ระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กร ตามมาตรฐานสากล BS 7799 กรณีศึกษา : สำนักหอสมุด มหาวิทยาลัยมหิดล

กฤษฎา แก้วผุดผ่อง

005.8
00A0203360 ก279ร
Title : ระบบต้นแบบการจัดการความเสี่ยง
ศูนย์สนเทศและหอสมุด มหาวิทยาลัยธุรกิจบัณฑิตย์

งานค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2551

Risk Assessment Prototype System for Information Assets with BS 7799 Standard

Case Study : Mahidol University Library and Information Center

KRISADA KEAWPHODPHONG

An Independent Study Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science (Computer and Communication Technology)

Department of Computer and Communication Technology

Graduate School, Dhurakij Pundit University

2008

เลขทะเบียน 0203360
วันลงทะเบียน - 1 พ.ค. 2552
เลขเรียกหนังสือ ก179ร
[2550]
ฉ.2

ใบรับรองงานค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญา วิทยาศาสตรมหาบัณฑิต

หัวข้องานค้นคว้าอิสระ ระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กร ตามมาตรฐานสากล BS 7799 กรณีศึกษา : สำนักหอสมุด มหาวิทยาลัยมหิดล

เสนอโดย กฤษฎา แก้วผุดผ่อง

สาขาวิชา เทคโนโลยีคอมพิวเตอร์และการสื่อสาร

อาจารย์ที่ปรึกษางานค้นคว้าอิสระ ผศ. ดร.ประณต บุญไชยอภิสิทธิ์

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบงานค้นคว้าอิสระแล้ว

.....ประธานกรรมการ

(รศ.ดร.ประสงค์ ปราณีตพลกรัง)

.....กรรมการและอาจารย์ที่ปรึกษางานค้นคว้าอิสระ

(ผศ.ดร.ประณต บุญไชยอภิสิทธิ์)

.....กรรมการ

(รศ.ดร.บงการ หอมนาน)

บัณฑิตวิทยาลัยรับรองแล้ว

..... คณบดีบัณฑิตวิทยาลัย

(ผศ.ดร.สมศักดิ์ ดำริชอบ)

วันที่ ...3.....เดือน ...มกราคม.....พ.ศ. .....2551.....

DPU

หัวข้องานค้นคว้าอิสระ	ระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กรตามมาตรฐานสากล BS 7799 กรณีศึกษา : สำนักหอสมุด มหาวิทยาลัยมหิดล
ชื่อผู้เขียน	กฤษฎา แก้วผุดผ่อง
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์
สาขาวิชา	เทคโนโลยีคอมพิวเตอร์และการสื่อสาร
ปีการศึกษา	2550

บทคัดย่อ

งานค้นคว้าอิสระ ระบบต้นแบบการจัดการความเสี่ยง สำหรับทรัพย์สินสารสนเทศในองค์กรตามมาตรฐานสากล BS 7799 กรณีศึกษา : สำนักหอสมุด มหาวิทยาลัยมหิดล ดำเนินการศึกษาและพัฒนาโดยใช้แนวทางมาตรฐานของอังกฤษที่เรียกว่า BS 7799 (British Standard) หรือมาตรฐานสากล ISO/IEC 17799:2005 และ ISO/IEC 27001 ที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร โดยแบ่งเนื้อหาออกเป็น 11 หัวข้อหลัก (Domain) ซึ่งในแต่ละหัวข้อประกอบด้วยวัตถุประสงค์ที่แตกต่างกัน รวมทั้งสิ้น 39 วัตถุประสงค์ (Control objectives) และภายใต้วัตถุประสงค์แต่ละข้อ ประกอบด้วยมาตรการสำหรับใช้ในการรักษาความปลอดภัยที่แตกต่างกันรวมจำนวน 133 ข้อ (Controls)

มาตรฐาน ISO/IEC 27001 ว่าด้วยเรื่องของข้อกำหนด ในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยให้กับองค์กร และใช้แนวทางการประเมินความเสี่ยงมาประกอบการพิจารณาหาวิธีการหรือมาตรการเพื่อป้องกัน ลดความเสี่ยง และรักษาทรัพย์สินสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยในระดับที่เหมาะสม รวมไปถึงการรักษาความปลอดภัยของข้อมูล ซึ่งเป็นส่วนสำคัญส่วนหนึ่งในการบริหารหน่วยงานให้เป็นไปอย่างมีประสิทธิภาพ อันจะนำไปสู่ความปลอดภัยในหน่วยงาน

กระบวนการจัดการประเมินความเสี่ยงมีการจัดทำขึ้น เพื่อศึกษาถึงปัญหาหรือภัยคุกคามในรูปแบบต่างๆ ที่จะก่อให้เกิดความเสียหายต่อทรัพย์สินด้านสารสนเทศขององค์กร โดยมีการจัดหมวดหมู่ของทรัพย์สินออกเป็น 5 หมวดคือ อุปกรณ์คอมพิวเตอร์ (Hardware) โปรแกรม (Software) บุคลากร (People) ข้อมูล (Information) และงานบริการ (Service) เพื่อทำการคำนวณหาค่าความเสี่ยงที่เกิดกับทรัพย์สินในแต่ละหมวด แล้วทำการจัดระดับของความเสี่ยง รวมไปถึงการศึกษาเพื่อค้นหาถึงจุดอ่อนของตัวข้อมูลและทรัพย์สินนั้นๆ ซึ่งเป็นสาเหตุที่ก่อให้เกิดปัญหาและภัยคุกคาม เพื่อนำ

ความเสี่ยงที่เกินระดับที่องค์กรสามารถยอมรับได้ ไปดำเนินการควบคุมและแก้ไขความเสี่ยงโดยการออกเป็นมาตรการป้องกันเพื่อให้บุคลากรในหน่วยงานปฏิบัติตาม รวมทั้งยังเป็นการกำหนดรูปแบบการรับมือในเรื่องความปลอดภัยได้อย่างมีระบบและมีประสิทธิภาพ

การพัฒนาระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กร ยังสามารถช่วยในการเผยแพร่ข้อมูลให้ผู้ใช้งานได้ทราบถึง แนวทางในการจัดทำการบริหารความเสี่ยงสำหรับทรัพย์สินสารสนเทศภายในองค์กร กระบวนการจัดการประเมินความเสี่ยง ผู้ใช้งานได้ทราบถึง ช่องโหว่ ภัยคุกคาม ระดับของความเสี่ยงที่เกิดขึ้นต่อทรัพย์สินในประเภทต่าง ๆ รวมไปถึงแนวทางการป้องกัน และสามารถค้นหาทรัพย์สิน ที่ผู้ใช้ต้องการทราบถึงรายละเอียดในการจัดการความเสี่ยงสำหรับทรัพย์สินนั้น แล้วเชื่อมโยงไปยังข้อมูลเหล่านั้นได้ และแสดงรายงานการจัดระดับความเสี่ยงของทรัพย์สินให้ผู้ใช้งานได้ทราบและเป็นการช่วยสร้างความมั่นใจในการติดต่อสื่อสารระหว่างหน่วยงาน ให้มีความมั่นคงปลอดภัยในระดับที่สูงขึ้นด้วย

DPU

Independent Study Title	Risk Assessment Prototype System for Information Assets with BS 7799 Standard Case Study : Mahidol University Library and Information Center
Author	Krisada Keawphodphong
Independent Study Advisor	Assistant Professor Dr.Pranot Boonchai-Apisit
Department	Computer and Communication Technology
Academic Year	2007

ABSTRACT

The development of risk assessment prototype system for information assets is concerning the security controls with BS 7799, ISO/IEC 17799:2005 and ISO/IEC 27001 as the standard. With ISO/IEC 17799 standard is composed of 11 domains which consists of 39 control objectives and 133 controls for creating a security.

ISO/IEC 27001 standard describes how to do a management system of information security and also include processes which continually monitor the effectiveness of security protections for the information and associated system.

Information assets are identified into 5 groups with hardware, software, people, information and service. A study on risk assessment prototype system for information assets aims at a risk analysis to find out risks from information assets in working process and knowing what the possible threats and vulnerabilities to those assets. Then calculate the risk value for them and findings a protection to improve the present state of information security into the appropriate level that the organization can be accepted and achieved through security controls implemented and maintained within the organization.

This independent study therefore looks at a main result are: (1) a people within an organization can have a knowledge to implement and maintain risk assessment and management processes within the organization with effectively; (2) a people can be selected an appropriate control objectives and controls from ISO/IEC 17799 standard to prevent assets from threats and vulnerabilities; (3) a people can be searched for the details concerning about risk assessment

processes; (4) a people can be seen a report by comparing between each level of risks value for information assets that has been analyzed.

DPU

กิตติกรรมประกาศ

งานค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงได้ด้วยดี ด้วยความอนุเคราะห์และเสียสละเวลาอันมีค่าของอาจารย์ที่ปรึกษางานค้นคว้าอิสระ ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์ ที่กรุณาแนะนำความรู้และสิ่งที่เป็นประโยชน์อย่างเอนกประการ ในการช่วยปรับปรุงงานค้นคว้าอิสระฉบับนี้ รองศาสตราจารย์ ดร.ประสงค์ ปราณีตพลกรัง ประธานกรรมการสอบงานค้นคว้าอิสระ และรองศาสตราจารย์ ดร.บงการ หอมนาน กรรมการผู้ทรงคุณวุฒิ ที่ได้สละเวลามาเป็นคณะกรรมการสอบงานค้นคว้าอิสระ ตลอดจนให้ข้อคิดเห็นอันเป็นประโยชน์ ในการทำให้งานค้นคว้าอิสระฉบับนี้มีคุณค่ามากยิ่งขึ้น

ขอขอบคุณมหาวิทยาลัยธุรกิจบัณฑิตย์ที่ให้การสนับสนุนทางด้านทุนการศึกษา

ขอขอบพระคุณท่านอาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้แก่ข้าพเจ้า

ขอกราบขอบพระคุณบิดามารดา ญาติพี่น้องทุกคน และน้อมระลึกถึงผู้มีพระคุณทุกคนที่ทำให้ข้าพเจ้ามีวันนี้ และขออุทิศความดีทั้งหลายของงานค้นคว้าอิสระฉบับนี้แก่ ผู้มีพระคุณทุกท่าน

ผู้เขียนหวังเป็นอย่างยิ่งว่า งานค้นคว้าอิสระฉบับนี้ จะเป็นประโยชน์กับผู้ที่ต้องการศึกษาด้านการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศภายในองค์กร และหากมีข้อผิดพลาดประการใดในงานค้นคว้าอิสระฉบับนี้ ผู้เขียนต้องกราบขออภัยเป็นอย่างสูงมา ณ ที่นี้ด้วย

กฤษฎา แก้วผุดผ่อง

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ฆ
บทคัดย่อภาษาอังกฤษ	จ
กิตติกรรมประกาศ	ช
สารบัญตาราง	ญ
สารบัญภาพ	ท
บทที่	
1. บทนำ	1
1.1 ที่มาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการวิจัย	3
1.3 ขอบเขตของการวิจัย	3
1.4 ประโยชน์ที่คาดว่าจะได้รับ	3
2. แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง	4
2.1 ทรัพย์สินสารสนเทศกับการใช้งานในห้องสมุด	4
2.2 องค์ประกอบในระบบงานคอมพิวเตอร์	4
2.3 มาตรฐานการรักษาความปลอดภัยข้อมูล	11
2.4 การบริหารความเสี่ยง	18
2.5 ภาษาพีเอชพี	38
2.6 งานวิจัยที่เกี่ยวข้อง	41
3. ระเบียบวิธีวิจัย	43
3.1 ขั้นตอนการดำเนินการวิจัย	43
3.2 อุปกรณ์และเครื่องมือที่ใช้ในการวิจัย	43
3.3 ระยะเวลาในการดำเนินการวิจัย	45
3.4 สรุป	46
4. การวิเคราะห์และการออกแบบระบบ	47
4.1 การศึกษาด้านการจัดการความเสี่ยง	47
4.2 การวิเคราะห์ระบบ	116
4.3 การออกแบบระบบ	118

สารบัญ (ต่อ)

	หน้า
5. ผลการจัดทำและการทดสอบระบบ	122
5.1 การใช้งานเว็บเพจหน้าข้อมูลหลัก	122
5.2 การใช้งานเว็บเพจหน้าตารางประเมินความเสี่ยง	127
5.3 การใช้งานเว็บเพจหน้าสืบค้นข้อมูลทรัพย์สิน	128
5.4 การใช้งานเว็บเพจหน้ารายงานการจัดระดับความเสี่ยง	131
6. สรุปผลการวิจัย	134
6.1 สรุปผลการวิจัย	134
6.2 อภิปรายผลการศึกษา	135
6.3 ข้อเสนอแนะ	135
บรรณานุกรม	136
ภาคผนวก	139
ภาคผนวก ก การตรวจสอบมาตรการป้องกันสำหรับทรัพย์สินในองค์กร	140
ประวัติผู้เขียน	143

สารบัญตาราง

ตารางที่ หน้า

2.1 แสดงระดับของโอกาสในการเกิดภัยคุกคาม (Probability) 37
2.2 แสดงระดับของผลกระทบและความเสียหายต่อทรัพย์สิน (Impact) 37
2.3 แสดงระดับของค่าความเสี่ยงโดยรวม 38
3.1 ระยะเวลาในการดำเนินการวิจัย 45
4.1 รายชื่อทรัพย์สินทางด้านอุปกรณ์คอมพิวเตอร์ 48
4.2 รายชื่อทรัพย์สินทางด้านโปรแกรม 48
4.3 รายชื่อทรัพย์สินทางด้านบุคลากร 49
4.4 รายชื่อทรัพย์สินทางด้านข้อมูล 49
4.5 รายชื่อทรัพย์สินทางด้านงานบริการ 49
4.6 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server (มาตรการที่ 9.1.2) 51
4.7 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server (มาตรการที่ 9.2.1) 51
4.8 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server (มาตรการที่ 9.2.4) 52
4.9 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server (มาตรการที่ 10.1.1) 52
4.10 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server (มาตรการที่ 10.4.1) 53
4.11 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ (มาตรการที่ 9.1.2) 53
4.12 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ (มาตรการที่ 9.2.1) 54
4.13 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ (มาตรการที่ 9.2.4) 54
4.14 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ (มาตรการที่ 10.1.1) 55

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

4.15 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ (มาตรการที่ 10.4.1) 55
4.16 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 7.1.1) 56
4.17 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 7.1.2) 56
4.18 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 9.2.1) 57
4.19 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 9.2.4) 57
4.20 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 9.2.6) 58
4.21 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 9.2.7) 58
4.22 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 10.4.1) 59
4.23 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 10.5.1) 59
4.24 การประเมินความเสี่ยงสำหรับสื่อบันทึกข้อมูลแผ่นซีดี (มาตรการที่ 9.2.7) 60
4.25 การประเมินความเสี่ยงสำหรับสื่อบันทึกข้อมูลแผ่นซีดี (มาตรการที่ 10.7.1) 60
4.26 การประเมินความเสี่ยงสำหรับสื่อบันทึกข้อมูลแผ่นซีดี (มาตรการที่ 10.7.2) 61
4.27 การประเมินความเสี่ยงสำหรับเทปแบ็คอัพ (มาตรการที่ 9.2.7) 61

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

4.28 การประเมินความเสี่ยงสำหรับเทปแบ็คอัพ (มาตรการที่ 10.7.1) 62
4.29 การประเมินความเสี่ยงสำหรับเทปแบ็คอัพ (มาตรการที่ 10.7.2) 62
4.30 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูล SQL Server (มาตรการที่ 12.4.3) 63
4.31 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูล SQL Server (มาตรการที่ 12.5.1) 63
4.32 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูล SQL Server (มาตรการที่ 12.6.1) 64
4.33 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Microsoft Windows (มาตรการที่ 10.4.1) 64
4.34 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Microsoft Windows (มาตรการที่ 12.4.1) 65
4.35 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Microsoft Windows (มาตรการที่ 12.4.3) 65
4.36 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Microsoft Windows (มาตรการที่ 12.5.1) 66
4.37 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Microsoft Windows (มาตรการที่ 12.6.1) 66
4.38 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Linux (มาตรการที่ 12.4.1) 67
4.39 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Linux (มาตรการที่ 12.4.3) 67
4.40 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Linux (มาตรการที่ 12.5.1) 68

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

4.41 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Linux (มาตรการที่ 12.6.1) 68
4.42 การประเมินความเสี่ยงสำหรับโปรแกรมต่าง ๆ (มาตรการที่ 12.6.1) 69
4.43 การประเมินความเสี่ยงสำหรับบุคลากร (มาตรการที่ 8.1.1) 69
4.44 การประเมินความเสี่ยงสำหรับบุคลากร (มาตรการที่ 8.1.2) 70
4.45 การประเมินความเสี่ยงสำหรับบุคลากร (มาตรการที่ 8.2.2) 70
4.46 การประเมินความเสี่ยงสำหรับบุคลากร (มาตรการที่ 8.3.2) 71
4.47 การประเมินความเสี่ยงสำหรับบุคลากร (มาตรการที่ 8.3.3) 71
4.48 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 6.1.5) 72
4.49 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 7.1.3) 72
4.50 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 8.3.3) 73
4.51 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 10.5.1) 73
4.52 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 10.10.2) 74
4.53 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 11.2.1) 74

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

4.54 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 12.4.1) 75
4.55 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 12.4.3) 75
4.56 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 6.1.5) 76
4.57 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 7.1.3) 76
4.58 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 8.3.3) 77
4.59 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 10.5.1) 77
4.60 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 10.10.2) 78
4.61 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 11.2.1) 78
4.62 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 12.4.1) 79
4.63 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 12.4.3) 79
4.64 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 6.1.5) 80
4.65 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 7.1.3) 80
4.66 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 8.3.3) 81

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

4.67 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 10.5.1) 81
4.68 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 10.10.2) 82
4.69 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 11.2.1) 82
4.70 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 12.4.1) 83
4.71 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 12.4.3) 83
4.72 การประเมินความเสี่ยงสำหรับงานบริการ Internet (มาตรการที่ 8.2.2) 84
4.73 การประเมินความเสี่ยงสำหรับงานบริการ Internet (มาตรการที่ 10.6.1) 84
4.74 การประเมินความเสี่ยงสำหรับงานบริการ Internet (มาตรการที่ 11.5.2) 85
4.75 การประเมินความเสี่ยงสำหรับงานบริการ Internet (มาตรการที่ 11.5.5) 85
4.76 การประเมินความเสี่ยงสำหรับระบบปรับอากาศ (ห้อง Server) (มาตรการที่ 9.2.4) 86
4.77 การประเมินความเสี่ยงสำหรับงานบริหารจัดการ กำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 8.3.3) 86
4.78 การประเมินความเสี่ยงสำหรับงานบริหารจัดการ กำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 11.2.1) 87
4.79 การประเมินความเสี่ยงสำหรับงานบริหารจัดการ กำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 11.2.2) 87

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

4.80 การประเมินความเสี่ยงสำหรับงานบริหารจัดการ
กำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 11.2.4) 88
4.81 การประเมินความเสี่ยงสำหรับงานบริหารจัดการ
กำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 11.5.1) 88
4.82 การประเมินความเสี่ยงสำหรับงานบริหารจัดการ
กำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 11.5.2) 89
4.83 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์
(มาตรการที่ 9.2.1) 89
4.84 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์
(มาตรการที่ 9.2.4) 90
4.85 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์
(มาตรการที่ 9.2.7) 90
4.86 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์
(มาตรการที่ 10.3.1) 91
4.87 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์
(มาตรการที่ 10.3.2) 91
4.88 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์
(มาตรการที่ 14.1.2) 92
4.89 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์
(มาตรการที่ 10.4.1) 92
4.90 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์
(มาตรการที่ 10.5.1) 93
4.91 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์
(มาตรการที่ 11.5.4) 93
4.92 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์
(มาตรการที่ 14.1.2) 94

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

4.93 การประเมินความเสี่ยงสำหรับงานบริการระบบ Web Server (มาตรการที่ 8.2.2) 94
4.94 การประเมินความเสี่ยงสำหรับงานบริการระบบ Web Server (มาตรการที่ 13.1.2) 95
4.95 การประเมินความเสี่ยงสำหรับงานบริการระบบ Web Server (มาตรการที่ 14.1.2) 95
4.96 การประเมินความเสี่ยงสำหรับงานบริการระบบห้องสมุดอัตโนมัติ (มาตรการที่ 8.2.2) 96
4.97 การประเมินความเสี่ยงสำหรับงานบริการระบบห้องสมุดอัตโนมัติ (มาตรการที่ 13.1.2) 96
4.98 การประเมินความเสี่ยงสำหรับงานบริการระบบห้องสมุดอัตโนมัติ (มาตรการที่ 14.1.2) 97
4.99 การประเมินความเสี่ยงสำหรับงานบริการระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 8.2.2) 97
4.100 การประเมินความเสี่ยงสำหรับงานบริการระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 13.1.2) 98
4.101 การประเมินความเสี่ยงสำหรับงานบริการระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 14.1.2) 98
4.102 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (อุปกรณ์คอมพิวเตอร์ - เครื่องแม่ข่ายระบบ Web Server) 99
4.103 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (อุปกรณ์คอมพิวเตอร์ - เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ) 100
4.104 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (อุปกรณ์คอมพิวเตอร์ - เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง) 102
4.105 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (อุปกรณ์คอมพิวเตอร์ - สื่อบันทึกข้อมูลแผ่นซีดี) 103

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

4.106 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (อุปกรณ์คอมพิวเตอร์ - เทปแบ็คอัพ) 103
4.107 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (โปรแกรม - ระบบฐานข้อมูล SQL Server) 104
4.108 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (โปรแกรม - ระบบปฏิบัติการ Microsoft Windows) 104
4.109 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (โปรแกรม – ระบบปฏิบัติการ Linux) 105
4.110 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (โปรแกรม – โปรแกรมต่าง ๆ) 106
4.111 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (บุคลากร) 106
4.112 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (ข้อมูล - ระบบ Web Server) 107
4.113 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (ข้อมูล - ระบบห้องสมุดอัตโนมัติ) 108
4.114 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (ข้อมูล - ระบบฐานข้อมูลสหบรรณานุกรม) 108
4.115 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ - งานบริการ Internet) 109
4.116 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ - ระบบปรับอากาศห้องServer) 109
4.117 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานบริหารจัดการกำหนดสิทธิ การเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้) 110
4.118 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์) 110

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

4.119 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ–งานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์) 112
4.120 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานบริการระบบ Web Server) 113
4.121 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานบริการระบบห้องสมุดอัตโนมัติ) 114
4.122 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานบริการระบบฐานข้อมูลสหบรรณานุกรม) 115
4.123 แสดงรายชื่อทรัพย์สินทางด้านอุปกรณ์คอมพิวเตอร์ 118
4.124 แสดงรายชื่อทรัพย์สินทางด้านโปรแกรม 119
4.125 แสดงรายชื่อทรัพย์สินทางด้านบุคลากร 119
4.126 แสดงรายชื่อทรัพย์สินทางด้านข้อมูล 120
4.127 แสดงรายชื่อทรัพย์สินทางด้านงานบริการ 120

สารบัญภาพ

ภาพที่	หน้า
2.1 เปรียบเทียบโดเมนของ ISO 17799 เวอร์ชั่น 2000 และ 2005	12
2.2 กระบวนการ Plan-Do-Check-Act	16
2.3 ความสัมพันธ์ระหว่างความเสี่ยง จุดอ่อน และภัยคุกคาม	19
2.4 แสดงขั้นตอนการทำงานของหน้าเว็บพีเอชพี	39
4.1 กระบวนการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศ	47
4.2 Use Cases diagram การค้นหาข้อมูลทรัพย์สินสารสนเทศ	117
5.1 หน้าหลักแสดงรายละเอียด แนวทางการจัดทำประเมินความเสี่ยง	122
5.2 หน้าแสดงรายละเอียด เหตุจูงใจในการจัดการความเสี่ยง	123
5.3 หน้าแสดงรายละเอียด วัตถุประสงค์ในการจัดการความเสี่ยง	123
5.4 หน้าแสดงรายละเอียด ประโยชน์ที่ได้รับจากการจัดการความเสี่ยง	124
5.5 หน้าแสดงรายละเอียด องค์ประกอบในระบบงานคอมพิวเตอร์	124
5.6 หน้าแสดงรายละเอียด มาตรฐานการรักษาความปลอดภัยข้อมูล	125
5.7 หน้าแสดงรายละเอียด การจัดการความเสี่ยง	125
5.8 หน้าแสดงรายละเอียด กระบวนการ ในการรักษาความปลอดภัยข้อมูลขององค์กร	126
5.9 หน้าแสดงรายละเอียด กระบวนการในการจัดการความเสี่ยง	126
5.10 หน้าแสดงรายละเอียด ตารางประเมินความเสี่ยงอุปกรณ์คอมพิวเตอร์	127
5.11 ตารางแสดงค่าการประเมินความเสี่ยง สำหรับเครื่องแม่ข่ายระบบ Web Server	128
5.12 หน้าสืบค้นข้อมูลทรัพย์สินสำหรับอุปกรณ์คอมพิวเตอร์	129
5.13 หน้าแสดงผลลัพธ์การสืบค้น พบข้อมูลทรัพย์สิน สำหรับอุปกรณ์คอมพิวเตอร์	129
5.14 หน้าแสดงผลลัพธ์การสืบค้น ไม่พบข้อมูลทรัพย์สิน สำหรับอุปกรณ์คอมพิวเตอร์	130
5.15 หน้าเว็บตารางแสดงค่าการประเมินความเสี่ยง สำหรับเครื่องแม่ข่ายระบบ Web Server	130

สารบัญภาพ (ต่อ)

ภาพที่ หน้า

5.16 หน้าเว็บแสดงรายงานการจัดระดับความเสี่ยง
สำหรับอุปกรณ์คอมพิวเตอร์ 131
5.17 หน้าเว็บแสดงรายงานการจัดระดับความเสี่ยง
แยกตามระดับค่าความเสี่ยง 132
5.18 หน้าเว็บแสดงค่าความเสี่ยงที่ต้องการแก้ไขอย่างเร่งด่วน
มีค่าระหว่าง 45 – 63 133

DPU

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

โดยปกติแล้วการทำงานทางด้านระบบคอมพิวเตอร์ จะมีองค์ประกอบทั่วไปอยู่ 4 อย่าง คือ อุปกรณ์คอมพิวเตอร์ (Hardware) โปรแกรม (Software) บุคลากร (People) ข้อมูล (Information) และนอกจากองค์ประกอบทั้ง 4 อย่างนี้แล้ว ในปัจจุบันยังมีองค์ประกอบอีกอย่างหนึ่ง ที่กล่าวได้ว่าเป็นส่วนสำคัญต่อระบบงานทางด้านคอมพิวเตอร์คือ งานบริการ (Service) ซึ่งจะมีส่วนเกี่ยวข้องกับระบบงานต่างๆ ที่มีให้บริการแก่ผู้ใช้งานภายในองค์กร ได้แก่งานบริการที่เกี่ยวข้องกับโปรแกรมการใช้งานที่ผู้ใช้ได้รับจากระบบงานต่างๆ เช่น ระบบงานด้านอินเทอร์เน็ต ระบบงานด้านเว็บเซิร์ฟเวอร์ ระบบงานด้านฐานข้อมูล เป็นต้น

จากการที่ผู้ศึกษาได้ทำการศึกษาถึงระบบงานทางด้านคอมพิวเตอร์ทั้ง 5 องค์ประกอบดังกล่าวแล้วนั้น สามารถกล่าวได้ว่า องค์ประกอบต่างๆ มีความเกี่ยวข้องและสัมพันธ์กัน คือเป็นทรัพย์สินสารสนเทศ (Asset) ที่มีความสำคัญต่อองค์กร ทั้งนี้ปัญหาหรือภัยคุกคามที่มีต่อทรัพย์สินที่ผู้ศึกษาพบอยู่เสมอคือ ความไม่มั่นคงปลอดภัยที่เกิดขึ้นต่อทรัพย์สินสารสนเทศเหล่านั้น อันได้แก่

1. การปฏิบัติงานผิดพลาด อันเนื่องมาจากผู้ใช้ขาดความรู้ในการปฏิบัติงาน หรือไม่ได้รับการฝึกอบรมอย่างพอเพียง รวมทั้งการขาดคู่มือในการปฏิบัติงานที่ดี

2. การใช้งานระบบเกิดความผิดพลาด เนื่องจากผู้ใช้งานขาดความตระหนัก ในด้านการรักษาความปลอดภัยในการใช้งาน

3. การใช้ทรัพย์สินสารสนเทศ ไปในทางที่ไม่ได้รับอนุญาต เพราะขาดกลไกในการเฝ้าระวังในการใช้งานเครื่องคอมพิวเตอร์ของพนักงานหรือเจ้าหน้าที่อย่างเป็นระบบ

4. ทรัพย์สินสารสนเทศถูกขโมย เนื่องจากขาดการป้องกันทางกายภาพในการเข้า ออกภายในอาคารจากบุคคลภายนอก

5. อุปกรณ์บางอย่างทำงานผิดพลาดเพราะไม่มีการบำรุงรักษาอย่างพอเพียง

6. อุปกรณ์คอมพิวเตอร์เกิดการชำรุดเสียหายเพราะไม่มีอุปกรณ์ที่ช่วยสำรองไฟฟ้า

7. เกิดการเข้าถึงข้อมูลของระบบโดยไม่ได้รับอนุญาต ทำให้ความลับข้อมูลขององค์กรถูกเปิดเผย

8. เครื่องคอมพิวเตอร์ติดไวรัสเพราะไม่ได้มีการปรับปรุงตัวสแกนไวรัสอย่างสม่ำเสมอ

9. เกิดการสวมรอยบุคคลอื่นเพื่อเข้าใช้งานระบบอันเป็นผลสืบเนื่องจากไม่มีการจัดการรหัสผ่านในการเข้าใช้ระบบงานที่ดี

10. เกิดการสวมรอยบุคคลอื่นเพื่อเข้าใช้งานระบบ ซึ่งเป็นผลสืบเนื่องจากไม่มีการดูแลจัดการรหัสผ่านในการเข้าใช้ระบบงานที่ดี

11. ข้อมูลระบบขาดความถูกต้อง เนื่องจากไม่มีกระบวนการตรวจสอบข้อมูล ที่อยู่ในระหว่างการประมวลผล

12. การให้บริการข้อมูลระบบต่อผู้ใช้งานขาดความต่อเนื่อง เพราะขาดการวางแผนในการกู้คืนระบบยามฉุกเฉิน

13. โปรแกรมคอมพิวเตอร์ทำงานผิดพลาดเพราะการกำหนดค่าของระบบไม่ถูกต้อง

โดยเฉพาะในกรณีของข้อมูล ซึ่งอยู่ในรูปแบบดิจิตอล และจะจัดเก็บไว้ที่ใดที่หนึ่งในเครือข่าย บางครั้งข้อมูลเหล่านี้อาจต้องถูกส่งผ่านเครือข่ายไปยังที่ต่างๆ ซึ่งข้อมูลเหล่านี้ อาจถูกลักลอบนำไปใช้ในทางที่ผิด หรืออาจทำให้ใช้การไม่ได้จากผู้ที่ไม่หวังดี

จากผลกระทบของความไม่มั่นคงปลอดภัยที่เกิดขึ้นอยู่เสมอ และก่อให้เกิดความเสียหายต่อทรัพย์สินสารสนเทศที่มีอยู่ภายในองค์กร จึงเป็นความตั้งใจของผู้วิจัยที่จะประยุกต์ใช้แนวทางการจัดการประเมินความเสี่ยงตามมาตรฐานสากล BS7799 (British Standard) ซึ่งมีการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ (Asset) แยกตามองค์ประกอบของระบบงานคอมพิวเตอร์ออกเป็น 5 หมวดคือ อุปกรณ์คอมพิวเตอร์ (Hardware) โปรแกรม (Software) บุคลากร (People) ข้อมูล (Information) และงานบริการ (Service) เพื่อทำการศึกษาถึงปัญหาหรือภัยคุกคามในรูปแบบต่างๆ รวมไปถึงการศึกษาเพื่อค้นหาถึงจุดอ่อนของตัวข้อมูลและทรัพย์สินนั้นๆ ซึ่งเป็นสาเหตุที่ก่อให้เกิดความเสียหายเพื่อนำความเสี่ยงที่เกินระดับที่องค์กรยอมรับได้ ไปดำเนินการควบคุมและแก้ไขความเสี่ยง เพื่อออกเป็นมาตรการป้องกันให้แก่บุคลากรในหน่วยงานนำไปปฏิบัติตาม และเป็นแนวทางการสร้างความมั่นคงปลอดภัยให้เกิดขึ้นต่อทรัพย์สินสารสนเทศ ได้อย่างเป็นระบบและมีประสิทธิภาพมากยิ่งขึ้น

1.2 วัตถุประสงค์ของการวิจัย

วัตถุประสงค์ของการวิจัย มีดังต่อไปนี้

1. เพื่อศึกษาระบบความมั่นคงปลอดภัยทางด้านข้อมูลและสารสนเทศภายในหน่วยงานขององค์กรโดยสร้างระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กรตามมาตรฐานสากล BS 7799 ขึ้นมาได้อย่างมีประสิทธิภาพ

2. เพื่อกำหนดรูปแบบการรับมือในเรื่องความปลอดภัยของระบบที่คาดว่าจะเกิดขึ้น ได้อย่างมีระบบและมีประสิทธิภาพ

1.3 ขอบเขตของการวิจัย

ขอบเขตของการวิจัย มีดังต่อไปนี้

1. จัดทำระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กรตามมาตรฐานสากล BS 7799 โดยใช้มาตรการป้องกันตามแนวทางของเอกสารหนังสือ มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2) ประจำปี 2549 เป็นแนวทางเปรียบเทียบเพื่อหาถึงภัยคุกคามหรือปัญหา และจุดอ่อน ที่เกิดขึ้น ใน 5 หมวด อันได้แก่ อุปกรณ์คอมพิวเตอร์ โปรแกรม บุคลากร ข้อมูล และงานบริการ ในการจัดทำการประเมินความเสี่ยง

2. จัดทำกระบวนการจัดการประเมินความเสี่ยง

3. เพื่อเผยแพร่ข้อมูลที่มีส่วนเกี่ยวข้องกับ กระบวนการในการจัดทำการประเมินความเสี่ยงผ่านทางระบบออนไลน์ขององค์กร โดยการประยุกต์ใช้โปรแกรมภาษาเอชทีเอ็มแอลและภาษาสคริปต์พีเอชพี

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับ มีดังต่อไปนี้

1. เป็นต้นแบบใช้สำหรับจัดทำด้านการประเมินความเสี่ยงสำหรับทรัพย์สินสารสนเทศภายในองค์กร

2. องค์กรสามารถสร้างระบบบริหารจัดการความมั่นคงปลอดภัย สำหรับทรัพย์สินด้านสารสนเทศขึ้นมาได้อย่างมีคุณภาพและมีประสิทธิภาพ ในระดับมาตรฐานสากล

3. บุคคลภายในองค์กรเกิดความตระหนัก ถึงความสำคัญของความปลอดภัย ทางด้านสารสนเทศ ภายในองค์กรมากขึ้น

4. มีการวางแผนการปฏิบัติงานที่เป็นแบบแผนและมีความรับผิดชอบที่ชัดเจน

บทที่ 2
แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

2.1 ทรัพย์สินสารสนเทศกับการใช้งานในห้องสมุด

สำนักหอสมุด มหาวิทยาลัยมหิดล ให้บริการทางวิชาการ เพื่อสนับสนุน การเรียนการสอนการค้นคว้า วิจัย ของ อาจารย์ นักศึกษา และบุคลากรอื่นๆ ตามหลักสูตร และนโยบายของมหาวิทยาลัย ตลอดจนการส่งเสริมการศึกษาหาความรู้ และการสืบค้นสารนิเทศด้วยตนเอง ซึ่งในปัจจุบันได้พัฒนาการดำเนินงาน ให้บริการด้านห้องสมุด โดยการใช้เทคโนโลยีคอมพิวเตอร์ทางด้านอุปกรณ์คอมพิวเตอร์ และโปรแกรมสำเร็จรูปที่ได้มีการพัฒนาขึ้นมา ประกอบกับระบบการสื่อสารที่ทันสมัย ทรัพยากรทางด้านอิเล็กทรอนิกส์ที่มีภายในห้องสมุด ประกอบด้วย วารสารอิเล็กทรอนิกส์ ฐานข้อมูลอิเล็กทรอนิกส์ หนังสืออิเล็กทรอนิกส์ และฐานข้อมูลคอมพิวเตอร์

สำนักหอสมุดได้มีการใช้งานเครื่องแม่ข่าย เพื่อจัดเก็บและให้บริการข้อมูลต่างๆ รวมทั้งการสืบค้นฐานข้อมูล มาใช้ในการจัดเก็บทรัพยากรดังกล่าว และได้มีการพัฒนาการดำเนินงาน ระบบห้องสมุดใหม่ โดยการนำระบบห้องสมุดอัตโนมัติ (Automated Library) เข้ามาใช้งาน ซึ่งช่วยให้มหาวิทยาลัยของรัฐทุกแห่งที่ใช้งานในระบบเดียวกัน สามารถเชื่อมโยงและแลกเปลี่ยนข้อมูลกันเป็นข่ายงานได้ทั่วประเทศ ขณะนี้สำนักหอสมุด มหาวิทยาลัยมหิดล ได้ให้บริการ นักศึกษา และบุคลากรของมหาวิทยาลัยในระบบอัตโนมัติดังกล่าว ซึ่งจะอำนวยความสะดวกให้แก่ผู้ใช้ห้องสมุดในการที่จะตรวจสอบรายชื่อทรัพยากรห้องสมุดที่มีอยู่ในฐานข้อมูลของสำนักหอสมุดได้จากเครื่องคอมพิวเตอร์ที่ติดตั้งภายในสำนักหอสมุด ศาลายา หรือในห้องสมุดคณะ สถาบันต่างๆ ของมหาวิทยาลัยมหิดล หรือเรียกค้นจากเครื่องคอมพิวเตอร์ภายในสำนักงาน หรือเครื่องส่วนตัวเพื่อต่อมายังฐานข้อมูล ของสำนักหอสมุด ในลักษณะออนไลน์ผ่านทางระบบสื่อสารเครือข่ายอินเทอร์เน็ต และอินทราเน็ต ของมหาวิทยาลัยมหิดล

2.2 องค์ประกอบในระบบงานคอมพิวเตอร์ (วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล, 2548 : 52)

การทำงานด้านระบบงานคอมพิวเตอร์ โดยปกติแล้วมีองค์ประกอบทั่วไปอยู่ 4 อย่างคือ อุปกรณ์คอมพิวเตอร์ โปรแกรม บุคลากร และข้อมูล นอกเหนือจากนั้นแล้ว ยังกล่าวได้ว่ามีอีกหนึ่งองค์ประกอบที่สำคัญคืองานบริการ ซึ่งแต่ละอย่างมีรายละเอียดดังนี้

อุปกรณ์คอมพิวเตอร์ (Hardware) (วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล, 2548 : 110-136)

เป็นอุปกรณ์ที่จับต้อง สัมผัสและสามารถมองเห็นได้อย่างเป็นรูปธรรม ฮาร์ดแวร์ของคอมพิวเตอร์จะมีแบบที่ติดตั้งอยู่ภายในตัวเครื่องคอมพิวเตอร์ (เช่น ซีพียู เมนบอร์ด แรม) และที่ติดตั้งอยู่ภายนอกเครื่องคอมพิวเตอร์ (เช่น คีย์บอร์ด เมาส์ จอภาพ เครื่องพิมพ์) รวมทั้งอุปกรณ์ใช้งานทางด้านระบบเครือข่าย เมื่อใดก็ตามที่ฮาร์ดแวร์ตัวใดตัวหนึ่งเสียหาย หรือไม่สามารถใช้งานได้ ก็สามารถเปลี่ยนหรือซ่อมแซมได้รวมไปถึงอุปกรณ์ที่เกี่ยวข้องกับการใช้งานร่วมกับคอมพิวเตอร์ ซึ่งจะทำงานประสานกันตั้งแต่การป้อนข้อมูลเข้า (input) การประมวลผล (process) และการแสดงของผลลัพธ์ (output) ตามระบบการทำงานของคอมพิวเตอร์ ซึ่งสามารถแบ่งออกได้เป็น 4 ประเภทหลักๆ ดังนี้

