เครื่องมือสนับสนุนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้แบบรูปความมั่นคง

นางสาวปรมาภรณ์ ร่วมจินดา

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2556

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย
บทคัดย่อและแฟ้มข้อมูลฉบับเต็มของวิทยานิพนธ์ตั้งแต่ปีการศึกษา 2554 ที่ให้บริการในคลังปัญญาจุฬาฯ (CUIR)
เป็นแฟ้มข้อมูลของนิสิตเจ้าของวิทยานิพนธ์ที่ส่งผ่านทางบัณฑิตวิทยาลัย
The abstract and full text of theses from the academic year 2011 in Chulalongkorn University Intellectual Repository(CUIR)
are the thesis authors' files submitted through the Graduate School.

A Supporting Tool for Information Security Standards Storage and Retrieval using Security Patterns

Miss Poramaporn Ruamjinda

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Software Engineering
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2013

Copyright of Chulalongkorn University

หัวข้อวิทยานิพนธ์	เครื่องมือสนับสนุนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐาน ความมั่นคงสารสนเทศโดยใช้แบบรูปความมั่นคง
โดย	นางสาวปรมาภรณ์ ร่วมจินดา
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.บัณฑิต เอื้ออาภรณ์)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.วันชัย ริ้วไพบูลย์)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล)

..... กรรมการ
(รองศาสตราจารย์ ดร. ทวิตีย์ เสนีวงศ์ ณ อยุธยา)

..... กรรมการภายนอกมหาวิทยาลัย
(รองศาสตราจารย์ ดร. วีระ บุญจริง)

ปรมาภรณ์ ร่วมจินดา : เครื่องมือสนับสนุนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐาน ความมั่นคงสารสนเทศโดยใช้แบบรูปความมั่นคง (A Supporting Tool for Information Security Standards Storage and Retrieval using Security Patterns) อ. ที่ปรึกษาวิทยานิพนธ์หลัก : ผศ. นครทิพย์ พร้อมพูล, 100 หน้า.

การกำหนดนโยบายความมั่นคงสารสนเทศขององค์กรต่าง ๆ นั้นมีวัตถุประสงค์หลักเพื่อให้การดำเนินการทางอิเล็กทรอนิกส์ในองค์กรมีความมั่นคงและเชื่อถือได้ ปัญหาโดยทั่วไปที่มักประสบคือ การกำหนดนโยบายความมั่นคงสารสนเทศมักขึ้นอยู่กับประสบการณ์และความเชี่ยวชาญของผู้ที่เกี่ยวข้อง การประยุกต์ใช้มาตรฐานที่ได้รับการยอมรับและแนวปฏิบัติที่ดีด้านความมั่นคงสารสนเทศน่าจะช่วยทุเลาปัญหาดังกล่าวได้ อย่างไรก็ตามในแต่ละองค์กรหรือโครงการอาจมีการกำหนดนโยบายความมั่นคงที่มีความหลากหลายในสถานการณ์ที่แตกต่างกัน จึงเป็นผลให้ต้องมีการเลือกบริบทให้เหมาะสมในการประยุกต์ใช้มาตรฐานและแนวปฏิบัติที่ดี ปัจจุบันมาตรฐานไอเอสโอ/ไออีซี 27002 และหนังสือแบบรูปความมั่นคงเขียนโดย M. Schumarker และคณะ ซึ่งทั้งสองรายการได้ระบุแนวปฏิบัติที่ดีที่องค์กรต่างๆ สามารถนำไปประยุกต์ใช้ในหลายบริบทได้

งานวิจัยนี้นำเสนอเครื่องมือสนับสนุนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง (ไอเอสโอ/ไออีซี 27002) โดยใช้หลักการจัดเก็บและค้นคืนสารสนเทศของแบบจำลองปริภูมิเวคเตอร์ เพื่อช่วยสนับสนุนการค้นคืนบริบทความมั่นคงจากส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศนั้น ได้ตรงตามความต้องการของผู้ใช้ จาก 3 วิธีการ คือ 1) คำสำคัญที่ปรากฏในโครงสร้างข้อมูลความมั่นคงสารสนเทศที่สร้างจากแบบรูปความมั่นคง 2) คำสำคัญทั่วไปและ 3) ความสัมพันธ์ระหว่างแบบรูปความมั่นคง โดยได้ทำการทดลองในกลุ่มผู้ใช้งานสองประเภทคือ ผู้เชี่ยวชาญด้านความมั่นคงและผู้ใช้งานทั่วไป

ผลที่ได้จากการทดลองแสดงให้เห็นว่า การค้นคืนโดยใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ มีประสิทธิผลที่ดีกว่าการค้นคืนโดยใช้คำสำคัญในทั้งสองกลุ่มทดลอง และในตัววัดค่ามัชฌิมฮาร์โมนิกและค่าระลึก แต่มีประสิทธิผลลดลงในตัววัดความแม่นยำ โดยจากกลุ่มตัวอย่างผู้เชี่ยวชาญ การค้นคืนโดยใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ ให้ค่าระลึกเฉลี่ยและค่ามัชฌิมฮาร์โมนิกเพิ่มขึ้นเป็น 115.05% และ 49.14% ตามลำดับ แต่ให้ค่าความแม่นยำลดลง 6.33% และสำหรับผู้ใช้ทั่วไปการค้นคืนโดยใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ ให้ค่าระลึกเฉลี่ยและค่ามัชฌิมฮาร์โมนิกเพิ่มขึ้นเป็น 354.26% และ 180.62% ตามลำดับ แต่ให้ค่าความแม่นยำลดลง 9.27%

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต.....

สาขาวิชา วิศวกรรมซอฟต์แวร์ ลายมือชื่อ อ. ที่ปรึกษาวิทยานิพนธ์หลัก.....

ปีการศึกษา 2556

5470962021 : MAJOR COMPUTER ENGINEERING

KEYWORDS : INFORMATION RETRIEVAL/INFORMATION SECURITY/SECURITY PATTERN/SECURITY STANDARD

PORAMAPORN RUAMJINDA : A SUPPORTING TOOL FOR INFORMATION SECURITY STANDARDS STORAGE AND RETRIEVAL USING SECURITY PATTERNS. ADVISOR : ASST. PROF. NAKORNTHIP PROMPOON, 100 pp.

The main goal of security policy establishment in any organization is to provide the security and reliability of the electronic operation. General problem that organization may face is that this policy establishment usually depends on the stakeholders' expertise and experience. The application of the widely accept security standards and best practices may help alleviate this problem. However, in any organization or project may have to establish different security policies in various scenarios. This results in the selection of the appropriate content of security standards and practices. At present, ISO 27002 and the textbook named Security Patterns [1] written by M. Schumarker etc. are provided best practices for any organization may be applied in security context.

This research proposes a tool for the storage and retrieval of information security standards (ISO 27002) using information retrieval principle based on Vector Space Model in order to retrieve the standard document sections that relevant to the user need. There are three methods: 1) a method of using keywords appeared in information security structure constructed from security patterns, 2) a method of using only keywords, and 3) a method of using the relationship among security patterns. In addition, the proposed methods were applied to two user groups: security expert and regular user.

The experiment result indicated that in both groups of users, the retrieval of document section of security standard using keywords appeared in information security structure earned a higher result than using only keywords in recall and harmonic mean evaluation metric but yielded a less efficient in precision. From the expert user group, the average recall and the harmonic mean increased 115.05% and 49.14% respectively, while the precision decreased 6.33%. In the regular security user, the average recall value and the harmonic mean increased 354.26% and 180.62%, respectively, while the precision decreased 27.9%.

Department : Computer Engineering Student's Signature .....

Field of Study : Software Engineering Advisor's Signature .....

Academic Year : .....2013.....

กิตติกรรมประกาศ

ข้าพเจ้าขอขอบพระคุณ ศาสตราจารย์นครทิพย์ พร้อมพูล อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่เสียสละเวลาช่วยเหลือให้คำปรึกษา คำแนะนำและข้อคิดเห็นที่มีประโยชน์ ทำให้การจัดทำวิทยานิพนธ์ให้สำเร็จลุล่วงไปด้วยดี ร่วมถึงความเอาใจใส่ต่าง ๆ ที่เป็นแรงผลักดันและส่งเสริมให้งานวิจัยสำเร็จลุล่วงไปได้ด้วยดี

ขอขอบพระคุณ รองศาสตราจารย์ ดร.วันชัย ริ้วไพบูลย์สิน ประธานกรรมการสอบวิทยานิพนธ์ และรองศาสตราจารย์ ดร. ทวิตีย์ เสนีวงศ์ ณ อยุธยา กรรมการสอบวิทยานิพนธ์ ที่กรุณาให้ คำแนะนำต่าง ๆ ทำให้วิทยานิพนธ์นี้มีความถูกต้องและสมบูรณ์มากขึ้น

ขอขอบพระคุณ คุณพ่อ คุณแม่ ที่ให้ความรัก ความห่วงใย คอยให้กำลังใจ พร้อมทั้งให้ความช่วยเหลือ และสนับสนุนในด้านค่าใช้จ่ายในการศึกษาจนสำเร็จลุล่วงได้

ขอขอบคุณพี่ ๆ ที่ศูนย์คอมพิวเตอร์ มหาวิทยาลัยกรุงเทพและเพื่อน ๆ ทุกคนสำหรับคำปรึกษาที่ดีในทุก ๆ ด้านรวมทั้งกำลังใจและความช่วยเหลือ
อื่นๆ ที่มอบให้มาโดยตลอด

ขอขอบคุณห้องปฏิบัติการวิศวกรรมซอฟต์แวร์ สำหรับที่ทำงานอันแสนอบอุ่นตลอดเวลาที่ทำงานร่วมกัน

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง

บทคัดย่อภาษาอังกฤษ ..... จ

กิตติกรรมประกาศ ..... ฉ

สารบัญ ..... ช

สารบัญตาราง ..... ญ

สารบัญรูป ..... ฏ

บทที่ 1 บทนำ 1

1.1 ความเป็นมาและความสำคัญของปัญหา 1

1.2 วัตถุประสงค์ของการวิจัย 2

1.3 ขอบเขตของการวิจัย 3

1.4 ขั้นตอนการวิจัย 3

1.5 ประโยชน์ที่คาดว่าจะได้รับ 3

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 5

2.1 แนวคิดและทฤษฎี 5

2.1.1 นโยบายความมั่นคงสารสนเทศ (Information Security Policy) 5

2.1.2 เอกสารมาตรฐาน ไอเอสโอ/ไออีซี 27002:2005 7

2.1.3 แบบรูปความมั่นคง (Security Pattern) 8

2.1.4 การจัดเก็บและค้นคืนสารสนเทศ (Information Retrieval and Storage) 11

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง 17

2.2.1 แบบรูปความมั่นคง (Security Pattern) 17

2.2.2 การจัดเก็บและค้นคืนสารสนเทศ (Information Retrieval and Storage) 18

บทที่ 3 การวิเคราะห์และออกแบบระบบ 19

หน้า

3.1 การวิเคราะห์แบบรูปความมั่นคงเพื่อจำแนกแบบรูปความมั่นคงตามหลักของ ซี.ไอ.เอ.เอ 20
3.2 การวิเคราะห์และออกแบบวิธีการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐาน ไอเอสโอ/ไออีซี 27002 21
3.2.1 ส่วนการจัดเก็บ 23
3.2.2 ส่วนการค้นคืน 31
3.2.3 การประเมินประสิทธิผลของระบบการค้นคืน 39
บทที่ 4 การพัฒนาเครื่องมือ 40
4.1 ระบุกลุ่มผู้ใช้ 40
4.2 ความต้องการเชิงหน้าที่ 40
4.3 ความต้องการที่ไม่ใช่หน้าที่ 42
4.4 โครงสร้างของเครื่องมือ 42
4.4.1 สถาปัตยกรรมของเครื่องมือ 42
4.4.2 สภาพแวดล้อมที่ใช้ในการพัฒนาเครื่องมือ 43
4.4.3 การออกแบบแบบจำลองข้อมูล 44
4.5 การทำงานและส่วนต่อประสานผู้ใช้ 46
4.5.1 ส่วนการจัดเก็บแบบรูปความมั่นคง 47
4.5.2 ส่วนการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง 48
บทที่ 5 การทดสอบระบบและการประเมินผลการทำงานของระบบ 52
5.1 การประเมินคุณภาพของเครื่องมือต้นแบบ 52
5.2 การทดสอบความครบถ้วนของฟังก์ชันการทำงานของเครื่องมือต้นแบบ 52
5.3 การทดสอบความถูกต้องของฟังก์ชันการทำงานของเครื่องมือต้นแบบ 54
5.4 การทดลองเพื่อเปรียบเทียบผลจากการค้นคืน 57
5.4.1 วัตถุประสงค์ของการทดลอง 57
5.4.2 วิธีการทดลอง 58

หน้า

5.5 ตัวอย่างการทดลองและประเมินผลการทดลอง 62
5.6 การประเมินผลการทดลอง 65
บทที่ 6 สรุปผลการวิจัย 69
6.2 สรุปผลการวิจัย 69
6.3 ข้อจำกัดของงานวิจัย 71
6.4 งานวิจัยในอนาคต 71
6.4 ผลงานตีพิมพ์จากวิทยานิพนธ์ 72
รายการอ้างอิง 73
ภาคผนวก 75
ภาคผนวก ก แบบรูปความมั่นคงที่ใช้ในการทดลอง 76
ภาคผนวก ข โจทย์ปัญหาและข้อคำถามที่ใช้ในการทดลอง 82
ภาคผนวก ค ตัวอย่างค่าระลึก ค่าความแม่นยำและค่ามัชฌิมฮาร์โมนิก ที่ได้จากการทดลอง..... 93
ภาคผนวก ง รายละเอียดโครงสร้างตารางที่ทำการจัดเก็บในฐานข้อมูล 96
ประวัติผู้เขียนวิทยานิพนธ์ 100

สารบัญตาราง

หน้า

ตารางที่ 2.1 รายละเอียดโครงสร้างแบบรูปความมั่นคงของ M. SCHUMACHER และคณะ 10
ตารางที่ 3.1 การจัดเก็บส่วนของเอกสารมาตรฐานด้านความมั่นคง 23
ตารางที่ 3.2 ตัวอย่างการจัดเก็บแฟ้มดัชนีผกผันของส่วนเอกสาร 29
ตารางที่ 3.3 ตัวอย่างการจัดเก็บแฟ้มดัชนีผกผันของแบบรูปความมั่นคงที่ระบุค่าน้ำหนักของแต่ละดัชนี 29
ตารางที่ 3.4 ตัวอย่างผลลัพธ์จากการสร้างข้อคำถามใหม่จากตัวอย่างข้อคำถามเมื่อผู้ใช้ทำการเลือก 34
ตารางที่ 3.5 ผลลัพธ์จากกิจกรรมสกัดคำสำคัญจากข้อคำถามในวิธีการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงโดยใช้คำสำคัญจากตัวอย่างข้อคำถาม 2 รายการ 35
ตารางที่ 3.6 ผลลัพธ์จากกิจกรรมสกัดคำสำคัญจากข้อคำถามในวิธีการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงโดยใช้คำสำคัญจากตัวอย่างในข้อ 5.1 35
ตารางที่ 4.1 อธิบายคลาสของระบบ 45
ตารางที่ 5.1 มิติปัจจัยการประเมินคุณภาพและมาตรวัดที่ใช้ 52
ตารางที่ 5.2 การทดสอบความครบถ้วนของฟังก์ชันการทำงานของเครื่องมือต้นแบบ 53
ตารางที่ 5.3 การทดสอบความถูกต้องของการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง 54
ตารางที่ 5.4 การทดสอบความถูกต้องของการค้นคืนส่วนของเอกสารมาตฐานความมั่นคงโดยใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ 55
ตารางที่ 5.5 การทดสอบความถูกต้องของการจัดทำดัชนีเอกสาร 56
ตารางที่ 5.6 การทดสอบความถูกต้องของการจัดเก็บแบบรูปความมั่นคง 56
ตารางที่ 5.7 กลุ่มหน่วยทดลอง 60
ตารางที่ 5.8 ตัวอย่างส่วนเอกสารที่เกี่ยวข้องที่ระบุโดยผู้เชี่ยวชาญ 62
ตารางที่ 5.9 ตัวอย่างข้อคำถามและการขยายข้อคำถาม 63
ตารางที่ 5.10 ตัวอย่างผลการทดลองที่ได้จากการทดลอง 64
ตารางที่ 5.11 เปรียบเทียบผลการทดลองโดยใช้ ค่าระลึก ค่าความแม่นยำ และค่ามัชฌิมฮาร์โมนิกสำหรับผู้ใช้ทั่วไป 65
ตารางที่ 5.12 เปรียบเทียบผลการทดลองโดยใช้ ค่าระลึก ค่าความแม่นยำ และค่ามัชฌิมฮาร์โมนิกสำหรับผู้เชี่ยวชาญ 66

หน้า

ตารางที่ 5.13 เปรียบเทียบผลการทดลองโดยใช้ ค่าระลึก ค่าความแม่นยำและค่ามัชฌิมฮาร์โมนิก จาก 2 กลุ่มหน่วยทดลอง 68
ตารางที่ ก.1 แสดงแบบรูปความมั่นคงที่ใช้ในงานวิจัย [1] 76
ตารางที่ ก.2 การจำแนกแบบรูปความมั่นคงตามหลักของ ซี.ไอ.เอ.เอ 77
ตารางที่ ก.3 ตารางแสดงเงื่อนไขระหว่างแบบรูป [5] 78
ตารางที่ ก.4 ตารางแสดงความสัมพันธ์ระหว่างแบบรูป [5] 80
ตารางที่ ข.1 โจทย์ปัญหาที่ใช้ในการทดลอง 82
ตารางที่ ข.2 ตัวอย่างข้อคำถามที่ใช้ในการทดลอง 86
ตารางที่ ค.1 ตัวอย่างผลการทดลองของแต่ละข้อคำถามที่ใช้ 93
ตารางที่ ง.1 โครงสร้างข้อมูลของตาราง spProperties 96
ตารางที่ ง.2 โครงสร้างข้อมูลของตาราง SpCategories 96
ตารางที่ ง.3 โครงสร้างข้อมูลของตาราง securityPatterns 96
ตารางที่ ง.4 โครงสร้างข้อมูลของตาราง spDetails 97
ตารางที่ ง.5 โครงสร้างข้อมูลของตาราง spRelationships 97
ตารางที่ ง.6 โครงสร้างข้อมูลของตาราง spStructures 97
ตารางที่ ง.7 โครงสร้างข้อมูลของตาราง sdStructures 97
ตารางที่ ง.8 โครงสร้างข้อมูลของตาราง sdDetails 98
ตารางที่ ง.9 โครงสร้างข้อมูลของตาราง spPropRelationships 98
ตารางที่ ง.10 โครงสร้างข้อมูลของตาราง Term 98
ตารางที่ ง.11 โครงสร้างข้อมูลของตาราง spInvertedfile 99
ตารางที่ ง.12 โครงสร้างข้อมูลของตาราง sdInvertedfile 99
ตารางที่ ง.13 โครงสร้างข้อมูลของตาราง sdInvertedfile 99
ตารางที่ ง.14 โครงสร้างข้อมูลของตาราง role 99

