการระบุความเสี่ยง (แบบสอบถามที่ใช้ในการระบุความเสี่ยงแสดงไว้ในภาคผนวก ก-1) สำหรับผู้มีส่วนเกี่ยวข้องในการระบุความเสี่ยงประกอบไปด้วย

| | | | |
|---|---|---|---|
| • | หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ | 1 | คน |
| • | ตัวแทนหัวหน้าสำนักงานพัฒนาคุณภาพ | 1 | คน |
| • | ตัวแทนระบบงานบริการผู้ป่วย | 1 | คน |
| • | ตัวแทนระบบงาน Back Office | 1 | คน |
| | รวม | 4 | คน |
| | อายุงานเฉลี่ย | 12 | ปี |

**4.3 ผลการระบุความเสี่ยง**

ผลการระบุความเสี่ยงแยกเป็นความเสี่ยงด้านบุคลากร ความเสี่ยงด้านเทคโนโลยี ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ และความเสี่ยงด้านกฎหมาย ได้แสดงไว้ในตารางที่ 4.1-4.5 ดังต่อไปนี้

ตารางที่ 4.1 ผลการระบุความเสี่ยงด้านบุคลากร

| **ความเสี่ยงด้านบุคลากร** | |
|---|---|
| **ลำดับที่** | **ความเสี่ยง** |
| 1 | ขาดวิศวกรวางแผนระบบ |
| 2 | ใช้งานโปรแกรมบางโปรแกรมไม่เป็น |
| 3 | ใช้งานโปรแกรมใหม่ๆไม่เป็น |
| 4 | ขาดผู้รับผิดชอบหลักในการให้คำปรึกษาด้าน IT |
| 5 | คีย์รหัสประเภทคนไข้ผิด |
| 6 | ยกเลิกข้อมูลค่ารักษาพยาบาลที่คีย์ผิดไม่ได้ |
| 7 | คีย์รหัสการรักษาพยาบาลผิด |
| 8 | ไม่มีผู้รับผิดชอบหลักในการแก้ปัญหาเมื่ออินเตอร์เน็ตใช้งานไม่ได้ |
| 9 | คีย์ข้อมูลทั่วๆไปผิด |
| 10 | คีย์ข้อมูลบุคลากรผิด |
| 11 | แก้ไขสิทธิของผู้ป่วยไม่ได้ |
| 12 | คีย์สิทธิต่างๆของคนไข้ผิด |
| 13 | แก้ไขข้อมูลของบุคลากรที่คีย์ผิดไม่ได้ |
| 14 | เสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต |

ตารางที่ 4.2 ผลการระบุความเสี่ยงด้านเทคโนโลยี

| ความเสี่ยงด้านเทคโนโลยี | |
|---|---|
| **ลำดับที่** | **ความเสี่ยง** |
| 1 | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย |
| 2 | คอมพิวเตอร์ติดไวรัสบูตเซกเตอร์ (Boot Sector Virus) |
| 3 | คอมพิวเตอร์ติดไวรัสไฟล์ข้อมูล (File Virus) |
| 4 | คอมพิวเตอร์ติดโทรจันไวรัส (Trojan Horse Virus) |
| 5 | คอมพิวเตอร์ติดมาโครไวรัส (Macro Virus) |
| 6 | อีเมลล์ไวรัส (Email Virus) |

ตารางที่ 4.3 ผลการระบุความเสี่ยงด้านข้อมูล

| ความเสี่ยงด้านข้อมูล | |
|---|---|
| **ลำดับที่** | **ความเสี่ยง** |
| 1 | ข้อมูลเวชระเบียนผู้ป่วยสูญหายบางรายการ/ทั้งหมด |
| 2 | สิทธิต่างๆของผู้ป่วยเปลี่ยนแต่ไม่มีการแก้ไขในระบบ |
| 3 | รายชื่อคนไข้หายไปจากระบบ |
| 4 | ค่ารักษาพยาบาลเปลี่ยนแปลง แต่หน้าจอยังแสดงค่าเดิม |
| 5 | ข้อมูลของบุคลากรหายไป |
| 6 | ย้ายข้อมูลคนไข้จากวอร์ดหนึ่งไปยังอีกวอร์ดหนึ่งไม่ได้ |
| 7 | จำหน่ายข้อมูลคนไข้ไม่ได้ |
| 8 | ค้นหาข้อหาข้อมูลที่ต้องการใช้ ในอินเตอร์เน็ตไม่พบ |
| 9 | ข้อมูลบุคลากรในระบบกับสถานะปัจจุบันไม่ตรงกัน |
| 10 | ค้นหาข้อหาข้อมูลที่ต้องการใช้ ในระบบโรงพยาบาลไม่พบ |
| 11 | รายการค่ารักษาพยาบาลบางรายการของผู้ป่วยหายไป |

ตารางที่ 4.4 ผลการระบุความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์

| ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ | |
|---|---|
| **ลำดับที่** | **ความเสี่ยง** |
| 1 | แก้ไขโปรแกรมไม่ทัน |
| 2 | ระบบคอมพิวเตอร์ล่ม |
| 3 | พิมพ์ใบเสร็จรับเงินแต่ข้อมูลออกมาไม่ครบแต่หน้าจอแสดงข้อมูลครบ |
| 4 | สั่งพิมพ์สติกเกอร์ไม่ออก |
| 5 | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน |
| 6 | สั่งพิมพ์ใบเสร็จรับเงินไม่ได้ |
| 7 | Down load ข้อมูลต่างๆได้ช้า |
| 8 | สั่งพิมพ์ใบนัดหมายคนไข้ไม่ได้ |
| 9 | สั่งพิมพ์บัตรไม่ได้ |
| 10 | เข้าใช้งานโปรแกรมไม่ได้ |
| 11 | คอมพิวเตอร์ Restart เอง |
| 12 | บันทึกข้อมูลลงไปในโปรแกรมไม่ได้ |
| 13 | เวลาในระบบไม่ตรงกับเวลาจริง |
| 14 | คอมพิวเตอร์ประมวลผลช้า |
| 15 | เครื่องมองไม่เห็น CD-ROM |
| 16 | จำนวน Computer ไม่เพียงพอต่อการใช้งาน |
| 17 | หน้าจอค้างสีฟ้า (Blue Screen of Death) |
| 18 | สั่งพิมพ์เอกสารต่างๆไม่ได้ |
| 19 | ใช้เวลานานในการเข้าโปรแกรมต่างๆ |
| 20 | ข้อมูลที่แสดงบนหน้าจอกับที่พิมพ์ออกมาไม่ตรงกัน |
| 21 | CD-ROM ไม่อ่านแผ่นCD |

ตารางที่ 4.5 ผลการระบุความเสี่ยงด้านกฎหมาย

| ความเสี่ยงด้านกฎหมาย | |
|---|---|
| **ลำดับที่** | **ความเสี่ยง** |
| 1 | ใช้โปรแกรมบางประเภทกับคอมพิวเตอร์หลายเครื่องเกินจำนวนที่ Software License กำหนด |
| 2 | บุคลากรนำ Software ละเมิดลิขสิทธิ์มาลงใช้เอง |

## 4.4 สรุปประเด็นความเสี่ยง

โดยการวิเคราะห์และสังเคราะห์ความเสี่ยง สามารถสรุปประเด็นความเสี่ยงทั้งหมดได้ดังนี้

### 4.4.1 การวิเคราะห์และสังเคราะห์ความเสี่ยง

ผลการระบุความเสี่ยงทั้งหมด คือ ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านเทคโนโลยี ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ และความเสี่ยงด้านกฎหมาย สามารถระบุความเสี่ยงได้ทั้งหมด 54 ความเสี่ยง จากนั้นนำความเสี่ยงที่ได้ทั้งหมดมาทำการวิเคราะห์และสังเคราะห์เพื่อที่จะรวมความเสี่ยงทั้งหมดให้เป็นประเด็น เนื่องจากความเสี่ยงหลายๆความเสี่ยงจัดได้ว่าเป็นความเสี่ยงที่เป็นประเด็นเดียวกัน ซึ่งสามารถวิเคราะห์และสังเคราะห์ความเสี่ยงได้ดังตารางต่อไปนี้

ตารางที่ 4.6 ผลการวิเคราะห์และสังเคราะห์ความเสี่ยงด้านบุคลากร

| ความเสี่ยงด้านบุคลากร | |
|---|---|
| **ลำดับที่** | **ประเด็นความเสี่ยง** |
| **1** | **ขาดบุคลากรในบางตำแหน่งที่ควรจะมี** |
| | ขาดวิศวกรวางแผนระบบ |
| | ขาดผู้รับผิดชอบหลักในการให้คำปรึกษาด้าน IT |
| | ไม่มีผู้รับผิดชอบหลักในการแก้ปัญหาเมื่ออินเตอร์เน็ตใช้งานไม่ได้ |
| **2** | **บุคลากรใช้งานโปรแกรมไม่เป็น** |
| | ใช้งานโปรแกรมบางโปรแกรมไม่เป็น |
| | ใช้งานโปรแกรมใหม่ๆไม่เป็น |
| **3** | **บุคลากรคีย์ข้อมูลผิด** |
| | คีย์รหัสประเภทคนไข้ผิด |
| | คีย์รหัสการรักษาพยาบาลผิด |
| | คีย์ข้อมูลทั่วๆไปผิด |
| | คีย์ข้อมูลบุคลากรผิด |
| | คีย์สิทธิต่างๆของคนไข้ผิด |
| **4** | **บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น** |
| | ยกเลิกข้อมูลค่ารักษาพยาบาลที่คีย์ผิดไม่ได้ |
| | แก้ไขสิทธิของผู้ป่วยไม่ได้ |
| | แก้ไขข้อมูลของบุคลากรที่คีย์ผิดไม่ได้ |
| **5** | **บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต** |
| | เสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต |

ตารางที่ 4.7 ผลการวิเคราะห์และสังเคราะห์ความเสี่ยงด้านเทคโนโลยี

| **ความเสี่ยงด้านเทคโนโลยี** | |
|---|---|
| **ลำดับที่** | **ประเด็นความเสี่ยง** |
| **1** | **บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย** |
| | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย |
| **2** | **เครื่องคอมพิวเตอร์ติดไวรัส** |
| | คอมพิวเตอร์ติดไวรัสบูตเซกเตอร์ (Boot Sector Virus) |
| | คอมพิวเตอร์ติดไวรัสไฟล์ข้อมูล (File Virus) |
| | คอมพิวเตอร์ติดโทรจันไวรัส (Trojan Horse Virus) |
| | คอมพิวเตอร์ติดมาโครไวรัส (Macro Virus) |
| | อีเมลล์ไวรัส (Email Virus) |

ตารางที่ 4.8 ผลการวิเคราะห์และสังเคราะห์ความเสี่ยงด้านข้อมูล

| **ความเสี่ยงด้านข้อมูล** | |
|---|---|
| **ลำดับที่** | **ประเด็นความเสี่ยง** |
| **1** | **ไม่มีการ Update ข้อมูล** |
| | สิทธิต่างๆของผู้ป่วยเปลี่ยนแต่ไม่มีการแก้ไขในระบบ |
| | ค่ารักษาพยาบาลเปลี่ยนแปลง แต่หน้าจอยังแสดงค่าเดิม |
| | ข้อมูลบุคลากรในระบบกับสถานะปัจจุบันไม่ตรงกัน |
| **2** | **ข้อมูลสูญหาย** |
| | ข้อมูลเวชระเบียนผู้ป่วยสูญหายบางรายการ/ทั้งหมด |
| | รายชื่อคนไข้หายไปจากระบบ |
| | ข้อมูลของบุคลากรหายไป |
| | รายการค่ารักษาพยาบาลบางรายการของผู้ป่วยหายไป |
| **3** | **ย้ายหรือถ่ายโอนข้อมูลไม่ได้** |
| | ย้ายข้อมูลคนไข้จากวอร์ดหนึ่งไปยังอีกวอร์ดหนึ่งไม่ได้ |
| | จำหน่ายข้อมูลคนไข้ไม่ได้ |
| **4** | **ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ** |
| | ค้นหาข้อหาข้อมูลที่ต้องการใช้ ในอินเตอร์เน็ตไม่พบ |
| | ค้นหาข้อหาข้อมูลที่ต้องการใช้ ในระบบโรงพยาบาลไม่พบ |

ตารางที่ 4.9 ผลการวิเคราะห์และสังเคราะห์ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์

| ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ | |
|---|---|
| **ลำดับที่** | **ประเด็นความเสี่ยง** |
| **1** | **แก้ไขโปรแกรมไม่ทัน** |
| | แก้ไขโปรแกรมไม่ทัน |
| **2** | **ระบบคอมพิวเตอร์ล่ม** |
| | ระบบคอมพิวเตอร์ล่ม |
| **3** | **เครื่องคอมพิวเตอร์ทำงานช้า** |
| | Down load ข้อมูลต่างๆได้ช้า |
| | คอมพิวเตอร์ประมวลผลช้า |
| | ใช้เวลานานในการเข้าโปรแกรมต่างๆ |
| **4** | **โปรแกรมทำงานผิดพลาด** |
| | พิมพ์ใบเสร็จรับเงินแต่ข้อมูลออกมาไม่ครบแต่หน้าจอแสดงข้อมูลครบ |
| | บันทึกข้อมูลลงไปในโปรแกรมไม่ได้ |
| | เวลาในระบบไม่ตรงกับเวลาจริง |
| | ข้อมูลที่แสดงบนหน้าจอกับที่พิมพ์ออกมาไม่ตรงกัน |
| **5** | **สั่งพิมพ์(Print)ข้อมูลไม่ได้** |
| | สั่งพิมพ์สติ๊กเกอร์ไม่ออก |
| | สั่งพิมพ์ใบเสร็จรับเงินไม่ได้ |
| | สั่งพิมพ์ใบนัดหมายคนไข้ไม่ได้ |
| | สั่งพิมพ์บัตรไม่ได้ |
| | สั่งพิมพ์เอกสารต่างๆไม่ได้ |
| **6** | **Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน** |
| | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน |
| **7** | **เข้าใช้งานโปรแกรมไม่ได้** |
| | เข้าใช้งานโปรแกรมไม่ได้ |
| **8** | **คอมพิวเตอร์ Restart เอง** |
| | คอมพิวเตอร์ Restart เอง |

ตารางที่ 4.9 ผลการวิเคราะห์และสังเคราะห์ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ (ต่อ)

| ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ | |
|---|---|
| **ลำดับที่** | **ประเด็นความเสี่ยง** |
| **9** | **CD-ROM ใช้งานไม่ได้** |
| | เครื่องมองไม่เห็น CD-ROM |
| | CD-ROM ไม่อ่านแผ่นCD |
| **10** | **หน้าจอค้างสีฟ้า (Blue Screen of Death)** |
| | หน้าจอค้างสีฟ้า (Blue Screen of Death) |
| **11** | **จำนวน Computer ไม่เพียงพอต่อการใช้งาน** |
| | จำนวน Computer ไม่เพียงพอต่อการใช้งาน |

ตารางที่ 4.10 ผลการวิเคราะห์และสังเคราะห์ความเสี่ยงด้านกฎหมาย

| ความเสี่ยงด้านกฎหมาย | |
|---|---|
| **ลำดับที่** | **ประเด็นความเสี่ยง** |
| **1** | **ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์** |
| | ใช้โปรแกรมบางประเภทกับคอมพิวเตอร์หลายเครื่องเกินจำนวนที่ Software License กำหนด |
| | บุคลากรนำ Software ละเมิดลิขสิทธิ์มาลงใช้เอง |

### 4.4.2 ประเด็นความเสี่ยงทั้งหมด

หลังจากทำการวิเคราะห์และสังเคราะห์ความเสี่ยงทั้งหมด 54 ความเสี่ยง จากความเสี่ยงด้านต่างๆ คือ ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านเทคโนโลยี ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ และความเสี่ยงด้านกฎหมาย สามารถสรุปเป็นประเด็นความเสี่ยงได้ทั้งหมด 23 ประเด็นความเสี่ยงดังนี้

ตารางที่ 4.11 สรุปประเด็นความเสี่ยงทั้งหมด

| ลำดับที่ | ประเด็นความเสี่ยง |
|---|---|
| 1 | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี |
| 2 | บุคลากรใช้งานโปรแกรมไม่เป็น |
| 3 | บุคลากรคีย์ข้อมูลผิด |
| 4 | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น |
| 5 | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต |
| 6 | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย |
| 7 | เครื่องคอมพิวเตอร์ติดไวรัส |
| 8 | ไม่มีการ Update ข้อมูล |
| 9 | ข้อมูลสูญหาย |
| 10 | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ |
| 11 | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ |
| 12 | แก้ไขโปรแกรมไม่ทัน |
| 13 | ระบบคอมพิวเตอร์ล่ม |
| 14 | เครื่องคอมพิวเตอร์ทำงานช้า |
| 15 | โปรแกรมทำงานผิดพลาด |
| 16 | สั่งพิมพ์(Print)ข้อมูลไม่ได้ |
| 17 | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน |
| 18 | เข้าใช้งานโปรแกรมไม่ได้ |
| 19 | คอมพิวเตอร์ Restart เอง |
| 20 | CD-ROM ใช้งานไม่ได้ |
| 21 | หน้าจอค้างสีฟ้า (Blue Screen of Death) |
| 22 | จำนวน Computer ไม่เพียงพอต่อการใช้งาน |
| 23 | ใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์ |

ประเด็นความเสี่ยงทั้งหมดทั้ง 23 ประเด็น จะถูกนำไปประเมินความเสี่ยงในขั้นตอนต่อไป เพื่อทำการพิจารณาว่าประเด็นความเสี่ยงใดอยู่ในระดับที่ยอมรับได้หรือประเด็นความเสี่ยงใดอยู่ในระดับที่ยอมรับไม่ได้ และเพื่อจัดลำดับว่าประเด็นความเสี่ยงใดมีความสำคัญมากน้อยเพียงใด

# บทที่ 5

# การประเมินความเสี่ยงและจัดลำดับความเสี่ยง

หลังจากทำการระบุความเสี่ยงเสร็จสิ้นแล้ว ขั้นตอนต่อมาคือการประเมินความเสี่ยง การประเมินความเสี่ยงนั้นมีวัตถุประสงค์เพื่อวิเคราะห์และประเมินค่าของความเสี่ยงแต่ละประเด็น ซึ่งการประเมินความเสี่ยงนั้นจะทำให้ทราบว่าประเด็นความเสี่ยงนั้นมีความสำคัญมากน้อยเพียงใดต่อการดำเนินงานขององค์กร โดยประเด็นความเสี่ยงที่มีค่า RPN สูงกว่าจะถือว่ามีความสำคัญมากกว่าประเด็นความเสี่ยงที่มีค่า RPN ต่ำกว่า และประเด็นความเสี่ยงที่มีค่า RPN สูงกว่าจะต้องได้รับการบริหารจัดการก่อนประเด็นความเสี่ยงที่มีค่า RPN ต่ำกว่าเสมอ นอกจากนี้การประเมินความเสี่ยงยังมีวัตถุประสงค์เพื่อเป็นตัวกำหนดว่าความเสี่ยงใดอยู่ในระดับที่ยอมรับได้หรือความเสี่ยงใดอยู่ในระดับที่ยอมรับไม่ได้ ซึ่งประเด็นความเสี่ยงที่อยู่ในระดับที่ยอมรับได้จะไม่จำเป็นต้องสร้างแผนจัดการความเสี่ยง ส่วนประเด็นความเสี่ยงที่อยู่ในระดับที่ยอมรับไม่ได้จะต้องสร้างแผนจัดการความเสี่ยง โดยการประเมินความเสี่ยงในการวิจัยชิ้นนี้จะใช้การประเมินความเสี่ยงโดยใช้ค่า RPN (Risk Priority Number) ซึ่งจะทำการพิจารณาให้คะแนนแต่ละประเด็นความเสี่ยงโดยพิจารณาจาก3 ปัจจัยดังต่อไปนี้ 1.ความรุนแรงของความเสี่ยง (Severity; S) 2.โอกาสในการเกิดความเสี่ยง (Occurrence; O) 3.ความสามารถในการตรวจพบความเสี่ยง (Detection; D)

## 5.1 หลักเกณฑ์การประเมินความเสี่ยง

สำหรับหลักเกณฑ์การประเมินความเสี่ยงนั้น จะใช้หลักการของ RPN (Risk Priority Number) ซึ่งจะทำการพิจารณาให้คะแนนแต่ละประเด็นความเสี่ยงโดยพิจารณาจาก3 ปัจจัยดังต่อไปนี้ 1.ความรุนแรงของความเสี่ยง (Severity; S) 2.โอกาสในการเกิดความเสี่ยง (Occurrence; O) 3.ความสามารถในการตรวจพบความเสี่ยง (Detection; D) ซึ่งมีรายละเอียดดังต่อไปนี้

- ความรุนแรงของความเสี่ยง (Severity; S)

สำหรับความรุนแรงของความเสี่ยงอันเกิดจากการใช้คอมพิวเตอร์และอินเตอร์เน็ตในโรงพยาบาลจะพิจารณาความรุนแรงโดยพิจารณาจากผลกระทบทางด้าน การสูญเสียเวลาการทำงานและผลกระทบต่อผู้ป่วยหรือผู้มารับบริการ โดยจะพิจารณาให้คะแนนอยู่ในระดับ 1-5 คะแนน

ตามลำดับความรุนแรงหากความเสี่ยงนั้นๆเกิดขึ้น โดยเกณฑ์การให้คะแนนความรุนแรงของความเสี่ยงได้แสดงไว้ในตารางที่ 5.1

ตารางที่ 5.1 การกำหนดระดับความรุนแรงของความเสี่ยง (S)

| ระดับคะแนน | ความรุนแรง | ความหมาย |
|---|---|---|
| 1 | น้อยมาก | ■ เสียเวลาการทำงานน้อยมาก<br>■ ส่งผลกระทบต่อผู้ป่วยน้อยมาก |
| 2 | น้อย | ■ เสียเวลาการทำงานน้อย<br>■ ส่งผลกระทบต่อผู้ป่วยน้อย |
| 3 | ปานกลาง | ■ เสียเวลาการทำงานปานกลาง<br>■ ส่งผลกระทบต่อผู้ป่วยปานกลาง |
| 4 | มาก | ■ เสียเวลาการทำงานมาก<br>■ ส่งผลกระทบต่อผู้ป่วยมาก |
| 5 | มากที่สุด | ■ เสียเวลาการทำงานมากที่สุด<br>■ ส่งผลกระทบต่อผู้ป่วยมากที่สุด<br>■ ขัดต่อกฎหมาย |

เนื่องจากการพิจารณาให้คะแนนความรุนแรงของความเสี่ยงต้องทำการพิจารณาผลกระทบ 2 ด้านหลักๆ คือ การสูญเสียเวลาการทำงานและผลกระทบต่อผู้ป่วย ดังนั้นจะมีบางกรณีที่คะแนนความรุนแรงของความเสี่ยงจะมีความขัดแย้งกันอยู่ กล่าวคืออาจจะมีบางความเสี่ยงที่หากเกิดขึ้นอาจจะเสียเวลาการทำงานอยู่ในระดับหนึ่งแต่กลับมีผลกระทบต่อผู้ป่วยอยู่อีกระดับหนึ่ง ซึ่งหากเกิดเหตุการณ์ในกรณีนี้จะต้องพิจารณาให้คะแนนความรุนแรงของความเสี่ยงที่อยู่ในระดับที่สูงกว่าเสมอ

ยกตัวอย่างเช่น ความเสี่ยง ก. หากเกิดขึ้นทำให้เสียเวลาการทำงานปานกลาง ซึ่งระดับคะแนนที่ต้องให้ คือ 3 แต่ในขณะเดียวกันความเสี่ยง ก. หากเกิดขึ้นจะส่งผลกระทบต่อผู้ป่วยมาก ซึ่งระดับคะแนนที่ต้องให้ คือ 4 ในกรณีนี้สามารถสรุประดับคะแนนความรุนแรงของความเสี่ยงได้เท่ากับ 4 กล่าวคือให้คะแนนตามคะแนนความรุนแรงของความเสี่ยงที่อยู่ในระดับที่สูงกว่า

และหากความเสี่ยงใดๆก็ตามหากเกิดขึ้นแล้วส่งผลกระทบทำให้ขัดต่อกฎหมายจะถือว่าความเสี่ยงนั้นอยู่ในระดับคะแนนความรุนแรงของความเสี่ยงขั้นสูงที่สุดเสมอ

- โอกาสในการเกิดความเสี่ยง (Occurrence; O)

สำหรับโอกาสในการเกิดความเสี่ยง จะพิจารณาให้คะแนนอยู่ในระดับ 1-5 คะแนนเช่นเดียวกับระดับความรุนแรงของความเสี่ยง โดยเกณฑ์การให้คะแนนโอกาสในการเกิดความเสี่ยงได้แสดงไว้ในตารางที่ 5.2

ตารางที่ 5.2 การกำหนดระดับโอกาสในการเกิดความเสี่ยง (O)

| ระดับคะแนน | โอกาสเกิด | ความหมาย |
|---|---|---|
| 1 | น้อยมาก | ■ เกิดได้เฉพาะสถานการณ์ผิดปกติ : ทุกปี |
| 2 | น้อย | ■ สามารถเกิดขึ้นได้น้อยครั้ง : ทุก 6 เดือน |
| 3 | ปานกลาง | ■ อาจเกิดขึ้นได้บ้าง บางโอกาส : ทุกเดือน |
| 4 | มาก | ■ เกิดขึ้นได้เป็นปกติมักเกิดซ้ำบ่อยๆ : ทุกสัปดาห์ |
| 5 | มากที่สุด | ■ ไม่สามารถหลีกเลี่ยงได้ มีโอกาสเกิดสูงมาก : ทุกวัน |

- ความสามารถในการตรวจพบความเสี่ยง (Detection; D)

สำหรับความสามารถในการตรวจพบความเสี่ยง สามารถพิจารณาได้จากประสิทธิภาพขององค์กรในการตรวจพบความเสี่ยงหากความเสี่ยงนั้นเกิดขึ้น และสามารถพิจารณาได้จากการควบคุมที่มีอยู่เดิมในการป้องกันไม่ให้ความเสี่ยงนั้นเกิดขึ้น ซึ่งการพิจารณาให้คะแนนความสามารถในการตรวจพบความเสี่ยงจะให้คะแนนอยู่ในระดับ 1-5 คะแนน โดยเกณฑ์การให้คะแนนความสามารถในการตรวจพบความเสี่ยงได้แสดงไว้ในตารางที่ 5.3

ตารางที่ 5.3 การกำหนดระดับความสามารถในการตรวจพบความเสี่ยง (D)

| ระดับคะแนน | ประสิทธิภาพ | ความหมาย |
|---|---|---|
| 1 | สูงที่สุด | ■ สามารถตรวจพบได้แน่นอนเป็นส่วนใหญ่/มีการควบคุมที่ดีมาก |
| 2 | สูง | ■ มีโอกาสสูงในการตรวจพบ/มีการควบคุมที่ดี |
| 3 | ปานกลาง | ■ อาจตรวจพบได้ในบางครั้ง/มีการควบคุมปานกลาง |
| 4 | ต่ำ | ■ มีโอกาสตรวจพบน้อยมาก/มีการควบคุมที่ไม่ค่อยดี |
| 5 | ต่ำมาก | ■ ไม่สามารถตรวจพบได้เลย/ไม่มีการควบคุม |

**5.2 หลักเกณฑ์การยอมรับได้และยอมรับไม่ได้ของความเสี่ยง**

นอกจากจะมีการกำหนดหลักเกณฑ์ในการประเมินความเสี่ยงแล้ว จะต้องมีการกำหนดหลักเกณฑ์การยอมรับและไม่ยอมรับความเสี่ยงด้วย เพื่อเป็นการพิจารณาว่าประเด็นความเสี่ยงใดที่สามารถยอมรับได้หรือยอมรับไม่ได้ เพื่อเป็นการกำหนดว่าประเด็นความเสี่ยงใดที่ต้องสร้างแผนจัดการความเสี่ยง โดยประเด็นความเสี่ยงที่อยู่ในระดับที่ยอมรับได้จะไม่จำเป็นต้องสร้างแผนจัดการความเสี่ยง ส่วนประเด็นความเสี่ยงที่อยู่ในระดับที่ยอมรับไม่ได้จะต้องสร้างแผนจัดการความเสี่ยง ซึ่งในงานวิจัยชิ้นนี้ได้มีการกำหนดเกณฑ์การยอมรับได้และยอมรับไม่ได้ของแต่ละประเด็นความเสี่ยงโดยอิงตามค่า RPN ของแต่ละประเด็นความเสี่ยงดังต่อไปนี้

ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับมากที่สุด(คะแนน=5) หากมีค่า RPN น้อยกว่าหรือเท่ากับ 20 จะถือว่าประเด็นความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับมาก(คะแนน=4) หากมีค่า RPN น้อยกว่าหรือเท่ากับ 16 จะถือว่าประเด็นความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับปานกลาง(คะแนน=3) หากมีค่า RPN น้อยกว่าหรือเท่ากับ 12 จะถือว่าประเด็นความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับน้อย(คะแนน=2) หากมีค่า RPN น้อยกว่าหรือเท่ากับ 8 จะถือว่าประเด็นความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับน้อยมาก(คะแนน=1) หากมีค่า RPN น้อยกว่าหรือเท่ากับ 4 จะถือว่าประเด็นความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

กล่าวโดยสรุปก็คือ ประเด็นความเสี่ยงที่อยู่ในระดับที่ยอมรับได้จะต้องมีระดับโอกาสในการเกิดโดยเฉลี่ยเมื่อคิดรวมเป็นค่า RPN อยู่ในระดับน้อย (คะแนน=2) หรือน้อยมาก (คะแนน=1) และในทำนองเดียวกันประเด็นความเสี่ยงที่อยู่ในระดับที่ยอมรับได้จะต้องมีระดับการตรวจพบหรือระดับการควบคุมอยู่ในระดับประสิทธิภาพที่สูง (คะแนน=2) หรือสูงที่สุด (คะแนน=1)

**5.3 วิธีการและผู้มีส่วนเกี่ยวข้องในการประเมินความเสี่ยง**

สำหรับวิธีการในการประเมินความเสี่ยงนั้นจะใช้วิธีการใช้แบบสอบถามในการประเมินความเสี่ยง (แบบสอบถามที่ใช้ในการประเมินความเสี่ยงแสดงไว้ในภาคผนวก ก-2) สำหรับผู้ที่มีส่วน

เกี่ยวข้องในการประเมินความเสี่ยงนั้นจะต้องเป็นผู้ที่มีประสบการณ์ในการทำงานสูงหรืออาจจะเป็นผู้ที่มีความรู้ทางด้านการใช้คอมพิวเตอร์และอินเตอร์เน็ตในโรงพยาบาล และจะต้องเป็นบุคลากรที่ทำงานอยู่ในระบบงานด้านบริการผู้ป่วย หรือ เป็นบุคลากรที่ทำงานอยู่ในระบบงานด้าน Back Office ของทางโรงพยาบาล ซึ่งบุคลากรผู้มีส่วนเกี่ยวข้องในการประเมินความเสี่ยงมีรายละเอียดดังต่อไปนี้

- หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ 1 คน
- ตัวแทนหัวหน้าสำนักงานพัฒนาคุณภาพ 1 คน
- ตัวแทนระบบงานบริการผู้ป่วย 1 คน
- ตัวแทนระบบงาน Back Office 1 คน

รวม 4 คน
อายุงานเฉลี่ย 12 ปี

นอกจากบุคลากรภายในองค์กรผู้เกี่ยวข้องในการประเมินความเสี่ยงที่ได้กล่าวไปแล้วในข้างต้น การประเมินความเสี่ยงในงานวิจัยชิ้นนี้ยังมีผู้เกี่ยวข้องอีก 1 คน คือผู้ชำนาญงานคอมพิวเตอร์และอินเตอร์เน็ตจากภายนอกองค์กร ซึ่งจะเป็นผู้ให้คำปรึกษาทางด้านระดับความรุนแรงและโอกาสในเกิดความเสี่ยงนั้นๆ

## 5.4 ผลการประเมินความเสี่ยง

จากการตอบแบบสอบถามของบุคลากรผู้เกี่ยวข้องในการประเมินความเสี่ยงสามารถสรุปออกมาเป็นคะแนนจากการประเมินความเสี่ยงและสรุปออกมาเป็นค่า RPN ได้ดังนี้

### 5.4.1 คะแนนจากการประเมินความเสี่ยง

สำหรับคะแนนจากการประเมินความเสี่ยงของความเสี่ยงแต่ละประเด็นในด้านของ ระดับความรุนแรงของความเสี่ยง (S), ระดับโอกาสในการเกิดความเสี่ยง (O) และระดับความสามารถในการตรวจพบความเสี่ยง (D) ได้แสดงไว้ในตารางที่ 5.4 และได้แสดงตัวอย่างผลกระทบของประเด็นความเสี่ยง 23 ประเด็นความเสี่ยงไว้ในภาคผนวก ข

ตารางที่ 5.4 คะแนนที่ได้จากการประเมินความเสี่ยง

| ข้อ | ประเด็นความเสี่ยง | ระดับคะแนน | | |
|---|---|---|---|---|
| | | S | O | D |
| 1 | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | 4 | 3 | 3 |
| 2 | บุคลากรใช้งานโปรแกรมไม่เป็น | 4 | 2 | 3 |
| 3 | บุคลากรคีย์ข้อมูลผิด | 4 | 5 | 2 |
| 4 | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | 3 | 5 | 3 |
| 5 | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | 4 | 5 | 3 |
| 6 | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | 3 | 3 | 4 |
| 7 | เครื่องคอมพิวเตอร์ติดไวรัส | 5 | 5 | 4 |
| 8 | ไม่มีการUpdateข้อมูล | 4 | 4 | 2 |
| 9 | ข้อมูลสูญหาย | 5 | 5 | 2 |
| 10 | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | 4 | 5 | 3 |
| 11 | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | 2 | 4 | 4 |
| 12 | แก้ไขโปรแกรมไม่ทัน | 3 | 3 | 4 |
| 13 | ระบบคอมพิวเตอร์ล่ม | 5 | 4 | 4 |
| 14 | เครื่องคอมพิวเตอร์ทำงานช้า | 4 | 3 | 4 |
| 15 | โปรแกรมทำงานผิดพลาด | 4 | 4 | 3 |
| 16 | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | 4 | 5 | 2 |
| 17 | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | 2 | 3 | 3 |
| 18 | เข้าใช้งานโปรแกรมไม่ได้ | 5 | 4 | 3 |
| 19 | คอมพิวเตอร์ Restart เอง | 5 | 4 | 4 |
| 20 | CD-ROM ใช้งานไม่ได้ | 2 | 3 | 3 |
| 21 | หน้าจอค้างสีฟ้า (Blue Screen of Death) | 5 | 2 | 4 |
| 22 | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | 4 | 3 | 2 |
| 23 | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | 5 | 2 | 4 |

### 5.4.2 สรุปค่า RPN

หลังจากได้คะแนนของความเสี่ยงแต่ละประเด็นในด้านของ ระดับความรุนแรงของความเสี่ยง (S), ระดับโอกาสในการเกิดความเสี่ยง (O) และระดับความสามารถในการตรวจพบความเสี่ยง (D) จากนั้นทำการคำนวณหาค่า RPN ของประเด็นความเสี่ยงทั้งหมด สำหรับค่า RPN สามารถคำนวณได้โดยนำคะแนนทั้งสามส่วนคือ ระดับความรุนแรงของความเสี่ยง (S), ระดับโอกาสในการเกิดความเสี่ยง (O) และระดับความสามารถในการตรวจพบความเสี่ยง (D) มาคูณกัน (RPN = S x O x D) ซึ่งค่า RPN ของประเด็นความเสี่ยงทั้งหมดได้แสดงไว้ในตารางที่ 5.5

ตารางที่ 5.5 สรุปค่า RPN ของประเด็นความเสี่ยงทั้งหมด

| ข้อ | ประเด็นความเสี่ยง | ระดับคะแนน | | | |
|---|---|---|---|---|---|
| | | S | O | D | RPN |
| 1 | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | 4 | 3 | 3 | **36** |
| 2 | บุคลากรใช้งานโปรแกรมไม่เป็น | 4 | 2 | 3 | **24** |
| 3 | บุคลากรคีย์ข้อมูลผิด | 4 | 5 | 2 | **40** |
| 4 | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | 3 | 5 | 3 | **45** |
| 5 | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | 4 | 5 | 3 | **60** |
| 6 | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | 3 | 3 | 4 | **36** |
| 7 | เครื่องคอมพิวเตอร์ติดไวรัส | 5 | 5 | 4 | **100** |
| 8 | ไม่มีการUpdateข้อมูล | 4 | 4 | 2 | **32** |
| 9 | ข้อมูลสูญหาย | 5 | 5 | 2 | **50** |
| 10 | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | 4 | 5 | 3 | **60** |
| 11 | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | 2 | 4 | 4 | **32** |
| 12 | แก้ไขโปรแกรมไม่ทัน | 3 | 3 | 4 | **36** |
| 13 | ระบบคอมพิวเตอร์ล่ม | 5 | 4 | 3 | **60** |
| 14 | เครื่องคอมพิวเตอร์ทำงานช้า | 4 | 3 | 4 | **48** |
| 15 | โปรแกรมทำงานผิดพลาด | 4 | 4 | 3 | **48** |
| 16 | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | 4 | 5 | 2 | **40** |

ตารางที่ 5.5 สรุปค่า RPN ของประเด็นความเสี่ยงทั้งหมด (ต่อ)

| ข้อ | ประเด็นความเสี่ยง | ระดับคะแนน | | | |
|---|---|---|---|---|---|
| | | S | O | D | RPN |
| 17 | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | 2 | 3 | 3 | **18** |
| 18 | เข้าใช้งานโปรแกรมไม่ได้ | 5 | 4 | 3 | **60** |
| 19 | คอมพิวเตอร์ Restart เอง | 5 | 4 | 4 | **80** |
| 20 | CD-ROM ใช้งานไม่ได้ | 2 | 3 | 3 | **18** |
| 21 | หน้าจอค้างสีฟ้า (Blue Screen of Death) | 5 | 2 | 4 | **40** |
| 22 | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | 4 | 3 | 2 | **24** |
| 23 | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | 5 | 2 | 4 | **40** |

### 5.4.3 การพิจารณาความเสี่ยงที่ยอมรับได้และยอมรับไม่ได้

หลังจากทำการสรุปค่า RPN ของประเด็นความเสี่ยงทั้งหมดเสร็จสิ้นแล้ว ขั้นตอนต่อมาคือการพิจารณาว่าประเด็นความเสี่ยงใดอยู่ในระดับที่ยอมรับได้หรืออยู่ในระดับที่ยอมรับไม่ได้ โดยการพิจารณาจะใช้หลักเกณฑ์ในการพิจารณาที่กำหนดไว้ในหัวข้อที่ 5.2 และจากการพิจารณาพบว่าประเด็นความเสี่ยงทั้งหมดอยู่ในระดับยอมรับไม่ได้ กล่าวคือ ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับมากที่สุด (คะแนน=5) มีค่า RPN มากกว่า 20, ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับมาก (คะแนน=4) มีค่า RPN มากกว่า 16, ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับปานกลาง(คะแนน=3) มีค่า RPN มากกว่า 12 และประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับน้อย (คะแนน=2) มีค่า RPN มากกว่า 8 ดังนั้นประเด็นความเสี่ยงทั้งหมด 23 ประเด็น จะต้องสร้างแผนจัดการความเสี่ยง

## 5.5 การจัดลำดับความเสี่ยง

หลังจากทำการประเมินความเสี่ยงเสร็จสิ้นแล้ว ขั้นตอนต่อมาคือ การจัดลำดับความเสี่ยง เพื่อทำการเรียงลำดับความสำคัญของความเสี่ยง ซึ่งการเรียงลำดับความเสี่ยงนั้นจะถือว่าประเด็นความเสี่ยงที่มีค่า RPN สูงกว่ามีความสำคัญมากกว่าประเด็นความเสี่ยงที่มีค่า RPN ต่ำกว่า และหากประเด็นความเสี่ยงใดๆมีค่า RPN เท่ากัน สามารถที่จะจัดลำดับความสำคัญของความเสี่ยงนั้นๆได้โดยพิจารณาจาก

ระดับคะแนนความรุนแรงของประเด็นความเสี่ยงนั้นๆ หากระดับคะแนนความรุนแรงของประเด็นความเสี่ยงใดมีค่าสูงกว่าก็จะถือว่าประเด็นความเสี่ยงนั้นมีลำดับความสำคัญมากกว่า และหากพิจารณาระดับความรุนแรงของความเสี่ยงนั้นๆแล้วพบว่ามีระดับคะแนนความรุนแรงเท่ากันก็จะถือว่าประเด็นความเสี่ยงนั้นๆ มีความ สำคัญอยู่ในระดับเดียวกัน