1. อุปกรณ์นำข้อมูลเข้า (Input Device) เป็นอุปกรณ์ที่เกี่ยวข้องกับการนำข้อมูล หรือชุดคำสั่งเข้ามายังระบบเพื่อให้คอมพิวเตอร์ทำการประมวลผลต่อไปได้ ซึ่งอาจเป็นตัวเลข ตัวอักษร ภาพ กราฟิก เสียง หรือวิดีโอ เป็นต้น อุปกรณ์นำข้อมูลเข้าที่สามารถพบเห็นได้ส่วนมากในปัจจุบันมีตัวอย่างดังต่อไปนี้

- คีย์บอร์ด (Keyboard) เป็นอุปกรณ์นำข้อมูลเข้าที่นิยมใช้กันมากที่สุด พบเห็นได้ในการใช้งานทั่วไป โดยรับข้อมูลป้อนเข้าที่เป็นตัวอักษร อักขระพิเศษ ตัวเลข รวมถึงชุดคำสั่งต่างๆ ตัวอุปกรณ์จะมีกลุ่มของแป้นพิมพ์วางเรียงต่อกันเหมือนกับ เครื่องพิมพ์ดีด ผู้ใช้งานระบบสามารถเลือกกดปุ่มใดๆได้ทันที โดยข้อมูลทั้งหมดซึ่งป้อนเข้ามา จะถูกส่งไปเก็บภายในหน่วยความจำของระบบ และแปลงให้เป็นรหัสที่คอมพิวเตอร์เข้าใจ หลังจากนั้นจึงจะนำไปประมวลผลต่อไป

- เมาส์ (Mouse) เป็นอุปกรณ์ที่ใช้สำหรับในการชี้ตำแหน่งการทำงาน รวมถึงสั่งการให้เครื่องคอมพิวเตอร์ทำงานบางคำสั่ง ที่มีการโต้ตอบกันระหว่างผู้ใช้กับคอมพิวเตอร์ โดยใช้มือเป็นตัวบังคับทิศทางและใช้นิ้วสำหรับการกดเลือกคำสั่งงาน

- จอสัมผัส (Touch screen) เป็นอุปกรณ์ที่สามารถใช้นิ้วมือแตะเพื่อบังคับหรือสั่งการไปยังหน้าจอคอมพิวเตอร์ได้เลย โดยไม่จำเป็นต้องใช้เมาส์หรือแป้นพิมพ์

- เว็บแคม (Web cam) เป็นกล้องถ่ายวิดีโออีกประเภทหนึ่ง ที่ใช้สำหรับการถ่ายภาพเคลื่อนไหวแต่ภาพที่ได้จะมีลักษณะหยาบและมีขนาดไฟล์เล็กจึงนิยมใช้สำหรับในการเผยแพร่ข้อมูลบนอินเทอร์เน็ต หรือนำไปใช้ประโยชน์กับโปรแกรมสนทนาบนเว็บบาง ประเภทเพื่อให้เห็นหน้าตาของคู่สนทนาระหว่างที่พิมพ์โต้ตอบกัน ซึ่งสามารถบันทึกได้ทั้งภาพเคลื่อนไหวและภาพนิ่ง

- สแกนเนอร์ (Scanner) เป็นอุปกรณ์ที่อ่านข้อมูลประเภทภาพถ่าย โดยผู้ใช้เพียงแค่วางภาพถ่ายหรือเอกสารลงไปบนแท่นวางแล้วสั่งให้เครื่องอ่านหรือสแกน ก็สามารถเก็บรูปภาพหรือเอกสารสำคัญต่างๆเหล่านั้นไว้ในคอมพิวเตอร์ได้ หลักการทำงานจะเหมือนกับเครื่องถ่ายเอกสารคือ

ใช้ลำแสงกวาดผ่านกระดาษหรือเอกสารนั้น แล้วส่งภาพเข้าคอมพิวเตอร์ เพื่อแปลงสัญญาณดิจิตอล และเรียกใช้ต่อไป

- เครื่องอ่านบาร์โค้ด (Bar code reader) โดยปกติแล้วตัวเลขของรหัสหนังสือที่ใช้ในการจัดเก็บข้อมูลของหนังสือมักจะมีจำนวนหลักที่ค่อนข้างมาก เมื่อต้องการเรียกใช้ หรือตรวจสอบ โดยการป้อนข้อมูลผ่านแป้นพิมพ์จะทำให้เกิดความผิดพลาดขึ้นได้ง่าย จึงได้มีการพิมพ์รหัสหนังสือออกมาเป็นแบบรหัสแท่งสีดำและขาวต่อเนื่องกันไป เรียกว่า บาร์โค้ด (Bar code) ซึ่งนำไปใช้พิมพ์แทนรหัสของหนังสือ โดยใช้เครื่องอ่านรหัสนี้ที่เรียกว่าเครื่องอ่านบาร์โค้ด (Bar code reader)

- เครื่องสแกนลายนิ้วมือ (Fingerprint) เป็นอุปกรณ์ที่ใช้สำหรับการตรวจสอบข้อมูลส่วนตัวบุคคลเฉพาะอย่าง ซึ่งนำมาใช้กับงานป้องกันและรักษาความปลอดภัยในหน่วยงาน

2. หน่วยเก็บข้อมูลสำรอง (Secondary Storage Device) จัดเป็นอุปกรณ์ที่ใช้เก็บบันทึกผลลัพธ์ ข้อมูลหรือกลุ่มคำสั่งต่างๆเพื่อไว้ใช้สำหรับในอนาคต ในปัจจุบันนี้มีสื่อที่ผลิตมาสำหรับใช้เก็บข้อมูลสำรองหลากหลายชนิด ซึ่งสามารถแบ่งตามรูปแบบของสื่อที่เก็บได้ดังนี้

2.1 สื่อเก็บข้อมูลแบบจานแม่เหล็ก (Magnetic Disk Device) มีหลายประเภทได้แก่

- ฟล็อปปี้ดิสก์ (Floppy disks) เป็นสื่อเก็บบันทึกข้อมูลที่ได้รับความนิยมและใช้งานอย่างแพร่หลายในช่วงที่ผ่านมา สามารถที่จะบันทึกข้อมูลซ้ำได้

- ฮาร์ดดิสก์ (Hard disks) เป็นอุปกรณ์เก็บบันทึกข้อมูลที่มีโครงสร้างคล้ายกับดิสเก็ตต์ แต่จุข้อมูลมากกว่าและมีความเร็วในการเข้าถึงข้อมูลสูงกว่า ส่วนใหญ่จะถูกติดตั้งภายในเครื่องคอมพิวเตอร์เพื่อใช้สำหรับเก็บตัวโปรแกรมระบบปฏิบัติการ รวมถึงโปรแกรมประยุกต์อื่นๆ

2.2 สื่อเก็บข้อมูลแบบแสง (Optical Storage Device) นับเป็นสื่อเก็บข้อมูลสำรองที่ได้รับความนิยมมากในปัจจุบัน ซึ่งใช้หลักการทำงานของแสงเข้ามาช่วย การจัดเก็บข้อมูลจะคล้ายกับแผ่นจานแม่เหล็กแต่ต่างกันที่การแบ่งวงของแทรค จะแบ่งเป็นลักษณะคล้ายรูปก้นหอย และเริ่มเก็บบันทึกข้อมูลจากส่วนด้านในออกมาด้านนอก มีหลายประเภทได้แก่

- CD (Compact disc) เป็นสื่อเก็บบันทึกข้อมูลแบบแสง ที่ใช้อย่างแพร่หลายซึ่งแยกออกตามประเภทได้ดังนี้

- CD-ROM (Compact disc read only memory) เป็นสื่อเก็บบันทึกข้อมูลที่นิยมใช้ สำหรับการเก็บบันทึกข้อมูลทางคอมพิวเตอร์ เช่น ระบบปฏิบัติการหรือโปรแกรมประยุกต์เพื่อใช้สำหรับการติดตั้งภายในคอมพิวเตอร์ โดยผู้ใช้สามารถอ่านข้อมูลได้อย่างเดียวแต่ไม่สามารถเขียนหรือบันทึกข้อมูลซ้ำได้

- CD-R (Compact disc recordable) เป็นแผ่นที่สามารถใช้ไดรว์สำหรับเขียนแผ่น (CDWriter) เพื่อทำการบันทึกข้อมูลได้ และหากเขียนข้อมูลลงไปแล้วยังไม่เต็มแผ่นก็สามารถ

เขียนเพิ่มเติมได้ แต่ไม่สามารถลบข้อมูลที่เขียนไว้แล้วได้ เนื่องจากเนื้อที่บนแผ่นแต่ละจุดจะเขียนข้อมูลได้ครั้งเดียว เขียนแล้วเขียนเลยจะลบทิ้งอีกไม่ได้ เหมาะสำหรับการบันทึกไฟล์ข้อมูลเพื่อเก็บรักษาทั่วไปเช่น ภาพถ่ายจากกล้องดิจิตอล เพลง หรือไฟล์งานข้อมูล ซึ่งอยู่ในเครื่องคอมพิวเตอร์ส่วนตัว

- CD-RW (Compact disc rewritable) แผ่นชนิดนี้มีลักษณะเหมือนกันกับแผ่น CD-R ทุกประการแต่มีข้อดีกว่าคือนอกจากเขียนบันทึกข้อมูลได้หลายครั้งแล้ว ยังสามารถลบข้อมูลและเขียนซ้ำใหม่ได้เรื่อยๆเหมือนกับการบันทึกและเขียนซ้ำของดิสเก็ตต์ เหมาะสำหรับผู้ที่ต้องการบันทึกข้อมูลที่มีการเปลี่ยนแปลงบ่อยและเก็บข้อมูลไว้ในระยะเวลาอันสั้น

- DVD (Digital Versatile Disc/Digital Video Disc) เป็นสื่อเก็บบันทึกข้อมูลแบบแสง ที่ผลิตมาเพื่อตอบสนองกับงานเก็บข้อมูลที่มีความจุสูง ซึ่งแยกออกตามประเภทได้ดังนี้

- DVD-ROM เป็นแผ่น DVD ที่มักใช้สำหรับเก็บข้อมูลขนาดใหญ่มาก ซึ่งผู้ใช้สามารถอ่านข้อมูลได้อย่างเดียวแต่ไม่สามารถเขียนหรือบันทึกข้อมูลซ้ำได้

- DVD-R และ DVD+R เป็นแผ่น DVD ที่เขียนและบันทึกข้อมูลได้เพียงครั้งเดียว เหมือนกับการเขียนแผ่น CD-R แต่ต่างกันที่ความเร็วในการเขียนข้อมูลลงแผ่น

- DVD-RW และ DVD+RW เป็นแผ่น DVD ที่เขียนและบันทึกข้อมูลซ้ำได้หลายๆครั้งซึ่งวิธีการเขียนข้อมูลอาจเติมเฉพาะข้อมูลใหม่ลงไปโดยลบอันเก่าทิ้งทั้งแผ่น หรือจะนำข้อมูลอันเก่ามารวมกับของใหม่ แล้วเขียนไปพร้อมๆกันก็ได้

2.3 สื่อเก็บข้อมูลแบบเทป (Tape Device) เป็นอุปกรณ์บันทึกข้อมูลที่เหมาะสำหรับการสำรองข้อมูล(backup) ซึ่งเก็บข้อมูลได้ในจำนวนมาก มีลักษณะการเข้าถึงข้อมูลแบบเรียงลำดับต่อเนื่องกันไป (sequential access) โดยเทปที่ใช้ในการเก็บข้อมูล มีการผลิตขึ้นมาหลากหลายขนาดแตกต่างกันไป เช่น DAT หรือ DDS (Digital Audio Tape หรือ Digital Data Storage) มีความจุข้อมูลอยู่ที่ 2 GB-240 GB DLT (Digital Linear Tape)มีความจุข้อมูลอยู่ที่ 20 GB-229 GB LTO (Linear Tape-Open) มีความจุข้อมูลอยู่ที่ 100 GB-200 GB

3. อุปกรณ์แสดงผลลัพธ์ (Output Device) เป็นอุปกรณ์ที่ใช้ในการแสดงผลลัพธ์ที่ได้จากการประมวลผลของคอมพิวเตอร์ โดยผลลัพธ์ที่แสดงออกมา จะมีทั้งข้อมูล ตัวอักษร ภาพนิ่ง ภาพเคลื่อนไหว หรือเสียง ซึ่งแบ่งประเภทได้ดังนี้

3.1 อุปกรณ์แสดงผลหน้าจอ (Display device) เป็นอุปกรณ์สำหรับการแสดงผลในรูปแบบภาพกราฟิกและผู้ใช้สามารถเห็นผลลัพธ์ได้แค่ชั่วคราวเท่านั้น เมื่อไฟดับหรือปิดการทำงานของเครื่องคอมพิวเตอร์ลงไปจะไม่สามารถเห็นได้อีกเช่น

- จอซีอาร์ที (CRT Monitor) เป็นอุปกรณ์แสดงผลที่มักนิยมใช้กับคอมพิวเตอร์ประเภทพีซี ซึ่งเป็นเทคโนโลยีเดียวกับหลอดภาพของโทรทัศน์ มีหลายขนาดตั้งแต่ 14 15 17 และ 19 นิ้ว

- จอแอลซีดี (LCD Monitor) เป็นอุปกรณ์แสดงผลอีกแบบหนึ่ง ที่แต่เดิมนิยมใช้กับเครื่องคอมพิวเตอร์แบบโน้ตบุ๊ค ปัจจุบันได้นำมาใช้กับเครื่องพีซีทั่วไป เนื่องจากมีขนาดบาง เบา สะดวกในการเคลื่อนย้าย และยังไม่เปลืองพื้นที่สำหรับการทำงาน

3.2 อุปกรณ์สำหรับพิมพ์งาน (Printing Device) เป็นอุปกรณ์การแสดงผลที่แสดงออกมาให้อยู่ในรูปแบบข้อมูล รายงาน หรือรูปภาพ ซึ่งสามารถจับต้องหรือเก็บรักษาไว้ได้อย่างถาวรเช่น

- เครื่องพิมพ์แบบดอทเมตริกซ์ (Dot matrix Printer) เป็นเครื่องพิมพ์ซึ่งทำงานโดยใช้หัวเข็มพิมพ์กระทบลงไปที่ผ้าหมึก และตัวกระดาษโดยตรง แต่มีข้อจำกัดในเรื่องการพิมพ์งานที่เป็นสี นอกจากนี้คุณภาพของงาน ความคดชัดและความเร็วจะต่ำกว่าเครื่องพิมพ์แบบอื่นๆ

- เครื่องพิมพ์แบบเลเซอร์ (Laser Printer) เป็นเครื่องพิมพ์ที่ได้คุณภาพของงานที่มีความละเอียดสูงมาก และพิมพ์ได้เร็วกว่าแบบดอทเมตริกซ์

- เครื่องพิมพ์แบบอิงค์เจ็ต (Ink-jet Printer) เป็นเครื่องพิมพ์ที่มีการทำงานโดยอาศัยน้ำหมึกพ่นลงไปบนกระดาษตรงจุดที่ต้องการและสามารถเลือกใช้ได้ทั้งหมึกสีและขาวดำ

4. อุปกรณ์ทางด้านระบบเครือข่าย

- ตัวรวมสาย (Hub) เป็นอุปกรณ์ที่จำเป็นในการเชื่อมต่อทางระบบเครือข่าย ซึ่งทำให้เครื่องคอมพิวเตอร์ทุกเครื่องส่งสัญญาณถึงกันได้หมด

- อุปกรณ์เลือกเส้นทาง (Router) เป็นอุปกรณ์ที่ใช้ในการเลือกเส้นทางการสื่อสารเพื่อเชื่อมต่อวงจรเครือข่ายท้องถิ่น (LAN) มีเซิร์ฟเวอร์เป็นเสมือนสถานีบริการ เพื่อรองรับผู้ใช้งานด้านคอมพิวเตอร์จำนวนมากในองค์กร router เป็นอุปกรณ์ทำงานคล้าย bridge แต่จะสามารถเชื่อมต่อระบบที่ใช้สื่อ หรือสายสัญญาณต่างชนิดกันได้ เช่น เชื่อมต่อ Ethernet LAN ที่ส่งข้อมูลด้วยสาย UTP : Unshielded Twisted Pair เข้ากับอีเทอร์เน็ตอีกเครือข่าย ที่สำคัญยังทำหน้าที่เลือกหรือกำหนดเส้นทางที่จะส่งข้อมูล ระหว่างเครือข่ายและแปลงข้อมูลให้เหมาะสมกับการนำส่ง

- อุปกรณ์ควบคุมการรับ-ส่งข้อมูลในระบบเครือข่ายไร้สาย (Access Point) จะใช้คลื่นความถี่วิทยุ นิยมใช้สำหรับเครือข่ายระยะใกล้ (LAN) ปัจจุบัน access point 1 จุด สามารถรองรับคอมพิวเตอร์เครือข่ายได้ตั้งแต่ 10-255 เครื่อง

โปรแกรม (Software) (วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล, 2548 : 52-53)

เป็นองค์ประกอบทางนามธรรมที่ไม่สามารถจับต้อง หรือสัมผัสได้ เหมือนกับฮาร์ดแวร์ ซอฟต์แวร์เป็นส่วนของโปรแกรมคอมพิวเตอร์ที่มีการบรรจุคำสั่ง เพื่อให้คอมพิวเตอร์สามารถทำงานได้ตามที่ผู้ใช้ต้องการ และระบบคอมพิวเตอร์ก็จะไม่สามารถทำงานได้หากปราศจากชุดคำสั่งที่เขียนไว้เหล่านี้ ซึ่งซอฟต์แวร์แบ่งได้เป็น 2 ประเภทใหญ่ๆ คือ

1. ซอฟต์แวร์ระบบ (System Software) เป็นซอฟต์แวร์กลุ่มที่ทำหน้าที่ควบคุมระบบการทำงานของเครื่องคอมพิวเตอร์ ซึ่งในกลุ่มประเภทนี้เป็นที่รู้จักกันเป็นอย่างดีคือระบบปฏิบัติการ (Operating System) เช่น วินโดวส์ (Microsoft Windows) ลีนุกซ์ (Linux) เป็นต้น

2. ซอฟต์แวร์ประยุกต์ (Application Software) เป็นกลุ่มของซอฟต์แวร์ที่สามารถติดตั้งได้ในภายหลังทั้งนี้ขึ้นอยู่กับความเหมาะสมและการประยุกต์ใช้งานเป็นหลัก โดยอาจมีบริษัทผู้ผลิตขึ้นมาเพื่อจำหน่ายโดยตรงทั้งที่ให้เลือกใช้ฟรี ซื้อ ทำเอง หรือจ้างเขียนโดยเฉพาะ

บุคลากร (People) (วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล, 2548 : 54-59)

บุคลากรที่เกี่ยวข้องกับคอมพิวเตอร์ เป็นองค์ประกอบอีกอย่างหนึ่งที่สำคัญมาก เพราะหากบุคลากรไม่มีความรู้ความเข้าใจในการใช้งานเกี่ยวกับระบบคอมพิวเตอร์ ก็จะทำให้การใช้งานไม่มีประสิทธิภาพหรือไม่ได้ผลลัพธ์ตามเป้าหมาย กลุ่มบุคลากรที่เกี่ยวข้องทั้งหมดแบ่งออกได้เป็น 3 กลุ่มด้วยกันคือ

1. กลุ่มผู้ใช้งานทั่วไป (User) เป็นผู้ใช้งานระดับล่างซึ่งไม่จำเป็นต้องมีความเชี่ยวชาญ ก็สามารถใช้งานได้โดยศึกษาจากคู่มือการปฏิบัติงานหรือคู่มือใช้งานโปรแกรมที่นำมาใช้ หรืออาจต้องเข้ารับการอบรมบ้าง เพื่อให้สามารถใช้งานได้ บุคลากรกลุ่มนี้มีจำนวนมากที่สุดในหน่วยงาน และลักษณะงานมักเกี่ยวข้องกับการใช้งานคอมพิวเตอร์ทั่วไป เช่น งานธุรการ งานป้อนข้อมูล เป็นต้น

2. กลุ่มผู้เชี่ยวชาญ (Computer Technician) ส่วนใหญ่มักจะเป็นบุคลากรที่มีความชำนาญทางด้านเทคนิคโดยเฉพาะเช่น ช่างเทคนิคคอมพิวเตอร์ ซึ่งมีหน้าที่หลักคือการแก้ปัญหาที่เกิดขึ้นกับระบบในหน่วยงานให้สามารถใช้งานได้ตามปกติ นักวิเคราะห์ระบบจะมีหน้าที่ในการวิเคราะห์ความต้องการของผู้ใช้ในหน่วยงานว่าต้องการระบบโปรแกรมหรือลักษณะงานแบบไหน อย่างไร เพื่อจะพัฒนาระบบงานให้ตรงกับความต้องการมากที่สุด นักเขียนโปรแกรมจะทำการสร้างระบบงานตามที่นักวิเคราะห์ระบบได้ออกแบบมาเพื่อให้ระบบนั้นสามารถใช้งานได้จริง

3. กลุ่มผู้บริหาร (CIO -- Chief Information Officer) ในหน่วยงานขนาดใหญ่ที่ต้องอาศัยเทคโนโลยีคอมพิวเตอร์ขับเคลื่อนงานธุรกิจในองค์กร อาจต้องมีบุคลากรในตำแหน่ง CIO ซึ่ง

ทำหน้าที่กำหนดทิศทาง นโยบายและแผนงานทางคอมพิวเตอร์ในองค์กรทั้งหมดว่าควรเป็นไปในรูปแบบใด

ข้อมูล (Information) (วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล, 2548 : 60)

ข้อมูลเป็นองค์ประกอบที่สำคัญที่ใช้สำหรับการประมวลผลซึ่งการทำงานของระบบด้านคอมพิวเตอร์ จะเกี่ยวข้องกับข้อมูลตั้งแต่การนำข้อมูลเข้า จนกลายเป็นข้อมูลที่สามารถใช้ประโยชน์ต่อได้หรือที่เรียกว่า สารสนเทศ ข้อมูลสำหรับการนำมาประมวลผลด้วยคอมพิวเตอร์นั้นจะได้มาจากแหล่งข้อมูลที่มีแหล่งกำเนิดของข้อมูลที่อยู่ภายในองค์กรทั่วไป ข้อมูลที่ได้มานั้นอาจมาจากพนักงานหรือมีอยู่แล้วในองค์กร เช่น รายชื่อพนักงาน รายชื่อสมาชิกห้องสมุด รายชื่อทรัพยากรของห้องสมุด รายงานการใช้ระบบห้องสมุดอัตโนมัติ เป็นต้น

งานบริการ (Service)

นอกเหนือจากองค์ประกอบทั้ง 4 อย่างข้างต้นแล้ว ในปัจจุบันยังมีงานบริการซึ่งเป็นอีกองค์ประกอบหนึ่ง ที่สามารถกล่าวได้ว่าเป็นส่วนสำคัญต่อระบบงานทางด้านคอมพิวเตอร์ คือซึ่งจะมีส่วนเกี่ยวข้องกับระบบงานต่างๆ ที่มีให้บริการแก่ผู้ใช้งานภายในองค์กร โดยแบ่งเป็นกลุ่มได้ดังนี้

1. Computing Service เป็นบริการที่เกี่ยวข้องกับโปรแกรมการใช้งาน ที่ผู้ใช้ได้รับจากระบบงานต่างๆ เช่น ระบบงานด้านไปรษณีย์อิเล็กทรอนิกส์ (E-mail) ระบบในการจัดหาหรือสั่งซื้อหนังสือ (Acquisition) ระบบจัดเก็บทรัพยากรภายในห้องสมุด (Cataloging) ระบบให้บริการยืม คืนหนังสือ (Circulation) ระบบสำรองข้อมูลห้องสมุดอัตโนมัติ (System Administration) เป็นต้น

2. Communication Service เป็นบริการที่เกี่ยวข้องกับทางด้านเครือข่าย ที่ผู้ใช้บริการได้ใช้ประโยชน์จากการใช้งานเครือข่าย เช่น ผู้ใช้บริการสามารถใช้เครือข่ายเพื่อที่จะเข้าถึงระบบงานหรือสามารถที่จะค้นหาข้อมูลที่ต้องการจากแหล่งข้อมูลทางด้านอินเทอร์เน็ตต่างๆ รวมไปถึงการส่งไปรษณีย์อิเล็กทรอนิกส์ (E-mail) ได้

3. Technical Service เป็นบริการที่เกี่ยวข้องกับทางด้านเทคนิคเช่น ระบบทำความเย็น ระบบระบายอากาศภายในห้องปฏิบัติการเครื่องแม่ข่าย การมีระบบด้านจ่ายไฟฟ้าสำรอง และระบบสำรองกระแสไฟฟ้า (UPS) เพื่อให้งานบริการสามารถดำเนินงานได้อย่างต่อเนื่อง และมีความปลอดภัย

2.3 มาตรฐานการรักษาความปลอดภัยข้อมูล

จักรกฤษณ์ แร่ทอง (2547) กล่าวว่า BS7799 (British Standard 7799) เป็นมาตรฐานที่เกี่ยวกับการจัดการในเรื่องความปลอดภัยของข้อมูล ที่ออกโดย British Standards Institution ซึ่งถูกตีพิมพ์ครั้งแรกในเดือนเมษายน ค.ศ. 1991 โดยใช้ชื่อว่า BS7799:1999 มาตรฐานนี้เป็นส่วนหนึ่งของมาตรฐาน ISO (International Standard Organization) ต่อมาในเดือนตุลาคมปี ค.ศ.2000 ได้มีการปรับปรุงบางส่วนของมาตรฐาน และถูกตีพิมพ์เป็นครั้งที่ 2 ภายใต้ชื่อ ISO/IEC17799:2000 ในวันที่1 ธันวาคม ค.ศ. 2000 มาตรฐานนี้ถูกกำหนดขึ้นมาเพื่อเป็นแนวทางในการจัดการด้านความปลอดภัยของข้อมูลภายในองค์กร โดยมีการกำหนดแนวทางสำหรับด้านการพัฒนามาตรฐานความปลอดภัย และการปฏิบัติงานเพื่อให้เกิดการจัดการที่มีประสิทธิภาพ รวมไปถึงการสร้างความมั่นใจในการติดต่อระหว่างองค์กร เนื่องจากข้อมูลถือเป็นสินทรัพย์ที่มีความสำคัญเช่นเดียวกับสินทรัพย์ทางธุรกิจอื่นๆดังนั้นการรักษาความปลอดภัยข้อมูล การประเมินและการบริหารความเสี่ยงที่เกิดขึ้นจึงถือเป็นสิ่งสำคัญในการบริหารงานองค์กรให้มีประสิทธิภาพ

ปริญญา หอมเอนก (2548) กล่าวว่า มาตรฐานในการรักษาความปลอดภัยทางด้านข้อมูลสารสนเทศที่ได้รับความนิยมมากที่สุดและเป็นที่รู้จักทั่วโลกในเวลานี้คือ มาตรฐาน ISO/IEC17799 ซึ่งถูกพัฒนาต่อยอดมาจากมาตรฐาน BS7799 ซึ่งองค์กรในหลายประเทศทั่วโลก กำลังดำเนินการ Audit หรือ ตรวจสอบระบบสารสนเทศของตนเอง เพื่อที่จะให้องค์กรได้รับการรับรองมาตรฐาน BS7799 part 2 จาก CB (Certification Body) เช่น BSI (British Standard Institute) การนำมาตรฐาน ISO/IEC 17799 มาประยุกต์ใช้กับองค์กรนั้นโดยไม่จำเป็นที่ต้องได้รับ การรับรองมาตรฐาน BS7799 part 2 จาก CB เสมอไป องค์กรอาจจะนำเอามาตรฐาน ISO/IEC 17799 มาใช้เพื่อความปลอดภัยที่ดีขึ้นของระบบสารสนเทศภายในองค์กรเอง โดยนำกระบวนการทางด้าน ISMS (Information Security Management System) ประกอบไปด้วย P-D-C-A (Plan-Do-Check-Act) ที่ถูกกำหนดอยู่ใน BS7799 part 2 มาใช้ แต่หากทางองค์กรต้องการได้รับการยอมรับจากคู่ค้าหรือลูกค้าในระดับมาตรฐานโลก องค์กรก็สามารถดำเนินการเพื่อให้ได้มาซึ่งการรับรองมาตรฐาน BS7799 part 2 จาก CB ต่อไป ซึ่งโดยทั่วไปแล้ว กระบวนการเตรียมการ และ ตรวจสอบจะใช้เวลาประมาณ 6 เดือน ถึง 1 ปี ขึ้นกับขนาดของแต่ละองค์กร ขณะนี้มีองค์กรในประเทศไทยที่ได้รับการรับรองมาตรฐาน BS7799 part 2 จาก BSI แล้ว ซึ่งนับว่าเป็นองค์กรแรกในประเทศไทย ถ้าเทียบกับประเทศญี่ปุ่นที่มีจำนวนองค์กรได้รับการรับรองมาตรฐาน BS7799 part 2 มากที่สุดในโลก กว่า 900 องค์กร ยังถือว่าประเทศไทยเราเพิ่งจะเริ่มต้นเท่านั้น ข้อมูลเพิ่มเติมดูที่ http://www.xisec.com

สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ (2545) กล่าวว่า มาตรฐานด้าน ISO 17799 (BS 7799) เป็นมาตรฐานด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ ที่มีความเกี่ยวข้องกับข้อมูล

2400

โดยตรง เนื่องจากการรักษาความปลอดภัยของข้อมูลเป็นส่วนที่มีความสำคัญส่วนหนึ่ง ในการที่จะบริหารหน่วยงานให้มีประสิทธิภาพ และเป็นการนำไปสู่ความปลอดภัยให้เกิดขึ้นแก่หน่วยงาน โดยมาตรฐานดังกล่าว จะสามารถสร้างให้หน่วยงานภาครัฐของประเทศไทย สามารถก้าวไปสู่การเป็นรัฐบาลอิเล็กทรอนิกส์ที่มีความปลอดภัยสูงขึ้น นำไปสู่การลดความเสียหายต่อการดำเนินงาน ต่อบุคลากรและต่อหน่วยงานภาครัฐ ยิ่งไปกว่านั้นจะช่วยส่งผลไปสู่ระดับที่สูงยิ่งขึ้นในระดับเศรษฐกิจของประเทศ และทำให้รัฐบาลอิเล็กทรอนิกส์ของประเทศไทยเป็นที่ยอมรับในระดับสากล

จตุชัย แพงจันทร์ (2550 : 31) กล่าวว่า แม่แบบของการบริหารความปลอดภัยของข้อมูลที่ได้รับความนิยมมากที่สุด และได้กำหนดให้เป็นมาตรฐานนานาชาติคือ BS 7799 ซึ่งเป็นมาตรฐานที่มีการพัฒนาโดยประเทศอังกฤษ มาตรฐานนี้ประกอบด้วย 2 ส่วนคือ

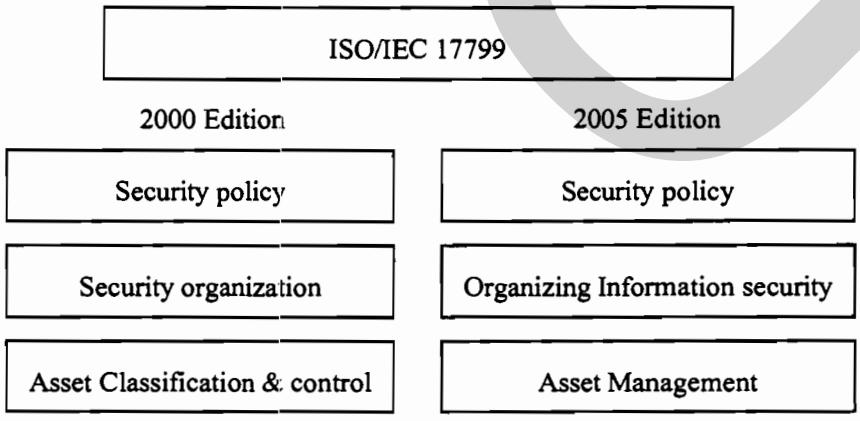
1. BS7799-1 ซึ่งต่อมาได้มีการปรับเปลี่ยนเป็นมาตรฐาน ISO/IEC 17799 : Information Technology Code of Practice for Information Security Management

2. BS7799-2 ซึ่งต่อมาได้รับการยอมรับให้เป็นมาตรฐานด้าน ISO 27001 : Information Security Management Specification with Guidance for Use

จุดมุ่งหมายของมาตรฐานนี้ ก็เพื่อต้องการให้คำแนะนำสำหรับการบริหารด้านการรักษาความปลอดภัย สำหรับผู้ที่มีหน้าที่ในการเริ่มต้นออกแบบติดตั้งและดูแลระบบในการรักษาด้านความปลอดภัยขององค์กร ซึ่งเป็นพื้นฐานสำหรับการพัฒนามาตรฐานการรักษาความปลอดภัยขององค์กรและระเบียบปฏิบัติที่มีประสิทธิภาพเพื่อสร้างความมั่นใจให้กับองค์กร และหน่วยงานอื่นที่เกี่ยวข้อง

มาตรฐาน BS 7799-1 (ISO/IEC 17799) (จตุชัย แพงจันทร์, 2550 : 31-33)

มาตรฐาน ISO/IEC 17799 เริ่มแรกได้ประกาศใช้ขึ้นเมื่อปี 2000 ซึ่งประกอบไปด้วย 10 โดเมน และต่อมาได้มีการปรับปรุงอีกครั้งเมื่อปี 2005 และปรับให้มี 11 โดเมนดังภาพที่ 2.1



ภาพที่ 2.1 เปรียบเทียบโดเมนของ ISO 17799 เวอร์ชั่น 2000 และ 2005

Personnel security	Human resources security
Physical & environmental security	Physical & environmental security
Communications & Operations Management	Communications & Operations Management
Access control	Access control
System development & maintenance	Information systems acquisition, development and maintenance
	Information security incident management
Business continuity management	Business continuity management
Compliance	Compliance

ภาพที่ 2.1 (ต่อ) เปรียบเทียบโดเมนของ ISO 17799 เวอร์ชั่น 2000 และ 2005

ที่มา: Master in Security

มาตรฐาน ISO 17799 แบ่งออกเป็น 11 โดเมน (Domain) ดังนี้

1. Security Policy-A5 (นโยบายการรักษาความปลอดภัย) เป็นสิ่งแรกที่สำคัญ และจำเป็นสำหรับองค์กรที่ต้องมีเพื่อเป็นแนวทาง และสนับสนุนการรักษาความปลอดภัยข้อมูล

2. Organizing Information Security-A6 (การจัดโครงสร้างระบบการรักษาด้านความปลอดภัยขององค์กร) มีจุดประสงค์เพื่อการบริหารความปลอดภัยของข้อมูลภายในองค์กร และดูแลควบคุมระบบการรักษาความปลอดภัยของข้อมูล และระบบที่ต้องมีการเข้า ถึงจากภายนอกองค์กร

3. Asset Management-A7 (การจัดการทรัพย์สิน) เป็นสิ่งที่มีความจำเป็นสำหรับการดูแลและควบคุมการเข้าถึงข้อมูลที่มีชั้นความลับ

4. Human Resource Security-A8 (การรักษาความปลอดภัยในระดับบุคลากร) โดยมีจุดมุ่งหมายดังนี้

- เพื่อลดความเสี่ยงที่อาจเกิดเนื่องจากความผิดพลาดของคน การขโมย การฉ้อโกง หรือหลอกลวง และการใช้งานระบบในทางที่ผิด
- เพื่อทำให้มั่นใจว่า ผู้ใช้มีความระมัดระวังเกี่ยวกับ ทางด้านภัยคุกคามต่อการรักษาความปลอดภัยของข้อมูลและมีระบบป้องกัน และรองรับนโยบายทางด้านการรักษาความปลอดภัยในการปฏิบัติงานปกติของพนักงาน
- ลดความเสียหายที่อาจเกิดขึ้นจากเหตุการณ์ การทำงานที่ผิดพลาดของระบบ และเรียนรู้จากบทเรียนต่างๆ

5. Physical and Environmental Security–A9 (การรักษาความปลอดภัยทางด้านกายภาพและสภาพแวดล้อม) มีจุดมุ่งหมายเพื่อ

- ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อจะทำลายหรือขัดขวางการดำเนินธุรกิจขององค์กร
- ป้องกันการสูญเสีย และการขัดขวางการดำเนินธุรกิจขององค์กร
- ป้องกันการขโมยข้อมูล และการใช้ทรัพยากรขององค์กร

6. Communications and Operations Management-A10 (การสื่อสารและการบริหารการปฏิบัติงาน) มีจุดมุ่งหมายดังนี้

- เพื่อทำให้แน่ใจว่าระบบจัดการข้อมูลนั้นทำงานอย่างถูกต้องและปลอดภัย
- ลดความเสี่ยงในการที่ระบบล่ม
- รักษาความคงสภาพ และมั่นคงของซอฟต์แวร์และข้อมูล
- เพื่อรักษาความคงสภาพ และความพร้อมใช้งานของระบบสื่อสารข้อมูล และระบบจัดการข้อมูล
- เพื่อป้องกันและรักษาความปลอดภัยข้อมูลบนเครือข่าย และการป้องกันโครงสร้างของระบบ
- ป้องกันการสูญเสียต่อทรัพย์สิน และการขัดขวางต่อการดำเนินธุรกิจ

- ป้องกันการสูญเสีย การดัดแปลงแก้ไข และการใช้งานข้อมูลในทางที่ผิดเมื่อต้องมีการแลกเปลี่ยนข้อมูลระหว่างองค์กร

7. Access Cotrol-A11 (การควบคุมการเข้าถึงระบบ) มีจุดมุ่งหมายเพื่อ

- ควบคุมการเข้าถึงข้อมูล
- ป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต
- ป้องกันการให้บริการทางเครือข่าย
- ป้องกันการเข้าใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต
- ตรวจจับเหตุการณ์ที่ผิดหรือไม่ได้รับอนุญาต
- รักษาความปลอดภัย เมื่อมีการใช้งานอุปกรณ์เคลื่อนที่ และการใช้งานการสื่อสารทางด้านโทรคมนาคม

8. Information systems acquisition, development and maintenance-A12 (การดูแลและพัฒนาระบบ) มีวัตถุประสงค์ดังนี้

- เพื่อให้แน่ใจว่าระบบที่พัฒนาหรือสร้างนั้นมีความปลอดภัยเพียงพอสำหรับการใช้งานจริง
- ป้องกันการสูญเสีย หรือมีการเปลี่ยนแปลงแก้ไข และการใช้งานข้อมูลในทางที่ผิดในแอพพลิเคชัน
- ป้องกันความลับ การพิสูจน์ทราบตัวตน และความคงสภาพของข้อมูล
- ทำให้แน่ใจว่าโครงการต่างๆ นั้นให้ความสำคัญกับการรักษาความปลอดภัย
- ดูแลรักษาความปลอดภัยของแอพพลิเคชันและข้อมูล

9. Information security incident management-A13 (การบริหารและจัดการเหตุการณ์ละเมิดความปลอดภัย) ซึ่งมีมาตรการ 2 ส่วนคือ

- การรายงานเหตุการณ์ จุดอ่อน หรือช่องโหว่ที่เกี่ยวข้องกับความปลอดภัย
- การบริหารและจัดการเหตุการณ์ละเมิดความปลอดภัย เพื่อให้มีความรวดเร็วและมีประสิทธิภาพ

10. Business Continuity Management-A14 (การบริหารความต่อเนื่องของธุรกิจ) เพื่อป้องกันเหตุการณ์ที่จะขัดขวางการดำเนินธุรกิจจากเหตุการณ์ล้มเหลวขนาดใหญ่หรือภัยธรรมชาติ