สารบัญรูป

หน้า

รูปที่ 2.1 ภาพรวมของระบบค้นคืนสารสนเทศ 12
รูปที่ 2.2 การจัดทำดัชนีเอกสาร 13
รูปที่ 3.1 ขั้นตอนการทำวิจัย 19
รูปที่ 3.2 แผนภาพกิจกรรมของการจัดเก็บและค้นคืนส่วนของเอกสาร 22
รูปที่ 3.3 ตัวอย่างส่วนประกอบมาตรฐานความมั่นคงที่จัดเก็บ (ส่วนบทนำ) 24
รูปที่ 3.4 ตัวอย่างส่วนประกอบมาตรฐานความมั่นคงที่จัดเก็บ (ส่วนข้อกำหนดนโยบาย) 25
รูปที่ 3.5 ตัวอย่างโครงสร้างแบบรูปความมั่นคงที่จัดเก็บ 26
รูปที่ 3.6 แผนภาพกิจกรรมการจัดเก็บเอกสารเพื่อทำดัชนีและค่าน้ำหนัก 27
รูปที่ 3.7 แผนภาพกิจกรรมการจัดเก็บแบบรูปความมั่นคงเพื่อทำดัชนีและค่าน้ำหนัก 27
รูปที่ 3.8 ตารางน้ำหนักระหว่างส่วนของเอกสารกับดัชนีตามแบบจำลองปริภูมิเวคเตอร์ 28
รูปที่ 3.9 ตัวอย่างโครงสร้างข้อมูลความมั่นคงสารสนเทศ 31
รูปที่ 3.10 ตัวอย่างการสร้างข้อคำถามใหม่กรณีผู้ใช้เลือกโหนด “Enterprise Security and Risk Management” 32
รูปที่ 3.11 ตัวอย่างข้อคำถามใหม่ที่เกี่ยวเนื่องกับข้อคำถามที่เลือกโดยพิจารณาความสัมพันธ์ระหว่างแบบรูปความมั่นคง 33
รูปที่ 3.12 ตัวอย่างผลลัพธ์ที่ได้จากการค้นคืนส่วนเอกสารมาตรฐานความมั่นคง 38
รูปที่ 3.13 ตัวอย่างผลลัพธ์ที่ได้จากการค้นคืนแบบรูปความมั่นคง 38
รูปที่ 3.14 แผนภาพกิจกรรมการประเมินประสิทธิผลของระบบ 39
รูปที่ 4.1 ยูสเคสของระบบ 41
รูปที่ 4.2 แผนภาพดีพลอยเมนต์ของระบบ 43
รูปที่ 4.3 คลาสของข้อมูลที่จัดเก็บ 45
รูปที่ 4.4 เมนูหลักของเครื่องมือต้นแบบ 47
รูปที่ 4.5 ส่วนการจัดเก็บแบบรูปความมั่นคง 48
รูปที่ 4.6 ส่วนต่อประสานสำหรับค้นคืนส่วนเอกสารมาตรฐานโดยใช้คำสำคัญ 49
รูปที่ 4.7 ส่วนต่อประสานสำหรับการค้นคืนส่วนเอกสารมาตรฐานโดยใช้แบบรูปความมั่นคง 50
รูปที่ 4.8 ตัวอย่างผลลัพธ์ส่วนของเอกสารมาตรฐานความมั่นคงที่เกี่ยวข้อง 51
รูปที่ 5.1 แผนภาพกิจกรรมขั้นตอนการทดลอง 58
รูปที่ 5.2 แผนภาพกิจกรรมการทดลองสำหรับค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง

หน้า

สารสนเทศ 61

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

การกำหนดนโยบายด้านความมั่นคงสารสนเทศ (Information Security Policy Establishment) เป็นการกำหนดกฎหมายและระเบียบปฏิบัติเพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคง และเชื่อถือได้ โดยเลือกใช้ มาตรฐาน แนวทางปฏิบัติ หรือกรอบปฏิบัติที่เกี่ยวข้องเข้ามาช่วยลดความเสี่ยงต่อความเสียหายต่อข้อมูลสารสนเทศขององค์กร รวมทั้งเสริมสร้างและยกระดับความมั่นคงให้องค์กรมากขึ้นด้วย

ในปัจจุบันมาตรฐานไอเอสโอ/ไออีซี 27002 เป็นมาตรฐานหนึ่งที่ได้รับความนิยมในการนำมาช่วยในการกำหนดนโยบายความมั่นคงสารสนเทศ ซึ่งรวบรวมระเบียบปฏิบัติ ด้านการรักษาความมั่นคงสารสนเทศไว้โดยแยกเป็นมาตรการความมั่นคงปลอดภัย จำนวน 133 ข้อ โดยมีเนื้อหาระบุถึงข้อควรปฏิบัติในการควบคุมความมั่นคงของข้อมูลที่องค์กรควรนำไปใช้

อย่างไรก็ตามในแต่ละองค์กรหรือโครงการอาจมีการกำหนดนโยบายความมั่นคงที่มีความหลากหลายในสถานการณ์ที่แตกต่างกัน จึงเป็นผลให้ต้องมีการเลือกบริบทให้เหมาะสมในการประยุกต์ใช้มาตรฐานและแนวปฏิบัติที่ดี ทางผู้วิจัยได้เล็งเห็นถึงปัญหา เรื่องความรู้และประสบการณ์ด้านการกำหนดนโยบายและความมั่นคงสารสนเทศของผู้ต้องการศึกษาเอกสารมาตรฐานเพื่อช่วยในการกำหนดนโยบายความมั่นคงสารสนเทศ อาจจะทำให้เกิดการละเลยปัญหาบางรายการ ทำให้นโยบายความมั่นคงสารสนเทศที่กำหนดขึ้นมาไม่ครบถ้วนหรือไม่ชัดเจน ทำให้เกิดความเสี่ยงต่อข้อมูลสารสนเทศที่สำคัญภายในองค์กร รวมทั้งการใช้เวลาในการศึกษานาน เพื่อแก้ไขปัญหานี้จำเป็นที่จะต้องมีการบริหารจัดการในการจัดเก็บและค้นหามาตรฐานความมั่นคงสารสนเทศที่ได้จากกระบวนการพัฒนาซอฟต์แวร์อย่างเป็นระบบ จึงได้นำการจัดเก็บและค้นคืนสารสนเทศ (Information Storage and Retrieval) มาประยุกต์ใช้กับการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ จึงทำให้สามารถทำการระบุหรือค้นหาคำตอบได้จากระบบจัดการฐานข้อมูลได้เพียงระบุสิ่งที่ต้องการลงในโครงสร้างที่ต้องการ โดยในงานวิจัยนี้ ได้นำเอาแบบรูปความมั่นคง (Security

Pattern) [1] มาช่วยในการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ เพื่อแก้ไขปัญหาความหลากหลายของประสบการณ์ของผู้ต้องการกำหนดนโยบาย เพราะแบบรูปความมั่นคงนั้นได้ผ่านการวิเคราะห์ และตรวจสอบโดยผู้เชี่ยวชาญ โดยมีจุดประสงค์เพื่อแก้ไขปัญหาด้านความมั่นคงที่เคยปรากฏมาแล้ว ทำให้การพัฒนาซอฟต์แวร์โดยใช้แบบรูปความมั่นคง มีความถูกต้องครอบคลุมปัญหา และมีความรวดเร็วในการพัฒนา โดยเฉพาะอย่างยิ่งระบบความมั่นคงที่เคร่งครัดในเรื่องการป้องกัน (Prevention) การตรวจหา (Detection) และการกู้คืน (Recovery) [1]

งานวิจัยนี้เสนอวิธีการและพัฒนาเครื่องมือสนับสนุนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศที่สอดคล้องกับแบบรูปความมั่นคงของ M. Schumarker และคณะ [1] โดยเริ่มจากกระบวนการสร้างโครงสร้างข้อมูลความมั่นคงสารสนเทศ (Information Security Structure) ซึ่งเป็นแผนภาพต้นไม้ที่แสดงความสัมพันธ์จากแบบรูปความมั่นคง เพื่อนำมาใช้ช่วยให้การค้นคืนมีประสิทธิผลเพิ่มมากขึ้น โดยเสนอใช้วิธีการค้นคืน สำหรับผู้ค้นคืนที่มีประสบการณ์ มีความเชี่ยวชาญด้านความมั่นคงปลอดภัย สามารถค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้คำสำคัญ โดยใช้ภาษาธรรมชาติ เนื่องจากผู้ใช้กลุ่มนี้มีความชำนาญและความรู้เรื่องคำศัพท์ที่เกี่ยวข้องอยู่แล้ว สำหรับผู้ค้นคืนที่ไม่มีประสบการณ์ด้านความมั่นคงสารสนเทศมากนักสามารถค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลสารสนเทศ (Information Security Structure) ที่สร้างขึ้นเป็นแผนภาพต้นไม้ที่แสดงความสัมพันธ์จากคุณลักษณะด้านความมั่นคง กลุ่มแบบรูปความมั่นคง แบบรูปความมั่นคง และคำสำคัญของแต่ละแบบรูปความมั่นคง ซึ่งจะช่วยเพิ่มประสิทธิผลในการค้นคืนและลดระยะห่างของประสบการณ์ของผู้ต้องการกำหนดนโยบายให้น้อยลงไป ทั้งนี้มีการนำส่วนของความสัมพันธ์ระหว่างแบบรูปที่ระบุไว้ในงานวิจัย [5] มาช่วยในการขยายข้อคำถาม เพื่อให้ผลลัพธ์ที่ได้ครอบคลุมมากยิ่งขึ้น ในงานวิจัยนี้ใช้การเปรียบเทียบความคล้ายคลึงของข้อคำถามกับส่วนของเอกสารใช้เทคนิคปริภูมิเวคเตอร์ (Vector Space Model) และประเมินการสืบค้น ด้วยค่าระลึก (Recall) ค่าความแม่นยำ (Precision) และค่ามัชฌิมฮาร์โมนิก (Harmonic mean)

1.2 วัตถุประสงค์ของการวิจัย

1) เสนอวิธีการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ โดยใช้โครงสร้างข้อมูลสารสนเทศ ที่สร้างจากแบบรูปความมั่นคง

2) ออกแบบและพัฒนาเครื่องมือสนับสนุนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ โดยใช้โครงสร้างข้อมูลสารสนเทศ ซึ่งสร้างจากแบบรูปความมั่นคง รวมถึงการประเมินประสิทธิผลของผลลัพธ์ได้จากเครื่องมือ

1.3 ขอบเขตของการวิจัย

1) ออกแบบและพัฒนาระบบสนับสนุนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลสารสนเทศ ตามที่นำเสนอโดย M. Schumacher และคณะ [1] ผู้วิจัยได้ออกแบบแบบรูปความมั่นคงออกเป็น 4 กลุ่ม โดยมีแบบรูปรวมทั้งสิ้น 20 แบบรูป ดังภาคผนวก ก ตาราง ก.1

2) เอกสารมาตรฐานความมั่นคงและแบบรูปความมั่นคงที่ใช้ในการวิจัยมีเนื้อหาเป็นข้อความภาษาอังกฤษเท่านั้น

3) ผู้ใช้งานสามารถระบุข้อคำถามเป็นภาษาอังกฤษเท่านั้น

4) เอกสารที่นำมาค้นคืนเป็นเอกสารมาตรฐาน ไอเอสโอ/ไออีซี 27002

1.4 ขั้นตอนการวิจัย

1) ศึกษา วิเคราะห์แบบรูปความมั่นคง ตลอดจนหาความสัมพันธ์ระหว่างแบบรูปความมั่นคง

2) วิเคราะห์และออกแบบการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานด้านความมั่นคงสารสนเทศโดยใช้แบบรูปความมั่นคง

3) พัฒนาระบบต้นแบบ

4) ทดสอบเครื่องมือต้นแบบและประเมินผลการค้นคืน

5) สรุปผลการวิจัยและจัดทำรายงานวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) ได้ความสัมพันธ์ระหว่างแบบรูปความมั่นคงของทั้งหมด 20 แบบรูป ที่นำเสนอโดย M.Schumacher และคณะ [1] เพื่อนำไปเป็นส่วนหนึ่งในการขยายข้อคำถามเพื่อเพิ่มประสิทธิผลในการค้นคืน

2) ได้กระบวนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ ตั้งแต่ขั้นตอนการวิเคราะห์ออกแบบ จนถึงการประเมินวิธีการค้นคืน

3) ได้เครื่องมือต้นแบบสำหรับการจัดเก็บและค้นคืนเพื่อเป็นตัวช่วยในการกำหนดนโยบายด้านความมั่นคงสารสนเทศ และลดเวลาในการศึกษาข้อมาตรฐานที่ตรงตามความต้องการของผู้ใช้

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎี

งานวิจัยนี้ได้ประยุกต์ใช้เทคนิคการค้นคืนสารสนเทศมาช่วยในการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ โดยพิจารณาจากแบบรูปความมั่นคง เพื่อเป็นเครื่องมือสนับสนุนในการกำหนดนโยบายความมั่นคงสารสนเทศ ผู้วิจัยได้ศึกษาทฤษฎีที่เกี่ยวข้องในงานวิจัย ดังนี้ นโยบายความมั่นคงสารสนเทศ แบบรูปความมั่นคง และการจัดเก็บและค้นคืนสารสนเทศ มีรายละเอียดดังต่อไปนี้

2.1.1 นโยบายความมั่นคงสารสนเทศ (Information Security Policy)

นโยบายความมั่นคงสารสนเทศมีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงสำหรับสารสนเทศภายในองค์กร เพื่อให้สอดคล้องและเป็นไปตามข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

ผู้บริหารองค์กรต้องจัดทำเอกสารนโยบายความมั่นคง (Information Security Policy Document) ขององค์กรอย่างเป็นลายลักษณ์อักษร โดยที่เอกสารนโยบายนี้ต้องได้รับการอนุมัติจากผู้บริหารองค์กรก่อนนำไปใช้งาน และต้องเผยแพร่ให้พนักงานภายในองค์กรและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้อง ได้รับทราบ แต่ในแง่ความมั่นคงนั้นถึงแม้จะมีการจัดทำนโยบายความมั่นคงที่เป็นลายลักษณ์อักษร แต่ก็ไม่ได้เป็นไปตามมาตรฐาน นอกจากนั้นยังไม่ได้มีการนำไปปฏิบัติอย่างเป็นระบบ

คุณสมบัติพื้นฐานของความมั่นคงสารสนเทศ ตามแนวคิดกลุ่มอุตสาหกรรมความมั่นคงของคอมพิวเตอร์ หรือที่เรียกว่าแบบรูป ซี.ไอ.เอ (C.I.A Model) [3] มี สามคุณสมบัติ คือ

1) ความลับของข้อมูล (Confidentiality) คือการที่ผู้ที่จะเข้าถึงสารสนเทศเฉพาะอย่างได้ก็ต่อเมื่อได้รับสิทธิ์ที่เพียงพอเท่านั้น อาจมีการใช้มาตรการต่าง ๆ หลายประการ ตัวอย่างเช่น แบ่งหมวดหมู่สารสนเทศ การเก็บเอกสารอย่างปลอดภัย หรือการใช้นโยบายความมั่นคงทั่วไป เป็นต้น

2) บูรณภาพ (Integrity) คือการป้องกันความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล และวิธีการประมวลผล ต้องการควบคุมความผิดพลาดไม่ให้ผู้มีไม่มีสิทธิ์ แก้ไข หรือเปลี่ยนแปลง

3) สภาพพร้อมใช้งานของข้อมูล (Availability) คือให้บุคคลผู้มีสิทธิ์เท่านั้นเข้าถึงข้อมูลได้ทุกเมื่อที่ต้องการ ต้องมีการควบคุมไม่ให้ ระบบล้มเหลว มีสมรรถภาพทำงานอย่างต่อเนื่อง และป้องกันไม่ให้ผู้ไม่มีสิทธิ์มาทำให้ระบบหยุดการทำงาน

โดยองค์ประกอบที่เพิ่มเติมเข้ามา 5 คุณสมบัติ คือ

(1) ความเป็นส่วนตัว (Privacy) คือสารสนเทศที่ถูกเก็บรวบรวม ใช้ และบันทึกโดยองค์กรจะถูกใช้เฉพาะในวัตถุประสงค์ที่เจ้าของข้อมูลทราบในตอนที่ข้อมูลถูกรวบรวมเท่านั้น

(2) การแสดงตัว (Identification) คือการระบุถึงตัวผู้เข้าระบบตั้งแต่ในตอนแรกที่เข้ามาใช้งาน

(3) การพิสูจน์ตัวจริง (Authentication) คือการพิสูจน์ตัวตน จะเกิดเมื่อการควบคุมจัดให้มีการพิสูจน์ว่าผู้ใช้มีเอกลักษณ์ตามที่กำหนด

(4) การอนุญาต (Authorization) คือหลังจากการที่เอกลักษณ์ของผู้ใช้ได้รับการพิสูจน์ จะมีกระบวนการอนุญาตที่ทำให้แน่ใจได้ว่าผู้ใช้ (บุคคล หรือคอมพิวเตอร์) ได้รับอนุญาตที่ถูกต้อง เพื่อให้เข้าถึง ปรับปรุงแก้ไข หรือลบเนื้อหาของสินทรัพย์สารสนเทศ

(5) ความรับผิดชอบ (Accountability) คือเป็นคุณสมบัติที่เกี่ยวกับการที่สามารถระบุถึงผู้ที่กระทำต่อสินทรัพย์ขององค์กรได้ว่าใครเป็นผู้กระทำ

การที่จะจัดทำนโยบายความมั่นคงของข้อมูลขึ้นมาสำหรับองค์กรใด ๆ นั้น ไม่ใช่แค่การนำคำแนะนำต่าง ๆ จากมาตรฐาน หรือเอกสารที่สามารถหาได้ทั่วไปมาใช้แล้วจะประสบผลสำเร็จ เนื่องจากในแต่ละองค์กรก็มีรูปแบบการดำเนินงานและวัฒนธรรมองค์กรที่แตกต่างกันไป ดังนั้นในแต่ละองค์กรจำเป็นต้องมีกระบวนการในการออกแบบ และพัฒนานโยบายความมั่นคงที่สอดคล้องกับรูปแบบการดำเนินธุรกิจ และความต้องการขององค์กรนั้น ๆ

ในงานวิจัยนี้ ออกแบบเครื่องมือเพื่อค้นคืนส่วนเอกสารมาตรฐานด้านความมั่นคงสารสนเทศที่มีความคล้ายคลึงกับส่วนเอกสารมาตรฐานด้านความมั่นคงที่ผู้ใช้ต้องการศึกษา เพื่อช่วยในการกำหนดนโยบายความมั่นคงสารสนเทศได้ครอบคลุมและรวดเร็วขึ้น

2.1.2 เอกสารมาตรฐาน ไอเอสโอ/ไออีซี 27002:2005

ไอเอสโอ/ไออีซี 27002 [4] เป็นมาตรฐานการจัดการข้อมูลที่สำคัญเพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่อง กำหนดขึ้นโดยองค์กร ISO (The International Organization for Standardization) และ IEC (The International Electrotechnical Commission) มาตรฐานนี้เป็นมาตรฐานสากลที่มุ่งเน้นด้านรักษาความมั่นคงให้กับระบบสารสนเทศขององค์กร และใช้เป็นมาตรฐานอ้างอิงเพื่อใช้เป็นแนวทางในการเสริมสร้างความมั่นคงให้กับระบบสารสนเทศของ โดยที่ ISO 27002:2005 – Code of practice for information security management มีเนื้อหาระบุถึงข้อควรปฏิบัติในการควบคุมความมั่นคงของข้อมูลที่องค์กรควรนำไปใช้ ซึ่งจะมีทั้งหมด 133 หัวข้อ แบ่งออกเป็น 11 หมวดหลักดังรายละเอียดต่อไปนี้