เนื่องจากประเด็นความเสี่ยงที่มีค่า RPN สูงกว่า จะถือว่าเป็นประเด็นความเสี่ยงที่มีความรุนแรงมากกว่าประเด็นความเสี่ยงที่มีค่า RPN ต่ำกว่า มีโอกาสในการเกิดสูงกว่าประเด็นความเสี่ยงที่มีค่า RPN ต่ำกว่า และมีระดับในการตรวจพบหรือระดับการควบคุมที่มีอยู่เดิมอยู่ในระดับที่แย่กว่าประเด็นความเสี่ยงที่มีค่า RPN ต่ำกว่า หรือกล่าวโดยสรุปคือ ประเด็นความเสี่ยงที่มีค่า RPN สูงกว่า มีโอกาสที่จะก่อให้เกิดความเสียหายต่อองค์กรได้มากกว่าประเด็นความเสี่ยงที่มีค่า RPN ต่ำกว่า ดังนั้นจึงต้องให้ความสำคัญในการบริหารจัดการความเสี่ยงนั้นๆก่อนเสมอ

ผลการจัดลำดับความเสี่ยงตามระดับคะแนนค่า RPN จากระดับคะแนนค่า RPN จากมากไปน้อยได้แสดงไว้ในตารางที่ 5.6

ตารางที่ 5.6 ผลการจัดลำดับความเสี่ยงตามระดับคะแนนค่า RPN จากมากไปน้อย

| ข้อ | ประเด็นความเสี่ยง | ระดับคะแนน | | | |
|---|---|---|---|---|---|
| | | **S** | **O** | **D** | **RPN** |
| 1 | เครื่องคอมพิวเตอร์ติดไวรัส | 5 | 5 | 4 | **100** |
| 2 | คอมพิวเตอร์ Restart เอง | 5 | 4 | 4 | **80** |
| 3 | ระบบคอมพิวเตอร์ล่ม | 5 | 4 | 3 | **60** |
| | เข้าใช้งานโปรแกรมไม่ได้ | 5 | 4 | 3 | **60** |
| 4 | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | 4 | 5 | 3 | **60** |
| | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | 4 | 5 | 3 | **60** |
| 5 | ข้อมูลสูญหาย | 5 | 5 | 2 | **50** |
| 6 | เครื่องคอมพิวเตอร์ทำงานช้า | 4 | 3 | 4 | **48** |
| | โปรแกรมทำงานผิดพลาด | 4 | 4 | 3 | **48** |
| 7 | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | 3 | 5 | 3 | **45** |
| 8 | หน้าจอค้างสีฟ้า (Blue Screen of Death) | 5 | 2 | 4 | **40** |
| | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | 5 | 2 | 4 | **40** |
| 9 | บุคลากรคีย์ข้อมูลผิด | 4 | 5 | 2 | **40** |
| | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | 4 | 5 | 2 | **40** |
| 10 | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | 4 | 3 | 3 | **36** |
| 11 | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | 3 | 3 | 4 | **36** |
| | แก้ไขโปรแกรมไม่ทัน | 3 | 3 | 4 | **36** |
| 12 | ไม่มีการUpdateข้อมูล | 4 | 4 | 2 | **32** |
| 13 | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | 2 | 4 | 4 | **32** |
| 14 | บุคลากรใช้งานโปรแกรมไม่เป็น | 4 | 2 | 3 | **24** |
| | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | 4 | 3 | 2 | **24** |
| 15 | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | 2 | 3 | 3 | **18** |
| | CD-ROM ใช้งานไม่ได้ | 2 | 3 | 3 | **18** |

เมื่อพิจารณาจากผลการจัดลำดับความเสี่ยงตามตารางที่ 5.6 พบว่า ประเด็นความเสี่ยงทั้งหมด 23 ประเด็นความเสี่ยง เมื่อทำการจัดลำดับความเสี่ยงจะทำการจัดลำดับได้ทั้งหมด 15 ลำดับ และประเด็นความเสี่ยงทั้งหมดทั้ง 15 ลำดับจะต้องถูกนำไปสร้างแผนจัดการความเสี่ยงในขั้นตอนต่อไปเรียงตามลำดับความสำคัญ

# บทที่ 6

# การสร้างและการประยุกต์ใช้แผนจัดการความเสี่ยง

เมื่อทำการประเมินความเสี่ยงและทำการจัดลำดับความเสี่ยงเสร็จสิ้นแล้ว ขั้นตอนต่อไป คือ การสร้างแผนจัดการความเสี่ยง ซึ่งแผนการจัดการความเสี่ยงที่ดีนั้นจะต้องสร้างขึ้นมาโดยพิจารณาจากปัจจัยหรือสาเหตุพื้นฐานของความเสี่ยงนั้นๆ ดังนั้นสิ่งที่ต้องทำในขั้นตอนแรกของการสร้างแผนจัดการความเสี่ยง คือ การวิเคราะห์ปัจจัยเสี่ยงหรือการวิเคราะห์สาเหตุพื้นฐานของการเกิดความเสี่ยง ซึ่งในงานวิจัยชิ้นนี้จะใช้วิธีการ Fault Tree Analysis หรือ FTA ในการวิเคราะห์สาเหตุพื้นฐานของการเกิดความเสี่ยง และเมื่อทำการวิเคราะห์สาเหตุพื้นฐานของการเกิดความเสี่ยงเสร็จสิ้นแล้ว ขั้นตอนต่อไปคือการสร้างแผนจัดการความเสี่ยง ซึ่งการสร้างแผนจัดการความเสี่ยงจะเป็นไปโดยยึดแนวทางในการสร้างแผนจัดการความเสี่ยง 4 แนวทาง ได้แก่

1. Take-การยอมรับความเสี่ยง (Risk Acceptance)
2. Treat-การลด/ควบคุมความเสี่ยง (Risk Reduction/Control)
3. Terminate-การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)
4. Transfer-การกระจาย/โอนความเสี่ยง (Risk Sharing/Spreading)

และนอกจากการสร้างแผนจัดการความเสี่ยงโดยใช้แนวทาง 4 แนวทางที่กล่าวไปแล้วข้างต้น แผนจัดการความเสี่ยงที่สร้างขึ้นมาต้องพิจารณาความเหมาะสมด้วยซึ่งงานวิจัยชิ้นนี้จะพิจารณาความเหมาะสมของแผนจัดการความเสี่ยงโดยพิจารณาความเหมาะสมใน 2 ด้าน คือ

ก. ความมีประสิทธิภาพของแผนจัดการความเสี่ยง

ข. ความเป็นไปได้ในการปฏิบัติตามแผนจัดการความเสี่ยง

และหลังจากเสร็จสิ้นขั้นตอนการสร้างแผนจัดการความเสี่ยงแล้วขั้นตอนต่อไปคือการนำเอาแผนจัดการความเสี่ยงที่ได้ไปประยุกต์ใช้ในโรงพยาบาลที่ทำการวิจัย

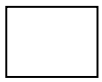
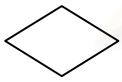
## 6.1 การวิเคราะห์สาเหตุพื้นฐานของการเกิดความเสี่ยง

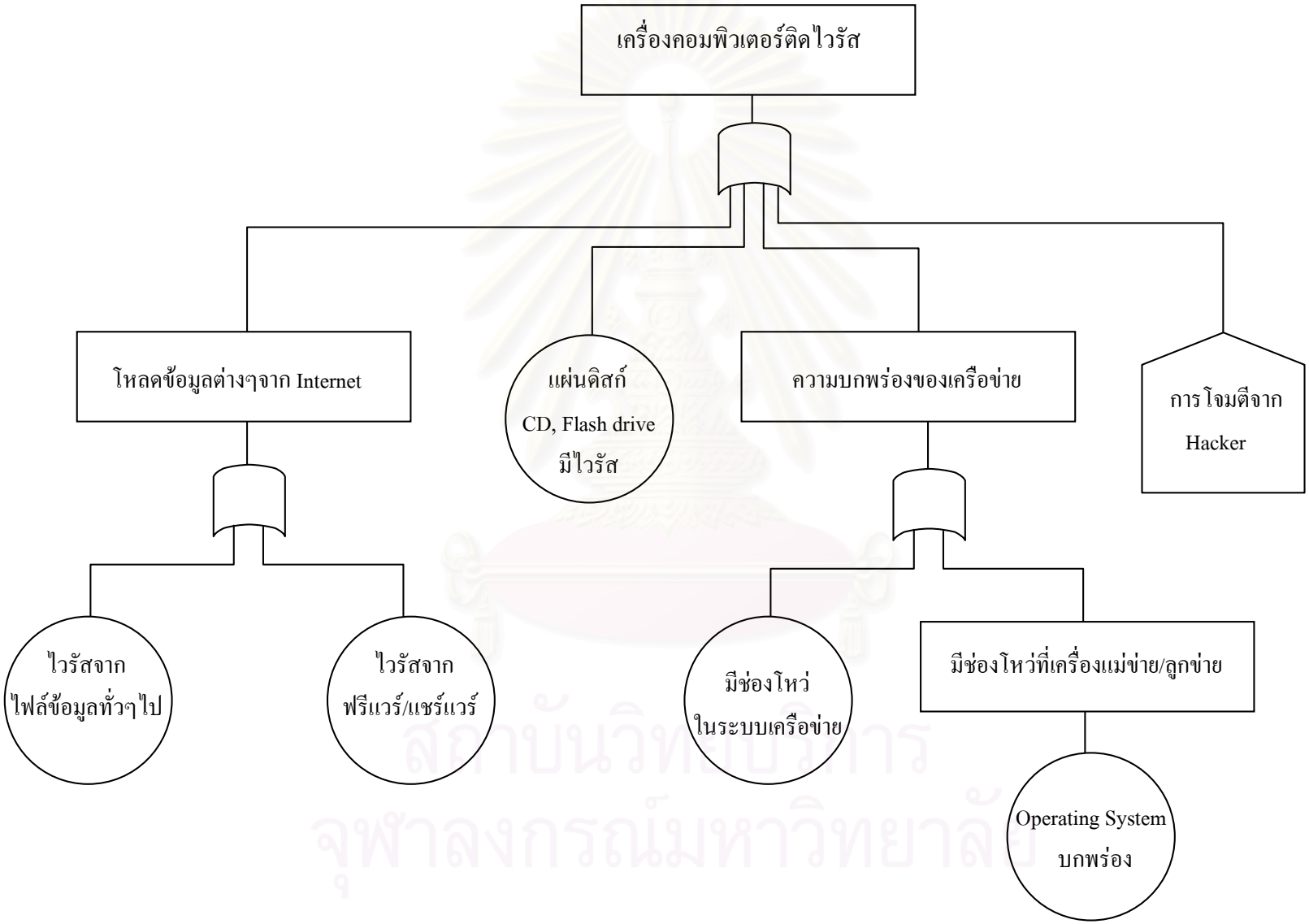
การวิเคราะห์สาเหตุพื้นฐานของการเกิดความเสี่ยงจะใช้วิธีการ Fault Tree Analysis หรือ FTA หรือในภาษาไทยเรียกว่า วิธีการการวิเคราะห์แขนงความบกพร่องหรือแผนภูมิต้นไม้ (Tree Diagrams) ซึ่งเป็นการวิเคราะห์หาสาเหตุของความบกพร่องต่างๆที่เกี่ยวข้องกับงานวิธีการทำงานและกระบวนการ

ต่างๆอย่างเป็นระบบ แสดงให้เห็นถึงความเกี่ยวโยงที่จะนำไปสู่เหตุการณ์ที่ไม่ต้องการให้เกิดขึ้น เพื่อจะได้นำข้อมูลที่ได้มาหามาตรฐานในการควบคุมและป้องกันต่อไป ซึ่งวิธีการวิเคราะห์แบบ FTA นั้น การวิเคราะห์จะแสดงความสัมพันธ์ของเหตุการณ์ต่าง ๆ ด้วยรูปภาพทำให้เห็นภาพได้อย่างชัดเจน และเข้าใจง่ายขึ้น โดยสัญลักษณ์ต่างๆที่ใช้ในการวิเคราะห์แบบ FTA นั้นได้แสดงไว้ในตารางที่ 6.1

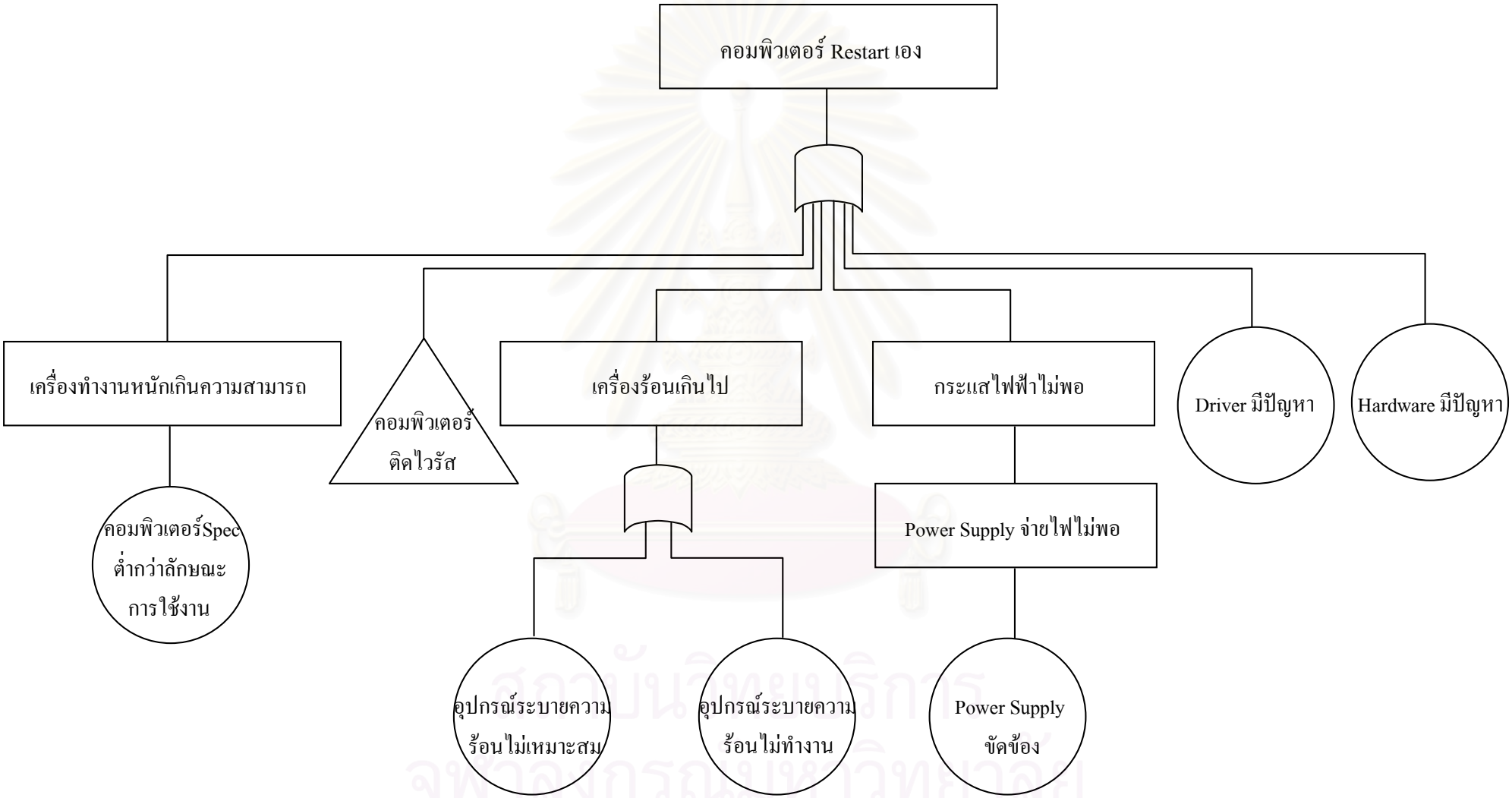
ส่วนวิธีการสร้างแผนผังแบบ FTA สามารถสรุปได้ดังนี้ สาเหตุที่ยังสามารถวิเคราะห์ต่อลงไปได้อีกจะเขียนแทนด้วยรูปสี่เหลี่ยม  ส่วนสาเหตุที่เป็นสาเหตุย่อยที่เกิดได้ตามปกติไม่ต้องวิเคราะห์ต่อไปจะเขียนแทนด้วยรูปวงกลม  ส่วนเหตุการณ์ที่เกิดขึ้นจากปัจจัยภายนอกที่อาจเกิดขึ้นได้หรือไม่ก็ได้จะเขียนแทนด้วยรูปห้าเหลี่ยม  และเมื่อต้องการอ้างถึงเหตุการณ์ที่อยู่ในแผนผังอื่นๆ ซึ่งมีรายละเอียดเหมือนกันจะเขียนแทนด้วยรูปสามเหลี่ยม  ส่วนสัญลักษณ์ที่ใช้เชื่อมต่อเหตุการณ์ต่างๆเข้าด้วยกันมี 2 แบบคือ แบบ “และ” เขียนแทนด้วยรูป  และแบบ “หรือ” เขียนแทนด้วยรูป  เหตุการณ์ที่เชื่อมด้วย “และ” หมายถึง จะต้องเกิดเหตุการณ์ที่เป็นสาเหตุย่อยทุกเหตุการณ์ขึ้นพร้อมกันจึงจะเกิดเหตุการณ์นั้นขึ้นได้ ส่วนเหตุการณ์ที่เชื่อมด้วย “หรือ” หมายถึง หากเหตุการณ์ย่อยเกิดขึ้นเพียงเหตุการณ์เดียว ก็ทำให้เกิดเหตุการณ์นั้นได้ และจากการวิเคราะห์สาเหตุพื้นฐานของการเกิดความเสี่ยงโดยใช้วิธีการ FTA ของประเด็นความเสี่ยงทั้งหมด 23 ประเด็นความเสี่ยง เรียงลำดับตามค่า RPN จากมากไปน้อย ได้ผลการวิเคราะห์ดังรูปที่ 6.1-6.23

ตารางที่ 6.1 สัญลักษณ์ที่ใช้ในการวิเคราะห์ Fault Tree Analysis (FTA)

| ประเภท | สัญลักษณ์ | ชื่อ | ความหมาย |
|---|---|---|---|
| Event Symbol |  | Fault Event | เหตุการณ์อยู่ระหว่างกลาง (Intermediate Event) เป็นเหตุการณ์ย่อยที่ส่งผลให้เหตุการณ์อื่นต่อไป ต้องถูกทำการวิเคราะห์ลงไปอีก |
| |  | Basic Event | เหตุการณ์ย่อยที่เกิดขึ้นได้ตามปกติเห็นได้ชัดเจนโดยไม่ต้องทำการวิเคราะห์หาสาเหตุต่อไป เป็นสาเหตุแรกของการเกิดความบกพร่องและจะอยู่ในส่วนล่างสุดของทุกๆเหตุการณ์ |
| |  | Undeveloped Event | เหตุการณ์ย่อยที่ไม่มีข้อมูลเพียงพอ หรือยุ่งยากซับซ้อนหรือเป็นข้อมูลที่ไม่เกี่ยวข้องกับ Top Event จึงไม่วิเคราะห์ต่อไป แต่ถ้ามีข้อมูลเพิ่มเติมก็สามารถวิเคราะห์ต่อไปได้ |
| |  | House Event/ External Event | เหตุการณ์ภายนอกหรือปัจจัยภายนอกที่เป็นสาเหตุให้เกิดเหตุการณ์ต่างๆต้องพิจารณาว่าจะเกิดหรือไม่บางทีเรียกว่า Switch Event หรือ Normal Event |
| |  | Tree Transfer | ใช้เขียนเพื่ออ้างถึงเหตุการณ์หนึ่งซึ่งอยู่ในกิ่งก้านอื่นของแผนภูมิซึ่งเป็นเหตุการณ์ที่เหมือนกัน โดยไม่ต้องเขียนเหตุการณ์นั้นซ้ำอีก |
| Logic Gate |  | Or Gate | แสดงความสัมพันธ์ว่าเหตุการณ์หนึ่งจะเกิดขึ้นได้จะต้องมีสาเหตุมาจากสาเหตุใดสาเหตุหนึ่งของเหตุการณ์ย่อยหรือมากกว่านั้น |
| |  | And Gate | แสดงความสัมพันธ์ว่าเหตุการณ์หนึ่งจะเกิดขึ้นได้จะต้องมีสาเหตุมาจากเหตุการณ์ย่อยทุกๆเหตุการณ์เกิดขึ้นพร้อมกัน |
| |  | Inhibit Gate | แสดงกรณีที่เหตุการณ์ใดๆจะเกิดขึ้นได้ก็ต่อเมื่อมีเงื่อนไข (Condition) หรือข้อจำกัด (Restriction) หรือองค์ประกอบอื่นๆซึ่งจะเสริมให้เกิดเหตุการณ์นั้นๆ เช่น อุณหภูมิ ความดัน เป็นต้น |

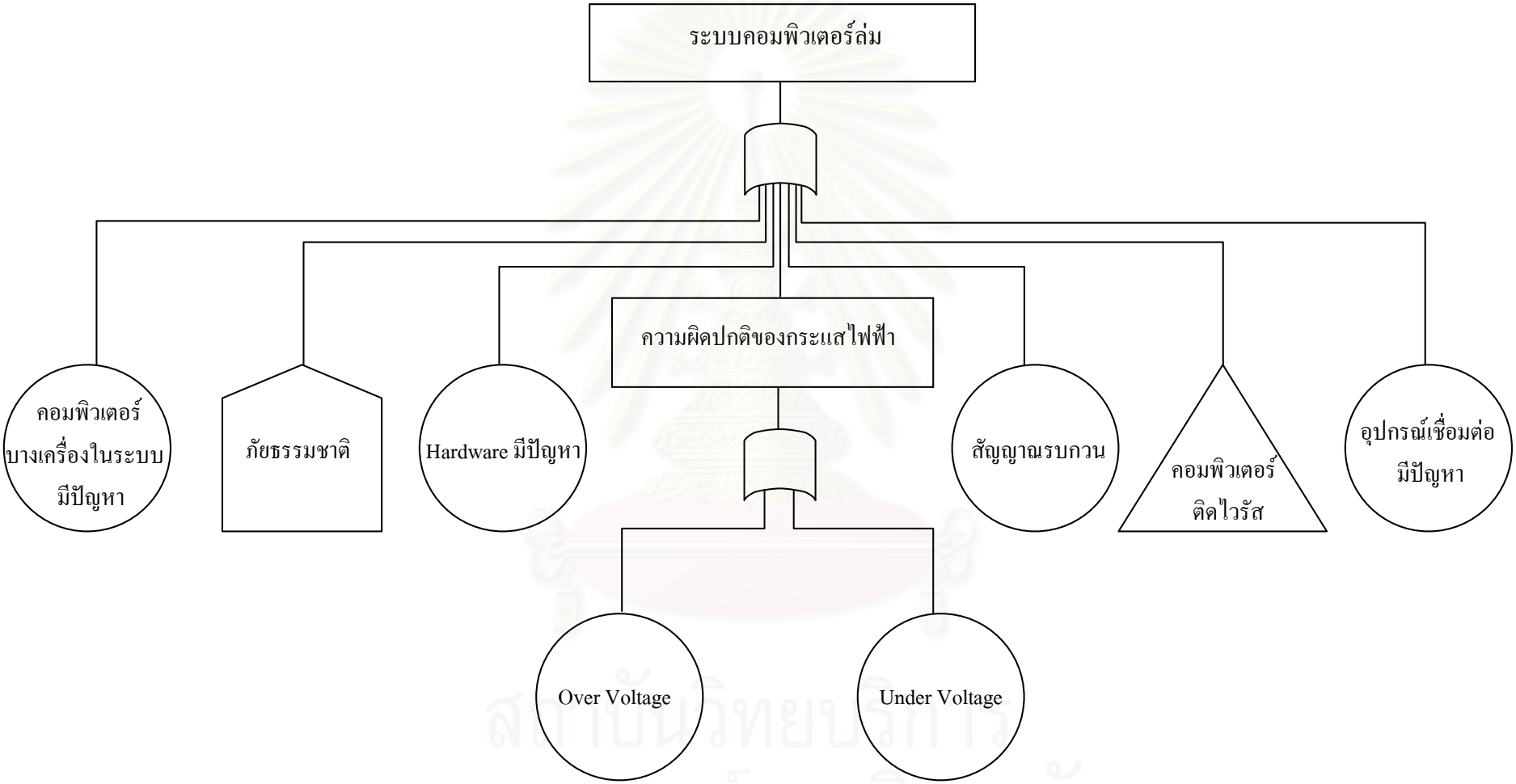



รูปที่ 6.1 FTA ของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส





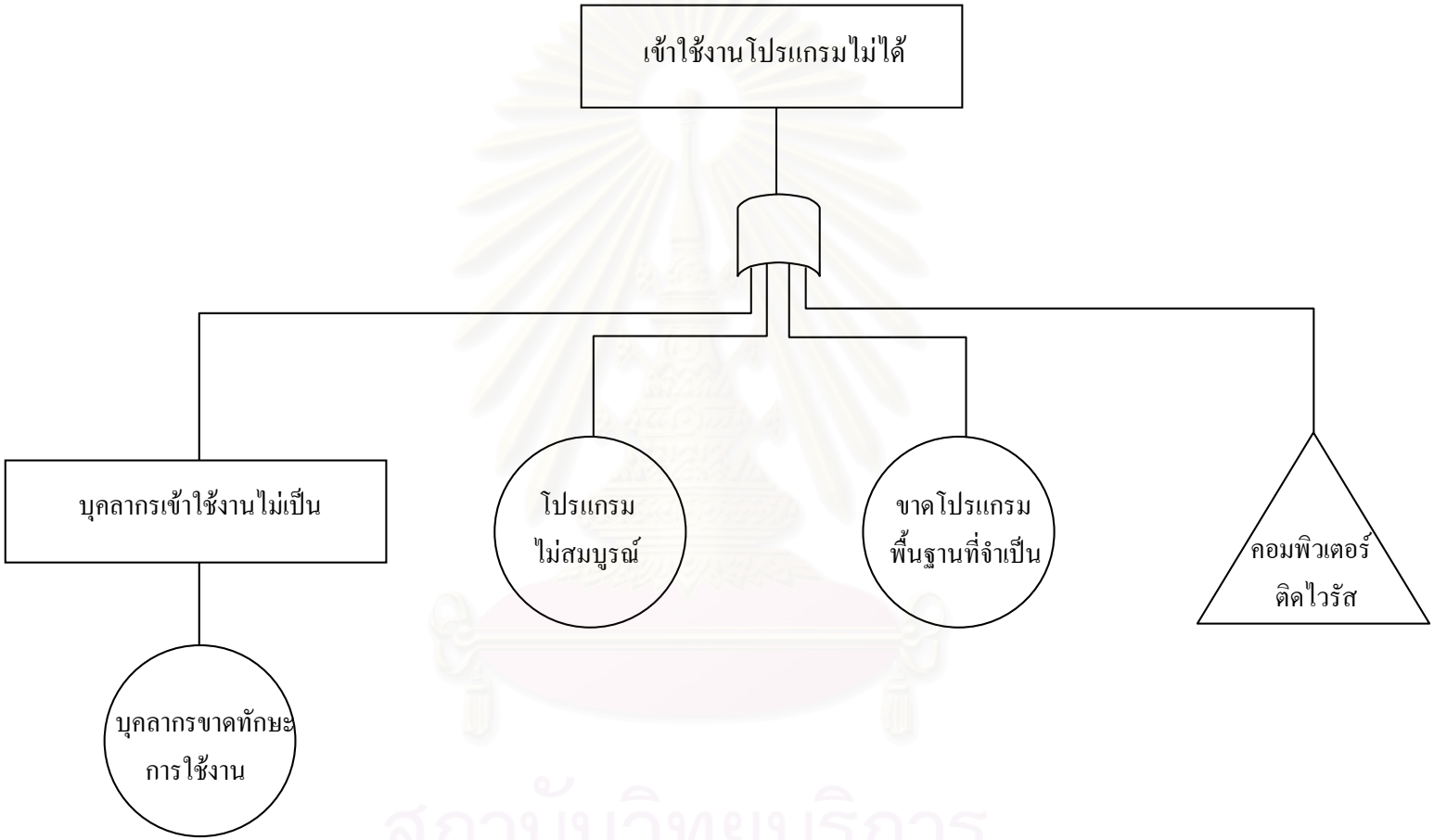

รูปที่ 6.2 FTA ของประเด็นความเสี่ยงคอมพิวเตอร์ Restart เอง








รูปที่ 6.3 FTA ของประเด็นความเสี่ยงระบบคอมพิวเตอร์ล่ม

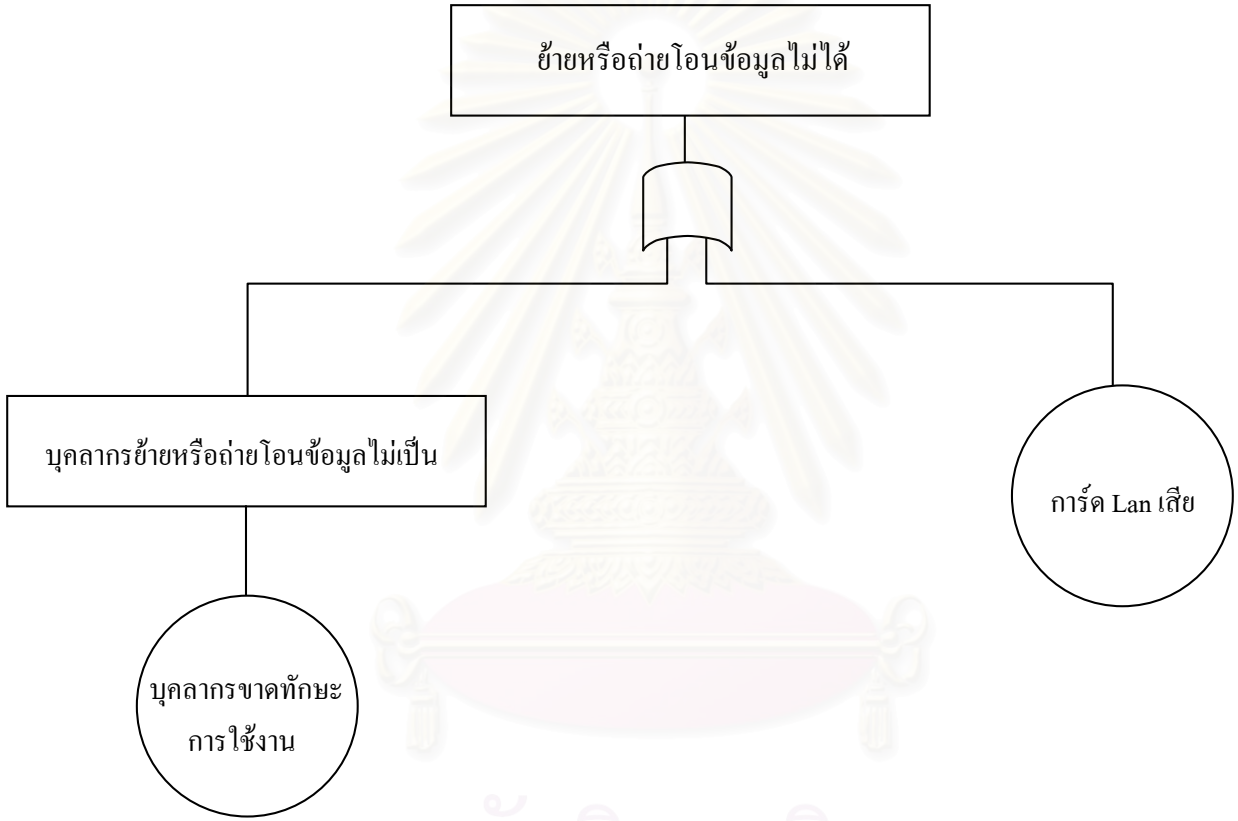



รูปที่ 6.4 FTA ของประเด็นความเสี่ยงเข้าใช้งานโปรแกรมไม่ได้



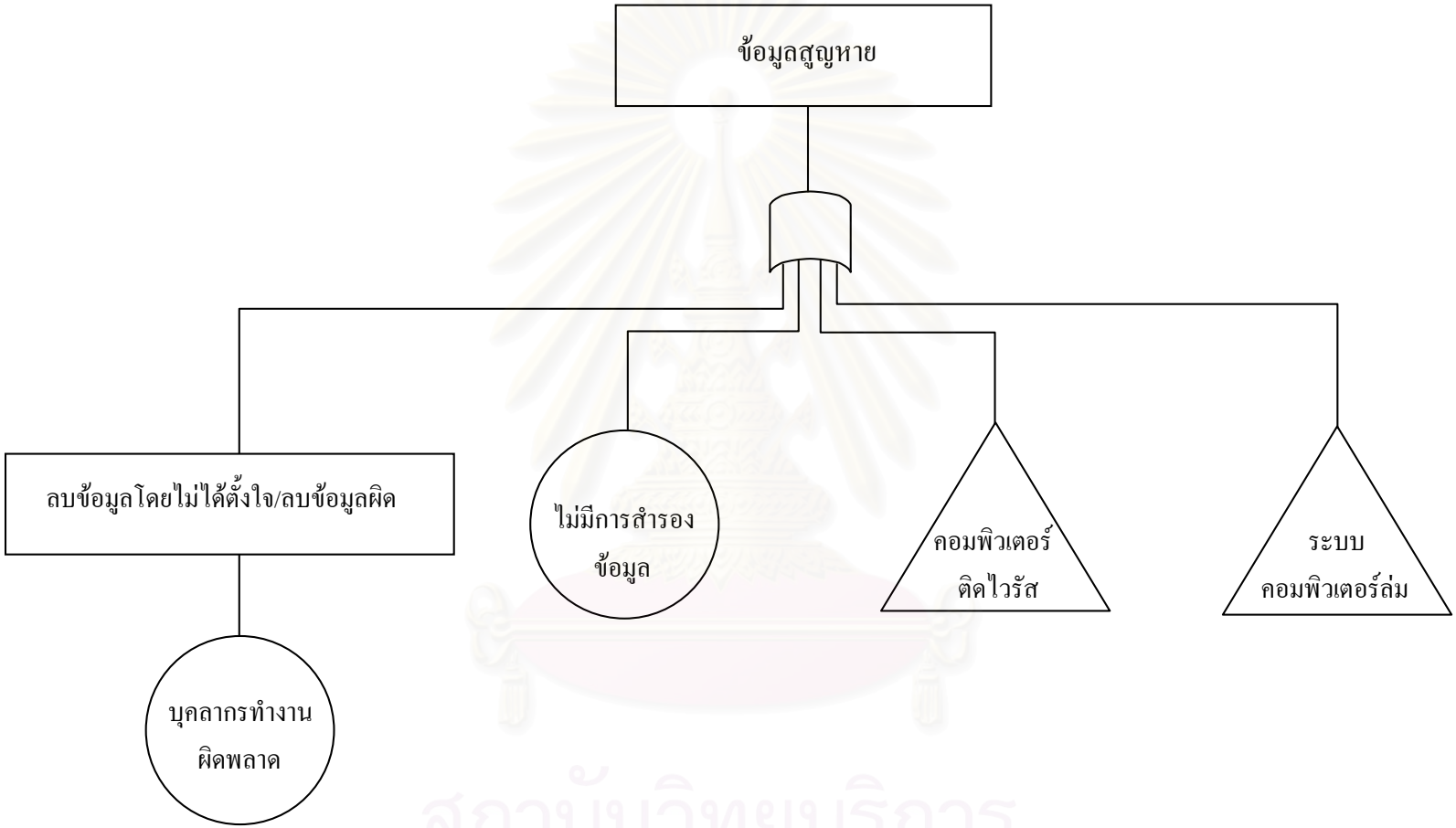

รูปที่ 6.5 FTA ของประเด็นความเสี่ยงบุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต

61

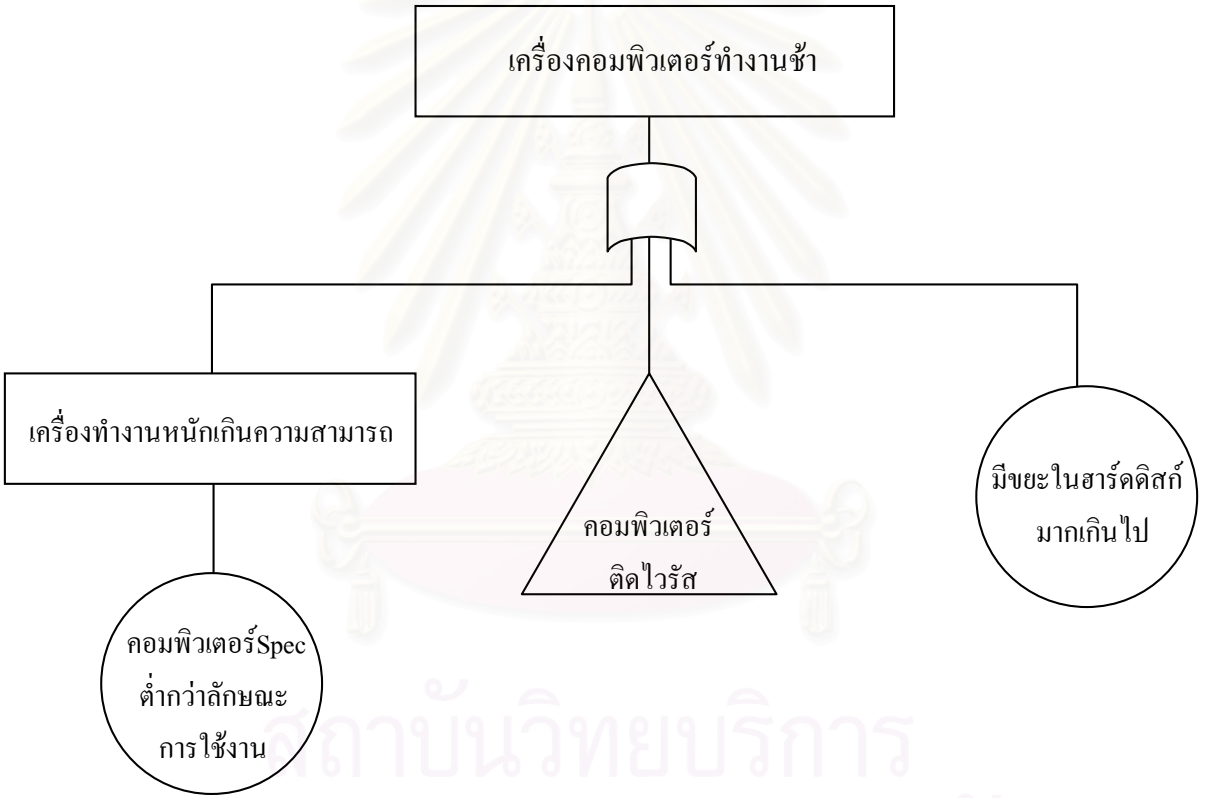





รูปที่ 6.6 FTA ของประเด็นความเสี่ยงย้ายหรือถ่ายโอนข้อมูลไม่ได้



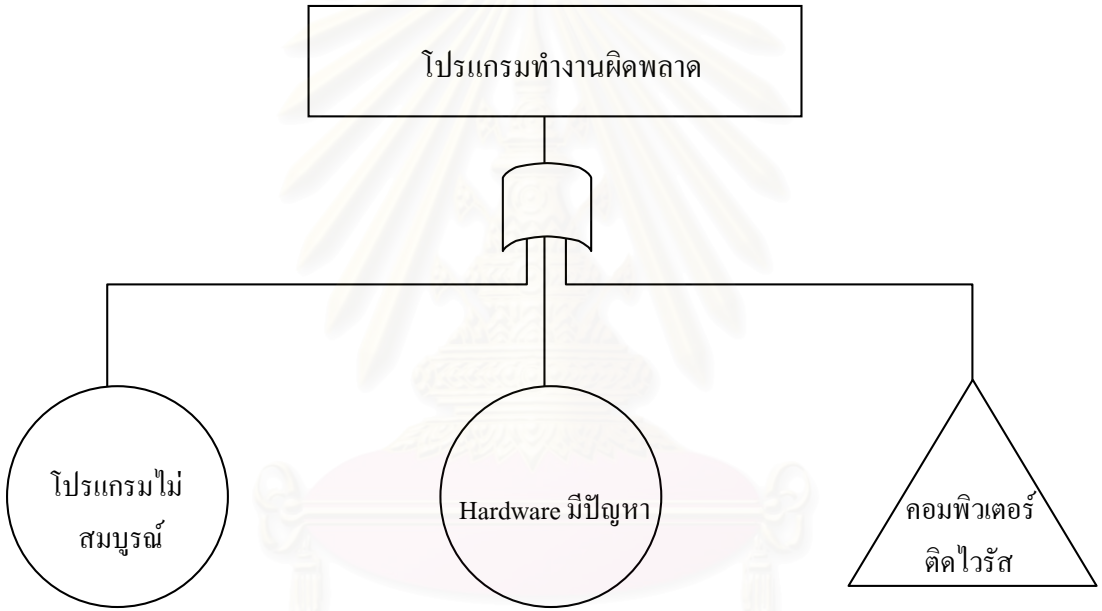

รูปที่ 6.7 FTA ของประเด็นความเสี่ยงข้อมูลสูญหาย






64

รูปที่ 6.8 FTA ของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ทำงานช้า

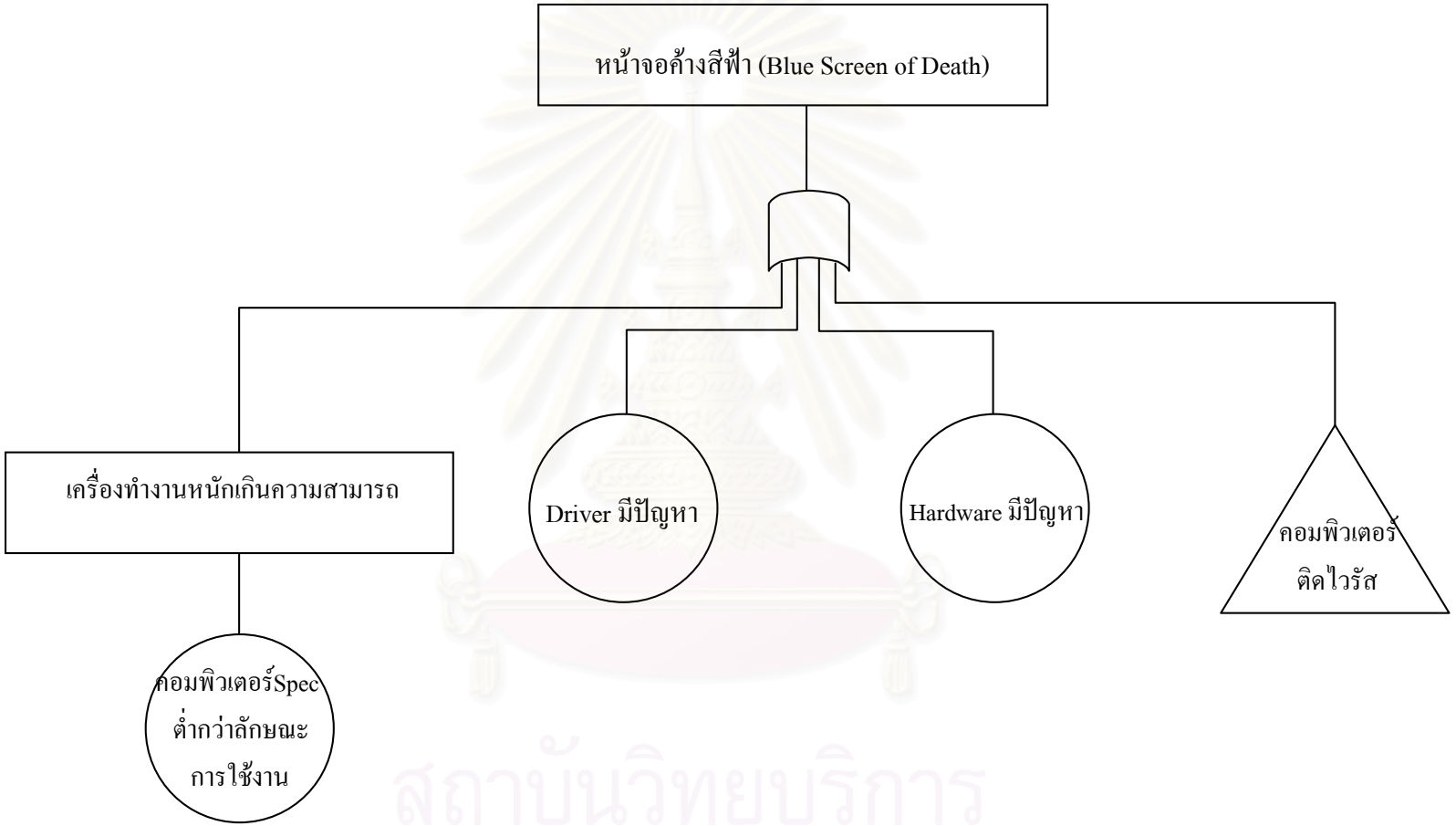





รูปที่ 6.9 FTAของประเด็นความเสี่ยงโปรแกรมทำงานผิดพลาด



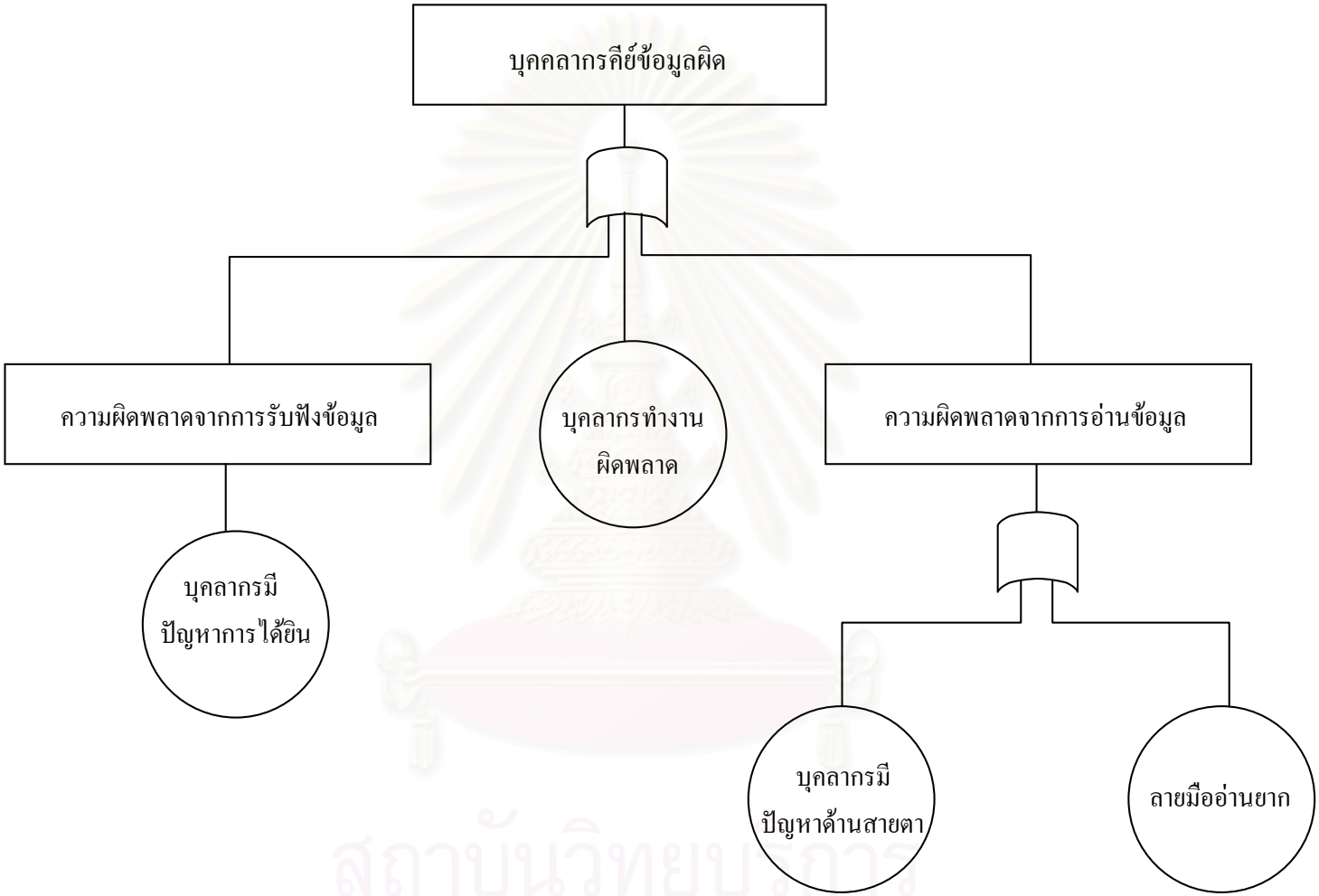

รูปที่ 6.10 FTAของประเด็นความเสี่ยงบุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น



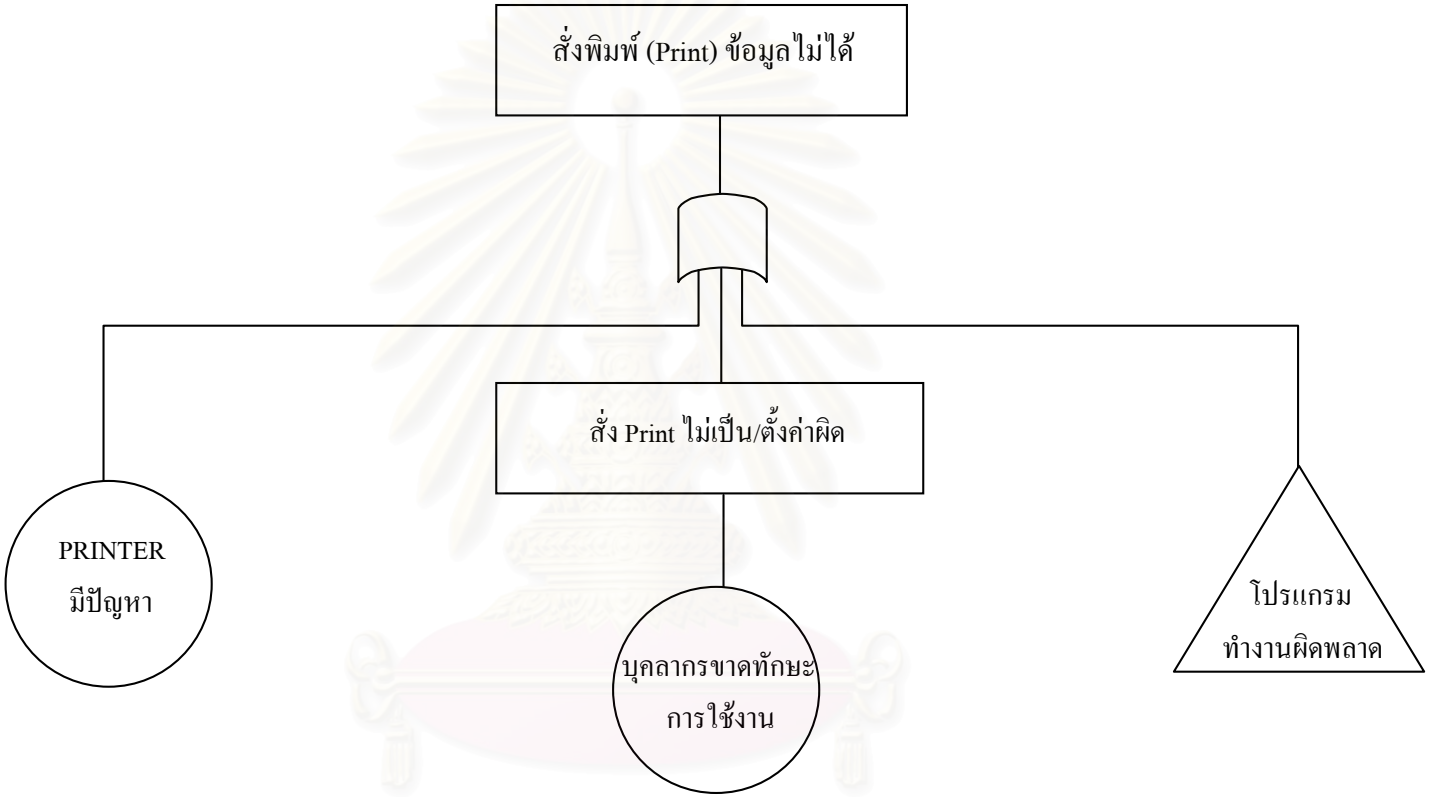

รูปที่ 6.11 FTAของประเด็นความเสี่ยงหน้าจอค้างสีฟ้า (Blue Screen of Death)




รูปที่ 6.12 FTAของประเด็นความเสี่ยงใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์




รูปที่ 6.13 FTA ของประเด็นความเสี่ยงบุคคลากรคีย์ข้อมูลผิด

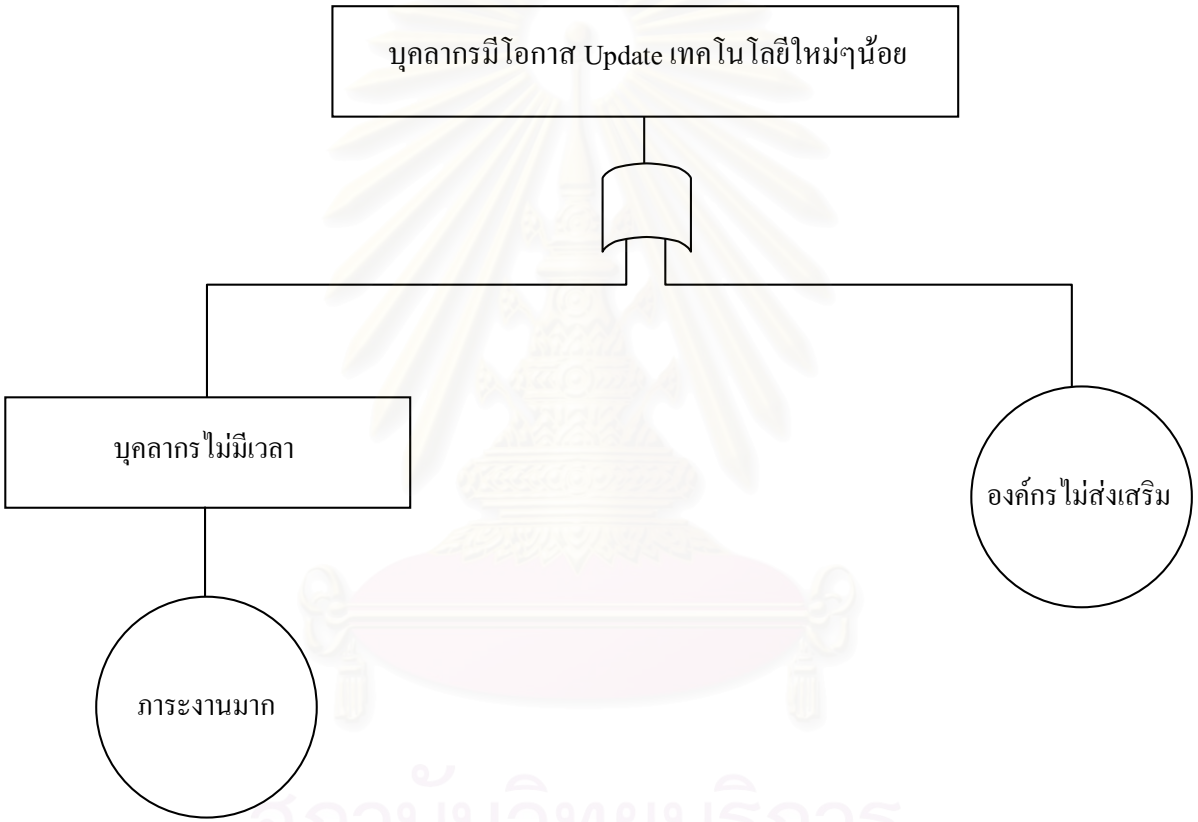





รูปที่ 6.14 FTA ของประเด็นความเสี่ยงสั่งพิมพ์ (Print) ข้อมูลไม่ได้



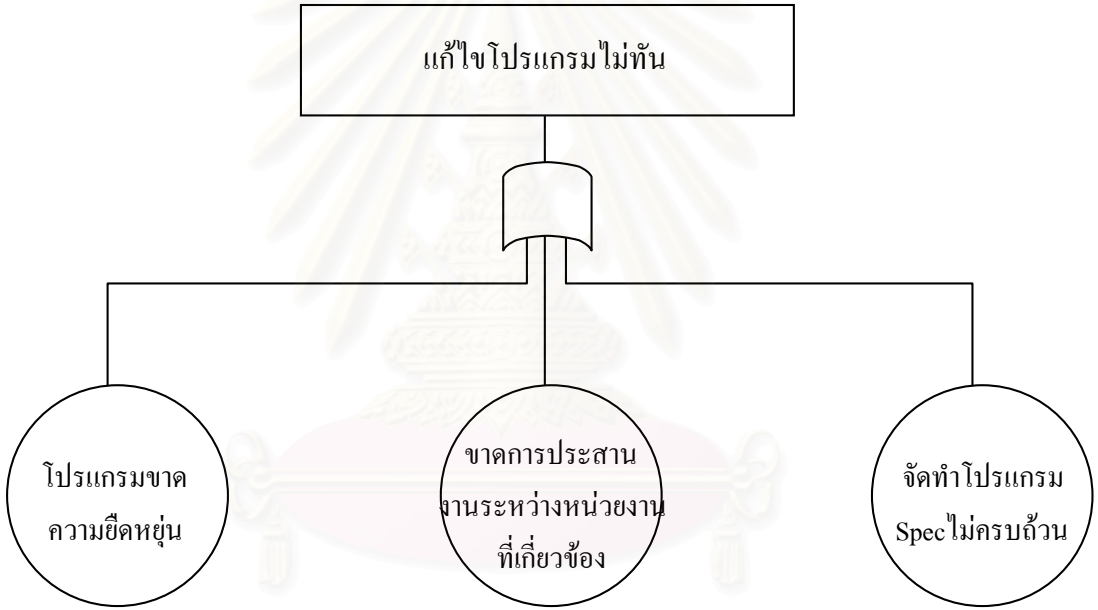

รูปที่ 6.15 FTAของประเด็นความเสี่ยงขาดบุคลากรในบางตำแหน่งที่ควรจะมี







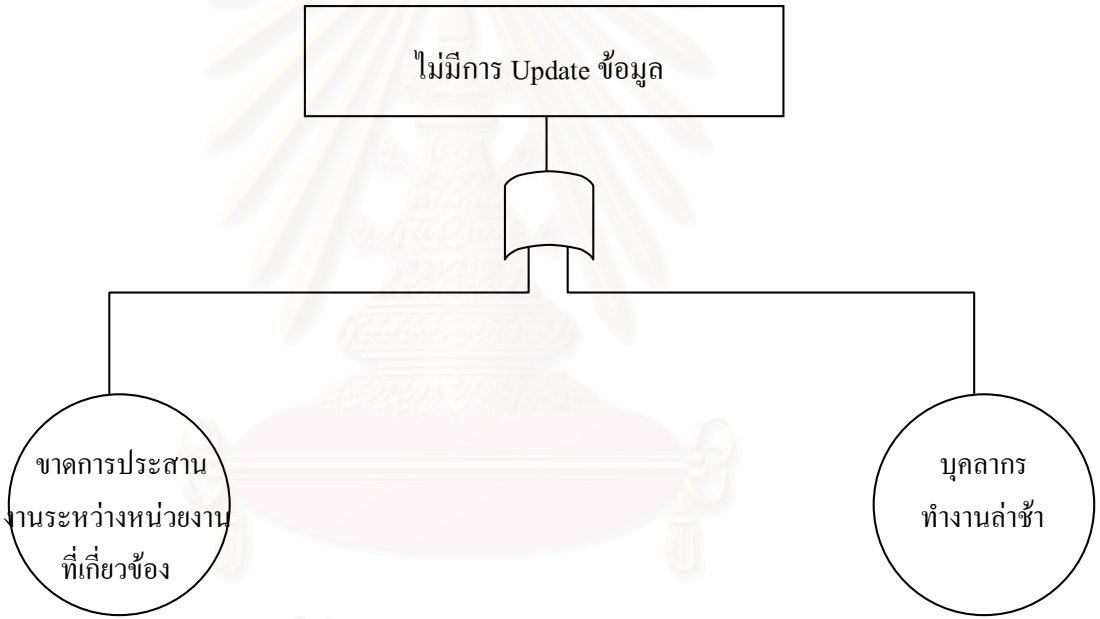

รูปที่ 6.16 FTA ของประเด็นความเสี่ยงบุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย






73

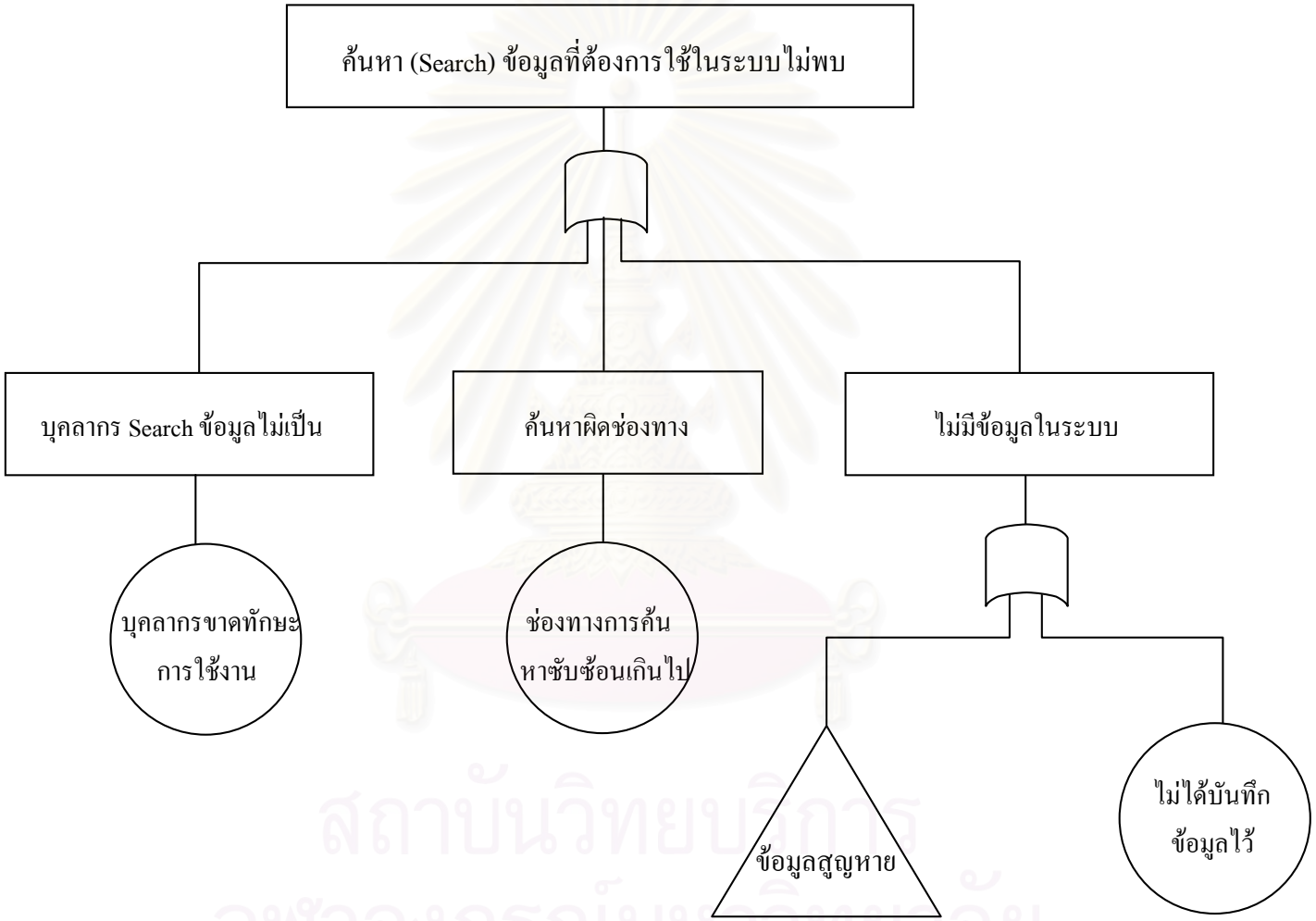
รูปที่ 6.17 FTAของประเด็นความเสี่ยงแก้ไขโปรแกรมไม่ทัน






74

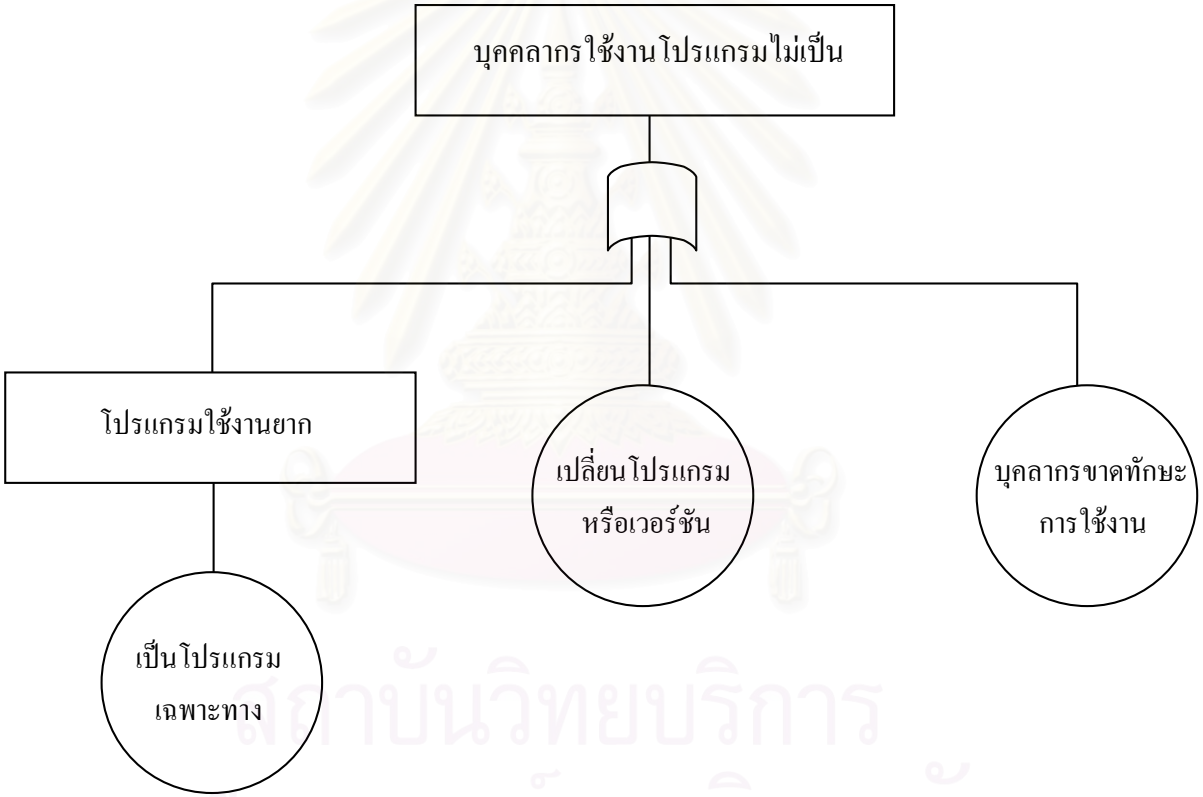
รูปที่ 6.18 FTAของประเด็นความเสี่ยงไม่มีการ Update ข้อมูล








รูปที่ 6.19 FTAของประเด็นความเสี่ยงค้นหา (Search) ข้อมูลที่ต้องการใช้ในระบบไม่พบ




รูปที่ 6.20 FTA ของประเด็นความเสี่ยงบุคคลากรใช้งานโปรแกรมไม่เป็น



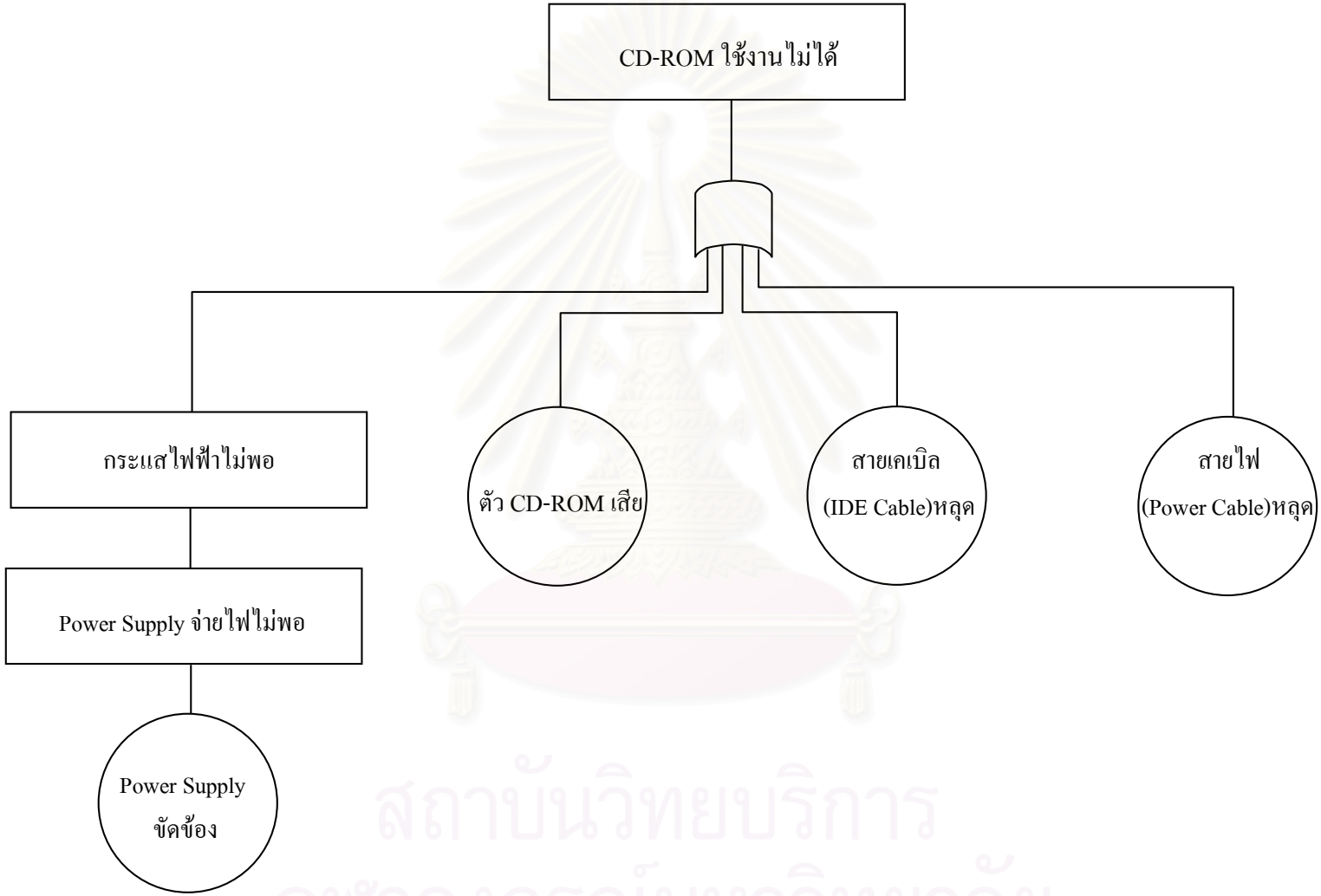



รูปที่ 6.21 FTAของประเด็นความเสี่ยงจำนวน Computer ไม่เพียงพอต่อการใช้งาน






รูปที่ 6.22 FTA ของประเด็นความเสี่ยง Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน




รูปที่ 6.23 FTAของประเด็นความเสี่ยง CD-ROM ใช้งานไม่ได้

## 6.2 สรุปสาเหตุพื้นฐานของการเกิดความเสี่ยง

หลังจากทำการวิเคราะห์หาสาเหตุพื้นฐานของประเด็นความเสี่ยงต่างๆ โดยใช้วิธีการ FTA พบว่าสาเหตุพื้นฐาน ของการเกิดประเด็นความเสี่ยงต่างๆ ส่วนใหญ่มีสาเหตุมาจากปัจจัยภายใน มีเพียงส่วนน้อยเท่านั้นที่เกิดจากปัจจัยภายนอก ซึ่งสาเหตุพื้นฐานของการเกิดความเสี่ยงส่วนใหญ่เกิดจากบุคลากร, ฮาร์ดแวร์ และ ซอฟท์แวร์ โดยสามารถสรุปสาเหตุพื้นฐานของการเกิดประเด็นความเสี่ยงต่างๆเรียงลำดับตามค่า RPN จากมากไปหาน้อย ได้ดังตารางที่6.2-6.24

ตารางที่ 6.2 สาเหตุพื้นฐานของการเกิดความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส

| **ความเสี่ยง** | **เครื่องคอมพิวเตอร์ติดไวรัส** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| <u>ปัจจัยภายใน</u><br>■ ไวรัสจากไฟล์ข้อมูลทั่วๆไป<br>■ ไวรัสจากฟรีแวร์/แชร์แวร์<br>■ แผ่นดิสก์,CD, Flash drive มีไวรัส<br>■ มีช่องโหว่ในระบบเครือข่าย<br>■ Operating System บกพร่อง<br><u>ปัจจัยภายนอก</u><br>■ การโจมตีจาก Hacker | |

ตารางที่ 6.3 สาเหตุพื้นฐานของการเกิดความเสี่ยงคอมพิวเตอร์ Restart เอง

| **ความเสี่ยง** | **คอมพิวเตอร์ Restart เอง** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| <u>ปัจจัยภายใน</u><br>■ อุปกรณ์ระบายความร้อนไม่ทำงาน<br>■ อุปกรณ์ระบายความร้อนไม่เหมาะสม<br>■ Power Supply ขัดข้อง<br>■ คอมพิวเตอร์ติดไวรัส | |

ตารางที่ 6.4 สาเหตุพื้นฐานของการเกิดความเสี่ยงระบบคอมพิวเตอร์ล่ม

| **ความเสี่ยง** | **ระบบคอมพิวเตอร์ล่ม** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| <u>ปัจจัยภายใน</u><br>■ สัญญาณรบกวน<br>■ Under Voltage<br>■ Over Voltage<br>■ Hardware มีปัญหา<br>■ คอมพิวเตอร์ติดไวรัส<br>■ คอมพิวเตอร์บางเครื่องในระบบมีปัญหา<br>■ อุปกรณ์เชื่อมต่อมีปัญหา<br><u>ปัจจัยภายนอก</u><br>■ ภัยธรรมชาติ | |

ตารางที่ 6.5 สาเหตุพื้นฐานของการเกิดความเสี่ยงเข้าใช้งานโปรแกรมไม่ได้

| **ความเสี่ยง** | **เข้าใช้งานโปรแกรมไม่ได้** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| <u>ปัจจัยภายใน</u><br>■ บุคลากรขาดทักษะการใช้งาน<br>■ โปรแกรมไม่สมบูรณ์<br>■ ขาดโปรแกรมพื้นฐานที่จำเป็น<br>■ คอมพิวเตอร์ติดไวรัส | |

ตารางที่ 6.6 สาเหตุพื้นฐานของการเกิดความเสี่ยงบุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต

| **ความเสี่ยง** | **บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| <u>ปัจจัยภายใน</u><br>■ บุคลากรขาดความรับผิดชอบ<br>■ ขาดการควบคุมการใช้งาน | |

ตารางที่ 6.7 สาเหตุพื้นฐานของการเกิดความเสี่ยงย้ายหรือถ่ายโอนข้อมูลไม่ได้

| **ความเสี่ยง** | **ย้ายหรือถ่ายโอนข้อมูลไม่ได้** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ บุคลากรขาดทักษะการใช้งาน<br>■ การ์ด Lan เสีย | |

ตารางที่ 6.8 สาเหตุพื้นฐานของการเกิดความเสี่ยงข้อมูลสูญหาย

| **ความเสี่ยง** | **ข้อมูลสูญหาย** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ บุคลากรทำงานผิดพลาด<br>■ ไม่มีการสำรองข้อมูล<br>■ ระบบคอมพิวเตอร์ล่ม<br>■ คอมพิวเตอร์ติดไวรัส | |

ตารางที่ 6.9 สาเหตุพื้นฐานของการเกิดความเสี่ยงเครื่องคอมพิวเตอร์ทำงานช้า

| **ความเสี่ยง** | **เครื่องคอมพิวเตอร์ทำงานช้า** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน<br>■ มีขยะในฮาร์ดดิสก์มากเกินไป<br>■ คอมพิวเตอร์ติดไวรัส | |

ตารางที่ 6.10 สาเหตุพื้นฐานของการเกิดความเสี่ยงโปรแกรมทำงานผิดพลาด

| **ความเสี่ยง** | **โปรแกรมทำงานผิดพลาด** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ โปรแกรมไม่สมบูรณ์<br>■ คอมพิวเตอร์ติดไวรัส<br>■ Hardware มีปัญหา | |

ตารางที่ 6.11 สาเหตุพื้นฐานของการเกิดความเสี่ยงบุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น

| **ความเสี่ยง** | **บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ บุคลากรขาดทักษะการใช้งาน<br>■ โปรแกรม Edit Dataไม่ได้หลังบันทึก | |

ตารางที่ 6.12 สาเหตุพื้นฐานของการเกิดความเสี่ยงหน้าจอค้างสีฟ้า (Blue Screen of Death)

| **ความเสี่ยง** | **หน้าจอค้างสีฟ้า (Blue Screen of Death)** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ Hardware มีปัญหา<br>■ คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน<br>■ คอมพิวเตอร์ติดไวรัส | |

ตารางที่ 6.13 สาเหตุพื้นฐานของการเกิดความเสี่ยงใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์

| **ความเสี่ยง** | **ใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ บุคลากรนำโปรแกรมมาลงเอง<br>■ บุคลากรโหลดโปรแกรมละเมิดลิขสิทธิ์จากอินเตอร์เน็ต<br>■ ละเมิด Site/Network Licens | |

ตารางที่ 6.14 สาเหตุพื้นฐานของการเกิดความเสี่ยงบุคลากรคีย์ข้อมูลผิด

| **ความเสี่ยง** | **บุคลากรคีย์ข้อมูลผิด** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ บุคลากรทำงานผิดพลาด<br>■ บุคลากรมีปัญหาการได้ยิน<br>■ บุคลากรมีปัญหาด้านสายตา<br>■ ลายมืออ่านยาก | |

ตารางที่ 6.15 สาเหตุพื้นฐานของการเกิดความเสี่ยงสั่งพิมพ์ (Print) ข้อมูลไม่ได้

| **ความเสี่ยง** | **สั่งพิมพ์ (Print) ข้อมูลไม่ได้** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ บุคลากรขาดทักษะการใช้งาน<br>■ PRINTER มีปัญหา<br>■ โปรแกรมทำงานผิดพลาด | |

ตารางที่ 6.16 สาเหตุพื้นฐานของการเกิดความเสี่ยงขาดบุคลากรในบางตำแหน่งที่ควรจะมี

| **ความเสี่ยง** | **ขาดบุคลากรในบางตำแหน่งที่ควรจะมี** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ ภาระ/ลักษณะงานเพิ่ม<br>■ ไม่มีการประเมินภาระ/ลักษณะงาน | |

ตารางที่ 6.17 สาเหตุพื้นฐานของการเกิดความเสี่ยงบุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย

| **ความเสี่ยง** | **บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ ภาระงานมาก<br>■ องค์กรไม่ส่งเสริม | |

ตารางที่ 6.18 สาเหตุพื้นฐานของการเกิดความเสี่ยงแก้ไขโปรแกรมไม่ทัน

| **ความเสี่ยง** | **แก้ไขโปรแกรมไม่ทัน** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ โปรแกรมขาดความยืดหยุ่น<br>■ ขาดการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง<br>■ จัดทำโปรแกรม Spec ไม่ครบถ้วน | |

ตารางที่ 6.19 สาเหตุพื้นฐานของการเกิดความเสี่ยงไม่มีการ Update ข้อมูล

| **ความเสี่ยง** | **ไม่มีการ Update ข้อมูล** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ ขาดการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง<br>■ บุคลากรทำงานล่าช้า | |