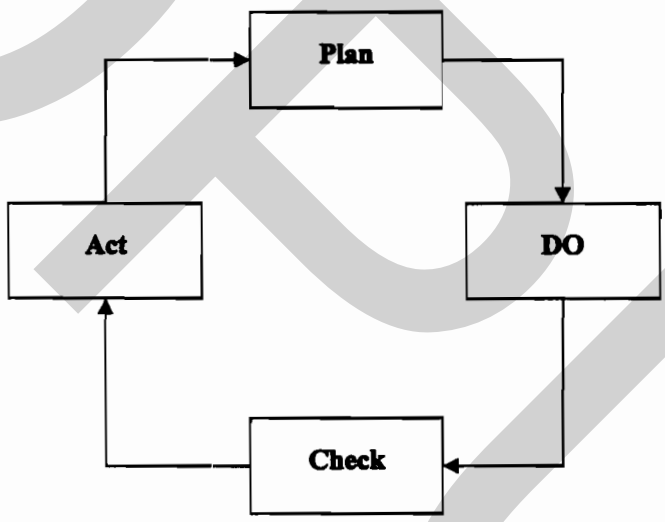
11. Compliance-A15 (ไม่ขัดต่อกฎหมาย) มีวัตถุประสงค์เพื่อ

- ป้องกันการขัดต่อกฎหมายแพ่งและอาญา กฎ ระเบียบ และสัญญาต่างๆ
- เพื่อทำให้แน่ใจว่าระบบนั้น ไม่ขัดต่อนโยบายการรักษาความปลอดภัย ขององค์กรหรือมาตรฐาน

- เพื่อให้เพิ่มประสิทธิภาพของระบบตรวจสอบและลดการรบกวนต่อการปฏิบัติงานในปกติ

มาตรฐาน BS 7799-2 (ISO 27001) (จตุชัย แพงจันทร์, 2550 : 34-35)

เป็นมาตรฐานเกี่ยวกับการบริหารการรักษาความปลอดภัยข้อมูล และเป็นแนวทางในการสร้าง ดูแล และปรับปรุงระบบบริหารการรักษาความปลอดภัยข้อมูล (The Information Security Management System (ISMS)) โดยใช้โมเดลการบริหารแบบ Plan-Do-Check-Act (PDCA) มาช่วยในการสร้างและพัฒนาระบบการรักษาความปลอดภัย ดังนั้นมาตรฐาน ISO/IEC 27001 จึงเป็นแนวทางพื้นฐานเพื่อที่จะสร้างระบบควบคุม เพื่อให้บรรลุภารกิจขององค์กร เพื่อให้สามารถบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และเพื่อให้แน่ใจว่าระบบนั้นควรได้รับการปรับปรุงเมื่อถึงเวลา



ภาพที่ 2.2 กระบวนการ Plan-Do-Check-Act

ที่มา: Master in Security

กระบวนการจัดทำ Plan มีดังนี้

1. กำหนดขอบเขตของ ISMS
2. กำหนดนโยบายของ ISMS
3. กำหนดวิธีการประเมินความเสี่ยง
4. ระบุความเสี่ยง
5. ประเมินความเสี่ยง

6. วิเคราะห์หนทางในการแก้ปัญหาความเสี่ยง
7. กำหนดวัตถุประสงค์ในการควบคุมและมาตรการในการควบคุม
8. เตรียมการแถลงแนวทางในการประยุกต์ใช้

กระบวนการจัดทำ Do มีดังนี้

1. กำหนดแผนการกำจัดความเสี่ยง
2. ปฏิบัติตามแผนลดความเสี่ยง
3. ติดตั้งระบบควบคุม
4. ฝึกอบรมพนักงานเพื่อให้ระวัง
5. บริหารการปฏิบัติการ
6. บริหารทรัพยากร
7. กำหนดขั้นตอนการปฏิบัติเพื่อตรวจจับและตอบโต้ เมื่อเกิดเหตุการณ์ที่เกี่ยวกับความปลอดภัย

กระบวนการจัดทำ Check มีดังนี้

1. ปฏิบัติตามขั้นตอนการเฝ้าระวัง
2. ตรวจพิจารณาว่า ISMS มีประสิทธิภาพเพียงพอหรือไม่
3. ตรวจพิจารณาว่าความเสี่ยงยังอยู่ในระดับที่ยอมรับได้หรือไม่
4. ตรวจสอบ ISMS ภายใน
5. ตรวจพิจารณาการบริหารงานปกติของ ISMS
6. บันทึกการปฏิบัติ และเหตุการณ์ที่มีผลกระทบต่อ ISMS

กระบวนการจัดทำ Act มีดังนี้

1. ปรับปรุงส่วนที่มีปัญหา
2. แก้ไขปัญหาที่เกิดขึ้น และป้องกันไม่ให้เกิดขึ้นอีก
3. ประยุกต์ใช้เกี่ยวกับบทเรียนที่ได้รับ
4. เผยแพร่บทเรียนที่ได้รับให้กับผู้ที่เกี่ยวข้อง
5. ทำให้แน่ใจว่าการปรับปรุงระบบนั้นบรรลุวัตถุประสงค์ที่ตั้งไว้

มาตรฐาน BS 7799-3 (จตุชัย แพงจันทร์, 2550 : 35)

เป็นมาตรฐานที่ใช้เป็นแนวทางในการบริหารความเสี่ยงทางด้านการรักษาความปลอดภัยข้อมูล และเป็นแนวทางในการจัดทำมาตรฐาน BS 7799-2 และเหมาะสำหรับองค์กรทุกขนาด โดยเนื้อหาที่สำคัญของมาตรฐานนี้ประกอบด้วย

1. ความเสี่ยงเกี่ยวกับความปลอดภัยของข้อมูลในองค์กร
2. การประเมินความเสี่ยง
3. วิธีปฏิบัติเพื่อลดความเสี่ยงและการบริหารการตัดสินใจ
4. การดำเนินกิจกรรมเกี่ยวกับการบริหารความเสี่ยง

มาตรฐาน BS 7799-3 นี้ต้องทำควบคู่อย่างใกล้ชิดกับมาตรฐาน ISO 17799 และ ISO 27001 เพื่อทำให้แน่ใจว่ากระบวนการรักษาความปลอดภัยนั้นกระทำอย่างต่อเนื่อง

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2) ประจำปี 2549

ในประเทศไทย คณะทำงาน คณะอนุกรรมการความมั่นคงภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ถูกจัดตั้งขึ้นตามพระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้นำเอามาตรฐาน ISO 17799 มาเป็นแนวทางในการกำหนดมาตรฐานการรักษาความปลอดภัยทางด้านอิเล็กทรอนิกส์ โดยมีการปรับเปลี่ยนให้มีความเหมาะสมกับสภาวะแวดล้อม และสถานการณ์ทางด้านเทคโนโลยีสารสนเทศในประเทศไทย และปัจจุบัน มาตรฐาน ISO 17799 ได้มีการปรับปรุงถึงฉบับ Second Edition ซึ่งการจัดทำหนังสือ "มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2) ประจำปี 2549" โดยมีข้อมูลแหล่งที่มาจาก http://www.thaicert.nectec.or.th/event/SecurityStandard/SecurityStandardV2-2549.pdf จะมีเนื้อหาที่สอดคล้องกับมาตรฐานสากล ISO/IEC 17799 ซึ่งในปัจจุบันมาตรฐาน ISO/IEC 17799:2000 ได้รับการปรับปรุงให้ทันสมัยมากยิ่งขึ้น โดยให้มีความสอดคล้องกับเนื้อหาใหม่ ของมาตรฐาน ISO/IEC 17799:2005 ที่ได้รับการปรับปรุงเพิ่มเติม ซึ่งประกอบด้วยมาตรการป้องกันทั้งหมด 133 ข้อ ภายใต้ 39 วัตถุประสงค์ และเพื่อให้มีความเหมาะสมสำหรับการนำไปใช้เป็นแนวทางการศึกษาเพื่อสร้างความมั่นคงปลอดภัย อีกทั้งยังช่วยเอื้อประโยชน์เป็นอย่างมาก ให้กับภารกิจด้านการเสริมสร้างความมั่นคงปลอดภัย ให้กับระบบสารสนเทศต่าง ๆ ขององค์กรทั้งภาครัฐและเอกชน

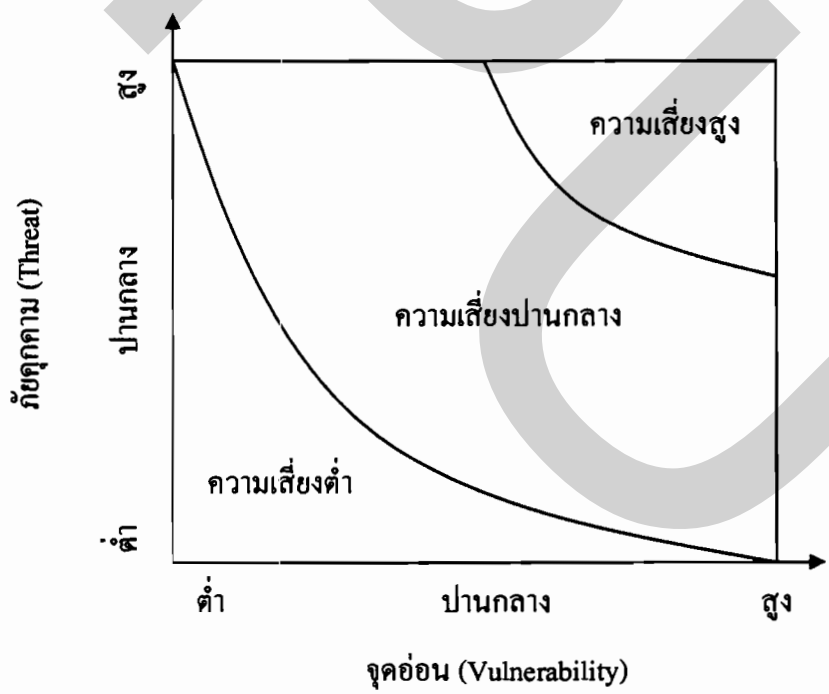
2.4 การบริหารความเสี่ยง (จตุชัย แพงจันทร์, 2550 : 39-40)

การรักษาความปลอดภัยของข้อมูลเป็นกระบวนการในเชิงรุกเพื่อบริหารความเสี่ยง แต่ที่ผ่านมาโดยส่วนใหญ่แล้ว การรักษาความปลอดภัยนั้น จะเป็นแบบเชิงรับ กล่าวคือองค์กรจะรอให้มีเหตุการณ์เกิดขึ้นก่อนแล้วค่อยหาวิธีการที่จะป้องกันเหตุการณ์นั้น ซึ่งการทำในลักษณะเช่นนี้อาจเกิดความเสียหายกับองค์กรมากเกินคาดก็ได้ โดยการจัดการในเชิงรุกนั้น เป็นขั้นตอนที่ทำก่อนที่จะเกิดเหตุการณ์ขึ้น ถ้าการรักษาความปลอดภัยนั้นเป็นแบบเชิงรับ ค่าใช้จ่ายสำหรับระบบการรักษาความ

ปลอดภัยนั้น ไม่สามารถประเมินได้ อย่างไรก็ตามค่าความเสียหายเมื่อเกิดเหตุการณ์นั้นไม่สามารถทราบได้จนกว่าจะเกิดเหตุการณ์ขึ้นก่อน และเนื่องจากองค์กรไม่ได้เตรียมการไว้ล่วงหน้า ก่อนที่จะเกิดเหตุการณ์ จึงทำให้ไม่สามารถทราบได้ถึงความเสียหายจากเหตุการณ์นั้น ดั้งนั้นความเสี่ยงขององค์กรไม่อาจทราบได้จนกว่าจะเกิดเหตุการณ์ขึ้นจริงๆ ซึ่งการรักษาด้านความปลอดภัยนั้น จะมีส่วนเกี่ยวข้องกับการบริหารความเสี่ยงอย่างใกล้ชิด ถ้าไม่มีความเข้าใจเกี่ยวกับความเสี่ยงขององค์กรแล้ว การใช้ทรัพยากรขององค์กรเพื่อการรักษาความปลอดภัยนั้นอาจมากเกินความจำเป็น หรือน้อยกว่าที่ควรจะเป็นก็ได้ นอกจากนี้การประเมินความเสี่ยงก็อาจใช้เป็นพื้นฐาน สำหรับการประเมินค่าของทรัพย์สินขององค์กรไปพร้อมกันได้ด้วย

ความเสี่ยง (Risk) (จตุชัย แพงจันทร์, 2550 : 41-42)

เป็นพื้นฐานที่ทำให้ต้องมีการรักษาความปลอดภัย (Security) ความเสี่ยงคือ ความเป็นไปได้ที่มีการสูญเสียบางสิ่งที่ปกป้องอยู่ ถ้าไม่มีความเสี่ยงก็ไม่จำเป็นต้องมีการรักษาความปลอดภัย เมื่อมีการประเมินความเสี่ยง จึงมีความจำเป็นที่จะต้องเข้าใจถึงจุดอ่อนหรือช่องโหว่ (Vulnerability) และภัยคุกคาม (Threat) ขององค์กร เมื่อรวมจุดอ่อนเข้ากับภัยคุกคาม ก็จะกลายเป็นความเสี่ยง ถ้าไม่มีจุดอ่อนก็จะไม่มีความเสี่ยงหรือถ้าไม่มีภัยคุกคามก็จะไม่มีความเสี่ยงเช่นกัน



ภาพที่ 2.3 ความสัมพันธ์ระหว่างความเสี่ยง จุดอ่อน และภัยคุกคาม

ที่มา: Master in Security

จุดอ่อนหรือช่องโหว่ (Vulnerability) (จตุชัย แพงจันทร์, 2550 : 42)

เป็นช่องทางที่สามารถใช้สำหรับการโจมตีได้ ซึ่งจุดอ่อนหรือช่องโหว่ อาจมีอยู่ภายในระบบคอมพิวเตอร์และเครือข่าย โดยเป็นช่องทางโอกาสที่ให้ผู้ไม่ประสงค์ดี สามารถเจาะเข้าระบบหรือเครือข่ายได้ จุดอ่อนนั้นมีหลายระดับขึ้นอยู่กับความยากง่าย และระดับของความชำนาญทางด้านเทคนิคที่จะสามารถใช้ประโยชน์จากมันได้ นอกจากนี้ผลกระทบที่เกิดขึ้น จากการใช้ประโยชน์จากจุดอ่อนดังกล่าวก็จะนับรวมเข้าไปด้วย ยกตัวอย่างเช่น จุดอ่อนประเภทที่ง่ายต่อการเจาะเข้า ซึ่งอาจเป็นเพราะสคริปต์ (Script) ที่ใช้สำหรับเจาะเข้าระบบนั้นหาได้ง่าย และเมื่อทำสำเร็จผู้บุกรุกสามารถควบคุมระบบได้ทั้งหมด จุดอ่อนประเภทนี้ก็จะจัดว่ามีความอันตรายในระดับสูง ในทางตรงกันข้ามถ้าเป็นจุดอ่อนประเภทที่ต้องใช้ความชำนาญสูง และอาจต้องใช้ทรัพยากรจำนวนมากในการเจาะเข้าระบบ ถ้าเจาะเข้าระบบได้แล้ว แต่ได้ข้อมูลที่ไม่ถือว่าสำคัญมากนัก จุดอ่อนประเภทเหล่านี้ก็ถือได้ว่ามีอันตรายในระดับต่ำ จุดอ่อนนั้นไม่ได้มีกับเฉพาะระบบคอมพิวเตอร์ และระบบเครือข่ายเท่านั้นแต่จะรวมถึงทางด้านกายภาพ พนักงานและข้อมูล หรือทรัพย์สิน ที่ไม่ได้อยู่ในรูปแบบอิเล็กทรอนิกส์ด้วย

ภัยคุกคาม (Threat) (จตุชัย แพงจันทร์, 2550 : 43-44)

เป็นสิ่งที่อาจเกิดขึ้นและมีอันตรายต่อทรัพย์สินขององค์กร ภัยคุกคามนั้นประกอบด้วย 3 ส่วนคือ

1. เป้าหมาย (Target) เป้าหมายของการโจมตีในที่นี้ หมายถึง องค์ประกอบด้านต่างๆ ของการรักษาความปลอดภัยที่กล่าวถึงคือ ความลับ ความคงสภาพ และความพร้อมใช้งาน ซึ่งภัยคุกคามแต่ละด้านนั้นขึ้นอยู่กับเหตุผลหรือแรงจูงใจ

ความลับ (Confidentiality) ในการรักษาความลับของข้อมูลต่างๆ ภายในหน่วยงาน ซึ่งอาจกระทำได้หลากหลายวิธีด้วยกัน ไม่ว่าจะเป็น การกำหนดสิทธิ์การเข้าถึงข้อมูล เนื่องจากข้อมูลมีความสำคัญและไม่สามารถเปิดเผยให้รับทราบโดยทั่วกันได้และจะเป็นเป้าหมายก็ต่อเมื่อความลับของข้อมูลถูกเปิดเผยต่อผู้ที่ไม่ได้รับอนุญาต ซึ่งในกรณีเช่นนี้ก็เกิดขึ้นเนื่องจากบางคนอาจต้องการทราบข้อมูลที่ห้ามคนอื่นทราบ เช่น ความลับทางราชการ ความลับทางธุรกิจ และข้อมูลส่วนบุคคลเป็นต้น อย่างไรก็ตามข้อมูลที่เป็นข้อมูลส่วนบุคคลที่เก็บไว้โดยเฉพาะในองค์กรทางธุรกิจ ก็อาจจะกลายเป็นเป้าหมายได้เช่นกัน

ความคงสภาพ (Integrity) เป็นความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล โดยจำเป็นต้องให้มีการกำหนดมาตรการ หรือแนวทางในการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล เพื่อไว้ป้องกันความผิดพลาด หรือการเข้าแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต ซึ่งจะตกเป็นเป้าหมายเมื่อภัยคุกคามนั้น

พยายามที่จะเปลี่ยนแปลงข้อมูล ผู้บุกรุกในกรณีนี้พยายามที่จะเปลี่ยนแปลงข้อมูลของคนอื่น หรือหลอกลวงให้เชื่อว่าข้อมูลที่ให้ไปถูกต้อง

ความพร้อมใช้งาน (Availability) เป็นความพร้อมสำหรับผู้มีสิทธิ์ในการเข้าถึงข้อมูลในระบบต่างๆ ของหน่วยงาน ต้องสามารถเข้าใช้ข้อมูลได้ในช่วงเวลาที่ต้องการอย่างต่อเนื่อง โดยไม่เกิดเหตุขัดข้อง ซึ่งจะเป็นเป้าหมายเมื่อมีการโจมตีแบบปฏิเสธการให้บริการ โดยการโจมตีนี้ก็อาจมีเป้าหมายเป็นข้อมูลระบบที่ให้บริการข้อมูล หรือเป็นโครงสร้างข้อมูลขององค์กร ซึ่งในการโจมตีนั้นอาจมีเป้าหมายเพื่อทำลายคุณสมบัติของข้อมูล และทรัพย์สินทางด้านสารสนเทศทั้ง 3 ด้านคือ ความลับ ความคงสภาพ และความพร้อมใช้งาน

2. ผู้โจมตี (Agent) เป็นผู้ที่กระทำการใดๆ ที่ก่อให้เกิดผลทางด้านลบกับองค์กร โดยต้องสามารถเข้าถึงระบบ สถานที่ หรือข้อมูลที่ต้องการ ซึ่งองค์ประกอบที่สำคัญของการเข้าถึงคือ โอกาส โอกาสนั้นเกิดขึ้นกับสถานที่หรือเครือข่ายได้เช่น เพียงแค่พนักงานเปิดประตูทิ้งไว้

ผู้โจมตีนั้นจำเป็นต้องมีความรู้หรือข้อมูลเกี่ยวกับเป้าหมาย เช่น บัญชีผู้ใช้ รหัสผ่าน ที่อยู่ หรือหมายเลขไอพี ระบบรักษาความปลอดภัย เป็นต้น ผู้โจมตียิ่งมีข้อมูลเกี่ยวกับเป้าหมายมากเท่าใด ยิ่งทำให้ผู้โจมตีมีความรู้เกี่ยวกับจุดอ่อน หรือช่องโหว่ของเป้าหมายมากขึ้นเท่านั้น และผู้โจมตีก็ยิ่งมีโอกาสที่จะรู้วิธีในการใช้ประโยชน์จากจุดอ่อนเหล่านั้นได้ง่าย

ผู้โจมตีนั้นต้องมีแรงจูงใจที่จะกระทำต่อเป้าหมาย ซึ่งแรงจูงใจเป็นคุณสมบัติที่สำคัญที่ควรพิจารณาเพราะจะเป็นสิ่งที่บอกถึงเป้าหมายหลัก สิ่งที่ต้องควรพิจารณาประกอบด้วย ความท้าทาย ความอยากได้ และความตั้งใจที่จะทำอันตรายต่อองค์กรหรือบุคคลใดบุคคลหนึ่ง

ภัยคุกคามเกิดขึ้นเมื่อ ผู้โจมตีมีความรู้เกี่ยวกับเป้าหมายที่ต้องการ และสามารถเข้าถึงได้ด้วยแรงจูงใจ ซึ่งผู้โจมตีอาจเป็นบุคคลดังต่อไปนี้

พนักงาน ซึ่งสามารถเข้าถึงระบบ และมีความรู้ทางด้านที่เกี่ยวกับระบบ เพราะเป็นสิ่งที่จำเป็นสำหรับการทำงาน

พนักงานเก่า ซึ่งคุ้นเคยกับระบบเป็นอย่างดี เนื่องจากคุ้นเคยโดยการทำงานที่นั่นมาก่อน บางบริษัทหรือองค์กรนั้นอาจมีกระบวนการที่ยังหละหลวมอยู่ และเมื่อพนักงานออกจากงาน ทำให้พนักงานเก่าบางคนที่ออกไปแล้วอาจยังมีสิทธิ์ที่จะสามารถเข้าถึงระบบได้

แฮคเกอร์ เป็นบุคคลที่มีแรงจูงใจที่จะทำอันตรายให้บริษัทเสมอ จะด้วยความสามารถในระดับใดก็แล้วแต่ แฮคเกอร์นั้นอาจจะมีหรือไม่มีความรู้ หรือมีข้อมูลเกี่ยวกับระบบ และเครือข่ายขององค์กรก็ได้ การเข้าถึงระบบนั้นอาจผ่านช่องโหว่ หรือจุดอ่อนที่ระบบยังคงมีอยู่ได้

ศัตรูหรือคู่แข่ง เป็นกลุ่มที่ต้องการจะรู้ข้อมูลขององค์กรเสมอ เช่นคู่แข่งทางด้านการค้าอาจต้องการทำลายศักยภาพของคู่แข่งเพื่อให้ได้เปรียบทางด้านการค้า

3. เหตุการณ์ (Event) เป็นวิธีการที่ผู้โจมตีอาจทำอันตรายต่อองค์กร เช่น แฮคเกอร์อาจทำอันตรายโดยการแก้ไขหน้าเว็บไซต์ขององค์กร ได้แก่

- การบุกรุกเข้าห้องควบคุมโดยไม่ได้รับอนุญาต
- การทำลายระบบโดยไม่ได้ตั้งใจ
- การเจาะเข้าระบบโดยไม่ได้รับอนุญาต
- การแก้ไขข้อมูลที่สำคัญทั้งที่ตั้งใจและไม่ตั้งใจ
- การใช้บัญชีผู้ใช้ในทางที่ผิด หรือเกินกว่าที่ได้รับอนุญาต

กระบวนการในการรักษาความปลอดภัยข้อมูล (จตุชัย แพงจันทร์, 2550 : 45-67)

เป็นกระบวนการที่ต้องทำอย่างต่อเนื่อง ประกอบด้วย 5 ขั้นตอนหลักดังนี้คือ

1. การประเมินความเสี่ยง (Risk Assessment) เพื่อแนะนำแนวทางที่ใช้ในการประเมินภัยคุกคาม และความเสี่ยงขององค์กร เพื่อตอบคำถามต่าง ๆ เช่น เราต้องการจะปกป้องอะไรบ้าง ใครหรืออะไรที่เป็นภัยคุกคาม จุดอ่อน หรือช่องโหว่ หรือจะเกิดความเสียหายมากน้อยเท่าใดเมื่อถูกโจมตีจุดอ่อน หรือช่องโหว่เหล่านั้น หรือมูลค่าทรัพย์สินขององค์กรมีอะไรบ้างและเท่าไร และเราจะป้องกันหรือแก้ไขช่องโหว่ หรือจุดอ่อนได้อย่างไร

ผลที่ได้จากการประเมินความเสี่ยง คือข้อแนะนำเกี่ยวกับวิธีป้องกัน เพื่อปกป้องความลับ ความคงสภาพ และความพร้อมใช้งาน และยังคงสามารถทำงานและให้บริการได้ปกติ การประเมินความเสี่ยงสามารถทำได้ โดยการใช้ทรัพยากรภายในหรือภายนอกก็ได้และต้องอาศัยความร่วมมือกันในทุกฝ่าย ถ้าไม่ได้รับความร่วมมือ อาจทำให้การประเมินความเสี่ยงไม่ได้ผลหรือไม่มีประสิทธิภาพ ซึ่งขั้นตอนที่สำคัญของการประเมินความเสี่ยงมี 6 ข้อดังนี้คือ

1.1 การกำหนดขอบเขต เป็นขั้นตอนที่สำคัญที่สุดของกระบวนการ ในการประเมินความเสี่ยง เนื่องจากขอบเขตเป็นสิ่งที่กำหนดว่าอะไรที่จะทำหรือไม่ทำในระหว่างการประเมิน และเป็นการระบุว่าอะไรที่เราจะปกป้อง ความสำคัญของสิ่งที่เราพยายามจะปกป้อง และจะต้องปกป้องถึงระดับไหนและละเอียดเพียงใด นอกจากนี้การกำหนดขอบเขต ยังเกี่ยวข้องกับว่าระบบใด หรือแอพพลิเคชันใดที่จะถูกประเมินบ้าง

1.2 เก็บรวบรวมข้อมูล ขั้นตอนนี้เป็นการรวบรวมนโยบาย และระเบียบปฏิบัติที่มีประกาศใช้อยู่ในปัจจุบันและบอกได้ว่าอะไรที่หายไปหรือไม่ได้มีการเก็บไว้ในรูปแบบของเอกสาร การสัมภาษณ์ หรือสนทนากับบุคคลหลักๆ ขององค์กรซึ่งอาจช่วยให้ได้ข้อมูลเกี่ยวกับด้านนี้ได้

1.3. วิเคราะห์นโยบายและระเบียบปฏิบัติ สำหรับการทบทวน และวิเคราะห์นโยบายและระเบียบปฏิบัติขององค์กรที่ประกาศใช้งานในปัจจุบัน เป็นการตรวจสอบดูว่าองค์กรนั้นจัดอยู่ในระดับใดของมาตรฐานความปลอดภัย มาตรฐานความปลอดภัยที่นิยมคือ ISO 17799 (BS 7799) อีกทั้งควรตรวจสอบว่า ส่วนใดขององค์กรที่ไม่ได้ตามมาตรฐาน และควรจะวิเคราะห์ดูว่ามีความจำเป็นที่จะต้องทำให้ได้ตามมาตรฐานหรือไม่ เนื่องจากมาตรฐานทางด้านการรักษาความปลอดภัยนั้นมีอยู่ค่อนข้างมากและส่วนใหญ่จะเป็นมาตรฐานที่ใช้กับองค์กรทั่วไปโดยมาตรฐานเหล่านี้อาจไม่ได้มีการคำนึงถึงลักษณะเฉพาะของแต่ละองค์กร ดังนั้น บางมาตรฐานก็ไม่จำเป็น แต่สำหรับบางองค์กรก็อาจต้องทำมากกว่าที่มาตรฐานกำหนดก็ได้

1.4. วิเคราะห์ภัยคุกคาม (Threat Analysis)

1.5. วิเคราะห์จุดอ่อนหรือช่องโหว่ (Vulnerability Analysis) ทั้งนี้โดยมีจุดประสงค์ของการวิเคราะห์ช่องโหว่ (Vulnerability Analysis) ก็เพื่อเป็นการทดสอบสถานภาพขององค์กร ในปัจจุบันว่าล่อแหลมต่อการถูกโจมตี หรือถูกทำลายมากน้อยแค่ไหน หรือเป็นการทดสอบการรักษาความลับ ความคงสภาพ และความพร้อมใช้งานของข้อมูลที่สำคัญขององค์กร และนอกจากนี้ยังเป็นการทดสอบว่าเครื่องมือหรือระบบที่ใช้สำหรับป้องกัน และรักษาความปลอดภัยนั้น มีประสิทธิภาพเพียงพอหรือไม่

ปัญหาส่วนใหญ่ที่เกิดจากการใช้เครื่องมือเหล่านี้ คือการวิเคราะห์ข้อมูลที่ได้ เนื่องจากเครื่องมือส่วนใหญ่จะรายงานข้อมูลไม่สมบูรณ์มากนัก ยังต้องอาศัยการวิเคราะห์จากผู้ที่ใช้เครื่องมือเหล่านี้ ดังนั้นผู้ที่ใช้เครื่องมือเหล่านี้ จำเป็นที่จะต้องมีความรู้ที่เกี่ยวกับเรื่องการรักษาความปลอดภัยค่อนข้างมาก และในขั้นตอนของการวิเคราะห์ความเสี่ยงนี้ จะรวมถึงการทดลองเจาะเข้าระบบด้วยเพื่อทดสอบว่าระบบมีความปลอดภัยมากน้อยแค่ไหน ซึ่งในการทดสอบนั้นอาจจะเพื่อค้นหาข้อมูลที่สำคัญ เช่น ไฟล์ที่เก็บรหัสผ่าน ข้อมูลที่มีชั้นความลับสูง เป็นต้น การทดสอบเจาะเข้าระบบนั้นแบ่งออกเป็น 2 ประเภท คือ การทดสอบเจาะเข้าระบบโดยมีข้อมูลที่เกี่ยวกับบางระบบ และการเจาะระบบโดยเริ่มจากการไม่มีข้อมูลเกี่ยวกับระบบเลย ซึ่งการเจาะประเภทแรกนั้น มักจะทำโดยเริ่มจากเครือข่ายภายใน โดยสมมติว่า ผู้ที่พยายามเจาะระบบนั้นเป็นพนักงานขององค์กรที่พอมีความรู้ หรือข้อมูลเกี่ยวกับระบบหรือเครือข่ายขององค์กร ส่วนประเภทที่สองนั้น เป็นการทดลองเจาะระบบจากภายนอก โดยสมมติว่าเป็นผู้ใช้ทั่วไปที่ไม่มีความรู้ หรือข้อมูลเกี่ยวกับองค์กรมากนัก

ช่องโหว่หรือจุดอ่อนที่ค้นพบนั้น สามารถจะจัดระดับความเสี่ยงต่อองค์กรทั้งจากภายในและภายนอก จุดอ่อนที่มีระดับความเสี่ยงต่ำ หมายถึง จุดอ่อนที่มีความรุนแรงต่ำ และความเปิดเผย (Exposure) ต่ำ จุดอ่อนที่มีความเสี่ยงสูงหมายถึง จุดอ่อนที่อาจก่อให้เกิดความเสียหายต่อระบบสูง

หรือมีระดับความรุนแรงสูงและโจมตีง่าย โดยการจัดระดับความเสี่ยงของช่องโหว่หรือจุดอ่อนที่ถูกค้นพบก็จะช่วยลำดับความสำคัญว่าช่องโหว่หรือจุดอ่อนไหนจำเป็นที่ต้องแก้ไขหรือป้องกันก่อน

1.6. ประเมินความเสี่ยง กระบวนการรักษาความปลอดภัยของข้อมูล มีการเริ่มต้น ที่การประเมินความเสี่ยงหรือการประเมินสถานการณ์ การประเมินความเสี่ยงนั้น จะตอบคำถามที่ว่าเราอยู่ตรงไหน และเรากำลังจะไปที่ไหน การประเมินค่าความเสี่ยงนั้น จะรวมถึงการประเมินมูลค่าของทรัพย์สินประเภทข้อมูลขององค์กร ค่าความเสี่ยงของภัยและช่องโหว่ หรือจุดอ่อนของระบบที่อาจทำให้เกิดภัยกับข้อมูลเหล่านั้นได้ และความเสี่ยงโดยรวมขององค์กร ซึ่งเป็นขั้นตอนที่สำคัญเนื่องจากถ้าไม่ทราบสถานการณ์ปัจจุบันเกี่ยวกับความเสี่ยงต่อองค์กรก็ไม่สามารถติดตั้ง และใช้งานเครื่องมือสำหรับป้องกัน และรักษาความปลอดภัยให้ทรัพย์สินขององค์กรได้ และในการประเมินควรคำนึงถึงปัจจัยต่าง ๆ ที่มีส่วนเกี่ยวข้องดังนี้

1.6.1 การประเมินค่านั้นสามารถทำได้ โดยทำตามขั้นตอนการบริหารความเสี่ยง หลังจากที่สามารถระบุความเสี่ยงต่อภัยและค่าความเสียหายจากภัยนั้นแล้ว เราก็สามารถจะเลือกใช้เครื่องมือหรือระบบป้องกันที่เหมาะสม และมีประสิทธิภาพเพื่อป้องกันภัยต่าง ๆ เหล่านั้นได้ โดยจุดมุ่งหมายของการประเมินค่าความเสี่ยงภัยของข้อมูลนั้นประกอบด้วย

- เพื่อประเมินค่าของทรัพย์สินประเภทข้อมูล
- เพื่อประเมินค่าความเสี่ยงภัยที่มีต่อความลับ ความคงสภาพ และความพร้อมใช้งานของทรัพย์สินข้อมูล
- เพื่อตรวจสอบและค้นหาจุดอ่อน หรือช่องโหว่ของระบบในขณะนั้น
- เพื่อประเมินความเสี่ยงขององค์กรที่เกี่ยวกับทรัพย์สินประเภทข้อมูล
- เพื่อแนะนำวิธีปฏิบัติต่อข้อมูล สำหรับช่วยลดความเสี่ยง ให้อยู่ในระดับที่สามารถยอมรับได้
- เพื่อใช้เป็นข้อมูลที่เกี่ยวข้องกับการวางรากฐาน ใช้ในการสร้างระบบการรักษาความปลอดภัย

1.6.2 การประเมินสถานการณ์ในปัจจุบันขององค์กรนั้น แบ่งออกได้ดังนี้

- การวิเคราะห์ความเสี่ยงอยู่ในระดับระบบ (System-Level Vulnerability) เป็นการประเมินเพื่อหาจุดอ่อนของคอมพิวเตอร์แต่ละเครื่องที่ใช้งานในองค์กร ซึ่งเป็นการตรวจสอบระบบเพื่อให้ทราบว่าระบบดังกล่าว สามารถบังคับให้เป็นไปตามนโยบายการรักษาความปลอดภัยในขณะนั้นหรือไม่

- การวิเคราะห์ความเสี่ยงที่อยู่ในระดับของเครือข่าย (Network-Level risk Assessment) เป็นการประเมินค่าความเสี่ยงต่อภัยต่าง ๆ ของระบบคอมพิวเตอร์ และเครือข่าย ทั่วทั้งองค์กร รวมถึงโครงสร้างระบบการจัดการข้อมูลขององค์กร

- การวิเคราะห์ความเสี่ยงในระดับขององค์กร (Organization-Wide Risk Assessment) เป็นการวิเคราะห์และประเมินความเสี่ยงของทั้งองค์กรโดยรวม เพื่อที่จะระบุถึงภัยต่อข้อมูลขององค์กรโดยตรง เพื่อวิเคราะห์และค้นหาจุดอ่อนของการปฏิบัติ และการจัดการข้อมูลขององค์กร โดยจะต้องเก็บข้อมูลที่จัดเก็บในทุกรูปแบบ ไม่ว่าจะเป็นการจัดเก็บทางด้านกายภาพ เช่น บนกระดาษ หรือในรูปแบบของอิเล็กทรอนิกส์ในระบบคอมพิวเตอร์

- การตรวจสอบ (Audit) จะเป็นการตรวจสอบที่เกี่ยวกับนโยบายทางด้านการรักษาความปลอดภัย และตรวจวิเคราะห์ว่าองค์กรได้ปฏิบัติ หรือมีการบังคับใช้นโยบายเหล่านั้นหรือไม่

- การทดสอบเจาะเข้าระบบ (Penetration Test) จะเป็นการทดสอบการเจาะเข้าระบบ เพื่อทดสอบความสามารถขององค์กรในการตอบโต้ต่อการบุกรุก โดยการทดสอบประเภทนี้ควรทำกับเฉพาะองค์กรที่มีระบบการรักษาความปลอดภัยค่อนข้างแข็งแกร่ง เพราะการทดลองเจาะเข้าระบบอาจสร้างความเสียหายให้องค์กรได้

1.6.3 ในการประเมินองค์กรนั้น เราควรเก็บรวบรวมข้อมูลจาก 3 แหล่ง คือ พนักงาน เอกสาร และจากการสำรวจตามสภาพจริง ต้องมีการสัมภาษณ์พนักงานที่ทำงานเกี่ยวกับด้านการรักษาความปลอดภัย และผู้ที่เข้าใจและรู้เรื่องเกี่ยวกับลักษณะงานขององค์กรนั้น ๆ การสัมภาษณ์ทั้งผู้บริหารและพนักงานที่ปฏิบัติงานจริง ก็จะได้ข้อมูลที่ต่างมุมกัน ในการสัมภาษณ์นั้นไม่ควรทำให้ผู้ที่ถูกสัมภาษณ์นั้นรู้สึกเหมือนว่าตัวเองกำลังถูกตรวจสอบอยู่ โดยก่อนสัมภาษณ์ควรอธิบายให้ผู้ที่ถูกสัมภาษณ์นั้นเข้าใจถึงจุดประสงค์ของการประเมิน และอธิบายได้ว่าผลที่ได้นั้นจะมีส่วนช่วยในการป้องกัน และรักษาความปลอดภัยให้ทรัพย์สินขององค์กรได้อย่างไร นอกจากนี้ควรอธิบายว่าข้อมูลที่ได้จากการสัมภาษณ์นั้นจะไม่ระบุชื่อของผู้ให้สัมภาษณ์ หรือจะไม่มีผลในด้านลบต่อผู้ที่ถูกสัมภาษณ์โดยตรง

2. กำหนดนโยบาย (Policy) นโยบายและระเบียบปฏิบัติจัดเป็นขั้นตอนต่อไป หลังจากที่ได้ประเมินสถานการณ์ด้านความเสี่ยงไปแล้ว นโยบายและระเบียบปฏิบัตินับเป็นสิ่งที่จะกำหนดถึงระดับความปลอดภัยขององค์กรที่คาดหวังไว้ และเป็นสิ่งที่กำหนดงานที่ต้องทำ ในระหว่างขั้นตอนการติดตั้งระบบด้านการรักษาความปลอดภัย ถ้าไม่มีนโยบายก็จะไม่มีแผนสำหรับองค์กร ที่จะทำให้การรักษาความปลอดภัยขององค์กรมีประสิทธิภาพได้ อย่างน้อยที่สุดนโยบายและระเบียบการปฏิบัติดังต่อไปนี้ควรมีในแต่ละองค์กรสำหรับขั้นตอนการรักษาความปลอดภัย

- นโยบายข้อมูล (Information Policy) ควรกำหนดว่าข้อมูลแบบใด ที่มีความสำคัญ และข้อมูลเหล่านี้ซึ่งประกอบด้วยการจัดเก็บ การถ่ายโอน และการทำลาย นโยบายนี้จะเป็นสิ่งที่เป็นพื้นฐานเพื่อตอบคำถามว่า ทำไมจึงต้องมีการรักษาความปลอดภัย

- นโยบายการรักษาความปลอดภัย (Security Policy) มีการกำหนดเกี่ยวกับระบบที่ควบคุมทางด้านเทคนิคคอมพิวเตอร์ต่าง ๆ

- นโยบายการใช้งาน (Usage Policy) มีการกำหนดนโยบายขององค์กรเกี่ยวกับการใช้งานคอมพิวเตอร์ที่ถูกต้องและเหมาะสม

- นโยบายการสำรอง (Backup Policy) มีการกำหนดความจำเป็น ที่มีส่วนเกี่ยวข้องกับการสำรองระบบคอมพิวเตอร์

- ระเบียบปฏิบัติเมื่อเกิดเหตุการณ์ (Incident Handling Procedure) มีการกำหนดด้านจุดมุ่งหมายและขั้นตอนเกี่ยวกับการจัดการกับเหตุการณ์ที่เกิดขึ้นเกี่ยวกับข้อมูล