1) Security Policy ครอบคลุมเรื่องนโยบายการจัดการความมั่นคงของข้อมูลในองค์กร การเล็งเห็นถึงความสำคัญของนโยบายฯ และการให้การสนับสนุนจากผู้บริหารระดับสูงเพื่อสนับสนุนให้มีการนำนโยบายฯ ไปใช้อย่างมีประสิทธิภาพ

2) Organizational of Information Security ครอบคลุมเรื่องการจัดตั้งหน่วยงานขึ้นเพื่อประสานงานและดำเนินงานด้านการดูแลรักษาความมั่นคงของข้อมูล ตลอดจนการบริหารจัดการด้านความมั่นคงของข้อมูลภายในองค์กร การติดต่อประสานงานทั้งภายในและภายนอกองค์กร

3) Asset Management ครอบคลุมเรื่องการจัดทำทะเบียนทรัพย์สิน การจัดจำแนกประเภทของข้อมูลตามระดับความสำคัญ การควบคุมการเข้าถึงข้อมูลแต่ละประเภท และการควบคุมทรัพย์สินด้านสารสนเทศขององค์กร

4) Human Resources Security ครอบคลุมเรื่องการบริหารจัดการความมั่นคงในส่วนที่เกี่ยวข้องกับพนักงาน และผู้วิจัย ตั้งแต่เริ่มรับพนักงานใหม่ จวบจนสิ้นสุดสถานภาพการเป็นพนักงาน ซึ่งครอบคลุมประเด็นที่สำคัญต่าง ๆ อาทิเช่น การให้ความรู้ด้านความมั่นคงแก่พนักงาน การให้พนักงานลงนามในข้อตกลงไม่เปิดเผยข้อมูล เป็นต้น

5) Physical and Environmental Security ครอบคลุมเรื่องการรักษาความมั่นคงของสถานที่ทำงาน ได้แก่ การควบคุมการเข้า-ออกของบุคคล และทรัพย์สิน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและป้องกันการเสียหายหรือสูญหายของทรัพย์สิน

6) Communications and Operations Management ครอบคลุมเรื่องการรักษาความมั่นคงให้แก่คอมพิวเตอร์ ระบบเครือข่าย และการประมวลผลข้อมูล เช่น การป้องกันไวรัสคอมพิวเตอร์ การ

สำรองข้อมูล การควบคุมความมั่นคงของระบบเครือข่าย การกำจัดสื่อบันทึกข้อมูล การควบคุมความมั่นคงในการใช้งานอีเมล เป็นต้น

7) Access Control ครอบคลุมเรื่องการควบคุมการเข้าถึงข้อมูล และการป้องกันการเข้าถึงข้อมูลโดยผู้ไม่ได้รับอนุญาตทั้งจากการเข้าใช้งานภายในองค์กร และการเข้าถึงระบบจากระยะไกล (Remote Access)

8) Information Systems Acquisition, Development and Maintenance ครอบคลุมเรื่องการจัดซื้อ-จัดหา พัฒนา ติดตั้ง และบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย ซอฟต์แวร์ ฮาร์ดแวร์ และอุปกรณ์สารสนเทศต่าง ๆ เพื่อให้อุปกรณ์เหล่านั้นมีความมั่นคงและทำงานได้อย่างมีประสิทธิภาพ

9) Information Security Incident Management ครอบคลุมเรื่องการรายงาน และการบริหารจัดการเหตุละเมิดความมั่นคงของข้อมูล เพื่อให้เหตุดังกล่าวได้รับการแก้ไขอย่างทันท่วงที และป้องกันไม่ให้เกิดเหตุซ้ำขึ้นอีกในอนาคต

10) Business Continuity Management ครอบคลุมเรื่องการจัดทำ และทดสอบแผนความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Plan หรือ BCP) ซึ่งก็คือวิธีการปฏิบัติเพื่อรับมือสำหรับกรณีที่เกิดความผิดพลาดขึ้นกับระบบสารสนเทศ หรือความผิดพลาดที่เกิดจากภัยธรรมชาติ เพื่อให้เกิดความเสียหายน้อยที่สุดและเพื่อให้ธุรกิจสามารถฟื้นตัวกลับมาดำเนินงานตามปกติได้เร็วที่สุด

11) Compliance ครอบคลุมการปฏิบัติงานที่ถูกต้องตามกฎหมาย หรือข้อตกลงต่าง ๆ ที่องค์กรได้กระทำร่วมกับผู้อื่น เช่น การใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ (License) ถูกต้อง การปกป้องข้อมูลส่วนบุคคล เป็นต้น

2.1.3 แบบรูปความมั่นคง (Security Pattern)

แบบรูปความมั่นคง คือแบบแผนหรือแนวทางที่ใช้ในการแก้ปัญหาที่มักเกิดขึ้นเสมอในการออกแบบพัฒนาระบบ แก้ไขปัญหาด้านความมั่นคงซึ่งปรากฏซ้ำ ๆ โดยแต่ละแบบรูปใช้คุณสมบัติทางด้านความมั่นคง 4 คุณสมบัติ ได้แก่ ความเป็นความลับ บูรณภาพ ความรับผิดชอบ และสภาพพร้อมใช้งาน โดยมีรายละเอียดดังต่อไปนี้

1) ความเป็นความลับ (Confidentiality) คือคุณสมบัติที่เกี่ยวกับการเปิดเผยความลับเพียงบุคคลหรือหน่วยงานที่ได้รับอนุญาตโดยองค์กร

2) บูรณภาพ (Integrity) คือคุณสมบัติที่เกี่ยวกับการที่สินทรัพย์ขององค์กรจะไม่โดนเปลี่ยนแปลงแก้ไขไปจากที่องค์กรต้องการ

3) ความรับผิดชอบ (Accountability) คือคุณสมบัติที่เกี่ยวกับการที่สามารถระบุถึงผู้ที่กระทำต่อสินทรัพย์ขององค์กร

4) สภาพพร้อมใช้งาน (Availability) คือคุณสมบัติที่เกี่ยวกับการที่สินทรัพย์ขององค์กรที่อยู่ในกระบวนการทางธุรกิจต้องสามารถเข้าถึงได้

ในงานวิจัยของ M. Schumacher และคณะ [1] ได้นำเสนอแบบรูปความมั่นคงการบูรณาการความมั่นคงและวิศวกรรมระบบ (Security Patterns: Integrating Security and Systems Engineering) โดยแบบรูปที่สร้างขึ้นนั้นสามารถ โดยแบ่งออกเป็น 8 กลุ่มรวมทั้งสิ้น 46 แบบรูป รายการกลุ่มของแบบรูปความมั่นคงมีรายละเอียด ดังนี้

1) กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management Patterns)

2) กลุ่มแบบรูปการระบุตัวตนและการพิสูจน์ตัวจริง (Identification & Authentication (I&A) Patterns)

3) กลุ่มแบบรูปแบบจำลองควบคุมการเข้าถึง (Access Control Model Patterns)

4) กลุ่มแบบรูปสถาปัตยกรรมการควบคุมการเข้าถึงระบบ (System Access Control Architecture Patterns)

5) กลุ่มแบบรูปการควบคุมการเข้าถึงระบบการทำงาน (Operating System Access Control Patterns)

6) กลุ่มแบบรูปการตรวจสอบ (Accounting Patterns)

7) กลุ่มแบบรูปสถาปัตยกรรมไฟร์วอลล์ (Firewall Architecture Patterns)

8) กลุ่มแบบรูปความปลอดภัยในการใช้อินเทอร์เน็ต (Secure Internet Applications Patterns)

ผู้วิจัยได้นำแบบรูปที่ได้อ้างอิงมาจากงานวิจัย [5] มาประยุกต์ใช้ในการวิจัยรวมทั้งสิ้น 4 กลุ่ม จำนวน 20 แบบรูปได้แก่ กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง กลุ่มแบบรูปการระบุตัวตนและการพิสูจน์ตัวจริง กลุ่มแบบรูปแบบจำลองควบคุมการเข้าถึง และกลุ่มแบบรูปสถาปัตยกรรมไฟร์วอลล์ โดยมีโครงสร้างของแบบรูปความมั่งคงของ M. Schumacher และคณะ [1] ดังที่กล่าวไว้ดังนี้

ตารางที่ 2.1 รายละเอียดโครงสร้างแบบรูปความมั่นคงของ M. Schumacher และคณะ [5]

ส่วนประกอบ	รายละเอียดของส่วนประกอบ
ชื่อ (Name)	ชื่อของแบบรูปความมั่นคง
ชื่อเรียกอื่นของแบบรูป (Also Known As)	ชื่อแบบรูปที่รู้จักทั่วไป หรือปรากฏในรู้คำอื่นที่มีความหมายเดียวกัน
ตัวอย่าง (Example)	ตัวอย่างของปัญหาที่มีการนำแบบรูปความมั่นคงแบบรูปไปใช้
บริบท (Context)	กล่าวถึงสถานการณ์ที่ควรนำแบบรูปความมั่นคงดังกล่าวไปใช้
ผลเฉลย (Solution)	ผลเฉลยภายใต้แบบรูปความมั่นคง
โครงสร้าง (Structure)	อธิบายรายละเอียดโครงสร้างของแบบรูปความมั่นคง
ไดนามิก (Dynamics)	อธิบายเหตุการณ์ของพฤติกรรมขณะการใช้งานของแบบรูปความมั่นคง
การทำให้เกิดผล (Implementation)	ตัวชี้นำการใช้งานแบบรูปความมั่นคงโดยไม่ได้บังคับให้ทำตามทั้งหมด
ตัวอย่างการแก้ไข (Example Resolved)	ตัวอย่างการแก้ไขปัญหาด้วยแบบรูปความมั่นคง
ส่วนแปรผัน (Variants)	คำอธิบายถึงส่วนที่แตกต่างหรือรายละเอียดพิเศษของแบบรูป
การนำไปใช้ที่ทราบ (Known Uses)	ตัวอย่างการนำไปใช้ของแบบรูปความมั่นคงในระบบที่ใช้งานจริง
ผลที่ได้ (Consequence)	ประโยชน์ที่ได้รับและผลเสียที่เป็นไปได้ของแบบรูป
เห็นได้จาก (See Also)	ทำการอ้างถึงแบบรูปความมั่นคงอื่นที่แก้ไขปัญหาเดียวกัน

2.1.4 การจัดเก็บและค้นคืนสารสนเทศ (Information Retrieval and Storage)

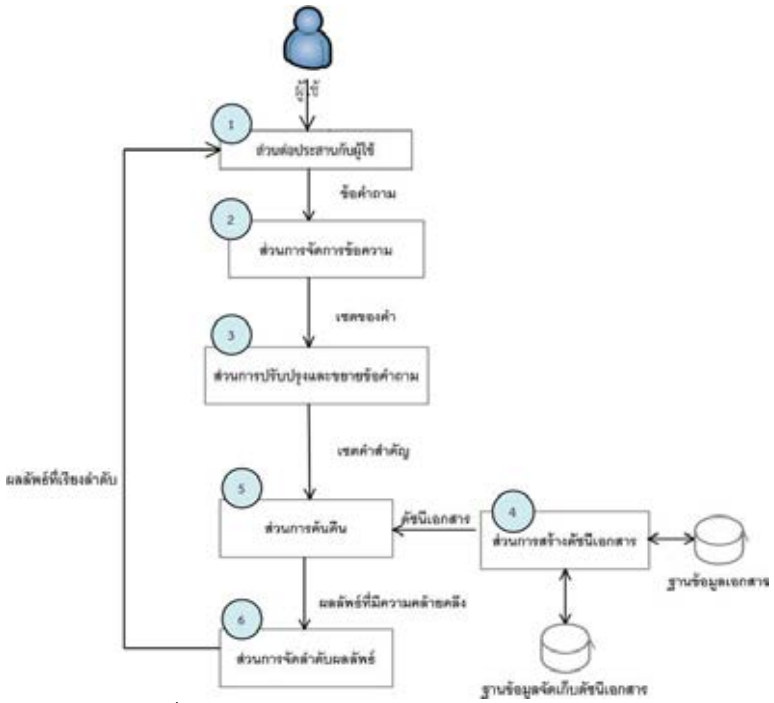
การค้นคืนสารสนเทศ [6] คือกระบวนการในการค้นคืนสารสนเทศที่ได้มีการจัดเก็บอยู่ในแหล่งเก็บ เพื่อให้ได้สารสนเทศที่ตรงกับความต้องการของผู้ใช้มากที่สุด โดยแบบจำลองหลักของการค้นคืนสารสนเทศ มีทั้งหมด 3 แบบจำลองหลัก ดังนี้

1) แบบจำลองเชิงตรรกะ (Boolean Model) เป็นตัวแบบจะทำการเทียบคำที่ปรากฏในเอกสารเพียงว่าปรากฏหรือไม่ปรากฏเท่านั้น โดยมีการใช้ตัวดำเนินการ และ (and) หรือ (or) ไม่ (not) ในการเทียบคำในเอกสาร

2) แบบจำลองปริภูมิเวคเตอร์ (Vector Space Model) เป็นตัวแบบที่พัฒนาต่อจากแบบจำลองเชิงตรรกะ โดยมีการจัดทำการใช้งานความถี่ที่ปรากฏในเอกสาร และค่าน้ำหนักในการคำนวณ จึงได้ค่าที่หลากหลายกว่าการทำการเทียบดูเพียงแค่ว่ามีหรือไม่มีดังแบบจำลองเชิงตรรกะ ซึ่งผลลัพธ์จะเป็นการค้นคืนที่เรียงลำดับตามความคล้ายคลึง

3) แบบจำลองความน่าจะเป็น (Probabilistic Model) เป็นตัวแบบที่นำค่าสถิติการเกิดของคำและลำดับของหน้าที่ของคำ เข้ามาช่วยในการคำนวณหาความน่าจะเป็น และคำที่มีโอกาสการเกิดมากที่สุด ข้อจำกัดของวิธีการนี้คือจะต้องมีฐานข้อมูลที่มีการตัดคำที่ถูกต้อง และกำหนดหน้าที่ของคำเพื่อที่จะได้นำไปใช้ในการสร้างสถิติ

จากการวิเคราะห์ข้อดีข้อเสียของทั้งสามแบบจำลอง ผู้วิจัยเลือกใช้แบบจำลองปริภูมิเวคเตอร์เพื่อทำการค้นคืนเอกสาร



รูปที่ 2.1 ภาพรวมของระบบค้นคืนสารสนเทศ [6]

ระบบการค้นคืนสารสนเทศโดยทั่วไปมีกระบวนการ แสดงดังรูปที่ 2.1 โดยมีรายละเอียดดังนี้

1) ส่วนต่อประสานผู้ใช้ (User Interface) คือส่วนที่ติดต่อกับผู้ใช้งาน เป็นส่วนรับข้อมูลที่ผู้ใช้ต้องการเข้าสู่ระบบและแสดงผลลัพธ์ที่ได้ให้แก่ผู้ใช้ระบบ

2) ส่วนการจัดการข้อความ (Text Transformations) คือส่วนที่ดำเนินการกับข้อความหรือเอกสารซึ่งให้ได้มาซึ่งดัชนีของเอกสารนั้นๆ

3) ส่วนการปรับปรุงและขยายข้อคำถาม (Query Expansion and Modification) คือส่วนที่ดำเนินการกับข้อคำถาม ซึ่งให้ได้มาซึ่งดัชนีของข้อคำถาม และมีการขยายข้อคำถามด้วยตัวดำเนินการต่าง ๆ เช่น การหาคำที่มีความหมายเหมือนกับดัชนีที่ได้จากข้อคำถาม เป็นต้น

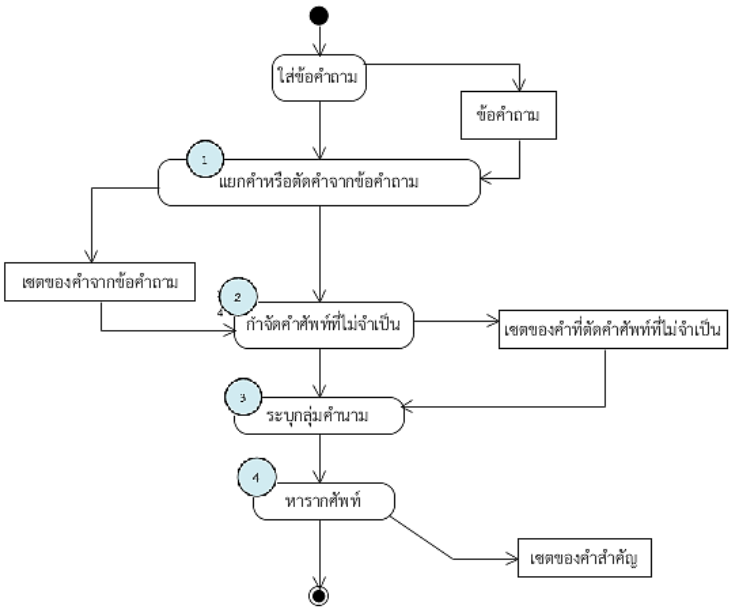
4) ส่วนการจัดทำดัชนีเอกสาร (Indexing) คือการจัดดัชนีของเอกสารที่ได้จากส่วนจัดการข้อความให้อยู่ในแบบรูปโครงสร้าง ในที่นี้ คือแฟ้มดัชนีผกผัน (Inverted File) [6] โดยองค์ประกอบของโครงสร้างแฟ้มผกผันมีทั้งสิ้น 2 องค์ประกอบได้แก่ กลุ่มคำศัพท์ (Vocabulary) กับเหตุการณ์ (Occurrences)

5) ส่วนการค้นคืน (Retrieval) คือส่วนการหาค่าความคล้ายคลึงระหว่างเอกสารและข้อคำถามที่รับเข้ามา

6) ส่วนการจัดลำดับผลลัพธ์ (Ranking) คือส่วนที่ทำหน้าที่เรียงลำดับค่าความคล้ายคลึงที่คำนวณได้จากขั้นตอนการค้นคืนเพื่อแสดงผลลัพธ์โดยเรียงจากมากไปน้อย

2.1.4.1 การจัดทำดัชนีในการจัดเก็บเอกสารและการคำนวณค่าน้ำหนักของดัชนีของเอกสาร

ดัชนี คือคำที่สามารถระบุถึงเอกสารที่เราต้องการที่จะทำการค้นคืน หากมีคำร้องขอเข้าสู่ระบบซึ่งในหนึ่งเอกสารจะมีหลายดัชนีในการระบุถึงโดยในการจัดทำดัชนีในการจัดเก็บเอกสารเป็นกระบวนการสำคัญที่มีผลต่อการค้นคืน เพราะหากทำการจัดทำดัชนีที่ไม่ตรงกับเอกสาร หรือหากให้น้ำหนักในคำที่ไม่สำคัญมากกว่าคำที่มีความสำคัญ (Keyword) จะทำให้ระบบการค้นคืนผิดพลาดหรือระบบอาจใช้การไม่ได้เลย โดยมีกระบวนการการจัดทำดัชนีดังรูปที่ 2.2