ตารางที่ 6.20 สาเหตุพื้นฐานของการเกิดความเสี่ยงค้นหา (Search) ข้อมูลที่ต้องการใช้ในระบบไม่พบ

| **ความเสี่ยง** | **ค้นหา (Search) ข้อมูลที่ต้องการใช้ในระบบไม่พบ** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ บุคลากรขาดทักษะการใช้งาน<br>■ ช่องทางการค้นหาซับซ้อนเกินไป<br>■ ไม่ได้บันทึกข้อมูลไว้<br>■ ข้อมูลสูญหาย | |

ตารางที่ 6.21 สาเหตุพื้นฐานของการเกิดความเสี่ยงบุคลากรใช้งานโปรแกรมไม่เป็น

| **ความเสี่ยง** | **บุคลากรใช้งานโปรแกรมไม่เป็น** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ บุคลากรขาดทักษะการใช้งาน<br>■ เป็นโปรแกรมเฉพาะทาง<br>■ เปลี่ยนโปรแกรมหรือเวอร์ชัน | |

ตารางที่ 6.22 สาเหตุพื้นฐานของการเกิดความเสี่ยงจำนวน Computer ไม่เพียงพอต่อการใช้งาน

| **ความเสี่ยง** | **จำนวน Computer ไม่เพียงพอต่อการใช้งาน** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ ไม่มีการสอบถามความต้องการ<br>■ อยู่ระหว่างการส่งซ่อม | |

ตารางที่ 6.23 สาเหตุพื้นฐานของการเกิดความเสี่ยง Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน

| **ความเสี่ยง** | **Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ สำรวจข้อมูลไม่ละเอียดก่อนเขียนโปรแกรม<br>■ ไม่มีการทดสอบใช้งานก่อนใช้จริง | |

ตารางที่ 6.24 สาเหตุพื้นฐานของการเกิดความเสี่ยง CD-ROM ใช้งานไม่ได้

| **ความเสี่ยง** | **CD-ROM ใช้งานไม่ได้** |
|---|---|
| **สาเหตุพื้นฐาน** | |
| ปัจจัยภายใน<br>■ Power Supply ขัดข้อง<br>■ ตัว CD-ROM เสีย<br>■ สายเคเบิล(IDE Cable) หลุด<br>■ สายไฟ(Power Cable) หลุด | |

## 6.3 การสร้างแผนจัดการความเสี่ยง

หลังจากทำการสรุปสาเหตุพื้นฐานของการเกิดความเสี่ยงทั้งหมดแล้ว ขั้นตอนถัดมา คือ การสร้างแผนจัดการความเสี่ยง

### 6.3.1 แนวทางในการสร้างแผนจัดการความเสี่ยง

การสร้างแผนจัดการความเสี่ยงนั้นจะพิจารณาสร้างจากสาเหตุพื้นฐานของการเกิดความเสี่ยง ซึ่งจะทำให้แผนจัดการความเสี่ยงนั้นมีประสิทธิภาพมาก สำหรับแนวทางในการสร้างแผนจัดการความเสี่ยงนั้นมีแนวทางในการสร้างแผนจัดการความเสี่ยง 4 แนวทางด้วยกัน ซึ่งแนวทางทั้ง 4 แนวทางมีรายละเอียดดังต่อไปนี้

1. Take-การยอมรับความเสี่ยง (Risk Acceptance) คือ การยอมรับให้มีความเสี่ยงนั้นๆ ปรากฏอยู่ เนื่องจากว่าในบางกรณีความเสี่ยงนั้นๆไม่สามารถที่จะสร้างแผนจัดการความเสี่ยงได้ หรืออาจจะ

สามารถสร้างแผนจัดการความเสี่ยงได้ แต่เมื่อทำการสร้างแผนจัดการความเสี่ยงนั้นๆแล้วจะนำมาซึ่งการสูญเสียในด้านต่างๆมากกว่าที่จะปล่อยให้ความเสี่ยงนั้นๆคงอยู่หรือเกิดขึ้น จึงต้องยอมรับความเสี่ยงนั้นๆให้คงอยู่ แต่อย่างไรก็ตามก็ต้องมีมาตรการในการจัดการเพื่อให้สามารถจัดการ ติดตามและดูแลความเสี่ยงนั้นๆหากความเสี่ยงนั้นเกิดขึ้น

2. Treat-การลด/ควบคุมความเสี่ยง (Risk Reduction/Control) คือ การออกแบบระบบการควบคุมภายใน เพื่อควบคุม ป้องกัน หรือลดโอกาสในการเกิดความเสี่ยงนั้นๆ ซึ่งการออกแบบระบบการควบคุมภายในอาจทำได้โดยการ สร้างระบบการทำงาน การติดตามตรวจสอบ ออกมาตรการ ออกฎกำหนดวิธีการต่างๆในการปฏิบัติงาน เป็นต้น

3. Terminate-การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การหลีกเลี่ยง, การหยุด หรือการเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง เช่น การหลีกเลี่ยงการทำกิจกรรมนั้นๆ การปรับเปลี่ยนรูปแบบการดำเนินการหรือระบบต่างๆ เป็นต้น

4. Transfer-การกระจาย/โอนความเสี่ยง (Risk Sharing/Spreading) คือ การกระจายความเสี่ยงของกระบวนการต่างๆเพื่อลดความสูญเสีย เช่น การทำประกันความเสียหายที่อาจจะเกิดขึ้น ได้แก่ การประกันภัย, การจ้างบุคคลภายนอก (Outsource) ซึ่งเป็นการถ่ายโอนความเสี่ยงไปยังบริษัทประกันและบริษัทภายนอก, การเก็บข้อมูลในหลายๆรูปแบบ หรือการกระจายที่เก็บข้อมูลที่สำคัญ เป็นต้น

ส่วนการจะเลือกใช้แนวทางใดใน 4 แนวทางนี้ในการสร้างแผนจัดการความเสี่ยงนั้น จะต้องพิจารณาตามความเหมาะสมเนื่องจากว่าความเสี่ยงบางความเสี่ยงสามารถสร้างแผนจัดการความเสี่ยงได้มากว่า 1 แนวทาง หรือบางความเสี่ยงอาจเลือกได้เพียงแนวทางเดียว

โดยการสร้างแผนจัดการความเสี่ยงของ 23 ประเด็นความเสี่ยงโดยใช้แนวทางทั้ง 4 แนวทางแสดงไว้ในภาคผนวก ค

### 6.3.2 การประเมินความเหมาะสมของแผนจัดการความเสี่ยง

ขั้นตอนสำคัญอีกขั้นตอนหนึ่งในการสร้างแผนจัดการความเสี่ยง คือ การประเมินความเหมาะสมของแผนจัดการความเสี่ยง ซึ่งการประเมินความเหมาะสมของแผนจัดการความเสี่ยงนั้นแต่ละสถานประกอบการอาจจะมีหลักเกณฑ์ในการประเมินความเหมาะสมของแผนจัดการความเสี่ยงต่างกันออกไป ตามลักษณะและวัตถุประสงค์ของการดำเนินงานของสถานประกอบการนั้นๆ หรือแม้ข้อจำกัดต่างๆของสถานประกอบการนั้นๆ ซึ่งในการทำวิจัยครั้งนี้ ผู้วิจัยได้มีการกำหนดหลักเกณฑ์ในการประเมินความเหมาะสมของแผนจัดการความเสี่ยงไว้สองด้าน คือ ด้านความมีประสิทธิภาพของแผนจัดการความเสี่ยงและด้านความเป็นไปได้ในการปฏิบัติตามแผนจัดการความเสี่ยง ซึ่งมีรายละเอียดดังต่อไปนี้

ด้านความมีประสิทธิภาพของแผนจัดการความเสี่ยง สามารถพิจารณาได้จาก การคาดการณ์ว่า แผนจัดการความเสี่ยงนั้นเมื่อนำมาใช้แล้วจะสามารถป้องกันไม่ให้ความเสี่ยงนั้นๆเกิดขึ้นได้ หรือทำให้โอกาสในการเกิดความเสี่ยงนั้นๆลดลง

ด้านความเป็นไปได้ในการปฏิบัติตามแผนจัดการความเสี่ยง สามารถพิจารณาได้จาก แผนจัดการความเสี่ยงที่สร้างขึ้นมานั้นเมื่อนำไปปฏิบัติแล้วต้องไม่ขัดกับนโยบายขององค์กรหรือสถานประกอบการ และต้องไม่เป็นอุปสรรคต่อการปฏิบัติงานของบุคลากร

วิธีการประเมินว่าแผนจัดการความเสี่ยงใดเหมาะสมหรือไม่เหมาะสม คือ

- ด้านความมีประสิทธิภาพของแผนจัดการความเสี่ยง
  - หากแผนจัดการความเสี่ยงใดที่คาดการณ์ว่าจะทำให้ความเสี่ยงนั้นมีโอกาสเกิดลดลง จะถือว่าแผนจัดการความเสี่ยงนั้นมีประสิทธิภาพ
- ด้านความเป็นไปได้ในการปฏิบัติตามแผนจัดการความเสี่ยง
  - หากแผนจัดการความเสี่ยงใดไม่ขัดกับนโยบายขององค์กร จะถือว่าแผนจัดการความเสี่ยงนั้นมีความเป็นไปได้ในการปฏิบัติ
  - หากแผนจัดการความเสี่ยงใดเมื่อนำไปปฏิบัติแล้วไม่เป็นอุปสรรคต่อการปฏิบัติงานของบุคลากร จะถือว่าแผนจัดการความเสี่ยงนั้นมีความเป็นไปได้ในการปฏิบัติ

กล่าวโดยสรุป คือ หากแผนจัดการความเสี่ยงใดขัดกับข้อใดข้อหนึ่ง จะถือว่าแผนจัดการความเสี่ยงนั้นไม่มีความเหมาะสมและจะไม่นำไปปฏิบัติ

การประเมินความเหมาะสมของแผนจัดการความเสี่ยงใช้แบบสอบถามที่ใช้ในการประเมินความเหมาะสมของแผนจัดการความเสี่ยงดังที่ได้แสดงไว้ในภาคผนวก ก-3 โดยผู้ที่ทำการประเมินความเหมาะสมของแผนจัดการความเสี่ยง คือ บุคลากรของโรงพยาบาลที่ทำการวิจัย ประกอบด้วย

| | | |
|---|---|---|
| • หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ | 1 | คน |
| • ตัวแทนหัวหน้าสำนักงานพัฒนาคุณภาพ | 1 | คน |
| • ตัวแทนระบบงานบริการผู้ป่วย | 1 | คน |
| • ตัวแทนระบบงาน Back Office | 1 | คน |
| รวม | 4 | คน |
| อายุงานเฉลี่ย | 12 | ปี |

นอกจากบุคลากรภายในผู้เกี่ยวข้องในการประเมินความเหมาะสมของแผนจัดการความเสี่ยงที่ได้กล่าวไปแล้วในข้างต้น การประเมินความเหมาะสมของแผนจัดการความเสี่ยงวิจัยชิ้นนี้ยังมีผู้เกี่ยวข้องอีก 1 คน คือ ผู้ชำนาญงานด้านคอมพิวเตอร์และอินเตอร์เน็ตจากภายนอกองค์กร ซึ่งจะเป็นผู้ให้คำปรึกษาทางด้านประสิทธิภาพของแผนจัดการความเสี่ยง

**6.3.3 แผนจัดการความเสี่ยง**

สำหรับแผนจัดการความเสี่ยงทั้งหมดซึ่งได้ผ่านการประเมินความเหมาะสมของแผนจัดการความเสี่ยงแล้วได้แสดงไว้ในตารางที่ 6.25-6.47

ตารางที่ 6.25 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส

| **ความเสี่ยง** | **เครื่องคอมพิวเตอร์ติดไวรัส** | | |
|---|---|---|---|
| **ค่า RPN** | **100** | **ลำดับความสำคัญ** | **1** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ ไวรัสจากไฟล์ข้อมูลทั่วๆไป<br>■ ไวรัสจากฟรีแวร์/แชร์แวร์<br>■ แผ่นดิสก์,CD, Flash drive มีไวรัส | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ Scan ทุกไฟล์ที่ Download มาจากอินเตอร์เน็ต<br>■ ห้ามใช้โปรแกรมประเภทฟรีแวร์/แชร์แวร์<br>■ Scan แผ่นดิสก์,CDและ Flash drive ก่อนการใช้งาน | ■ ใช้โปรแกรมตรวจจับและกำจัดไวรัส (Anti-virus)<br>■ Update โปรแกรมประเภท Anti-virus อย่างสม่ำเสมอ |
| ■ มีช่องโหว่ในระบบเครือข่าย | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ Update Firewall ให้เป็นปัจจุบันอยู่เสมอ | |
| ■ Operating System บกพร่อง | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ ทำการตรวจสอบชุดปรับปรุง (Patch หรือ Service Pack) ให้เป็นปัจจุบันอยู่เสมอ | |
| ■ การโจมตีจาก Hacker | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ หลีกเลี่ยงการดาวน์โหลดข้อมูลและโปรแกรมต่างๆที่ไม่เกี่ยวข้องกับการทำงานจากเว็บไซท์<br>■ หลีกเลี่ยงการเปิดอีเมล์ที่ไม่ทราบที่มาที่แน่นอน<br>■ หลีกเลี่ยงการเปิดไฟล์แนบโดยอัตโนมัติหรือการตั้งค่าในโปรแกรมอีเมล์ให้ดาวน์โหลดไฟล์โดยอัตโนมัติ<br>■ Scan ไฟล์หรือโปรแกรมที่ติดมากับ E-mail ก่อนที่จะเปิดอ่านหรือเก็บลงบนฮาร์ดดิสก์<br>■ Block เว็บไซท์ที่ไม่เกี่ยวข้องกับการทำงาน | |

ตารางที่ 6.26 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงคอมพิวเตอร์ Restart เอง

| **ความเสี่ยง** | **คอมพิวเตอร์ Restart เอง** | | |
|---|---|---|---|
| **ค่า RPN** | **80** | **ลำดับความสำคัญ** | **2** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | | <u>กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน</u><br>■ เลือกการ์ดจอและแรมให้เหมาะสมกับการใช้งาน | |
| ■ อุปกรณ์ระบายความร้อนไม่ทำงาน | | <u>วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง</u><br>■ กำหนดระยะเวลาในการตรวจสอบสายไฟที่ต่อกับพัดลมระบายความร้อนให้อยู่ในสภาพที่พร้อมใช้งาน<br>■ กำหนดระยะเวลาทำความสะอาดพัดลมระบายความร้อนโดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น<br>■ จัดสายไฟภายในเครื่องให้เรียบร้อยไม่ขวางทางลมของพัดลม | |
| ■ อุปกรณ์ระบายความร้อนไม่เหมาะสม | | <u>กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน</u><br>■ เลือกชนิดของอุปกรณ์ระบายความร้อนให้เหมาะสมกับการใช้งาน<br>■ เลือกขนาดของอุปกรณ์ระบายความร้อนให้เหมาะสมกับการใช้งาน | |
| ■ Power Supply ขัดข้อง | | <u>วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง</u><br>■ กำหนดระยะเวลาในการตรวจสอบ ขั้วต่อภายในระหว่าง Power Supply กับ อุปกรณ์ฮาร์ดแวร์อื่นๆภายในเครื่องให้แน่นอยู่เสมอ<br>■ กำหนดระยะเวลาในการทำความสะอาดพัดลมที่ติดอยู่กับ Power Supply โดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น<br>■ เลือกใช้ขนาดกำลังไฟฟ้า(ค่าวัตต์) ของ Power Supply ให้เหมาะสมกับฮาร์ดแวร์อื่นๆที่ใช้ | |
| ■ Driver มีปัญหา | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ อัพเดท Driverให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ | |
| ■ Hardware มีปัญหา | | <u>วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง</u><br>■ เมื่อ การ์ดจอ,แรม หรือ Power Supply ชำรุดต้องส่งซ่อมหรือเปลี่ยนใหม่ตามความเหมาะสม | |
| ■ คอมพิวเตอร์ติดไวรัส | | ■ ใช้แผนจัดการความเสี่ยงในตารางที่ 6.25 | |

ตารางที่ 6.27 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงระบบคอมพิวเตอร์ล่ม

| **ความเสี่ยง** | **ระบบคอมพิวเตอร์ล่ม** | | |
|---|---|---|---|
| **ค่า RPN** | **60** | **ลำดับความสำคัญ** | **3** |
| **สาเหตุพื้นฐาน** | **แผนจัดการความเสี่ยง** | | |
| ■ สัญญาณรบกวน | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ หลีกเลี่ยงการเดินสาย LAN คู่ไปกับสายสัญญาณอื่นๆ<br>■ ติดตั้งอุปกรณ์ป้องกันสัญญาณรบกวนที่มาจากสายส่งและจากอุปกรณ์ต่าง ๆ | | ■ ทำการ Backup Procedures |
| ■ Under Voltage<br>■ Over Voltage | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ ติดตั้งอุปกรณ์ประเภท UPS ป้องกันไฟขาดหรือเกิน | | |
| ■ Hardware มีปัญหา | <u>กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้</u><br>■ หากมีการเปลี่ยนฮาร์ดแวร์ใหม่ต้องมีการตรวจสอบว่าฮาร์ดแวร์ที่เปลี่ยนใหม่สามารถทำงานร่วมกับฮาร์ดแวร์ที่มีอยู่เดิมได้ | | |
| ■ คอมพิวเตอร์ติดไวรัส | ■ ใช้แผนจัดการความเสี่ยงในตารางที่ 6.25 | | |
| ■ คอมพิวเตอร์บางเครื่องในระบบมีปัญหา | ■ วางระบบเครือข่ายแบบใยแมงมุม | | |
| ■ อุปกรณ์เชื่อมต่อมีปัญหา | <u>วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง</u><br>■ เดินสาย LAN ให้เป็นระเบียบเรียบร้อย<br>■ กำหนดระยะเวลาในการตรวจสอบสาย LAN ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ<br>■ กำหนดระยะเวลาในการตรวจสอบPort เชื่อมต่อให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ | | |
| ■ ภัยธรรมชาติ | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ ห้องที่เก็บเครื่องแม่ข่าย(Server) ต้องมั่นคงแข็งแรง | | |

ตารางที่ 6.28 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงเข้าใช้งานโปรแกรมไม่ได้

| **ความเสี่ยง** | **เข้าใช้งานโปรแกรมไม่ได้** | | |
|---|---|---|---|
| **ค่า RPN** | **60** | **ลำดับความสำคัญ** | **3** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ บุคลากรขาดทักษะการใช้งาน | | <u>จัดอมรมบุคลากร</u><br>■ มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | |
| ■ โปรแกรมไม่สมบูรณ์ | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ กำหนดให้ผู้มีความชำนาญงานเป็นผู้ติดตั้งโปรแกรม<br>■ กรณีที่เป็นโปรแกรมสำเร็จรูปต้องใช้โปรแกรมที่ถูกลิขสิทธิ์<br>■ กรณีที่เป็นโปรแกรมที่ทางโรงพยาบาลเขียนเองต้องมีการทดสอบการใช้งานก่อนการนำมาใช้งานจริง | |
| ■ ขาดโปรแกรมพื้นฐานที่จำเป็น | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ ติดตั้งโปรแกรมพื้นฐานที่โปรแกรมนั้นๆต้องการให้ครบ | |
| ■ คอมพิวเตอร์ติดไวรัส | | ■ ใช้แผนจัดการความเสี่ยงในตารางที่ 6.25 | |

ตารางที่ 6.29 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงบุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต

| **ความเสี่ยง** | **บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต** | | |
|---|---|---|---|
| **ค่า RPN** | **60** | **ลำดับความสำคัญ** | **4** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ บุคลากรขาดความรับผิดชอบ | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | |
| ■ ขาดการควบคุมการใช้งาน | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ ห้ามติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการทำงาน<br>■ Block เว็บไซท์ที่ไม่เกี่ยวข้องกับการทำงาน | |

ตารางที่ 6.30 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงย้ายหรือถ่ายโอนข้อมูลไม่ได้

| **ความเสี่ยง** | **ย้ายหรือถ่ายโอนข้อมูลไม่ได้** | | |
|---|---|---|---|
| **ค่า RPN** | **60** | **ลำดับความสำคัญ** | **4** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ บุคลากรขาดทักษะการใช้งาน | | <u>จัดอมรมบุคลากร</u><br>■ มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | |
| ■ การ์ด Lan เสีย | | <u>วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง</u><br>■ กำหนดระยะเวลาในการตรวจสอบการ์ด Lanให้อยู่ในสภาพพร้อมใช้งานเสมอ<br>■ เมื่อการ์ด Lan เสียต้องมีการซ่อมหรือเปลี่ยนใหม่ตามความเหมาะสม | |

ตารางที่ 6.31 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงข้อมูลสูญหาย

| **ความเสี่ยง** | **ข้อมูลสูญหาย** | | |
|---|---|---|---|
| **ค่า RPN** | **50** | **ลำดับความสำคัญ** | **5** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ บุคลากรทำงานผิดพลาด | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | |
| ■ ไม่มีการสำรองข้อมูล | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ ทำการสำรองข้อมูล(Backup) อย่างสม่ำเสมอ | |
| ■ ระบบคอมพิวเตอร์ล่ม | | ■ ใช้แผนจัดการความเสี่ยงในตารางที่ 6.27 | |
| ■ คอมพิวเตอร์ติดไวรัส | | ■ ใช้แผนจัดการความเสี่ยงในตารางที่ 6.25 | |

ตารางที่ 6.32 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ทำงานช้า

| **ความเสี่ยง** | **เครื่องคอมพิวเตอร์ทำงานช้า** | | |
|---|---|---|---|
| **ค่า RPN** | **48** | **ลำดับความสำคัญ** | **6** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | | <u>กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน</u><br>■ เลือกซีพียูให้เหมาะสมกับการใช้งาน<br>■ เลือกRamให้เหมาะสมกับการใช้งาน<br>■ เลือกขนาดฮาร์ดดิสก์ให้เหมาะสมกับการใช้งาน | |
| ■ มีขยะในฮาร์ดดิสก์มากเกินไป | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ กำหนดระยะเวลาในการทำ Disk Cleanup<br>■ กำหนดระยะเวลาในการทำ Disk Defragmenter<br>■ ลบ Temporary Files อย่างสม่ำเสมอ | |
| ■ คอมพิวเตอร์ติดไวรัส | | ■ ใช้แผนจัดการความเสี่ยงในตารางที่ 6.25 | |

ตารางที่ 6.33 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงโปรแกรมทำงานผิดพลาด

| **ความเสี่ยง** | **โปรแกรมทำงานผิดพลาด** | | |
|---|---|---|---|
| **ค่า RPN** | **48** | **ลำดับความสำคัญ** | **6** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ โปรแกรมไม่สมบูรณ์ | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ ต้องให้ผู้มีความชำนาญงานเป็นผู้ติดตั้งโปรแกรม<br>■ กรณีที่เป็นโปรแกรมสำเร็จรูปต้องใช้โปรแกรมที่ถูกลิขสิทธิ์<br>■ กรณีที่เป็นโปรแกรมที่ทางโรงพยาบาลเขียนเองต้องมีการทดสอบการใช้งานก่อนการนำมาใช้งานจริง | |
| ■ คอมพิวเตอร์ติดไวรัส | | ■ ใช้แผนจัดการความเสี่ยงในตารางที่ 6.25 | |
| ■ Hardware มีปัญหา | | <u>วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง</u><br>■ กำหนดระยะเวลาในการตรวจสอบHardware(Input/Output)ให้อยู่ในสภาพที่พร้อมใช้งาน | |

ตารางที่ 6.34 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงบุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น

| **ความเสี่ยง** | **บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น** | | |
|---|---|---|---|
| **ค่า RPN** | **45** | **ลำดับความสำคัญ** | **7** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ บุคลากรขาดทักษะการใช้งาน | | <u>จัดอมรมบุคลากร</u><br>■ มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | |
| ■ โปรแกรม Edit Data ไม่ได้หลังบันทึก | | ■ เขียนโปรแกรมให้สามารถ Edit Data ได้ตามลักษณะการใช้งาน | |

ตารางที่ 6.35 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงหน้าจอค้างสีฟ้า (Blue Screen of Death)

| **ความเสี่ยง** | **หน้าจอค้างสีฟ้า (Blue Screen of Death)** | | |
|---|---|---|---|
| **ค่า RPN** | **40** | **ลำดับความสำคัญ** | **8** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ Hardware มีปัญหา | | <u>วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง</u><br>■ กำหนดระยะเวลาในการตรวจสอบ Hardware ทุกชิ้นส่วนให้อยู่ในสภาพพร้อมใช้งานเสมอ | |
| ■ คอมพิวเตอร์ติดไวรัส | | ■ ใช้แผนจัดการความเสี่ยงในตารางที่ 6.25 | |
| ■ Driver มีปัญหา | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ อัพเดท Driver ให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ | |
| ■ คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | | <u>กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน</u><br>■ กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน | |

ตารางที่ 6.36 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์

| **ความเสี่ยง** | **ใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์** | | |
|---|---|---|---|
| **ค่า RPN** | **40** | **ลำดับความสำคัญ** | **8** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ บุคลากรนำโปรแกรมมาลงเอง<br>■ บุคลากรโหลดโปรแกรมละเมิดลิขสิทธิ์จากอินเตอร์เน็ต | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ ห้ามบุคลากรนำโปรแกรมมาลงเองโดยไม่ได้รับอนุญาต<br>■ ห้ามบุคลากรโหลดโปรแกรมละเมิดลิขสิทธิ์จากอินเตอร์เน็ต | |
| ■ ละเมิด Site/Network Licens | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ ต้องศึกษา Site/Network Licens ของโปรแกรมที่จะนำมาใช้ให้ละเอียดก่อนนำโปรแกรมนั้นๆมาใช้งาน | |

ตารางที่ 6.37 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงบุคคลากรคีย์ข้อมูลผิด

| **ความเสี่ยง** | **บุคคลากรคีย์ข้อมูลผิด** | | |
|---|---|---|---|
| **ค่า RPN** | **9** | **ลำดับความสำคัญ** | **40** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ บุคลากรทำงานผิดพลาด | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | |
| ■ บุคลากรมีปัญหาการได้ยิน<br>■ บุคลากรมีปัญหาด้านสายตา | | ■ มีการตรวจสุขภาพให้กับบุคลากรผู้ใช้งานคอมพิวเตอร์ทุกปี | |
| ■ ลายมืออ่านยาก | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ ออกแบบแบบฟอร์มต่างๆที่ต้องใช้ในโรงพยาบาลให้เป็นแบบฟอร์มที่ต้องใช้ลายมือเขียนน้อยที่สุด | |

ตารางที่ 6.38 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงสั่งพิมพ์ (Print) ข้อมูลไม่ได้

| **ความเสี่ยง** | **สั่งพิมพ์ (Print) ข้อมูลไม่ได้** | | |
|---|---|---|---|
| **ค่า RPN** | **9** | **ลำดับความสำคัญ** | **40** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ บุคลากรขาดทักษะการใช้งาน | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ จัดทำคู่มือการใช้งานเบื้องต้นโดยมีรายละเอียด<br>1. วิธีการสั่งพิมพ์<br>2. วิธีตรวจสอบสถานะของ Printer ว่าพร้อมใช้งานหรือไม่ | |
| ■ PRINTER มีปัญหา | | <u>วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง</u><br>■ ตรวจสอบอุปกรณ์ต่อเชื่อมต่างๆระหว่าง Printer กับคอมพิวเตอร์ให้อยู่ในสภาพพร้อมใช้งาน | |
| ■ โปรแกรมทำงานผิดพลาด | | ■ ใช้แผนจัดการความเสี่ยงในตารางที่ 6.33 | |

ตารางที่ 6.39 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงขาดบุคลากรในบางตำแหน่งที่ควรจะมี

| **ความเสี่ยง** | **ขาดบุคลากรในบางตำแหน่งที่ควรจะมี** | | |
|---|---|---|---|
| **ค่า RPN** | **36** | **ลำดับความสำคัญ** | **10** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ ภาระ/ลักษณะงานเพิ่ม | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ มีการกำหนดระยะเวลาในการประชุมหารือร่วมกันของทุกฝ่ายที่เกี่ยวข้องเพื่อประเมินภาระงานและลักษณะงาน เพื่อสรรหาบุคลากรให้เหมาะสมกับงานและเพียงพอต่อภาระงาน | |
| ■ ไม่มีการประเมินภาระ/ลักษณะงาน | | | |

ตารางที่ 6.40 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงบุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย

| **ความเสี่ยง** | **บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย** | | |
|---|---|---|---|
| **ค่า RPN** | **36** | **ลำดับความสำคัญ** | **11** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ▪ ภาระงานมาก<br>▪ องค์กรไม่ส่งเสริม | | ▪ มีการส่งเสริมและจัดสรรเวลาเพื่อให้บุคลากรผู้เกี่ยวข้องเข้าอบรมหลักสูตรต่างๆด้าน IT ตามความเหมาะสม | |

ตารางที่ 6.41 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงแก้ไขโปรแกรมไม่ทัน

| **ความเสี่ยง** | **แก้ไขโปรแกรมไม่ทัน** | | |
|---|---|---|---|
| **ค่า RPN** | **36** | **ลำดับความสำคัญ** | **11** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ▪ โปรแกรมขาดความยืดหยุ่น | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>▪ มีการออกแบบและเขียนโปรแกรมให้ยืดหยุ่นและปรับเปลี่ยนได้ง่าย | |
| ▪ ขาดการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>▪ มีการติดต่อสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องให้รวดเร็วเพื่อให้ทันต่อการเปลี่ยนแปลง | |
| ▪ จัดทำโปรแกรม Spec ไม่ครบถ้วน | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>▪ มีการสำรวจข้อมูลให้ละเอียดก่อนจัดทำโปรแกรม | |

ตารางที่ 6.42 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงไม่มีการ Update ข้อมูล

| **ความเสี่ยง** | **ไม่มีการ Update ข้อมูล** | | |
|---|---|---|---|
| **ค่า RPN** | **32** | **ลำดับความสำคัญ** | **12** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ▪ ขาดการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>▪ มีการติดต่อสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องให้รวดเร็วเพื่อให้ทันต่อการเปลี่ยนแปลง | |
| ▪ บุคลากรทำงานล่าช้า | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>▪ มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | |

ตารางที่ 6.43 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงค้นหา (Search) ข้อมูลที่ต้องการใช้ในระบบไม่พบ

| **ความเสี่ยง** | **ค้นหา (Search) ข้อมูลที่ต้องการใช้ในระบบไม่พบ** | | |
|---|---|---|---|
| **ค่า RPN** | **32** | **ลำดับความสำคัญ** | **13** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ บุคลากรขาดทักษะการใช้งาน | | <u>จัดอมรมบุคลากร</u><br>■ มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | |
| ■ ช่องทางการค้นหาซับซ้อนเกินไป | | ■ กำหนดช่องทางการเข้าถึงข้อมูลให้ง่ายต่อการเข้าถึงข้อมูล | |
| ■ ไม่ได้บันทึกข้อมูลไว้ | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ กำหนดให้ชัดเจนว่าข้อมูลใดต้องทำการบันทึกไว้ | |
| ■ ข้อมูลสูญหาย | | ■ ใช้แผนจัดการความเสี่ยงในตารางที่ 6.31 | |

ตารางที่ 6.44 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงบุคคลากรใช้งานโปรแกรมไม่เป็น

| **ความเสี่ยง** | **บุคคลากรใช้งานโปรแกรมไม่เป็น** | | |
|---|---|---|---|
| **ค่า RPN** | **24** | **ลำดับความสำคัญ** | **14** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ บุคลากรขาดทักษะการใช้งาน | | <u>จัดอมรมบุคลากร</u><br>■ มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | |
| ■ เป็นโปรแกรมเฉพาะทาง | | | |
| ■ เปลี่ยนโปรแกรมหรือเวอร์ชัน | | | |

ตารางที่ 6.45 แผนจัดการความเสี่ยงของประเด็นความเสี่ยงจำนวน Computer ไม่เพียงพอต่อการใช้งาน

| **ความเสี่ยง** | **จำนวน Computer ไม่เพียงพอต่อการใช้งาน** | | |
|---|---|---|---|
| **ค่า RPN** | **24** | **ลำดับความสำคัญ** | **14** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ ไม่มีการสำรวจความต้องการ | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ มีการสำรวจความต้องการก่อนจัดหาคอมพิวเตอร์ในแต่ละครั้ง | |
| ■ อยู่ระหว่างการส่งซ่อม | | ■ จัดให้มีเครื่องคอมพิวเตอร์สำรองกรณีที่เครื่องหลักถูกส่งซ่อม | |

ตารางที่ 6.46 แผนจัดการความเสี่ยงของประเด็นความเสี่ยง Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน

| **ความเสี่ยง** | **Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน** | | |
|---|---|---|---|
| **ค่า RPN** | **18** | **ลำดับความสำคัญ** | **15** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ สำรวจข้อมูลไม่ละเอียดก่อนเขียนโปรแกรม | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ ก่อนจัดทำโปรแกรมต้องมีการสำรวจข้อมูลการใช้งานให้ละเอียด | |
| ■ ไม่มีการทดสอบใช้งานก่อนใช้จริง | | <u>ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน</u><br>■ เมื่อจัดทำโปรแกรมเสร็จแล้วต้องมีการทดสอบใช้งานก่อนที่จะนำโปรแกรมนั้นไปใช้งานจริง | |

ตารางที่ 6.47 แผนจัดการความเสี่ยงของประเด็นความเสี่ยง CD-ROM ใช้งานไม่ได้

| **ความเสี่ยง** | **CD-ROM ใช้งานไม่ได้** | | |
|---|---|---|---|
| **ค่า RPN** | **18** | **ลำดับความสำคัญ** | **15** |
| **สาเหตุพื้นฐาน** | | **แผนจัดการความเสี่ยง** | |
| ■ Power Supply ขัดข้อง | | <u>วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง</u><br>■ กำหนดระยะเวลาในการตรวจสอบ ขั้วต่อภายในระหว่าง Power Supply กับ CD-ROM ให้อยู่ในสภาพพร้อมใช้งานเสมอ<br>■ กำหนดระยะเวลาในการทำความสะอาดพัดลมที่ติดอยู่กับ Power Supply โดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น | |
| ■ ตัว CD-ROM เสีย | | <u>วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง</u><br>■ เปลี่ยน CD-ROM ใหม่ | |
| ■ สายเคเบิล(IDE Cable) หลุด<br>■ สายไฟ(Power Cable) หลุด | | <u>วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง</u><br>■ กำหนดระยะเวลาในการตรวจสอบ สายเคเบิล(IDE Cable) และสายไฟ(Power Cable) ให้อยู่ในสภาพพร้อมใช้งานเสมอ | |

เมื่อพิจารณาแผนจัดการความเสี่ยงทั้งหมดจากตารางที่ 6.25-6.47 พบว่าแผนจัดการความเสี่ยงของหลายๆประเด็นความเสี่ยงสามารถใช้แผนจัดการความเสี่ยงร่วมกันได้หรือสามารถดำเนินงานในขั้นตอนการปฏิบัติตามแผนจัดการความเสี่ยงพร้อมๆกันได้ ซึ่งสามารถสรุปแผนจัดการความเสี่ยงที่เป็นแผนจัดการความเสี่ยงหลักๆได้ดังต่อไปนี้

1. ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน
2. กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน
3. วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง
4. จัดอมรมบุคลากร

ซึ่งได้สรุปรายละเอียดของแผนจัดการความเสี่ยงหลัก 4 แผนหลักไว้ในภาคผนวก ง

## 6.4 การประยุกต์ใช้แผนจัดการความเสี่ยง

หลังจากขั้นตอนการสร้างแผนจัดการความเสี่ยงเสร็จสิ้นแล้ว ขั้นตอนต่อมาคือการประยุกต์ใช้แผนจัดการความเสี่ยง ซึ่งขั้นตอนการประยุกต์ใช้แผนจัดการความเสี่ยงนั้นไม่ได้จัดอยู่ในทฤษฎีขั้นตอนการบริหารความเสี่ยง แต่ในความเป็นจริงแล้วการที่จะนำแผนจัดการความเสี่ยงไปปฏิบัติตามแผนที่ได้สร้างไว้จะต้องมีการประยุกต์หรือปรับใช้เพื่อให้การปฏิบัติตามแผนจัดการความเสี่ยงที่สร้างขึ้นจะได้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

### 6.4.1 การนำแผนจัดการความเสี่ยงไปใช้ในการดำเนินงาน

โดยปกติการนำแผนจัดการความเสี่ยงไปใช้ในการดำเนินงานจะให้ความสำคัญกับแผนจัดการความเสี่ยงของประเด็นความเสี่ยงที่มีความสำคัญมากกว่าก่อน กล่าวคือ แผนจัดการความเสี่ยงของประเด็นความเสี่ยงที่มีค่า RPN สูงกว่าจะต้องถูกนำมาใช้ในการดำเนินงานก่อนเพื่อที่จะจัดการกับความเสี่ยงนั้นๆ แต่จากการพิจารณาจากแผนจัดการความเสี่ยงที่ได้สร้างขึ้นพบว่าแผนจัดการความเสี่ยงของประเด็นความเสี่ยงทั้ง 23 ประเด็น สามารถดำเนินงานไปพร้อมกันได้แต่จะแตกต่างกันในรายละเอียดของแผน กล่าวคือ แผนจัดการความเสี่ยงของประเด็นความเสี่ยงทั้งหมดจะดำเนินงานไปพร้อมกันโดยแบ่งเป็นแผนจัดการความเสี่ยงหลักๆ 4 แผน คือ ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน, กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน, วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง และ จัดอบรมบุคลากร ส่วนระยะเวลาในการเริ่มดำเนินงานมีดังต่อไปนี้

1. ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน สามารถเริ่มแผนได้เมื่อผู้บริหารระดับสูงอนุมัติ

2. กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน สามารถเริ่มแผนได้เมื่อมีการสั่งซื้อคอมพิวเตอร์ชุดใหม่

3.วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง สามารถเริ่มแผนได้ทันที

4.จัดอมรมบุคลากร สามารถเริ่มแผนได้เมื่อผู้บริหารระดับสูงอนุมัติ

นอกจากนี้ยังมีแผนจัดการความเสี่ยงบางส่วนที่ไม่ได้จัดอยู่ในแผนหลักที่ต้องดำเนินงานด้วย คือ บางส่วนของแผนจัดการความเสี่ยงของประเด็นความเสี่ยง ดังต่อไปนี้ ประเด็นความเสี่ยงระบบคอมพิวเตอร์ล่ม, ประเด็นความเสี่ยงบุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น, ประเด็นความเสี่ยงบุคลากรคีย์ข้อมูลผิด, ประเด็นความเสี่ยงบุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย, ประเด็นความเสี่ยงค้นหา (Search) ข้อมูลที่ต้องการใช้ในระบบไม่พบ และ ประเด็นความเสี่ยงจำนวน Computer ไม่เพียงพอต่อการใช้งาน

**6.4.2 ข้อมูลที่ต้องกำหนดและบันทึก**

เพื่อให้ผู้ที่เกี่ยวข้องในการดำเนินตามแผนจัดการความเสี่ยงมีความเข้าใจตรงกันและสามารถปฏิบัติตามแผนจัดการความเสี่ยงได้อย่างมีประสิทธิภาพในการนำแผนจัดการความเสี่ยงไปใช้จะต้องมีการกำหนดข้อมูลต่างๆที่ผู้เกี่ยวข้องจำเป็นจะต้องทราบด้วยซึ่งข้อมูลต่างๆที่ผู้มีส่วนเกี่ยวข้องจำเป็นจะต้องทราบมีดังต่อไปนี้ คือ แผนจัดการความเสี่ยง, วัตถุประสงค์ในการดำเนินงาน, รายละเอียดของแผนจัดการความเสี่ยง, ผู้รับผิดชอบหลักและหน้าที่ของผู้รับผิดชอบหลัก, ผู้มีส่วนเกี่ยวข้องและหน้าที่ของผู้มีส่วนเกี่ยวข้อง, กำหนดการในการเริ่มดำเนินงาน, กำหนดการที่คาดว่าจะดำเนินงานเสร็จสิ้น, งบประมาณที่คาดว่าจะใช้ และงบประมาณที่ใช้จริง นอกจากข้อมูลต่างๆเหล่านี้จะทำให้ผู้ที่เกี่ยวข้องในการดำเนินตามแผนจัดการความเสี่ยงมีความเข้าใจตรงกันและสามารถปฏิบัติตามแผนจัดการความเสี่ยงได้อย่างมีประสิทธิภาพแล้ว ข้อมูลต่างๆเหล่านี้ยังช่วยให้สามารถติดตามผลของแผนจัดการความเสี่ยงในส่วนของการดำเนินงานได้อีกด้วย