- ระเบียบปฏิบัติที่เกี่ยวกับการบริหารจัดการบัญชีของผู้ใช้ (Account Management Procedure) มีการกำหนดขั้นตอนการปฏิบัติ เมื่อต้องเพิ่มบัญชีผู้ใช้ใหม่ และการลบทิ้งบัญชีผู้ใช้ที่ไม่ได้ใช้งานแล้ว

- แผนการฟื้นฟูหลังภัยร้ายแรง (Disaster Recovery Plan) มีการกำหนดแผนสำหรับฟื้นฟูหรือกู้ระบบคอมพิวเตอร์คืนหลังจากที่เกิดภัยธรรมชาติหรือภัยที่เกิดจากมนุษย์

ในการลำดับการกำหนดนโยบาย ถ้าองค์กรยังไม่มีนโยบายใด ๆ เลย เราควรเลือกที่จะกำหนดนโยบายใดก่อน คำตอบนั้นขึ้นอยู่กับความเสี่ยงขององค์กรในขณะนั้น ถ้าการป้องกันข้อมูลเป็นสิ่งที่มีความเสี่ยงสูงแล้ว ก็ควรเริ่มพัฒนานโยบายข้อมูลก่อน ในขณะที่ถ้าความเสี่ยงเกี่ยวกับการสูญเสียธุรกิจ อันเนื่องมาจากการขาดแผนการสำหรับฟื้นฟูหลังภัยธรรมชาติ นโยบายการฟื้นฟูหลังภัยร้ายแรงก็ควรเป็นจุดเริ่มต้น อีกปัจจัยหนึ่งที่ควรพิจารณาก็คือ ระยะเวลาสำหรับการวางเอกสารนโยบายเหล่านั้น แผนการฟื้นฟูจากภัยร้ายแรง มีแนวโน้มที่จะใช้ระยะเวลานาน เนื่องจากต้องมีรายละเอียดค่อนข้างมาก และจะเกี่ยวกับหลายหน่วยงานย่อยและบุคลากรมากหรือบางทีอาจจะต้องเกี่ยวข้องกับบริษัทข้างนอกซึ่งอาจต้องจ้างเข้ามาเพื่อช่วยในการทำระบบสำรองเพื่อใช้สำหรับกู้ระบบคอมพิวเตอร์ทั้งหมดคืนหากเกิดปัญหาขึ้น

นโยบายหนึ่งที่ควรกำหนดขึ้นในช่วงแรก ๆ ของกระบวนการคือนโยบายทางด้านข้อมูล นโยบายข้อมูลจะเป็นสิ่งที่กำหนดพื้นฐานว่าข้อมูลขององค์กรมีความสำคัญอย่างไร และมีวิธีป้องกันอย่างไร นอกจากนี้นโยบายจะเป็นตัวที่กำหนดการฝึกอบรม สำหรับพนักงานเพื่อให้ทราบวิธีปฏิบัติและปฏิบัติต่อข้อมูลอย่างระมัดระวัง

อย่างไรก็ตามเป็นไปได้ที่อาจจะมีการเขียนหลาย ๆ นโยบายขึ้นพร้อมกัน เนื่องจากแต่ละนโยบายอาจจะเกี่ยวข้องกับบุคลากรที่ต่างกันเล็กน้อย ยกตัวอย่างเช่น ผู้ดูแลระบบอาจต้องมีส่วนเกี่ยวข้องกับนโยบายการรักษาความปลอดภัยมากกว่านโยบายด้านข้อมูล ในกรณีนี้หน่วยงานรักษาความปลอดภัยอาจเป็นหน่วยงานแม่ที่ควรต้องดำเนินการทำนโยบายการรักษาความปลอดภัย หรือฝ่ายบุคคลอาจต้องเกี่ยวข้องกับนโยบายการใช้งาน และนโยบายการจัดการเกี่ยวกับบัญชีผู้ใช้มากกว่านโยบายการสำรองระบบ การกำหนดนโยบายนั้นก็อาจเริ่มจากการร่างหัวข้อเรื่องคร่าว ๆ หรือนโยบายคร่าว ๆ ก็ได้

โดยส่วนใหญ่ฝ่ายการรักษาความปลอดภัยนั้นอาจเริ่มจากนโยบายเล็ก ๆ ที่จะต้องเขียนข้อความไม่เยอะและไม่เกี่ยวข้องกับหลายหน่วยงานหรือบุคลากรมากนัก ซึ่งอาจเป็นโอกาสสำหรับฝ่ายรักษาความปลอดภัยที่จะเริ่มเรียนรู้และเข้าใจวิธีที่จะสร้างนโยบายอื่น ๆ

ในการปรับปรุงนโยบายที่มีใช้อยู่แล้ว ถ้าองค์กรมีนโยบายและระเบียบปฏิบัติอยู่แล้ว ก็เป็นสิ่งที่ได้เปรียบอย่างไรก็ตามนโยบายและระเบียบปฏิบัติเหล่านี้อาจต้องมีการปรับปรุงให้มีความทันสมัย ถ้าฝ่ายรักษาความปลอดภัยเป็นหน่วยงานที่สร้างนโยบายและระเบียบปฏิบัติเหล่านั้นก็อาจเริ่มจากการรวบรวมคณะที่จัดทำนโยบายนั้น โดยเริ่มพิจารณาจากเอกสารที่มีอยู่แล้ว และวิเคราะห์ว่ามีจุดด้อยตรงไหน

ถ้าเอกสารนั้นเขียนโดยบุคคล หรือคณะบุคคลที่ยังทำงานอยู่ในองค์กรนั้น บุคคลหรือคณะนั้น ควรมีส่วนร่วมในการปรับปรุงนโยบายให้ทันสมัยด้วย อย่างไรก็ตามฝ่ายการรักษาความปลอดภัย ควรเป็นหน่วยงานหลักที่ควบคุมกระบวนการปรับปรุงนี้ โดยกระบวนการก็ควรจะเริ่มจากเอกสารที่มีอยู่และค่อยพิจารณาจุดด้อยของนโยบายเหล่านั้น

ในกรณีที่คณะที่จัดทำนโยบายไม่ได้อยู่ในองค์กรนั้นแล้ว โดยส่วนใหญ่การเริ่มต้นจากศูนย์อาจเป็นสิ่งที่ง่ายกว่า พิจารณาว่าใครควรเกี่ยวข้องด้วย และเชิญเข้าร่วมกระบวนการปรับปรุงหรือพัฒนาใหม่ และควรแจ้งให้คณะทราบว่าทำไมเอกสารเก่าจึงไม่เพียงพอ

3. การติดตั้งระบบป้องกัน (Implementation) ในการบังคับใช้นโยบายสำหรับการรักษาความปลอดภัยให้ได้ผลนั้นต้องเกี่ยวข้องกับการจัดหาเครื่องมือ เทคนิค และระบบควบคุมการเข้าถึงทางกายภาพ พร้อมทั้งอาจต้องจ้างเจ้าหน้าที่รักษาความปลอดภัยเพิ่ม การบังคับใช้นั้นอาจต้องมีการคอนฟิกระบบใหม่ซึ่งอาจไม่ได้อยู่ในการควบคุม และดูแลของฝ่ายรักษาความปลอดภัย ในกรณีนี้ในการติดตั้งซอฟต์แวร์ระบบการรักษาความปลอดภัยนั้นต้องเกี่ยวข้องกับผู้ดูแลระบบ และผู้ดูแลเครือข่ายด้วย โดยต้องมีการตรวจสอบดูว่าการติดตั้งแต่ละระบบนั้นมีผลต่อสภาพแวดล้อมโดยรวมอย่างไร และมีผลกระทบต่อระบบควบคุมอื่นอย่างไร เช่น การเพิ่มระบบการรักษาความปลอดภัยทางด้านกายภาพนั้นอาจมีผลทำให้ความจำเป็นในการเข้ารหัสข้อมูลนั้นน้อยลง หรือในทางกลับกัน

หรือการติดตั้งไฟร์วอลล์ อาจจะช่วยลดช่องโหว่หรือจุดอ่อนของระบบได้ทันที ซึ่งแนวทางในการออกแบบและติดตั้งระบบเพื่อรักษาความปลอดภัยมีแนวทางต่าง ๆ ดังนี้

3.1 ระบบรายงานการรักษาความปลอดภัย ระบบนี้จะเป็นกลไก ที่ช่วยให้ฝ่ายรักษาความปลอดภัยทราบถึงการปฏิบัติตามนโยบายของพนักงานทั่วไป และเป็นสิ่งที่ใช้ติดตามทางด้านสถานภาพในปัจจุบัน ที่เกี่ยวกับจุดอ่อนโดยรวมขององค์กรด้วย การรายงานนั้นอาจเป็นแบบใช้มือหรืออาจเป็นแบบอัตโนมัติ โดยส่วนใหญ่จะใช้ทั้งสองวิธีควบคู่กันไป

3.2 การเฝ้าระวังการใช้งานระบบ การมอนิเตอร์การใช้งานระบบ จัดว่าเป็นกลไกที่ใช้สำหรับการตรวจสอบการปฏิบัติตามนโยบายการใช้งานของพนักงานซึ่งอาจจะรวมถึงซอฟต์แวร์ที่ใช้มอนิเตอร์การใช้งานอินเตอร์เน็ต จุดมุ่งหมายของการมอนิเตอร์ก็เพื่อตรวจดูว่าพนักงานคนใดที่ชอบฝ่าฝืนนโยบายขององค์กรบ่อย ๆ บางซอฟต์แวร์อาจสามารถป้องกันการเข้าถึงได้และเก็บล็อคเกี่ยวกับความพยายามที่จะฝ่าฝืนไว้ ซอฟต์แวร์บางตัวอาจสามารถลบเกมที่ติดตั้งบนเครื่องได้ หรืออาจเก็บล็อคเกี่ยวกับการติดตั้งโปรแกรมใหม่เข้าไปในระบบก็ได้

3.3 การสแกนช่องโหว่ระบบ การสแกนระบบเพื่อค้นหาจุดอ่อนได้กลายเป็นหัวข้อที่สำคัญเกี่ยวกับการรักษาความปลอดภัย การติดตั้งระบบปฏิบัติการโดยดีฟอลต์นั้นจะมี โพรเซสที่ไม่จำเป็นต้องถูกติดตั้งด้วย และรวมถึงจุดอ่อนและช่องโหว่ด้วย ในขณะที่การตรวจสอบเพื่อค้นหาจุดอ่อนและช่องโหว่ของระบบนั้นเป็นเรื่องที่ง่ายเมื่อใช้เครื่องมือที่มีในปัจจุบัน แต่การแก้ปัญหานั้นเป็นเรื่องที่ยากและต้องใช้เวลา

สำหรับฝ่ายทางด้านการรักษาความปลอดภัย ต้องคอยติดตามว่า มีระบบที่ติดตั้งในเครือข่ายกี่ระบบ และแต่ละระบบมีจุดอ่อนหรือช่องโหว่ใดบ้าง และต้องคอยตรวจสอบเป็นประจำ การรายงานเกี่ยวกับจุดอ่อนหรือช่องโหว่นั้น ต้องแจ้งให้ผู้ดูแลระบบแก้ไขหรือทำการป้องกัน ถ้ามีการติดตั้งระบบใหม่ควรแจ้งให้ทุกฝ่ายทราบเพื่อจะได้สแกนและป้องกันก่อนที่จะถูกเจาะเข้าระบบ

3.4 การปฏิบัติตามนโยบาย การบังคับให้เป็นไปตามนโยบายในด้านการรักษาความปลอดภัยนั้นเป็นเรื่องที่ต้องใช้เวลาพอสมควร การตรวจสอบว่ามีการปฏิบัติตามนโยบายนั้นมี 2 วิธี คือแบบอัตโนมัติและแบบทำด้วยมือ แบบที่ไม่อัตโนมัตินั้นผู้รักษาความปลอดภัยต้องคอยตรวจเช็คทุกระบบเพื่อดูว่ามีการฝ่าฝืนนโยบายหรือระเบียบหรือไม่ โดยอาจตรวจสอบล็อคไฟล์ หรืออาจใช้เครื่องมืออื่นเพื่อมอนิเตอร์เหตุการณ์ต่าง ๆ ที่เกิดขึ้นในระบบ วิธีนี้เป็นวิธีที่ใช้เวลามากและมีโอกาสที่จะเกิดข้อผิดพลาดขึ้นเยอะ บางองค์กรอาจสุ่มเลือกบางระบบเพื่อสแกน วิธีนี้อาจช่วยลดเวลาในการทำแต่ก็เป็นวิธีที่ไม่สมบูรณ์

ในปัจจุบันมีซอฟต์แวร์หลายชุดที่สามารถทำงานแบบอัตโนมัติ การติดตั้งนั้นอาจใช้เวลาและค่อนข้างยุ่งยาก แต่เมื่อติดตั้งเสร็จซอฟต์แวร์ก็จะตรวจเช็คการปฏิบัติตามนโยบายได้ภายใน

เวลาที่ไม่นานนัก การติดตั้งนั้นต้องอาศัยความช่วยเหลือจากผู้ดูแลระบบเนื่องจากต้องติดตั้งกับทุกระบบที่มีกลไกนี้เพื่อที่จะตรวจสอบการปฏิบัติตามนโยบายอย่างเคร่งครัด และจะรายงานให้ผู้ดูแลระบบทราบตามช่วงเวลาที่กำหนด

3.5 ระบบพิสูจน์ทราบตัวตน (Authentication Systems) จะเป็นกลไกที่ใช้ตรวจสอบผู้ใช้ที่ต้องการล็อคอินเข้าใช้งานระบบ หรือเครือข่าย นอกจากนี้ยังเป็นกลไกสำหรับตรวจสอบการเข้าสถานที่ที่ต้องห้ามด้วย ในการตรวจสอบเพื่อพิสูจน์ทราบนั้นอาจต้องใช้รหัสผ่าน สมาร์ทการ์ด หรือไบโอเมติกก็ได้ ทุกระบบที่ใช้งานภายในองค์กรควรต้องมีระบบพิสูจน์ตัวตน นั่นหมายความว่าผู้ใช้แต่ละคนต้องได้รับการฝึกอบรม เพื่อใช้งานระบบพิสูจน์ตัวตนนี้ ถ้าไม่ได้รับการฝึกอบรมการใช้งานที่ดีอาจใช้เวลานี้ไปทำงานอย่างอื่น ดังนั้น ถ้ามีการเปลี่ยนแปลงระบบในการพิสูจน์ทราบใหม่ก็จำเป็นที่จะต้องจัดอบรมให้ผู้ใช้ก่อน

ระบบพิสูจน์ทราบตัวตนจะมีผลกระทบกับทุกระบบขององค์กร ไม่ควรติดตั้งและใช้งานระบบพิสูจน์ทราบตัวตนก่อน โดยที่ไม่ได้วางแผนล่วงหน้าก่อน ผู้ดูแลและรักษาความปลอดภัยควรทำงานร่วมกับผู้ดูแลระบบ เพื่อให้การติดตั้งและใช้งานระบบพิสูจน์ทราบตัวตนให้เป็นไปอย่างราบรื่นไม่ติดขัด

3.6 การติดตั้งระบบรักษาความปลอดภัย สำหรับการใช้งานอินเตอร์เน็ตนั้น จัดเป็นระบบที่ต้องใช้ไฟร์วอลล์ และ VPN (Virtual Private Network) ซึ่งอาจต้องเปลี่ยนโครงสร้างของเครือข่าย บางทีสิ่งที่สำคัญที่สุดเกี่ยวกับการรักษาความปลอดภัยอินเตอร์เน็ตก็คือ ตำแหน่งของการติดตั้งระบบควบคุมการเข้าถึง เช่น ไฟร์วอลล์ซึ่งต้องติดตั้งระหว่างอินเตอร์เน็ตและเครือข่ายภายใน ถ้าไม่มีระบบป้องกันนี้ ระบบที่อยู่ภายในเครือข่ายก็อาจจะถูกเปิด ให้สามารถถูกโจมตีได้ตลอดเวลา การติดตั้งไฟร์วอลล์นั้นไม่ใช่เป็นเรื่องที่ง่าย ซึ่งบางครั้งอาจรบกวนการใช้งานอินเตอร์เน็ต ของผู้ใช้ภายในด้วย

ทั้งนี้การปรับเปลี่ยนโครงสร้างของเครือข่ายนั้น นับเป็นสิ่งที่ต้องทำควบคู่ไปกับการติดตั้งไฟร์วอลล์และระบบควบคุมการใช้งานอื่น โดยในการติดตั้งระบบนี้ไม่ควรที่จะทำจนกว่าการออกแบบโครงสร้างพื้นฐานของเครือข่าย เสร็จสมบูรณ์แล้ว เพื่อที่จะได้สามารถกำหนดขนาดและประสิทธิภาพของไฟร์วอลล์ ให้เหมาะสมกับปริมาณข้อมูลที่ต้องวิ่งผ่านไฟร์วอลล์ และเพื่อที่จะได้สามารถกำหนดกฎการควบคุมของไฟร์วอลล์เพื่อให้เป็นไปตามนโยบายที่วางไว้

VPN นับเป็นส่วนที่สำคัญสำหรับระบบด้านการรักษาความปลอดภัยให้อินเตอร์เน็ต ในขณะที่ VPN ป้องกันข้อมูลที่วิ่งผ่านอินเตอร์เน็ตโดยมีการเข้ารหัสข้อมูลไว้ นอกจากนี้ VPN ยังช่วยขยายเครือข่ายขององค์กรได้ด้วย

3.7 ระบบตรวจจับและป้องกันการบุกรุก IDS (Intrusion Detection System) เป็นระบบเตือนภัยของเครือข่ายสัญญาณเตือนขโมย เป็นระบบที่ใช้สำหรับการตรวจจับผู้ไม่ประสงค์ดีที่พยายามจะบุกรุกเข้าสถานที่ต้องห้าม IDS ก็ทำงานคล้ายกัน โดยจะแยกแยะได้ระหว่างการเข้าถึงส่วนของเครือข่ายที่ต้องห้ามที่ได้รับอนุญาตหรือเป็นการเข้ามาโดยผิดปกติ IDS นั้นมีหลายประเภท การเลือกใช้งานนั้นก็ขึ้นอยู่กับความเสี่ยงและทรัพยากรที่มีอยู่ขององค์กร IDS อาจต้องใช้ทรัพยากรค่อนข้างมากจากฝ่ายรักษาความปลอดภัย

ระบบตรวจจับการบุกรุกที่รู้จักกันมากที่สุดคือซอฟต์แวร์ป้องกันไวรัส ซึ่งซอฟต์แวร์นี้ควรต้องติดตั้งลงในคอมพิวเตอร์ทุกเครื่องรวมถึงเซิร์ฟเวอร์ด้วย ซอฟต์แวร์ป้องกันไวรัสเป็น IDS ที่ใช้ทรัพยากรน้อยที่สุด และ IDS อื่น ๆ ยังประกอบด้วยประเภทต่าง ๆ เช่น การตรวจสอบล็อคไฟล์ด้วยมือ การตรวจสอบล็อคไฟล์แบบอัตโนมัติ Host-based IDS และ Network-based IDS

การตรวจสอบล็อคไฟล์ด้วยมืออาจเป็นวิธีที่อาจได้ผลดี แต่เป็นวิธีที่ใช้เวลามากและมีโอกาสที่จะเกิดข้อผิดพลาดได้สูง โดยธรรมชาติแล้ว คนเรานั้นจะไม่สามารถตรวจสอบล็อคไฟล์ได้อย่างมีประสิทธิภาพเท่าที่ควร เนื่องจากอาจมีจำนวนมากเกินความสามารถ ซอฟต์แวร์ที่ใช้ตรวจวิเคราะห์ล็อคแบบอัตโนมัตินั้นอาจเป็นทางออกที่ดีกว่า การติดตั้ง IDS นั้นก็ไม่ควรทำจนกว่าจะได้ระบุพื้นที่ที่เป็นเขตที่มีความเสี่ยงสูง

3.8 การเข้ารหัสข้อมูลหรือเอ็นคริพชัน (Encryption) จะเป็นวิธีที่ใช้ปกป้องความลับ (Confidentiality) ของข้อมูล กลไกในการเข้ารหัสข้อมูลนั้นอาจใช้สำหรับป้องกันข้อมูลในระหว่างที่ส่งผ่านเครือข่าย หรือระหว่างที่จัดเก็บในอุปกรณ์การจัดเก็บข้อมูล เช่น ฮาร์ดดิสก์ เป็นต้น ในการเลือกใช้การเข้ารหัสแต่ละวิธีมี 2 สิ่งที่ต้องพิจารณาคือ อัลกอริธึม (Algorithms) และ การบริหารคีย์ (Key Management) โดยสิ่งหนึ่งที่ควรคำนึงถึงเมื่อจะใช้งานการเข้ารหัสคือกระบวนการในการเข้ารหัสข้อมูลนั้นอาจทำให้การไหลของข้อมูลช้าลง ดังนั้น จึงไม่มีความจำเป็นที่ต้องเข้ารหัสทุก ๆ ข้อมูลที่มี

3.8.1 อัลกอริธึม เมื่อติดตั้งระบบการเข้ารหัสข้อมูลแล้วนั้น จุดประสงค์ของการเข้ารหัสข้อมูลนั้น จะเป็นสิ่งที่กำหนดการเลือกอัลกอริธึม การเข้ารหัสแบบไพรเวทคีย์เอ็นคริพชัน (Private Key Encryption) จะทำงานเร็วกว่าพับลิกคีย์เอ็นคริพชัน (Public Key Encryption) อย่างไรก็ตามไพรเวทคีย์เอ็นคริพชันไม่สามารถใช้สำหรับการพิสูจน์ตัวตน เช่น ดิจิตอลซิกเนเจอร์ (Digital Signature) ได้ ซึ่งในการเลือกอัลกอริธึมนั้นควรเลือกที่เป็นที่รู้จักดี ซึ่งได้มีการทดสอบอย่างเปิดเผยมาแล้วว่ามีประสิทธิภาพที่ดี เพราะถ้าใช้อัลกอริธึมที่ไม่รู้จักกับระบบนั้นอาจมีช่องโหว่หรือจุดอ่อนในตัวก็ได้

3.8.2 การบริหารคีย์ ในการติดตั้งกลไกในการเข้ารหัสข้อมูลนั้น จะมีบางส่วนที่เกี่ยวข้องกับการจัดการคีย์ สำหรับการเข้ารหัสแบบจุดต่อจุด (Point-to-Point) ซึ่งโดยส่วนใหญ่จะใช้การเข้ารหัสแบบไพรเวทเอ็นคริพชันนั้น ระบบจะต้องมีการอัพเดตคีย์เป็นประจำซึ่งส่วนระบบที่ต้องใช้การเข้ารหัสแบบพับลิกคีย์เอ็นคริพชัน จำเป็นต้องมีการแจกจ่ายใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ไปยังผู้ใช้จำนวนมาก ทำให้ปัญหาที่เกิดขึ้นนั้นยุ่งยากกว่าเมื่อต้องติดตั้งระบบนี้ควรต้องกำหนดให้มีเวลาสำหรับทดสอบการจัดการคีย์ด้วย ซึ่งข้อควรระวังอย่างหนึ่งคือโปรแกรมทดลองนั้นส่วนใหญ่จะมีข้อกำหนดเกี่ยวกับจำนวนผู้ใช้ ในขณะที่เมื่อติดตั้งใช้งานจริงนั้น จะเกี่ยวข้องกับผู้ใช้จำนวนที่มากกว่ามาก

3.9 การรักษาความปลอดภัยทางด้านกายภาพนั้น ส่วนใหญ่มักจะถูกให้แยกออกจากการรักษาความปลอดภัยข้อมูลหรือทางด้านการสื่อสาร การติดตั้งระบบกล้องวงจรปิด กุญแจ การ์ดรูด หรือยามนั้น โดยส่วนใหญ่จะไม่เป็นที่เข้าใจโดยเจ้าหน้าที่รักษาความปลอดภัยข้อมูล ถ้าในกรณีอย่างนี้ควรหาความช่วยเหลือจากภายนอก เนื่องจากระบบรักษาความปลอดภัยทางด้านกายภาพนั้นจะมีผลกระทบต่อพนักงาน คล้ายกับระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์ เมื่อติดตั้งกล้องวงจรปิด หรือการที่ต้องใช้การ์ดรูดเข้ารูดออกจากที่ทำงาน พนักงานต้องการเวลาในการที่จะปรับตัวให้เข้ากับสภาพแวดล้อมใหม่นี้ เมื่อองค์กรกำหนดให้พนักงานทุกคน ต้องติดป้ายแสดงตนเมื่อพนักงานทำหาย องค์กรก็ต้องกำหนดระเบียบปฏิบัติเมื่อบัตรเกิดหาย ไม่เช่นนั้นก็อาจเป็นช่องโหว่หรือจุดอ่อนของระบบได้

ระเบียบปฏิบัติที่ถูกต้องนั้นต้องรวมขั้นตอน หรือวิธีในการพิสูจน์ทราบ ให้แน่ชัดว่าบุคคลที่กำลังพยายามจะเข้ามานั้นเป็นผู้ที่ได้รับอนุญาตจริง การพิสูจน์ตัวตนแบบนี้อาจรวมถึงการที่บัตรมีรูปถ่าย เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยสามารถตรวจสอบได้ บางองค์กรอาจใช้วิธีการพิสูจน์ตัวตนแค่การเซ็นชื่อเท่านั้น ซึ่งนี่อาจเปิดโอกาสให้ผู้ไม่หวังดีสามารถบุกรุกเข้าสถานที่ได้ง่าย

เมื่อติดตั้งระบบรักษาความปลอดภัยทางด้านกายภาพแล้ว ก็ควรจะพิจารณาดาต้าเซ็นเตอร์เป็นพื้นที่ที่ต้องให้ความสำคัญเป็นพิเศษ ดาต้าเซ็นเตอร์นั้นควรมีระบบป้องกันที่หนาแน่น และควรติดตั้งระบบป้องกันไฟไหม้ ระบบควบคุมอุณหภูมิ และระบบสำรองไฟฟ้าที่ดี การติดตั้งระบบเหล่านี้อาจต้องมีการปรับปรุงพื้นที่อย่างมาก การติดตั้งระบบ UPS ใหม่ อาจจำเป็นต้องชัตดาวน์ระบบชั่วคราวซึ่งต้องมีการวางแผนล่วงหน้าอย่างดี

3.10 คณะทำงาน เมื่อได้มีการติดตั้งระบบป้องกัน และรักษาความปลอดภัยใหม่นั้นจะต้องมีเจ้าหน้าที่ที่ดูแลอย่างเหมาะสม บางระบบอาจต้องมีผู้ดูแลระบบอยู่ตลอดเวลา เช่น ระบบพิสูจน์ทราบตัวตน ไฟร์วอลล์ และ IDS เป็นต้น กลไกอื่นอาจต้องมีผู้รับผิดชอบที่จะดำเนินการ

ต่อเมื่อมีเหตุการณ์เกิดขึ้น เช่น การสแกนหาจุดอ่อนของระบบ ซึ่งเมื่อมีการพบจุดอ่อนหรือช่องโหว่ก็จำเป็นต้องให้ผู้ดูแลระบบแก้ไขจุดอ่อนดังกล่าว

ในการฝึกอบรมให้พนักงานนั้น จำเป็นที่ต้องมีเจ้าหน้าที่ที่ถนัดทางด้านนี้ อย่างน้อยที่สุดเจ้าหน้าที่รักษาความปลอดภัยก็ควรจะต้องเข้ามามีส่วนร่วมในการฝึกอบรมเพื่อตอบข้อซักถามต่าง ๆ ที่อาจมีจากพนักงาน ซึ่งเป็นสิ่งที่จำเป็น ถึงแม้ว่าผู้ที่บรรยายจะเป็นเจ้าหน้าที่จากฝ่ายบริหารบุคคล

ประเด็นสุดท้ายที่สำคัญเกี่ยวกับเจ้าหน้าที่คือ ความรับผิดชอบทางด้านการรักษาความปลอดภัยองค์กรนั้นควรถือเป็นหน้าที่และความรับผิดชอบของพนักงานทุกคนในองค์กร นอกจากนี้ควรมีคณะทำงานที่รับผิดชอบทางด้านนี้โดยเฉพาะ เพื่อทำหน้าที่ในการพัฒนานโยบาย ที่เกี่ยวข้องกับการรักษาความปลอดภัย และการบังคับใช้นโยบายเหล่านั้น ซึ่งคณะนี้อาจตั้งเป็นฝ่ายรักษาความปลอดภัย โดยความรับผิดชอบนั้นควรจะตกอยู่กับหัวหน้าฝ่าย

4. การฝึกอบรม (Training) เนื่องจากองค์กรไม่สามารถ ที่จะป้องกันข้อมูลที่สำคัญขององค์กรได้โดยการปราศจากความร่วมมือจากพนักงานขององค์กรทุกคน การจัดการฝึกอบรมเพื่อให้มีรับทราบนั้น ก็เป็นการแจ้งข้อมูลที่จำเป็นให้พนักงานแต่ละคนทราบ การฝึกอบรมนั้นอาจจัดเป็นการประชุมหรือการตีพิมพ์ผ่านสื่อต่าง ๆ ขององค์กร เช่น วารสาร หรือปิดประกาศในที่ต่าง ๆ วิธีที่ดีที่สุดคือ การใช้ทั้ง 3 วิธีควบคู่กันไป และจะต้องทำเป็นประจำด้วย โดยผู้ที่มีส่วนเกี่ยวข้องในการฝึกอบรมมีดังต่อไปนี้

4.1 พนักงาน อาจจะต้องมีการฝึกอบรมเพื่อทำความเข้าใจและทราบว่าการรักษาความปลอดภัยมีความสำคัญอย่างไร นอกจากนี้ควรแจ้งให้ทราบว่าข้อมูลใดมีความสำคัญและเป็นความลับขององค์กร และต้องช่วยกันปกป้องข้อมูลเหล่านั้นไม่ให้รั่วไหลออกไป การฝึกอบรมนั้นจะช่วยให้พนักงานทั่วไปรับทราบข้อมูลที่ควรทราบ รู้วิธีจัดการเกี่ยวกับรหัสผ่าน และช่วยป้องกันจากการถูกโจมตี โดยการฝึกอบรมนั้นควรเป็นแบบสั้น ๆ ควรใช้เวลาประมาณ 1-2 ชั่วโมง พนักงานใหม่ควรได้รับการฝึกอบรมนี้ โดยกำหนดให้เป็นส่วนหนึ่งของการปฐมนิเทศ ส่วนพนักงานเก่าก็ควรได้รับการฝึกอบรมนี้อย่างน้อย 2 ปีต่อครั้ง

4.2 ผู้ดูแลระบบ การฝึกอบรมนั้นก็เป็นสิ่งสำคัญและจำเป็นสำหรับผู้ดูแลระบบด้วย ผู้ดูแลระบบควรปรับความรู้ให้ทันสมัยอยู่เสมอ เช่น เทคนิคการเจาะระบบแบบต่าง ๆ หรือภัยที่อาจเกิดขึ้นได้ และการติดตั้งแพตซ์เพื่อป้องกันการโจมตีใหม่ ๆ การฝึกอบรมประเภทนี้ควรจัดให้มีบ่อยครั้ง เช่น ประมาณเดือนละครั้งและควรมีการเชิญผู้ที่เชี่ยวชาญทางด้านนี้โดยเฉพาะมาฝึกอบรม การฝึกอบรมประเภทนี้อาจจัดให้เป็นส่วนหนึ่งของการประชุมประจำของผู้ดูแลระบบเพื่อช่วยลดเวลา

0203360

นอกจากนี้เจ้าหน้าที่รักษาความปลอดภัย ควรจะมีการส่งข้อมูลใหม่ ๆ ที่เกี่ยวกับการรักษาความปลอดภัย ให้ผู้ดูแลระบบทราบทันทีที่ได้รับทราบ แทนที่จะรอแจ้งในที่ประชุม การทำเช่นนี้ก็เป็นการช่วยเพิ่มความสัมพันธ์และการทำงานร่วมกันอย่างมีประสิทธิภาพ ระหว่างเจ้าหน้าที่รักษาความปลอดภัยและผู้ดูแลระบบ

4.3 นักพัฒนาแอพพลิเคชัน การฝึกอบรมสำหรับนักพัฒนาโปรแกรมหรือนักพัฒนาแอพพลิเคชันนั้น ควรเป็นส่วนหนึ่งที่เพิ่มจากการฝึกอบรมพนักงานทั่วไป โดยส่วนที่เพิ่มขึ้นมานั้นควรเป็นเรื่องเกี่ยวกับเทคนิคการเขียนโปรแกรมอย่างไรเพื่อให้มีความปลอดภัย นอกจากนี้ก็ควรจะอธิบายถึงเหตุผลและหน้าที่ของฝ่ายรักษาความปลอดภัย ในระหว่างที่ได้มีการพัฒนา กระบวนการรักษาความปลอดภัย

สำหรับโครงการใหม่ฝ่ายรักษาความปลอดภัยนั้น ควรที่จะมีส่วนร่วม ในระหว่างการออกแบบด้วย ซึ่งเป็นการเปิดโอกาส ให้ฝ่ายการรักษาความปลอดภัยได้มีการพิจารณาเกี่ยวกับ เรื่องความปลอดภัย ก่อนที่จะผลิตในระหว่างการอบรมนั้น ควรจะอธิบายให้นักพัฒนาโปรแกรมทราบถึงคุณค่าของความปลอดภัยในช่วงต้นของการผลิตซอฟต์แวร์

4.4 ผู้บริหาร ถ้าผู้บริหารไม่สนับสนุนก็จะไม่มีระบบการรักษาความปลอดภัยสำหรับในองค์กร ดังนั้นคณะผู้บริหารควรได้รับรายงานสถานภาพและความก้าวหน้าเกี่ยวกับโครงการติดตั้งระบบการรักษาความปลอดภัย การเสนอผู้บริหารนั้นควรรวมกับเรื่องอื่นเข้าไปด้วย เช่น การตลาด การศึกษา เป็นต้น ในการเสนอหรือรายงานผู้บริหารประจำนั้นควรมีการรวมเกี่ยวกับผลที่ได้จากการประเมินสถานการณ์ปัจจุบัน และความก้าวหน้าของแต่ละโครงการด้วย ถ้าเป็นไปได้ควรมีมาตรฐานการวัดที่ออกมาเป็นตัวเลข เพื่อบ่งบอกถึงระดับความปลอดภัยขององค์กร หรือการรายงานนั้นควรมีตัวเลขทางด้านสถิติด้วย เช่น จำนวนช่องโหว่ของแต่ละระบบ หรือจำนวนครั้งที่มีการฝ่าฝืนนโยบายหรือมีความพยายามที่จะเจาะเข้าระบบ ในระหว่างการเสนอผู้บริหารนั้น ควรจะนำข้อมูลที่ฝึกอบรมพนักงานทั่วไปให้ทราบด้วยเพื่อเป็นการเตือนผู้บริหารให้ทราบถึงความรับผิดชอบที่มีต่อองค์กร

4.5 คณะเจ้าหน้าที่ฝ่ายรักษาความปลอดภัย ก็ควรปรับปรุงความรู้เกี่ยวกับการรักษาความปลอดภัยเป็นประจำเพื่อจะได้สามารถให้บริการกับองค์กรได้ การฝึกอบรมข้างนอกก็เป็นส่วนที่สำคัญ แต่ทั้งนี้การเชิญวิทยากรหรือผู้เชี่ยวชาญจากภายนอกมาให้บริการภายในก็เป็นสิ่งที่จำเป็นเช่นกัน นอกจากนี้การผลัดกันเสนอข้อมูลเกี่ยวกับเทคนิคหรือเทคโนโลยีใหม่ ๆ ก็เป็นสิ่งที่อาจช่วยได้ เช่น เจ้าหน้าที่แต่ละคนอาจได้รับมอบหมาย เพื่อให้เสนอเรื่องที่เกี่ยวกับการรักษาความปลอดภัยโดยอาจเป็นเรื่องที่ชอบหรือกำลังเป็นที่สนใจ หรือเป็นเรื่องที่เจ้าหน้าที่ส่วนใหญ่ ยังขาดความรู้และชำนาญ หรือความสามารถอยู่

ศูนย์สนเทศและหอสมุด
มหาวิทยาลัยธุรกิจบัณฑิตย์

5. การตรวจสอบ (Audit) จัดว่าเป็นขั้นตอนสุดท้าย ในกระบวนการรักษาความปลอดภัย หลังจากที่ได้ประเมินสถานการณ์ขององค์กร แล้วก็กำหนดนโยบายและระเบียบปฏิบัติ ติดตั้งระบบรักษาความปลอดภัยที่จำเป็น ฝึกอบรมเจ้าหน้าที่และพนักงานทั่วไป และท้ายสุดคือการตรวจสอบว่ามีการฝ่าฝืนนโยบายและระเบียบปฏิบัติหรือไม่ เมื่อเรากล่าวถึงการตรวจสอบที่เกี่ยวกับด้านการรักษาความปลอดภัยนั้น เรามักจะหมายถึง การตรวจสอบ 3 ประเภทดังต่อไปนี้

5.1 การตรวจสอบการปฏิบัติตามนโยบาย (Policy Adherence Audit) เป็นเรื่องหลักของการตรวจสอบองค์กร ซึ่งได้มีนโยบายที่กำหนดเกี่ยวกับการรักษาความปลอดภัยขององค์กรแล้ว การตรวจสอบจะตอบคำถามองค์กรนั้นว่า มีระดับความปลอดภัย ตามที่ได้คาดหวังไว้หรือไม่ การตรวจสอบนั้นอาจทำโดยเจ้าหน้าที่ภายในเอง หรืออาจเป็นบุคลากรที่มีความชำนาญจากภายนอก มาตรวจสอบก็ได้ ไม่ว่ากรณีใด ๆ ก็ตามการตรวจสอบนั้นไม่สามารถทำได้ถ้าไม่ได้รับความร่วมมือจากคณะผู้ดูแลระบบ

การตรวจสอการปฏิบัติตามนโยบายนั้น ไม่ควรที่จะเน้นในเฉพาะระบบคอมพิวเตอร์เท่านั้น ควรให้ความสำคัญกับข้อมูลที่มีอยู่ในรูปแบบอื่นด้วย ควรตรวจสอบด้วยว่านโยบายข้อมูลนั้นมีการปฏิบัติตามเคร่งครัดแค่ไหน หรือเอกสารที่มีข้อมูลที่สำคัญมีการจัดเก็บหรือรับส่งอย่างไร

การตรวจสอบควรกระทำปีละครั้ง ในการตรวจสอบนั้น อาจทำโดยเจ้าหน้าที่จากฝ่ายรักษาความปลอดภัย หรืออาจจะเป็นการดีกว่าที่จะตั้งฝ่ายตรวจสอบต่างหาก หรืออาจจ้างบริษัทข้างนอก ซึ่งมีความชำนาญทางด้านนี้โดยเฉพาะมาทำงานให้ เพราะจะได้ตรวจสอบการทำงานของฝ่ายรักษาความปลอดภัยด้วย

5.2 การประเมินโครงการใหม่ สำหรับคอมพิวเตอร์และเครือข่าย นับเป็นเทคโนโลยีที่มีการเปลี่ยนแปลงตลอดเวลา ซึ่งจะทำให้ผลที่ได้จากการประเมินนั้นอาจล้าสมัยในไม่ช้า เนื่องจากจุดอ่อนหรือช่องโหว่เก่าอาจถูกป้องกันไว้หมดแล้วในระบบใหม่ แต่ก็อาจจะมีช่องโหว่ หรือจุดอ่อนใหม่ที่ยังไมได้ค้นพบก็ได้ ด้วยเหตุนี้การประเมินสถานการณ์ควรกระทำเป็นประจำ การประเมินทั้งระบบหรือองค์กรนั้น ควรกระทำปีละครั้งหรือสองปีครั้งก็ได้ และเมื่อมีโครงการที่ต้องติดตั้ง หรือพัฒนาระบบใหม่ ก็ควรจะมีการประเมินหรือตรวจทดลองระบบใหม่ก่อนทุกครั้งว่ามีความปลอดภัยมากน้อยแค่ไหนก่อนที่จะใช้งานจริง ซึ่งถ้าเป็นการพัฒนาระบบใหม่นั้น ก็ควรจะมีการตรวจสอบในระหว่างการออกแบบ เพื่อจะได้แก้ไขปัญหา ก่อนที่จะผลิตออกมาใช้งานจริง