รูปที่ 2.2 การจัดทำดัชนีเอกสาร [6]

โดยเริ่มจากการนำเอกสารเข้ามา โดยหลังจากนั้นมีกระบวนการต่าง ๆ โดยอธิบายเรียงลำดับได้ดังนี้

1) ทำการแยกคำ ตัดคำจาก เอกสารหรือข้อความ เป็นขั้นตอนที่เริ่มจากการนำชุดข้อมูลหรือเอกสารที่ถูกจัดเก็บอยู่ในคลังมาทำการวิเคราะห์และแบ่งเป็นรายการของคำที่ปรากฏในแต่ละเอกสาร

2) การกำจัดละเว้น (Stopwords) โดยคำกลุ่มนี้มักเป็นคำที่สามารถพบได้บ่อย ๆ มีความถี่สูงๆ เช่น ‘a’, ‘am, ‘are’, ‘and’ เป็นต้น

3) การระบุกลุ่มคำนาม (Noun Groups) ได้แก่ คำนามคำเดียว (Single Noun) นามวลีสองคำใกล้กัน (Two Adjacent Nouns) หรือ สามคำใกล้กันเป็นต้น (Three Adjacent Nouns)

4) การหารากศัพท์ (Stemming) เป็นการทำหารากของคำศัพท์นั้นๆ เช่น ‘connecting’ จะถูกแปลงเป็น ‘connect’ เป็นต้น

โดยในงานวิจัยนี้ ได้ใช้การทำรากศัพท์โดยขั้นตอนวิธีการของพอร์ตเตอร์ (Porter’s Algorithm) [7]

การตัดคำเพื่อหารากศัพท์โดยใช้พอร์ตเตอร์อัลกอริทึม คือกระบวนการลดรูปคำสำคัญที่แตกต่างกันให้อยู่ในรูปของรากศัพท์ แต่การทำงานของพอร์ตเตอร์อัลกอริทึมไม่ได้พยายามหารากศัพท์ที่ถูกต้องของคำสำคัญนั้นๆ เพียงแต่พยายามสร้างรูปแบบของคำสำคัญให้มีลักษณะทั่วไป ที่เหมือนกันโดยการตัดส่วนที่ไม่เหมือนกันออกไป ตัวอย่างเช่น

CONNECT
CONNECTED
CONNECTING
CONNECTION
CONNECTIONS

จากตัวอย่างของกลุ่มคำสำคัญนี้ เมื่อทำการตัดคำด้วยพอร์ทเตอร์อัลกอริทึม ผลที่ได้คือ CONNECT ซึ่งเป็นลักษณะโดยทั่วไปของกลุ่มคำสำคัญกลุ่มนี้

เมื่อได้ดัชนีของเอกสารนั้นๆ แล้ว ใช้แบบจำลองปริภูมิเวคเตอร์ [8] เพื่อหาความคล้ายคลึง โดยเริ่มจากการหาความถี่ของการปรากฏของคำๆนั้นในแต่ละเอกสาร ค่าความถี่ที่ปรากฏในเอกสาร (Term Frequency) โดยใช้สมการ (1)

$$tf_{i.j} = \begin{cases} 1 + logf_{i.j} \;\; if \; f_{i.j} > 0 \\ 0 \;\; otherwise \end{cases} \quad (1)$$

โดยที่

$tf_{i.j}$ คือค่าความถี่ที่ได้จากการคำนวณของดัชนี i ที่ปรากฏในเอกสารที่ j

$f_{i.j}$ คือความถี่ที่ได้การนับดัชนี i ที่ปรากฏในเอกสารที่ j

หลังจากนั้นหาค่าความถี่ของเอกสารที่มีคำนั้นๆ ปรากฏอยู่ ด้วยสมการในการคำนวณค่าผกผันของความถี่ของเอกสาร (Inverse Document Frequency: idf) แสดงดังสมการ (2) ดังต่อไปนี้

$$idf_i = log\frac{N}{n_i} \tag{2}$$

โดยที่

idf_i คือค่าผกผันของความถี่ของเอกสารที่มีดัชนี i ปรากฏ

N คือจำนวนเอกสารทั้งหมดในระบบ

n_i คือจำนวนเอกสารทั้งหมดที่มีดัชนี i ปรากฏ

เมื่อได้ค่า จาก สมการที่ (1) และ (2) แล้ว นำมาหาค่าน้ำหนักของดัชนีแต่ละตัว แสดงดังสมการ (3) ดังต่อไปนี้

$$w_{i,j} = \begin{cases} \left(1 + logf_{i,j}\right) \times log\frac{N}{n_i} & if\ f_{i.j} > 0 \\ 0 & otherwise \end{cases} \tag{3}$$

โดยที่

$w_{i,j}$ คือน้ำหนักของดัชนี i นั้นในเอกสาร j

2.1.4.2 การหาค่าความคล้ายคลึงระหว่างเอกสารและข้อคำถามที่รับเข้ามา

การคำนวณค่าความคล้ายคลึงของข้อคำถามของผู้ใช้กับตัวเอกสารว่ามีความคล้ายคลึงกันเท่าใด หลักการในการคำนวณความคล้ายคลึงของแบบจำลองปริภูมิเวคเตอร์ ได้แก่ การวัดความคล้ายคลึงแบบโคไซน์ (Cosine Similarity) มาคำนวณค่าความคล้ายคลึงระหว่างตัวข้อคำถาม i กับเอกสารที่ j โดยใช้สมการ (4) ดังต่อไปนี้

$$sim(d_j, q) = \frac{\sum_{i=1}^{t} w_{i,j} \times w_{i,q}}{\sqrt{\sum_{i=1}^{t} w_{i,j}^2} \times \sqrt{\sum_{j=1}^{t} w_{i,q}^2}} \quad (4)$$

โดยที่

$sim(d_j, q)$	คือค่าความคล้ายคลึงระหว่างเอกสารที่ j กับคำถาม
$w_{i,j}$	คือค่าน้ำหนักของดัชนี i ในเอกสารที่ j
$w_{i,q}$	คือค่าน้ำหนักของดัชนี i ในคำถามที่ป้อนเข้าไป
t	คือจำนวนดัชนีที่ใช้ในการคำนวณ

2.1.4.3 การประเมินประสิทธิผลของการค้นคืน

การประเมินประสิทธิผลของกระบวนทำการค้นคืน สามารถทำการเปรียบเทียบโดยใช้ ค่าความแม่นยำ (Precision) กับ ค่าระลึก (Recall) และค่ามัชฌิมฮาร์โมนิก (Harmonic mean) โดยมีสมการดังต่อไปนี้ (5) -(7)

1) ค่าระลึก [6]

$$Recall = \frac{|R \cap A|}{|R|} \quad (5)$$

2) ค่าความแม่นยำ [6]

$$Precision = \frac{|R \cap A|}{|A|} \quad (6)$$

โดยที่

$\|R \cap A\|$	คือจำนวนเอกสารที่ตรงตามความต้องการของผู้ใช้
$\|R\|$	คือจำนวนเอกสารทั้งหมดที่ผู้เชี่ยวชาญเลือกที่ตรงกับข้อคำถาม
$\|A\|$	คือจำนวนเอกสารทั้งหมดที่ได้ถูกทำการค้นคืนขึ้นมาทั้งหมด

3) ค่ามัชฌิมฮาร์โมนิก [6]

$$F = \frac{2}{\frac{1}{r}+\frac{1}{P}} \quad (7)$$

โดยที่

F คือค่ามัชฌิมฮาร์โมนิก

r คือค่าระลึก

P คือค่าความแม่นยำของเอกสารลำดับที่ j

j คือลำดับของเอกสารที่ j

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

2.2.1 แบบรูปความมั่นคง (Security Pattern)

กวิน สุภาพร และคณะ ได้นำเสนอการกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง [5] โดย นำเสนอไวยากรณ์ของรูปแบบความมั่นคงที่ได้มาจากการวิเคราะห์แบบรูปความมั่นคง จากหนังสือแบบรูปความมั่นคงการบูรณาการความมั่นคงและวิศวกรรมระบบ (Security Patterns: Integrating Security and Systems Engineering) [1] ซึ่งครอบคลุมจำนวน 20 แบบรูป 4 กลุ่มแบบรูปความมั่นคง ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยงการระบุตัวตนและการพิสูจน์ตัวตน แบบจำลองควบคุมการเข้าถึง และสถาปัตยกรรมไฟล์วอลล์

สิ่งที่นำมาพิจารณาใช้จากงานวิจัยนี้ คือความสัมพันธ์ระหว่างแบบรูปความมั่นคงและเงื่อนไขการใช้แบบรูป เพื่อมาช่วยในการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ ที่มีความสัมพันธ์หรือเกี่ยวข้องกับความต้องการของผู้ใช้

Munawar Hafiz และคณะ ได้นำเสนองานวิจัย การบริหารจัดการแบบรูปความมั่นคง (Towards an Organization of Security Patterns) [9] โดยการแบ่งกลุ่มแบบรูปความมั่นคงในด้านต่าง ๆ เพื่อสะดวกต่อผู้ใช้นำไปใช้ให้ตรงกับด้านที่ผู้ใช้ต้องการ เช่น แบ่งกลุ่มตามโดเมน (Domain Concepts) คือความเป็นความลับ (Confidentiality) บูรณภาพ (Integrity) และ ความพร้อมใช้ (Availability) แบ่งตามบริบท (Context) และแบ่งตามโดเมนของปัญหา (Problem Domain) เป็นต้น

สิ่งที่นำมาพิจารณาใช้จากงานวิจัยนี้ คือแนวทางการแบ่งกลุ่มแบบรูปความมั่นคงตามขอบเขต เพื่อมาช่วยเพิ่มประสิทธิผลในการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง

2.2.2 การจัดเก็บและค้นคืนสารสนเทศ (Information Retrieval and Storage)

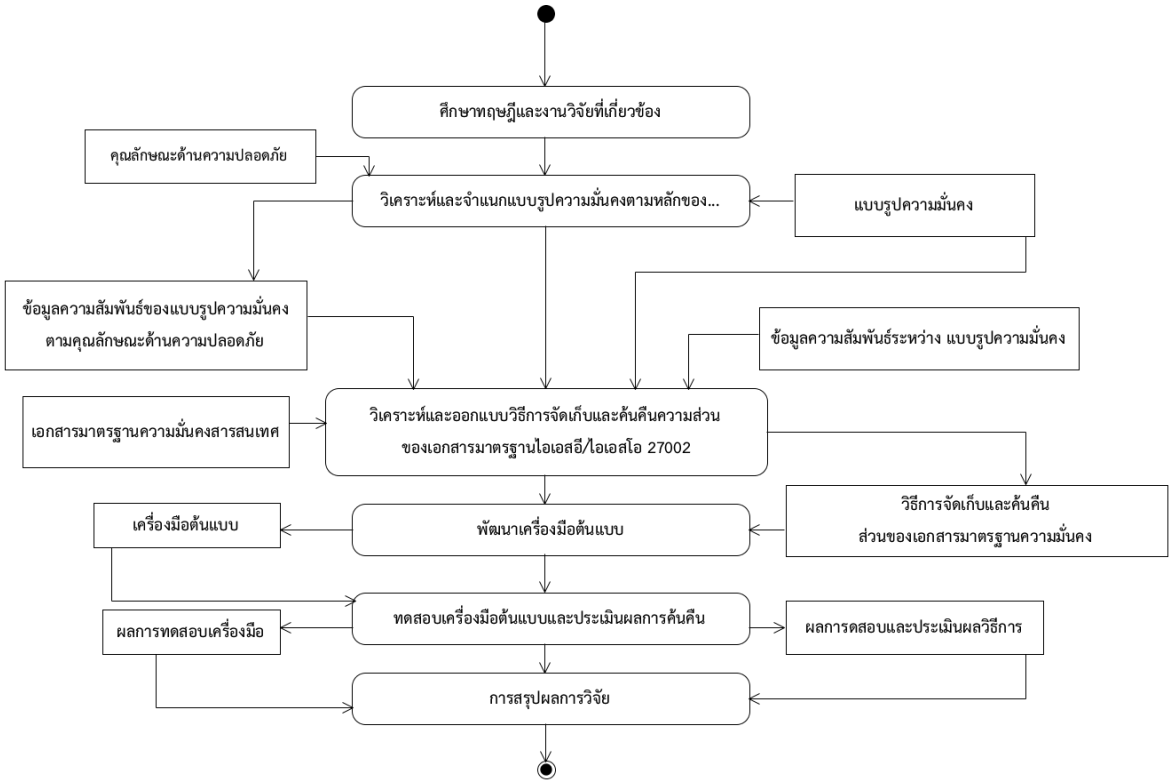
Andrea De Lucia และ คณะ ได้เสนองานวิจัย การกู้คืนเส้นเชื่อมเพื่อตามรอยในระบบจัดการสินทรัพย์ของซอฟต์แวร์โดยการใช้วิธีการทางการค้นคืนสารสนเทศ (Recovering Traceability Links in Software Artifact Management Systems using Information Retrieval Methods) [10] โดยการนำหลักการค้นคืนเข้ามาช่วยตามรอยของสินทรัพย์ที่มีอยู่ในระบบ โดยเปรียบเทียบความคล้ายคลึงระหว่างสินทรัพย์ที่ผู้ใช้กำหนดเพื่อนำมาแสดงผลโดยได้มีการพัฒนาระบบการจัดการสินทรัพย์ชื่อว่า “Advanced Artifact Management System: ADAMS”

สิ่งที่นำมาพิจารณาใช้จากงานวิจัยนี้ คือการนำแนวความคิดในการใช้การค้นคืนสารสนเทศมาช่วยในการค้นคืนเอกส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้แบบรูปความมั่นคง

บทที่ 3

การวิเคราะห์และออกแบบระบบ

งานวิจัยนี้ เสนอการออกแบบวิธีการและพัฒนาระบบต้นแบบสนับสนุนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลสารสนเทศ เพื่อช่วยในการค้นหาข้อกำหนดหรือแนวทางปฏิบัติในการจัดการดูแลความมั่นคงสารสนเทศที่มีความคล้ายคลึงกับความต้องการของผู้ใช้ โดยข้อกำหนดหรือแนวทางปฏิบัติที่ค้นคืนได้มานั้น สามารถระบุได้ว่ามาจากส่วนใดของเอกสารมาตรฐานความมั่นคงสารสนเทศ และเกี่ยวข้องกับแบบรูปความมั่นคงใด โดยในงานวิจัยนี้ได้ดำเนินการตามรูปที่ 3.1



รูปที่ 3.1 ขั้นตอนการทำวิจัย

จากรูปที่ 3.1 สามารถอธิบายขั้นตอนการทำวิจัยดังนี้

1) ศึกษาทฤษฎีที่เกี่ยวข้อง เป็นขั้นตอนการวิเคราะห์ทฤษฎีที่เกี่ยวข้องที่ได้กล่าวไปในบทที่ 2 โดยมุ่งเน้นไปที่การจัดเก็บและค้นคืนสารสนเทศ แบบรูปความมั่นคง เพื่อนำมาใช้ในการออกแบบ

วิธีการและพัฒนาระบบต้นแบบสนับสนุนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ

2) วิเคราะห์และจำแนกแบบรูปความมั่นคงตามหลักของ ซี.ไอ.เอ.เอ เป็นขั้นตอนเพื่อจำแนกแบบรูปความมั่นคง ตามคุณลักษณะด้านความปลอดภัยบนแนวคิดด้านความปลอดภัยพื้นฐาน เพื่อใช้อ้างอิงในการสร้างโครงสร้างข้อมูลความมั่นคงสารสนเทศ ผลลัพธ์ที่ได้จากขั้นตอนนี้คือ ตารางแบบรูปความมั่นคงที่จำแนกตามหลักของ ซี.ไอ.เอ.เอ

3) วิเคราะห์และออกแบบวิธีการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานไอเอสโอ/ไออีซี 27002 ขั้นตอนนี้เริ่มจากการจัดเก็บแบบรูปความมั่นคงและเอกสารมาตรฐานไอเอสโอ/ไออีซี 27002 เข้าสู่ระบบ หลังจากนั้นสร้างโครงสร้างข้อมูลความมั่นคงสารสนเทศ (Information Security Structure) จากแบบรูปความมั่นคง เพื่อนำมาใช้ช่วยเพิ่มประสิทธิผลในการค้นคืน โดยข้อมูลที่ค้นคืนได้นั้น คือส่วนของเอกสารมาตรฐานความมั่นคงที่มีความคล้ายคลึงกับข้อคำถามและข้อมูลแบบรูปความมั่นคง โดยเสนอใช้วิธีการค้นคืน 3 วิธีการ คือ 1) การค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยพิจารณาแบบรูปความมั่นคง 2) การค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้คำสำคัญ 3)การค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยพิจารณาความสัมพันธ์ของแบบรูปความมั่นคง

4) พัฒนาเครื่องมือต้นแบบสนับสนุนวิธีการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานไอเอสโอ/ไออีซี 27002 เพื่อสามารถนำไปประยุกต์ใช้ได้จริง รวมถึงนำไปทดสอบและประเมินผลการค้นคืนด้วย แสดงรายละเอียดในบทที่ 4

5) ทดสอบเครื่องมือต้นแบบและประเมินประสิทธิผลการค้นคืน เป็นขั้นตอนในการทดสอบว่าเครื่องมือต้นแบบมีความสามารถตามความต้องการเชิงหน้าที่หรือไม่ และประเมินประสิทธิผลวิธีการที่นำเสนอ ว่ามีความแม่นยำและความครบถ้วนในการค้นคืนผลลัพธ์หรือไม่ ซึ่งแสดงรายละเอียดในบทที่ 5

6) สรุปผลการวิจัย เป็นขั้นตอนการสรุปผลที่ได้จากงานวิจัย รวมถึงแนวทางในการพัฒนางานวิจัยในอนาคต แสดงรายละเอียดในบทที่ 6