โดยผู้วิจัยได้ทำการสร้างแบบฟอร์มในการบันทึกข้อมูลในการดำเนินตามแผนจัดการความเสี่ยงพร้อมคำอธิบายในการกรอกแบบฟอร์มไว้ในภาคผนวก จ

# บทที่ 7

## การติดตามผลแผนจัดการความเสี่ยง

หลังจากมีการประยุกต์ใช้แผนจัดการความเสี่ยงขั้นตอนต่อมา คือ การติดตามและประเมินผลแผนจัดการความเสี่ยง เพื่อเป็นการทบทวนว่าหลังจากดำเนินงานตามแผนจัดการความเสี่ยงนั้นแล้วสามารถทำให้ระดับความเสี่ยงที่หลงเหลืออยู่นั้นอยู่ในระดับที่ยอมรับได้หรือไม่ หากระดับความเสี่ยงที่หลงเหลืออยู่ในระดับที่ยอมรับได้แสดงว่าแผนจัดการความเสี่ยงนั้นสามารถจัดการกับความเสี่ยงนั้นได้อยู่ในระดับที่น่าพอใจ(ระดับที่องค์กรหรือสถานประกอบการนั้นๆกำหนดว่าอยู่ในระดับที่ยอมรับได้) และหากระดับความเสี่ยงที่หลงเหลืออยู่นั้นอยู่ในระดับที่ยอมรับไม่ได้ แสดงว่าแผนจัดการความเสี่ยงนั้นไม่สามารถจัดการกับความเสี่ยงนั้นได้ จะต้องมีการปรับปรุงหรือเปลี่ยนแปลงแผนจัดการความเสี่ยงนั้นๆ ตามความเหมาะสมเพื่อให้สามารถจัดการกับความเสี่ยงได้ และการติดตามผลแผนจัดการความเสี่ยงนั้นจะต้องทำอย่างสม่ำเสมอเนื่องจากปัจจัยต่างๆที่เกี่ยวข้องกับความเสี่ยงทั้งปัจจัยภายนอกและปัจจัยภายในอาจมีการเปลี่ยนแปลงไปตามกาลเวลา

จากการประยุกต์ใช้แผนจัดการความเสี่ยงพบว่า มีแผนจัดการความเสี่ยงเพียงแผนเดียวจาก 4 แผนหลักที่สามารถดำเนินงานได้ทันที คือ วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง แต่การที่จะติดตามผลแผนจัดการความเสี่ยงและประเมินว่าแผนจัดการความเสี่ยงสามารถจัดการกับความเสี่ยงต่างๆได้หรือไม่จะต้องดำเนินงานให้ครบทั้ง 4 แผนก่อนจึงจะสามารถทำการติดตามและประเมินผลแผนจัดการความเสี่ยงได้ ดังนั้นงานวิจัยชิ้นนี้จะทำการติดตามผลแผนจัดการความเสี่ยงโดยใช้วิธีการประเมินความเสี่ยงแบบคาดหมาย (Expected) เพื่อเปรียบเทียบค่า RPN ของความเสี่ยงก่อนและหลังจากมีแผนจัดการความเสี่ยง และนำค่า RPN ที่ได้ไปเปรียบเทียบกับเกณฑ์การยอมรับได้ของความเสี่ยง เพื่อประเมินว่าแผนจัดการความเสี่ยงนั้นสามารถจัดการกับความเสี่ยงนั้นๆให้อยู่ในระดับที่ยอมรับได้ได้หรือไม่ และเมื่อมีการนำแผนจัดการความเสี่ยงมาใช้ในการดำเนินงานครบทั้ง 4 แผนหลักแล้ว จะต้องมีการติดตามอย่างเป็นรูปธรรมว่าแผนจัดการความเสี่ยงที่นำมาใช้ในการดำเนินงานนั้นสามารถที่จะบริหารจัดการกับประเด็นความเสี่ยงนั้นๆได้ตามที่ได้คาดหมายเอาไว้ในการประเมินความเสี่ยงแบบคาดหมายหลังจากมีแผนจัดการความเสี่ยงหรือไม่

## 7.1 การประเมินความเสี่ยงแบบคาดหมายหลังจากมีแผนจัดการความเสี่ยง

การประเมินความเสี่ยงแบบคาดหมายหลังจากมีแผนจัดการความเสี่ยงนั้นจะใช้วิธีการและเกณฑ์การประเมินความเสี่ยงเหมือนกับวิธีการและหลักเกณฑ์การประเมินความเสี่ยงดังที่ได้กล่าวไปแล้วใน บทที่ 5 แต่จะมีความแตกต่างกันเล็กน้อย คือ ระดับความรุนแรงของความเสี่ยง (Severity; S) จะไม่มีการประเมินใหม่แต่จะใช้ค่าเดิมจากการที่ได้ประเมินไว้แล้วในบทที่ 5 จะมีการประเมินเฉพาะสองปัจจัยที่เหลือ คือ โอกาสในการเกิดความเสี่ยง (Occurrence; O) และ ความสามารถในการตรวจพบความเสี่ยง (Detection; D) เนื่องจากการที่มีแผนจัดการความเสี่ยงนั้นจะไม่ช่วยให้ระดับความรุนแรงของความเสี่ยงลดลงหากความเสี่ยงนั้นเกิดขึ้น แต่จะทำให้ระดับโอกาสในการเกิดความเสี่ยงลดลง และทำให้ความสามารถในการตรวจพบความเสี่ยงหรือระดับการควบคุมความเสี่ยงมีประสิทธิภาพมากขึ้นเท่านั้น สำหรับแบบสอบถามที่ใช้ในการประเมินความเสี่ยงหลังจากมีแผนจัดการความเสี่ยงได้แสดงไว้ในภาคผนวก ก-4 และหลังจากประเมินระดับโอกาสในการเกิดความเสี่ยงและความสามารถในการตรวจพบความเสี่ยงหรือระดับการควบคุมความเสี่ยงเสร็จสิ้นแล้ว ขั้นตอนต่อไปนำค่าที่ได้ทั้งสองค่าไปคำนวณร่วมกับระดับความรุนแรงของความเสี่ยงเดิม เพื่อคิดเป็นค่า RPN ของความเสี่ยงหลังจากมีแผนจัดการความเสี่ยงซึ่งจะทำให้ทราบระดับความเสี่ยงที่หลงเหลืออยู่ โดยผลการประเมินระดับโอกาสในการเกิดความเสี่ยง (Occurrence; O) และ ความสามารถในการตรวจพบความเสี่ยง (Detection; D) ได้แสดงไว้ในตารางที่ 7.1 ส่วนผลการคำนวณค่า RPN หลังจากมีแผนจัดการความเสี่ยงหรือระดับความเสี่ยงที่หลงเหลืออยู่ได้แสดงไว้ในตารางที่ 7.2 โดยลำดับของความเสี่ยงในตารางที่ 7.1 และ 7.2 จะเรียงลำดับตามค่า RPN เดิมจากมากไปหาน้อย (ตามลำดับความสำคัญ)

ตารางที่ 7.1 ผลการประเมินระดับโอกาสในการเกิดความเสี่ยง (Occurrence; O) และความสามารถในการตรวจพบความเสี่ยง (Detection; D) หลังจากมีแผนจัดการความเสี่ยง

| ข้อ | ประเด็นความเสี่ยง | ระดับคะแนน | |
|---|---|---|---|
| | | O | D |
| 1 | เครื่องคอมพิวเตอร์ติดไวรัส | 2 | 1 |
| 2 | คอมพิวเตอร์ Restart เอง | 2 | 1 |
| 3 | ระบบคอมพิวเตอร์ล่ม | 1 | 1 |
| | เข้าใช้งานโปรแกรมไม่ได้ | 2 | 1 |
| 4 | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | 3 | 1 |
| | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | 2 | 1 |
| 5 | ข้อมูลสูญหาย | 1 | 1 |
| 6 | เครื่องคอมพิวเตอร์ทำงานช้า | 2 | 1 |
| | โปรแกรมทำงานผิดพลาด | 2 | 1 |
| 7 | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | 2 | 1 |
| 8 | หน้าจอค้างสีฟ้า (Blue Screen of Death) | 1 | 1 |
| | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | 1 | 1 |
| 9 | บุคลากรคีย์ข้อมูลผิด | 3 | 1 |
| | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | 3 | 1 |
| 10 | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | 1 | 1 |
| 11 | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | 2 | 1 |
| | แก้ไขโปรแกรมไม่ทัน | 2 | 1 |
| 12 | ไม่มีการUpdateข้อมูล | 2 | 1 |
| 13 | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | 2 | 1 |
| 14 | บุคลากรใช้งานโปรแกรมไม่เป็น | 1 | 1 |
| | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | 1 | 1 |
| 15 | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | 1 | 1 |
| | CD-ROM ใช้งานไม่ได้ | 1 | 1 |

ตารางที่ 7.2 ค่า RPN หลังจากมีแผนจัดการความเสี่ยง

| ข้อ | ประเด็นความเสี่ยง | ระดับคะแนน | | | |
|---|---|---|---|---|---|
| | | S | O | D | RPN |
| 1 | เครื่องคอมพิวเตอร์ติดไวรัส | 5 | 2 | 1 | **10** |
| 2 | คอมพิวเตอร์ Restart เอง | 5 | 2 | 1 | **10** |
| 3 | ระบบคอมพิวเตอร์ล่ม | 5 | 1 | 1 | **5** |
| | เข้าใช้งานโปรแกรมไม่ได้ | 5 | 2 | 1 | **10** |
| 4 | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | 4 | 3 | 1 | **12** |
| | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | 4 | 2 | 1 | **8** |
| 5 | ข้อมูลสูญหาย | 5 | 1 | 1 | **5** |
| 6 | เครื่องคอมพิวเตอร์ทำงานช้า | 4 | 2 | 1 | **8** |
| | โปรแกรมทำงานผิดพลาด | 4 | 2 | 1 | **8** |
| 7 | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | 3 | 2 | 1 | **6** |
| 8 | หน้าจอค้างสีฟ้า (Blue Screen of Death) | 5 | 1 | 1 | **5** |
| | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | 5 | 1 | 1 | **5** |
| 9 | บุคลากรคีย์ข้อมูลผิด | 4 | 3 | 1 | **12** |
| | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | 4 | 3 | 1 | **12** |
| 10 | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | 4 | 1 | 1 | **4** |
| 11 | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | 3 | 2 | 1 | **6** |
| | แก้ไขโปรแกรมไม่ทัน | 3 | 2 | 1 | **6** |
| 12 | ไม่มีการUpdateข้อมูล | 4 | 2 | 1 | **8** |
| 13 | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | 2 | 2 | 1 | **4** |
| 14 | บุคลากรใช้งานโปรแกรมไม่เป็น | 4 | 1 | 1 | **4** |
| | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | 4 | 1 | 1 | **4** |
| 15 | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | 2 | 1 | 1 | **2** |
| | CD-ROM ใช้งานไม่ได้ | 2 | 1 | 1 | **2** |

**7.2 การประเมินผลแผนจัดการความเสี่ยง**

สำหรับการประเมินผลแผนจัดการความเสี่ยงจะใช้วิธีการเปรียบเทียบค่า RPN ก่อนมีแผนจัดการความเสี่ยง เปรียบเทียบกับ ค่า RPN ที่ได้จากการประเมินความเสี่ยงแบบคาดหมายหลังจากมีแผนจัดการความเสี่ยง กล่าวคือนำค่า RPN ในตารางที่ 5.6 กับค่า RPN ในตารางที่ 7.2 มาเปรียบเทียบกัน โดยการเปรียบเทียบจะพิจารณาว่า ประเด็นความเสี่ยงต่างๆเหล่านั้นมีค่า RPN ลดลงจนอยู่ในระดับที่ยอมรับได้หรือไม่ โดยมีเกณฑ์การยอมรับได้ของประเด็นความเสี่ยงดังต่อไปนี้

ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับมากที่สุด(คะแนน=5) หากมีค่า RPN น้อยกว่าหรือเท่ากับ 20 จะถือว่าประเด็นความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับมาก(คะแนน=4) หากมีค่า RPN น้อยกว่าหรือเท่ากับ 16 จะถือว่าประเด็นความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับปานกลาง(คะแนน=3) หากมีค่า RPN น้อยกว่าหรือเท่ากับ 12 จะถือว่าประเด็นความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับน้อย(คะแนน=2) หากมีค่า RPN น้อยกว่าหรือเท่ากับ 8 จะถือว่าประเด็นความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

ประเด็นความเสี่ยงที่มีความรุนแรงอยู่ในระดับน้อยมาก(คะแนน=1) หากมีค่า RPN น้อยกว่าหรือเท่ากับ 4 จะถือว่าประเด็นความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

ซึ่งหากประเด็นของความเสี่ยงนั้นๆมีค่า RPN อยู่ในระดับที่ยอมรับได้ แสดงว่าแผนจัดการความเสี่ยงนั้นๆมีประสิทธิภาพสามารถจัดการกับประเด็นความเสี่ยงนั้นๆได้ ซึ่งผลการเปรียบเทียบค่า RPN ของประเด็นความเสี่ยงก่อนและหลังมีแผนจัดการความเสี่ยงได้แสดงไว้ในตารางที่ 7.3

ตารางที่ 7.3 ผลการเปรียบเทียบค่า RPN ของประเด็นความเสี่ยงก่อนและหลังมีแผนจัดการความเสี่ยง

| ข้อ | ประเด็นความเสี่ยง | ค่า RPN | |
|---|---|---|---|
| | | ก่อนมีแผน | หลังมีแผน |
| 1 | เครื่องคอมพิวเตอร์ติดไวรัส | **100** | **10** |
| 2 | คอมพิวเตอร์ Restart เอง | **80** | **10** |
| 3 | ระบบคอมพิวเตอร์ล่ม | **60** | **5** |
| | เข้าใช้งานโปรแกรมไม่ได้ | **60** | **10** |
| 4 | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | **60** | **12** |
| | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | **60** | **8** |
| 5 | ข้อมูลสูญหาย | **50** | **5** |
| 6 | เครื่องคอมพิวเตอร์ทำงานช้า | **48** | **8** |
| | โปรแกรมทำงานผิดพลาด | **48** | **8** |
| 7 | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | **45** | **6** |
| 8 | หน้าจอค้างสีฟ้า (Blue Screen of Death) | **40** | **5** |
| | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | **40** | **5** |
| 9 | บุคลากรคีย์ข้อมูลผิด | **40** | **12** |
| | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | **40** | **12** |
| 10 | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | **36** | **4** |
| 11 | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | **36** | **6** |
| | แก้ไขโปรแกรมไม่ทัน | **36** | **6** |
| 12 | ไม่มีการUpdateข้อมูล | **32** | **8** |
| 13 | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | **32** | **4** |
| 14 | บุคลากรใช้งานโปรแกรมไม่เป็น | **24** | **4** |
| | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | **24** | **4** |
| 15 | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | **18** | **2** |
| | CD-ROM ใช้งานไม่ได้ | **18** | **2** |

จากการพิจารณาผลการเปรียบเทียบค่า RPN ของประเด็นความเสี่ยงก่อนและหลังมีแผนจัดการความเสี่ยงในตารางที่ 7.3 พบว่าหลังจากมีแผนจัดการความเสี่ยง ทุกประเด็นความเสี่ยงมีค่า RPN ลดลง และเมื่อพิจารณาค่า RPN ของแต่ละประเด็นความเสี่ยงพบว่าอยู่ในระดับที่ยอมรับได้ ดังนั้นจึงสามารถประเมินผลแผนจัดการความเสี่ยงได้ว่า แผนจัดการความเสี่ยงมีประสิทธิภาพสามารถจัดการกับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

### 7.3 ข้อมูลที่ต้องติดตามหลังการใช้แผนจัดการความเสี่ยง

เมื่อมีการนำแผนจัดการความเสี่ยงมาใช้ในการดำเนินงานครบทั้ง 4 แผนหลักแล้ว จะต้องมีการติดตามอย่างเป็นรูปธรรมว่าแผนจัดการความเสี่ยงที่นำมาใช้ในการดำเนินงานนั้นสามารถที่จะบริหารจัดการกับประเด็นความเสี่ยงนั้นๆได้ตามที่ได้คาดหมายเอาไว้ในการประเมินความเสี่ยงแบบคาดหมายหลังจากมีแผนจัดการความเสี่ยงหรือไม่ โดยมีการกำหนดประเด็นความเสี่ยงที่ต้องติดตาม ข้อมูลที่ต้องติดตาม และความถี่ในการติดตาม หลังจากจากนำแผนจัดการความเสี่ยงมาใช้ในการดำเนินงานครบทั้ง 4 แผนหลัก ดังตารางที่ 7.4

ตารางที่ 7.4 ข้อมูลที่ต้องติดตามหลังจากนำแผนจัดการความเสี่ยงมาใช้ในการดำเนินงานครบทั้ง 4 แผนหลัก

| ลำดับ | ประเด็นความเสี่ยง | ข้อมูลที่ต้องติดตาม | ความถี่ |
|---|---|---|---|
| 1 | ■ เครื่องคอมพิวเตอร์ติดไวรัส | ■ สถิติการติดไวรัสของเครื่องคอมพิวเตอร์<br>หมายเหตุ เนื่องจากในบางครั้งมีไวรัสชนิดใหม่เกิดขึ้นซึ่งอาจทำให้ไม่สามารถ SCAN พบได้แม้ว่าคอมพิวเตอร์จะติดไวรัส ในกรณีนี้สามารถอนุมานได้จากผลกระทบที่เกิดขึ้นจากคอมพิวเตอร์ติดไวรัส (แสดงไว้ในตัวอย่างผลกระทบของประเด็นความเสี่ยง 23 ประเด็นความเสี่ยง) | ทุก 6 เดือน |
| 2 | ■ คอมพิวเตอร์ Restart เอง | ■ สถิติการ Restart เองของคอมพิวเตอร์ | ทุก 6 เดือน |
| 3 | ■ ระบบคอมพิวเตอร์ล่ม | ■ สถิติการล่มของระบบคอมพิวเตอร์ | ทุก 1 ปี |
| 4 | ■ เข้าใช้งานโปรแกรมไม่ได้ | ■ สถิติการเข้าใช้งานโปรแกรมไม่ได้ของบุคลากร โดยต้องแบ่งแยกเป็น 2 ประเด็นคือ<br>1. เข้าใช้งานโปรแกรมสำเร็จรูปไม่ได้<br>2. เข้าใช้งานโปรแกรมที่โรงพยาบาลเขียนขึ้นไม่ได้ | ทุก 6 เดือน |

ตารางที่ 7.4 ข้อมูลที่ต้องติดตามหลังจากนำแผนจัดการความเสี่ยงมาใช้ในการดำเนินงานครบทั้ง 4 แผนหลัก(ต่อ)

| ลำดับ | ประเด็นความเสี่ยง | ข้อมูลที่ต้องติดตาม | ความถี่ |
|---|---|---|---|
| 5 | ■ บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | ■ สุ่มตรวจการเข้าใช้โปรแกรมที่ไม่เกี่ยวข้องกับการทำงานของบุคลากร<br>■ สุ่มตรวจการเข้าเว็บไซท์ที่ไม่เกี่ยวข้องกับการทำงานของบุคลากร | ทุก 1 เดือน |
| 6 | ■ ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | ■ สถิติการย้ายหรือถ่ายโอนข้อมูลไม่ได้ | ทุก 6 เดือน |
| 7 | ■ ข้อมูลสูญหาย | ■ สถิติการสูญหายของข้อมูล | ทุก 1 ปี |
| 8 | ■ เครื่องคอมพิวเตอร์ทำงานช้า | ■ เวลาที่ใช้ในการเข้าหน้าจอการใช้งานหลัก<br>■ เวลาที่ใช้ในการเข้าสู่โปรแกรมการใช้งาน<br>■ เวลาที่ใช้ในการประมวลผลของคอมพิวเตอร์<br>หมายเหตุ ข้อมูลเหล่านี้สอบถามได้จากบุคลากรผู้ใช้งานคอมพิวเตอร์ | ทุก 6 เดือน |
| 9 | ■ โปรแกรมทำงานผิดพลาด | ■ สถิติการทำงานผิดพลาดของโปรแกรม | ทุก 6 เดือน |
| 10 | ■ บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | ■ สถิติการยกเลิกหรือแก้ไขข้อมูลไม่ได้ | ทุก 6 เดือน |
| 11 | ■ หน้าจอค้างสีฟ้า (Blue Screen of Death) | ■ สถิติการเกิดหน้าจอค้างสีฟ้า | ทุก 1 ปี |
| 12 | ■ ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | ■ สุ่มตรวจโปรแกรมที่บุคลากรอาจนำมาติดตั้งเอง<br>■ สุ่มตรวจโปรแกรมที่บุคลากรอาจโหลดมาจากอินเตอร์เน็ต(ส่วนใหญ่ละเมิดลิขสิทธิ์)<br>■ ตรวจสอบโปรแกรมถูกลิขสิทธิ์ว่าลงโปรแกรมถูกต้องตาม Site/Network Licens หรือไม่ | ทุก 1 ปี |
| 13 | ■ บุคลากรคีย์ข้อมูลผิด | ■ สถิติของข้อมูลที่ผิดพลาดจากความเป็นจริง(ในส่วนที่เกิดจากบุคลากร) | ทุก 1 เดือน |
| 14 | ■ สั่งพิมพ์(Print)ข้อมูลไม่ได้ | ■ สถิติการสั่งพิมพ์(Print)ข้อมูลไม่ได้ | ทุก 1 เดือน |
| 15 | ■ ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | ■ สถิติที่บุคลากรต้องไปปฏิบัติงานในภาระงานที่ไม่ใช่หน้าที่หลักของตนเอง | ทุก 1 ปี |
| 16 | ■ บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | ■ ประเมินวิธีการทำงานของบุคลากรโดยพิจารณาเทียบกับสิ่งที่บุคลกรได้รับการอบรม | ทุก 6 เดือน |

ตารางที่ 7.4 ข้อมูลที่ต้องติดตามหลังจากนำแผนจัดการความเสี่ยงมาใช้ในการดำเนินงานครบทั้ง 4 แผนหลัก(ต่อ)

| ลำดับ | ประเด็นความเสี่ยง | ข้อมูลที่ต้องติดตาม | ความถี่ |
|---|---|---|---|
| 17 | ■ แก้ไขโปรแกรมไม่ทัน | ■ ระยะเวลาที่ใช้ในการแก้ไขโปรแกรม<br>■ การแก้ไขโปรแกรมทันต่อความเปลี่ยนแปลง<br>หมายเหตุ ข้อมูลเหล่านี้สอบถามได้จากบุคลากรผู้ใช้งานคอมพิวเตอร์ | ทุก 6 เดือน |
| 18 | ■ ไม่มีการUpdateข้อมูล | ■ ตรวจทานเปรียบเทียบข้อมูลในระบบคอมพิวเตอร์กับข้อมูลจริง ณ ขณะนั้นให้ตรงกัน | ทุก 6 เดือน |
| 19 | ■ ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | ■ ความยากง่ายหรือเวลาที่ใช้ในการเข้าถึงข้อมูลในระบบ<br>■ การพบข้อมูลที่ต้องการใช้<br>หมายเหตุ ข้อมูลเหล่านี้สอบถามได้จากบุคลากรผู้ใช้งานคอมพิวเตอร์ | ทุก 6 เดือน |
| 20 | ■ บุคลากรใช้งานโปรแกรมไม่เป็น | ■ ประเมินระยะเวลาในการทำงานจริงของบุคลากรเทียบกับระยะเวลาที่ควรจะใช้ในการทำงานเกี่ยวกับโปรแกรมต่างๆ | ทุก 1 ปี |
| 21 | ■ จำนวน Computer ไม่เพียงพอต่อการใช้งาน | ■ ประเมินภาระงานที่ต้องใช้คอมพิวเตอร์กับจำนวนคอมพิวเตอร์<br>■ มีคอมพิวเตอร์สำรองใช้ในกรณีที่ส่งซ่อม | ทุก 1 ปี |
| 22 | ■ Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | ■ Option การใช้งานของโปรแกรมเพียงพอต่อความต้องการการใช้งาน<br>หมายเหตุ ข้อมูลนี้สอบถามได้จากบุคลากรผู้ใช้งานคอมพิวเตอร์ | ทุก 1 ปี |
| 23 | ■ CD-ROM ใช้งานไม่ได้ | ■ ปัญหาการใช้งานที่เกี่ยวข้องกับ CD-ROM | ทุก 1 ปี |

# บทที่ 8

# สรุปและข้อเสนอแนะ

ในส่วนสุดท้ายของงานวิจัยคือการสรุปผลการวิจัยและข้อเสนอแนะ โดยส่วนแรกจะเป็นการสรุปผลการวิจัยในทุกๆขั้นตอน ส่วนที่สองจะเป็นข้อเสนอแนะต่างๆ

## 8.1 สรุปผลการวิจัย

ขั้นตอนแรกของงานวิจัยเริ่มต้นจากการศึกษาทฤษฎีและงานวิจัยต่างๆที่เกี่ยวข้องจากนั้นจึงทำการศึกษาข้อมูลการนำคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการ ในปี พ.ศ. 2547 ถึง พ.ศ. 2549 โดยแหล่งข้อมูลหลักที่ทำการศึกษา คือ แหล่งข้อมูลจากการสำรวจข้อมูลเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานสถิติแห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งได้ทำการสำรวจการใช้คอมพิวเตอร์และอินเตอร์เน็ต ของสถานประกอบการต่างๆ 5 ประเภท คือ ธุรกิจและบริการ, การผลิต, การก่อสร้าง, การขนส่งทางบกและตัวแทนธุรกิจการท่องเที่ยว และ โรงพยาบาล และจากผลการศึกษาข้อมูลพบว่า สถานประกอบการต่างๆ มีการนำคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการเพิ่มขึ้นทุกปี นอกจากนี้ยังพบว่าการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในสถานประกอบการต่างๆ เหล่านี้ยังมีปัญหาในการใช้งานคอมพิวเตอร์และอินเตอร์เน็ตอยู่ในหลายๆด้าน ซึ่งผู้วิจัยได้ทำการศึกษาปัญหาต่างๆที่เกิดขึ้นและได้สรุปปัญหาทั้งหมดออกมาเป็นปัญหาหลักๆในด้านต่างๆดังต่อไปนี้

1. ปัญหาด้านบุคลากร
2. ปัญหาด้านเทคโนโลยี
3. ปัญหาด้านข้อมูล
4. ปัญหาด้านฮาร์ดแวร์และซอฟท์แวร์
5. ปัญหาด้านกฎหมาย

ภายหลังจากทำการศึกษาข้อมูลการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการและได้สรุปถึงปัญหาหลักๆที่เกิดขึ้นจากการใช้คอมพิวเตอร์และอินเตอร์เน็ตเสร็จสิ้นแล้ว ขั้นตอนต่อมาคือการเข้าไปศึกษาและทำการวิจัยในสถานประกอบการ เพื่อทำการศึกษาวิจัยในหัวข้อเรื่องการบริหาร

ความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในสถานประกอบการ โดยสถานประกอบการกรณีศึกษาในงานวิจัยชิ้นนี้ คือ โรงพยาบาลแห่งหนึ่ง

สำหรับโรงพยาบาลที่เป็นกรณีศึกษาในการวิจัยครั้งนี้เป็นโรงพยาบาลขนาดใหญ่ ซึ่งโรงพยาบาลแห่งนี้ได้มีการนำเอาคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในการดำเนินงานอย่างเป็นทางการตั้งแต่ ปี พ.ศ. 2532 หรือประมาณ 18 ปีที่แล้ว ซึ่งข้อมูลเบื้องต้นของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในโรงพยาบาลแห่งนี้ มีดังต่อไปนี้ ปัจจุบันทางโรงพยาบาลใช้ระบบหลัก คือ ระบบ HIS (Hospital Information System) โดยมีจำนวนคอมพิวเตอร์ทั้งสิ้น 850 เครื่อง เครื่องพิมพ์ 650 เครื่อง ในส่วนของซอฟท์แวร์ที่ใช้มี 2 ประเภท คือ ซอฟท์แวร์สำเร็จรูปและซอฟท์แวร์ที่ทางโรงพยาบาลเขียนขึ้นใช้งานเองตามลักษณะของงาน และจากการศึกษาระบบงานในโรงพยาบาลพบว่าระบบงานในโรงพยาบาลที่ใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำงาน ประกอบไปด้วยสองส่วนหลักๆ คือ ส่วนที่หนึ่งคือระบบงานบริการผู้ป่วย ซึ่งเป็นระบบงานหลักของโรงพยาบาล และส่วนที่สอง คือ ระบบงานการบริหารจัดการเรื่องทั่วๆไปในโรงพยาบาลที่ไม่เกี่ยวข้องกับผู้ป่วย หรือระบบงานสนับสนุนงานหลักหรือที่เรียกว่าระบบงาน Back Office ส่วนวัตถุประสงค์ในการนำคอมพิวเตอร์และอินเตอร์เน็ตมาใช้ในการดำเนินงานของทางโรงพยาบาล คือ ระบบคอมพิวเตอร์ On-line ของโรงพยาบาลต้องพร้อมใช้งานตลอด 24 ชั่วโมง เพื่อให้บริการผู้ป่วยในด้านต่างๆ รวมไปถึงงานด้านอื่นๆในโรงพยาบาล ด้วยความรวดเร็ว ถูกต้องและปลอดภัย”

เมื่อทำการศึกษาระบบงานที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และอินเตอร์เน็ตของโรงพยาบาลแล้วขั้นตอนต่อมาคือการระบุความเสี่ยง ซึ่งในขั้นตอนการระบุความเสี่ยงนั้นได้มีการกำหนดวัตถุประสงค์ในการบริหารความเสี่ยงไว้ดังต่อไปนี้ จะทำการบริหารความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในโรงพยาบาลในด้านต่างๆตามปัญหาหลักๆทั้ง 5 ด้านคือ

1. ความเสี่ยงด้านบุคลากร
2. ความเสี่ยงด้านเทคโนโลยี
3. ความเสี่ยงด้านข้อมูล
4. ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์
5. ความเสี่ยงด้านกฎหมาย

ส่วนขอบเขตในการระบุความเสี่ยง คือ การจะพิจารณาว่าเหตุการณ์หรือสถานการณ์ใดบ้างที่จัดว่าเป็นความเสี่ยงในการดำเนินงานนั้นสามารถพิจารณาได้โดย หากเหตุการณ์หรือสถานการณ์นั้นเกิดขึ้นจะทำให้เกิดอุปสรรคในการดำเนินงานหรือทำให้ไม่สามารถบรรลุวัตถุประสงค์ของการดำเนินงาน โดยจะทำการระบุความเสี่ยงในด้านต่างๆตามวัตถุประสงค์ของการบริหารความเสี่ยง ได้แก่ ความเสี่ยงด้านบุคลากร ความเสี่ยงด้านเทคโนโลยี ความเสี่ยงด้านข้อมูล ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ และความเสี่ยงด้านกฎหมาย โดยผลการระบุความเสี่ยงมีดังต่อไปนี้ เป็นความเสี่ยงด้านบุคลากร 14 ความเสี่ยง ความเสี่ยงด้านเทคโนโลยี 6 ความเสี่ยง ความเสี่ยงด้านข้อมูล 11 ความเสี่ยง ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ 21 ความเสี่ยง และความเสี่ยงด้านกฎหมาย 2 ความเสี่ยง รวมทั้งสิ้น 54 ความเสี่ยง หลังจากนั้นได้ทำการวิเคราะห์ความเสี่ยงทั้งหมดพบว่ามีอยู่หลายๆความเสี่ยงที่จัดได้ว่าเป็นประเด็นความเสี่ยงเดียวกัน จึงได้ทำการรวมความเสี่ยงนั้นๆเข้าเป็นประเด็นเดียวกันจาก 54 ความเสี่ยง สรุปออกมาเป็น 23 ประเด็นความเสี่ยง ดังต่อไปนี้

- ขาดบุคลากรในบางตำแหน่งที่ควรจะมี
- บุคลากรใช้งานโปรแกรมไม่เป็น
- บุคลากรคีย์ข้อมูลผิด
- บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น
- บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต
- บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย
- เครื่องคอมพิวเตอร์ติดไวรัส
- ไม่มีการ Update ข้อมูล
- ข้อมูลสูญหาย
- ย้ายหรือถ่ายโอนข้อมูลไม่ได้
- ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ
- แก้ไขโปรแกรมไม่ทัน
- ระบบคอมพิวเตอร์ล่ม
- เครื่องคอมพิวเตอร์ทำงานช้า
- โปรแกรมทำงานผิดพลาด
- สั่งพิมพ์(Print)ข้อมูลไม่ได้
- Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน

- เข้าใช้งานโปรแกรมไม่ได้
- คอมพิวเตอร์ Restart เอง
- CD-ROM ใช้งานไม่ได้
- หน้าจอค้างสีฟ้า (Blue Screen of Death)
- จำนวน Computer ไม่เพียงพอต่อการใช้งาน
- ใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์

จากนั้นนำประเด็นความเสี่ยงทั้งหมดไปประเมินความเสี่ยง โดยทำการประเมินความเสี่ยง 3 ด้าน คือ ความรุนแรงของความเสี่ยง (Severity; S) โอกาสในการเกิดความเสี่ยง (Occurrence; O) และความสามารถในการตรวจพบความเสี่ยง (Detection; D) จากนั้นนำค่าที่ได้จากการประเมินนำไปคิดเป็นค่า RPN (Risk Priority Number) เพื่อเป็นการพิจารณาว่าประเด็นความเสี่ยงต่างๆอยู่ในระดับที่ยอมรับได้หรือยอมรับไม่ได้ และจากนั้นนำเอาประเด็นความเสี่ยงที่อยู่ในระดับที่ยอมรับไม่ได้ไปจัดลำดับความสำคัญของความเสี่ยงเรียงตามลำดับค่า RPN จากมากไปหาน้อย และผลการประเมินความเสี่ยงพบว่า ประเด็นความเสี่ยงทั้งหมด 23 ประเด็นอยู่ในระดับที่ยอมรับไม่ได้ และมีผลการจัดลำดับความสำคัญของความเสี่ยงได้ทั้งหมด 15 ลำดับ ดังตารางที่ 8.1

ตารางที่ 8.1 ประเด็นความเสี่ยงที่อยู่ในระดับที่ยอมรับไม่ได้เรียงตามลำดับค่า RPN

| ข้อ | ประเด็นความเสี่ยง | ระดับคะแนน | | | |
|---|---|---|---|---|---|
| | | **S** | **O** | **D** | **RPN** |
| 1 | เครื่องคอมพิวเตอร์ติดไวรัส | 5 | 5 | 4 | **100** |
| 2 | คอมพิวเตอร์ Restart เอง | 5 | 4 | 4 | **80** |
| 3 | ระบบคอมพิวเตอร์ล่ม | 5 | 4 | 3 | **60** |
| | เข้าใช้งานโปรแกรมไม่ได้ | 5 | 4 | 3 | **60** |
| 4 | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | 4 | 5 | 3 | **60** |
| | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | 4 | 5 | 3 | **60** |
| 5 | ข้อมูลสูญหาย | 5 | 5 | 2 | **50** |
| 6 | เครื่องคอมพิวเตอร์ทำงานช้า | 4 | 3 | 4 | **48** |
| | โปรแกรมทำงานผิดพลาด | 4 | 4 | 3 | **48** |
| 7 | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | 3 | 5 | 3 | **45** |
| 8 | หน้าจอค้างสีฟ้า (Blue Screen of Death) | 5 | 2 | 4 | **40** |
| | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | 5 | 2 | 4 | **40** |
| 9 | บุคลากรคีย์ข้อมูลผิด | 4 | 5 | 2 | **40** |
| | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | 4 | 5 | 2 | **40** |
| 10 | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | 4 | 3 | 3 | **36** |
| 11 | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | 3 | 3 | 4 | **36** |
| | แก้ไขโปรแกรมไม่ทัน | 3 | 3 | 4 | **36** |
| 12 | ไม่มีการUpdateข้อมูล | 4 | 4 | 2 | **32** |
| 13 | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | 2 | 4 | 4 | **32** |
| 14 | บุคลากรใช้งานโปรแกรมไม่เป็น | 4 | 2 | 3 | **24** |
| | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | 4 | 3 | 2 | **24** |
| 15 | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | 2 | 3 | 3 | **18** |
| | CD-ROM ใช้งานไม่ได้ | 2 | 3 | 3 | **18** |

เมื่อทำการประเมินความเสี่ยงและทำการจัดลำดับความเสี่ยงเสร็จสิ้นแล้ว ขั้นตอนต่อไป คือ การสร้างแผนจัดการความเสี่ยง โดยขั้นตอนแรกของการสร้างแผนจัดการความเสี่ยง คือ การวิเคราะห์ปัจจัยเสี่ยงหรือการวิเคราะห์สาเหตุพื้นฐานของการเกิดความเสี่ยง ซึ่งในงานวิจัยชิ้นนี้จะใช้วิธีการ Fault Tree Analysis หรือ FTA ในการวิเคราะห์สาเหตุพื้นฐานของการเกิดความเสี่ยง ซึ่งผลจากการทำการวิเคราะห์ปัจจัยเสี่ยงหรือการวิเคราะห์สาเหตุพื้นฐานของการเกิดความเสี่ยงของประเด็นความเสี่ยงทั้งหมดพบว่า สาเหตุพื้นฐานของการเกิดของความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ตนั้นเกิดจากปัจจัยภายใน โดยส่วนใหญ่เกิดจากพฤติกรรมและวิธีการใช้งานของบุคลากร จากนั้นนำสาเหตุพื้นฐานของการเกิดความเสี่ยงที่ได้นำไปเป็นข้อมูลในการสร้างแผนจัดการความเสี่ยง โดยมีแนวทางในการสร้างแผนจัดการความเสี่ยง 4 แนวทาง ดังต่อไปนี้

1. Take-การยอมรับความเสี่ยง (Risk Acceptance)
2. Treat-การลด/ควบคุมความเสี่ยง (Risk Reduction/Control)
3. Terminate-การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)
4. Transfer-การกระจาย/โอนความเสี่ยง (Risk Sharing/Spreading)

ภายหลังจากทำการสร้างแผนจัดการความเสี่ยงเสร็จสิ้นแล้วจะต้องมีการประเมินด้วยว่าแผนจัดการความเสี่ยงที่ถูกสร้างขึ้นนั้นมีความเหมาะสมหรือไม่ โดยมีเกณฑ์และวิธีการประเมินความเหมาะสมของแผนจัดการความเสี่ยงดังต่อไปนี้

1. ด้านความมีประสิทธิภาพของแผนจัดการความเสี่ยง
   - หากแผนจัดการความเสี่ยงใดที่คาดการณ์ว่าจะทำให้ความเสี่ยงนั้นมีโอกาสเกิดลดลง จะถือว่าแผนจัดการความเสี่ยงนั้นมีประสิทธิภาพ
2. ด้านความเป็นไปได้ในการปฏิบัติตามแผนจัดการความเสี่ยง
   - หากแผนจัดการความเสี่ยงใดไม่ขัดกับนโยบายขององค์กร จะถือว่าแผนจัดการความเสี่ยงนั้นมีความเป็นไปได้ในการปฏิบัติ
   - หากแผนจัดการความเสี่ยงใดเมื่อนำไปปฏิบัติแล้วไม่เป็นอุปสรรคต่อการปฏิบัติงานของบุคลากร จะถือว่าแผนจัดการความเสี่ยงนั้นมีความเป็นไปได้ในการปฏิบัติ

กล่าวโดยสรุป คือ หากแผนจัดการความเสี่ยงใดขัดกับข้อใดข้อหนึ่ง จะถือว่าแผนจัดการความเสี่ยงนั้นไม่มีความเหมาะสมและจะไม่นำไปปฏิบัติ

ผลจากการสร้างแผนจัดการความเสี่ยงพบว่าแผนจัดการความเสี่ยงของประเด็นความเสี่ยงทั้งหมดสามารถสรุปแผนจัดการความเสี่ยงที่เป็นแผนจัดการความเสี่ยงหลักๆได้ดังต่อไปนี้

1. ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน
2. กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน
3. วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง
4. จัดอมรมบุคลากร

ขั้นตอนต่อไปคือการนำแผนจัดการความเสี่ยงทั้งหมดไปประยุกต์ใช้ ซึ่งมีระยะเวลาในการเริ่มดำเนินงานดังต่อไปนี้

1. ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน สามารถเริ่มแผนได้เมื่อผู้บริหารอนุมัติ
2. กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน สามารถเริ่มแผนได้เมื่อมีการสั่งซื้อคอมพิวเตอร์ชุดใหม่
3. วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง สามารถเริ่มแผนได้ทันที
4. จัดอมรมบุคลากร สามารถเริ่มแผนได้เมื่อผู้บริหารอนุมัติ