5.3 การทดลองเจาะระบบ (Penetration Testing) สำหรับการทดลองเจาะระบบนั้นหลายครั้งที่การทดลองเจาระบบนั้นจัดไว้ในช่วงของการประเมินสถานการณ์ การทดลองเจาะระบบนั้นคือการใช้เครื่องมือเพื่อทดลองเจาะระบบหรือองค์กรโดยใช้ประโยชน์จากจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักกันทั่วไป ซึ่งถ้าการเจาะระบบสำเร็จ ข้อมูลที่ได้จากการทดสอบนี้ คือทราบว่าองค์กรหรือ

ระบบมีจุดอ่อน หรือช่องโหว่เพิ่มขึ้นอย่างน้อยหนึ่งจุด ถ้าการทดสอบเจาะเข้าระบบไม่เป็นผลสำเร็จ ผลที่ได้จากการทดสอบกณคือ ผู้ทดสอบไม่สามารถจะเจาะเข้าระบบผ่านทางจุดอ่อนนั้นได้ แต่ไม่ได้หมายความว่าจุดอ่อนของระบบนั้นไม่มี ซึ่งหลังจากที่องค์กรได้ประเมินสถานการณ์ แล้วทราบว่าระบบมีความเสี่ยงสูง ดังนั้นจึงตัดสินใจที่จะติดตั้งระบบควบคุมการเข้าถึงระบบ การทดสอบเจาะระบบก็อาจเป็นเครื่องมือที่ใช้ทดสอบระบบนี้ได้

การทดสอบเจาะระบบนั้นเหมาะสำหรับการตรวจสอบระบบควบคุมดังต่อไปนี้

- ความสามารถและประสิทธิภาพของ IDS ที่จะตรวจจับการบุกรุกได้
- ความเพียงพอของข้อมูลที่ให้พนักงานรับทราบในระหว่างการฝึกอบรม
- ข้อมูลที่ได้จากการเรียนรู้ระบบเครือข่ายผ่านระบบควบคุมต่าง ๆ
- ความเหมาะสมของระบบรักษาความปลอดภัยทางด้านกายภาพของที่ตั้งนั้น ๆ

การทดสอบจะเพื่อจุดประสงค์ใดก็ตาม ก่อนที่จะทดสอบนั้น ควรมีการวางแผนอย่างละเอียดรอบคอบ และจะต้องแจ้งให้องค์กรทราบล่วงหน้า นอกจากนี้องค์กรควรต้องกำหนดขอบเขตของการทดสอบ การทดสอบเจาะระบบจากภายนอกนั้น จะถูกจำกัดด้วยลิงค์ที่เชื่อมต่อจากภายนอก ซึ่งอาจจะรวม หรืออาจจะไม่รวมถึงระบบหมุนโมเด็มก็ได้ นอกจากนี้ควรมีการทดสอบระบบรักษาความปลอดภัยทางด้านกายภาพด้วย โดยอาจจะให้บางคนพยายามที่จะบุกเข้าสถานที่ ที่มีการควบคุมขอบเขตในเรื่องของเวลาอาจเป็นช่วงเวลาทำงานหรืออาจจะเป็นช่วงนอกเวลาทำงานก็ได้ โดยอาจจะอนุญาตให้ผู้ทดสอบสามารถเข้าถึงระบบขององค์กรได้ องค์กรต่าง ๆ อาจเริ่มต้นกระบวนการรักษาความปลอดภัยจากการทดสอบเจาะเข้าระบบ การทำลักษณะนี้อาจจะไม่เกิดผลดีมากนัก เนื่องจากการทดสอบเจาะเข้าระบบนั้นอาจไม่ได้ข้อมูลที่เพียงพอเพื่อจัดการความเสี่ยงขององค์กร

การรักษาความปลอดภัยนั้นเกี่ยวกับการบริหารจัดการความเสี่ยง ถ้าระบบไม่มีความเสี่ยงก็ไม่จำเป็นต้องมีระบบการรักษาความปลอดภัย แต่ถ้าระบบมีความเสี่ยง ก็จำเป็นต้องรู้ว่าเสี่ยงมากน้อยแค่ไหน และต้องออกแบบและติดตั้งระบบอะไร เพื่อที่จะช่วยลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ และงบประมาณที่ใช้ไปกับระบบการรักษาความปลอดภัยนั้น อย่างน้อยก็ไม่ควรจะเกินมูลค่าทรัพย์สินที่ต้องการปกป้อง และที่สำคัญคือไม่มากจนเกินความจำเป็น

การรักษาความปลอดภัยนั้นเป็นกระบวนการ โดยทุกคนจะต้องให้ความร่วมมือเป็นอย่างดี เพราะไม่เช่นนั้นข้อมูลอาจเล็ดลอดออกทางใดทางหนึ่งได้ กระบวนการรักษาความปลอดภัยนั้นประกอบด้วย 5 ขั้นตอนหลักคือ การประเมินความเสี่ยง การกำหนดนโยบาย การออกแบบและติดตั้งระบบ การรักษาความปลอดภัย การฝึกอบรมพนักงาน และการตรวจสอบ ซึ่งแต่ละขั้นตอนนั้นมีความจำเป็นและสำคัญทั้งสิ้น ควรจะกระทำอย่างต่อเนื่อง และปรับให้เข้ากับสถานการณ์และความเสี่ยงในตอนนั้น ๆ

กระบวนการจัดการประเมินความเสี่ยง

(ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, 2550, มิถุนายน)

กระบวนการที่ใช้ในการจัดการประเมินความเสี่ยง มีขั้นตอนดังนี้

1. กำหนดทรัพย์สินก่อนว่ามีทรัพย์สินอะไรบ้าง เพื่อจะไปทำการระบุความเสี่ยง ความเสี่ยงคือโอกาสที่ภัยคุกคามจะใช้ประโยชน์จากจุดอ่อนที่มีอยู่ในระบบ มีอยู่ในทรัพย์สิน ในขั้นแรกต้องไปวิเคราะห์ตัวภัยคุกคาม จุดอ่อน ออกมาก่อน

2. การประเมินความเสี่ยง คือการศึกษาว่าความเสี่ยงอยู่ในระดับสูงหรือต่ำ ต้องไปดูว่าองค์กรมีความเสี่ยงอะไรบ้าง ระดับความเสี่ยงเป็นอย่างไร ต้องแสดงให้ดูทั้งสูงและต่ำร่วมกัน ถ้าความเสี่ยงอยู่ในระดับต่ำก็สามารถยอมรับได้ แต่หากในขณะที่ความเสี่ยงอยู่ในระดับสูง ก็ต้องไปกำหนดแผนในการที่จะแก้ไขให้ดีขึ้น

3. กำหนดทางเลือกในการที่จะไปจัดการกับความเสี่ยง โดยการนำมาตรการควบคุมที่มีการเลือกมาจากมาตรการป้องกันในมาตรฐาน ISO 17799 ตัวอย่างเช่น ความเสี่ยงในรูปแบบหนึ่งที่จะต้องจัดการคือเรื่องของไวรัส นับเป็นภัยคุกคามอย่างหนึ่ง ซึ่งมาตรการที่ใช้ป้องกันไวรัสจะอยู่ในข้อใดข้อหนึ่ง ในทั้งหมด 133 ข้อ ที่ว่าด้วยเรื่องการจัดการไวรัส โดยการนำภัยคุกคามนี้ไปหาข้อเปรียบเทียบ เพื่อที่จะบอกได้ว่าไวรัสที่เป็นความเสี่ยงขององค์กร อยู่ภายใต้วัตถุประสงค์ใด และก็มาตรการข้อใดที่อยู่ในมาตรฐาน ISO 17799

สำหรับทางเลือกในการป้องกัน อาจมีได้หลากหลาย เช่น การมีรูปแบบที่องค์กรจะใช้ป้องกันไวรัสที่ดี น่าจะเป็นแบบ client-server คือมีเครื่องแม่ข่ายเครื่องหนึ่ง ซึ่งทำหน้าที่ปรับปรุงข้อมูลที่เป็นรายชื่อของไวรัสตัวใหม่ ๆ ที่เกิดขึ้นมาใหม่ มาเก็บไว้ที่ตัวเองแล้วกระจายรายชื่อเหล่านี้ให้กับเครื่องลูกข่าย เพื่อให้ข้อมูลรูปแบบของไวรัสมีความใหม่ ได้รับการปรับปรุงให้ทันสมัยทั่วถึงและเท่าเทียมกัน ซึ่งเมื่อเทียบกับการปรับปรุงรายชื่อไวรัสใหม่ ๆ ลักษณะแบบนี้ จะทำให้รายชื่อหรือรูปแบบของไวรัสแต่ละเครื่องไม่เท่ากัน เครื่องไหนที่ล้าสมัยก็จะไม่สามารถป้องกันตัวเองได้

ดังนั้นทางเลือกในการติดตั้งโปรแกรม จะเห็นได้เป็น 2 ทางเลือก ทางเลือกหนึ่งคือแบบ client-server และอีกแบบหนึ่งคือแบบ 1 เครื่องต่อ 1 โปรแกรม (stand alone) เพราะฉะนั้นจะต้องประเมินทางเลือก ในการที่จะจัดการกับความเสี่ยงจากทางเลือกทั้งสอง จะต้องพิจารณาถึงข้อดีและข้อเสีย และให้เลือกทางที่ดีที่สุดในการจัดการความเสี่ยง ซึ่งก็คือควรเลือกแบบ client-server ที่เป็นทางเลือกสุดท้าย ที่จะต้องไปทำแผนป้องกันขึ้นมา และเมื่อมีการจัดทำแผนการป้องกัน สำหรับภัยคุกคามนั้นขึ้นมาแล้ว ก็จะต้องมีการนำไปฝึกอบรมเพื่อสอนให้แก่ผู้ใช้งานได้ทราบ เพื่อให้ผู้ใช้เกิดความตระหนักและรู้ถึงวิธีการที่จะป้องกันตนเองจากภัยคุกคามเหล่านั้น ซึ่งจะช่วยทำให้ระดับความเสี่ยงของภัยคุกคามเหล่านั้นที่มีต่อองค์กรมีระดับลดลง อยู่ในระดับที่องค์กรสามารถยอมรับได้

การจัดระดับความเสี่ยง (Risk Prioritisation)

(ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, 2550, มิถุนายน)

โอกาสการเกิดภัยคุกคาม (Probability) คือ ระดับของโอกาสการเกิดภัยคุกคามในแต่ละจุดอ่อนนั้น สามารถแบ่งเป็น 5 ระดับโดยคิดจากโอกาสการเกิดขึ้นตามช่วงเวลา ดังตารางที่ 2.1

ตารางที่ 2.1 แสดงระดับของโอกาสในการเกิดภัยคุกคาม (Probability)

Probability	คำอธิบาย	ระดับ
Very High	ระดับสูงมาก - มีโอกาสเกิดบ่อย อาจเกิดขึ้นเกือบทุกเดือน	9
High	ระดับสูง - มีโอกาสเกิดหลายครั้งต่อปี	7
Medium	ระดับกลาง - มีโอกาสเกิดขึ้น ปีละครั้ง	5
Low	ระดับต่ำ - มีโอกาสเกิดยาก อาจเกิดได้ในรอบสามปี	3
Very Low	ระดับต่ำมาก - มีโอกาสเกิดยากมาก	1

ผลกระทบต่อทรัพย์สิน (Impact) คือ ระดับของผลกระทบและความรุนแรงที่เกิดขึ้นต่อข้อมูลและทรัพย์สินสารสนเทศขององค์กร สามารถแบ่งเป็น 4 ระดับ ดังตารางที่ 2.2

ตารางที่ 2.2 แสดงระดับของผลกระทบและความเสียหายต่อทรัพย์สิน (Impact)

Probability	คำอธิบาย	ระดับ
Very High	ระดับสูงมาก - แสดงถึงว่ารายการทรัพย์สินนี้หากมีความเสียหายจะมีผลกระทบสูงมาก	7
High	ระดับสูง - แสดงถึงว่ารายการทรัพย์สินนี้หากมีความเสียหายจะมีผลกระทบสูง	5
Medium	ระดับกลาง - แสดงถึงว่ารายการทรัพย์สินนี้หากมีความเสียหายจะมีผลกระทบปานกลาง	3
Low	ระดับต่ำ - แสดงถึงว่ารายการทรัพย์สินนี้หากมีความเสียหายจะมีผลกระทบต่ำ	1

ค่าความเสี่ยง (Risk Value) คือ ค่าของความเสี่ยงโดยรวมทั้งหมด ที่เกิดขึ้นกับทรัพย์สินสารสนเทศในแต่ละรายการ ซึ่งคำนวณหาค่าได้จากสูตร

Risk Value = Probability * Impact

ระดับค่าความเสี่ยงโดยรวมสามารถสรุปดังตารางที่ 2.3 โดยประกอบด้วย

ค่าความเสี่ยงที่สามารถยอมรับได้มีค่าตั้งแต่ 1-15

ค่าความเสี่ยงที่มีค่าปานกลางควรดำเนินการแก้ไขมีค่าตั้งแต่ 21-35

ค่าความเสี่ยงที่ต้องการแก้ไขอย่างเร่งด่วนมีค่าตั้งแต่ 45-63

ตารางที่ 2.3 แสดงระดับของค่าความเสี่ยงโดยรวม

Impact \ Probability	Very High(9)	High(7)	Medium(5)	Low(3)	Very Low(1)
Low (1)	9	7	5	3	1
Medium (3)	27	21	15	9	3
High (5)	45	35	25	15	5
Very High (7)	63	49	35	21	7

2.5 ภาษาพีเอชพี

กิติศักดิ์ เจริญโภคานนท์ (2548 : 2-4) กล่าวถึง เหตุผลในการที่จะเลือกใช้ PHP ของนักพัฒนาเว็บ มีลักษณะดังต่อไปนี้

1. ความรวดเร็วในการพัฒนาโปรแกรม เนื่องจากPHP เป็นสคริปต์ในแบบ Embeded คือสามารถแทรกร่วมกับภาษา HTML ได้อย่างอิสระ และหากมีการพัฒนาโค้ดไว้ในรูปแบบของ Class ที่เขียนขึ้นเพียงครั้งเดียวแล้วเรียกใช้งานได้ตลอด ทำให้มีความสะดวกและรวดเร็ว ในการจะนำไปใช้พัฒนาโปรแกรมต่าง ๆ

2. PHP เป็นโค้ดแบบเปิดเผย (Open Source) เนื่องจาก PHP มีกลุ่มของผู้ใช้งานอยู่เป็นจำนวนมากทั่วโลก และมีเว็บไซต์อยู่เป็นจำนวนมาก ที่เป็นแหล่งรวบรวมซอสโค้ดโปรแกรม หรือจะเป็นบทความต่าง ๆ ซึ่งทำให้ผู้ใช้มือใหม่ ๆ หรือผู้ที่ต้องการศึกษา สามารถค้นหาซอสโค้ดมาเป็นแนวทางในการพัฒนาโปรแกรมได้ง่ายขึ้น

3. การบริหารหน่วยความจำ (Memory Usage) มีการใช้งานหน่วยความจำที่ดี กล่าวคือ PHP จะไม่เรียกใช้หน่วยความจำตลอดเวลา ทำให้เซิรฟเวอร์ไม่จำเป็นต้องมีทรัพยากรมากนัก

4. ความเป็นอิสระต่อระบบปฏิบัติการ สืบเนื่องมาจาก เว็บแอพพลิเคชั่นที่ถูกสร้างขึ้นมาสามารถที่จะรันได้หลายระบบปฏิบัติการ ไม่ว่าจะเป็น Unix, Linux หรือ Windows เป็นต้น

กิติศักดิ์ เจริญโภคานนท์ กล่าวถึงการทำงานของเว็บ PHP ไว้ดังภาพที่ 2.4 โดยมีลักษณะขั้นตอนการทำงานต่าง ๆ ดังนี้

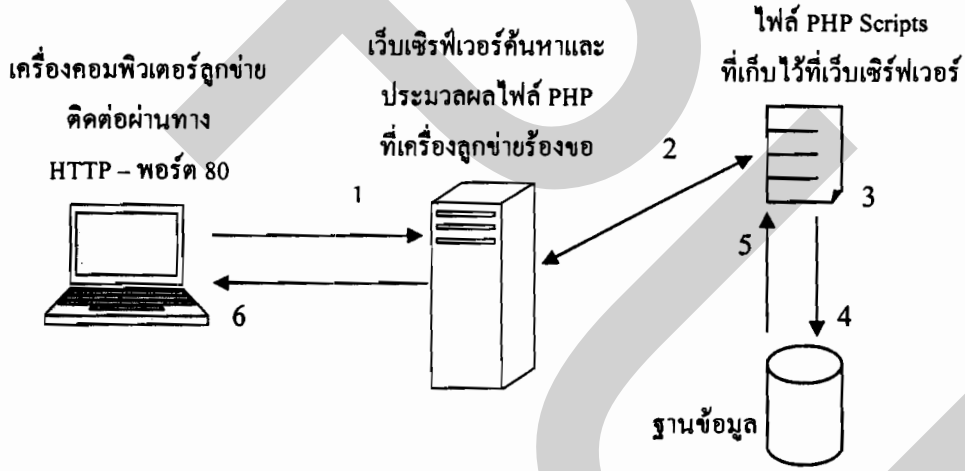
ขั้นตอนที่ 1 ฝั่งเครื่องลูกข่าย (Client) จะทำการร้องขอ หรือเรียกใช้งานไฟล์ PHP ที่เก็บในเครื่องแม่ข่าย (Server) ผ่านทางโปรโตคอล http ที่พอร์ต 80

ขั้นตอนที่ 2 ฝั่งเครื่องแม่ข่าย (Server) จะทำการค้นหาไฟล์ PHP ตัวที่ถูกร้องขอ แล้วทำการประมวลผลไฟล์ PHP ตามที่เครื่องลูกข่ายทำการร้องขอมา

ขั้นตอนที่ 3 ทำการประมวลผลไฟล์ PHP

ขั้นตอนที่ 4 และ 5 เป็นการติดต่อกับฐานข้อมูล และนำข้อมูลในฐานข้อมูลมาใช้ร่วมกับการประมวลผล

ขั้นตอนที่ 6 ส่งผลลัพธ์จากการประมวลผลไปให้เครื่องลูกข่าย



ภาพที่ 2.4 แสดงขั้นตอนการทำงานของหน้าเว็บพีเอชพี

ที่มา: คู่มือเรียนเขียนเว็บอีคอมเมิร์ซด้วย PHP 5 ครอบคลุมเวอร์ชั่นล่าสุด 5.1

กิตติ ภักดีวัฒนะกุล (2547 : 7) กล่าวว่า การสร้างเว็บเพจด้วย PHP นั้น สามารถที่จะใช้โปรแกรมที่เป็นเครื่องมือสำหรับสร้างเว็บไซต์ อาทิเช่น Macromedia Dreamweaver, FrontPage, EditPlus, Notepad เป็นต้น โค้ดของภาษา PHP ที่นิยม จะใช้อยู่ภายใต้เครื่องหมาย <? และจบด้วย ?> ซึ่งเรียกว่า Short style จะแตกต่างจากโค้ดของภาษา HTML เพราะ HTML จะใช้เครื่องหมาย < และ

จบด้วย > แท็กของ PHP เป็นตัวบอกเว็บเซิร์ฟเวอร์ของ PHP ว่า โค้ดของภาษา PHP เริ่มต้นและสิ้นสุดที่ไหน หมายถึง การแปล (interpret) แท็กต่างๆ จะเกิดขึ้นที่ฝั่งเซิร์ฟเวอร์ (Server Side Script)

รูปแบบของ PHP มี 4 แบบดังนี้

1. Short Style เช่น

```
<? echo "My program PHP. <BR>" ; ?>
```

รูปแบบนี้จะใช้ตามรูปแบบของ SGML (Standard Generalized Markup Language)

2. XML Style เช่น

```
<? Php echo "My Program PHP. <BR>"; ?>
```

รูปแบบนี้สามารถใช้ได้กับภาษา XML (Extensible Markup Language)

3. Script Style เช่น

```
<Script Language='php'>echo "My program PHP.<BR>"; </Script>
```

ใช้ร่วมกับภาษา HTML ซึ่งระบุภาษาลงไปใน Script เหมือนกับการใช้ Javascript

4. ASP Style เช่น

```
<% echo "My Program PHP. <BR>"; %>
```

ใช้รูปแบบของแท็กเหมือนกับภาษา ASP (Active Server Page)

สาธิต ชัยวิวัฒน์ตระกูล (2550 : 19) กล่าวว่า PHP เป็นซอฟท์แวร์โอเพ่นซอร์ซ ซึ่งได้เปิดเผยซอร์ซโค้ด ผู้อ่านสามารถดาวน์โหลดมาใช้งานได้ฟรีโดยไม่เสียค่าใช้จ่าย และPHP สามารถทำงานได้บนระบบปฏิบัติการที่หลากหลาย ไม่ว่าจะเป็น Windows, Mac OS X, Linux, Solaris, Unix และอื่นๆ สามารถจะทำงานบน Web Server ได้หลายชนิดด้วยกัน เช่น Apache, IIS, Omni HTTPd อีกทั้งยังสามารถทำงานร่วมกับระบบฐานข้อมูลได้หลากหลายชนิด เช่น MySQL, Oracle, Sybase, Informix, DB2, PostgreSQL เป็นต้น อีกทั้งมีไลบรารี ให้สามารถใช้งานมากมายและส่วนขยายเพิ่มเติมการทำงาน (extension) ที่ช่วยอำนวยความสะดวกในการใช้งานมากมาย ตั้งแต่การใช้งานเบื้องต้น และไปจนถึงการใช้งานขั้นสูง ไม่ว่าจะเป็นการสร้างรูปภาพ การสร้างกราฟ การสร้างเอกสาร PDF การสร้าง Flash Movie การทำงานร่วมกับ XML นอกจากนี้ PHP ยังสามารถทำงานร่วมกับโพรโตคอลต่างๆ ได้หลากหลาย เช่น LDAP, IMAP, SNMP, POP3, HTTP, COM เป็นต้น

สมประสงค์ ธิตินิลนิธิ (2545 : 14) กล่าวถึง กลไกในการทำงานของเว็บเพจ สำหรับการสร้างเว็บเพจที่มีความฉลาดสามารถทำได้ดังนี้ คือ การฝังสคริปต์หรือชุดคำสั่งที่ทำงานทางฝั่งเซิร์ฟเวอร์ (server-side script) ไว้ในเว็บเพจ โดยการทำงานของเว็บเพจที่ฝังสคริปต์ภาษา PHP ไว้ เมื่อเว็บบราวเซอร์มีการร้องขอไฟล์ PHP ไฟล์ใด เว็บเซิร์ฟเวอร์ก็จะเรียก PHP engine ขึ้นมาแปล (interpret) และประมวลผลคำสั่งที่อยู่ในไฟล์ PHP นั้น โดยอาจมีการดึงข้อมูลจากฐานข้อมูล หรือ

เขียนข้อมูลลงไปยังฐานข้อมูลด้วย หลังจากนั้นผลลัพธ์ในแบบของ HTML (และสคริปต์ที่ทำงานทางฝั่งบราวเซอร์ เช่น client-side JavaScript) จะถูกส่งกลับไปยังบราวเซอร์ โดยบราวเซอร์ก็จะแสดงผลตามคำสั่ง HTML ที่ได้รับมา ซึ่งย่อมไม่มีคำสั่ง PHP ใดๆ หลงเหลืออยู่ เนื่องจากคำสั่งทั้งหมดถูกแปลและประมวลผลโดย PHP engine ที่ฝั่งเซิร์ฟเวอร์

2.6 งานวิจัยที่เกี่ยวข้อง

Chen Chung Shih (2005) ศึกษาเรื่อง การประเมินความเสี่ยงและการจัดการด้านความมั่นคงปลอดภัยให้กับข้อมูลและสารสนเทศในองค์กร งานวิจัยครั้งนี้ได้รวบรวมทฤษฎี และกฎต่าง ๆ ตามแนวทางของการจัดการด้านความมั่นคงปลอดภัย และการนำมาตรฐาน BS 7799 มาประยุกต์ใช้ในการรักษาความปลอดภัยให้กับข้อมูลและสารสนเทศในองค์กร โดยมีวัตถุประสงค์เพื่อจะศึกษาถึงแนวความคิดในการจัดการด้านการรักษาความปลอดภัยให้กับข้อมูล และการลงทุนเพื่อจะสร้างความรักษาปลอดภัยขึ้นมาภายใต้งบประมาณที่มีอยู่อย่างจำกัด และนำมาใช้งานได้อย่างมีประสิทธิภาพ

Fredrik M Andersson (2004) ศึกษาเรื่อง การนำมาตรฐาน ISO 17799 มาช่วยจัดการด้านความมั่นคงปลอดภัยให้กับข้อมูลในองค์กร ซึ่งในปัจจุบันบริษัทส่วนใหญ่จะมีความตระหนักถึงความสำคัญของข้อมูล เปรียบได้กับทรัพย์สินที่มีค่ามาก มีความต้องการให้ข้อมูลปลอดภัย การนำมาตรฐาน ISO 17799 เข้ามาใช้ช่วยทำให้การทำงานมีความปลอดภัยมากยิ่งขึ้น วัตถุประสงค์ในการจัดทำงานวิจัยนี้ เพื่อศึกษาถึงสถานะปัจจุบันด้านความปลอดภัยของข้อมูลที่มีต่อองค์กร และเป็นการสร้างความต่อเนื่องในการทำงานให้กับธุรกิจ เพื่อให้สามารถดำเนินงาน ได้อย่างต่อเนื่อง และเพื่อเป็นการสร้างกลไกในการเฝ้าระวังความลับ ความสมบูรณ์ครบถ้วน ให้เกิดขึ้นกับข้อมูลที่มีความสำคัญ

Lauri Helenius (2004) ศึกษาเรื่อง ภัยคุกคามที่มีผลกระทบต่อความปลอดภัย ทางด้านข้อมูลในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ระหว่างธุรกิจด้วยกัน เนื่องจากที่ผ่านมาปัญหาและภัยคุกคาม เป็นสิ่งหนึ่งที่มีผลกระทบต่อความปลอดภัยของข้อมูลในการดำเนินงานทางธุรกิจ ซึ่งภัยคุกคามเหล่านี้ ช่วยทำให้เห็นถึงช่องโหว่ หรือจุดอ่อนที่เกิดขึ้นกับข้อมูลเหล่านั้น และช่วยสร้างความตระหนักให้มีเกิดขึ้นในการดำเนินงานทางธุรกิจในอนาคต ซึ่งการรักษาความปลอดภัยให้กับข้อมูลนับเป็นสิ่งสำคัญในการประกอบการและทำธุรกรรมทางอิเล็กทรอนิกส์ เนื่องจากจะเกี่ยวข้องกับการรักษาความลับทางธุรกิจ ความครบถ้วนและความพร้อมใช้งานของข้อมูล การนำมาตรฐาน BS7799 เข้ามาใช้งานภายในองค์กร มีวัตถุประสงค์เพื่อกำหนดระดับของมาตรฐานในการรักษาความปลอดภัยให้กับข้อมูลที่ใช้งานในองค์กร ให้มีประสิทธิภาพและความปลอดภัยมากยิ่งขึ้น

Oumeshsingh Sookdawoor (2005) ศึกษาเรื่อง นโยบายและแนวทางการปฏิบัติด้านการรักษาความปลอดภัยให้กับข้อมูลและสารสนเทศของบริษัทต่าง ๆ ที่ส่วนใหญ่มีความจำเป็นในการใช้งานทางด้านเทคโนโลยีสารสนเทศในพื้นที่ของมอริเชียส (Mauritius) การวิจัยครั้งนี้ มีวัตถุประสงค์เพื่อหาแนวทางในการจัดทำการประเมินความเสี่ยงและการรักษาความปลอดภัย ให้กับสารสนเทศของธุรกิจ โดยใช้มาตรฐานที่เป็นสากลเช่น BS 7799 สำหรับแนวทางในการจัดทำนโยบายทางด้านการรักษาความปลอดภัยให้กับสารสนเทศขององค์กร และการนำนโยบายที่ได้สร้างขึ้นมาปฏิบัติใช้อย่างจริงจังให้เกิดผลและมีประสิทธิภาพ

DPU

บทที่ 3
ระเบียบวิธีวิจัย

3.1 ขั้นตอนการดำเนินการวิจัย

ขั้นตอนการดำเนินการวิจัย มีดังต่อไปนี้

1. ศึกษาข้อมูลทรัพย์สินสารสนเทศภายในองค์กร
2. เก็บรวบรวมและจัดหมวดหมู่ของทรัพย์สินสารสนเทศแยกตามประเภทระบบงาน
3. ประเมินความเสี่ยงทางด้านทรัพย์สินสารสนเทศ
4. กำหนดมาตรการป้องกัน
5. วิเคราะห์และออกแบบระบบต้นแบบ
6. จัดทำและทดสอบการเผยแพร่ข้อมูล
7. สรุปผลการวิจัยและข้อเสนอแนะ

3.2 อุปกรณ์และเครื่องมือที่ใช้ในการวิจัย

3.2.1 อุปกรณ์ฮาร์ดแวร์ที่จะนำมาใช้

1. เครื่องเซิร์ฟเวอร์
   - หน่วยประมวลผล Intel Xeon 2.4 Ghz
   - หน่วยความจำ (RAM) 1 Gigabyte
   - ความจุของฮาร์ดดิสก์ 136 Gigabyte
   - จอภาพขนาด 15 นิ้ว
   - เม้าส์ และแป้นพิมพ์
2. เครื่องไคลเอนต์
   - เครื่องคอมพิวเตอร์ ระดับ Pentium IV 2.4 Ghz
   - หน่วยความจำ (RAM) 256 Megabyte
   - ความจุของฮาร์ดดิสก์ 60 Gigabyte
   - จอภาพขนาด 15 นิ้ว
   - เม้าส์ และแป้นพิมพ์

3. เครื่องคอมพิวเตอร์โน้ตบุ๊ค

- ระดับ Pentium M 1.73 Ghz
- หน่วยความจำ (RAM) 2 Gigabyte
- ความจุของฮาร์ดดิสก์ 60 Gigabyte
- จอภาพขนาด 15 นิ้ว
- เม้าส์ และแป้นพิมพ์

3.2.2 ซอฟต์แวร์ที่จะนำมาใช้

1. เครื่องเซิร์ฟเวอร์

- ระบบปฏิบัติการ Windows 2003 Server
- Appserv สำหรับจัดทำเว็บเซิร์ฟเวอร์
- ความจุของฮาร์ดดิสก์ 136 Gigabyte
- จอภาพขนาด 15 นิ้ว
- เม้าส์ และแป้นพิมพ์

2. เครื่องไคลเอนต์

- ระบบปฏิบัติการ Windows XP Professional
- เว็บเบราว์เซอร์ Internet Explorer 6.0

DPU

3.3 ระยะเวลาในการดำเนินการวิจัย

ระยะเวลาในการดำเนินการวิจัย สรุปได้ดังตารางที่ 3.1

ตารางที่ 3.1 ระยะเวลาในการดำเนินการวิจัย

ระยะเวลาดำเนินงาน (เดือน)	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1. ศึกษาข้อมูลทางด้านทรัพย์สินสารสนเทศภายในองค์กร												
2. จัดหมวดหมู่ของทรัพย์สินสารสนเทศแยกตามระบบงาน												
3. ประเมินความเสี่ยงทางด้านทรัพย์สินสารสนเทศ												
4. กำหนดมาตรการป้องกัน												
5. วิเคราะห์และออกแบบระบบต้นแบบ												
6. จัดทำและทดสอบการเผยแพร่ข้อมูล												
7. สรุปผลการวิจัยและข้อเสนอแนะ												
8. เรียบเรียงงานค้นคว้าอิสระ												

3.4 สรุป

ขั้นตอนในการดำเนินการวิจัย ผู้วิจัยได้มีการแบ่งขั้นตอนที่จะศึกษาออกเป็น 7 ขั้นตอน ได้แก่ ขั้นตอนของการศึกษาข้อมูลทรัพย์สินสารสนเทศภายในองค์กร ขั้นตอนการจัดหมวดหมู่ของทรัพย์สินสารสนเทศ เพื่อแยกตามระบบงาน ขั้นตอนการประเมินความเสี่ยงที่เกี่ยวกับด้านทรัพย์สินสารสนเทศ ขั้นตอนการกำหนดมาตรการป้องกัน ขั้นตอนการวิเคราะห์และออกแบบระบบต้นแบบ ขั้นตอนการจัดทำและทดสอบการเผยแพร่ข้อมูล และขั้นตอนการสรุปผลการวิจัยและข้อเสนอแนะ

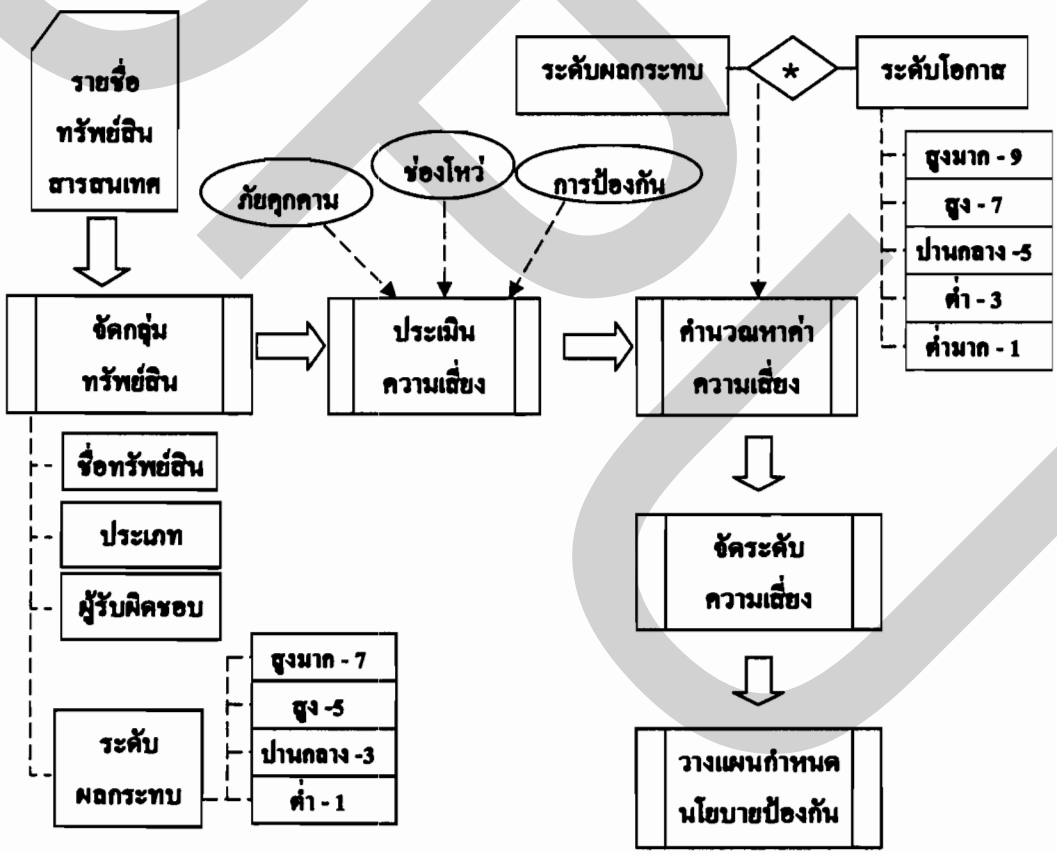
DPU

บทที่ 4
การวิเคราะห์และการออกแบบระบบ

เนื้อหาของบทนี้กล่าวถึง การศึกษาด้านการจัดการความเสี่ยง การวิเคราะห์ระบบ และการออกแบบระบบ โดยมีรายละเอียดดังต่อไปนี้

4.1 การศึกษาด้านการจัดการความเสี่ยง

กระบวนการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศ ประกอบด้วยขั้นตอน และข้อมูลต่าง ๆ ซึ่งสามารถสรุปได้ดังภาพที่ 4.1 โดยมีรายละเอียดดังต่อไปนี้



ภาพที่ 4.1 กระบวนการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศ

4.1.1 การจัดกลุ่มของทรัพย์สินสารสนเทศ การจัดการความเสี่ยง จัดทำโดยแบ่งหมวดหมู่ของทรัพย์สินสารสนเทศ (Asset Inventory) แยกตามองค์ประกอบของระบบงานคอมพิวเตอร์ ซึ่งได้แก่ อุปกรณ์คอมพิวเตอร์ โปรแกรม บุคลากร ข้อมูล และบริการ สามารถสรุปได้ดังตารางที่ 4.1 – 4.5 โดยมีรายละเอียดดังต่อไปนี้

ตารางที่ 4.1 รายชื่อทรัพย์สินทางด้านอุปกรณ์คอมพิวเตอร์

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
เครื่องแม่ข่ายสำหรับระบบ Web Server	เครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
เครื่องแม่ข่ายสำหรับระบบห้องสมุดอัตโนมัติ	เครื่องแม่ข่าย	ฝ่ายเทคโนโลยีสารสนเทศ
เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง	เครื่องลูกข่าย	ฝ่ายงานต่าง ๆ
สื่อบันทึกข้อมูลแผ่นซีดี	สื่อบันทึกข้อมูล	ฝ่ายเทคโนโลยีสารสนเทศ
เทปแบ็คอัพ	สื่อบันทึกข้อมูล	ฝ่ายเทคโนโลยีสารสนเทศ

ตารางที่ 4.2 รายชื่อทรัพย์สินทางด้านโปรแกรม

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
ระบบฐานข้อมูล SQL Server	ระบบฐานข้อมูล	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบปฏิบัติการ Microsoft Windows	ระบบปฏิบัติการ	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบปฏิบัติการ Linux	ระบบปฏิบัติการ	ฝ่ายเทคโนโลยีสารสนเทศ
โปรแกรมต่าง ๆ	โปรแกรม	ฝ่ายเทคโนโลยีสารสนเทศ

ตารางที่ 4.3 รายชื่อทรัพย์สินทางด้านบุคลากร

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
บุคลากร	ผู้บริหารระดับสูง	บุคลากร
บุคลากร	ผู้บริหารระดับกลาง	บุคลากร
บุคลากร	พนักงานทั่วไป	บุคลากร

ตารางที่ 4.4 รายชื่อทรัพย์สินทางด้านข้อมูล

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
ระบบ Web Server	ข้อมูล	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบห้องสมุดอัตโนมัติ	ข้อมูล	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบฐานข้อมูลสหบรรณานุกรม	ข้อมูล	ฝ่ายเทคโนโลยีสารสนเทศ

ตารางที่ 4.5 รายชื่อทรัพย์สินทางด้านงานบริการ

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
งานบริการ Internet	Communication	ฝ่ายเทคโนโลยีสารสนเทศ
ระบบปรับอากาศ (ห้องServer)	Technical	ฝ่ายอาคารสถานที่
งานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้	Computing	ฝ่ายเทคโนโลยีสารสนเทศ
งานติดตั้ง บำรุงรักษาอุปกรณ์คอมพิวเตอร์	Technical	ฝ่ายเทคโนโลยีสารสนเทศ
งานติดตั้ง บำรุงรักษาโปรแกรมคอมพิวเตอร์	Technical	ฝ่ายเทคโนโลยีสารสนเทศ

ตารางที่ 4.5 (ต่อ) รายชื่อทรัพย์สินทางด้านงานบริการ

ชื่อทรัพย์สิน	ประเภท	ผู้รับผิดชอบ
งานบริการระบบ Web Server	Computing	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริการระบบห้องสมุดอัตโนมัติ	Computing	ฝ่ายเทคโนโลยีสารสนเทศ
งานบริการระบบฐานข้อมูลสหบรรณานุกรม	Computing	ฝ่ายเทคโนโลยีสารสนเทศ