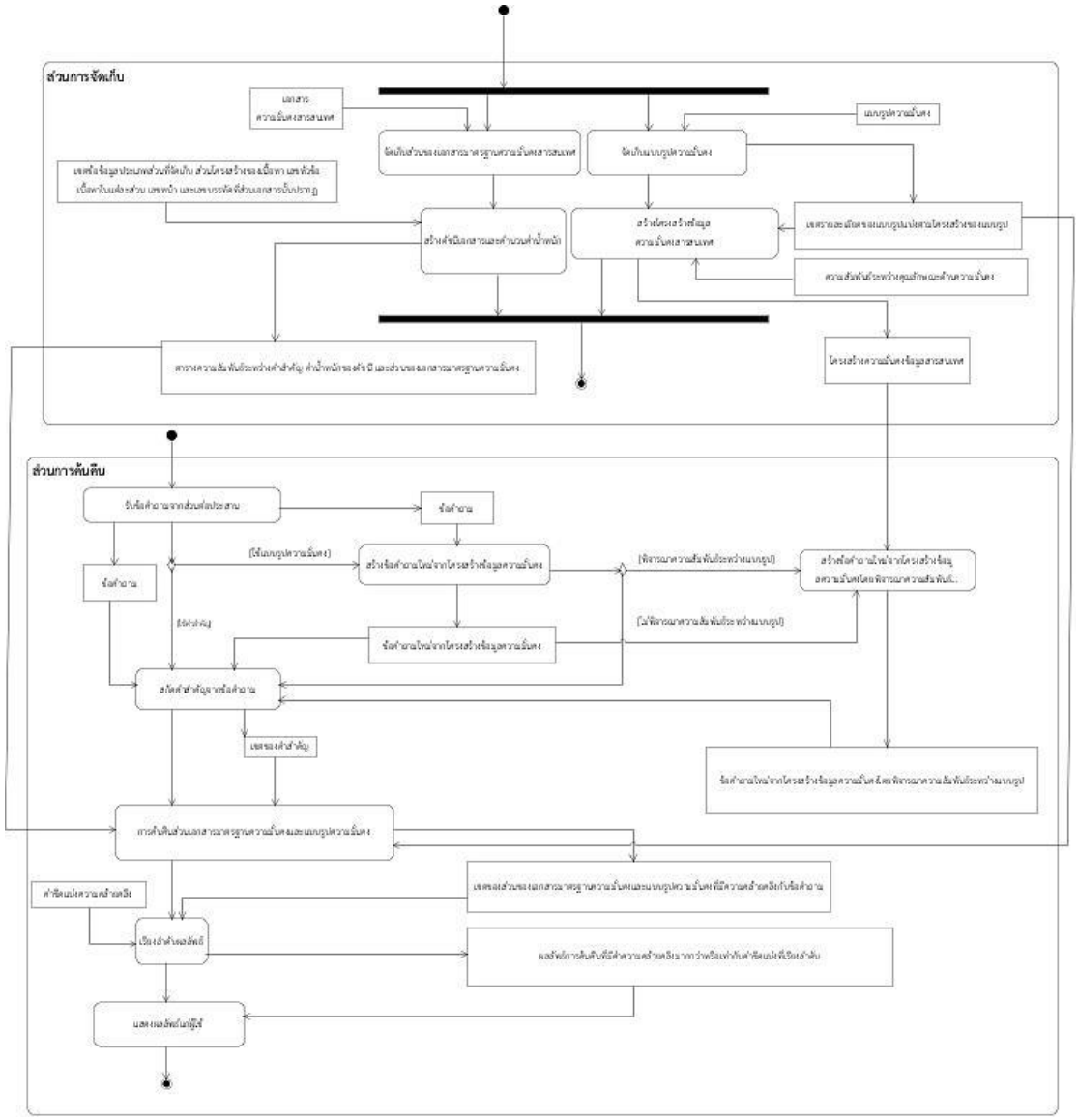
3.1 การวิเคราะห์แบบรูปความมั่นคงเพื่อจำแนกแบบรูปความมั่นคงตามหลักของ ซี.ไอ.เอ.เอ

ในขั้นตอนนี้มีจุดประสงค์เพื่อจำแนกแบบรูปความมั่นคง ตามคุณลักษณะด้านความปลอดภัยบนแนวคิดด้านความปลอดภัยพื้นฐาน 4 ด้าน [3] ได้แก่ ความลับของข้อมูล ความบูรณภาพ สภาพ

พร้อมใช้งานของข้อมูล และความรับผิดชอบต่อข้อมูล โดยใช้แบบรูปความมั่นคงทั้งสิ้น 20 แบบรูป ที่นำเสนอโดย M.Schumacher และคณะ [1] ซึ่งผู้เชี่ยวชาญด้านความมั่นคงสารสนเทศจะเป็นผู้จำแนก โดยจะวิเคราะห์จากการนำไปใช้ของแบบรูป ตัวอย่างเช่น แบบรูปความการออกแบบและใช้รหัสผ่าน (Password design and use) เป็นแบบรูปเกี่ยวกับวิธีที่ดีที่สุดในการเลือกใช้และใช้งานรหัสผ่านสำหรับระบบหรือองค์กรเพื่อรักษาความลับของข้อมูล แบบรูปนี้จึงใช้แนวคิดด้าน ความลับของข้อมูล เป็นต้น ผลลัพธ์ที่ได้จากขั้นตอนนี้ คือความเกี่ยวข้องกันระหว่างแบบรูปและคุณลักษณะความมั่นคงสารสนเทศ ซึ่งจะนำไปใช้อ้างอิงในการสร้างโครงสร้างข้อมูลสารสนเทศ เพื่อช่วยในการค้นคืนส่วนเอกสารความมั่นคงสารสนเทศ ซึ่งสามารถจำแนกได้ดังตารางที่ ก.2 ในภาคผนวก ก

3.2 การวิเคราะห์และออกแบบวิธีการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานไอเอสโอ/ไออีซี 27002

วิธีการจัดเก็บและค้นคืนที่นำเสนอเป็นการค้นคืนส่วนของเอกสารมาตรฐานไอเอสโอ/ไออีซี 27002 และแบบรูปความมั่นคง โดยภาพรวมของงานแสดงได้ด้วยแผนภาพกิจกรรมดังรูปที่ 3.2 ประกอบด้วย 2 ส่วนหลัก คือ 1) ส่วนการจัดเก็บ 2) ส่วนการค้นคืน



รูปที่ 3.2 แผนภาพกิจกรรมของการจัดเก็บและค้นคืนส่วนของเอกสาร
มาตรฐานความมั่นคงสารสนเทศ

จากรูปที่ 3.2 อธิบายรายละเอียดแต่ละส่วน มีดังต่อไปนี้

3.2.1 ส่วนการจัดเก็บ

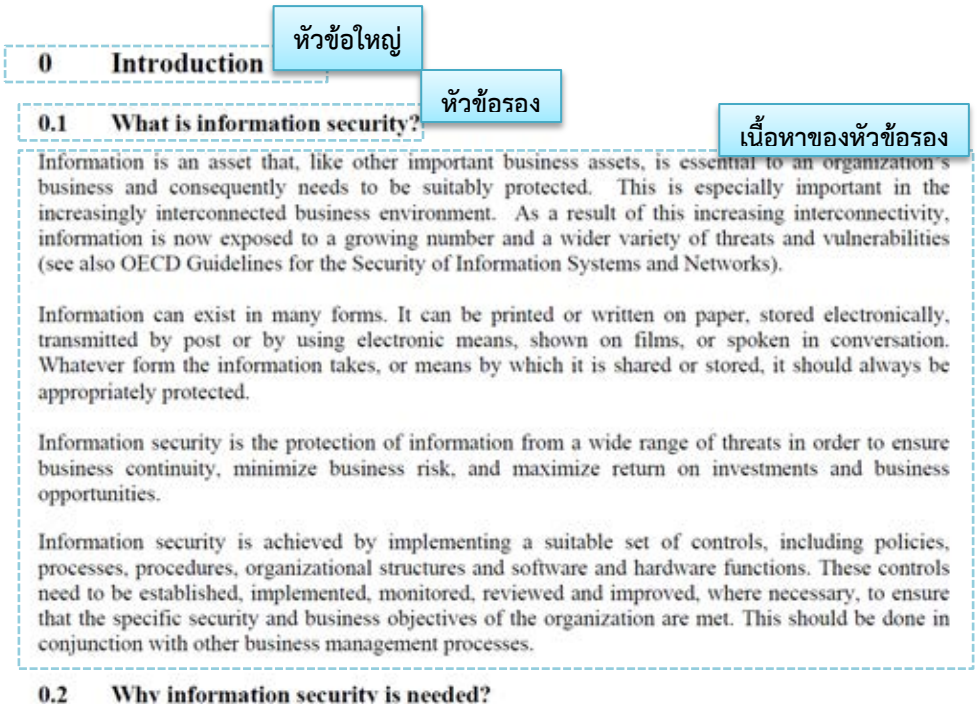
1) การจัดเก็บส่วนของเอกสารมาตรฐานด้านความมั่นคง

ขั้นตอนนี้จะจัดเก็บส่วนของเอกสารมาตรฐานด้านความมั่นคง ไอเอสโอ/ไออีซี 27002 เข้าสู่ฐานข้อมูลเชิงสัมพันธ์ โดยแยกการจัดเก็บเป็น 2 ส่วน คือการเก็บส่วนบทนำ (Introduction) ซึ่งเป็นส่วนที่กล่าวถึงความรู้ทั่วไปที่เกี่ยวข้องกับเอกสารมาตรฐานความมั่นคง และส่วนข้อกำหนดนโยบาย (Clause) ซึ่งจากการศึกษาเอกสารมาตรฐานด้านความมั่นคง ไอเอสโอ/ไออีซี 27002 ทั้งสองส่วนพบว่ามีโครงสร้างของเนื้อหาที่แตกต่างกัน งานวิจัยนี้จึงจัดเก็บเนื้อหาจากส่วนของโครงสร้างที่แตกต่างกันด้วย ดังตารางที่ 3.1 ตัวอย่างส่วนของเอกสารที่จัดเก็บ แสดงดังรูปที่ 3.3 และ 3.4

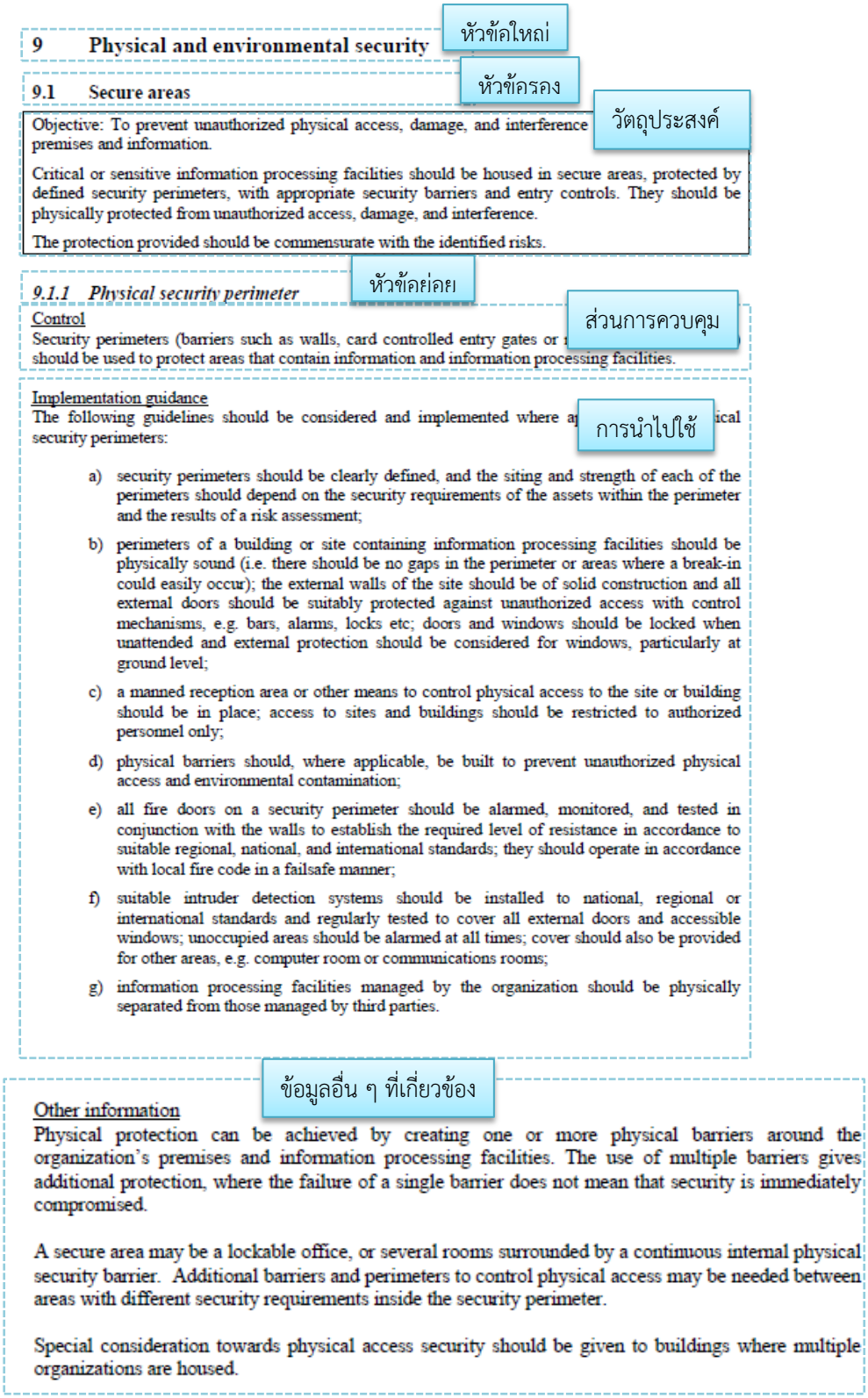
ข้อมูลที่จัดเก็บจากขั้นตอนนี้ คือประเภทส่วนที่จัดเก็บ ส่วนโครงสร้างของเนื้อหา เลขหัวข้อเนื้อหาในแต่ละส่วน เลขหน้า และเลขบรรทัดที่ส่วนเอกสารนั้นปรากฏ

ตารางที่ 3.1 การจัดเก็บส่วนของเอกสารมาตรฐานด้านความมั่นคง

ลำดับ	โครงสร้างของเนื้อหา	ส่วนบทนำ	ส่วนข้อกำหนดนโยบาย
1	หัวข้อใหญ่	✓	✓
2	หัวข้อรอง	✓	✓
3	วัตถุประสงค์	✗	✓
4	หัวข้อย่อย	✗	✓
5	ส่วนการควบคุม	✗	✓
6	การนำไปใช้	✗	✓
7	ข้อมูลอื่นๆที่เกี่ยวข้อง	✗	✓
8	เนื้อหาของหัวข้อรอง	✓	✗



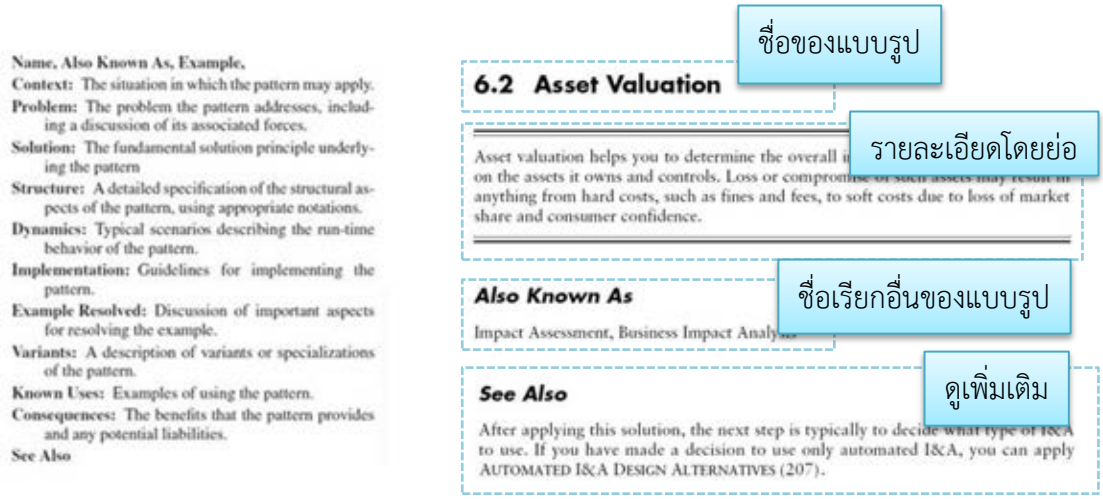
รูปที่ 3.3 ตัวอย่างส่วนประกอบมาตรฐานความมั่นคงที่จัดเก็บ (ส่วนบทนำ) [4]



รูปที่ 3.4 ตัวอย่างส่วนประกอบมาตรฐานความมั่นคงที่จัดเก็บ (ส่วนข้อกำหนดนโยบาย) [4]

2) การจัดเก็บแบบรูปความมั่นคง

ในขั้นตอนนี้จะจัดเก็บแบบรูปความมั่นคงทั้งสิ้น 20 แบบรูป โดยนำมาจากหนังสือแบบรูปความมั่นคงการบูรณการความมั่นคงและวิศวกรรมระบบของ M. Schumacher และคณะ [1] มาเป็นกรณีศึกษา โดยใช้เนื้อหาจาก 4 โครงสร้าง ได้แก่ ชื่อของแบบรูป ชื่อเรียกอื่นของแบบรูป รายละเอียดโดยย่อของแบบรูปแต่ละแบบรูป และทำการอ้างถึงแบบรูปความมั่นคงอื่นที่แก้ไขปัญหาเดียวกัน ซึ่งแสดงตัวอย่างเนื้อหาจากทั้ง 4 โครงสร้างดังรูปที่ 3.5 นำเป็นข้อมูลนำเข้าเพื่อสร้างโครงสร้างข้อมูลสารสนเทศ และเนื้อหาจากทุกโครงสร้างที่ได้กล่าวไว้ในหัวข้อ 2.1.3 จะเป็นข้อมูลผลลัพธ์ที่ได้จากการค้นคืน ตัวอย่างโครงสร้างของแบบรูปความมั่นคง



รูปที่ 3.5 ตัวอย่างโครงสร้างแบบรูปความมั่นคงที่จัดเก็บ [1]

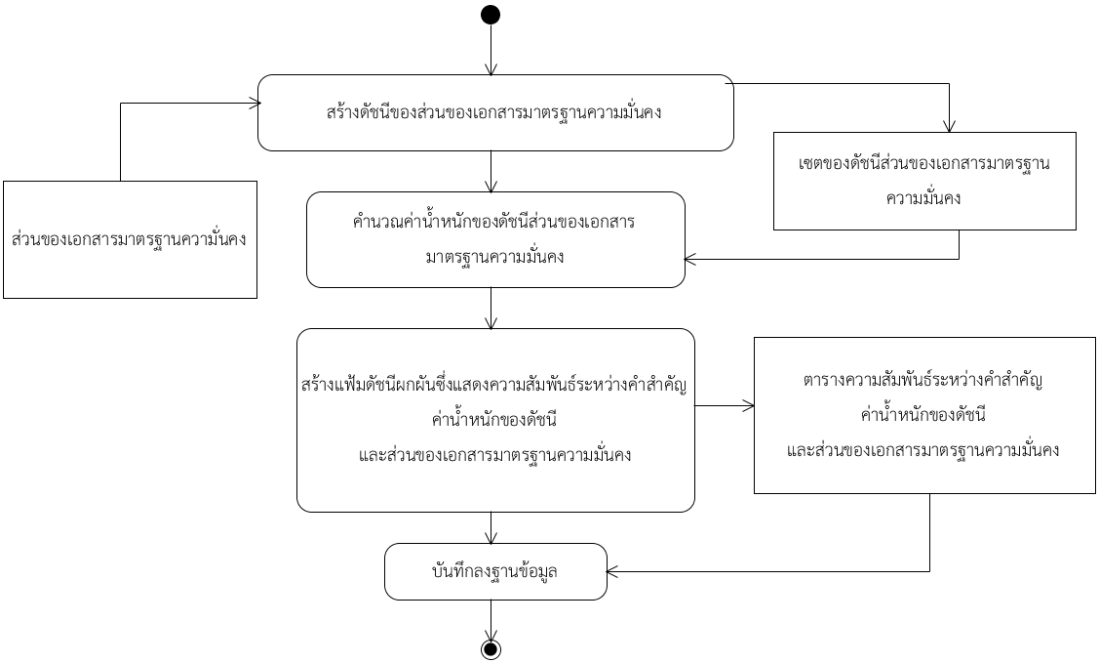
3) กระบวนการจัดทำดัชนีและคำนวณค่าน้ำหนักของดัชนีเอกสาร