หลังจากมีการประยุกต์ใช้แผนจัดการความเสี่ยงขั้นตอนต่อมา คือ การติดตามและประเมินผลแผนจัดการความเสี่ยง จากการประยุกต์ใช้แผนจัดการความเสี่ยงพบว่า มีแผนจัดการความเสี่ยงเพียงแผนเดียวจากทั้งหมด 4 แผนหลักที่สามารถดำเนินงานได้ทันที คือ วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง แต่การที่จะติดตามผลแผนจัดการความเสี่ยงและประเมินว่าแผนจัดการความเสี่ยงสามารถจัดการกับความเสี่ยงต่างๆได้หรือไม่จะต้องดำเนินงานให้ครบทั้ง 4 แผนก่อนจึงจะสามารถทำการติดตามและประเมินผลแผนจัดการความเสี่ยงได้ ดังนั้นงานวิจัยชิ้นนี้จะทำการติดตามผลแผนจัดการความเสี่ยงโดยใช้วิธีการประเมินความเสี่ยงแบบคาดหมาย (Expected) เพื่อเปรียบเทียบค่า RPN ของความเสี่ยงก่อนและหลังจากมีแผนจัดการความเสี่ยง และนำค่า RPN ที่ได้ไปเปรียบเทียบกับเกณฑ์การยอมรับได้ของความเสี่ยง เพื่อประเมินว่าแผนจัดการความเสี่ยงนั้นสามารถจัดการกับความเสี่ยงนั้นๆให้อยู่ในระดับที่ยอมรับได้ได้หรือไม่ โดยการประเมินความเสี่ยงแบบคาดหมายหลังจากมีแผนจัดการความเสี่ยงนั้นจะใช้วิธีการและเกณฑ์การประเมินแบบเดียวกับการประเมินความเสี่ยงก่อนมีแผนจัดการความเสี่ยงแต่จะต่างกันตรงที่ การประเมินความเสี่ยงแบบคาดหมายหลังจากมีแผนจัดการความเสี่ยงจะทำการประเมินเพียง 2 ปัจจัย คือ โอกาสในการเกิดความเสี่ยง (Occurrence; O) และความสามารถในการตรวจพบความเสี่ยง (Detection; D) ส่วนความรุนแรงของความเสี่ยง (Severity; S)

จะใช้ค่าเดิมจากการประเมินความเสี่ยงก่อนมีแผนจัดการความเสี่ยง จากนั้นนำค่าที่ได้จากการประเมินไปคิดเป็นค่า RPN และนำไปเปรียบเทียบกับค่า RPN ก่อนมีแผนจัดการความเสี่ยง ซึ่งผลการเปรียบเทียบค่า RPN ก่อนและหลังมีแผนจัดการความเสี่ยงได้แสดงไว้ในตารางที่ 8.2

ตารางที่ 8.2 ผลการเปรียบเทียบค่า RPN ของประเด็นความเสี่ยงก่อนและหลังมีแผนจัดการความเสี่ยง

| ข้อ | ประเด็นความเสี่ยง | ค่า RPN | |
|---|---|---|---|
| | | ก่อนมีแผน | หลังมีแผน |
| 1 | เครื่องคอมพิวเตอร์ติดไวรัส | **100** | **10** |
| 2 | คอมพิวเตอร์ Restart เอง | **80** | **10** |
| 3 | ระบบคอมพิวเตอร์ล่ม | **60** | **5** |
| | เข้าใช้งานโปรแกรมไม่ได้ | **60** | **10** |
| 4 | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | **60** | **12** |
| | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | **60** | **8** |
| 5 | ข้อมูลสูญหาย | **50** | **5** |
| 6 | เครื่องคอมพิวเตอร์ทำงานช้า | **48** | **8** |
| | โปรแกรมทำงานผิดพลาด | **48** | **8** |
| 7 | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | **45** | **6** |
| 8 | หน้าจอค้างสีฟ้า (Blue Screen of Death) | **40** | **5** |
| | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | **40** | **5** |
| 9 | บุคลากรคีย์ข้อมูลผิด | **40** | **12** |
| | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | **40** | **12** |
| 10 | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | **36** | **4** |
| 11 | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | **36** | **6** |
| | แก้ไขโปรแกรมไม่ทัน | **36** | **6** |
| 12 | ไม่มีการUpdateข้อมูล | **32** | **8** |
| 13 | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | **32** | **4** |
| 14 | บุคลากรใช้งานโปรแกรมไม่เป็น | **24** | **4** |
| | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | **24** | **4** |
| 15 | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | **18** | **2** |
| | CD-ROM ใช้งานไม่ได้ | **18** | **2** |

จากการพิจารณาผลการเปรียบเทียบค่า RPN ของประเด็นความเสี่ยงก่อนและหลังมีแผนจัดการความเสี่ยงในตารางที่ 8.2 พบว่าหลังจากมีแผนจัดการความเสี่ยง ทุกประเด็นความเสี่ยงมีค่า RPN ลดลง และเมื่อพิจารณาค่า RPN ของแต่ละประเด็นความเสี่ยงพบว่าอยู่ในระดับที่ยอมรับได้ ดังนั้นจึงสามารถประเมินผลแผนจัดการความเสี่ยงได้ว่า แผนจัดการความเสี่ยงมีประสิทธิภาพสามารถจัดการกับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

และเมื่อมีการนำแผนจัดการความเสี่ยงมาใช้ในการดำเนินงานครบทั้ง 4 แผนหลักแล้ว จะต้องมีการติดตามอย่างเป็นรูปธรรมว่าแผนจัดการความเสี่ยงที่นำมาใช้ในการดำเนินงานนั้นสามารถที่จะบริหารจัดการกับประเด็นความเสี่ยงนั้นๆได้ตามที่ได้คาดหมายเอาไว้ในการประเมินความเสี่ยงแบบคาดหมายหลังจากมีแผนจัดการความเสี่ยงหรือไม่ โดยมีการกำหนดประเด็นความเสี่ยงที่ต้องติดตาม ข้อมูลที่ต้องติดตาม และความถี่ในการติดตาม หลังจากจากนำแผนจัดการความเสี่ยงมาใช้ในการดำเนินงานครบทั้ง 4 แผนหลัก ดังตารางที่ 7.4 (อยู่ในบทที่ 7)

**8.2 ปัญหาและข้อจำกัดในการทำวิจัย**

1. ขั้นตอนการเก็บข้อมูลใช้เวลานานเนื่องจากบุคลากรผู้ให้ข้อมูลมีภาระงานประจำที่ต้องรับผิดชอบมาก ดังนั้นจึงต้องใช้ระยะเวลาในการรอการตอบกลับแบบสอบถามนาน

**8.3 ข้อเสนอแนะ**

1. ในการเก็บข้อมูลในขั้นตอนของการระบุความเสี่ยงควรใช้รูปแบบในการเก็บข้อมูลหลายๆรูปแบบร่วมกัน เช่น การใช้แบบสอบถาม การสัมภาษณ์ การประชุมระดมสมอง เป็นต้น ซึ่งการเก็บข้อมูลโดยใช้รูปแบบการเก็บข้อมูลหลายๆรูปแบบจะทำให้มีโอกาสในการได้รับข้อมูลที่ครบถ้วนสมบูรณ์มากกว่าการเก็บข้อมูลโดยใช้รูปแบบการเก็บข้อมูลรูปแบบใดรูปแบบหนึ่งเพียงรูปแบบเดียว
2. การนำแผนจัดการความเสี่ยงไปใช้ในการดำเนินงานต้องมีการชี้แจงให้บุคลากรผู้มีส่วนเกี่ยวข้องเข้าใจว่าแผนจัดการความเสี่ยงเป็นการควบคุม ป้องกัน และลดโอกาสในการเกิดความเสี่ยงไม่ได้เป็นการจับผิดการทำงานของบุคลากร เพื่อป้องกันไม่ให้บุคลากรมีอคติกับแผนจัดการความเสี่ยงเพราะหากบุคลากรมีอคติกับแผนจัดการความเสี่ยงอาจจะไม่ได้รับความร่วมมืออย่างเต็มที่จากบุคลากรในการดำเนินงานตามแผนจัดการความเสี่ยง

# รายการอ้างอิง

## ภาษาไทย


การไฟฟ้านครหลวง. บทความความหมายของความเสี่ยง. แหล่งที่มา: http://www.mea.or.th/mearmo/data/risk_total.pdf [ธันวาคม 2549]

คณะกรรมการบริหารความเสี่ยง การไฟฟ้านครหลวง. คู่มือการบริหารความเสี่ยงการไฟฟ้านครหลวง, พฤศจิกายน 2547.

เจนเนตร มณีนาค. การบริหารจัดการความเสี่ยงระดับองค์กรจากหลักการสู่ภาคปฏิบัติ. กรุงเทพฯ: ไฟนอลการพิมพ์, 2548.

นฤมล สะอาดโฉม. Risk Management การบริหารความเสี่ยง. กรุงเทพฯ: ก.พลพิมพ์ (1996) จำกัด, 2548.

ประเสริฐ อัครประถมพงศ์ และ ธารชุดา อมรเพชรกุล. การพัฒนาระบบบริหารความเสี่ยงในส่วนการพัสดุ สำนักบริหารแผนและการคลัง. วิทยานิพนธ์ปริญญามหาบัณฑิต, ภาควิชาวิศวกรรมอุตสาหการ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2546.


## ภาษาอังกฤษ


Hank Marquis (2006, December 21), Fault Tree Analysis in 6 Steps [online].Available from: http://www.itsmwatch.com/itil/article.php/11700_3650536_1

Ronald L. Meier. (2000, October), Integrating Enterprise-Wide Risk Management Concepts into Industrial Technology Curricula [online].Available from: http://www.nait.org

# ภาคผนวก

# ภาคผนวก ก
# แบบสอบถามที่ใช้ในการทำวิจัย

# ภาคผนวก ก-1
# แบบสอบถามที่ใช้ในการระบุความเสี่ยง

***แบบสอบถาม***

***การระบุความเสี่ยงของการใช้คอมพิวเตอร์และอินเตอร์เน็ต***

**ข้อมูลของบุคลากรผู้ให้ข้อมูล**

ตำแหน่ง ..... ฝ่าย ..... อายุการทำงาน ..... ปี

**คำอธิบาย :** ความเสี่ยง หมายถึง เหตุการณ์หรือสถานการณ์ใดๆที่เคยเกิดขึ้นหรืออาจจะเกิดขึ้นในอนาคต และเมื่อเหตุการณ์หรือสถานการณ์นั้นๆเกิดขึ้นจะส่งผลทำให้เกิดอุปสรรคในการทำงานหรือทำให้ไม่สามารถบรรลุวัตถุประสงค์ของการดำเนินงาน

**คำสั่ง :** กรุณาระบุความเสี่ยงที่ท่านคาดว่าอาจจะเกิดขึ้นของการใช้คอมพิวเตอร์และอินเตอร์เน็ตในการทำงานในองค์กรของท่านในด้านต่างๆดังต่อไปนี้

1. ความเสี่ยงด้านบุคลากร คือ ความเสี่ยงต่างๆที่เกี่ยวข้องกับบุคลากรในการใช้คอมพิวเตอร์และอินเตอร์เน็ต เช่น ความผิดพลาดด้านต่างๆที่เกิดจากการใช้งานคอมพิวเตอร์และอินเตอร์เน็ตของบุคลากร เป็นต้น

2. ความเสี่ยงด้านเทคโนโลยี คือ ความเสี่ยงต่างๆที่เกี่ยวข้องกับเทคโนโลยีในการใช้คอมพิวเตอร์และอินเตอร์เน็ต เช่น เทคโนโลยีต่างๆที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และอินเตอร์เน็ตมีความซับซ้อน หรือ ภัยคุกคามต่างๆอันเกิดจากเทคโนโลยีที่ก้าวหน้าเกี่ยวกับการใช้คอมพิวเตอร์และอินเตอร์เน็ต เป็นต้น

3. ความเสี่ยงด้านข้อมูล คือ ความเสี่ยงต่างๆที่เกี่ยวข้องกับข้อมูลในการใช้คอมพิวเตอร์และอินเตอร์เน็ต เช่น ความผิดพลาดต่างๆที่เกี่ยวข้องกับข้อมูล ข้อมูลสูญหาย เป็นต้น

4. ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์ คือ ความเสี่ยงต่างๆที่เกี่ยวข้องกับฮาร์ดแวร์และซอฟท์แวร์ในการใช้คอมพิวเตอร์และอินเตอร์เน็ต เช่น ความบกพร่องของฮาร์ดแวร์และซอฟท์แวร์ เป็นต้น

5. ความเสี่ยงด้านกฎหมาย คือ ความเสี่ยงต่างๆที่เกี่ยวข้องกับกฎหมายในการใช้คอมพิวเตอร์และอินเตอร์เน็ต เช่น การดำเนินงานใดๆที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และอินเตอร์เน็ตซึ่งอาจทำให้ขัดต่อกฎหมาย เป็นต้น

**1. ความเสี่ยงด้านบุคลากร**

.....

.....

.....

.....

.....

**2. ความเสี่ยงด้านเทคโนโลยี**

.....

.....

.....

.....

.....

**3. ความเสี่ยงด้านข้อมูล**

.....

.....

.....

.....

.....

**4. ความเสี่ยงด้านฮาร์ดแวร์และซอฟท์แวร์**

.....

.....

.....

.....

.....

**5. ความเสี่ยงด้านกฎหมาย**

.....

.....

.....

.....

.....

**ข้อเสนอแนะเพิ่มเติม**

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

*** ขอบพระคุณที่ให้ความร่วมมือในการอนุเคราะห์ข้อมูล ***

# ภาคผนวก ก-2
# แบบสอบถามที่ใช้ในการประเมินความเสี่ยง

# *แบบสอบถาม*
# *การประเมินความเสี่ยง*

**ข้อมูลของบุคลากรผู้ให้ข้อมูล**

ตำแหน่ง ..... ฝ่าย ..... อายุการทำงาน ..... ปี

**คำสั่ง :** กรุณากรอกระดับคะแนนของประเด็นความเสี่ยงต่างๆ ในด้านของ ความรุนแรงของความเสี่ยง (Severity; S) ในตารางที่ 4, โอกาสในการเกิดความเสี่ยง (Occurrence; O) ในตารางที่ 5 และความสามารถในการตรวจพบความเสี่ยง (Detection; D) ในตารางที่ 6 โดยใช้เกณฑ์การให้คะแนนในตารางที่ 1-3

***ตารางที่ 1 ระดับความรุนแรงของความเสี่ยง (Severity; S)***

| ระดับคะแนน | ความรุนแรง | ความหมาย |
|---|---|---|
| 1 | น้อยมาก | ■ เสียเวลาการทำงานน้อยมาก<br>■ ส่งผลกระทบต่อผู้ป่วยน้อยมาก |
| 2 | น้อย | ■ เสียเวลาการทำงานน้อย<br>■ ส่งผลกระทบต่อผู้ป่วยน้อย |
| 3 | ปานกลาง | ■ เสียเวลาการทำงานปานกลาง<br>■ ส่งผลกระทบต่อผู้ป่วยปานกลาง |
| 4 | มาก | ■ เสียเวลาการทำงานมาก<br>■ ส่งผลกระทบต่อผู้ป่วยมาก |
| 5 | มากที่สุด | ■ เสียเวลาการทำงานมากที่สุด<br>■ ส่งผลกระทบต่อผู้ป่วยมากที่สุด<br>■ ขัดต่อกฎหมาย |

**หมายเหตุ :** เนื่องจากการพิจารณาให้คะแนนความรุนแรงของความเสี่ยงต้องทำการพิจารณาผลกระทบ 2 ด้านหลักๆ คือ การสูญเสียเวลาการทำงานและผลกระทบต่อผู้ป่วย ดังนั้นจะมีบางกรณีที่คะแนนความรุนแรงของความเสี่ยงจะมีความขัดแย้งกันอยู่ กล่าวคืออาจจะมีบางความเสี่ยงที่หากเกิดขึ้นอาจจะเสียเวลาการทำงานอยู่ในระดับหนึ่งแต่กลับมีผลกระทบต่อผู้ป่วยอยู่อีกระดับหนึ่ง ซึ่งหากเกิดเหตุการณ์ในกรณีนี้จะต้องพิจารณาให้คะแนนความรุนแรงของความเสี่ยงที่อยู่ในระดับที่สูงกว่าเสมอ

***ตารางที่ 2 ระดับโอกาสในการเกิดความเสี่ยง (Occurrence; O)***

| ระดับคะแนน | โอกาสเกิด | ความหมาย |
|---|---|---|
| 1 | น้อยมาก | ■ เกิดได้เฉพาะสถานการณ์ผิดปกติ : ทุกปี |
| 2 | น้อย | ■ สามารถเกิดขึ้นได้น้อยครั้ง : ทุก 6 เดือน |
| 3 | ปานกลาง | ■ อาจเกิดขึ้นได้บ้าง บางโอกาส : ทุกเดือน |
| 4 | มาก | ■ เกิดขึ้นได้เป็นปกติมักเกิดซ้ำบ่อยๆ : ทุกสัปดาห์ |
| 5 | มากที่สุด | ■ ไม่สามารถหลีกเลี่ยงได้ มีโอกาสเกิดสูงมาก : ทุกวัน |

***ตารางที่ 3 ระดับความสามารถในการตรวจพบความเสี่ยง (Detection; D)***

| ระดับคะแนน | ประสิทธิภาพ | ความหมาย |
|---|---|---|
| 1 | สูงที่สุด | ■ สามารถตรวจพบได้แน่นอนเป็นส่วนใหญ่/มีการควบคุมที่ดีมาก |
| 2 | สูง | ■ มีโอกาสสูงในการตรวจพบ/มีการควบคุมที่ดี |
| 3 | ปานกลาง | ■ อาจตรวจพบได้ในบางครั้ง/มีการควบคุมปานกลาง |
| 4 | ต่ำ | ■ มีโอกาสตรวจพบน้อยมาก/มีการควบคุมที่ไม่ค่อยดี |
| 5 | ต่ำมาก | ■ ไม่สามารถตรวจพบได้เลย/ไม่มีการควบคุม |

***ตารางที่ 4 ระดับความรุนแรงของความเสี่ยง (Severity; S)***

| ลำดับที่ | ประเด็นความเสี่ยง | คะแนน |
|---|---|---|
| **1** | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | |
| **2** | บุคลากรใช้งานโปรแกรมไม่เป็น | |
| **3** | บุคลากรคีย์ข้อมูลผิด | |
| **4** | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | |
| **5** | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | |
| **6** | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | |
| **7** | เครื่องคอมพิวเตอร์ติดไวรัส | |
| **8** | ไม่มีการUpdateข้อมูล | |
| **9** | ข้อมูลสูญหาย | |
| **10** | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | |
| **11** | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | |
| **12** | แก้ไขโปรแกรมไม่ทัน | |
| **13** | ระบบคอมพิวเตอร์ล่ม | |
| **14** | เครื่องคอมพิวเตอร์ทำงานช้า | |
| **15** | โปรแกรมทำงานผิดพลาด | |
| **16** | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | |
| **17** | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | |
| **18** | เข้าใช้งานโปรแกรมไม่ได้ | |
| **19** | คอมพิวเตอร์ Restart เอง | |
| **20** | CD-ROM ใช้งานไม่ได้ | |
| **21** | หน้าจอค้างสีฟ้า (Blue Screen of Death) | |
| **22** | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | |
| **23** | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | |

***ตารางที่ 5 ระดับโอกาสในการเกิดความเสี่ยง (Occurrence; O)***

| ลำดับที่ | ประเด็นความเสี่ยง | คะแนน |
|---|---|---|
| **1** | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | |
| **2** | บุคลากรใช้งานโปรแกรมไม่เป็น | |
| **3** | บุคลากรคีย์ข้อมูลผิด | |
| **4** | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | |
| **5** | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | |
| **6** | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | |
| **7** | เครื่องคอมพิวเตอร์ติดไวรัส | |
| **8** | ไม่มีการUpdateข้อมูล | |
| **9** | ข้อมูลสูญหาย | |
| **10** | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | |
| **11** | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | |
| **12** | แก้ไขโปรแกรมไม่ทัน | |
| **13** | ระบบคอมพิวเตอร์ล่ม | |
| **14** | เครื่องคอมพิวเตอร์ทำงานช้า | |
| **15** | โปรแกรมทำงานผิดพลาด | |
| **16** | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | |
| **17** | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | |
| **18** | เข้าใช้งานโปรแกรมไม่ได้ | |
| **19** | คอมพิวเตอร์ Restart เอง | |
| **20** | CD-ROM ใช้งานไม่ได้ | |
| **21** | หน้าจอค้างสีฟ้า (Blue Screen of Death) | |
| **22** | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | |
| **23** | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | |

***ตารางที่ 6 ระดับความสามารถในการตรวจพบความเสี่ยง (Detection; D)***

| ลำดับที่ | ประเด็นความเสี่ยง | คะแนน |
|---|---|---|
| **1** | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | |
| **2** | บุคลากรใช้งานโปรแกรมไม่เป็น | |
| **3** | บุคลากรคีย์ข้อมูลผิด | |
| **4** | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | |
| **5** | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | |
| **6** | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | |
| **7** | เครื่องคอมพิวเตอร์ติดไวรัส | |
| **8** | ไม่มีการUpdateข้อมูล | |
| **9** | ข้อมูลสูญหาย | |
| **10** | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | |
| **11** | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | |
| **12** | แก้ไขโปรแกรมไม่ทัน | |
| **13** | ระบบคอมพิวเตอร์ล่ม | |
| **14** | เครื่องคอมพิวเตอร์ทำงานช้า | |
| **15** | โปรแกรมทำงานผิดพลาด | |
| **16** | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | |
| **17** | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | |
| **18** | เข้าใช้งานโปรแกรมไม่ได้ | |
| **19** | คอมพิวเตอร์ Restart เอง | |
| **20** | CD-ROM ใช้งานไม่ได้ | |
| **21** | หน้าจอค้างสีฟ้า (Blue Screen of Death) | |
| **22** | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | |
| **23** | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | |

**ข้อเสนอแนะเพิ่มเติม**

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

*** ขอบพระคุณที่ให้ความร่วมมือในการอนุเคราะห์ข้อมูล ***

# ภาคผนวก ก-3
# แบบสอบถามที่ใช้ในประเมินความเหมาะสมของแผนจัดการความเสี่ยง

# *แบบสอบถาม*
# *การประเมินความเหมาะสมของแผนจัดการความเสี่ยง*

**ข้อมูลของบุคลากรผู้ให้ข้อมูล**

ตำแหน่ง ..... ฝ่าย ..... อายุการทำงาน ..... ปี

**คำอธิบาย**

การประเมินความเหมาะสมของแผนจัดการความเสี่ยงจะพิจารณาความเหมาะสม 2 ด้าน คือ

1. ด้านความมีประสิทธิภาพของแผนจัดการความเสี่ยง
2. ด้านความเป็นไปได้ในการปฏิบัติตามแผนจัดการความเสี่ยง

โดยมีวิธีการประเมินความเหมาะสมดังต่อไปนี้

1. ด้านความมีประสิทธิภาพของแผนจัดการความเสี่ยง
   - หากแผนจัดการความเสี่ยงใดที่คาดการณ์ว่าจะทำให้ความเสี่ยงนั้นมีโอกาสเกิดลดลง จะถือว่าแผนจัดการความเสี่ยงนั้นมีประสิทธิภาพ
2. ด้านความเป็นไปได้ในการปฏิบัติตามแผนจัดการความเสี่ยง
   - หากแผนจัดการความเสี่ยงใดไม่ขัดกับนโยบายขององค์กร จะถือว่าแผนจัดการความเสี่ยงนั้นมีความเป็นไปได้ในการปฏิบัติ
   - หากแผนจัดการความเสี่ยงใดเมื่อนำไปปฏิบัติแล้วไม่เป็นอุปสรรคต่อการปฏิบัติงานของบุคลากร จะถือว่าแผนจัดการความเสี่ยงนั้นมีความเป็นไปได้ในการปฏิบัติ

**คำสั่ง**

1. กรุณาทำเครื่องหมาย / ลงในช่องว่างหมายเลข 1 หากท่านคิดว่าแผนจัดการความเสี่ยงนั้นมีประสิทธิภาพ หรือทำเครื่อง **x** ลงในช่องว่างหมายเลข 1 หากท่านคิดว่าแผนจัดการความเสี่ยงไม่มีประสิทธิภาพ
2. กรุณาทำเครื่องหมาย / ลงในช่องว่างหมายเลข 2 หากท่านคิดว่าแผนจัดการความเสี่ยงนั้นมีความเป็นไปได้ในการปฏิบัติ หรือทำเครื่อง **x** ลงในช่องว่างหมายเลข 2 หากท่านคิดว่าแผนจัดการความเสี่ยงเป็นไปไม่ได้ในการนำไปปฏิบัติ

*ตารางที่ 1 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงคอมพิวเตอร์ติดไวรัส*

| *คอมพิวเตอร์ติดไวรัส* | | 1 | 2 |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | | |
| ไวรัสจากไฟล์ข้อมูลทั่วๆไป | Scan ทุกไฟล์ที่ Download มาจากอินเตอร์เน็ต | | |
| ไวรัสจากฟรีแวร์/แชร์แวร์ | ห้ามใช้โปรแกรมประเภทฟรีแวร์/แชร์แวร์ | | |
| แผ่นดิสก์,CD, Flash drive มีไวรัส | Scan แผ่นดิสก์,CDและ Flash drive ก่อนการใช้งาน | | |
| มีช่องโหว่ในระบบเครือข่าย | Update Firewall ให้เป็นปัจจุบันอยู่เสมอ | | |
| Operating System บกพร่อง | ทำการตรวจสอบชุดปรับปรุง (Patch หรือ Service Pack) ให้เป็นปัจจุบันอยู่เสมอ | | |
| การโจมตีจาก Hacker | หลีกเลี่ยงการดาว์นโหลดข้อมูลและโปรแกรมต่างๆที่ไม่เกี่ยวข้องกับการทำงานจากเว็บไซท์ | | |
| | หลีกเลี่ยงการเปิดอีเมล์ที่ไม่ทราบที่มาที่แน่นอน | | |
| | หลีกเลี่ยงการเปิดไฟล์แนบโดยอัตโนมัติหรือการตั้งค่าในโปรแกรมอีเมล์ให้ดาวน์โหลดไฟล์โดยอัตโนมัติ | | |
| | Scan ไฟล์หรือโปรแกรมที่ติดมากับ E-mail ก่อนที่จะเปิดอ่านหรือเก็บลงบนฮาร์ดดิสก์ | | |
| | Block เว็บไซท์ที่ไม่เกี่ยวข้องกับการทำงาน | | |

*ตารางที่ 2 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงคอมพิวเตอร์ Restart เอง*

| *คอมพิวเตอร์ Restart เอง* | | | |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | **1** | **2** |
| คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | เลือกการ์ดจอและแรมให้เหมาะสมกับการใช้งาน | | |
| อุปกรณ์ระบายความร้อนไม่ทำงาน | กำหนดระยะเวลาในการตรวจสอบสายไฟที่ต่อกับพัดลมระบายความร้อนให้อยู่ในสภาพที่พร้อมใช้งาน | | |
| | กำหนดระยะเวลาทำความสะอาดพัดลมระบายความร้อนโดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น | | |
| | จัดสายไฟภายในเครื่องให้เรียบร้อยไม่ขวางทางลมของพัดลม | | |
| อุปกรณ์ระบายความร้อนไม่เหมาะสม | เลือกชนิดของอุปกรณ์ระบายความร้อนให้เหมาะสมกับการใช้งาน | | |
| | เลือกขนาดของอุปกรณ์ระบายความร้อนให้เหมาะสมกับการใช้งาน | | |
| Power Supply ขัดข้อง | กำหนดระยะเวลาในการตรวจสอบ ขั้วต่อภายในระหว่าง Power Supply กับ อุปกรณ์ฮาร์ดแวร์อื่นๆภายในเครื่องให้แน่นอยู่เสมอ | | |
| | กำหนดระยะเวลาในการทำความสะอาดพัดลมที่ติดอยู่กับ Power Supply โดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น | | |
| | เลือกใช้ขนาดกำลังไฟฟ้า(ค่าวัตต์) ของ Power Supply ให้เหมาะสมกับฮาร์ดแวร์อื่นๆที่ใช้ | | |
| Driver มีปัญหา | อัพเดท Driverให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ | | |
| Hardware มีปัญหา | เมื่อ การ์ดจอ,แรม หรือ Power Supply ชำรุดต้องส่งซ่อมหรือเปลี่ยนใหม่ตามความเหมาะสม | | |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 | | |

*ตารางที่ 3 ประเมินความเหมาะสมของแผนจัดการความเสี่ยง*

| ***ระบบคอมพิวเตอร์ล่ม*** | | | |
|---|---|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** | **1** | **2** |
| สัญญาณรบกวน | หลีกเลี่ยงการเดินสาย LAN คู่ไปกับสายสัญญาณอื่นๆ | | |
| | ติดตั้งอุปกรณ์ป้องกันสัญญาณรบกวนที่มาจากสายส่งและจากอุปกรณ์ต่าง ๆ | | |
| Under Voltage | ติดตั้งอุปกรณ์ประเภท UPS ป้องกันไฟขาดหรือเกิน | | |
| Over Voltage | | | |
| Hardware มีปัญหา | หากมีการเปลี่ยนฮาร์ดแวร์ใหม่ต้องมีการตรวจสอบว่าฮาร์ดแวร์ที่เปลี่ยนใหม่สามารถทำงานร่วมกับฮาร์ดแวร์ที่มีอยู่เดิมได้ | | |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 | | |
| คอมพิวเตอร์บางเครื่องในระบบมีปัญหา | วางระบบเครือข่ายแบบใยแมงมุม | | |
| อุปกรณ์เชื่อมต่อมีปัญหา | เดินสาย LAN ให้เป็นระเบียบเรียบร้อย | | |
| | กำหนดระยะเวลาในการตรวจสอบสาย LAN ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ | | |
| | กำหนดระยะเวลาในการตรวจสอบPort เชื่อมต่อให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ | | |
| ภัยธรรมชาติ | ห้องที่เก็บเครื่องแม่ข่าย(Server) ต้องมั่นคงแข็งแรง | | |

*ตารางที่ 4 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงเข้าใช้งานโปรแกรมไม่ได้*

| *เข้าใช้งานโปรแกรมไม่ได้* | | | |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | **1** | **2** |
| บุคลากรขาดทักษะการใช้งาน | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | | |
| โปรแกรมไม่สมบูรณ์ | กำหนดให้ผู้มีความชำนาญงานเป็นผู้ติดตั้งโปรแกรม | | |
| | กรณีที่เป็นโปรแกรมสำเร็จรูปต้องใช้โปรแกรมที่ถูกลิขสิทธิ์ | | |
| | กรณีที่เป็นโปรแกรมที่ทางโรงพยาบาลเขียนเองต้องมีการทดสอบการใช้งานก่อนการนำมาใช้งานจริง | | |
| ขาดโปรแกรมพื้นฐานที่จำเป็น | ติดตั้งโปรแกรมพื้นฐานที่โปรแกรมนั้นๆต้องการให้ครบ | | |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 | | |

*ตารางที่ 5 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงบุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต*

| *บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต* | | | |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | **1** | **2** |
| บุคลากรขาดความรับผิดชอบ | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | | |
| ขาดการควบคุมการใช้งาน | ห้ามติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการทำงา | | |
| | Block เว็บไซท์ที่ไม่เกี่ยวข้องกับการทำงาน | | |

*ตารางที่ 6 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงย้ายหรือถ่ายโอนข้อมูลไม่ได้*

| ***ย้ายหรือถ่ายโอนข้อมูลไม่ได้*** | | | |
|---|---|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** | **1** | **2** |
| บุคลากรขาดทักษะการใช้งาน | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | | |
| การ์ด Lan เสีย | กำหนดระยะเวลาในการตรวจสอบการ์ด Lan ให้อยู่ในสภาพพร้อมใช้งานเสมอ | | |
| | เมื่อการ์ด Lan เสียต้องมีการซ่อมหรือเปลี่ยนใหม่ตามความเหมาะสม | | |

*ตารางที่ 7 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงข้อมูลสูญหาย*

| ***ข้อมูลสูญหาย*** | | | |
|---|---|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** | **1** | **2** |
| บุคลากรทำงานผิดพลาด | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | | |
| ไม่มีการสำรองข้อมูล | ทำการสำรองข้อมูล(Backup) อย่างสม่ำเสมอ | | |
| ระบบคอมพิวเตอร์ล่ม | ใช้แผนจัดการความเสี่ยงในตารางที่ 3 | | |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 | | |

*ตารางที่ 8 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงเครื่องคอมพิวเตอร์ทำงานช้า*

| *เครื่องคอมพิวเตอร์ทำงานช้า* | | | |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | **1** | **2** |
| คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | เลือกซีพียูให้เหมาะสมกับการใช้งาน | | |
| | เลือกRamให้เหมาะสมกับการใช้งาน | | |
| | เลือกขนาดฮาร์ดดิสก์ให้เหมาะสมกับการใช้งาน | | |
| มีขยะในฮาร์ดดิสก์มากเกินไป | กำหนดระยะเวลาในการทำ Disk Cleanup | | |
| | กำหนดระยะเวลาในการทำ Disk Defragmenter | | |
| | ลบ Temporary Files อย่างสม่ำเสมอ | | |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 | | |

*ตารางที่ 9 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงโปรแกรมทำงานผิดพลาด*

| *โปรแกรมทำงานผิดพลาด* | | | |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | **1** | **2** |
| โปรแกรมไม่สมบูรณ์ | ต้องให้ผู้มีความชำนาญงานเป็นผู้ติดตั้งโปรแกรม | | |
| | กรณีที่เป็นโปรแกรมสำเร็จรูปต้องใช้โปรแกรมที่ถูกลิขสิทธิ์ | | |
| | กรณีที่เป็นโปรแกรมที่ทางโรงพยาบาลเขียนเองต้องมีการทดสอบการใช้งานก่อนการนำมาใช้งานจริง | | |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 | | |
| Hardware มีปัญหา | กำหนดระยะเวลาในการตรวจสอบHardware(Input/Output) ให้อยู่ในสภาพที่พร้อมใช้งาน | | |

*ตารางที่ 10 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงบุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น*

| *บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น* | | | |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | **1** | **2** |
| บุคลากรขาดทักษะการใช้งาน | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | | |
| โปรแกรม Edit Dataไม่ได้หลังบันทึก | เขียนโปรแกรมให้สามารถ Edit Data ได้ตามลักษณะการใช้งาน | | |

*ตารางที่ 11 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงหน้าจอค้างสีฟ้า (Blue Screen of Death)*

| *หน้าจอค้างสีฟ้า (Blue Screen of Death)* | | | |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | **1** | **2** |
| Hardware มีปัญหา | กำหนดระยะเวลาในการตรวจสอบ Hardware ทุกชิ้นส่วนให้อยู่ในสภาพพร้อมใช้งานเสมอ | | |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 | | |
| Driver มีปัญหา | อัพเดท Driverให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ | | |
| คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน | | |

*ตารางที่ 12ประเมินความเหมาะสมของแผนจัดการความเสี่ยงใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์*

| ***ใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์*** | | **1** | **2** |
|---|---|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** | | |
| บุคลากรนำโปรแกรมมาลงเอง | ห้ามบุคลากรนำโปรแกรมมาลงเองโดยไม่ได้รับอนุญาต | | |
| บุคลากรโหลดโปรแกรมละเมิดลิขสิทธิ์จากอินเตอร์เน็ต | ห้ามบุคลากรโหลดโปรแกรมละเมิดลิขสิทธิ์จากอินเตอร์เน็ต | | |
| ละเมิด Site/Network Licens | ต้องศึกษา Site/Network Licens ของโปรแกรมที่จะนำมาใช้ ให้ละเอียดก่อนนำโปรแกรมนั้นๆมาใช้งาน | | |

*ตารางที่ 13ประเมินความเหมาะสมของแผนจัดการความเสี่ยงบุคคลากรคีย์ข้อมูลผิด*

| ***บุคคลากรคีย์ข้อมูลผิด*** | | **1** | **2** |
|---|---|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** | | |
| บุคลากรทำงานผิดพลาด | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | | |
| บุคลากรมีปัญหาการได้ยิน | มีการตรวจสุขภาพให้กับบุคลากรผู้ใช้งานคอมพิวเตอร์ทุกปี | | |
| บุคลากรมีปัญหาด้านสายตา | | | |
| ลายมืออ่านยาก | ออกแบบแบบฟอร์มต่างๆที่ต้องใช้ในโรงพยาบาลให้เป็นแบบฟอร์มที่ต้องใช้ลายมือเขียนน้อยที่สุด | | |

*ตารางที่ 14 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงสั่งพิมพ์ (Print) ข้อมูลไม่ได้*

| *สั่งพิมพ์ (Print) ข้อมูลไม่ได้* | | 1 | 2 |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | | |
| บุคลากรขาดทักษะการใช้งาน | จัดทำคู่มือการใช้งานเบื้องต้นโดยมีรายละเอียด<br>1. วิธีการสั่งพิมพ์<br>2. วิธีตรวจสอบสถานะของ Printer ว่าพร้อมใช้งานหรือไม่ | | |
| PRINTER มีปัญหา | ตรวจสอบอุปกรณ์ต่อเชื่อมต่างๆระหว่าง Printer กับ คอมพิวเตอร์ให้อยู่ในสภาพพร้อมใช้งาน | | |
| โปรแกรมทำงานผิดพลาด | ใช้แผนจัดการความเสี่ยงในตารางที่ 9 | | |

*ตารางที่ 15 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงขาดบุคลากรในบางตำแหน่งที่ควรจะมี*

| *ขาดบุคลากรในบางตำแหน่งที่ควรจะมี* | | 1 | 2 |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | | |
| ภาระ/ลักษณะงานเพิ่ม | มีการกำหนดระยะเวลาในการประชุมหารือร่วมกันของทุกฝ่ายที่เกี่ยวข้องเพื่อประเมินภาระงานและลักษณะงานเพื่อสรรหาบุคลากรให้เหมาะสมกับงานและเพียงพอต่อภาระงาน | | |
| ไม่มีการประเมินภาระ/ลักษณะงาน | | | |

*ตารางที่ 16 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงบุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย*

| *บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย* | | 1 | 2 |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | | |
| ภาระงานมาก | มีการส่งเสริมและจัดสรรเวลาเพื่อให้บุคลากรผู้เกี่ยวข้องเข้าอบรมหลักสูตรต่างๆด้าน IT ตามความเหมาะสม | | |
| องค์กรไม่ส่งเสริม | | | |

*ตารางที่ 17 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงแก้ไขโปรแกรมไม่ทัน*

| *แก้ไขโปรแกรมไม่ทัน* | | 1 | 2 |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | | |
| โปรแกรมขาดความยืดหยุ่น | มีการออกแบบและเขียนโปรแกรมให้ยืดหยุ่นและปรับเปลี่ยนได้ง่าย | | |
| ขาดการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง | มีการติดต่อสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องให้รวดเร็วเพื่อให้ทันต่อการเปลี่ยนแปลง | | |
| จัดทำโปรแกรม Specไม่ครบถ้วน | มีการสำรวจข้อมูลให้ละเอียดก่อนจัดทำโปรแกรม | | |

*ตารางที่ 18 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงไม่มีการ Update ข้อมูล*

| *ไม่มีการ Update ข้อมูล* | | 1 | 2 |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | | |
| ขาดการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง | มีการติดต่อสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องให้รวดเร็วเพื่อให้ทันต่อการเปลี่ยนแปลง | | |
| บุคลากรทำงานล่าช้า | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | | |

*ตารางที่ 19 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงค้นหา (Search) ข้อมูลที่ต้องการใช้ในระบบไม่พบ*

| *ค้นหา (Search) ข้อมูลที่ต้องการใช้ในระบบไม่พบ* | | 1 | 2 |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | | |
| บุคลากรขาดทักษะการใช้งาน | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | | |
| ช่องทางการค้นหาซับซ้อนเกินไป | กำหนดช่องทางการเข้าถึงข้อมูลให้ง่ายต่อการเข้าถึงข้อมูล | | |
| ไม่ได้บันทึกข้อมูลไว้ | กำหนดให้ชัดเจนว่าข้อมูลใดต้องทำการบันทึกไว้ | | |
| ข้อมูลสูญหาย | ใช้แผนจัดการความเสี่ยงในตารางที่ 7 | | |