4.1.2 การประเมินความเสี่ยงและคำนวณหาค่าความเสี่ยงโดยรวม สำหรับขั้นตอนการประเมินหาความเสี่ยงที่จะเกิดขึ้นต่อทรัพย์สินสารสนเทศภายในองค์กร จะใช้แนวทางจากมาตรการควบคุม ซึ่งได้มีการนำมาจากหนังสือ "มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2) ประจำปี 2549" ซึ่งมีมาตรการป้องกันต่างๆ โดยนำมาตรการเหล่านั้นมาใช้เป็นตัวเปรียบเทียบ เพื่อค้นหาถึงช่องโหว่ (Vulnerability) ที่เป็นจุดอ่อน (Weakness) และจุดแข็ง (Strength) ที่มีอยู่แล้ว และภัยคุกคามหรือปัญหา (Threat) ที่เกิดขึ้น เพื่อจะนำไปคำนวณหาค่าความเสี่ยงโดยรวม (Risk Value)

ในการหาค่าความเสี่ยงโดยรวมที่เกิดขึ้นกับทรัพย์สินสารสนเทศในแต่ละประเภทนั้น จะมีการวิเคราะห์ถึงระดับของผลกระทบและระดับของโอกาส ที่จะเกิดขึ้นกับทรัพย์สินในแต่ละประเภท แล้วนำค่าของผลกระทบและโอกาสที่ได้มา เพื่อใช้ในการคำนวณหาค่าความเสี่ยงโดยรวม แล้วนำค่าของความเสี่ยงโดยรวมที่ได้ ไปทำการจัดลำดับแยกตามระดับของค่าความเสี่ยง และแยกตามกลุ่มของทรัพย์สินสารสนเทศ เพื่อที่จะทราบได้ว่าภายในองค์กรมีความเสี่ยงอะไรเกิดขึ้นบ้าง และระดับความเสี่ยงเป็นอย่างไร หากค่าของความเสี่ยงอยู่ในระดับที่สูง ก็จะจัดทำแผนการที่จะนำไปใช้เป็นแนวทางเพื่อกำหนดมาตรการป้องกันให้กับทรัพย์สินสารสนเทศนั้น ๆ เป็นขั้นตอนถัดไป สามารถสรุปได้ดังตารางที่ 4.6 – 4.101 โดยมีรายละเอียดดังต่อไปนี้

อุปกรณ์คอมพิวเตอร์ (Hardware)

ตารางที่ 4.6 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server (มาตรการที่ 9.1.2)

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบ Web Server					
A.9.1.2 การควบคุมการเข้า-ออก (Physical entry controls)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น		1	5	5	

ตารางที่ 4.7 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server (มาตรการที่ 9.2.1)

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบ Web Server					
A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) การจัดวางอุปกรณ์อยู่ในบริเวณที่มีคลื่นแม่เหล็กไฟฟ้ารบกวน	อุปกรณ์ทำงานผิดพลาด	7	5	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้า

ตารางที่ 4.8 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server (มาตรการที่ 9.2.4)

ชื่อทรัพย์สิน : เครื่อง แม่ข่ายระบบ Web Server					
A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการวางแผนในการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ	อุปกรณ์ทำงานผิดพลาด	7	5	35	กำหนดตารางการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ

ตารางที่ 4.9 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server (มาตรการที่ 10.1.1)

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบ Web Server					
A.10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ไม่มีคู่มือขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร	เกิดความผิดพลาดในการกำหนดค่าต่างๆให้กับอุปกรณ์	9	7	63	จัดทำคู่มือการปฏิบัติงานสำหรับเครื่อง server

ตารางที่ 4.10 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server (มาตรการที่ 10.4.1)

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบ Web Server					
A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) การใช้เครื่อง server เข้าถึงหน้าเว็บบางแห่งและดาวน์โหลดข้อมูลจากแหล่งที่ไม่เหมาะสม	เครื่อง server ติดไวรัส	7	5	35	- ติดตั้งโปรแกรมป้องกันไวรัส - ให้ความรู้แก่เจ้าหน้าที่ด้านความปลอดภัยของข้อมูล

ตารางที่ 4.11 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ (มาตรการที่ 9.1.2)

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ					
A.9.1.2 การควบคุมการเข้า-ออก (Physical entry controls)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น		1	5	5	

ตารางที่ 4.12 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ (มาตรการที่ 9.2.1)

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ					
A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) การจัดวางอุปกรณ์อยู่ในบริเวณที่มีคลื่นแม่เหล็กไฟฟ้ารบกวน	อุปกรณ์ทำงานผิดพลาด	7	5	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้ารบกวน

ตารางที่ 4.13 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ (มาตรการที่ 9.2.4)

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ					
A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการวางแผนในการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ	อุปกรณ์ทำงานผิดพลาด	7	5	35	กำหนดตารางการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ

ตารางที่ 4.14 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ (มาตรการที่ 10.1.1)

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ					
A.10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ไม่มีคู่มือขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร	เกิดความผิดพลาดในการกำหนดค่าต่างๆให้กับอุปกรณ์	9	7	63	- จัดทำคู่มือการปฏิบัติงานสำหรับเครื่อง server

ตารางที่ 4.15 การประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ (มาตรการที่ 10.4.1)

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ					
A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) การใช้เครื่อง server เข้าถึงหน้าเว็บบางแห่งและดาวน์โหลดข้อมูลจากแหล่งที่ไม่เหมาะสม	เครื่อง server ติดไวรัส	7	5	35	- ติดตั้งโปรแกรมป้องกันไวรัส - ให้ความรู้แก่เจ้าหน้าที่ด้านความปลอดภัยของข้อมูล

ตารางที่ 4.16 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 7.1.1)

ชื่อทรัพย์สิน : เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง					
A.7.1.1 การจัดทำบัญชีทรัพย์สิน (Inventory of assets)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการจัดทำและแก้ไขทะเบียนครุภัณฑ์คอมพิวเตอร์ให้ถูกต้องอยู่เสมอ		1	1	1	

ตารางที่ 4.17 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 7.1.2)

ชื่อทรัพย์สิน : เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง					
A.7.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) จัดให้มีการระบุผู้เป็นเจ้าของในเครื่องคอมพิวเตอร์แต่ละเครื่อง		1	1	1	

ตารางที่ 4.18 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 9.2.1)

ชื่อทรัพย์สิน : เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง					
A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) การจัดวางอุปกรณ์อยู่ในบริเวณที่มีคลื่นแม่เหล็กไฟฟ้ารบกวน	อุปกรณ์ทำงานผิดพลาด	7	5	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้ารบกวน

ตารางที่ 4.19 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 9.2.4)

ชื่อทรัพย์สิน : เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง					
A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการวางแผนในการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ	อุปกรณ์ทำงานผิดพลาด	7	5	35	กำหนดตารางการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ

ตารางที่ 4.20 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 9.2.6)

ชื่อทรัพย์สิน : เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง					
A.9.2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal of re-use of equipment)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการตรวจสอบการลบทิ้งของข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้งานแล้ว	ข้อมูลที่เป็นความลับถูกเปิดเผย	5	5	25	มีการตรวจสอบการลบทิ้งของข้อมูลภายในเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้งานแล้ว

ตารางที่ 4.21 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 9.2.7)

ชื่อทรัพย์สิน : เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง					
A.9.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) ห้ามนำทรัพย์สินในองค์กรออกไปภายนอก นอกจากได้รับอนุญาตเท่านั้น		3	5	15	

ตารางที่ 4.22 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 10.4.1)

ชื่อทรัพย์สิน : เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง					
A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการตรวจจับและป้องกันจากโปรแกรมไม่ประสงค์ดี อย่างทั่วถึง	- เครื่องคอมพิวเตอร์ทำงานผิดพลาด - เครื่องคอมพิวเตอร์ติดไวรัส	7	5	35	- ติดตั้งโปรแกรมเพื่อใช้ตรวจจับและป้องกันจากโปรแกรมไม่ประสงค์ดีอย่างทั่วถึง

ตารางที่ 4.23 การประเมินความเสี่ยงสำหรับเครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง (มาตรการที่ 10.5.1)

ชื่อทรัพย์สิน : เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง					
A.10.5.1 การสำรองข้อมูล (Back-up)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการสำรองข้อมูลที่สำคัญในเครื่องคอมพิวเตอร์ที่ใช้งานเฉพาะทางอย่างสม่ำเสมอ	ข้อมูลเกิดการสูญหายและขาดความครบถ้วน	5	7	35	วางแผนการสำรองข้อมูลอย่างสม่ำเสมอ

ตารางที่ 4.24 การประเมินความเสี่ยงสำหรับสื่อบันทึกข้อมูลแผ่นซีดี (มาตรการที่ 9.2.7)

ชื่อทรัพย์สิน : สื่อบันทึกข้อมูลแผ่นซีดี					
A.9.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) ไม่อนุญาตให้นำทรัพย์สินในองค์กรออกไปภายนอกนอกจากจะได้รับอนุญาตแล้วเท่านั้น		3	5	15	

ตารางที่ 4.25 การประเมินความเสี่ยงสำหรับสื่อบันทึกข้อมูลแผ่นซีดี (มาตรการที่ 10.7.1)

ชื่อทรัพย์สิน : สื่อบันทึกข้อมูลแผ่นซีดี					
A.10.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) ไม่อนุญาตให้นำสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ออกไปนอกองค์กรจนกว่าจะได้รับอนุญาตแล้วเท่านั้น		3	5	15	

ตารางที่ 4.26 การประเมินความเสี่ยงสำหรับสื่อบันทึกข้อมูลแผ่นซีดี (มาตรการที่ 10.7.2)

ชื่อทรัพย์สิน : สื่อบันทึกข้อมูลแผ่นซีดี					
A.10.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดขั้นตอนปฏิบัติที่ชัดเจนสำหรับการทำลายสื่อบันทึกข้อมูล	ข้อมูลที่สำคัญถูกเปิดเผยโดยไม่ได้รับอนุญาต	7	5	35	มีการกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลไว้อย่างชัดเจน

ตารางที่ 4.27 การประเมินความเสี่ยงสำหรับเทปแบ็คอัพ (มาตรการที่ 9.2.7)

ชื่อทรัพย์สิน : เทปแบ็คอัพ					
A.9.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) ไม่อนุญาตให้นำทรัพย์สินในองค์กรออกไปภายนอกนอกจากจะได้รับอนุญาตแล้วเท่านั้น		3	5	15	

ตารางที่ 4.28 การประเมินความเสี่ยงสำหรับเทปแบ็คอัพ (มาตรการที่ 10.7.1)

ชื่อทรัพย์สิน : เทปแบ็คอัพ					
A.10.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) ไม่อนุญาตให้นำสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ออกไปนอกองค์กรจนกว่าจะได้รับอนุญาตแล้วเท่านั้น		3	5	15	

ตารางที่ 4.29 การประเมินความเสี่ยงสำหรับเทปแบ็คอัพ (มาตรการที่ 10.7.2)

ชื่อทรัพย์สิน : เทปแบ็คอัพ					
A.10.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดขั้นตอนปฏิบัติที่ชัดเจนสำหรับการทำลายสื่อบันทึกข้อมูล	ข้อมูลที่สำคัญถูกเปิดเผยโดยไม่ได้รับอนุญาต	7	5	35	มีการกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลไว้อย่างชัดเจน

ชื่อทรัพย์สิน : ระบบฐานข้อมูล SQL Server					
A.12.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ		1	5	5	

ตารางที่ 4.31 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูล SQL Server (มาตรการที่ 12.5.1)

ชื่อทรัพย์สิน : ระบบฐานข้อมูล SQL Server					
A.12.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) การกำหนดขั้นตอนปฏิบัติในการควบคุมการแก้ไขระบบ ยังไม่ครอบคลุมทั้งหมด	การปฏิบัติงานของระบบผิดพลาด	5	5	25	จัดทำขั้นตอนปฏิบัติในการแก้ไขระบบที่มีความครอบคลุมในทุกขั้นตอน

ตารางที่ 4.32 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูล SQL Server (มาตรการที่ 12.6.1)

ชื่อทรัพย์สิน : ระบบฐานข้อมูล SQL Server					
A.12.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่และทำการปรับปรุงในระบบที่ใช้งานอย่างสม่ำเสมอ		1	7	7	

ตารางที่ 4.33 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Microsoft Windows (มาตรการที่ 10.4.1)

ชื่อทรัพย์สิน : ระบบปฏิบัติการ Microsoft Windows					
A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ผู้ใช้งานขาดความตระหนักในการตรวจจับ และป้องกันภัยจากโปรแกรมที่ไม่ประสงค์ดี	ระบบทำงานผิดพลาด	7	7	49	มีการสร้างความตระหนักในผู้ใช้ในการป้องกันภัยจากโปรแกรมที่ไม่ประสงค์ดี

ตารางที่ 4.34 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Microsoft Windows (มาตรการที่ 12.4.1)

ชื่อทรัพย์สิน : ระบบปฏิบัติการ Microsoft Windows					
A.12.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการควบคุมการติดตั้งโปรแกรมต่าง ๆ ลงไปยังระบบปฏิบัติการที่ให้บริการ	ระบบทำงานผิดพลาด	3	7	21	กำหนดให้มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งโปรแกรมต่าง ๆ ลงไปยังระบบปฏิบัติการที่ให้บริการ

ตารางที่ 4.35 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Microsoft Windows (มาตรการที่ 12.4.3)

ชื่อทรัพย์สิน : ระบบปฏิบัติการ Microsoft Windows					
A.12.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) จำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ		1	5	5	

ตารางที่ 4.36 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Microsoft Windows (มาตรการที่ 12.5.1)

ชื่อทรัพย์สิน : ระบบปฏิบัติการ Microsoft Windows					
A.12.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) การกำหนดขั้นตอนปฏิบัติในการควบคุมการแก้ไขระบบ ยังไม่ครอบคลุมทั้งหมด	การปฏิบัติงานของระบบผิดพลาด	5	5	25	จัดทำขั้นตอนปฏิบัติในการแก้ไขระบบที่มีความครอบคลุมในทุกขั้นตอน

ตารางที่ 4.37 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Microsoft Windows (มาตรการที่ 12.6.1)

ชื่อทรัพย์สิน : ระบบปฏิบัติการ Microsoft Windows					
A.12.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่และทำการปรับปรุงในระบบที่ใช้งานอย่างสม่ำเสมอ		1	7	7	

ตารางที่ 4.38 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Linux (มาตรการที่ 12.4.1)

ชื่อทรัพย์สิน : ระบบปฏิบัติการ Linux					
A.12.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการควบคุมการติดตั้งโปรแกรมต่าง ๆ ลงไปยังระบบปฏิบัติการที่ให้บริการ		3	3	9	

ตารางที่ 4.39 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Linux (มาตรการที่ 12.4.3)

ชื่อทรัพย์สิน : ระบบปฏิบัติการ Linux					
A.12.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ		1	5	5	

ตารางที่ 4.40 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Linux (มาตรการที่ 12.5.1)

ชื่อทรัพย์สิน : ระบบปฏิบัติการ Linux					
A.12.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) การกำหนดขั้นตอนปฏิบัติในการควบคุมการแก้ไขระบบ ยังไม่ครอบคลุมทั้งหมด	การปฏิบัติงานของระบบผิดพลาด	5	5	25	จัดทำขั้นตอนปฏิบัติในการแก้ไขระบบที่มีความครอบคลุมในทุกขั้นตอน

ตารางที่ 4.41 การประเมินความเสี่ยงสำหรับระบบปฏิบัติการ Linux (มาตรการที่ 12.6.1)

ชื่อทรัพย์สิน : ระบบปฏิบัติการ Linux					
A.12.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่และทำการปรับปรุงในระบบที่ใช้งานอย่างสม่ำเสมอ		1	7	7	

ตารางที่ 4.42 การประเมินความเสี่ยงสำหรับโปรแกรมต่าง ๆ (มาตรการที่ 12.6.1)

ชื่อทรัพย์สิน : โปรแกรมต่าง ๆ					
A.12.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ของโปรแกรม และปรับปรุงให้ทันสมัยอยู่เสมอ	ระบบถูกบุกรุกและข้อมูลเกิดความเสียหาย	7	5	35	มีการติดตามข้อมูลข่าวสารที่เกี่ยวกับช่องโหว่ของโปรแกรมและปรับปรุงให้ทันสมัยอยู่เสมอ

บุคลากร (People)

ตารางที่ 4.43 การประเมินความเสี่ยงสำหรับบุคลากร (มาตรการที่ 8.1.1)

ชื่อทรัพย์สิน : บุคลากร					
A.8.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and responsibilities)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) กำหนดความรับผิดชอบด้านความมั่นคงปลอดภัยสำหรับสารสนเทศให้แก่พนักงาน		1	5	5	

ตารางที่ 4.44 การประเมินความเสี่ยงสำหรับบุคลากร (มาตรการที่ 8.1.2)

ชื่อทรัพย์สิน : บุคลากร					
A.8.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการตรวจสอบคุณสมบัติของผู้สมัครโดยละเอียดเพื่อความปลอดภัยสำหรับสารสนเทศขององค์กร		1	5	5	

ตารางที่ 4.45 การประเมินความเสี่ยงสำหรับบุคลากร (มาตรการที่ 8.2.2)

ชื่อทรัพย์สิน : บุคลากร					
A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) การสร้างความตระหนักและให้ความรู้ด้านความมั่นคงปลอดภัยแก่พนักงาน ไม่มีความสม่ำเสมอ	การปฏิบัติงานเกิดการผิดพลาด	7	3	21	จัดให้มีการอบรมด้านการรักษาความมั่นคงปลอดภัยขององค์กรอย่างสม่ำเสมอ

ตารางที่ 4.46 การประเมินความเสี่ยงสำหรับบุคลากร (มาตรการที่ 8.3.2)

ชื่อทรัพย์สิน : บุคลากร					
A.8.3.2 การคืนทรัพย์สินขององค์กร (Return of assets)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการกำหนดให้ผู้ที่สิ้นสุดการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน		1	5	5	

ตารางที่ 4.47 การประเมินความเสี่ยงสำหรับบุคลากร (มาตรการที่ 8.3.3)

ชื่อทรัพย์สิน : บุคลากร					
A.8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการถอดถอนสิทธิในการเข้าถึงสารสนเทศของผู้ที่สิ้นสุดการจ้างงาน	ระบบสารสนเทศถูกใช้โดยไม่ได้รับอนุญาต	3	7	21	มีการทบทวนสิทธิในการเข้าถึงสารสนเทศของพนักงานอย่างสม่ำเสมอ

ข้อมูล (Information)

ตารางที่ 4.48 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 6.1.5)

ชื่อทรัพย์สิน : ระบบ Web Server					
A.6.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการจัดทำข้อตกลงห้ามเปิดเผยความลับขององค์กร		1	5	5	

ตารางที่ 4.49 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 7.1.3)

ชื่อทรัพย์สิน : ระบบ Web Server					
A.7.1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการจัดทำกฎระเบียบในการใช้งานสารสนเทศอย่างถูกวิธี เพื่อป้องกันความเสียหายต่อทรัพย์สิน		3	3	9	

ตารางที่ 4.50 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 8.3.3)

ชื่อทรัพย์สิน : ระบบ Web Server					
A.8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดความสม่ำเสมอในการทบทวน การถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงาน	การเข้าถึงระบบข้อมูลโดยไม่ได้รับอนุญาต	3	7	21	มีการทบทวนการถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงานอย่างสม่ำเสมอ

ตารางที่ 4.51 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 10.5.1)

ชื่อทรัพย์สิน : ระบบ Web Server					
A.10.5.1 การสำรองข้อมูล (Information back-up)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการสำรองข้อมูลอย่างสม่ำเสมอ		1	5	5	

ตารางที่ 4.52 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 10.10.2)

ชื่อทรัพย์สิน : ระบบ Web Server					
A.10.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอเพื่อป้องกันข้อผิดพลาดที่จะเกิดขึ้น		1	5	5	

ตารางที่ 4.53 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 11.2.1)

ชื่อทรัพย์สิน : ระบบ Web Server					
A.11.2.1 การลงทะเบียนพนักงาน (User registration)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนของพนักงานใหม่ในการกำหนดสิทธิเพื่อเข้าใช้งานระบบ		1	5	5	

ตารางที่ 4.54 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 12.4.1)

ชื่อทรัพย์สิน : ระบบ Web Server					
A.12.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการป้องกันการติดตั้งโปรแกรมต่างๆ ลงไปยังระบบที่ให้บริการ เพื่อป้องกันการผิดพลาดที่จะเกิดขึ้นในการทำงานของระบบ		1	5	5	

ตารางที่ 4.55 การประเมินความเสี่ยงสำหรับระบบ Web Server (มาตรการที่ 12.4.3)

ชื่อทรัพย์สิน : ระบบ Web Server					
A.12.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการจำกัดการเข้าถึงซอร์สโค้ดของระบบที่ให้บริการเพื่อป้องกันการเปลี่ยนแปลง		1	5	5	

ตารางที่ 4.56 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 6.1.5)

ชื่อทรัพย์สิน : ระบบห้องสมุดอัตโนมัติ					
A.6.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการจัดทำข้อตกลงห้ามเปิดเผยความลับขององค์กร		1	5	5	

ตารางที่ 4.57 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 7.1.3)

ชื่อทรัพย์สิน : ระบบห้องสมุดอัตโนมัติ					
A.7.1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการจัดทำกฎระเบียบในการใช้งานสารสนเทศอย่างถูกวิธี เพื่อป้องกันความเสียหายต่อทรัพย์สิน		3	3	9	

ตารางที่ 4.58 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 8.3.3)

ชื่อทรัพย์สิน : ระบบห้องสมุดอัตโนมัติ					
A.8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดความสม่ำเสมอในการทบทวน การถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงาน	การเข้าถึงระบบข้อมูลโดยไม่ได้รับอนุญาต	3	7	21	มีการทบทวนการถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงานอย่างสม่ำเสมอ

ตารางที่ 4.59 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 10.5.1)

ชื่อทรัพย์สิน : ระบบห้องสมุดอัตโนมัติ					
A.10.5.1 การสำรองข้อมูล (Information back-up)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการสำรองข้อมูลอย่างสม่ำเสมอ		1	5	5	

ตารางที่ 4.60 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 10.10.2)

ชื่อทรัพย์สิน : ระบบห้องสมุดอัตโนมัติ					
A.10.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอเพื่อป้องกันข้อผิดพลาดที่จะเกิดขึ้น		1	5	5	

ตารางที่ 4.61 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 11.2.1)

ชื่อทรัพย์สิน : ระบบห้องสมุดอัตโนมัติ					
A.11.2.1 การลงทะเบียนพนักงาน (User registration)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนของพนักงานใหม่ในการกำหนดสิทธิเพื่อเข้าใช้งานระบบ		1	5	5	

ตารางที่ 4.62 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 12.4.1)

ชื่อทรัพย์สิน : ระบบห้องสมุดอัตโนมัติ					
A.12.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการป้องกันการติดตั้งโปรแกรมต่างๆ ลงไปยังระบบที่ให้บริการ เพื่อป้องกันการผิดพลาดที่จะเกิดขึ้นในการทำงานของระบบ		1	5	5	

ตารางที่ 4.63 การประเมินความเสี่ยงสำหรับระบบห้องสมุดอัตโนมัติ (มาตรการที่ 12.4.3)

ชื่อทรัพย์สิน : ระบบห้องสมุดอัตโนมัติ					
A.12.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการจำกัดการเข้าถึงซอร์สโค้ดของระบบที่ให้บริการเพื่อป้องกันการเปลี่ยนแปลง		1	5	5	

ตารางที่ 4.64 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 6.1.5)

ชื่อทรัพย์สิน : ระบบฐานข้อมูลสหบรรณานุกรม					
A.6.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการจัดทำข้อตกลงห้ามเปิดเผยความลับขององค์กร		1	5	5	

ตารางที่ 4.65 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 7.1.3)

ชื่อทรัพย์สิน : ระบบฐานข้อมูลสหบรรณานุกรม					
A.7.1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการจัดทำกฎระเบียบในการใช้งานสารสนเทศอย่างถูกวิธี เพื่อป้องกันความเสียหายต่อทรัพย์สิน		3	3	9	

ตารางที่ 4.66 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 8.3.3)

ชื่อทรัพย์สิน : ระบบฐานข้อมูลสหบรรณานุกรม					
A.8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดความสม่ำเสมอในการทบทวน การถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงาน	การเข้าถึงระบบข้อมูลโดยไม่ได้รับอนุญาต	3	7	21	มีการทบทวนการถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงานอย่างสม่ำเสมอ

ตารางที่ 4.67 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 10.5.1)

ชื่อทรัพย์สิน : ระบบฐานข้อมูลสหบรรณานุกรม					
A.10.5.1 การสำรองข้อมูล (Information back-up)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการสำรองข้อมูลอย่างสม่ำเสมอ		1	5	5	

ตารางที่ 4.68 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 10.10.2)

ชื่อทรัพย์สิน : ระบบฐานข้อมูลสหบรรณานุกรม					
A.10.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการตรวจสอบการใช้งานระบบอย่างสม่ำเสมอเพื่อป้องกันข้อผิดพลาดที่จะเกิดขึ้น		1	5	5	

ตารางที่ 4.69 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 11.2.1)

ชื่อทรัพย์สิน : ระบบฐานข้อมูลสหบรรณานุกรม					
A.11.2.1 การลงทะเบียนพนักงาน (User registration)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนของพนักงานใหม่ในการกำหนดสิทธิเพื่อเข้าใช้งานระบบ		1	5	5	

ตารางที่ 4.70 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 12.4.1)

ชื่อทรัพย์สิน : ระบบฐานข้อมูลสหบรรณานุกรม					
A.12.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) ป้องกันการติดตั้งโปรแกรมลงไปยังระบบที่ให้บริการ เพื่อป้องกันระบบทำงานผิดพลาด		1	5	5	

ตารางที่ 4.71 การประเมินความเสี่ยงสำหรับระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 12.4.3)

ชื่อทรัพย์สิน : ระบบฐานข้อมูลสหบรรณานุกรม					
A.12.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) จำกัดการเข้าถึงซอร์สโค้ดของระบบเพื่อป้องกันการเปลี่ยนแปลง		1	5	5	

งานบริการ (Service)

A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ผู้ปฏิบัติงานขาดความตระหนักและความรู้ด้านความปลอดภัยในการใช้งานระบบ	การปฏิบัติงานผิดพลาด	7	5	35	มีการอบรมเพื่อสร้างความตระหนักด้านความปลอดภัยในการใช้งาน

ตารางที่ 4.73 การประเมินความเสี่ยงสำหรับงานบริการ Internet (มาตรการที่ 10.6.1)

ชื่อทรัพย์สิน : งานบริการ Internet					
A.10.6.1 มาตรการทางเครือข่าย (Network controls)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดความสม่ำเสมอในการดูแลระบบและสารสนเทศต่าง ๆ ที่ส่งผ่านเครือข่าย	เครื่องคอมพิวเตอร์ติดไวรัส	7	5	35	มีการดูแลรักษาความปลอดภัยให้กับระบบอย่างสม่ำเสมอ

ตารางที่ 4.74 การประเมินความเสี่ยงสำหรับงานบริการ Internet (มาตรการที่ 11.5.2)

ชื่อทรัพย์สิน : งานบริการ Internet					
A.11.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) ผู้ใช้งานต้องมีการระบุตัวตนก่อนเข้าใช้งานระบบ		1	5	5	

ตารางที่ 4.75 การประเมินความเสี่ยงสำหรับงานบริการ Internet (มาตรการที่ 11.5.5)

ชื่อทรัพย์สิน : งานบริการ Internet					
A.11.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการกำหนดให้ระบบตัดการใช้งานผู้ใช้ เมื่อไม่ได้ใช้งานตามระยะเวลาที่กำหนดไว้		1	5	5	

ตารางที่ 4.76 การประเมินความเสี่ยงสำหรับระบบปรับอากาศ (ห้อง Server) (มาตรการที่ 9.2.4)

ชื่อทรัพย์สิน : ระบบปรับอากาศ (ห้อง Server)					
A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดความสม่ำเสมอในการบำรุงรักษาอุปกรณ์และขาดความสมบูรณ์ในการใช้งาน	อุปกรณ์ทำงานผิดพลาดและเกิดความชำรุดเสียหาย	5	5	25	วางแผนการบำรุงรักษาอุปกรณ์ตามระยะเวลาที่กำหนด

ตารางที่ 4.77 การประเมินความเสี่ยงสำหรับงานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 8.3.3)

ชื่อทรัพย์สิน : งานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้					
A.8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการทบทวนการถอดถอนสิทธิในการเข้าถึงระบบสำหรับผู้ที่สิ้นสุดการจ้างงานแล้ว	การเข้าใช้งานระบบโดยไม่ได้รับอนุญาต	3	7	21	มีการทบทวนการถอดถอนสิทธิของผู้ที่สิ้นสุดการจ้างงานแล้วอย่างสม่ำเสมอ

ตารางที่ 4.78 การประเมินความเสี่ยงสำหรับงานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 11.2.1)

ชื่อทรัพย์สิน : งานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้					
A.11.2.1 การลงทะเบียนพนักงาน (User registration)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเพื่อกำหนดสิทธิให้กับผู้ใช้ระบบรายใหม่		1	5	5	

ตารางที่ 4.79 การประเมินความเสี่ยงสำหรับงานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 11.2.2)

ชื่อทรัพย์สิน : งานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้					
A.11.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) จัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน		1	5	5	

ตารางที่ 4.80 การประเมินความเสี่ยงสำหรับงานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 11.2.4)

ชื่อทรัพย์สิน : งานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้					
A.11.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดความสม่ำเสมอในการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเหมาะสม	การเข้าถึงระบบข้อมูลโดยไม่ได้รับอนุญาต	3	7	21	มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างสม่ำเสมอ

ตารางที่ 4.81 การประเมินความเสี่ยงสำหรับงานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 11.5.1)

ชื่อทรัพย์สิน : งานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้					
A.11.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีขั้นตอนปฏิบัติที่มีความปลอดภัยสำหรับการเข้าใช้งานระบบ		1	5	5	

ตารางที่ 4.82 การประเมินความเสี่ยงสำหรับงานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้ (มาตรการที่ 11.5.2)

ชื่อทรัพย์สิน : งานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้					
A.11.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีกระบวนการพิสูจน์ตัวตนของผู้ใช้งานก่อนเข้าใช้งานระบบบ		1	5	5	

ตารางที่ 4.83 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์ (มาตรการที่ 9.2.1)

ชื่อทรัพย์สิน : งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์					
A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) มีการจัดวางอุปกรณ์อยู่ในบริเวณที่มีคลื่นแม่เหล็กไฟฟ้ารบกวน	อุปกรณ์ทำงานผิดพลาด	7	5	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้ารบกวน

ตารางที่ 4.84 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์ (มาตรการที่ 9.2.4)

ชื่อทรัพย์สิน : งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์					
A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอเพื่อให้อยู่ในสภาพพร้อมใช้งาน	ขาดสภาพความพร้อมใช้ในการทำงาน	9	7	63	วางแผนการบำรุงรักษาอุปกรณ์ให้ทำงานได้อย่างต่อเนื่องและสม่ำเสมอ

ตารางที่ 4.85 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์ (มาตรการที่ 9.2.7)

ชื่อทรัพย์สิน : งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์					
A.9.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) ไม่อนุญาตให้นำทรัพย์สินขององค์กรออกนอกองค์กรนอกจากได้รับอนุญาตแล้วเท่านั้น		1	7	7	

ตารางที่ 4.86 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์ (มาตรการที่ 10.3.1)

ชื่อทรัพย์สิน : งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์					
A.10.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต	อุปกรณ์ที่มีสภาพความพร้อมใช้ในการทำงานมีจำนวนไม่พอเพียง	9	7	63	มีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต

ตารางที่ 4.87 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์ (มาตรการที่ 10.3.2)

ชื่อทรัพย์สิน : งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์					
A.10.3.2 การตรวจรับระบบ (System acceptance)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน		1	7	7	

ตารางที่ 4.88 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์ (มาตรการที่ 14.1.2)

ชื่อทรัพย์สิน : งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์					
A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการประเมินเหตุการณ์ที่จะทำให้การทำงานของอุปกรณ์ต่าง ๆ ติดขัดหรือหยุดชะงัก	ขาดความต่อเนื่องในการดำเนินงาน	9	7	63	มีการประเมินเหตุการณ์ต่างๆ ที่จะทำให้การทำงานหยุดชะงักและกำหนดแนวทางป้องกัน

ตารางที่ 4.89 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์ (มาตรการที่ 10.4.1)

ชื่อทรัพย์สิน : งานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์					
A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการตรวจจับและป้องกันโปรแกรมที่ไม่ประสงค์ดี		3	5	15	

ตารางที่ 4.90 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์ (มาตรการที่ 10.5.1)

ชื่อทรัพย์สิน : งานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์					
A.10.5.1 การสำรองข้อมูล (Information back-up)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการสำรองข้อมูลที่สำคัญอย่างสม่ำเสมอ	ข้อมูลที่ใช้งานขาดความครบถ้วน	3	7	21	วางแผนการสำรองข้อมูลที่สำคัญอย่างสม่ำเสมอ

ตารางที่ 4.91 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์ (มาตรการที่ 11.5.4)

ชื่อทรัพย์สิน : งานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์					
A.11.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการดูแลควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้	ระบบทำงานผิดพลาด	7	3	21	มีการกำหนดแนวทางในการควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้

ตารางที่ 4.92 การประเมินความเสี่ยงสำหรับงานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์ (มาตรการที่ 14.1.2)

ชื่อทรัพย์สิน : งานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์					
A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการประเมินเหตุการณ์ที่จะทำให้การทำงานของโปรแกรมต่าง ๆ ติดขัดหรือหยุดชะงัก	ขาดความต่อเนื่องในการดำเนินงานและระบบทำงานผิดพลาด	9	7	63	มีแนวทางการป้องกันเหตุการณ์ต่างๆ ที่จะทำให้การทำงานหยุดชะงัก

ตารางที่ 4.93 การประเมินความเสี่ยงสำหรับงานบริการระบบ Web Server (มาตรการที่ 8.2.2)

ชื่อทรัพย์สิน : งานบริการระบบ Web Server					
A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ผู้ใช้งานขาดความรู้และความตระหนักในด้านความปลอดภัยในการเข้าใช้งานระบบ	เกิดความเสียหายต่อระบบงาน	7	5	35	สร้างความตระหนักในความปลอดภัยให้แก่ผู้ใช้งานระบบ

ตารางที่ 4.94 การประเมินความเสี่ยงสำหรับงานบริการระบบ Web Server (มาตรการที่ 13.1.2)

ชื่อทรัพย์สิน : งานบริการระบบ Web Server					
A.13.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบงานอย่างสม่ำเสมอ	เกิดความเสียหายต่อระบบงาน	7	5	35	มีการบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบงานอย่างสม่ำเสมอ

ตารางที่ 4.95 การประเมินความเสี่ยงสำหรับงานบริการระบบ Web Server (มาตรการที่ 14.1.2)

ชื่อทรัพย์สิน : งานบริการระบบ Web Server					
A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการประเมินเหตุการณ์ที่จะทำให้การทำงานของระบบติดขัดหรือหยุดชะงัก	ขาดความต่อเนื่องในการทำงานและให้บริการของระบบงาน	7	7	49	ประเมินปัญหาของเหตุการณ์ต่างๆและกำหนดแนวทางป้องกัน

ตารางที่ 4.96 การประเมินความเสี่ยงสำหรับงานบริการระบบห้องสมุดอัตโนมัติ (มาตรการที่ 8.2.2)

ชื่อทรัพย์สิน : งานบริการระบบห้องสมุดอัตโนมัติ					
A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ผู้ใช้งานขาดความรู้และความตระหนักในด้านความปลอดภัยในการเข้าใช้งานระบบ	เกิดความเสียหายต่อระบบงาน	7	5	35	สร้างความตระหนักในความปลอดภัยให้แก่ผู้ใช้งานระบบ

ตารางที่ 4.97 การประเมินความเสี่ยงสำหรับงานบริการระบบห้องสมุดอัตโนมัติ (มาตรการที่ 13.1.2)

ชื่อทรัพย์สิน : งานบริการระบบห้องสมุดอัตโนมัติ					
A.13.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการบันทึกรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบอย่างสม่ำเสมอ	เกิดความเสียหายต่อระบบงาน	7	5	35	มีการบันทึกรายงานจุดอ่อนของระบบงานอย่างสม่ำเสมอ

ตารางที่ 4.98 การประเมินความเสี่ยงสำหรับงานบริการระบบห้องสมุดอัตโนมัติ (มาตรการที่ 14.1.2)

ชื่อทรัพย์สิน : งานบริการระบบห้องสมุดอัตโนมัติ					
A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการประเมินเหตุการณ์ที่จะทำให้การทำงานของระบบติดขัดหรือหยุดชะงัก	ขาดความต่อเนื่องในการทำงานและให้บริการของระบบงาน	7	7	49	ประเมินปัญหาของเหตุการณ์ต่างๆและกำหนดแนวทางป้องกัน

ตารางที่ 4.99 การประเมินความเสี่ยงสำหรับงานบริการระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 8.2.2)

ชื่อทรัพย์สิน : งานบริการระบบฐานข้อมูลสหบรรณานุกรม					
A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ผู้ใช้งานขาดความรู้และความตระหนักในด้านความปลอดภัยในการเข้าใช้งานระบบ	เกิดความเสียหายต่อระบบงาน	7	5	35	สร้างความตระหนักในความปลอดภัยให้แก่ผู้ใช้งานระบบ

ตารางที่ 4.100 การประเมินความเสี่ยงสำหรับงานบริการระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 13.1.2)

ชื่อทรัพย์สิน : งานบริการระบบฐานข้อมูลสหบรรณานุกรม					
A.13.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ไม่มีบันทึกรายงานจุดอ่อนด้านความปลอดภัยของระบบงานอย่างสม่ำเสมอ	เกิดความเสียหายต่อระบบงาน	7	5	35	บันทึกและทำรายงานจุดอ่อนด้านความมั่นคงปลอดภัยของระบบงานอย่างสม่ำเสมอ

ตารางที่ 4.101 การประเมินความเสี่ยงสำหรับงานบริการระบบฐานข้อมูลสหบรรณานุกรม (มาตรการที่ 14.1.2)

ชื่อทรัพย์สิน : งานบริการระบบฐานข้อมูลสหบรรณานุกรม					
A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน(W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) ขาดการประเมินเหตุการณ์ที่ทำให้การทำงานของระบบหยุดชะงัก	ขาดความต่อเนื่องในการให้บริการของระบบงาน	7	7	49	ประเมินปัญหาของเหตุการณ์และกำหนดแนวทางป้องกัน

4.1.3 การจัดระดับความเสี่ยงและวางแผนกำหนดนโยบายป้องกัน ในการจัดระดับค่าของความเสี่ยงที่มีต่อทรัพย์สินสารสนเทศ จะมีการจัดแบ่งตามลำดับของค่าความเสี่ยงโดยรวม โดยเรียงลำดับจากค่าความเสี่ยงสูงสุดไปหาลำดับน้อยสุด พร้อมการวางแผนเพื่อจะกำหนดนโยบายการป้องกันในแต่ละทรัพย์สิน ซึ่งจะทำการแยกตามประเภทของทรัพย์สินสารสนเทศ สามารถสรุปได้ดังตารางที่ 4.102 – 4.122

ค่าความเสี่ยงรวมที่ได้จะมีการแบ่งกลุ่มออกเป็น 3 กลุ่มดังนี้

1. ค่าความเสี่ยงที่ต้องการแก้ไขอย่างเร่งด่วนมีค่าระหว่าง 45 – 63
2. ค่าความเสี่ยงที่มีค่าปานกลางควรดำเนินการแก้ไขมีค่าระหว่าง 21 – 35
3. ค่าความเสี่ยงที่สามารถยอมรับได้มีค่าระหว่าง 1 - 15

ตารางที่ 4.102 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (อุปกรณ์คอมพิวเตอร์ - เครื่องแม่ข่ายระบบ Web Server)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
เครื่องแม่ข่ายระบบ Web Server	4	1. A.10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	63	จัดทำคู่มือการปฏิบัติงานสำหรับเครื่อง server
		2. A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)	35	- ติดตั้งโปรแกรมป้องกันไวรัส - ให้ความรู้แก่เจ้าหน้าที่ด้านความปลอดภัยของข้อมูล