หลังจากกระบวนการจัดเก็บส่วนของเอกสารมาตรฐานด้านความมั่นคงและแบบรูปความมั่นคงแล้ว จะมีกระบวนการจัดทำดัชนีและคำนวณค่าน้ำหนักของดัชนีเอกสาร ซึ่งแสดงในแผนภาพกิจกรรมที่ 3.6 และกระบวนการจัดทำดัชนีและคำนวณค่าน้ำหนักของดัชนีของแบบรูปความมั่นคงแสดงในแผนภาพกิจกรรมที่ 3.7

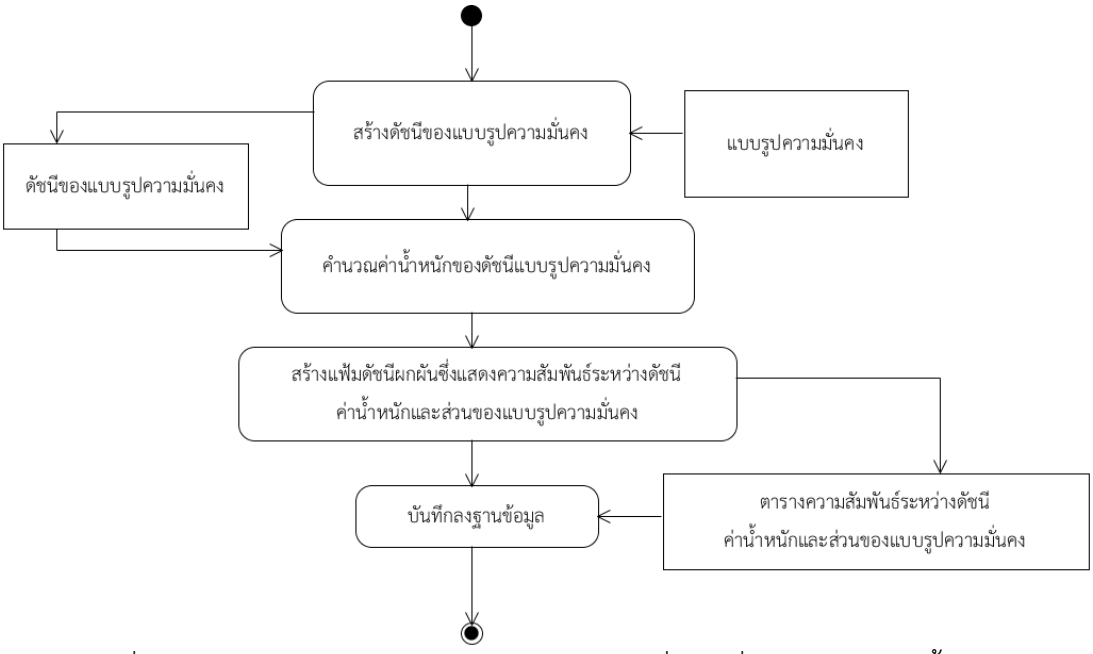
การจัดทำดัชนีของส่วนเอกสารมาตรฐานความมั่นคง จะทำการสกัดจากเนื้อหาในแต่ละส่วนโครงสร้างที่จัดเก็บ ส่วนดัชนีแบบรูปความมั่นคงจะสกัดจากโครงสร้างของแบบรูปความมั่นคง

ทั้งสิ้น 4 โครงสร้าง ได้แก่ ชื่อของแบบรูป ชื่อเรียกอื่นของแบบรูป รายละเอียดโดยย่อของแบบรูปแต่ละแบบรูปความมั่นคง และทำการอ้างถึงแบบรูปความมั่นคงอื่นที่แก้ไขปัญหาเดียวกัน

โดยรายละเอียดการจัดทำดัชนีของเอกสารและคำนวณค่าน้ำหนักในงานวิจัยนี้ จะใช้การสมการสำหรับคำนวณค่าน้ำหนักต่างๆ ดังที่ได้กล่าวไว้ในหัวข้อที่ 2.1.4.1



รูปที่ 3.6 แผนภาพกิจกรรมการจัดเก็บเอกสารเพื่อทำดัชนีและค่าน้ำหนัก



รูปที่ 3.7 แผนภาพกิจกรรมการจัดเก็บแบบรูปความมั่นคงเพื่อทำดัชนีและค่าน้ำหนัก

ดัชนีของเอกสารและค่าน้ำหนักของดัชนีที่ได้จากกระบวนการข้างต้น ถูกนำมาสร้างแฟ้มดัชนีผกผันของส่วนของเอกสารมาตรฐานความมั่นคงและแบบรูปความมั่นคง ซึ่งเป็นตารางข้อมูลจัดเก็บความสัมพันธ์ระหว่าง ดัชนี น้ำหนักของดัชนี และส่วนเอกสารตามแบบจำลองปริภูมิเวคเตอร์ แสดงดังรูปที่ 3.8 ซึ่งจะจัดเก็บลงฐานข้อมูลต่อไป

	DS_1	DS_2	DS_3	DS_4	$DS5_2$	...	DSn
T_1	$W_{1,1}$	$W_{,2,1}$	$W_{3,1}$	$W_{4,1}$	$W_{5,1}$	...	$W_{n,1}$
T_2	$W_{1,2}$	$W_{2,2}$	$W_{3,2}$	$W_{4,2}$	$W_{5,2}$	...	$W_{n,2}$
T_3	$W_{1,3}$	$W_{2,3}$	$W_{3,3}$	$W_{4,3}$	$W_{5,3}$	...	$W_{n,3}$
T_4	$W_{1,4}$	$W_{2,4}$	$W_{3,4}$	$W_{4,4}$	$W_{5,4}$	...	$W_{n,4}$
:	:	:	:	:	:		:
T_t	$W_{1,t}$	$W_{2,t}$	$W_{3,t}$	$W_{4,t}$	$W_{5,t}$	...	$W_{n,t}$

รูปที่ 3.8 ตารางน้ำหนักระหว่างส่วนของเอกสารกับดัชนีตามแบบจำลองปริภูมิเวคเตอร์

โดย

DS_i คือส่วนเอกสารมาตรฐานความมั่นคงสารสนเทศที่ i

T_j คือดัชนีที่ j ที่ปรากฏอยู่ในส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ

$W_{i,j}$ คือน้ำหนักของดัชนีที่ j ที่ปรากฏอยู่ส่วนเอกสารมาตรฐานความมั่นคงสารสนเทศที่ i

ตัวอย่างที่ 1 แสดงตัวอย่างการจัดเก็บดัชนีส่วนเอกสารมาตรฐานความมั่นคงซึ่งมีกำหนดรหัสโครงสร้าง 917 ซึ่งมีเนื้อหา ดังนี้

“0.1 What is information security?”

ผลลัพธ์จากกระบวนการจัดทำดัชนี inform secur

ตัวอย่างการจัดเก็บแฟ้มดัชนีผกผันของส่วนเอกสาร แสดงดังตารางที่ 3.2

ตารางที่ 3.2 ตัวอย่างการจัดเก็บแฟ้มดัชนีผกผันของส่วนเอกสาร

ดัชนี	รหัสส่วนของเอกสาร			
	917	918	919	โครงสร้างที่ N
inform	0.88	2.72	0.88	⋮
secur	0.88	12.57	3.9	

ตัวอย่างที่ 2 แสดงตัวอย่างการจัดเก็บดัชนีแบบรูปความมั่นคงซึ่งมีกำหนดรหัสโครงสร้าง 7 ซึ่งมีเนื้อหา ดังนี้

"Security Needs Identification for Enterprise Assets"

ผลลัพธ์จากกระบวนการจัดทำดัชนี asset enterpris identif need secur

ตัวอย่างการจัดเก็บแฟ้มดัชนีผกผันของแบบรูปความมั่นคง แสดงดังตารางที่ 3.3

ตารางที่ 3.3 ตัวอย่างการจัดเก็บแฟ้มดัชนีผกผันของแบบรูปความมั่นคงที่ระบุค่าน้ำหนักของแต่ละดัชนี

ดัชนี	รหัสโครงสร้างแบบรูป			
	7	918	919	โครงสร้างที่ N
asset	0.88	2.72	0.88	⋮
enterpris	0.88	12.57	3.9	
identif				
need				

4) การสร้างโครงสร้างข้อมูลความมั่นคงสารสนเทศ (Information Security Structuring)

วัตถุประสงค์ในการสร้างโครงสร้างข้อมูลความมั่นคงสารสนเทศ เพื่อใช้ในการสร้างข้อคำถามแก่ผู้ค้นคืนซึ่งช่วยให้การค้นคืนส่วนของเอกสารความมั่นคงสารสนเทศให้มีประสิทธิผลมากยิ่งขึ้น

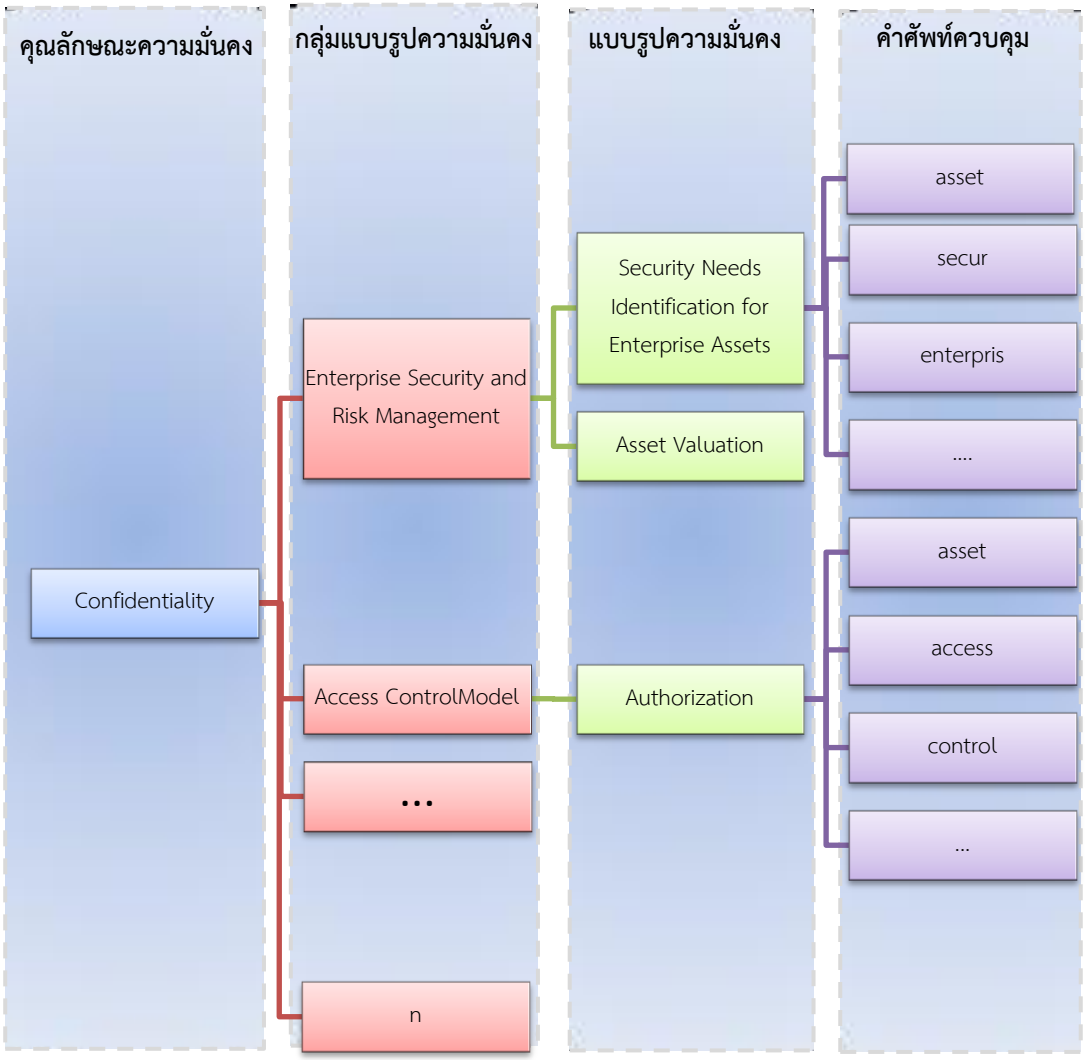
โครงสร้างข้อมูลความมั่นคงสารสนเทศที่สร้างขึ้น คือแผนภาพต้นไม้ที่ประกอบด้วยความสัมพันธ์แบบลำดับชั้นระหว่างคุณลักษณะด้านความมั่นคง กลุ่มของแบบรูปความมั่นคง ชื่อแบบ

รูปความมั่นคง และคำศัพท์ควบคุม ซึ่งความสัมพันธ์ระหว่างคุณลักษณะด้านความมั่นคงและแบบรูปความมั่นคงนั้นได้จากการจำแนกในหัวข้อที่ 3.1

แผนภาพต้นไม้ที่สร้างขึ้นนั้นโหนดแม่และโหนดลูกของกลุ่มนั้น ๆ จะมีความสัมพันธ์กัน โดยแบ่งออกเป็น 4 ลำดับชั้น ดังนี้

- ชั้นที่ 1 คือโหนดที่แสดงคุณลักษณะด้านความมั่นคง
- ชั้นที่ 2 คือโหนดที่แสดงกลุ่มของแบบรูปความมั่นคง
- ชั้นที่ 3 คือโหนดที่แสดงชื่อแบบรูปความมั่นคง ที่ได้จากข้อมูลนำเข้าจากขั้นตอน การจัดเก็บแบบรูปความมั่นคง
- ชั้นที่ 4 คำศัพท์ควบคุม คือดัชนีที่ได้จากกระบวนกระบวนการจัดทำดัชนีและคำนวณค่าน้ำหนักของดัชนีเของแบบรูปความมั่นคง ที่ได้กล่าวในหัวข้อก่อนหน้า จากนั้นจัดเก็บความถี่ของดัชนีเพื่อใช้ในการเรียงลำดับการแสดงผลลัพธ์ต่อไป ซึ่งในงานวิจัยนี้ใช้ความถี่เรียงลำดับมากสุด 5 อันดับแรกขึ้นมาแสดง สาเหตุเพราะ คำศัพท์ควบคุมที่มากจนเกินไปอาจทำให้ผลลัพธ์ที่ไม่จำเป็นเพิ่มมากขึ้นด้วย

จากตัวอย่างโครงสร้างของแบบรูปความมั่นคง ที่แสดงดังรูปที่ 3.9 สามารถอธิบายความสัมพันธ์ได้ว่า คุณลักษณะความมั่นคง “Confidentiality” เกี่ยวข้องกับ กลุ่มแบบรูปความมั่นคง ทั้งสิ้น n กลุ่ม โดยกลุ่มแบบรูปความมั่นคง “Enterprise Security and Risk Management” ประกอบด้วยแบบรูปความมั่นคง ทั้งสิ้น k แบบรูป โดยแบบรูปที่ชื่อ “Security Needs Identification for Enterprise Assets” มีคำศัพท์ควบคุมที่เรียงลำดับตามความถี่ คือ“asset” “secur” ถึง ... ตามลำดับ



รูปที่ 3.9 ตัวอย่างโครงสร้างข้อมูลความมั่นคงสารสนเทศ

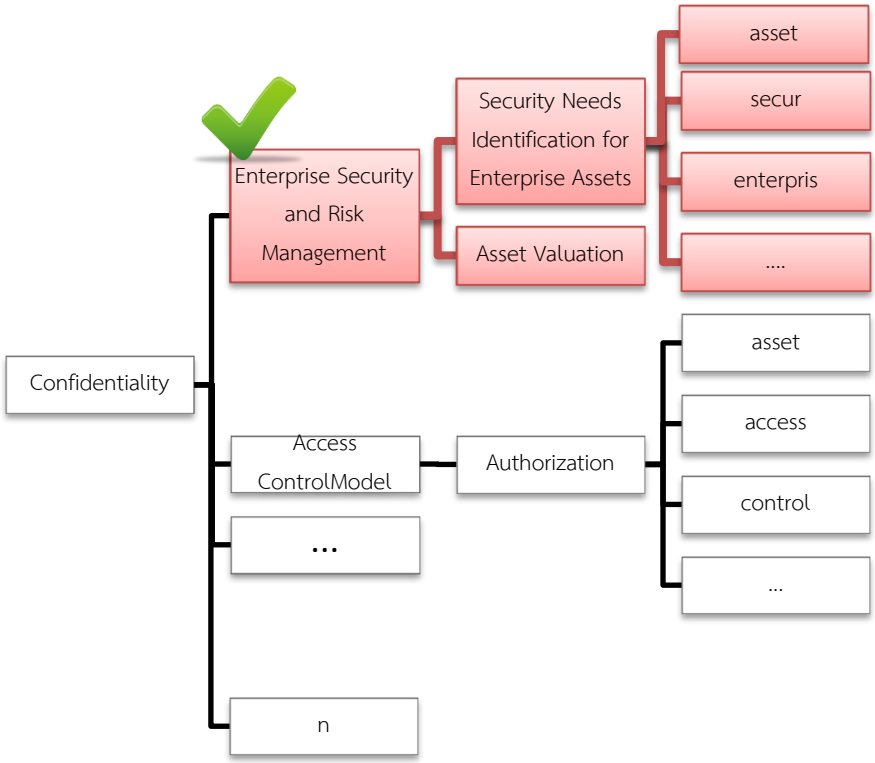
3.2.2 ส่วนการค้นคืน

1) การสร้างข้อคำถามใหม่

กระบวนการนี้มีจุดประสงค์เพื่อสร้างข้อคำถามใหม่จากโครงสร้างข้อมูลสารสนเทศที่ได้กล่าวมาแล้ว เพื่อนำเข้าสู่กระบวนการสกัดคำสำคัญเพื่อนำไปใช้เปรียบเทียบหาความคล้ายคลึงกับส่วนเอกสารในขั้นตอนการค้นคืนต่อไป เริ่มต้นจากผู้ใช้เลือกข้อคำถามจากโครงสร้างข้อมูลสารสนเทศ เนื่องจากโหนดแม่และโหนดลูกของกลุ่มนั้น ๆ จะมีความสัมพันธ์กัน ระบบจะท่องโหนดจากซ้ายไปขวาล่างโดยเริ่มจากโหนดที่ถูกเลือก ดังแสดงตัวอย่างการท่องโหนด ดังภาพที่ 3.10 หลังจากนั้นจะสร้างข้อคำถามใหม่ซึ่งได้คำของโหนดที่ถูกเลือกและแต่ละคำของโหนดลูกที่อยู่ภายใต้โหนดที่ผู้ใช้เลือก

ตัวอย่างที่ 3 จากตัวอย่างบางส่วนของโครงสร้างข้อมูลสารสนเทศในรูปที่ 3.10 สมมุติเหตุการณ์ให้ผู้ใช้เลือกโหนด *“Enterprise Security and Risk Management”*

ข้อคำถามใหม่ที่ได้คือ*“Confidentiality Security Needs Identification for Enterprise Assets Asset Valuation asset secur enterpris ...etc”*