*ตารางที่ 20 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงบุคคลากรใช้งานโปรแกรมไม่เป็น*

| *บุคคลากรใช้งานโปรแกรมไม่เป็น* | | | |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | **1** | **2** |
| บุคลากรขาดทักษะการใช้งาน | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | | |
| เป็นโปรแกรมเฉพาะทาง | | | |
| เปลี่ยนโปรแกรมหรือเวอร์ชัน | | | |

*ตารางที่ 21 ประเมินความเหมาะสมของแผนจัดการความเสี่ยงจำนวน Computer ไม่เพียงพอต่อการใช้งาน*

| *จำนวน Computer ไม่เพียงพอต่อการใช้งาน* | | | |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | **1** | **2** |
| ไม่มีการสำรวจความต้องการ | มีการสำรวจความต้องการก่อนจัดหาคอมพิวเตอร์ในแต่ละครั้ง | | |
| อยู่ระหว่างการส่งซ่อม | จัดให้มีเครื่องคอมพิวเตอร์สำรองกรณีที่เครื่องหลักถูกส่งซ่อม | | |

*ตารางที่ 22 ประเมินความเหมาะสมของแผนจัดการความเสี่ยง Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน*

| *Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน* | | | |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | **1** | **2** |
| สำรวจข้อมูลไม่ละเอียดก่อนเขียนโปรแกรม | ก่อนจัดทำโปรแกรมต้องมีการสำรวจข้อมูลการใช้งานให้ละเอียด | | |
| ไม่มีการทดสอบใช้งานก่อนใช้จริง | เมื่อจัดทำโปรแกรมเสร็จแล้วต้องมีการทดสอบใช้งานก่อนที่จะนำโปรแกรมนั้นไปใช้งานจริง | | |

*ตารางที่ 23 ประเมินความเหมาะสมของแผนจัดการความเสี่ยง CD-ROM ใช้งานไม่ได้*

| *CD-ROM ใช้งานไม่ได้* | | 1 | 2 |
|---|---|---|---|
| *สาเหตุพื้นฐาน* | *แผนจัดการความเสี่ยง* | | |
| Power Supply ขัดข้อง | กำหนดระยะเวลาในการตรวจสอบ ขั้วต่อภายในระหว่าง Power Supply กับ CD-ROM ให้อยู่ในสภาพพร้อมใช้งานเสมอ | | |
| | กำหนดระยะเวลาในการทำความสะอาดพัดลมที่ติดอยู่กับ Power Supply โดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น | | |
| ตัว CD-ROM เสีย | เปลี่ยน CD-ROM ใหม่ | | |
| สายเคเบิล(IDE Cable) หลุด | กำหนดระยะเวลาในการตรวจสอบ สายเคเบิล(IDE Cable) และสายไฟ(Power Cable) ให้อยู่ในสภาพพร้อมใช้งานเสมอ | | |
| สายไฟ(Power Cable) หลุด | | | |

**ข้อเสนอแนะเพิ่มเติม**

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

*** ขอบพระคุณที่ให้ความร่วมมือในการอนุเคราะห์ข้อมูล ***

# ภาคผนวก ก-4
# แบบสอบถามที่ใช้ในการประเมินความเสี่ยงหลังจากมีแผนจัดการความเสี่ยง

# *แบบสอบถาม*
# *การประเมินความเสี่ยงหลังจากมีแผนจัดการความเสี่ยง*

**ข้อมูลของบุคลากรผู้ให้ข้อมูล**

ตำแหน่ง ..... ฝ่าย ..... อายุการทำงาน ..... ปี

**คำสั่ง :** พิจารณาแผนจัดการความเสี่ยงในตารางที่ 3 ถึงตารางที่ 25 จากนั้นพิจารณาว่าหลังจากมีแผนจัดการความเสี่ยงต่างๆเหล่านี้จะทำให้ระดับคะแนนของความเสี่ยงในด้านของโอกาสในการเกิดความเสี่ยง (Occurrence; O) และ ความสามารถในการตรวจพบความเสี่ยง (Detection; D) อยู่ในระดับคะแนนเท่าใด โดยกรอกระดับคะแนนของประเด็นความเสี่ยงต่างๆ ในด้านของโอกาสในการเกิดความเสี่ยง (Occurrence; O) ในตารางที่ 26 และความสามารถในการตรวจพบความเสี่ยง (Detection; D) ในตารางที่ 27 โดยใช้เกณฑ์การให้คะแนนในตารางที่ 1-2

***ตารางที่ 1 ระดับโอกาสในการเกิดความเสี่ยง (Occurrence; O)***

| ระดับคะแนน | โอกาสเกิด | ความหมาย |
|---|---|---|
| 1 | น้อยมาก | ■ เกิดได้เฉพาะสถานการณ์ผิดปกติ : ทุกปี |
| 2 | น้อย | ■ สามารถเกิดขึ้นได้น้อยครั้ง : ทุก 6 เดือน |
| 3 | ปานกลาง | ■ อาจเกิดขึ้นได้บ้าง บางโอกาส : ทุกเดือน |
| 4 | มาก | ■ เกิดขึ้นได้เป็นปกติมักเกิดซ้ำบ่อยๆ : ทุกสัปดาห์ |
| 5 | มากที่สุด | ■ ไม่สามารถหลีกเลี่ยงได้ มีโอกาสเกิดสูงมาก : ทุกวัน |

***ตารางที่ 2 ระดับความสามารถในการตรวจพบความเสี่ยง (Detection; D)***

| ระดับคะแนน | ประสิทธิภาพ | ความหมาย |
|---|---|---|
| 1 | สูงที่สุด | ■ สามารถตรวจพบได้แน่นอนเป็นส่วนใหญ่/มีการควบคุมที่ดีมาก |
| 2 | สูง | ■ มีโอกาสสูงในการตรวจพบ/มีการควบคุมที่ดี |
| 3 | ปานกลาง | ■ อาจตรวจพบได้ในบางครั้ง/มีการควบคุมปานกลาง |
| 4 | ต่ำ | ■ มีโอกาสตรวจพบน้อยมาก/มีการควบคุมที่ไม่ค่อยดี |
| 5 | ต่ำมาก | ■ ไม่สามารถตรวจพบได้เลย/ไม่มีการควบคุม |

*ตารางที่ 3 แผนจัดการความเสี่ยงคอมพิวเตอร์ติดไวรัส*

| *คอมพิวเตอร์ติดไวรัส* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| ไวรัสจากไฟล์ข้อมูลทั่วๆไป | Scan ทุกไฟล์ที่ Download มาจากอินเตอร์เน็ต |
| ไวรัสจากฟรีแวร์/แชร์แวร์ | ห้ามใช้โปรแกรมประเภทฟรีแวร์/แชร์แวร์ |
| แผ่นดิสก์,CD, Flash drive มีไวรัส | Scan แผ่นดิสก์,CDและ Flash drive ก่อนการใช้งาน |
| มีช่องโหว่ในระบบเครือข่าย | Update Firewall ให้เป็นปัจจุบันอยู่เสมอ |
| Operating System บกพร่อง | ทำการตรวจสอบชุดปรับปรุง (Patch หรือ Service Pack) ให้เป็นปัจจุบันอยู่เสมอ |
| การโจมตีจาก Hacker | หลีกเลี่ยงการดาว์นโหลดข้อมูลและโปรแกรมต่างๆที่ไม่เกี่ยวข้องกับการทำงานจากเว็บไซท์ |
| | หลีกเลี่ยงการเปิดอีเมล์ที่ไม่ทราบที่มาที่แน่นอน |
| | หลีกเลี่ยงการเปิดไฟล์แนบโดยอัตโนมัติหรือการตั้งค่าในโปรแกรมอีเมล์ให้ดาวน์โหลดไฟล์โดยอัตโนมัติ |
| | Scan ไฟล์หรือโปรแกรมที่ติดมากับ E-mail ก่อนที่จะเปิดอ่านหรือเก็บลงบนฮาร์ดดิสก์ |
| | Block เว็บไซท์ที่ไม่เกี่ยวข้องกับการทำงาน |

***ตารางที่ 4 แผนจัดการความเสี่ยงคอมพิวเตอร์ Restart เอง***

| ***คอมพิวเตอร์ Restart เอง*** | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | เลือกการ์ดจอและแรมให้เหมาะสมกับการใช้งาน |
| อุปกรณ์ระบายความร้อนไม่ทำงาน | กำหนดระยะเวลาในการตรวจสอบสายไฟที่ต่อกับพัดลมระบายความร้อนให้อยู่ในสภาพที่พร้อมใช้งาน |
| | กำหนดระยะเวลาทำความสะอาดพัดลมระบายความร้อนโดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น |
| | จัดสายไฟภายในเครื่องให้เรียบร้อยไม่ขวางทางลมของพัดลม |
| อุปกรณ์ระบายความร้อนไม่เหมาะสม | เลือกชนิดของอุปกรณ์ระบายความร้อนให้เหมาะสมกับการใช้งาน |
| | เลือกขนาดของอุปกรณ์ระบายความร้อนให้เหมาะสมกับการใช้งาน |
| Power Supply ขัดข้อง | กำหนดระยะเวลาในการตรวจสอบ ขั้วต่อภายในระหว่าง Power Supply กับ อุปกรณ์ฮาร์ดแวร์อื่นๆภายในเครื่องให้แน่นอยู่เสมอ |
| | กำหนดระยะเวลาในการทำความสะอาดพัดลมที่ติดอยู่กับ Power Supply โดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น |
| | เลือกใช้ขนาดกำลังไฟฟ้า(ค่าวัตต์) ของ Power Supply ให้เหมาะสมกับฮาร์ดแวร์อื่นๆที่ใช้ |
| Driver มีปัญหา | อัพเดท Driverให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ |
| Hardware มีปัญหา | เมื่อ การ์ดจอ,แรม หรือ Power Supply ชำรุดต้องส่งซ่อมหรือเปลี่ยนใหม่ตามความเหมาะสม |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 |

***ตารางที่ 5 แผนจัดการความเสี่ยงระบบคอมพิวเตอร์ล่ม***

| ***ระบบคอมพิวเตอร์ล่ม*** | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| สัญญาณรบกวน | หลีกเลี่ยงการเดินสาย LAN คู่ไปกับสายสัญญาณอื่นๆ |
| | ติดตั้งอุปกรณ์ป้องกันสัญญาณรบกวนที่มาจากสายส่งและจากอุปกรณ์ต่าง ๆ |
| Under Voltage | ติดตั้งอุปกรณ์ประเภท UPS ป้องกันไฟขาดหรือเกิน |
| Over Voltage | |
| Hardware มีปัญหา | หากมีการเปลี่ยนฮาร์ดแวร์ใหม่ต้องมีการตรวจสอบว่าฮาร์ดแวร์ที่เปลี่ยนใหม่สามารถทำงานร่วมกับฮาร์ดแวร์ที่มีอยู่เดิมได้ |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 |
| คอมพิวเตอร์บางเครื่องในระบบมีปัญหา | วางระบบเครือข่ายแบบใยแมงมุม |
| อุปกรณ์เชื่อมต่อมีปัญหา | เดินสาย LAN ให้เป็นระเบียบเรียบร้อย |
| | กำหนดระยะเวลาในการตรวจสอบสาย LAN ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ |
| | กำหนดระยะเวลาในการตรวจสอบPort เชื่อมต่อให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ |
| ภัยธรรมชาติ | ห้องที่เก็บเครื่องแม่ข่าย(Server) ต้องมั่นคงแข็งแรง |

*ตารางที่ 6 แผนจัดการความเสี่ยงเข้าใช้งานโปรแกรมไม่ได้*

| *เข้าใช้งานโปรแกรมไม่ได้* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| บุคลากรขาดทักษะการใช้งาน | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน |
| โปรแกรมไม่สมบูรณ์ | กำหนดให้ผู้มีความชำนาญงานเป็นผู้ติดตั้งโปรแกรม |
| | กรณีที่เป็นโปรแกรมสำเร็จรูปต้องใช้โปรแกรมที่ถูกลิขสิทธิ์ |
| | กรณีที่เป็นโปรแกรมที่ทางโรงพยาบาลเขียนเองต้องมีการทดสอบการใช้งานก่อนการนำมาใช้งานจริง |
| ขาดโปรแกรมพื้นฐานที่จำเป็น | ติดตั้งโปรแกรมพื้นฐานที่โปรแกรมนั้นๆต้องการให้ครบ |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 |

*ตารางที่ 7 แผนจัดการความเสี่ยงบุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต*

| *บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| บุคลากรขาดความรับผิดชอบ | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ |
| ขาดการควบคุมการใช้งาน | ห้ามติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการทำงา |
| | Block เว็บไซท์ที่ไม่เกี่ยวข้องกับการทำงาน |

*ตารางที่ 8 แผนจัดการความเสี่ยงย้ายหรือถ่ายโอนข้อมูลไม่ได้*

| ***ย้ายหรือถ่ายโอนข้อมูลไม่ได้*** | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| บุคลากรขาดทักษะการใช้งาน | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน |
| การ์ด Lan เสีย | กำหนดระยะเวลาในการตรวจสอบการ์ด Lan ให้อยู่ในสภาพพร้อมใช้งานเสมอ |
| | เมื่อการ์ด Lan เสียต้องมีการซ่อมหรือเปลี่ยนใหม่ตามความเหมาะสม |

*ตารางที่ 9 แผนจัดการความเสี่ยงข้อมูลสูญหาย*

| ***ข้อมูลสูญหาย*** | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| บุคลากรทำงานผิดพลาด | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ |
| ไม่มีการสำรองข้อมูล | ทำการสำรองข้อมูล(Backup) อย่างสม่ำเสมอ |
| ระบบคอมพิวเตอร์ล่ม | ใช้แผนจัดการความเสี่ยงในตารางที่ 3 |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 |

*ตารางที่ 10 แผนจัดการความเสี่ยงเครื่องคอมพิวเตอร์ทำงานช้า*

| *เครื่องคอมพิวเตอร์ทำงานช้า* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | เลือกซีพียูให้เหมาะสมกับการใช้งาน |
| | เลือกRamให้เหมาะสมกับการใช้งาน |
| | เลือกขนาดฮาร์ดดิสก์ให้เหมาะสมกับการใช้งาน |
| มีขยะในฮาร์ดดิสก์มากเกินไป | กำหนดระยะเวลาในการทำ Disk Cleanup |
| | กำหนดระยะเวลาในการทำ Disk Defragmenter |
| | ลบ Temporary Files อย่างสม่ำเสมอ |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 |

*ตารางที่ 11 แผนจัดการความเสี่ยงโปรแกรมทำงานผิดพลาด*

| *โปรแกรมทำงานผิดพลาด* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| โปรแกรมไม่สมบูรณ์ | ต้องให้ผู้มีความชำนาญงานเป็นผู้ติดตั้งโปรแกรม |
| | กรณีที่เป็นโปรแกรมสำเร็จรูปต้องใช้โปรแกรมที่ถูกลิขสิทธิ์ |
| | กรณีที่เป็นโปรแกรมที่ทางโรงพยาบาลเขียนเองต้องมีการทดสอบการใช้งานก่อนการนำมาใช้งานจริง |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 |
| Hardware มีปัญหา | กำหนดระยะเวลาในการตรวจสอบHardware(Input/Output) ให้อยู่ในสภาพที่พร้อมใช้งาน |

*ตารางที่ 12 แผนจัดการความเสี่ยงบุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น*

| *บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| บุคลากรขาดทักษะการใช้งาน | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน |
| โปรแกรม Edit Dataไม่ได้หลังบันทึก | เขียนโปรแกรมให้สามารถ Edit Data ได้ตามลักษณะการใช้งาน |

*ตารางที่ 13 แผนจัดการความเสี่ยงหน้าจอค้างสีฟ้า (Blue Screen of Death)*

| *หน้าจอค้างสีฟ้า (Blue Screen of Death)* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| Hardware มีปัญหา | กำหนดระยะเวลาในการตรวจสอบ Hardware ทุกชิ้นส่วนให้อยู่ในสภาพพร้อมใช้งานเสมอ |
| คอมพิวเตอร์ติดไวรัส | ใช้แผนจัดการความเสี่ยงในตารางที่ 1 |
| Driver มีปัญหา | อัพเดท Driverให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ |
| คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน |

***ตารางที่ 14 แผนจัดการความเสี่ยงใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์***

| ***ใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์*** | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| บุคลากรนำโปรแกรมมาลงเอง | ห้ามบุคลากรนำโปรแกรมมาลงเองโดยไม่ได้รับอนุญาต |
| บุคลากรโหลดโปรแกรมละเมิดลิขสิทธิ์จากอินเตอร์เน็ต | ห้ามบุคลากรโหลดโปรแกรมละเมิดลิขสิทธิ์จากอินเตอร์เน็ต |
| ละเมิด Site/Network Licens | ต้องศึกษา Site/Network Licens ของโปรแกรมที่จะนำมาใช้ ให้ละเอียดก่อนนำโปรแกรมนั้นๆมาใช้งาน |

***ตารางที่ 15 แผนจัดการความเสี่ยงบุคคลากรคีย์ข้อมูลผิด***

| ***บุคคลากรคีย์ข้อมูลผิด*** | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| บุคลากรทำงานผิดพลาด | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ |
| บุคลากรมีปัญหาการได้ยิน | มีการตรวจสุขภาพให้กับบุคลากรผู้ใช้งานคอมพิวเตอร์ทุกปี |
| บุคลากรมีปัญหาด้านสายตา | |
| ลายมืออ่านยาก | ออกแบบแบบฟอร์มต่างๆที่ต้องใช้ในโรงพยาบาลให้เป็นแบบฟอร์มที่ต้องใช้ลายมือเขียนน้อยที่สุด |

*ตารางที่ 16 แผนจัดการความเสี่ยงสั่งพิมพ์ (Print) ข้อมูลไม่ได้*

| *สั่งพิมพ์ (Print) ข้อมูลไม่ได้* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| บุคลากรขาดทักษะการใช้งาน | จัดทำคู่มือการใช้งานเบื้องต้นโดยมีรายละเอียด<br>1. วิธีการสั่งพิมพ์<br>2. วิธีตรวจสอบสถานะของ Printer ว่าพร้อมใช้งานหรือไม่ |
| PRINTER มีปัญหา | ตรวจสอบอุปกรณ์ต่อเชื่อมต่างๆระหว่าง Printer กับ คอมพิวเตอร์ให้อยู่ในสภาพพร้อมใช้งาน |
| โปรแกรมทำงานผิดพลาด | ใช้แผนจัดการความเสี่ยงในตารางที่ 9 |

*ตารางที่ 17 แผนจัดการความเสี่ยงขาดบุคลากรในบางตำแหน่งที่ควรจะมี*

| *ขาดบุคลากรในบางตำแหน่งที่ควรจะมี* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| ภาระ/ลักษณะงานเพิ่ม | มีการกำหนดระยะเวลาในการประชุมหารือร่วมกันของทุกฝ่ายที่เกี่ยวข้องเพื่อประเมินภาระงานและลักษณะงาน เพื่อสรรหาบุคลากรให้เหมาะสมกับงานและเพียงพอต่อภาระงาน |
| ไม่มีการประเมินภาระ/ลักษณะงาน | |

*ตารางที่ 18 แผนจัดการความเสี่ยงบุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย*

| *บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| ภาระงานมาก | มีการส่งเสริมและจัดสรรเวลาเพื่อให้บุคลากรผู้เกี่ยวข้องเข้าอบรมหลักสูตรต่างๆด้าน IT ตามความเหมาะสม |
| องค์กรไม่ส่งเสริม | |

*ตารางที่ 19 แผนจัดการความเสี่ยงแก้ไขโปรแกรมไม่ทัน*

| *แก้ไขโปรแกรมไม่ทัน* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| โปรแกรมขาดความยืดหยุ่น | มีการออกแบบและเขียนโปรแกรมให้ยืดหยุ่นและปรับเปลี่ยนได้ง่าย |
| ขาดการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง | มีการติดต่อสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องให้รวดเร็วเพื่อให้ทันต่อการเปลี่ยนแปลง |
| จัดทำโปรแกรม Specไม่ครบถ้วน | มีการสำรวจข้อมูลให้ละเอียดก่อนจัดทำโปรแกรม |

*ตารางที่ 20 แผนจัดการความเสี่ยงไม่มีการ Update ข้อมูล*

| *ไม่มีการ Update ข้อมูล* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| ขาดการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง | มีการติดต่อสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องให้รวดเร็วเพื่อให้ทันต่อการเปลี่ยนแปลง |
| บุคลากรทำงานล่าช้า | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ |

*ตารางที่ 21 แผนจัดการความเสี่ยงค้นหา (Search) ข้อมูลที่ต้องการใช้ในระบบไม่พบ*

| *ค้นหา (Search) ข้อมูลที่ต้องการใช้ในระบบไม่พบ* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| บุคลากรขาดทักษะการใช้งาน | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน |
| ช่องทางการค้นหาซับซ้อนเกินไป | กำหนดช่องทางการเข้าถึงข้อมูลให้ง่ายต่อการเข้าถึงข้อมูล |
| ไม่ได้บันทึกข้อมูลไว้ | กำหนดให้ชัดเจนว่าข้อมูลใดต้องทำการบันทึกไว้ |
| ข้อมูลสูญหาย | ใช้แผนจัดการความเสี่ยงในตารางที่ 7 |

*ตารางที่ 22 แผนจัดการความเสี่ยงบุคคลากรใช้งานโปรแกรมไม่เป็น*

| *บุคคลากรใช้งานโปรแกรมไม่เป็น* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| บุคลากรขาดทักษะการใช้งาน | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน |
| เป็นโปรแกรมเฉพาะทาง | |
| เปลี่ยนโปรแกรมหรือเวอร์ชัน | |

*ตารางที่ 23 แผนจัดการความเสี่ยงจำนวน Computer ไม่เพียงพอต่อการใช้งาน*

| *จำนวน Computer ไม่เพียงพอต่อการใช้งาน* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| ไม่มีการสำรวจความต้องการ | มีการสำรวจความต้องการก่อนจัดหาคอมพิวเตอร์ในแต่ละครั้ง |
| อยู่ระหว่างการส่งซ่อม | จัดให้มีเครื่องคอมพิวเตอร์สำรองกรณีที่เครื่องหลักถูกส่งซ่อม |

*ตารางที่ 24 แผนจัดการความเสี่ยง Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน*

| *Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน* | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| สำรวจข้อมูลไม่ละเอียดก่อนเขียนโปรแกรม | ก่อนจัดทำโปรแกรมต้องมีการสำรวจข้อมูลการใช้งานให้ละเอียด |
| ไม่มีการทดสอบใช้งานก่อนใช้จริง | เมื่อจัดทำโปรแกรมเสร็จแล้วต้องมีการทดสอบใช้งานก่อนที่จะนำโปรแกรมนั้นไปใช้งานจริง |

*ตารางที่ 25 แผนจัดการความเสี่ยง CD-ROM ใช้งานไม่ได้*

| ***CD-ROM ใช้งานไม่ได้*** | |
|---|---|
| ***สาเหตุพื้นฐาน*** | ***แผนจัดการความเสี่ยง*** |
| Power Supply ขัดข้อง | กำหนดระยะเวลาในการตรวจสอบ ขั้วต่อภายในระหว่าง Power Supply กับ CD-ROM ให้อยู่ในสภาพพร้อมใช้งานเสมอ |
| | กำหนดระยะเวลาในการทำความสะอาดพัดลมที่ติดอยู่กับ Power Supply โดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น |
| ตัว CD-ROM เสีย | เปลี่ยน CD-ROM ใหม่ |
| สายเคเบิล(IDE Cable) หลุด | กำหนดระยะเวลาในการตรวจสอบ สายเคเบิล(IDE Cable) และสายไฟ(Power Cable) ให้อยู่ในสภาพพร้อมใช้งานเสมอ |
| สายไฟ(Power Cable) หลุด | |

***ตารางที่ 26 ระดับโอกาสในการเกิดความเสี่ยง (Occurrence; O)***

| ลำดับที่ | ประเด็นความเสี่ยง | คะแนน |
|---|---|---|
| **1** | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | |
| **2** | บุคลากรใช้งานโปรแกรมไม่เป็น | |
| **3** | บุคลากรคีย์ข้อมูลผิด | |
| **4** | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | |
| **5** | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | |
| **6** | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | |
| **7** | เครื่องคอมพิวเตอร์ติดไวรัส | |
| **8** | ไม่มีการUpdateข้อมูล | |
| **9** | ข้อมูลสูญหาย | |
| **10** | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | |
| **11** | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | |
| **12** | แก้ไขโปรแกรมไม่ทัน | |
| **13** | ระบบคอมพิวเตอร์ล่ม | |
| **14** | เครื่องคอมพิวเตอร์ทำงานช้า | |
| **15** | โปรแกรมทำงานผิดพลาด | |
| **16** | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | |
| **17** | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | |
| **18** | เข้าใช้งานโปรแกรมไม่ได้ | |
| **19** | คอมพิวเตอร์ Restart เอง | |
| **20** | CD-ROM ใช้งานไม่ได้ | |
| **21** | หน้าจอค้างสีฟ้า (Blue Screen of Death) | |
| **22** | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | |
| **23** | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | |

***ตารางที่ 27 ระดับความสามารถในการตรวจพบความเสี่ยง (Detection; D)***

| ลำดับที่ | ประเด็นความเสี่ยง | คะแนน |
|---|---|---|
| **1** | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | |
| **2** | บุคลากรใช้งานโปรแกรมไม่เป็น | |
| **3** | บุคลากรคีย์ข้อมูลผิด | |
| **4** | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | |
| **5** | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | |
| **6** | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | |
| **7** | เครื่องคอมพิวเตอร์ติดไวรัส | |
| **8** | ไม่มีการUpdateข้อมูล | |
| **9** | ข้อมูลสูญหาย | |
| **10** | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | |
| **11** | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | |
| **12** | แก้ไขโปรแกรมไม่ทัน | |
| **13** | ระบบคอมพิวเตอร์ล่ม | |
| **14** | เครื่องคอมพิวเตอร์ทำงานช้า | |
| **15** | โปรแกรมทำงานผิดพลาด | |
| **16** | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | |
| **17** | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | |
| **18** | เข้าใช้งานโปรแกรมไม่ได้ | |
| **19** | คอมพิวเตอร์ Restart เอง | |
| **20** | CD-ROM ใช้งานไม่ได้ | |
| **21** | หน้าจอค้างสีฟ้า (Blue Screen of Death) | |
| **22** | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | |
| **23** | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | |

**ข้อเสนอแนะเพิ่มเติม**

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....



*** ขอบพระคุณที่ให้ความร่วมมือในการอนุเคราะห์ข้อมูล ***

# ภาคผนวก ข
# ตัวอย่างผลกระทบของประเด็นความเสี่ยง 23 ประเด็นความเสี่ยง

**ตัวอย่างผลกระทบของประเด็นความเสี่ยง 23 ประเด็นความเสี่ยง**

ตารางแสดงตัวอย่างผลกระทบของประเด็นความเสี่ยง 23 ประเด็นความเสี่ยง

| ลำดับที่ | ประเด็นความเสี่ยง | ตัวอย่างผลกระทบ |
|---|---|---|
| 1 | เครื่องคอมพิวเตอร์ติดไวรัส | อาจส่งผลกระทบในหลายๆด้าน เช่น ทำให้ระบบคอมพิวเตอร์ล่ม, ทำให้คอมพิวเตอร์ restart เอง, ทำให้เข้าใช้งานโปรแกรมไม่ได้, ทำให้โปรแกรมทำงานผิดพลาด, ทำให้ข้อมูลสูญหาย, ทำให้เครื่องคอมพิวเตอร์ทำงานช้า เป็นต้น และอาจมีอีกหลายอาการที่อาจเกิดขึ้นได้ขึ้นอยู่กับชนิดของไวรัสที่อาจเกิดไวรัสชนิดใหม่ขึ้นมาในอนาคต |
| 2 | คอมพิวเตอร์ Restart เอง | - หากเกิดกับคอมพิวเตอร์ระบบงานบริการผู้ป่วย จะส่งผลให้ต้องหยุดบริการผู้ป่วย ณ ขณะนั้น ทำให้เกิดการรอของผู้ป่วย เช่น หากเกิดกับเครื่องที่ใช้จ่ายยาก็ต้องหยุดให้บริการผู้ป่วยขณะนั้นทำให้เกิดการรอของผู้ป่วย เป็นต้น<br>- หากเกิดกับระบบงาน Back Office จะทำให้บุคลากรเสียเวลาการทำงาน และในกรณีที่แย่ที่สุดอาจต้องเริ่มต้นงานใหม่ทั้งหมดในกรณีที่โปรแกรมที่กำลังใช้อยู่ก่อนที่เครื่องจะ Restart เอง ไม่ได้มีการบันทึกงานไว้โดยอัตโนมัติ<br>และส่วนใหญ่การที่เกิดเหตุการณ์ คอมพิวเตอร์ Restart เอง จะไม่เกิดขึ้นแค่ครั้งเดียวถ้าหากมีการใช้งานอย่างต่อเนื่อง ส่วนจะเกิดขึ้นเป็นความถี่เท่าไร ขึ้นอยู่กับสาเหตุพื้นฐานของการเกิด |
| 3 | ระบบคอมพิวเตอร์ล่ม | จะส่งผลให้ระบบนั้นๆใช้งานไม่ได้เลยแม้แต่เครื่องเดียว(แต่คอมพิวเตอร์ยังใช้งานในส่วนอื่นๆที่ไม่เกี่ยวข้องกับระบบนั้นๆได้) เช่น หากเกิดกับระบบหอผู้ป่วย จะส่งผลให้ย้ายข้อมูลผู้ป่วยไม่ได้ในกรณีที่ผู้ป่วยต้องย้ายตึก และการที่ระบบนั้นๆล่มก็จะส่งผลให้ระบบนั้นๆเชื่อมต่อกับระบบอื่นๆไม่ได้อีกด้วย เช่นหากระบบหอผู้ป่วยล่มก็จะทำให้ไม่สามารถเชื่อมต่อกับระบบจ่ายยาและเวชภัณฑ์ได้ ซึ่งจะส่งผลกระทบต่อการเบิกจ่ายยาและเวชภัณฑ์ กับผู้ป่วยที่อยู่ในหอผู้ป่วยนั้นๆด้วย เป็นต้น |

ตารางแสดงตัวอย่างผลกระทบของประเด็นความเสี่ยง 23 ประเด็นความเสี่ยง(ต่อ)

| ลำดับที่ | ประเด็นความเสี่ยง | ตัวอย่างผลกระทบ |
|---|---|---|
| 4 | เข้าใช้งานโปรแกรมไม่ได้ | - ในกรณีที่เกิดกับระบบงานบริการผู้ป่วย จะส่งผลให้ต้องหยุดให้บริการผู้ป่วยในกิจกรรมนั้นๆจนกว่าจะเข้าใช้โปรแกรมได้ เช่น เข้าใช้งานโปรแกรมที่ใช้นัดหมายผู้ป่วยไม่ได้ จะส่งผลให้พิมพ์ใบนัดหมายผู้ป่วยไม่ได้ ผู้ป่วยต้องเสียเวลารอจนกว่าจะเข้าใช้งานโปรแกรมได้ เป็นต้น<br>- ในกรณีที่เกิดกับระบบงาน Back Office จะส่งผลให้บุคลากรทำงานที่ต้องใช้โปรแกรมนั้นๆไม่ได้ |
| 5 | บุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต | ทำให้งานเสร็จช้ากว่าที่ควรจะเป็น โดยเฉพาะงานที่ไม่ได้มีการกำหนดเวลาในการส่งที่ชัดเจน เช่น การเดินเอกสารต่างๆในโรงพยาบาลอาจใช้เวลานานกว่าที่ควรจะเป็นหากบุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต เป็นต้น (มักเกิดกับระบบงาน Back Office) |
| 6 | ย้ายหรือถ่ายโอนข้อมูลไม่ได้ | - ในกรณีที่เกิดกับระบบงานบริการผู้ป่วย เช่น จำหน่ายข้อมูลผู้ป่วยที่เสียชีวิตออกจากระบบไม่ได้ส่งผลให้ข้อมูลในระบบกับความเป็นจริงไม่ตรงกันต้องเสียเวลากลับมาแก้ไข หรือย้ายข้อมูลของผู้ป่วยจากตึกหนึ่งไปยังอีกตึกหนึ่งไม่ได้จะส่งผลให้ข้อมูลในระบบกับความเป็นจริงไม่ตรงกันและส่งผลให้มีปัญหาในการจ่ายยาและเวชภัณฑ์ให้กับผู้ป่วย เป็นต้น<br>- ในกรณีที่เกิดกับระบบงาน Back Office เช่น การเดินเรื่องต่างๆในโรงพยาบาลโดยส่งข้อมูลจากอีกฝ่ายงานหนึ่งไปยังอีกฝ่ายงานหนึ่งทางระบบคอมพิวเตอร์ไม่ได้ อาจทำให้การเดินเรื่องนั้นๆใช้เวลานานกว่าที่ควรจะเป็นและต้องเสียเวลากลับมาตามเรื่องใหม่ ยกตัวอย่างเช่น มีผู้ป่วยหรือญาติผู้ป่วยต้องการร้องเรียนการบริการของทางโรงพยาบาลต่อผู้อำนวยการโรงพยาบาล โดยส่งผ่านทางฝ่ายสารบรรณ โดยฝ่ายสารบรรณจะต้องส่งข้อมูลการร้องเรียนผ่านทางระบบคอมพิวเตอร์ไปยังฝ่ายเลขานุการและหากการย้ายถ่ายหรือถ่ายโอนข้อมูลครั้งนี้ไม่สำเร็จ(โดยที่ฝ่ายสารบรรณเข้าใจว่าข้อมูลถูกส่งไปแล้ว) เมื่อผู้ร้องเรียนมาตามเรื่องก็จะทำให้เสียเวลาในการตามเรื่องและอาจต้องเสียเวลาในการเดินเรื่องใหม่ |

ตารางแสดงตัวอย่างผลกระทบของประเด็นความเสี่ยง 23 ประเด็นความเสี่ยง(ต่อ)

| ลำดับที่ | ประเด็นความเสี่ยง | ตัวอย่างผลกระทบ |
|---|---|---|
| 7 | ข้อมูลสูญหาย | เช่น ข้อมูลการจ่ายยาให้ผู้ป่วยสูญหายจะส่งผลให้การคิดค่ายาผิดพลาดจากความเป็นจริงต้องเสียเวลากลับมาแก้ไขใหม่ หรือข้อมูลเวชระเบียนผู้ป่วยสูญหายจะส่งกระทบต่อการรักษาผู้ป่วยในกรณีที่ต้องการใช้ข้อมูลในเวชระเบียนมาประกอบการรักษา และในบางครั้งอาจส่งผลกระทบทางด้านกฎหมายด้วยเนื่องจากข้อมูลเวชระเบียนสามารถนำไปเป็นหลักฐานทางกฎหมายได้(ในกรณีที่ต้องการใช้) เป็นต้น |
| 8 | เครื่องคอมพิวเตอร์ทำงานช้า | ทำให้ใช้เวลาในการทำงานมากเกินกว่าที่ควรจะเป็นเนื่องจากคอมพิวเตอร์ใช้เวลานานในการเข้าหน้าจอหลัก ใช้เวลานานในการเข้าสู่โปรแกรมการใช้งาน และใช้เวลานานในการประมวลผลแต่ละครั้ง |
| 9 | โปรแกรมทำงานผิดพลาด | เช่น โปรแกรมทำงานผิดพลาดทำให้ข้อมูลในระบบกับข้อมูลที่พิมพ์ออกมาไม่ตรงกัน ยกตัวอย่างเช่น พิมพ์ใบเสร็จรับเงินแต่ข้อมูลออกมาไม่ครบโดยที่หน้าจอแสดงข้อมูลครบซึ่งจะส่งผลให้ต้องเสียเวลาในการแก้ไขให้ถูกต้อง หรือใบนัดหมายที่พิมพ์ให้ผู้ป่วยไม่ตรงกับข้อมูลในระบบจะส่งผลให้ผู้ป่วยเข้าใจคลาดเคลื่อนจากความเป็นจริง อาจจะเป็นในเรื่องของวันและเวลาที่นัดทำให้ผู้ป่วยมาผิดวันและเวลา เป็นต้น |
| 10 | บุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น | ทำให้บุคลากรจากฝ่ายเทคโนโลยีสารสนเทศต้องไปทำการยกเลิกหรือแก้ไขข้อมูลต่างๆให้ ซึ่งทำให้เสียเวลาในการทำงานที่เกี่ยวข้องกับหน้าที่รับผิดชอบหลัก |
| 11 | หน้าจอค้างสีฟ้า (Blue Screen of Death) | ทำให้เข้าสู่ระบบการใช้งานไม่ได้ (ระยะเวลามากน้อยขึ้นอยู่กับสาเหตุพื้นฐานของการเกิด) |
| 12 | ใช้ Software ละเมิดลิขสิทธิ์ โดยรู้เท่าไม่ถึงการณ์ | ผิดกฎหมาย อาจทำให้เกิดการฟ้องร้องเสียชื่อเสียงขององค์กร |
| 13 | บุคลากรคีย์ข้อมูลผิด | เช่น บุคลากรคีย์รหัสค่ารักษาพยาบาลหรือรหัสค่ายาผิด ส่งผลให้การคิดค่ารักษาพยาบาลและค่ายาคลาดเคลื่อนจากความเป็นจริง ต้องเสียเวลากลับมาแก้ไขใหม่ เป็นต้น |

ตารางแสดงตัวอย่างผลกระทบของประเด็นความเสี่ยง 23 ประเด็นความเสี่ยง(ต่อ)

| ลำดับที่ | ประเด็นความเสี่ยง | ตัวอย่างผลกระทบ |
|---|---|---|
| 14 | สั่งพิมพ์(Print)ข้อมูลไม่ได้ | - ในกรณีที่เกิดกับระบบงานบริการผู้ป่วย จะส่งผลทำให้เกิดการรอของผู้ป่วยนานกว่าที่ควรจะเป็น เช่น สั่งพิมพ์สติ๊กเกอร์ฉลากยาไม่ได้ สั่งพิมพ์ใบเสร็จรับเงินไม่ได้ สั่งพิมพ์ใบนัดหมายคนไข้ไม่ได้ สั่งพิมพ์บัตรใหม่ของผู้ป่วยไม่ได้ เป็นต้น<br>- ในกรณีที่เกิดกับระบบงาน Back Office จะส่งผลให้บุคลากรเสียเวลาในการทำงาน (ระยะเวลามากน้อย ขึ้นอยู่กับข้อมูลที่ต้องการพิมพ์จะนำไปใช้ทำอะไร และใช้เมื่อไร) |
| 15 | ขาดบุคลากรในบางตำแหน่งที่ควรจะมี | ทำให้บุคลากรต้องไปปฏิบัติงานในส่วนที่ไม่ใช่หน้าที่หลักของตนเองอยู่บ่อยครั้ง ทำให้เสียเวลาในการทำงานหลักของตนเอง เช่น บุคลากรในฝ่ายเทคโนโลยีสารสนเทศผู้ที่มีหน้าที่ วิเคราะห์ออกแบบ และพัฒนาโปรแกรม แต่เมื่อมีการแจ้งปัญหาการใช้งานอินเตอร์เน็ตไม่ได้เข้ามาจากฝ่ายงานอื่นๆ บุคลากรคนนี้ต้องไปทำการแก้ไขให้เนื่องจากไม่มีผู้รับผิดชอบหลักโดยตรง เป็นต้น |
| 16 | บุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย | ทำให้บุคลากรมีวิธีการทำงานเกี่ยวกับการใช้คอมพิวเตอร์และอินเตอร์เน็ตที่ล้าสมัยเมื่อเทียบกับเทคโนโลยีที่เปลี่ยนไป เพราะในบางครั้งเทคโนโลยีที่เปลี่ยนไปสามารถช่วยให้การทำงานในงานเดิมได้เร็วขึ้น แต่หากบุคลากรไม่มีโอกาสได้ Update เทคโนโลยีใหม่ๆ ก็จะไม่ทราบวิธีการทำงานที่ทำให้ทำงานได้เร็วขึ้น และยังคงใช้วิธีการทำงานแบบเดิมซึ่งก็ไม่ได้ทำให้ทำงานได้ช้าลง แต่การที่ทำงานโดยใช้วิธีแบบเดิมทั้งๆที่มีวิธีอื่นๆที่ช่วยให้ทำงานได้เร็วขึ้นแต่บุคลากรไม่ทราบเพราะไม่มีโอกาสได้Updateเทคโนโลยีใหม่ๆก็ถือเป็นการเสียเวลางานอย่างหนึ่ง |
| 17 | แก้ไขโปรแกรมไม่ทัน | เนื่องจากการแก้ไขโปรแกรมจะทำการแก้ไขใน 2 กรณี คือ<br>1. โปรแกรมใช้งานยากหรือใช้แล้วมีปัญหาขัดข้องบ่อยครั้ง<br>2. มีการเปลี่ยนแปลงต่างๆเกิดขึ้นจึงต้องแก้ไขโปรแกรม<br>ดังนั้นผลกระทบจะแบ่งออกเป็น 2 กรณี คือ<br>1. ต้องใช้โปรแกรมที่ใช้งานยากและใช้แล้วมีปัญหาต่อไปจนกว่าจะถูกแก้ไขซึ่งส่งผลให้เสียเวลาในการทำงาน<br>2. ต้องเสียเวลากลับมาแก้ไขการทำงานที่เกิดจากการใช้โปรแกรม |