ตารางที่ 4.102 (ต่อ) การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (อุปกรณ์คอมพิวเตอร์ - เครื่องแม่ข่ายระบบ Web Server)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
เครื่องแม่ข่ายระบบ Web Server	4	3. A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้ารบกวน
		4. A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	35	กำหนดตารางการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ

ตารางที่ 4.103 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (อุปกรณ์คอมพิวเตอร์ - เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ	4	1. A.10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	63	จัดทำคู่มือการปฏิบัติงานสำหรับเครื่อง server

ตารางที่ 4.103 (ต่อ) การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ
(อุปกรณ์คอมพิวเตอร์ - เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ	4	2. A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)	35	- ติดตั้งโปรแกรมป้องกันไวรัส - ให้ความรู้แก่เจ้าหน้าที่ด้านความปลอดภัยของข้อมูล
		3. A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้ารบกวน
		4. A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	35	กำหนดตารางการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ

ตารางที่ 4.104 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ
(อุปกรณ์คอมพิวเตอร์ - เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
เครื่องคอมพิวเตอร์ จำนวน 100 เครื่อง	5	1. A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้ารบกวน
		2. A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	35	กำหนดตารางการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ
		3. A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)	35	- ติดตั้งโปรแกรมเพื่อใช้ตรวจจับและป้องกันจากโปรแกรมไม่ประสงค์ดีอย่างทั่วถึง
		4. A.10.5.1 การสำรองข้อมูล (Back-up)	35	วางแผนการสำรองข้อมูลอย่างสม่ำเสมอ
		5. A.9.2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal of re-use of equipment)	25	มีการตรวจสอบการลบทิ้งของข้อมูลภายในเครื่องคอมพิวเตอร์ที่ไม่ได้ใช้งานแล้ว

ตารางที่ 4.105 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (อุปกรณ์คอมพิวเตอร์ - สื่อบันทึกข้อมูลแผ่นซีดี)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
สื่อบันทึกข้อมูลแผ่นซีดี	1	A.10.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)	35	มีการกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลไว้อย่างชัดเจน

ตารางที่ 4.106 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (อุปกรณ์คอมพิวเตอร์ - เทปแบ็คอัพ)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
เทปแบ็คอัพ	1	A.10.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)	35	มีการกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลไว้อย่างชัดเจน

ตารางที่ 4.107 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (โปรแกรม - ระบบฐานข้อมูล SQL Server)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
ระบบฐานข้อมูล SQL Server	1	A.12.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)	25	จัดทำขั้นตอนปฏิบัติในการแก้ไขระบบที่มีความครอบคลุมในทุกขั้นตอน

ตารางที่ 4.108 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (โปรแกรม - ระบบปฏิบัติการ Microsoft Windows)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
ระบบปฏิบัติการ Microsoft Windows	3	1. A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)	49	มีการสร้างความตระหนักในผู้ใช้ในการป้องกันภัยจากโปรแกรมที่ไม่ประสงค์ดี
		2. A.12.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)	21	กำหนดให้มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งโปรแกรมต่าง ๆ ลงไปยังระบบปฏิบัติการที่ให้บริการ

ตารางที่ 4.108 (ต่อ) การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ
(โปรแกรม - ระบบปฏิบัติการ Microsoft Windows)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
ระบบปฏิบัติการ Microsoft Windows		3. A.12.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)	25	จัดทำขั้นตอนปฏิบัติในการแก้ไขระบบที่มีความครอบคลุมในทุกขั้นตอน

ตารางที่ 4.109 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ
(โปรแกรม – ระบบปฏิบัติการ Linux)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
ระบบปฏิบัติการ Linux	1	A.12.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change control procedures)	25	จัดทำขั้นตอนปฏิบัติในการแก้ไขระบบที่มีความครอบคลุมในทุกขั้นตอน

ตารางที่ 4.110 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (โปรแกรม – โปรแกรมต่าง ๆ)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
โปรแกรมต่าง ๆ	1	A.12.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)	35	มีการติดตามข้อมูลข่าวสารที่เกี่ยวกับช่องโหว่ของโปรแกรมและปรับปรุงให้ทันสมัยอยู่เสมอ

ตารางที่ 4.111 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (บุคลากร)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
บุคลากร	2	1. A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)	21	จัดให้มีการอบรมด้านการรักษาความมั่นคงปลอดภัยขององค์กรอย่างสม่ำเสมอ

ตารางที่ 4.111 (ต่อ) การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (บุคลากร)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
บุคลากร		2. A.8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)	21	มีการทบทวนสิทธิในการเข้าถึงสารสนเทศของพนักงานอย่างสม่ำเสมอ

ตารางที่ 4.112 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (ข้อมูล - ระบบ Web Server)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
ระบบ Web Server	1	A. 8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)	21	มีการทบทวนการถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงานอย่างสม่ำเสมอ

ตารางที่ 4.113 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (ข้อมูล - ระบบห้องสมุดอัตโนมัติ)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
ระบบห้องสมุดอัตโนมัติ	1	A. 8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)	21	มีการทบทวนการถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงานอย่างสม่ำเสมอ

ตารางที่ 4.114 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (ข้อมูล - ระบบฐานข้อมูลสหบรรณานุกรม)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
ระบบฐานข้อมูลสหบรรณานุกรม	1	A. 8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)	21	มีการทบทวนการถอดถอนสิทธิในการเข้าถึงระบบข้อมูลของผู้ที่สิ้นสุดการจ้างงานอย่างสม่ำเสมอ

ตารางที่ 4.115 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ - งานบริการ Internet)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
งานบริการ Internet	2	1. A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)	35	มีการอบรมเพื่อสร้างความตระหนักด้านความปลอดภัยในการใช้งาน
		2. A.10.6.1 มาตรการทางเครือข่าย (Network controls)	35	มีการดูแลรักษาความปลอดภัยให้กับระบบอย่างสม่ำเสมอ

ตารางที่ 4.116 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – ระบบปรับอากาศ ห้อง Server)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
ระบบปรับอากาศ ห้อง Server	1	A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	25	วางแผนการบำรุงรักษาอุปกรณ์ตามระยะเวลาที่กำหนด

ตารางที่ 4.117 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
งานบริหารจัดการกำหนดสิทธิการเข้าใช้งานในระบบต่าง ๆ ของผู้ใช้	2	1. A.8.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)	21	มีการทบทวนการถอดถอนสิทธิของผู้ที่สิ้นสุดการจ้างงานแล้วอย่างสม่ำเสมอ
		2. A.11.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)	21	มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างสม่ำเสมอ

ตารางที่ 4.118 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์	4	1. A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	63	วางแผนการบำรุงรักษาอุปกรณ์ให้ทำงานได้อย่างต่อเนื่องและสม่ำเสมอ

ตารางที่ 4.118 (ต่อ) การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์		2. A.10.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)	63	มีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต
		3. A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)	63	มีการประเมินเหตุการณ์ต่างๆที่จะทำให้การทำงานหยุดชะงักและกำหนดแนวทางป้องกัน
		4. A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้ารบกวน

ตารางที่ 4.119 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
งานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์	3	1. A. 14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)	63	มีแนวทางการป้องกันเหตุการณ์ต่างๆที่จะทำให้การทำงานหยุดชะงัก
		2. A.10.5.1 การสำรองข้อมูล (Information back-up)	21	วางแผนการสำรองข้อมูลที่สำคัญอย่างสม่ำเสมอ
		3. A.11.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)	21	มีการกำหนดแนวทางในการควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้

ตารางที่ 4.120 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานบริการระบบ Web Server)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
งานบริการระบบ Web Server	3	1. A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)	49	มีการประเมินเหตุการณ์ต่างๆที่จะทำให้การทำงานหยุดชะงักและกำหนดแนวทางป้องกัน
		2. A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)	35	สร้างความตระหนักในความปลอดภัยให้แก่ผู้ใช้งานระบบ
		3. A.13.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)	35	มีการบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบงานอย่างสม่ำเสมอ

ตารางที่ 4.121 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานบริการระบบห้องสมุดอัตโนมัติ)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
งานบริการระบบห้องสมุดอัตโนมัติ	3	1. A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)	49	มีการประเมินเหตุการณ์ต่างๆที่จะทำให้การทำงานหยุดชะงักและกำหนดแนวทางป้องกัน
		2. A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)	35	สร้างความตระหนักในความปลอดภัยให้แก่ผู้ใช้งานระบบ
		3. A.13.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)	35	มีการบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบงานอย่างสม่ำเสมอ

ตารางที่ 4.122 การจัดระดับความเสี่ยงแยกตามประเภทของทรัพย์สินสารสนเทศ (งานบริการ – งานบริการระบบฐานข้อมูลสหบรรณานุกรม)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
งานบริการระบบฐานข้อมูลสหบรรณานุ-กรม	3	1. A.14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)	49	มีการประเมินเหตุการณ์ต่างๆที่จะทำให้การทำงานหยุดชะงักและกำหนดแนวทางป้องกัน
		2. A.8.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education , and training)	35	สร้างความตระหนักในความปลอดภัยให้แก่ผู้ใช้งานระบบ
		3. A.13.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)	35	มีการบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบงานอย่างสม่ำเสมอ

4.2 การวิเคราะห์ระบบ

ในการศึกษาด้านการจัดการความเสี่ยง ที่เกิดขึ้นกับทรัพย์สินสารสนเทศ จะทำการแบ่งทรัพย์สินออกเป็นประเภทต่างๆ เพื่อจะค้นหาช่องโหว่ที่เป็นจุดอ่อนและปัญหาที่เกิดขึ้นจากจุดอ่อนเหล่านั้น ที่มีผลทำให้เกิดความเสี่ยงขึ้นในการใช้งานของผู้ใช้ที่มีต่อทรัพย์สินภายในองค์กร ข้อมูลที่มีการนำมาวิเคราะห์ จะช่วยทำให้องค์กรได้ทราบถึง ระดับของความเสี่ยงโดยรวมที่เกิดขึ้นในแต่ละทรัพย์สิน รวมไปถึงการกำหนดแนวทางในการจัดทำมาตรการป้องกันให้กับทรัพย์สิน เพื่อเป็นการช่วยลดระดับของความเสี่ยงที่มีต่อทรัพย์สินเหล่านั้นให้อยู่ในระดับที่องค์กรสามารถยอมรับได้

ระบบต้นแบบที่ใช้ในการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศ ซึ่งได้จัดทำขึ้นจะเก็บรวบรวมข้อมูลทั้งหมด ที่เกี่ยวข้องกับกระบวนการในการจัดการความเสี่ยงมากำหนดรูปแบบที่เหมาะสม เพื่อเผยแพร่ข้อมูลระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศให้มีขึ้นใช้ภายในองค์กร ระบบที่จัดทำขึ้นจะอยู่ในรูปแบบของหน้าเว็บเพจ บุคลากรภายในสามารถเข้ามาศึกษาถึงแนวทางในการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กร และสามารถสืบค้นรายการทรัพย์สินโดยแยกตามประเภทของทรัพย์สินที่ต้องการศึกษาได้

ภาพที่ 4.2 แสดง Use Cases diagram การค้นหาข้อมูลทรัพย์สินสารสนเทศ โดยบุคลากรภายใน สามารถสืบค้นข้อมูลด้านการจัดการความเสี่ยง ผ่านทางระบบเครือข่ายภายในองค์กรได้อย่างทั่วถึง ผ่านทางเครื่องคอมพิวเตอร์ที่ใช้งานภายใน ที่มีการเชื่อมต่อระบบเครือข่ายทั้งแบบมีสายและไร้สาย ข้อมูลเหล่านี้จะช่วยทำให้ผู้ใช้เกิดความเข้าใจและความตระหนัก ในการรักษาความปลอดภัยให้กับทรัพย์สินสารสนเทศในองค์กรมากยิ่งขึ้น

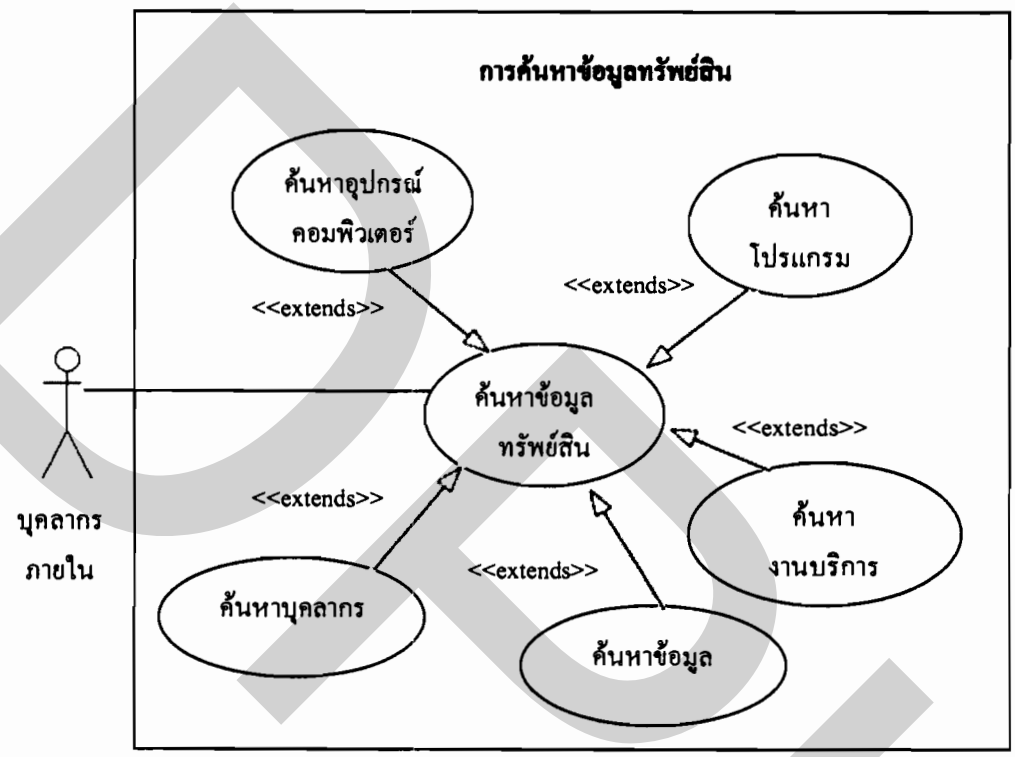
การประมวลผลข้อมูลของระบบจะเป็นลักษณะแบบ Web based ที่มีการติดต่อส่งข้อมูลถึงกันระหว่างเครื่องคอมพิวเตอร์แต่ละเครื่องผ่านทางหน้าเว็บเพจ ซึ่งเป็นเครื่องมือหลักในการรับส่งข้อมูล โดยส่งข้อมูลผ่านทางโปรแกรมเว็บบราวเซอร์เช่น Internet Explorer การประมวลผลบนหน้าเว็บเพจ จะเกี่ยวข้องกับการส่งถ่ายข้อมูลระหว่างเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น Web Server กับเครื่องคอมพิวเตอร์ที่เป็นฝ่ายเรียกใช้ข้อมูล (Client) ซึ่งประกอบด้วยขั้นตอนต่าง ๆ ดังนี้

1. ผู้ใช้จะส่งคำร้องขอไปยังเครื่องแม่ข่ายผ่านทางหน้าเว็บบราวเซอร์ โดยใช้โปรโตคอลแบบ HTTP

2. เครื่องแม่ข่าย Web Server รับคำร้องขอ แล้วค้นหาตำแหน่งของเว็บเพจที่ร้องขอ

3. เครื่องแม่ข่าย Web Server ทำการประมวลผลโค้ดภาษา และแปลงผลลัพธ์เป็นเอกสารในรูปภาษาพีเอชพี

4. เครื่องแม่ข่าย Web Server จะทำหน้าที่ส่งข้อมูลกลับไปยังเว็บบราวเซอร์ของเครื่องผู้เรียกใช้ข้อมูล (Client) ให้อยู่ในรูปแบบที่ใช้แสดงผลให้กับผู้ใช้สามารถอ่านได้



ภาพที่ 4.2 Use Cases diagram การค้นหาข้อมูลทรัพย์สินสารสนเทศ

4.3 การออกแบบระบบ

ในการออกแบบระบบจะกล่าวถึง 2 ส่วนคือ การออกแบบตารางจัดเก็บข้อมูล และการออกแบบหน้าเว็บเพจ โดยมีรายละเอียดดังนี้

4.3.1 การออกแบบตารางจัดเก็บข้อมูล สำหรับการจัดเก็บรายชื่อของทรัพย์สินสารสนเทศ เพื่อใช้สำหรับการสืบค้นข้อมูล จะมีการจัดเก็บแยกตามกลุ่มของทรัพย์สิน แบ่งออกเป็น 5 ประเภทคือ อุปกรณ์คอมพิวเตอร์ โปรแกรม บุคลากร ข้อมูล และงานบริการ ประกอบไปด้วย 5 ตารางดังนี้

1. ตารางรายละเอียดอุปกรณ์คอมพิวเตอร์ (ตารางที่ 4.123) จะจัดเก็บรายชื่อของทรัพย์สินต่าง ๆ ที่อยู่ภายใต้ประเภทของอุปกรณ์คอมพิวเตอร์ รวมไปถึงชื่อที่อยู่ของทรัพย์สิน เพื่อใช้สำหรับการเชื่อมโยงไปยังตารางแสดงค่าการประเมินความเสี่ยงสำหรับทรัพย์สินนั้น ๆ

ตารางที่ 4.123 แสดงรายชื่อทรัพย์สินทางด้านอุปกรณ์คอมพิวเตอร์

Hardware				
ลำดับ	ฟิลด์	ชนิด	ความกว้าง	หมายเหตุ
1	hw_id	varchar(4)	4	ลำดับที่ของทรัพย์สิน
2	hw_name	varchar(100)	100	ชื่อทรัพย์สิน
3	hw_url	varchar(100)	100	ชื่อที่อยู่ของทรัพย์สิน
4	hw_keyword	varchar(100)	100	คำที่ใช้ในการสืบค้นทรัพย์สิน

2. ตารางรายละเอียดโปรแกรม (ตารางที่ 4.124) จะจัดเก็บรายชื่อของทรัพย์สินต่าง ๆ ที่อยู่ภายใต้ประเภทของโปรแกรม และรวมไปถึงชื่อที่อยู่ของทรัพย์สิน เพื่อใช้สำหรับการเชื่อมโยงไปยังตารางแสดงค่าการประเมินความเสี่ยงสำหรับทรัพย์สินนั้น ๆ

ตารางที่ 4.124 แสดงรายชื่อทรัพย์สินทางด้านโปรแกรม

Software				
ลำดับ	ฟิลด์	ชนิด	ความกว้าง	หมายเหตุ
1	sw_id	varchar(4)	4	ลำดับที่ของทรัพย์สิน
2	sw_name	varchar(100)	100	ชื่อทรัพย์สิน
3	sw_url	varchar(100)	100	ชื่อที่อยู่ของทรัพย์สิน
4	sw_keyword	varchar(100)	100	คำที่ใช้ในการสืบค้นทรัพย์สิน

3. ตารางรายละเอียดบุคลากร (ตารางที่ 4.125) จะจัดเก็บรายชื่อของทรัพย์สินต่าง ๆ ที่อยู่ภายใต้ประเภทของบุคลากร รวมไปถึงชื่อที่อยู่ของทรัพย์สิน เพื่อใช้สำหรับการเชื่อมโยงไปยังตารางแสดงค่าการประเมินความเสี่ยงสำหรับทรัพย์สินนั้น ๆ

ตารางที่ 4.125 แสดงรายชื่อทรัพย์สินทางด้านบุคลากร

People				
ลำดับ	ฟิลด์	ชนิด	ความกว้าง	หมายเหตุ
1	p_id	varchar(4)	4	ลำดับที่ของทรัพย์สิน
2	p_name	varchar(100)	100	ชื่อทรัพย์สิน
3	p_url	varchar(100)	100	ชื่อที่อยู่ของทรัพย์สิน
4	p_keyword	varchar(100)	100	คำที่ใช้ในการสืบค้นทรัพย์สิน

4. ตารางรายละเอียดข้อมูล (ตารางที่ 4.126) จะจัดเก็บรายชื่อของทรัพย์สินต่าง ๆ ซึ่งอยู่ภายใต้ประเภทของข้อมูลและรวมไปถึงชื่อที่อยู่ของทรัพย์สินเพื่อใช้สำหรับการเชื่อมโยงไปยังตารางแสดงค่าการประเมินความเสี่ยงสำหรับทรัพย์สินนั้น ๆ

ตารางที่ 4.126 แสดงรายชื่อทรัพย์สินทางด้านข้อมูล

Information				
ลำดับ	ฟิลด์	ชนิด	ความกว้าง	หมายเหตุ
1	info_id	varchar(4)	4	ลำดับที่ของทรัพย์สิน
2	info_name	varchar(100)	100	ชื่อทรัพย์สิน
3	info_url	varchar(100)	100	ชื่อที่อยู่ของทรัพย์สิน
4	info_keyword	varchar(100)	100	คำที่ใช้ในการสืบค้นทรัพย์สิน

5. ตารางรายละเอียดงานบริการ (ตารางที่ 4.127) จะจัดเก็บรายชื่อของทรัพย์สินต่าง ๆ ที่อยู่ภายใต้ประเภทของงานบริการ รวมไปถึงชื่อที่อยู่ของทรัพย์สิน เพื่อใช้สำหรับการเชื่อมโยงไปยังตารางแสดงค่าการประเมินความเสี่ยงสำหรับทรัพย์สินนั้น ๆ

ตารางที่ 4.127 แสดงรายชื่อทรัพย์สินทางด้านงานบริการ

Service				
ลำดับ	ฟิลด์	ชนิด	ความกว้าง	หมายเหตุ
1	sv_id	varchar(4)	4	ลำดับที่ของทรัพย์สิน
2	sv_name	varchar(100)	100	ชื่อทรัพย์สิน
3	sv_url	varchar(100)	100	ชื่อที่อยู่ของทรัพย์สิน
4	sv_keyword	varchar(100)	100	คำที่ใช้ในการสืบค้นทรัพย์สิน

4.3.2 การออกแบบหน้าเว็บเพจ สำหรับหน้าเว็บเพจที่จัดทำระบบต้นแบบในการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศ มีการแบ่งข้อมูลออกเป็น 4 ส่วนดังนี้

1. ส่วนที่แสดงรายละเอียดถึงแนวทางการจัดการความเสี่ยง สำหรับทรัพย์สินสารสนเทศภายในองค์กร โดยจะกล่าวถึงความสำคัญและแนวคิดในการจัดการความเสี่ยง เพื่อให้ผู้ใช้ได้ศึกษาถึงกระบวนการในการจัดการความเสี่ยงและองค์ประกอบต่าง ๆ ที่มีส่วนเกี่ยวข้อง (ภาพที่ 5.1 – 5.9)

2. ส่วนที่เป็นการแบ่งประเภทของทรัพย์สิน ซึ่งแยกตามกลุ่มต่าง ๆ คือ กลุ่มของอุปกรณ์คอมพิวเตอร์ โปรแกรม บุคลากร ข้อมูล และงานบริการ ในส่วนนี้จะมีการแสดงรายละเอียดถึงการประเมินความเสี่ยงที่เกิดขึ้นกับทรัพย์สินในแต่ละประเภท (ภาพที่ 5.10 – 5.11)

3. ส่วนที่ใช้สำหรับในการสืบค้น เพื่อหาทรัพย์สินสารสนเทศ โดยให้ผู้ใช้สามารถสืบค้นรายชื่อของทรัพย์สิน ที่ต้องการทราบถึงรายละเอียดในการประเมินความเสี่ยงของทรัพย์สินนั้น รวมไปถึงรายละเอียดอื่น ๆ ที่เกี่ยวข้อง (ภาพที่ 5.12 – 5.15)

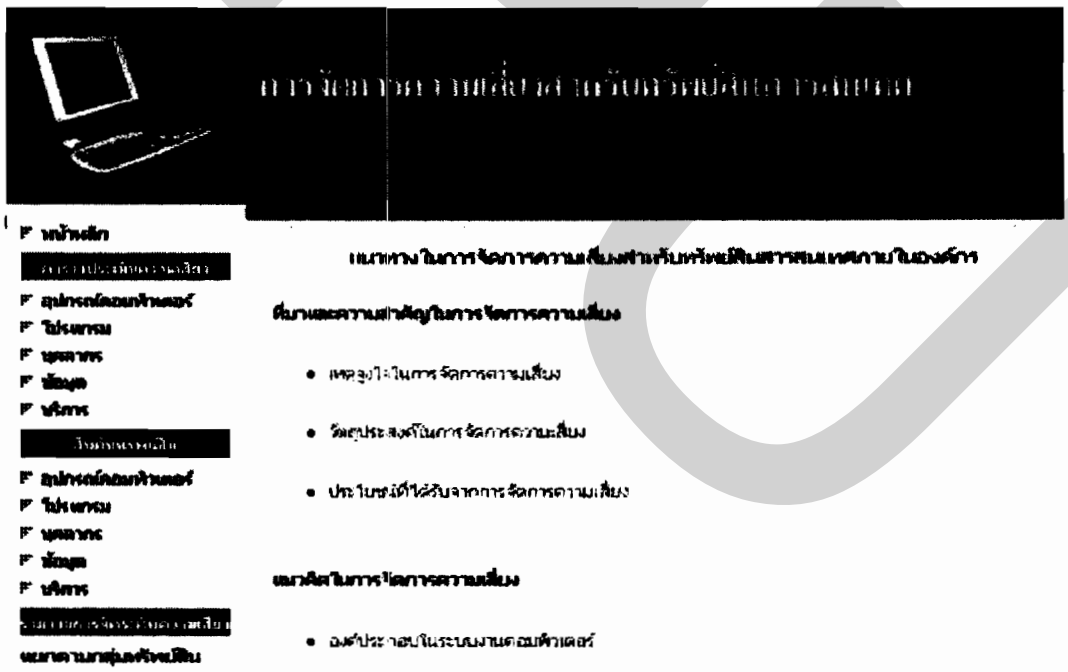
4. ส่วนสรุปรายงาน ที่แสดงถึงรายละเอียดในการจัดระดับของความเสี่ยงโดยรวม ที่มีต่อทรัพย์สินในแต่ละประเภท และแนวทางในการกำหนดมาตรการป้องกัน เพื่อให้ผู้ใช้ได้ทราบถึงการจัดระดับความเสี่ยงของทรัพย์สิน ซึ่งเรียงลำดับจากค่าความเสี่ยงสูงสุดไปหาลำดับน้อยสุด โดยแยกการจัดระดับตามประเภทของทรัพย์สินสารสนเทศ (ภาพที่ 5.16 – 5.18)

บทที่ 5
ผลการจัดทำและการทดสอบระบบ

การจัดทำและทดสอบในการใช้งานเว็บเพจ สำหรับระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศ จะจัดทำและทดสอบตามการออกแบบหน้าเว็บเพจที่แบ่งเป็น 4 ส่วน ได้แก่ การใช้งานเว็บเพจหน้าข้อมูลหลัก การใช้งานเว็บเพจหน้าตารางประเมินความเสี่ยง การใช้งานเว็บเพจหน้าสืบค้นข้อมูลทรัพย์สิน การใช้งานเว็บเพจหน้ารายงานการจัดระดับความเสี่ยง

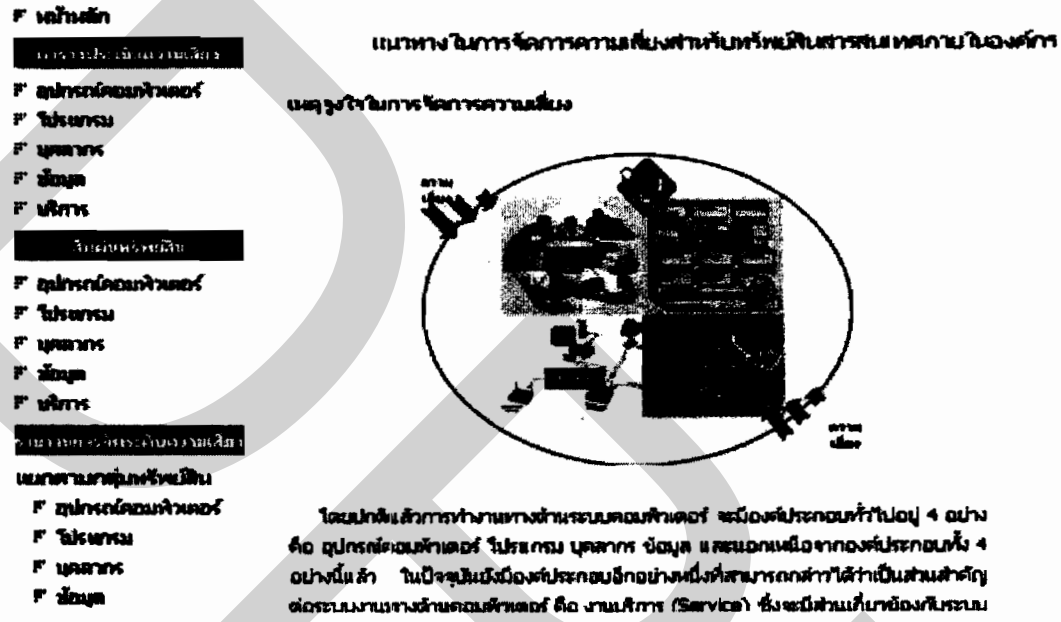
5.1 การใช้งานเว็บเพจหน้าข้อมูลหลัก

เมื่อผู้ใช้งานคลิกที่เมนูด้านซ้ายที่ชื่อ หน้าหลัก ดังภาพที่ 5.1 จะปรากฏหน้าเว็บเพจแสดงรายละเอียดที่เกี่ยวข้องกับการจัดทำประเมินความเสี่ยงซึ่งช่วยทำให้ผู้ใช้งานทราบถึง แนวทางในการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศภายในองค์กร โดยมีการแบ่งหัวข้อออกเป็น 2 ส่วนคือ ที่มาและความสำคัญในการจัดการความเสี่ยง และแนวคิดในการจัดการความเสี่ยง

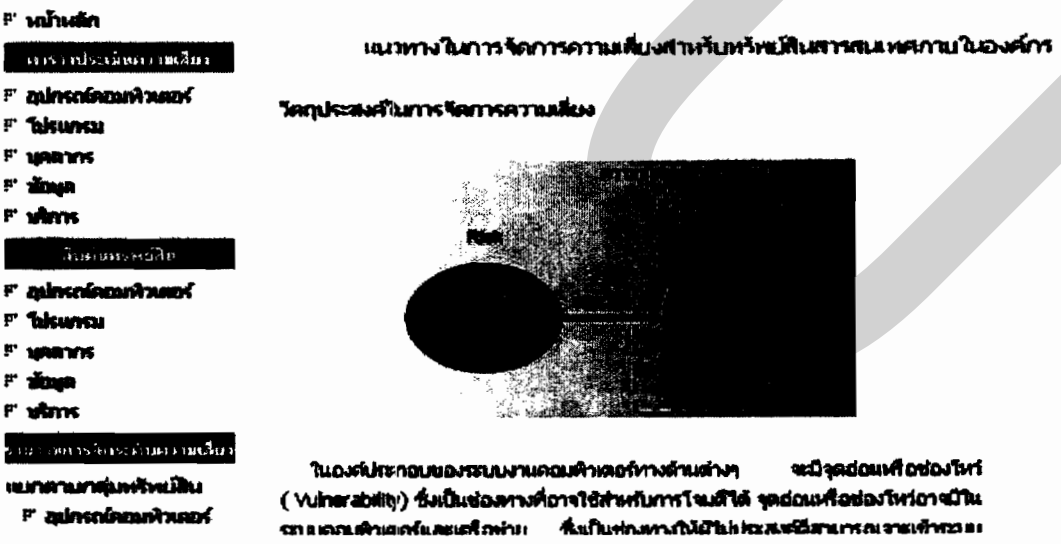


ภาพที่ 5.1 หน้าหลักแสดงรายละเอียดแนวทางการจัดทำประเมินความเสี่ยง

ส่วนแรก ในหัวข้อ ที่มาและความสำคัญในการจัดการความเสี่ยง จากภาพที่ 5.1 เมื่อผู้ใช้คลิกที่ชื่อเหตุจูงใจในการจัดการความเสี่ยง หรือวัตถุประสงค์ในการจัดการความเสี่ยง หรือประโยชน์ที่ได้รับจากการจัดการความเสี่ยง ระบบจะทำการเชื่อมโยงไปยังหน้าเว็บเพจของข้อมูลนั้นๆ เพื่อจะแสดงรายละเอียดที่เกี่ยวข้อง โดยจะปรากฏหน้าเว็บเพจ ดังภาพที่ 5.2 – 5.4



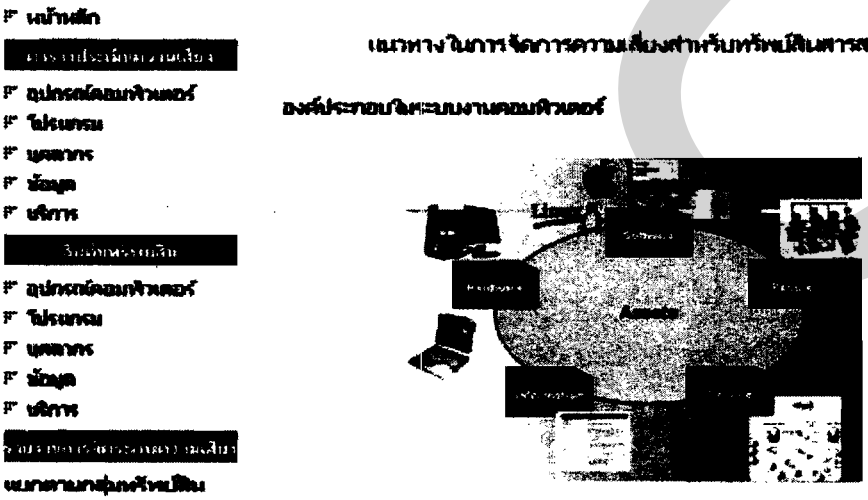
ภาพที่ 5.2 หน้าแสดงรายละเอียด เหตุจูงใจในการจัดการความเสี่ยง



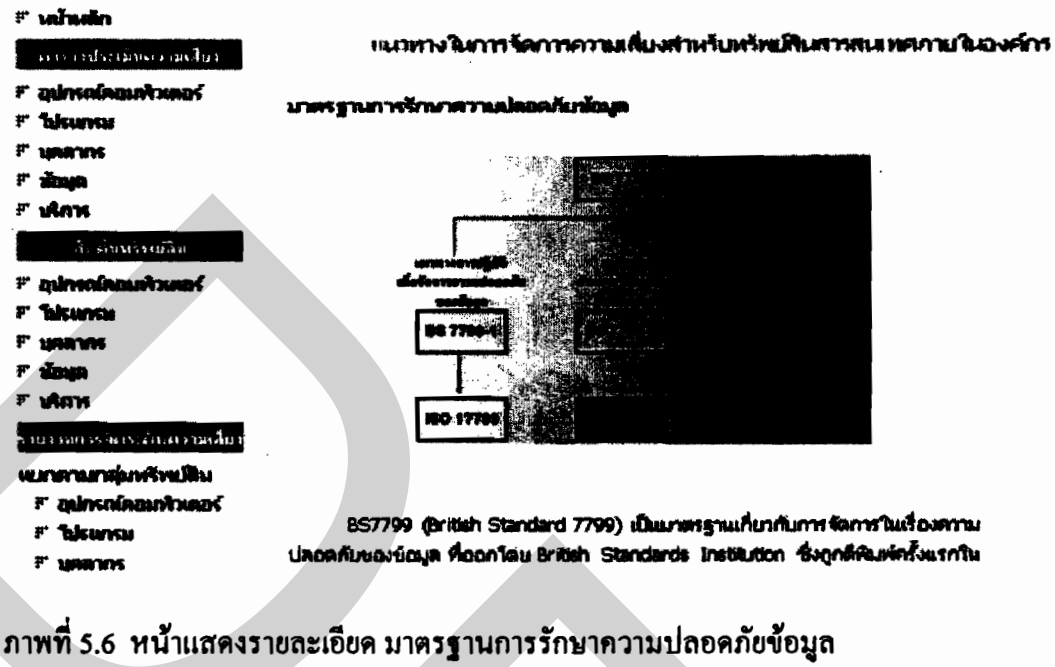
ภาพที่ 5.3 หน้าแสดงรายละเอียด วัตถุประสงค์ในการจัดการความเสี่ยง

ภาพที่ 5.4 หน้าแสดงรายละเอียด ประโยชน์ที่ได้รับจากการจัดการความเสี่ยง

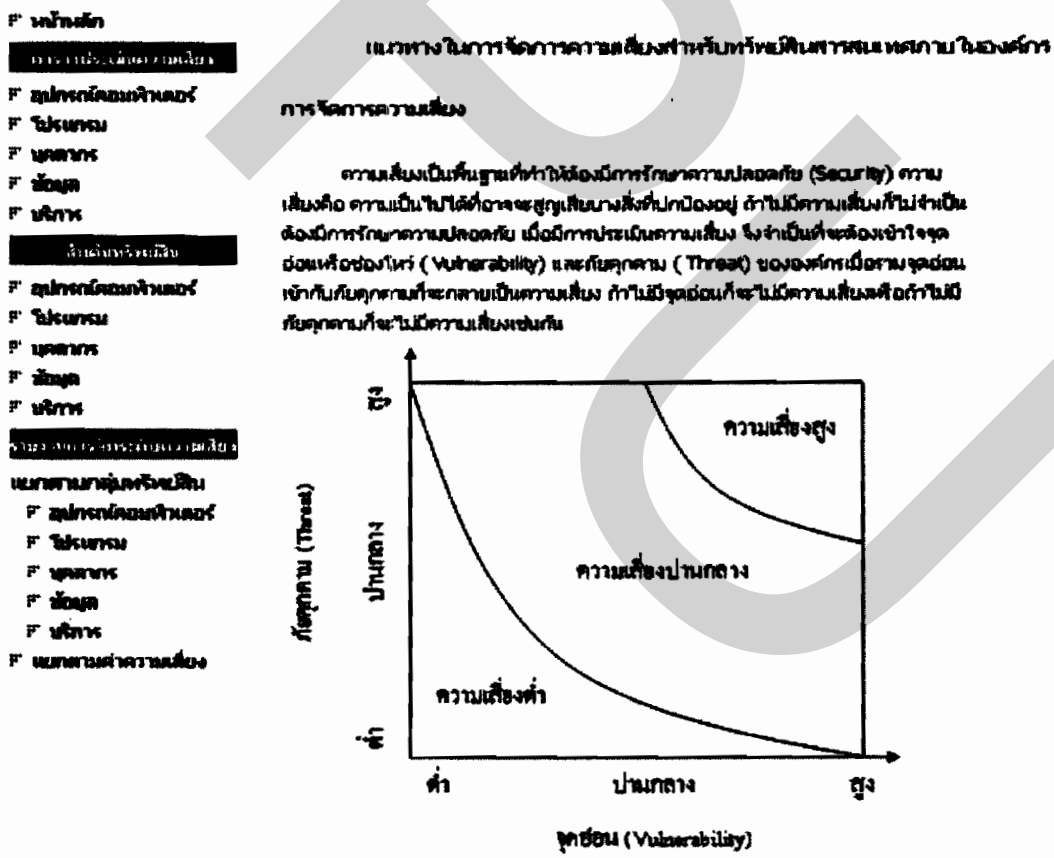
จากภาพที่ 5.1 ในส่วนที่สองจะเกี่ยวข้องแนวคิดในการจัดการความเสี่ยง จะประกอบไปด้วยรายละเอียดที่เกี่ยวกับ องค์ประกอบในระบบงานคอมพิวเตอร์ มาตรฐานการรักษาความปลอดภัยข้อมูลและการจัดการความเสี่ยง ข้อมูลในด้านการจัดการความเสี่ยงจะมีการแบ่งรายละเอียดออกเป็นส่วนย่อยได้แก่ นิยามของความเสี่ยง ความหมายของจุดอ่อนหรือช่องโหว่ ความหมายของภัยคุกคาม กระบวนการด้านการรักษาความปลอดภัยของข้อมูล และกระบวนการในการประเมินความเสี่ยง ซึ่งเมื่อผู้ใช้คลิกที่หัวข้อใดระบบก็จะทำการเชื่อมโยงไปยังหัวข้อนั้น ๆ และแสดงรายละเอียดต่าง ๆ ที่เกี่ยวข้อง ดังตัวอย่างแสดงในภาพที่ 5.5 – 5.9