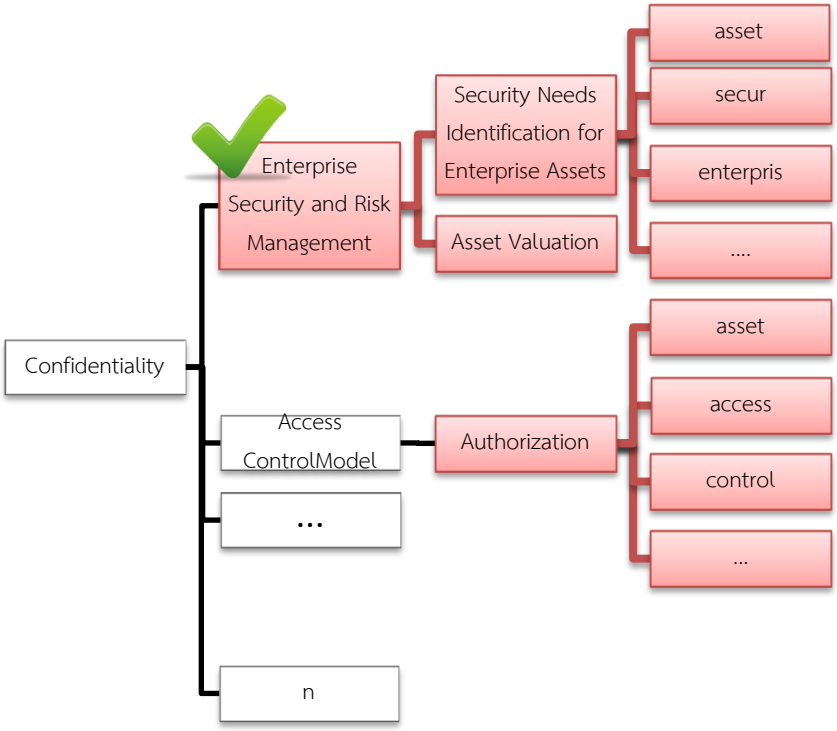
รูปที่ 3.10 ตัวอย่างการสร้างข้อคำถามใหม่กรณีผู้ใช้เลือกโหนด “Enterprise Security and Risk Management”

นอกจากนี้ผู้วิจัยนำเสนอการค้นคืนโดยพิจารณาความสัมพันธ์ระหว่างแบบรูปความมั่นคง มีวัตถุประสงค์เพื่อใช้ในการขยายข้อคำถามเพื่อเพิ่มประสิทธิผลในการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง ซึ่งความสัมพันธ์ของแบบรูปความมั่นคงที่ใช้ในงานวิจัยนี้เป็นไปตามกับความสัมพันธ์ที่กล่าวไว้ในงานวิจัย [5] ได้จัดทำไว้ โดยแสดงในตารางที่ ก.3 ในภาคผนวก ก เพื่อทำให้ผู้ใช้สามารถทำการนำผลลัพธ์ไปใช้งานได้อย่างครบถ้วนมากยิ่งขึ้น โดยจะทำการนำแบบรูปที่เลือกมาจากโครงสร้างข้อมูลความมั่นคงสารสนเทศที่สร้างขึ้นหาความสัมพันธ์ระหว่างแบบรูปและเงื่อนไขต่าง ๆ ผลลัพธ์ที่

ได้จะเป็นข้อคำถามชุดใหม่สำหรับความมั่นคงที่เกี่ยวเนื่องกัน เพื่อนำเข้าสู่กระบวนการสกัดคำสำคัญเพื่อนำไปใช้เปรียบเทียบหาความคล้ายคลึงกับส่วนเอกสารในขั้นตอนการค้นคืนต่อไป

ตัวอย่างที่ 4 จากผลลัพธ์จากตัวอย่างที่ 3 เมื่อพิจารณาความสัมพันธ์ระหว่างแบบรูปความมั่นคง ทำให้ได้ข้อคำถามใหม่ที่มีขนาดใหญ่ขึ้น แสดงดังรูปที่ 3.11

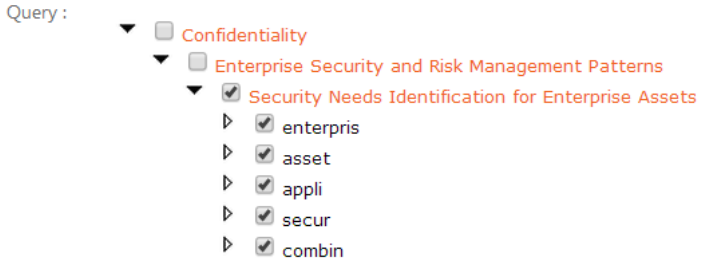
ข้อคำถามใหม่ที่ได้คือ“*Confidentiality Security Needs Identification for Enterprise Assets Asset Valuation asset secur enterpris Authorization access control ..etc*”



รูปที่ 3.11 ตัวอย่างข้อคำถามใหม่ที่เกี่ยวเนื่องกับข้อคำถามที่เลือกโดยพิจารณาความสัมพันธ์ระหว่างแบบรูปความมั่นคง

ตัวอย่างที่ 5 ตัวอย่างผลลัพธ์จากกิจกรรมสร้างข้อคำถามใหม่ แสดงดังตารางที่ 3.4

ตารางที่ 3.4 ตัวอย่างผลลัพธ์จากการสร้างข้อคำถามใหม่จากตัวอย่างข้อคำถามเมื่อผู้ใช้ทำการเลือก

กิจกรรมการค้นคืนของผู้ใช้	
ข้อคำถามใหม่จากโครงสร้างข้อมูลสารสนเทศ	Security Needs Identification for Enterprise Assets enterpris asset appli secur combin
ข้อคำถามใหม่เมื่อพิจารณาความสัมพันธ์ระหว่างแบบรูป	Label Enterprise Security and Risk Management Patterns Security Needs Identification for Enterprise Assets enterpris asset appli secur approach Asset Valuation enterpris asset control assess determin Threat Assessment can assess enterpris asset determin Vulnerability Assessment access assess enterpris asset also Risk Determination determin evalu risk Enterprise Security Approaches enterpris asset assess secur also Enterprise Security Services access enterpris asset control base Enterprise Partner Communication access enterpris applic busi commun Access Control Model Patterns Authorization access asset control check applic Role-Based Access Control access control can check appli Multilevel Security access control check applic 287 Reference Monitor access can secur 287 authent Role Rights Definition access can check 287 297

โดยการนำเสนอการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงโดยพิจารณาความสัมพันธ์ระหว่างแบบรูปความมั่นคง ไม่มีการทำการทดลองในงานวิจัยนี้เนื่องจากเป็นเพียงฟังก์ชันการทำงาน

สนับสนุนให้ผู้ใช้สามารถทำงานการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงที่เกี่ยวเนื่องกับผลลัพธ์ของการค้นคืนได้อย่างครบถ้วนมากยิ่งขึ้น

2) การสกัดคำสำคัญจากข้อคำถาม

กระบวนการนี้มีจุดประสงค์เพื่อสกัดคำสำคัญจากข้อคำถามที่รับเข้ามาจากส่วนรับข้อคำถาม เพื่อนำไปใช้เปรียบเทียบหาความคล้ายคลึงกับส่วนเอกสารมาตรฐานความมั่นคง ผลลัพธ์ที่ได้จากกระบวนการนี้ คือเซตของคำสำคัญและค่าน้ำหนักของคำสำคัญของข้อคำถาม

ขั้นตอนนี้เริ่มจากเมื่อผู้ใช้กรอกข้อคำถามผ่านส่วนต่อประสานผู้ใช้ ระบบจะมีส่วนการสกัดคำสำคัญจากข้อคำถาม การสกัดคำสำคัญและค่าน้ำหนักของข้อคำถาม ใช้กระบวนการเดียวกับการจัดทำดัชนีและคำนวณค่าน้ำหนัก และสมการสำหรับคำนวณค่าน้ำหนักต่างๆ ดังที่ได้กล่าวไว้ในหัวข้อที่ 2.1.4.1 ผลลัพธ์จากกระบวนการนี้ ประกอบด้วยเซตของคำสำคัญและค่าน้ำหนักของคำสำคัญของข้อคำถาม

ตัวอย่างที่ 6 ตัวอย่างผลลัพธ์จากกิจกรรมสกัดคำสำคัญจากข้อคำถามในวิธีการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงโดยใช้คำสำคัญจากตัวอย่างข้อคำถาม 2 รายการ แสดงดังตารางที่ 3.5

ตารางที่ 3.5 ผลลัพธ์จากกิจกรรมสกัดคำสำคัญจากข้อคำถามในวิธีการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงโดยใช้คำสำคัญจากตัวอย่างข้อคำถาม 2 รายการ

ตัวอย่างข้อคำถามที่ 6.1	Information security regarding physical conditions
ผลลัพธ์จากกระบวนการสกัดคำสำคัญ	condit inform physic regard secur
ตัวอย่างข้อคำถามที่ 6.2	Risk Assessment & Management
ผลลัพธ์จากกระบวนการสกัดคำสำคัญ	assess manag risk

ตัวอย่างที่ 7 จากผลลัพธ์ในตัวอย่างที่ 5 สามารถสกัดคำสำคัญได้ตารางที่ 3.6

ตารางที่ 3.6 ผลลัพธ์จากกิจกรรมสกัดคำสำคัญจากข้อคำถามในวิธีการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงโดยใช้คำสำคัญจากตัวอย่างในข้อ 5.1

ตัวอย่างข้อคำถามใหม่ที่ 5.1	Security Needs Identification for Enterprise Assets enterpris asset appli secur combin
ผลลัพธ์จากกระบวนการสกัดคำสำคัญ	appli asset enterpri enterpris identif need secur

3) การค้นคืน

การค้นคืนเอกสารในงานวิจัยนี้ใช้แบบจำลองปริภูมิเวคเตอร์ในการคำนวณค่าความคล้ายคลึงระหว่างส่วนของเอกสารและของข้อคำถาม เนื่องจากงานวิจัยนี้ได้หาค่าความคล้ายคลึงจากส่วนประกอบของเอกสารมาตรฐาน จึงมีการแบ่งการคำนวณค่าความคล้ายคลึงระหว่างข้อคำถามกับแต่ละส่วนของเอกสาร แสดงในสมการที่ (8)

$$sim(E_{m,j}, q) = \frac{\sum_{i=1}^{t} w_{i,j,m} \times w_{i,q}}{\sqrt{w_{i,j,m}^2} \times \sqrt{w_{i,q}^2}} \quad (8)$$

โดย

$sim(E_{m,j}, q)$ คือค่าความคล้ายคลึงระหว่างเอกสารที่ j ส่วนประกอบที่ m กับข้อคำถาม q

q คือข้อคำถาม

$E_{m,j}$ คือส่วนประกอบที่ m ในเอกสารที่ j

t คือจำนวนคำสำคัญที่ใช้ในการคำนวณ

$w_{i,j,m}$ คือค่าน้ำหนักของคำสำคัญ i ในเอกสารที่ j ส่วนประกอบที่ m

$w_{i,q}$ คือค่าน้ำหนักของคำสำคัญ i ของคำถามที่ป้อนเข้าไป

เนื่องจากการค้นคืนได้มาจากหลายส่วนประกอบซึ่งมีความสำคัญแตกต่างกัน จึงมีการกำหนดค่าน้ำหนักให้แต่ละส่วนประกอบที่ค้นเจอด้วย เมื่อได้ค่าความคล้ายคลึงที่ได้จากสมการที่ (8) คูณด้วยค่าน้ำหนักที่กำหนด และหารด้วยผลรวมค่าน้ำหนักของแต่ละองค์ประกอบ แสดงในสมการที่ (9)

$$sim(D_j, q) = \frac{\sum_{i=1}^{e} (sim(E_{m,j}, q) * w_m)}{TotalWeight} \quad (9)$$

โดย

$sim(D_j, q)$ คือค่าความคล้ายคลึงระหว่างเอกสารที่ j กับข้อคำถาม q

$sim(E_{m,j}, q)$	คือค่าความคล้ายคลึงของส่วนของเอกสารที่ j ส่วนประกอบที่ m
q	คือข้อคำถาม
$E_{m,j}$	คือส่วนประกอบที่ m ในเอกสารที่ j
w_m	คือค่าน้ำหนักของพิจารณาตามส่วนเอกสาร
$TotalWeight$	คือผลรวมค่าน้ำหนักทั้งหมด
e	คือจำนวนส่วนประกอบของเอกสาร

4) การเรียงลำดับผลลัพธ์

ขั้นตอนนี้มีจุดประสงค์เพื่อนำค่าความคล้ายคลึงมาเรียงลำดับจากมากไปน้อย และจะแสดงผลเฉพาะค่าที่มีความคล้ายคลึงมากกว่าค่าขีดแบ่งที่ผู้ใช้ระบุ โดยค่าขีดแบ่งมีค่าอยู่ในช่วง 0-1

5) การแสดงผลลัพธ์

ส่วนแสดงการค้นคืน คือส่วนแสดงผลลัพธ์ที่มีความคล้ายคลึงกับข้อคำถามที่ผ่านขั้นตอนการเรียงลำดับแล้ว ประกอบด้วยสองส่วนข้อมูล คือผลลัพธ์ที่ได้จากการค้นคืนส่วนเอกสารมาตรฐานความมั่นคง ซึ่งจะแสดง หัวข้อ เนื้อหา ค่าความคล้ายคลึง หน้าและเลขบรรทัด ส่วนการแสดงรายละเอียดผลลัพธ์ที่ได้จากการค้นคืนแบบรูปความมั่นคง จะประกอบด้วยโครงสร้างต่าง ๆ ของแบบรูปความมั่นคง ที่กล่าวไว้ในบทที่ 2.1.3

ตัวอย่างที่ 8 จากผลลัพธ์จากการสกัดคำในตัวอย่างที่ 7 เมื่อผ่านกระบวนการค้นคืน จะแสดงตัวอย่างผลลัพธ์จากการค้นคืนส่วนเอกสารมาตรฐานความมั่นคงดังรูปที่ 3.12 และตัวอย่างผลลัพธ์ที่ได้จากการค้นคืนแบบรูปความมั่นคง แสดงดังรูปที่ 3.13

No.	TiTle	Content	Similarity	Page No	Line No
1	10.3	10.3 System planning and acceptance	0.173913	54	31
2	9.1	9.1 Secure areas	0.173913	42	25
3	6.2	6.2 External parties	0.173913	27	19
4	13.1	13.1 Reporting information security events and weaknesses	0.173913	103	32
⋮	⋮	⋮	⋮	⋮	⋮

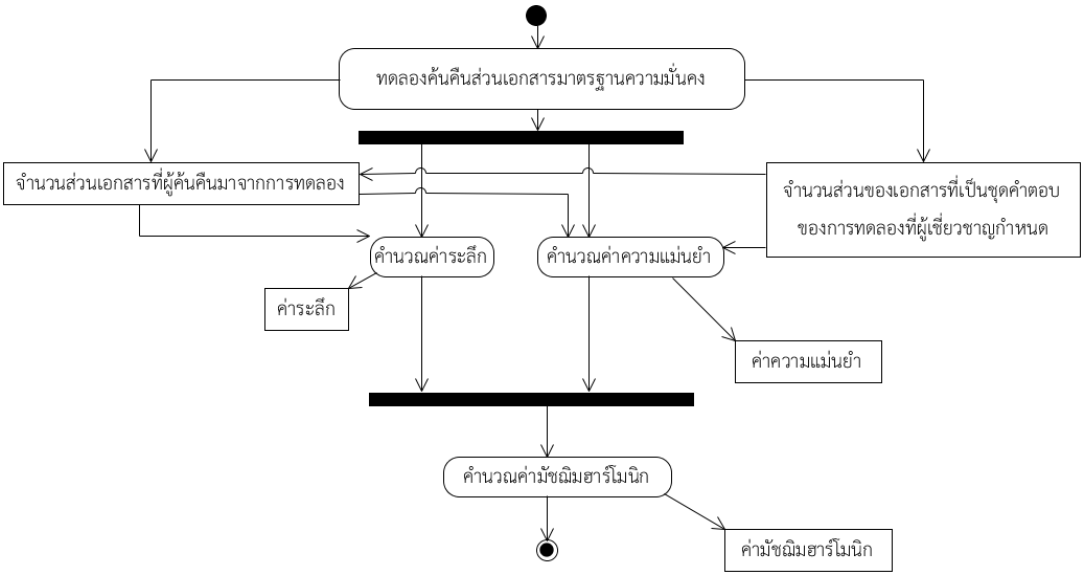
รูปที่ 3.12 ตัวอย่างผลลัพธ์ที่ได้จากการค้นคืนส่วนเอกสารมาตรฐานความมั่นคง

PID	Name	ExampleResolved	Variants	KnownUses	Consequences	...	See Also
SP1	Security Needs Identification for Enterprise Assets	This example solves...	—	Identification of enterprise assets and	SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89) has the followin...	...	After applying this assists in deciding how much protection is ....
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

รูปที่ 3.13 ตัวอย่างผลลัพธ์ที่ได้จากการค้นคืนแบบรูปความมั่นคง

3.2.3 การประเมินประสิทธิผลของระบบการค้นคืน

การประเมินประสิทธิผลของการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศนั้น ผู้วิจัยจะทำการประเมินจากผลที่ค้นคืนมาได้มีความถูกต้องและตรงกับที่ผู้เชี่ยวชาญต้องการหรือไม่ โดยทำการเปรียบเทียบโดยใช้จำนวนส่วนของเอกสารที่เป็นชุดคำตอบของการทดลองที่ผู้เชี่ยวชาญกำหนด เทียบได้ หรือ โดยในงานวิจัยนี้ได้ใช้การคำนวณ ค่าระลึก ค่าความแม่นยำและค่ามัชฌิมฮาร์โมนิก เป็นมาตรวัดประสิทธิผลของการค้นคืนของระบบการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง ดังแสดงในสมการที่ (5) ถึง (7) ตามลำดับ ดังแสดงลำดับการทำงานในแผนภาพกิจกรรมดังรูปที่ 3.14



รูปที่ 3.14 แผนภาพกิจกรรมการประเมินประสิทธิผลของระบบ

บทที่ 4

การพัฒนาเครื่องมือ

ในบทนี้จะกล่าวถึงรายละเอียดการพัฒนาเครื่องมือเพื่อใช้ในการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลสารสนเทศ โดยจะกล่าวถึงสถาปัตยกรรมของเครื่องมือและสภาพแวดล้อมที่ใช้ในการพัฒนาเครื่องมือ ซึ่งมีรายละเอียดดังนี้

4.1 ระบุกลุ่มผู้ใช้

จากการวิเคราะห์และประเมินความสามารถของเครื่องมือที่ได้พัฒนาขึ้น ผู้วิจัยจำแนกกลุ่มผู้ใช้งานออกเป็นสองกลุ่ม ดังต่อไปนี้

1) ผู้ใช้งานขั้นสุดท้าย (End User)