ตารางแสดงตัวอย่างผลกระทบของประเด็นความเสี่ยง 23 ประเด็นความเสี่ยง(ต่อ)

| ลำดับที่ | ประเด็นความเสี่ยง | ตัวอย่างผลกระทบ |
|---|---|---|
| | | ก่อนที่จะมีการแก้ไข เช่น ทางโรงพยาบาลมีนโยบายในการบันทึกข้อมูลผู้ป่วยเพิ่มเติม ยกตัวอย่างเช่น ทางโรงพยาบาลต้องการให้บันทึกข้อมูลญาติผู้ป่วยที่สามารถติดต่อได้ในกรณีที่ติดต่อกับผู้ป่วยไม่ได้ แต่แก้ไขโปรแกรมไม่ทันทำให้บันทึกข้อมูลส่วนที่เพิ่มเข้ามาลงไปในระบบไม่ได้ ต้องย้อนกลับมาบันทึกเพิ่มเติมหลังจากแก้ไขโปรแกรมเสร็จเรียบร้อยแล้ว |
| 18 | ไม่มีการUpdateข้อมูล | เช่น สิทธิการรักษาพยาบาลของผู้ป่วยตามประกาศของสำนักงานหลักประกันสุขภาพแห่งชาติ(สปสช.) มีการเปลี่ยนแปลง แต่ทางโรงพยาบาลยังไม่มีการ Update ข้อมูล โดยทางโรงพยาบาลยังใช้สิทธิการรักษาพยาบาลเดิมในการดำเนินงาน เมื่อเวลาผ่านไปหลังจากมีการ Update ข้อมูล แล้วจะต้องกลับมาแก้ไขข้อมูลให้ตรงกับความเป็นจริงโดยเริ่มแก้ไขข้อมูลจากวันที่ สปสช. ประกาศใช้สิทธิการรักษาพยาบาลของผู้ป่วย ซึ่งส่งผลให้เสียเวลาในการทำงาน |
| 19 | ค้นหา(Search)ข้อมูลที่ต้องการใช้ในระบบไม่พบ | ส่งผลให้บุคลากรต้องทำการหาข้อมูลจากแหล่งอื่น เช่น จากผู้มีส่วนเกี่ยวข้อง หรือเอกสารที่เกี่ยวข้อง แทนที่จะสามารถค้นหาข้อมูลได้ในระบบ หรือในกรณีที่เลวร้ายที่สุดอาจหาข้อมูลนั้นไม่ได้เลย |
| 20 | บุคลากรใช้งานโปรแกรมไม่เป็น | ทำให้บุคลากรไม่สามารถที่จะทำงานที่เกี่ยวข้องกับการใช้โปรแกรมนั้นๆได้ |
| 21 | จำนวน Computer ไม่เพียงพอต่อการใช้งาน | จำนวน Computer ไม่เพียงพอต่อการใช้งาน |
| 22 | Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน | บุคลากรผู้ใช้งานไม่ได้รับความสะดวกเท่าที่ควรในการใช้งานโปรแกรมนั้นๆ |
| 23 | CD-ROM ใช้งานไม่ได้ | เปิดข้อมูลจากแผ่น CD ไม่ได้, บันทึกข้อมูลลงแผ่น CD ไม่ได้ และ ติดตั้งโปรแกรมไม่ได้ |

# ภาคผนวก ค

## การสร้างแผนจัดการความเสี่ยงของ 23 ประเด็นความเสี่ยงโดยใช้แนวทางทั้ง 4 แนวทาง

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | **Take-ยอมรับ** | **Treat-ลด/ควบคุม** | **Terminate-หลีกเลี่ยง** | **Transfer-กระจาย/ถ่ายโอน** |
| ไวรัสจากไฟล์ข้อมูลทั่วๆไป | | Scan ทุกไฟล์ที่ Download มาจากอินเตอร์เน็ต | | |
| ไวรัสจากฟรีแวร์/แชร์แวร์ | | | ห้ามใช้โปรแกรมประเภทฟรีแวร์/แชร์แวร์ | |
| แผ่นดิสก์,CD, Flash drive มีไวรัส | | Scan แผ่นดิสก์,CDและ Flash drive ก่อนการใช้งาน | | |
| มีช่องโหว่ในระบบเครือข่าย | | Update Firewall ให้เป็นปัจจุบันอยู่เสมอ | | |
| Operating System บกพร่อง | | ทำการตรวจสอบชุดปรับปรุง(Patch หรือ Service Pack) ให้เป็นปัจจุบันอยู่เสมอ | | |
| การโจมตีจาก Hacker | | - Scan ไฟล์หรือโปรแกรมที่ติดมากับ E-mail ก่อนที่จะเปิดอ่านหรือเก็บลงบนฮาร์ดดิสก์<br>- Block เว็บไซท์ที่ไม่เกี่ยวข้องกับการทำงาน | - หลีกเลี่ยงการดาวน์โหลดข้อมูลและโปรแกรมต่างๆที่ไม่เกี่ยวข้องกับการทำงานจากเว็บไซท์<br>- หลีกเลี่ยงการเปิดอีเมล์ที่ไม่ทราบที่มาที่แน่นอน | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส (ต่อ)**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| การโจมตีจาก Hacker (ต่อ) | | | - หลีกเลี่ยงการเปิดไฟล์แนบโดยอัตโนมัติหรือการตั้งค่าในโปรแกรมอีเมล์ให้ดาวน์โหลดไฟล์โดยอัตโนมัติ | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงคอมพิวเตอร์ Restart เอง**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | | เลือกการ์ดจอและแรมให้เหมาะสมกับการใช้งาน | | |
| อุปกรณ์ระบายความร้อนไม่ทำงาน | | - กำหนดระยะเวลาในกาตรวจสอบสายไฟที่ต่อกับพัดลมระบายความร้อนให้อยู่ในสภาพที่พร้อมใช้งาน<br>- กำหนดระยะเวลาทำความสะอาดพัดลมระบายความร้อนโดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงคอมพิวเตอร์ Restart เอง (ต่อ)**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | **Take-ยอมรับ** | **Treat-ลด/ควบคุม** | **Terminate-หลีกเลี่ยง** | **Transfer-กระจาย/ถ่ายโอน** |
| อุปกรณ์ระบายความร้อนไม่ทำงาน (ต่อ) | | - จัดสายไฟภายในเครื่องให้เรียบร้อยไม่ขวางทางลมของพัดลม | | |
| อุปกรณ์ระบายความร้อนไม่เหมาะสม | | - เลือกชนิดของอุปกรณ์ระบายความร้อนให้เหมาะสมกับการใช้งาน<br>- เลือกขนาดของอุปกรณ์ระบายความร้อนให้เหมาะสมกับการใช้งาน | | |
| Power Supply ขัดข้อง | | - กำหนดระยะเวลาในการตรวจสอบขั้วต่อภายในระหว่าง Power Supply กับอุปกรณ์ฮาร์ดแวร์อื่นๆภายในเครื่องให้แน่นอยู่เสมอ<br>- กำหนดระยะเวลาในการทำความสะอาดพัดลมที่ติดอยู่กับ Power Supply โดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น<br>- เลือกใช้ขนาดกำลังไฟฟ้า(ค่าวัตต์)ของ Power Supply ให้เหมาะสมกับฮาร์ดแวร์อื่นๆที่ใช้ | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงคอมพิวเตอร์ Restart เอง (ต่อ)**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | **Take-ยอมรับ** | **Treat-ลด/ควบคุม** | **Terminate-หลีกเลี่ยง** | **Transfer-กระจาย/ถ่ายโอน** |
| Driver มีปัญหา | | อัพเดท Driverให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ | | |
| Hardware มีปัญหา | | | เมื่อ การ์ดจอ,แรม หรือ Power Supply ชำรุดต้องส่งซ่อมหรือเปลี่ยนใหม่ตามความเหมาะสม | |
| คอมพิวเตอร์ติดไวรัส | * ใช้แผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงระบบคอมพิวเตอร์ล่ม**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | **Take-ยอมรับ** | **Treat-ลด/ควบคุม** | **Terminate-หลีกเลี่ยง** | **Transfer-กระจาย/ถ่ายโอน** |
| สัญญาณรบกวน | | ติดตั้งอุปกรณ์ป้องกันสัญญาณรบกวนที่มาจากสายส่งและจากอุปกรณ์ต่าง ๆ | หลีกเลี่ยงการเดินสาย LAN คู่ไปกับสายสัญญาณอื่นๆ | |
| Under Voltage | | ติดตั้งอุปกรณ์ประเภท UPS ป้องกันไฟขาดหรือเกิน | | |
| Over Voltage | | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงระบบคอมพิวเตอร์ล่ม (ต่อ)**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | **Take-ยอมรับ** | **Treat-ลด/ควบคุม** | **Terminate-หลีกเลี่ยง** | **Transfer-กระจาย/ถ่ายโอน** |
| Hardware มีปัญหา | | หากมีการเปลี่ยนฮาร์ดแวร์ใหม่ต้องมีการตรวจสอบว่าฮาร์ดแวร์ที่เปลี่ยนใหม่สามารถทำงานร่วมกับฮาร์ดแวร์ที่มีอยู่เดิมได้ | | |
| คอมพิวเตอร์ติดไวรัส | * ใช้แผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส | | | |
| คอมพิวเตอร์บางเครื่องในระบบมีปัญหา | | วางระบบเครือข่ายแบบใยแมงมุม | | |
| อุปกรณ์เชื่อมต่อมีปัญหา | | - เดินสาย LAN ให้เป็นระเบียบเรียบร้อย<br>- กำหนดระยะเวลาในการตรวจสอบสาย LAN ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ<br>- กำหนดระยะเวลาในการตรวจสอบ Port เชื่อมต่อให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ | | |
| ภัยธรรมชาติ | | ห้องที่เก็บเครื่องแม่ข่าย(Server) ต้องมั่นคงแข็งแรง | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงเข้าใช้งานโปรแกรมไม่ได้**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | **Take-ยอมรับ** | **Treat-ลด/ควบคุม** | **Terminate-หลีกเลี่ยง** | **Transfer-กระจาย/ถ่ายโอน** |
| บุคลากรขาดทักษะการใช้งาน | | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | | |
| โปรแกรมไม่สมบูรณ์ | | - กำหนดให้ผู้มีความชำนาญงานเป็นผู้ติดตั้งโปรแกรม<br>- กรณีที่เป็นโปรแกรมสำเร็จรูปต้องใช้โปรแกรมที่ถูกลิขสิทธิ์<br>- กรณีที่เป็นโปรแกรมที่ทางโรงพยาบาลเขียนเองต้องมีการทดสอบการใช้งานก่อนการนำมาใช้งานจริง | | |
| ขาดโปรแกรมพื้นฐานที่จำเป็น | | ติดตั้งโปรแกรมพื้นฐานที่โปรแกรมนั้นๆต้องการให้ครบ | | |
| คอมพิวเตอร์ติดไวรัส | * ใช้แผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงบุคลากรเสียเวลาไปกับกิจกรรมอื่นๆที่ไม่ใช่การทำงานในการใช้คอมพิวเตอร์และอินเตอร์เน็ต**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| บุคลากรขาดความรับผิดชอบ | | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | | |
| ขาดการควบคุมการใช้งาน | | Block เว็บไซท์ที่ไม่เกี่ยวข้องกับการทำงาน | ห้ามติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการทำงาน | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงย้ายหรือถ่ายโอนข้อมูลไม่ได้**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| บุคลากรขาดทักษะการใช้งาน | | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | | |
| การ์ด Lan เสีย | | กำหนดระยะเวลาในการตรวจสอบการ์ด Lanให้อยู่ในสภาพพร้อมใช้งานเสมอ | เมื่อการ์ด Lan เสียต้องมีการซ่อมหรือเปลี่ยนใหม่ตามความเหมาะสม | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงข้อมูลสูญหาย**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| บุคลากรทำงานผิดพลาด | | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | | |
| ไม่มีการสำรองข้อมูล | | | | ทำการสำรองข้อมูล(Backup) อย่างสม่ำเสมอ |
| ระบบคอมพิวเตอร์ล่ม | * ใช้แผนจัดการความเสี่ยงของประเด็นความเสี่ยงระบบคอมพิวเตอร์ล่ม | | | |
| คอมพิวเตอร์ติดไวรัส | * ใช้แผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ทำงานช้า**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | | - เลือกซีพียูให้เหมาะสมกับการใช้งาน<br>- เลือกRamให้เหมาะสมกับการใช้งาน<br>- เลือกขนาดฮาร์ดดิสก์ให้เหมาะสมกับการใช้งาน | | |
| มีขยะในฮาร์ดดิสก์มากเกินไป | | - กำหนดระยะเวลาในการทำ Disk Cleanup | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ทำงานช้า (ต่อ)**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| มีขยะในฮาร์ดดิสก์มากเกินไป(ต่อ) | | - กำหนดระยะเวลาในการทำ Disk Defragmenter<br>- ลบ Temporary Files อย่างสม่ำเสมอ | | |
| คอมพิวเตอร์ติดไวรัส | * ใช้แผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงโปรแกรมทำงานผิดพลาด**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| โปรแกรมไม่สมบูรณ์ | | - ต้องให้ผู้มีความชำนาญงานเป็นผู้ติดตั้งโปรแกรม<br>- กรณีที่เป็นโปรแกรมที่ทางโรงพยาบาลเขียนเองต้องมีการทดสอบการใช้งานก่อนการนำมาใช้งานจริง | กรณีที่เป็นโปรแกรมสำเร็จรูปต้องใช้โปรแกรมที่ถูกลิขสิทธิ์ | |
| คอมพิวเตอร์ติดไวรัส | * ใช้แผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส | | | |
| Hardware มีปัญหา | | กำหนดระยะเวลาในการตรวจสอบ Hardware(Input/Output) ให้อยู่ในสภาพที่พร้อมใช้งาน | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงบุคคลากรยกเลิกหรือแก้ไขข้อมูลไม่ได้/ไม่เป็น**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| บุคลากรขาดทักษะการใช้งาน | | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | | |
| โปรแกรม Edit Dataไม่ได้หลังบันทึก | | เขียนโปรแกรมให้สามารถ Edit Data ได้ตามลักษณะการใช้งาน | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงหน้าจอค้างสีฟ้า (Blue Screen of Death)**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| Hardware มีปัญหา | | กำหนดระยะเวลาในการตรวจสอบ Hardware ทุกชิ้นส่วนให้อยู่ในสภาพพร้อมใช้งานเสมอ | | |
| คอมพิวเตอร์ติดไวรัส | * ใช้แผนจัดการความเสี่ยงของประเด็นความเสี่ยงเครื่องคอมพิวเตอร์ติดไวรัส | | | |
| Driver มีปัญหา | | อัพเดท Driverให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ | | |
| คอมพิวเตอร์Spec ต่ำกว่าลักษณะการใช้งาน | | กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงใช้ Software ละเมิดลิขสิทธิ์โดยรู้เท่าไม่ถึงการณ์**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| บุคลากรนำโปรแกรมมาลงเอง | | | - ห้ามบุคลากรนำโปรแกรมมาลงเองโดยไม่ได้รับอนุญาต | |
| บุคลากรโหลดโปรแกรมละเมิดลิขสิทธิ์จากอินเตอร์เน็ต | | | - ห้ามบุคลากรโหลดโปรแกรมละเมิดลิขสิทธิ์จากอินเตอร์เน็ต | |
| ละเมิด Site/Network Licens | | ต้องศึกษา Site/Network Licens ของโปรแกรมที่จะนำมาใช้ ให้ละเอียดก่อนนำโปรแกรมนั้นๆมาใช้งาน | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงบุคคลากรคีย์ข้อมูลผิด**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| บุคลากรทำงานผิดพลาด | | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | | |
| บุคลากรมีปัญหาการได้ยิน | | มีการตรวจสุขภาพให้กับบุคลากรผู้ใช้งานคอมพิวเตอร์ทุกปี | | |
| บุคลากรมีปัญหาด้านสายตา | | | | |
| ลายมืออ่านยาก | | ออกแบบแบบฟอร์มต่างๆที่ต้องใช้ในโรงพยาบาลให้เป็นแบบฟอร์มที่ต้องใช้ลายมือเขียนน้อยที่สุด | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงสั่งพิมพ์ (Print) ข้อมูลไม่ได้**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| บุคลากรขาดทักษะการใช้งาน | | จัดทำคู่มือการใช้งานเบื้องต้น โดยมีรายละเอียดดังนี้<br>1. วิธีการสั่งพิมพ์<br>2. วิธีตรวจสอบสถานะของ Printer ว่าพร้อมใช้งานหรือไม่ | | |
| PRINTER มีปัญหา | | ตรวจสอบอุปกรณ์ต่อเชื่อมต่างๆ ระหว่าง Printer กับ คอมพิวเตอร์ให้อยู่ในสภาพพร้อมใช้งาน | | |
| โปรแกรมทำงานผิดพลาด | * ใช้แผนจัดการความเสี่ยงของประเด็นความเสี่ยงโปรแกรมทำงานผิดพลาด | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงขาดบุคลากรในบางตำแหน่งที่ควรจะมี**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| ภาระ/ลักษณะงานเพิ่ม | | มีการกำหนดระยะเวลาในการประชุมหารือร่วมกันของทุกฝ่ายที่เกี่ยวข้องเพื่อประเมินภาระงานและลักษณะงาน เพื่อสรรหาบุคลากรให้เหมาะสมกับงานและเพียงพอต่อภาระงาน | | |
| ไม่มีการประเมินภาระ/ลักษณะงาน | | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงบุคลากรมีโอกาส Update เทคโนโลยีใหม่ๆน้อย**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| ภาระงานมาก | | มีการส่งเสริมและจัดสรรเวลาเพื่อให้บุคลากรผู้เกี่ยวข้องเข้าอบรมหลักสูตรต่างๆด้าน IT ตามความเหมาะสม | | |
| องค์กรไม่ส่งเสริม | | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงแก้ไขโปรแกรมไม่ทัน**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| โปรแกรมขาดความยืดหยุ่น | | มีการออกแบบและเขียนโปรแกรมให้ยืดหยุ่นและปรับเปลี่ยนได้ง่าย | | |
| ขาดการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง | | มีการติดต่อสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องให้รวดเร็วเพื่อให้ทันต่อการเปลี่ยนแปลง | | |
| จัดทำโปรแกรม Specไม่ครบถ้วน | | มีการสำรวจข้อมูลให้ละเอียดก่อนจัดทำโปรแกรม | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงไม่มีการ Update ข้อมูล**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | **Take-ยอมรับ** | **Treat-ลด/ควบคุม** | **Terminate-หลีกเลี่ยง** | **Transfer-กระจาย/ถ่ายโอน** |
| ขาดการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง | | มีการติดต่อสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องให้รวดเร็วเพื่อให้ทันต่อการเปลี่ยนแปลง | | |
| บุคลากรทำงานล่าช้า | | มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงค้นหา (Search) ข้อมูลที่ต้องการใช้ในระบบไม่พบ**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | **Take-ยอมรับ** | **Treat-ลด/ควบคุม** | **Terminate-หลีกเลี่ยง** | **Transfer-กระจาย/ถ่ายโอน** |
| บุคลากรขาดทักษะการใช้งาน | | มีการจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | | |
| ช่องทางการค้นหาซับซ้อนเกินไป | | กำหนดช่องทางการเข้าถึงข้อมูลให้ง่ายต่อการเข้าถึงข้อมูล | | |
| ไม่ได้บันทึกข้อมูลไว้ | | กำหนดให้ชัดเจนว่าข้อมูลใดต้องทำการบันทึกไว้ | | |
| ข้อมูลสูญหาย | * ใช้แผนจัดการความเสี่ยงของประเด็นความเสี่ยงข้อมูลสูญหาย | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงบุคคลากรใช้งานโปรแกรมไม่เป็น**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| บุคลากรขาดทักษะการใช้งาน | | การจัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน | | |
| เป็นโปรแกรมเฉพาะทาง | | | | |
| เปลี่ยนโปรแกรมหรือเวอร์ชัน | | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยงจำนวน Computer ไม่เพียงพอต่อการใช้งาน**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| ไม่มีการสำรวจความต้องการ | | มีการสำรวจความต้องการก่อนจัดหาคอมพิวเตอร์ในแต่ละครั้ง | | |
| อยู่ระหว่างการส่งซ่อม | จัดให้มีเครื่องคอมพิวเตอร์สำรองกรณีที่เครื่องหลักถูกส่งซ่อม | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยง Option การใช้งานของโปรแกรมไม่เพียงพอต่อความต้องการการใช้งาน**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| สำรวจข้อมูลไม่ละเอียดก่อนเขียนโปรแกรม | | ก่อนจัดทำโปรแกรมต้องมีการสำรวจข้อมูลการใช้งานให้ละเอียด | | |
| ไม่มีการทดสอบใช้งานก่อนใช้จริง | | เมื่อจัดทำโปรแกรมเสร็จแล้วต้องมีการทดสอบใช้งานก่อนที่จะนำโปรแกรมนั้นไปใช้งานจริง | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยง CD-ROM ใช้งานไม่ได้**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | Take-ยอมรับ | Treat-ลด/ควบคุม | Terminate-หลีกเลี่ยง | Transfer-กระจาย/ถ่ายโอน |
| Power Supply ขัดข้อง | | - กำหนดระยะเวลาในการตรวจสอบขั้วต่อภายในระหว่าง Power Supply กับ CD-ROM ให้อยู่ในสภาพพร้อมใช้งานเสมอ<br>- กำหนดระยะเวลาในการทำความสะอาดพัดลมที่ติดอยู่กับ Power Supply โดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น | | |
| ตัว CD-ROM เสีย | เปลี่ยน CD-ROM ใหม่ | | | |

**การสร้างแผนจัดการความเสี่ยงของประเด็นความเสี่ยง CD-ROM ใช้งานไม่ได้ (ต่อ)**

| สาเหตุพื้นฐาน | แผนจัดการความเสี่ยง | | | |
|---|---|---|---|---|
| | **Take-ยอมรับ** | **Treat-ลด/ควบคุม** | **Terminate-หลีกเลี่ยง** | **Transfer-กระจาย/ถ่ายโอน** |
| สายเคเบิล(IDE Cable) หลุด | | กำหนดระยะเวลาในการตรวจสอบสายเคเบิล(IDE Cable) และสายไฟ (Power Cable) ให้อยู่ในสภาพพร้อมใช้งานเสมอ | | |
| สายไฟ(Power Cable) หลุด | | | | |

# ภาคผนวก ง
# แผนจัดการความเสี่ยงหลัก 4 แผนหลัก

ตารางแสดงแผนจัดการความเสี่ยงหลักออกมาตรการควบคุมและกำหนดวิธีการใช้งาน

| ***ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน*** |
| --- |
| ■ Scan ทุกไฟล์ที่ Download มาจากอินเตอร์เน็ต<br>■ ห้ามใช้โปรแกรมประเภทฟรีแวร์/แชร์แวร์<br>■ Scan แผ่นดิสก์,CDและ Flash drive ก่อนการใช้งาน<br>■ Update Firewall ให้เป็นปัจจุบันอยู่เสมอ<br>■ ทำการตรวจสอบชุดปรับปรุง (Patch หรือ Service Pack) ให้เป็นปัจจุบันอยู่เสมอ<br>■ หลีกเลี่ยงการดาวน์โหลดข้อมูลและโปรแกรมต่างๆที่ไม่เกี่ยวข้องกับการทำงานจากเว็บไซท์<br>■ หลีกเลี่ยงการเปิดอีเมล์ที่ไม่ทราบที่มาที่แน่นอน<br>■ Block เว็บไซท์ที่ไม่เกี่ยวข้องกับการทำงาน<br>■ หลีกเลี่ยงการเปิดไฟล์แนบโดยอัตโนมัติหรือการตั้งค่าในโปรแกรมอีเมล์ให้ดาวน์โหลดไฟล์โดยอัตโนมัติ<br>■ Scan ไฟล์หรือโปรแกรมที่ติดมากับ E-mail ก่อนที่จะเปิดอ่านหรือเก็บลงบนฮาร์ดดิสก์<br>■ อัพเดท Driverให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ<br>■ หลีกเลี่ยงการเดินสาย LAN คู่ไปกับสายสัญญาณอื่นๆ<br>■ ติดตั้งอุปกรณ์ป้องกันสัญญาณรบกวนที่มาจากสายส่งและจากอุปกรณ์ต่าง ๆ<br>■ ติดตั้งอุปกรณ์ประเภท UPS ป้องกันไฟขาดหรือเกิน<br>■ ห้องที่เก็บเครื่องแม่ข่าย(Server) ต้องมั่นคงแข็งแรง<br>■ กำหนดให้ผู้มีความชำนาญงานเป็นผู้ติดตั้งโปรแกรม<br>■ โปรแกรมสำเร็จรูปต้องใช้โปรแกรมที่ถูกลิขสิทธิ์<br>■ โปรแกรมที่ทางโรงพยาบาลเขียนเองต้องมีการทดสอบการใช้งานก่อนการนำมาใช้งานจริง<br>■ ติดตั้งโปรแกรมพื้นฐานที่โปรแกรมใดๆต้องการให้ครบ<br>■ มีการประเมินผลการทำงานของบุคลากรเพื่อให้คุณให้โทษ<br>■ ห้ามติดตั้งโปรแกรมที่ไม่เกี่ยวข้องกับการทำงาน<br>■ ทำการสำรองข้อมูล(Backup) อย่างสม่ำเสมอ<br>■ กำหนดระยะเวลาในการทำ Disk Cleanup<br>■ กำหนดระยะเวลาในการทำ Disk Defragmenter<br>■ ลบ Temporary Files อย่างสม่ำเสมอ |

ตารางแสดงแผนจัดการความเสี่ยงหลักออกมาตรการควบคุมและกำหนดวิธีการใช้งาน(ต่อ)

| ***ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน*** |
|---|
| ■ อัพเดท Driverให้เป็นเวอร์ชันปัจจุบันอยู่เสมอ<br>■ ห้ามบุคลากรนำโปรแกรมมาลงเองโดยไม่ได้รับอนุญาต<br>■ ห้ามบุคลากรโหลดโปรแกรมละเมิดลิขสิทธิ์จากอินเตอร์เน็ต<br>■ ต้องศึกษา Site/Network Licens ของโปรแกรมที่จะนำมาใช้ ให้ละเอียดก่อนนำโปรแกรมนั้นๆมาใช้งาน<br>■ มีการตรวจสุขภาพให้กับบุคลากรผู้ใช้งานคอมพิวเตอร์ทุกปี<br>■ ออกแบบแบบฟอร์มต่างๆที่ต้องใช้ในโรงพยาบาลให้เป็นแบบฟอร์มที่ต้องใช้ลายมือเขียนน้อยที่สุด<br>■ จัดทำคู่มือการใช้งานเบื้องต้น<br>■ มีการกำหนดระยะเวลาในการประชุมหารือร่วมกันของทุกฝ่ายที่เกี่ยวข้องเพื่อประเมินภาระงานและลักษณะงาน เพื่อสรรหาบุคลากรให้เหมาะสมกับงานและเพียงพอต่อภาระงาน<br>■ มีการออกแบบและเขียนโปรแกรมให้ยืดหยุ่นและปรับเปลี่ยนได้ง่าย<br>■ มีการติดต่อสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องให้รวดเร็วเพื่อให้ทันต่อการเปลี่ยนแปลง<br>■ มีการสำรวจข้อมูลให้ละเอียดก่อนจัดทำโปรแกรม<br>■ มีการติดต่อสื่อสารระหว่างหน่วยงานที่เกี่ยวข้องให้รวดเร็วเพื่อให้ทันต่อการเปลี่ยนแปลง<br>■ กำหนดให้ชัดเจนว่าข้อมูลใดต้องทำการบันทึกไว้<br>■ มีการสำรวจความต้องการก่อนจัดหาคอมพิวเตอร์ในแต่ละครั้ง<br>■ จัดให้มีเครื่องคอมพิวเตอร์สำรองกรณีที่เครื่องหลักถูกส่งซ่อม |

ตารางแสดงแผนจัดการความเสี่ยงหลักกำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน

| ***กำหนด Spec คอมพิวเตอร์ให้เหมาะสมกับการใช้งาน*** |
|---|
| ■ เลือกการ์ดจอและแรมให้เหมาะสมกับการใช้งาน<br>■ เลือกชนิดของอุปกรณ์ระบายความร้อนให้เหมาะสมกับการใช้งาน<br>■ เลือกขนาดของอุปกรณ์ระบายความร้อนให้เหมาะสมกับการใช้งาน<br>■ หากมีการเปลี่ยนฮาร์ดแวร์ใหม่ต้องมีการตรวจสอบว่าฮาร์ดแวร์ที่เปลี่ยนใหม่สามารถทำงานร่วมกับฮาร์ดแวร์ที่มีอยู่เดิมได้<br>■ เลือกซีพียูให้เหมาะสมกับการใช้งาน<br>■ เลือกขนาดฮาร์ดดิสก์ให้เหมาะสมกับการใช้งาน |

ตารางแสดงแผนจัดการความเสี่ยงหลักวางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง

| ***วางแผนการบำรุงรักษา Hardware และ อุปกรณ์ที่เกี่ยวข้อง*** |
| --- |
| ■ กำหนดระยะเวลาในการตรวจสอบสายไฟที่ต่อกับพัดลมระบายความร้อนให้อยู่ในสภาพที่พร้อมใช้งาน<br>■ กำหนดระยะเวลาทำความสะอาดพัดลมระบายความร้อนโดยใช้แปรงทาสีขนอ่อนในการปัดฝุ่น<br>■ จัดสายไฟภายในเครื่องให้เรียบร้อยไม่ขวางทางลมของพัดลม<br>■ กำหนดระยะเวลาในการตรวจสอบ ขั้วต่อภายในระหว่าง Power Supply กับ อุปกรณ์ฮาร์ดแวร์อื่นๆภายในเครื่องให้แน่นอยู่เสมอ<br>■ กำหนดระยะเวลาในการทำความสะอาดพัดลมที่ติดอยู่กับ Power Supply<br>■ เดินสาย Lan ให้เป็นระเบียบเรียบร้อย<br>■ กำหนดระยะเวลาในการตรวจสอบสาย Lan ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ<br>■ กำหนดระยะเวลาในการตรวจสอบPort เชื่อมต่อให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ<br>■ กำหนดระยะเวลาในการตรวจสอบการ์ด Lanให้อยู่ในสภาพพร้อมใช้งานเสมอ<br>■ เมื่อการ์ด Lan เสียต้องมีการซ่อมหรือเปลี่ยนใหม่ตามความเหมาะสม<br>■ กำหนดระยะเวลาในการตรวจสอบHardware(Input/Output) ให้อยู่ในสภาพที่พร้อมใช้งาน<br>■ ตรวจสอบอุปกรณ์ต่อเชื่อมต่างๆระหว่าง Printer กับ คอมพิวเตอร์ให้อยู่ในสภาพพร้อมใช้งาน<br>■ กำหนดระยะเวลาในการตรวจสอบ ขั้วต่อภายในระหว่าง Power Supply กับ CD-ROM ให้อยู่ในสภาพพร้อมใช้งานเสมอ<br>■ กำหนดระยะเวลาในการตรวจสอบ สายเคเบิล(IDE Cable) และสายไฟ(Power Cable) ให้อยู่ในสภาพพร้อมใช้งานเสมอ |

ตารางแสดงแผนจัดการความเสี่ยงหลักจัดอมรมบุคลากร

| ***จัดอมรมบุคลากร*** |
| --- |
| ■ จัดอมรมระบบงานและทักษะการใช้งานโปรแกรมต่างๆให้กับบุคลากรผู้ใช้งาน |

# ภาคผนวก จ

## แบบฟอร์มในการบันทึกข้อมูลในการดำเนินตามแผนจัดการความเสี่ยง

แบบฟอร์มในการบันทึกข้อมูลในการดำเนินตามแผนจัดการความเสี่ยง

<table>
<tr><td colspan="6">แบบฟอร์มในการบันทึกข้อมูลในการดำเนินตามแผนจัดการความเสี่ยง</td></tr>
<tr><td colspan="2">ชื่อแผนจัดการความเสี่ยง</td><td colspan="4"></td></tr>
<tr><td colspan="2">วัตถุประสงค์</td><td colspan="4"></td></tr>
<tr><td colspan="6">รายละเอียดของแผนจัดการความเสี่ยงที่ต้องปฏิบัติ</td></tr>
<tr><td colspan="6"></td></tr>
<tr><td colspan="3">ผู้รับผิดชอบหลัก</td><td colspan="3">ผู้มีส่วนเกี่ยวข้อง</td></tr>
<tr><td colspan="3"></td><td colspan="3"></td></tr>
<tr><td>หน้าที่ของผู้รับผิดชอบหลัก</td><td colspan="2"></td><td>หน้าที่ของผู้มีส่วนเกี่ยวข้อง</td><td colspan="2"></td></tr>
<tr><td colspan="2">ว/ด/ป ที่เริ่มดำเนินงาน</td><td colspan="2">ว/ด/ป ที่คาดว่าจะเสร็จสิ้น</td><td colspan="2">ว/ด/ป ที่ดำเนินงานเสร็จสิ้น</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2">งบประมาณที่คาดว่าจะใช้</td><td></td><td colspan="2">งบประมาณที่ใช้จริง</td><td></td></tr>
<tr><td colspan="6">หมายเหตุ</td></tr>
<tr><td colspan="6"></td></tr>
</table>

***<u>คำอธิบายในการกรอกแบบฟอร์ม</u>***

1. ช่องชื่อแผนจัดการความเสี่ยง

ข้อมูลที่ต้องกรอก คือ ชื่อของแผนจัดการความเสี่ยง เช่น ออกมาตรการควบคุมและกำหนดวิธีการใช้งาน

2. ช่องวัตถุประสงค์

ข้อมูลที่ต้องกรอก คือ วัตถุประสงค์ในการปฏิบัติตามแผนจัดการความเสี่ยงนั้นๆ ซึ่งจะทำให้บุคลากรที่รับผิดชอบและบุคลากรที่เกี่ยวข้องกับแผนจัดการความเสี่ยงนั้นๆทราบถึงวัตถุประสงค์ในการปฏิบัติตามแผนนั้นๆ

3. ช่องรายละเอียดของแผนจัดการความเสี่ยงที่ต้องปฏิบัติ

ข้อมูลที่ต้องกรอก คือ สิ่งที่ต้องปฏิบัติตามแผนจัดการความเสี่ยงนั้นๆ

4. ช่องผู้รับผิดชอบหลัก

ข้อมูลที่ต้องกรอก คือ ชื่อของบุคลากรหรือฝ่ายงานที่เป็นผู้รับผิดชอบหลักในการดำเนินตามแผนจัดการความเสี่ยง ซึ่งอาจจะมีมากกว่า 1 คนหรือมากกว่า 1 ฝ่ายงาน

5. ช่องผู้มีส่วนเกี่ยวข้อง

ข้อมูลที่ต้องกรอก คือ ชื่อของบุคลากรหรือฝ่ายงานที่มีส่วนเกี่ยวข้องในการดำเนินตามแผนจัดการความเสี่ยง ซึ่งอาจจะมีมากกว่า 1 คนหรือมากกว่า 1 ฝ่ายงาน

6. ช่องหน้าที่ของผู้รับผิดชอบหลัก

ข้อมูลที่ต้องกรอก คือ หน้าที่หรือสิ่งที่ผู้รับผิดชอบหลักต้องปฏิบัติ ยกตัวอย่างเช่น ผู้รับผิดชอบหลักมีหน้าที่จัดอบรมตามแผนจัดการความเสี่ยงนั้นๆ เป็นต้น

7. ช่องหน้าที่ของผู้มีส่วนเกี่ยวข้อง

ข้อมูลที่ต้องกรอก คือ หน้าที่หรือสิ่งที่ผู้มีส่วนเกี่ยวข้องต้องปฏิบัติ ยกตัวอย่างเช่น ผู้มีส่วนเกี่ยวข้องมีหน้าที่เข้าอบรมตามแผนจัดการความเสี่ยงนั้นๆ เป็นต้น

8. ช่อง ว/ด/ป ที่เริ่มดำเนินงาน

ข้อมูลที่ต้องกรอก คือ กำหนดการ(วันที่ เดือน ปี พ.ศ.) ที่จะต้องเริ่มปฏิบัติตามแผนจัดการความเสี่ยงนั้นๆ ซึ่งจะทำให้บุคลากรทุกคนหรือทุกฝ่ายงานที่เกี่ยวข้องเข้าใจตรงกันถึงกำหนดการในการเริ่มดำเนินงาน

9. ช่อง ว/ด/ป ที่คาดว่าจะเสร็จสิ้น

ข้อมูลที่ต้องกรอก คือ กำหนดการ(วันที่ เดือน ปี พ.ศ.) ที่คาดว่าจะดำเนินงานเสร็จสิ้นตามแผนจัดการความเสี่ยงนั้น เพื่อเป็นการกำหนดกรอบเวลาในการดำเนินงาน

10. ช่อง ว/ด/ป ที่ดำเนินงานเสร็จสิ้น

ข้อมูลที่ต้องกรอก คือ วันที่ เดือน ปี พ.ศ. ที่ดำเนินงานตามแผนจัดการความเสี่ยงนั้นๆเสร็จสิ้น (กรอกหลังจากดำเนินงานเสร็จสิ้นแล้วจริงๆ) ซึ่งจะทำให้ทราบว่าแผนจัดการจัดการความเสี่ยงนั้นๆได้ดำเนินงานเสร็จสิ้นตามแผนแล้ว

11. ช่องงบประมาณที่คาดว่าจะใช้

ข้อมูลที่ต้องกรอก คือ งบประมาณหรือค่าใช้จ่ายที่คาดว่าจะใช้ในการดำเนินงานตามแผนจัดการความเสี่ยงนั้นๆ

12. ช่องงบประมาณที่ใช้จริง

ข้อมูลที่ต้องกรอก คือ งบประมาณหรือค่าใช้จ่ายที่ใช้จริงในการดำเนินงานตามแผนจัดการความเสี่ยงนั้นๆ

13. ช่องหมายเหตุ

ข้อมูลที่ต้องกรอก คือ ข้อมูลหรือรายละเอียดอื่นๆ ที่เกี่ยวข้องกับแผนจัดการความเสี่ยงนั้นๆ ซึ่งไม่มีช่องให้กรอก แต่อาจมีความจำเป็นที่จะต้องแจ้งให้ผู้มีส่วนเกี่ยวข้องทั้งหมดทราบ ให้กรอกข้อมูลหรือรายละเอียดต่างๆเหล่านั้นลงในช่องหมายเหตุ

***<u>หมายเหตุ</u>*** *ในบางกรณี ช่องที่ 9 (ช่อง ว/ด/ป ที่คาดว่าจะเสร็จสิ้น)และช่องที่ 10(ว/ด/ป ที่ดำเนินงานเสร็จสิ้น) อาจไม่จำเป็นต้องกรอกข้อมูลเนื่องจากแผนจัดการความเสี่ยงบางแผนต้องดำเนินไปเรื่อยๆจนกว่าจะมีการเปลี่ยนแปลงปรับปรุงหรือยกเลิกแผนนั้นๆ*

# ประวัติผู้เขียนวิทยานิพนธ์

นายเนติ จินดามาตย์ เกิดเมื่อวันที่ 2 มกราคม พ.ศ.2525 ที่จังหวัดชัยภูมิ เป็นบุตรคนที่ 3 ของ นายวิโรจน์ และ นางจินดา จินดามาตย์ สำเร็จการศึกษาหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมเคมี ภาควิชาวิศวกรรมเคมีและกระบวนการ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ ในปี พ.ศ.2548 และเข้าศึกษาต่อในหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิศวกรรมอุตสาหการ ภาควิชาวิศวกรรมอุตสาหการ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เมื่อปี พ.ศ.2548