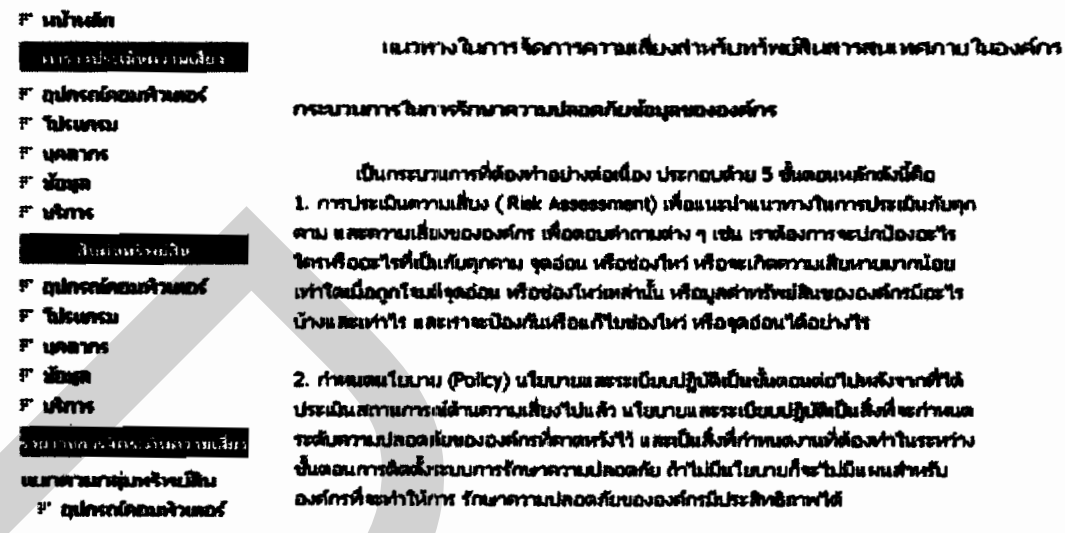
ภาพที่ 5.5 หน้าแสดงรายละเอียด องค์ประกอบในระบบงานคอมพิวเตอร์



ภาพที่ 5.6 หน้าแสดงรายละเอียด มาตรฐานการรักษาความปลอดภัยข้อมูล

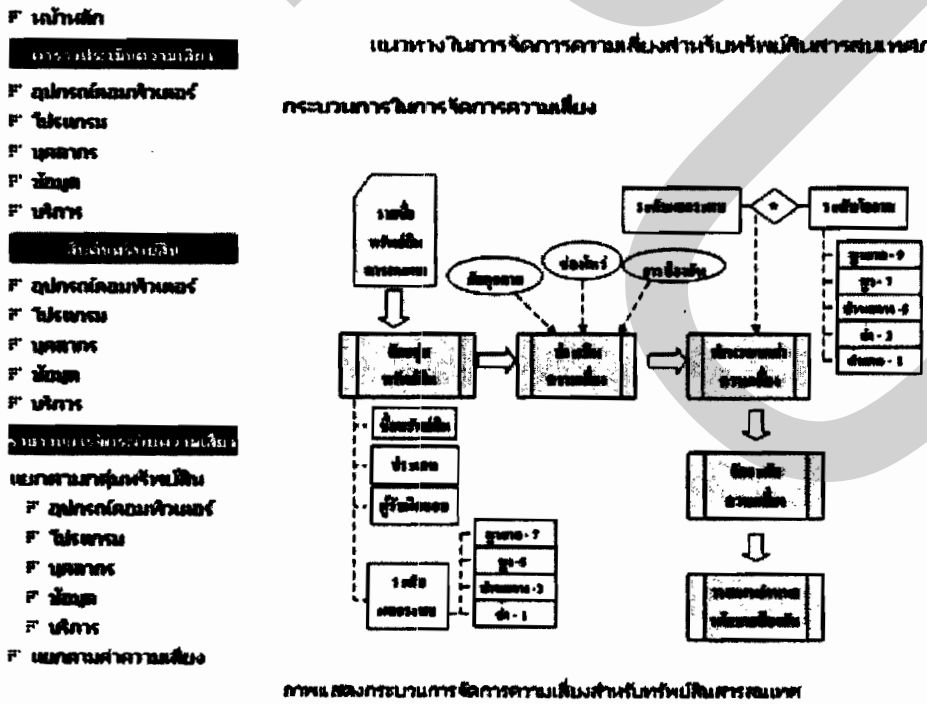


ภาพที่ 5.7 หน้าแสดงรายละเอียด การจัดการความเสี่ยง



ภาพที่ 5.8 หน้าแสดงรายละเอียด กระบวนการในการรักษาความปลอดภัยข้อมูลขององค์กร

ในหน้าเว็บแสดงรายละเอียดกระบวนการในการจัดการความเสี่ยง ผู้ใช้งานจะทราบถึงภาพรวมของแนวทางในการจัดทำระบบต้นแบบ รวมไปถึงขั้นตอนที่มีส่วนเกี่ยวข้องในการจัดการความเสี่ยงให้กับทรัพย์สินสารสนเทศในองค์กรได้อย่างเป็นลำดับ



ภาพที่ 5.9 หน้าแสดงรายละเอียด กระบวนการในการจัดการความเสี่ยง

5.2 การใช้งานเว็บเพจหน้าตารางประเมินความเสี่ยง

ในการจัดทำหน้าเว็บตารางประเมินความเสี่ยง จะจัดแบ่งตามประเภทของทรัพย์สิน 5 รายการคือ อุปกรณ์คอมพิวเตอร์ โปรแกรม บุคลากร ข้อมูล และบริการ เมื่อผู้ใช้งานคลิกที่เมนูด้านซ้ายที่ชื่อ อุปกรณ์คอมพิวเตอร์ ดังภาพที่ 5.10 จะปรากฏหน้าเว็บเพจแสดงตารางรายชื่ออุปกรณ์คอมพิวเตอร์ ซึ่งจะแสดงรายละเอียดของรายชื่อทรัพย์สินสารสนเทศทางด้านอุปกรณ์คอมพิวเตอร์ภายในองค์กร รวมไปถึงผู้รับผิดชอบที่เกี่ยวข้อง เพื่อให้ผู้ใช้ได้เห็นถึงทรัพย์สินประเภทต่างๆ ที่อยู่ในกลุ่มอุปกรณ์คอมพิวเตอร์ และทราบถึงจำนวนของทรัพย์สินที่จัดทำการประเมินความเสี่ยง จากภาพแสดงให้ผู้ใช้งานทราบว่ามีทรัพย์สินสำหรับอุปกรณ์คอมพิวเตอร์ทั้งหมด 5 รายการ ที่จะจัดทำการประเมินความเสี่ยง

ภาพที่ 5.10 หน้าแสดงรายละเอียด ตารางประเมินความเสี่ยงอุปกรณ์คอมพิวเตอร์

เมื่อผู้ใช้งานคลิกที่รายชื่อของทรัพย์สิน เครื่องแม่ข่ายสำหรับระบบ Web Server ดังในภาพที่ 5.10 ระบบจะทำการเชื่อมโยงไปหน้าเว็บข้อมูลตารางแสดงค่าการประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server ดังภาพที่ 5.11 เพื่อแสดงรายละเอียดที่เกี่ยวข้องกับการประเมินความเสี่ยงให้ผู้ใช้ได้ทราบ และสำหรับทรัพย์สินอื่นๆ ก็จะมีการเชื่อมโยงไปยังตารางของทรัพย์สินนั้น โดยมีข้อมูลที่เกี่ยวข้องกันดังนี้คือ จำนวนตารางทั้งหมดสำหรับการประเมินความเสี่ยง สำหรับเครื่องแม่ข่ายระบบ Web Server โดยแตกต่างกันไปตามมาตรการป้องกันและระดับของความเสี่ยง (จากภาพที่ 5.11 คือตารางที่ 1 – 5) และภายในตารางจะประกอบไปด้วยรายชื่อทรัพย์สิน มาตรการป้องกันที่จะใช้ตรวจสอบ (จากตัวอย่างคือ มาตรการที่ 9.1.2 และ 9.2.1) ช่องโหว่ที่ได้ตรวจสอบพบ

สำหรับเครื่องแม่ข่ายในระบบ Web Server รายละเอียดด้านภัยคุกคาม ระดับของโอกาส ระดับของผลกระทบ ความเสี่ยงโดยรวม และแนวทางการป้องกันในกรณีที่ตรวจพบช่องโหว่ที่เป็นจุดอ่อน

ตารางที่ 1 - 5 แสดงค่าการประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server

ตารางที่ 1

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบ Web Server					
A.9.1.2 การควบคุมการเข้า - ออก (Physical entry controls)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน (W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการอนุญาตให้ผ่านเข้า - ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น		1	5	5	

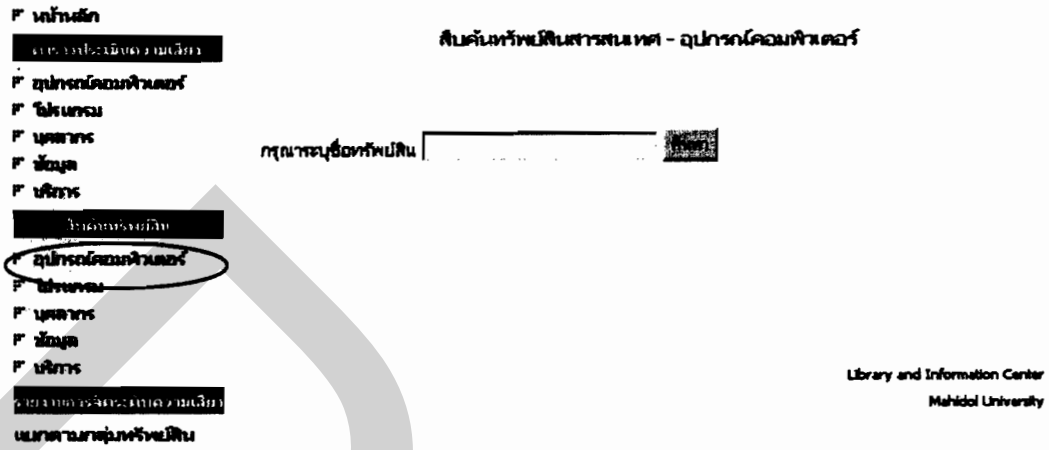
ตารางที่ 2

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบ Web Server					
A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน (W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) การจัดวางอุปกรณ์อยู่ในบริเวณที่มีคลื่นแม่เหล็กไฟฟ้ารบกวน	อุปกรณ์ทำงานผิดพลาด	7	5	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้า รบกวน

ภาพที่ 5.11 ตารางแสดงค่าการประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server

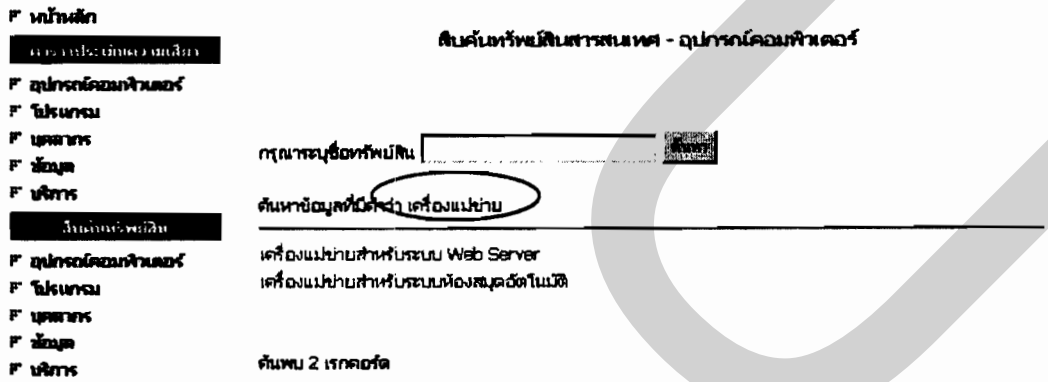
5.3 การใช้งานเว็บเพจหน้าสืบค้นข้อมูลทรัพย์สิน

ในการจัดทำหน้าสืบค้นข้อมูลสำหรับทรัพย์สิน จะจัดแบ่งตามประเภทของทรัพย์สิน ทั้ง 5 กลุ่มคือ อุปกรณ์คอมพิวเตอร์ โปรแกรม บุคลากร ข้อมูล และบริการ ซึ่งเมื่อผู้ใช้งานคลิกที่เมนูด้านซ้ายที่ชื่อ อุปกรณ์คอมพิวเตอร์ ดังภาพที่ 5.12 ระบบจะแสดงข้อมูลของหน้าเว็บเพจสืบค้นข้อมูลทรัพย์สินสารสนเทศภายในองค์กร ซึ่งเป็นการสืบค้นทรัพย์สินทางด้านอุปกรณ์คอมพิวเตอร์ เพื่อให้ผู้ใช้งานสามารถสืบค้นเพื่อหาทรัพย์สินประเภทต่าง ๆ โดยการพิมพ์รายชื่อทรัพย์สินที่ต้องการลงไปในกล่องรับข้อความที่ช่อง กรุณาระบุชื่อทรัพย์สิน เพื่อทำการค้นหารายชื่อทรัพย์สินที่อยู่ในระบบ

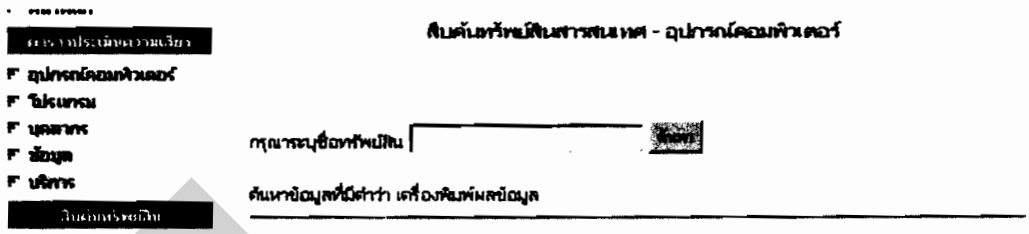


ภาพที่ 5.12 หน้าสืบค้นข้อมูลทรัพย์สินสำหรับอุปกรณ์คอมพิวเตอร์

จากภาพที่ 5.13 เมื่อผู้ใช้พิมพ์รายชื่อทรัพย์สินที่ชื่อ เครื่องแม่ข่าย ที่ต้องการสืบค้น และคลิกที่ปุ่มค้นหา ระบบจะแสดงผลลัพธ์ในการสืบค้น โดยแสดงรายละเอียดของรายชื่อที่สืบค้นและจำนวนรายชื่อทั้งหมดที่ค้นพบ ในกรณีที่สืบค้นแล้วไม่พบรายชื่อของทรัพย์สินนั้น จะแสดงหน้าจอในอีกลักษณะหนึ่งดังภาพที่ 5.14



ภาพที่ 5.13 หน้าแสดงผลลัพธ์การสืบค้น พบข้อมูลทรัพย์สิน สำหรับอุปกรณ์คอมพิวเตอร์



ภาพที่ 5.14 หน้าแสดงผลลัพธ์การสืบค้น ไม่พบข้อมูลทรัพย์สิน สำหรับอุปกรณ์คอมพิวเตอร์

เมื่อผู้ใช้คลิกที่รายชื่อ เครื่องแม่ข่ายสำหรับระบบ Web Server ที่สืบค้นพบ ดังภาพที่ 5.13 ระบบเชื่อมโยงไปยังหน้าเว็บที่แสดงรายละเอียดข้อมูล ตารางแสดงค่าการประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server เพื่อให้ผู้ใช้ได้ทราบ ดังภาพที่ 5.15

ตารางที่ 1 - 5 แสดงค่าการประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server

ตารางที่ 1

ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบ Web Server					
A.9.1.2 การควบคุมการเข้า - ออก (Physical entry controls)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน (W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(S) มีการอนุญาตให้ผ่านเข้า - ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น		1	5	5	

ตารางที่ 2

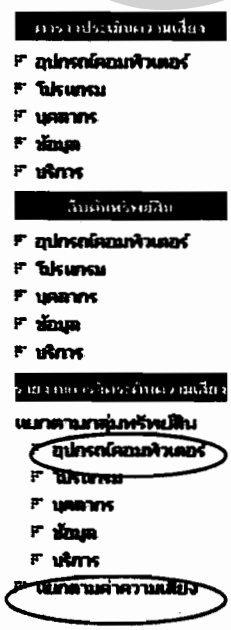
ชื่อทรัพย์สิน : เครื่องแม่ข่ายระบบ Web Server					
A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)					
ช่องโหว่ จุดแข็ง(S) / จุดอ่อน (W)	ภัยคุกคาม	ระดับของโอกาส	ระดับผลกระทบ	ความเสี่ยงรวม	การป้องกัน
(W) การจัดวางอุปกรณ์อยู่ในบริเวณที่มีคลื่นแม่เหล็กไฟฟ้ารบกวน	อุปกรณ์ทำงานผิดพลาด	7	5	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้า รบกวน

ภาพที่ 5.15 หน้าเว็บตารางแสดงค่าการประเมินความเสี่ยงสำหรับเครื่องแม่ข่ายระบบ Web Server

5.4 การใช้งานเว็บเพจหน้ารายงานการจัดระดับความเสี่ยง

ในการจัดทำหน้าเว็บแสดงรายงานการจัดระดับความเสี่ยง จะทำสรุปแยกเป็น 2 ส่วน คือ ส่วนแรกจะแยกตามกลุ่มหรือประเภทของทรัพย์สิน โดยจัดแบ่งทรัพย์สินออกเป็น 5 รายการคือ อุปกรณ์คอมพิวเตอร์ โปรแกรม บุคลากร ข้อมูล และบริการ ส่วนที่สองจะสรุปรายงานการจัดระดับความเสี่ยงแยกตามระดับของค่าความเสี่ยงโดยรวม ซึ่งเรียงลำดับจากค่ามากสุดไปยังค่าน้อยสุด

ในส่วนแรก เมื่อผู้ใช้งานคลิกที่เมนูด้านซ้ายที่ชื่อ อุปกรณ์คอมพิวเตอร์ ในหัวข้อรายงานการจัดระดับความเสี่ยง ดังภาพที่ 5.16 จะปรากฏหน้าจอแสดงรายงานการจัดระดับความเสี่ยงสำหรับทรัพย์สินสารสนเทศทั้งหมด ที่อยู่ในกลุ่มของอุปกรณ์คอมพิวเตอร์ มีรายละเอียดที่เกี่ยวข้องดังนี้คือ รายชื่อของทรัพย์สิน จำนวนจุดอ่อนที่ตรวจพบในทรัพย์สินนั้น มาตรการป้องกันที่ใช้ แล้วตรวจพบจุดอ่อน ค่าความเสี่ยงโดยรวมที่ได้ของทรัพย์สินแยกตามมาตรการป้องกัน และนโยบายการป้องกันที่จะนำไปปฏิบัติเพื่อแก้ไขจุดอ่อนที่ค้นพบ เพื่อให้ค่าของความเสี่ยงลดลงอยู่ในระดับที่องค์กรสามารถยอมรับได้



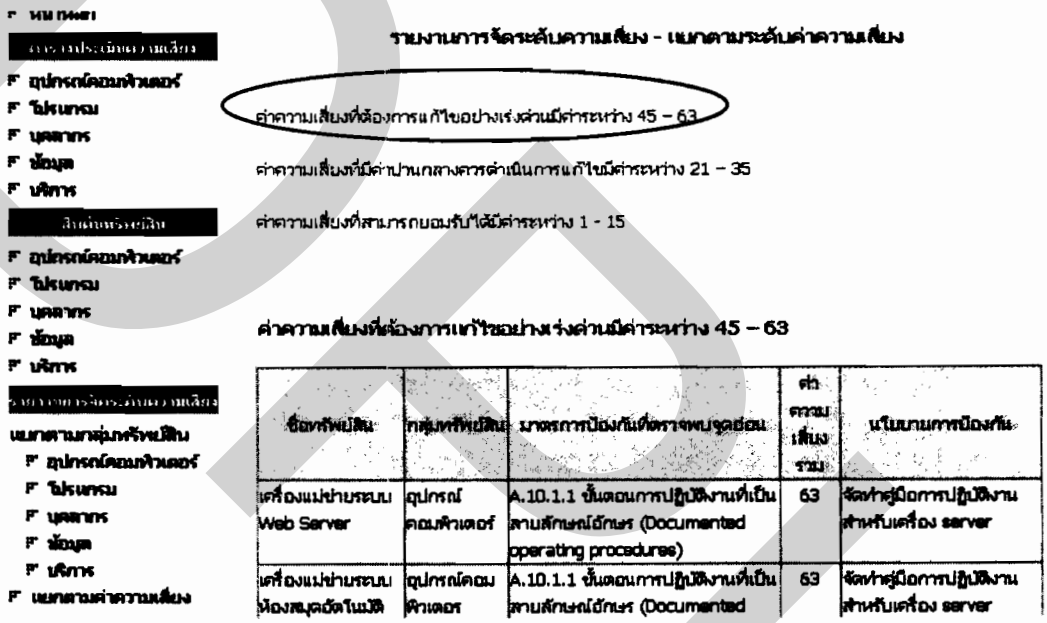
รายงานการจัดระดับความเสี่ยง

อุปกรณ์คอมพิวเตอร์ (Hardware)

ชื่อทรัพย์สิน	จำนวนจุดอ่อนที่พบ	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
เครื่องแม่ข่ายระบบ Web Server	4	1. A.10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	63	จัดทำคู่มือการปฏิบัติงานสำหรับเครื่อง server
		2. A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)	35	- ติดตั้งโปรแกรมป้องกันไวรัส - ให้ความรู้แก่เจ้าหน้าที่ด้านความปลอดภัยของข้อมูล
		3. A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้ารบกวน
		4. A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	35	กำหนดตารางการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ
เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ	4	1. A.10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	63	จัดทำคู่มือการปฏิบัติงานสำหรับเครื่อง server
		2. A.10.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)	35	- ติดตั้งโปรแกรมป้องกันไวรัส - ให้ความรู้แก่เจ้าหน้าที่ด้านความปลอดภัยของข้อมูล
		3. A.9.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment security)	35	มีการจัดวางอุปกรณ์ในตำแหน่งที่ปลอดภัยจากคลื่นแม่เหล็กไฟฟ้ารบกวน
		4. A.9.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	35	กำหนดตารางการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ

ภาพที่ 5.16 หน้าเว็บแสดงรายงานการจัดระดับความเสี่ยงสำหรับอุปกรณ์คอมพิวเตอร์

ในส่วนที่สอง เมื่อผู้ใช้งานคลิกเมนูด้านซ้ายชื่อ แยกตามค่าความเสี่ยง ในหัวข้อรายงานการจัดระดับความเสี่ยง ดังภาพที่ 5.16 จะปรากฏหน้าจอแสดงรายงานการจัดระดับความเสี่ยง โดยแยกตามระดับของค่าความเสี่ยง ดังภาพที่ 5.17 ซึ่งแบ่งออกเป็น 3 ช่วงคือ ช่วงที่หนึ่ง ค่าความเสี่ยงที่ต้องการแก้ไขอย่างเร่งด่วนมีค่าระหว่าง 45 – 63 ในช่วงที่สองคือ ค่าความเสี่ยงที่มีค่าปานกลางควรดำเนินการแก้ไขมีค่าระหว่าง 21 – 35 และช่วงที่สาม ค่าความเสี่ยงที่สามารถยอมรับได้มีค่าระหว่าง 1 – 15



ภาพที่ 5.17 หน้าเว็บแสดงรายงานการจัดระดับความเสี่ยง แยกตามระดับค่าความเสี่ยง

เมื่อผู้ใช้คลิกที่หัวข้อชื่อ ค่าความเสี่ยงที่ต้องการแก้ไขอย่างเร่งด่วนมีค่าระหว่าง 45 – 63 ระบบจะทำการเชื่อมโยงไปยังข้อมูลที่เกี่ยวข้อง ดังภาพที่ 5.18 ซึ่งแสดงรายละเอียดต่อไปนี้ ชื่อของทรัพย์สิน ที่มีค่าความเสี่ยงโดยรวมที่อยู่ระหว่าง 45 – 63 ชื่อกลุ่มของทรัพย์สิน มาตรการป้องกันที่ตรวจพบจุดอ่อน ค่าของความเสี่ยงโดยรวมที่ได้จากการคำนวณแล้ว และนโยบายในการป้องกันเพื่อนำไปปฏิบัติสำหรับแก้ไขจุดอ่อนที่ตรวจพบ

ค่าความเสี่ยงที่ต้องการแก้ไขอย่างเร่งด่วนมีค่าระหว่าง 45 – 63

ชื่อทรัพย์สิน	กลุ่มทรัพย์สิน	มาตรการป้องกันที่ตรวจพบจุดอ่อน	ค่าความเสี่ยงรวม	นโยบายการป้องกัน
เครื่องแม่ข่ายระบบ Web Server	อุปกรณ์คอมพิวเตอร์	A.10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	63	จัดทำคู่มือการปฏิบัติงานสำหรับเครื่อง server
เครื่องแม่ข่ายระบบห้องสมุดอัตโนมัติ	อุปกรณ์คอมพิวเตอร	A.10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	63	จัดทำคู่มือการปฏิบัติงานสำหรับเครื่อง server
งานติดตั้งและบำรุงรักษาอุปกรณ์คอมพิวเตอร์	งานบริการ	A. 9.2. 4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	63	วางแผนการบำรุงรักษาอุปกรณ์ให้ทำงานได้อย่างต่อเนื่องและสม่ำเสมอ
		A. 10.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)	63	มีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต
		A. 14.1. 2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)	63	มีการประเมินเหตุการณ์ต่างๆที่จะทำให้การทำงานหยุดชะงักและกำหนดแนวทางป้องกัน
งานติดตั้งและบำรุงรักษาโปรแกรมคอมพิวเตอร์	งานบริการ	A. 14.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)	63	มีแนวทางการป้องกันเหตุการณ์ต่างๆที่จะทำให้การทำงานหยุดชะงัก

ภาพที่ 5.18 หน้าเว็บแสดงค่าความเสี่ยงที่ต้องการแก้ไขอย่างเร่งด่วน มีค่าระหว่าง 45 – 63

บทที่ 6
สรุปผลการวิจัย

6.1 สรุปผลการวิจัย

การจัดทำระบบต้นแบบการจัดการความเสี่ยง สำหรับทรัพย์สินสารสนเทศภายในองค์กร ตามมาตรฐานสากล BS 7799 กรณีศึกษา : สำนักหอสมุด มหาวิทยาลัยมหิดล เกี่ยวข้องกับการศึกษา รวบรวมข้อมูล ทางด้านทรัพย์สินสารสนเทศภายในองค์กร โดยมีการจัดแบ่งหมวดหมู่ของทรัพย์สิน ออกเป็น 5 กลุ่ม ได้แก่ อุปกรณ์คอมพิวเตอร์ โปรแกรม บุคลากร ข้อมูล และงานบริการ เพื่อจะนำมา จัดทำประเมินความเสี่ยงถึงปัญหาที่จะเกิดขึ้นต่อทรัพย์สินเหล่านั้น และหาแนวทางป้องกัน แล้วนำ ข้อมูลเหล่านี้มาทำการพัฒนาระบบต้นแบบในการจัดการความเสี่ยงด้านทรัพย์สินสารสนเทศ ให้กับ ทาง สำนักหอสมุด มหาวิทยาลัยมหิดล โดยการใช้รูปแบบของการพัฒนาระบบในลักษณะการทำงาน แบบ Client-Server ร่วมกับการทำงานในระบบ Web-based โดยนำเสนอผ่านทางระบบออนไลน์ที่ใช้ งานภายในองค์กร เพื่อเผยแพร่ข้อมูลที่เกี่ยวข้องกับกระบวนการ ในการจัดทำการประเมินความเสี่ยง ได้แก่ แนวทางในการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศภายในองค์กร ตารางที่แสดงค่า การประเมินความเสี่ยงสำหรับทรัพย์สิน การสืบค้นทรัพย์สินสารสนเทศ รายงานการจัดระดับความ เสี่ยงที่มีต่อทรัพย์สิน โดยการประยุกต์ใช้โปรแกรม ภาษา HTML : Hypertext Markup Language ร่วมกับภาษาคริปท์ PHP : Hypertext Preprocessor เพื่อจะให้บุคลากรภายในองค์กร ซึ่งเป็นผู้ใช้งาน สามารถศึกษา และค้นหาข้อมูลทางด้านแนวทางในการจัดการความเสี่ยง ให้กับทรัพย์สินสารสนเทศ ภายในองค์กร ได้อย่างเป็นระบบ

การจัดทำหน้าเว็บเพจ เพื่อเผยแพร่ข้อมูลที่เกี่ยวข้องกับแนวทางในการจัดการความเสี่ยง สำหรับทรัพย์สินสารสนเทศให้แก่ผู้ใช้งานในองค์กร ได้มีการนำข้อมูลที่ศึกษาและวิเคราะห์ถึงด้าน การประเมินความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กร เพื่อจะออกแบบหน้าเว็บเพจโดยแบ่ง ข้อมูลออกเป็น 4 ส่วน ได้แก่ หน้าที่เป็นข้อมูลหลัก หน้าตารางประเมินความเสี่ยง หน้าสืบค้นข้อมูล ทรัพย์สิน และหน้ารายงานการจัดระดับความเสี่ยง

ผลการทดสอบการจัดทำหน้าเว็บเพจเพื่อเผยแพร่ข้อมูล ระบบต้นแบบการจัดการความ เสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กร สามารถสรุปได้ดังนี้

1. ระบบสามารถเผยแพร่ข้อมูลให้ผู้ใช้งานได้ทราบถึงแนวทางในการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศภายในองค์กร โดยสามารทราบถึง ความสำคัญในการจัดการความเสี่ยง และแนวคิดในการจัดทำ และกระบวนการในการประเมินความเสี่ยง

2. ระบบสามารถเผยแพร่ข้อมูลให้ผู้ใช้งานได้ทราบถึง ช่องโหว่ ภัยคุกคาม ระดับของความเสี่ยงที่เกิดขึ้นต่อทรัพย์สินในประเภทต่าง ๆ รวมไปถึงแนวทางการป้องกัน

3. ระบบสามารถให้ผู้ใช้งานค้นหาทรัพย์สิน ที่ผู้ใช้ต้องการทราบถึง รายละเอียดในการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศภายในองค์กร แล้วเชื่อมโยงไปยังข้อมูลเหล่านั้น เพื่อศึกษาได้

4. ระบบสามารถเผยแพร่ข้อมูลให้ผู้ใช้งานทราบถึง รายงานการจัดระดับความเสี่ยงของทรัพย์สินสารสนเทศโดยแยกตามประเภทของทรัพย์สินและระดับของค่าความเสี่ยงรวม

6.2 อภิปรายผลการศึกษา

ผลการศึกษาพบว่า ระบบต้นแบบของการจัดการความเสี่ยงที่ถูกพัฒนาขึ้นมา ผู้ใช้งานสามารถเข้าถึงข้อมูลได้ทุกสถานที่ จากการเชื่อมต่อระบบเครือข่ายภายในองค์กร ผ่านทางหน้าเว็บบราวเซอร์ต่าง ๆ ได้เช่น Internet Explorer, Firefox เป็นต้น การประมวลผลข้อมูลของระบบจะเป็นลักษณะแบบ Web based ซึ่งมีการติดต่อส่งข้อมูลถึงกันระหว่างเครื่องคอมพิวเตอร์แต่ละเครื่องผ่านทางหน้าเว็บเพจ โดยการใช้โปรโตคอล แบบ HTTP เพื่อจะส่งคำร้องขอไปยังเครื่องแม่ข่ายผ่านทางเว็บบราวเซอร์ซึ่งช่วยทำให้องค์กร สามารถที่จะสร้างระบบบริหารจัดการความมั่นคงปลอดภัย ของสารสนเทศขึ้นมาได้อย่างมีประสิทธิภาพ

6.3 ข้อเสนอแนะ

ระบบต้นแบบของการจัดการความเสี่ยงที่จัดทำขึ้นในการวิจัยครั้งนี้ สำหรับรายงานการจัดระดับความเสี่ยงสำหรับทรัพย์สินสารสนเทศ ระบบยังไม่สามารถจัดเรียงระดับของค่าความเสี่ยงโดยรวมได้เอง ยังคงต้องให้ผู้จัดทำระบบเป็นผู้จัดเรียงระดับของค่าความเสี่ยงที่ได้จากการประเมินความเสี่ยงแล้วด้วยตนเอง ก่อนนำข้อมูลเผยแพร่ผ่านบนหน้าเว็บเพจของระบบ และสำหรับรายชื่อทรัพย์สินที่อยู่ในระบบที่ใช้ในการสืบค้น หากต้องมีการเพิ่มรายชื่อทรัพย์สินเข้าไปในระบบเพื่อให้สามารถสืบค้นได้ จะต้องเพิ่มรายชื่อเข้าไปใหม่โดยผู้จัดทำระบบเอง

บรรณานุกรม

DPU

บรรณานุกรม

ภาษาไทย

หนังสือ

กิตติ ภักดีวัฒนะกุล. (2547). **คัมภีร์ PHP**. กรุงเทพฯ: เคทีพี คอมพ์ แอนด์ คอนซัลท์.

กิติศักดิ์ เจริญโภคานนท์. (2548). **คู่มือเรียนเขียนเว็บอีคอมเมิร์ซด้วย PHP 5 ครอบคลุมเวอร์ชั่นล่าสุด 5.1** . กรุงเทพฯ : ซัคเซส มีเดีย.

จตุชัย แพงจันทร์. (2550). **Master in Security**. นนทบุรี : ไอดีซีฯ.

วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล. (2548). **ความรู้เบื้องต้นเกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศ**. กรุงเทพฯ : โปรวิชั่น.

สมประสงค์ ชิตินิลนิธิ. (2545). **เรียนลัด PHP 4 ครอบคลุมเวอร์ชั่น 4.2**. กรุงเทพฯ: โปรวิชั่น

สาธิต ชัยวิวัฒน์ตระกูล. (2550). **เก่ง PHP5 ให้ครบสูตร**. กรุงเทพฯ: วิตตี้กรุ๊ป.

สารสนเทศจากสื่ออิเล็กทรอนิกส์

จักรกฤษณ์ แร่ทอง. (2547, มิถุนายน). ISO/IEC 17799 (BS 7799) เกี่ยวข้องกับข้อมูลอย่างไร. สืบค้นเมื่อ 10 พฤศจิกายน 2550, จาก **http://www.nextproject.net/article_detail.aspx?a_id=49.**

ปริญญา หอมเอนก. (2548, กรกฎาคม). สถานการณ์ขององค์กรในประเทศไทยเกี่ยวกับการรับรองมาตรฐาน BS 7799 Part 2 กับบทวิเคราะห์มาตรฐานการรักษาความปลอดภัยข้อมูลสารสนเทศ ISO/IEC 17799 Second Edition และมาตรฐาน ISO/IEC FDIS 27001 : 2005. สืบค้นเมื่อ 5 กุมภาพันธ์ 2550, จาก **http://www.acisonline.net/article_prinya_eweek_150748.htm**

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย. (2550). Risk Management based on BS 7799-3:2006. สืบค้นเมื่อ 24 มิถุนายน 2550, จาก **http://www.dpu.ac.th/graduate/mscct/upload/tutorial/13/04.Riskman.ppt**

สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ. (2545). ISO 17799 (BS 7799) ความมั่นคงปลอดภัยจากภาครัฐสู่ภาครัฐ. สืบค้นเมื่อ 27 กันยายน 2550, จาก

http://www.gits.net.th/knowledge/newsletter/ittalk/index.asp?MenuID=26&RootMenuID=8&Book=9)

ภาษาต่างประเทศ

DISSERTATIONS

Chen Chung Shih. (2005). **A Study on Risk Assessment and Management of Information Security**. MIS. Taiwan: Chung Yuan Christian University.

Fredrik M Andersson. (2004). **ISO/IEC 17799 Compliant**. Sweden: Stockholm University.

Lauri Helenius. (2004). **Analysing B2B e-order system security threats**. Finland: Helsinki University of Technology.

Oumeshsingh Sookdawoor. (2005). **An investigation of information security policies and practices in Mauritius**. MSC. South Africa: University of South Africa.

ภาคผนวก

DPU

ภาคผนวก ก

การตรวจสอบมาตรการป้องกันสำหรับทรัพย์สินในองค์กร

DPU

ในการตรวจสอบมาตรการป้องกันสำหรับทรัพย์สินสารสนเทศในองค์กร สามารถเก็บรวบรวมข้อมูลที่ต้องการศึกษาได้จาก ตัวอย่างแบบฟอร์มการตรวจสอบมาตรการป้องกัน (Physical Checklist) ซึ่งสามารถจัดทำได้โดยแยกตามมาตรการป้องกันที่มีทั้งหมด 11 โดเมนที่อยู่ในมาตรฐาน ISO/IEC 17799 (ดังภาพที่ 2.1) เพื่อที่จะศึกษาถึงมาตรการป้องกันในระบบงานเดิมที่มีต่อทรัพย์สินสารสนเทศภายในองค์กร แล้วนำข้อมูลเหล่านี้ไปวิเคราะห์เพื่อหาแนวทางป้องกัน ให้ความเสี่ยงที่มีต่อทรัพย์สินอยู่ในระดับที่องค์กรสามารถยอมรับได้

แบบฟอร์มการตรวจสอบมาตรการป้องกัน (Physical Checklist)

A.9 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

(Physical and Environmental security)

ลำดับที่	วัตถุประสงค์	มาตรการป้องกัน	การตรวจสอบ	สถานะภาพ
1	A.9.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)	A.9.1.1 การจัดทำบริเวณล้อมรอบ (Physical Security perimeter)	☐ สัมภาษณ์ ☐ สำรวจดูสถานที่	☐ พบ ☐ ไม่พบ
2		A.9.1.2 การควบคุมการเข้า-ออก (Physical entry controls)	☐ สัมภาษณ์ ☐ สำรวจดูสถานที่	☐ พบ ☐ ไม่พบ
3		A.9.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Security offices, room and facilities)	☐ สัมภาษณ์ ☐ สำรวจดูสถานที่	☐ พบ ☐ ไม่พบ

แบบฟอร์มการตรวจสอบมาตรการป้องกัน (Physical Checklist) (ต่อ)

A.10 การสื่อสารและการบริหารการปฏิบัติงาน

(Communications and Operations Management)

ลำดับที่	วัตถุประสงค์	มาตรการป้องกัน	การตรวจสอบ	สถานะภาพ
1	A.10.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)	A.10.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)	☐ สัมภาษณ์ ☐ สำรวจดูสถานที่	☐ พบ ☐ ไม่พบ
2		A.10.1.2 การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ (Change management)	☐ สัมภาษณ์ ☐ สำรวจดูสถานที่	☐ พบ ☐ ไม่พบ
3		A.10.1.3 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)	☐ สัมภาษณ์ ☐ สำรวจดูสถานที่	☐ พบ ☐ ไม่พบ

ประวัติผู้เขียน

ชื่อ-นามสกุล	นายกฤษฎา แก้วผุดผ่อง
ประวัติการศึกษา	คอมพิวเตอร์ธุรกิจบัณฑิต มหาวิทยาลัยอัสสัมชัญ 2541
ตำแหน่งและสถานที่ทำงานปัจจุบัน	นักวิชาการคอมพิวเตอร์ สำนักหอสมุด มหาวิทยาลัยมหิดล ตั้งอยู่ที่ ถนนพุทธมณฑล สาย 4 ตำบลศาลายา อำเภอพุทธมณฑล จังหวัดนครปฐม
ประสบการณ์ทำงาน	- ติดตั้งและบำรุงรักษาอุปกรณ์ และโปรแกรมคอมพิวเตอร์ - ติดตั้งและบำรุงรักษาเครื่องแม่ข่ายคอมพิวเตอร์
ทุนการศึกษา	ทุนการศึกษาจากมหาวิทยาลัยธุรกิจบัณฑิตย์

DPU