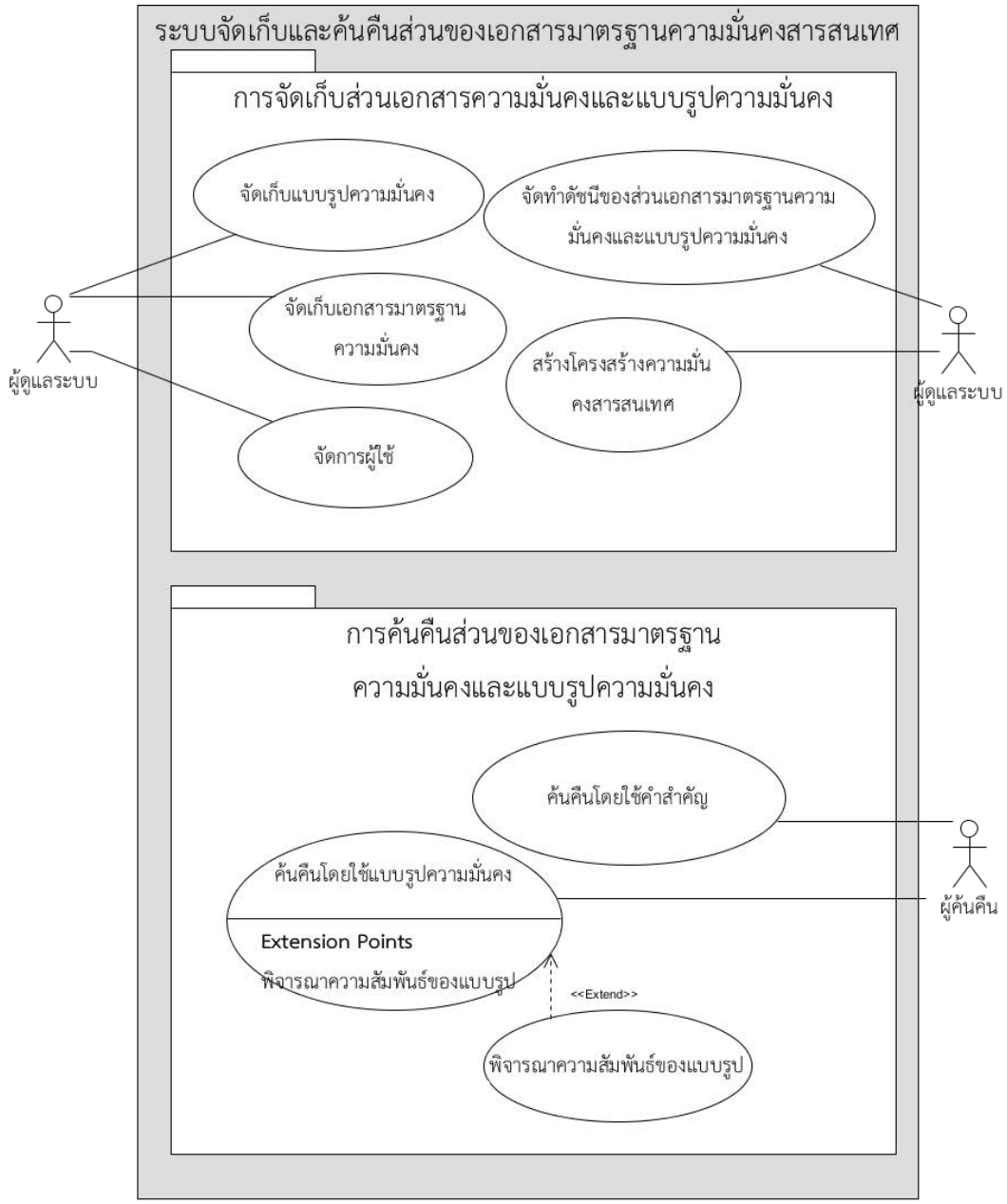
ผู้ใช้งานขั้นสุดท้าย คือ บุคคลใด ๆ ที่ใช้ค้นเครื่องมือค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศและข้อมูลแบบรูปความมั่นคง เพื่อนำผลลัพธ์ที่ได้จากการค้นคืนไปใช้ช่วยอำนวยความสะดวกในการศึกษานโยบายความมั่นคงสารสนเทศ

2) ผู้ดูแลระบบ (System Admin)

ผู้ใช้งานที่มีความรู้ความเชี่ยวชาญในเครื่องมือ ได้รับมอบหมายให้ดูแลและสามารถจัดการโครงสร้างและกระบวนการทำงานของเครื่องมือเป็นอย่างดี ผู้ดูแลระบบสามารถกำหนดสิทธิการเข้าใช้งานระบบของผู้ใช้ขั้นสุดท้าย

4.2 ความต้องการเชิงหน้าที่

ความต้องการเชิงหน้าที่ของระบบจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลสารสนเทศ อธิบายได้ด้วยแผนภาพยูสเคสของระบบดังรูปที่ 4.1



รูปที่ 4.1 ยูสเคสของระบบ

จากรูปที่ 4.1 ระบบการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงมีความต้องเชิงหน้าที่ดังนี้

1) ระบบต้องสามารถจัดเก็บแบบรูปความมั่นคงผ่านส่วนต่อประสานโดยจัดเก็บ เพื่อสร้างข้อมูลเบื้องต้นในการสร้างโครงสร้างข้อมูลความมั่นคงสารสนเทศ

2) ระบบต้องสามารถจัดเก็บเอกสารมาตรฐานความมั่นคงผ่านทางส่วนต่อประสานผู้ใช้แยกตามโครงสร้างของแบบรูปความมั่นคง

3) ระบบต้องสามารถจัดทำดัชนีจากส่วนเอกสารที่ได้จากกระบวนการจัดเก็บส่วนของเอกสารมาตรฐานความมั่นคง แบบรูปความมั่นคง และสามารถคำนวณหาค่าน้ำหนักของดัชนีได้

4) ระบบต้องสามารถสร้างโครงสร้างข้อมูลความมั่นคงสารสนเทศ ซึ่งรวมถึงทำหน้าที่ในการสกัดและหาค่าน้ำหนักของคำศัพท์ควบคุม เพื่อช่วยในการค้นคืน

5) ระบบต้องสามารถค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงและแบบรูปความมั่นคง โดยมีการขยายข้อคำถามการคำนวณความค่าความคล้ายคลึง ระหว่างตัวแทนของเอกสารกับข้อคำถาม และเรียงลำดับผลลัพธ์และนำเสนอผลลัพธ์ให้แก่ผู้ใช้

4.3 ความต้องการที่ไม่ใช่หน้าที่

ความต้องการที่ไม่ใช่หน้าที่เบื้องต้นของเครื่องมือค้นคืนส่วนเอกสารความมั่นคงสารสนเทศ มีทั้งหมด ความต้องการดังต่อไปนี้

1) ระบบต้องสามารถให้ผู้ดูแลระบบตรวจสอบการเข้าใช้ระบบของผู้ใช้ รวมถึงสิทธิ์การเข้าถึงในแต่ละส่วนของแต่ละประเภทผู้ใช้ กล่าวคือ ผู้ดูแลระบบสามารถจัดการหรือเข้าถึงได้ทุกส่วนของระบบ แต่สำหรับผู้ใช้ทั่วไป สามารถเข้าไปทำการค้นคืนได้เพียงอย่างเดียว

2) ระบบมีการแจ้งเตือนหากเกิดข้อผิดพลาดระหว่างใช้งาน

4.4 โครงสร้างของเครื่องมือ

4.4.1 สถาปัตยกรรมของเครื่องมือ

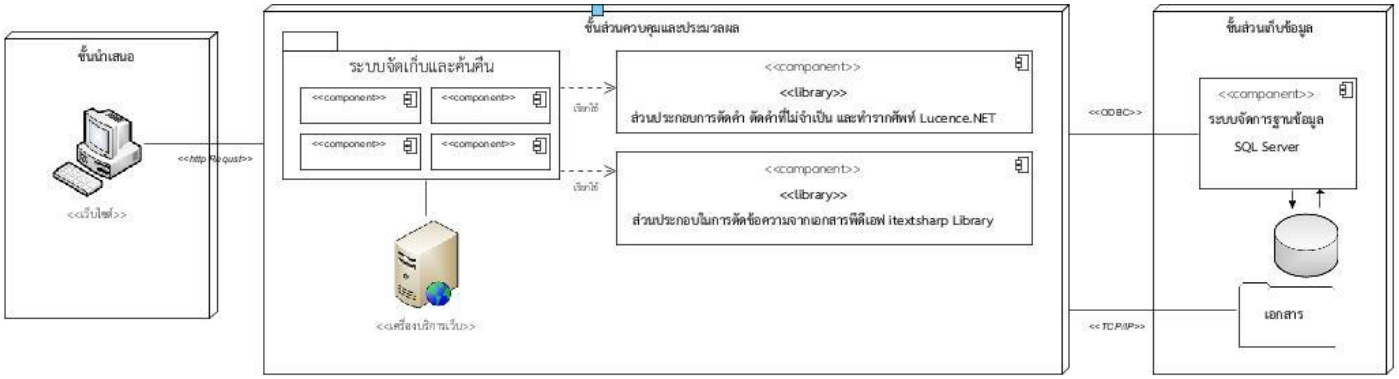
โครงสร้างของเครื่องมือที่พัฒนาขึ้น สำหรับจัดเก็บส่วนเอกสารมาตรฐานความมั่นคงโดยใช้แบบรูปความมั่นคงอธิบายได้ด้วยแผนภาพดีพลอยเมนต์ ซึ่งแสดงความสัมพันธ์ระหว่างส่วนประกอบต่าง ๆ ในระบบ จัดทำในงานวิจัยนี้ออกแบบตามหลักสถาปัตยกรรม 3 ชั้นส่วน (3-Teir) โดยแบ่งเป็น

1) ชั้นส่วนนำเสนอ เป็นส่วนที่ทำหน้าที่ต่อประสานกับผู้ใช้ระบบ พัฒนาในลักษณะโปรแกรมประยุกต์แบบเว็บ (Web-based Application) ทำหน้าที่เป็นส่วนต่อประสานกับผู้ใช้

2) ชั้นส่วนควบคุมและประมวลผล เป็นส่วนที่ทำหน้าที่ประมวลผลต่าง ๆ ตามที่กำหนด เช่น การจัดทำดัชนีเอกสาร, การสร้างโครงสร้างข้อมูลสารสนเทศ โดยมีส่วนประกอบภายนอกที่ถูกนำมาใช้ในการพัฒนาเครื่องมือในงานวิจัยนี้ส่วน ได้แก่ ส่วนประกอบโปรแกรมสำหรับการทำรากศัพท์

โดยขั้นตอนวิธีการของพอร์ตเตอร์ การทำดัชนี และขั้นตอนการตัดส่วนข้อความของเอกสารมาตรฐานความมั่นคง

3) ชั้นส่วนข้อมูล เป็นส่วนที่ใช้จัดเก็บข้อมูลต่าง ๆ ได้แก่ ส่วนของเอกสารมาตรฐานความมั่นคง แบบรูปความมั่นคง ดัชนีต่าง ๆ รวมถึงค่าน้ำหนักของดัชนี เป็นต้น แสดงดังรูปที่ 4.2



รูปที่ 4.2 แผนภาพดีพลอยเมนต์ของระบบ

4.4.2 สภาพแวดล้อมที่ใช้ในการพัฒนาเครื่องมือ

1) สภาพแวดล้อมที่ใช้ในการพัฒนาเครื่องมือด้านฮาร์ดแวร์

(1) หน่วยประมวลผล: Intel Core i5 รุ่นที่ 2 รหัส 2330M ความเร็ว 2.20 GHz แคช L3 ขนาด 3 MB

(2) ฮาร์ดดิสก์: 500GB ความเร็ว 5400 รอบต่อนาที

(3) แรม: 4GB แบบ DDR3 ความเร็วบัส 1333

(4) กราฟฟิกการ์ด: Intel HD Graphics 3000

2) สภาพแวดล้อมที่ใช้ในการพัฒนาเครื่องมือด้านซอฟต์แวร์

(1) ไมโครซอฟท์วิสชวลสตูดิโอ 2010 (Microsoft Visual Studio 2010) สำหรับพัฒนาเครื่องมือในการพัฒนาส่วนต่อประสานผู้ใช้ และสำหรับพัฒนาเครื่องมือต้นแบบทั้งหมด

(2) ไมโครซอฟท์เอสคิวแอลเมเนจเมนต์สตูดิโอ (Microsoft SQL Management Studio 2010) สำหรับจัดการข้อมูลในฐานข้อมูล

(3) ส่วนประกอบในการทำรากศัพท์ของขั้นตอนวิธีการของพอร์ตเตอร์ สำหรับการจัดทำรากศัพท์ ซึ่งงานวิจัยนี้ใช้จากเอพีไอหนึ่งของซอฟต์แวร์โอเพนซอร์ส อพาเชร์ ลูซีน ดอท เน็ต (Apache Lucence.NET) ซึ่งเป็นส่วนต่อประสานโปรแกรมประยุกต์ในการค้นคืนสารสนเทศ

(4) ส่วนประกอบในการตัดข้อความจากเอกสารพีดีเอฟ ซึ่งงานวิจัยนี้ใช้ไอเท็กซาร์(itextsharp Library) ซึ่งสนับสนุนการทำงานร่วมกับ ไมโครซอฟท์วิสชวลสตูดิโอ 2010

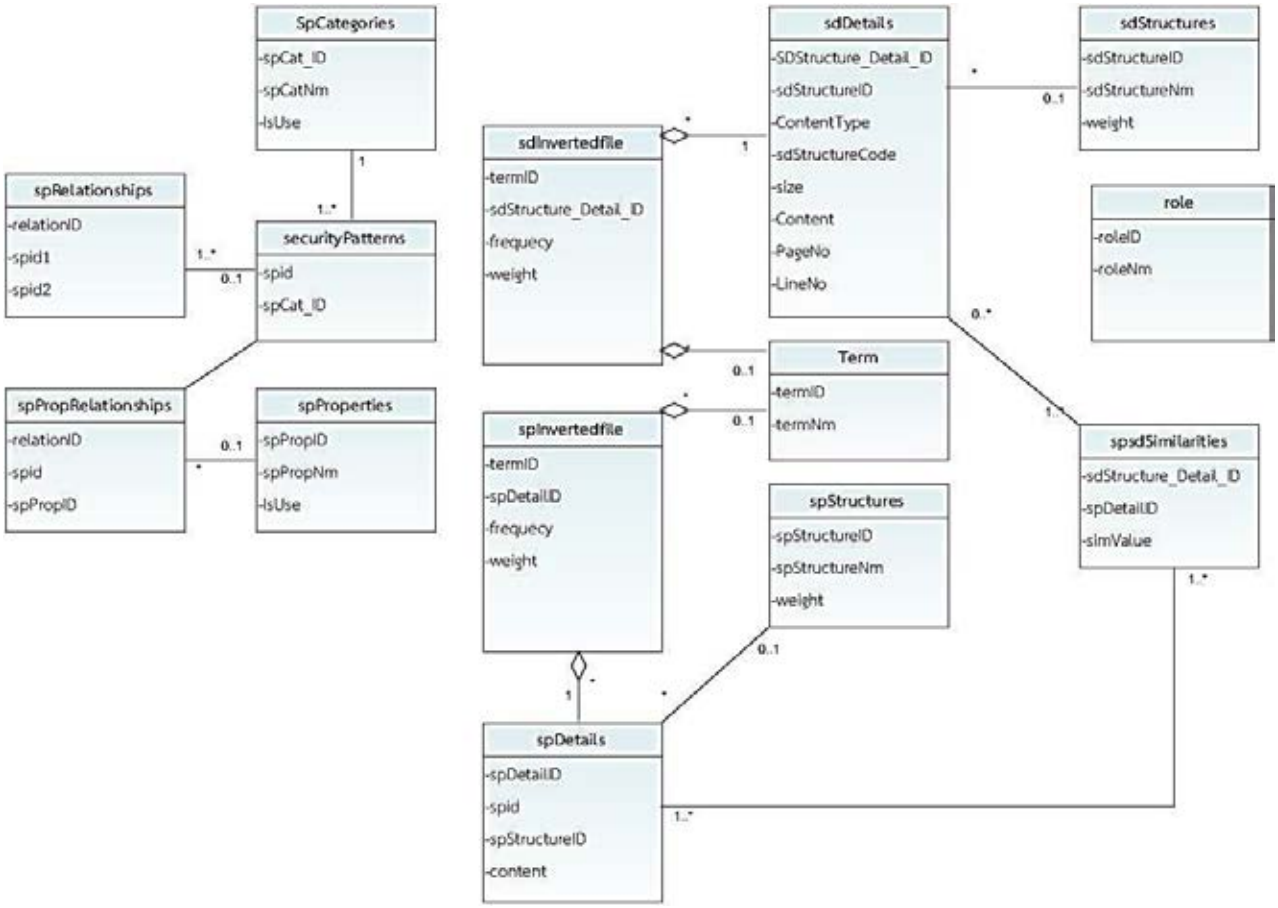
(5) ดิ อินเทอร์เน็ต เอกซ์โพลเรอร์ รุ่นที่ 9.0 (Internet Explorer Version 9)

(6) กูเกิลโครม (Google Chrome)

(7) ไมโครซอฟท์เวิร์ด (Microsoft word) และ ไมโครซอฟท์เอ็กเซส (Microsoft excel 2010)

4.4.3 การออกแบบแบบจำลองข้อมูล

ระบบจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลสารสนเทศ ผู้วิจัยออกแบบข้อมูลและโครงสร้างข้อมูลด้วยฐานข้อมูลเชิงสัมพันธ์ แสดงในแผนภาพแสดงความสัมพันธ์ของข้อมูลที่จัดเก็บ ในรูปที่ 4.3 และสามารถอธิบายแต่ละตารางดังตารางที่ 4.1 และ ภาคผนวก ค ตารงที่ ค.1-ค.13



รูปที่ 4.3 แผนภาพแสดงความสัมพันธ์ของข้อมูลที่จัดเก็บ

ตารางที่ 4.1 อธิบายตารางของระบบ

ตารางที่	ชื่อตาราง	คำอธิบาย
1	spProperties	จัดเก็บกลุ่มของคุณลักษณะด้านความมั่นคง
2	SpCategories	จัดเก็บกลุ่มของแบบรูปความมั่นคง
	securityPatterns	จัดเก็บความสัมพันธ์ระหว่างกลุ่มของแบบรูปและแบบรูป รวมทั้งน้ำหนักของแต่ละแบบรูป
3	spDetails	จัดเก็บรายละเอียดแบบรูปความมั่นคง
4	spRelationships	จัดเก็บความสัมพันธ์ระหว่างแบบรูปความมั่นคง
5	spStructures	จัดเก็บโครงสร้างของแบบรูปความมั่นคง
6	sdStructures	จัดเก็บโครงสร้างของเอกสารมาตรฐานความมั่นคง
7	sdDetails	จัดเก็บรายละเอียดของแต่ละส่วนเอกสารมาตรฐานความมั่นคง
8	spPropRelationships	จัดเก็บความสัมพันธ์ระหว่างแบบรูปกับคุณลักษณะด้านความมั่นคง

ตารางที่ 4.1 อธิบายตารางของระบบ (ต่อ)

ตารางที่	ชื่อตาราง	คำอธิบาย
9	Term	จัดเก็บดัชนีใด ๆ ที่ใช้ในระบบ
10	spInvertedfile	แฟ้มผกผันของแบบรูปความมั่นคง
11	sdInvertedfile	แฟ้มผกผันของส่วนของเอกสารมาตรฐานความมั่นคง
12	spsdSimilarities	จัดเก็บความค่าความคล้ายคลึงระหว่างแต่ละส่วนของเอกสารกับแต่ละแบบรูปความมั่นคง

4.5 การทำงานและส่วนต่อประสานผู้ใช้

ระบบจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมมั่นคงสารสนเทศโดยใช้แบบรูปความมั่นคง ประกอบด้วยหน้าจอหลัก ทั้งสิ้น 5 เมนู ดังรูปที่ 4.4 โดยรายละเอียดของแต่ละเมนูมีดังนี้

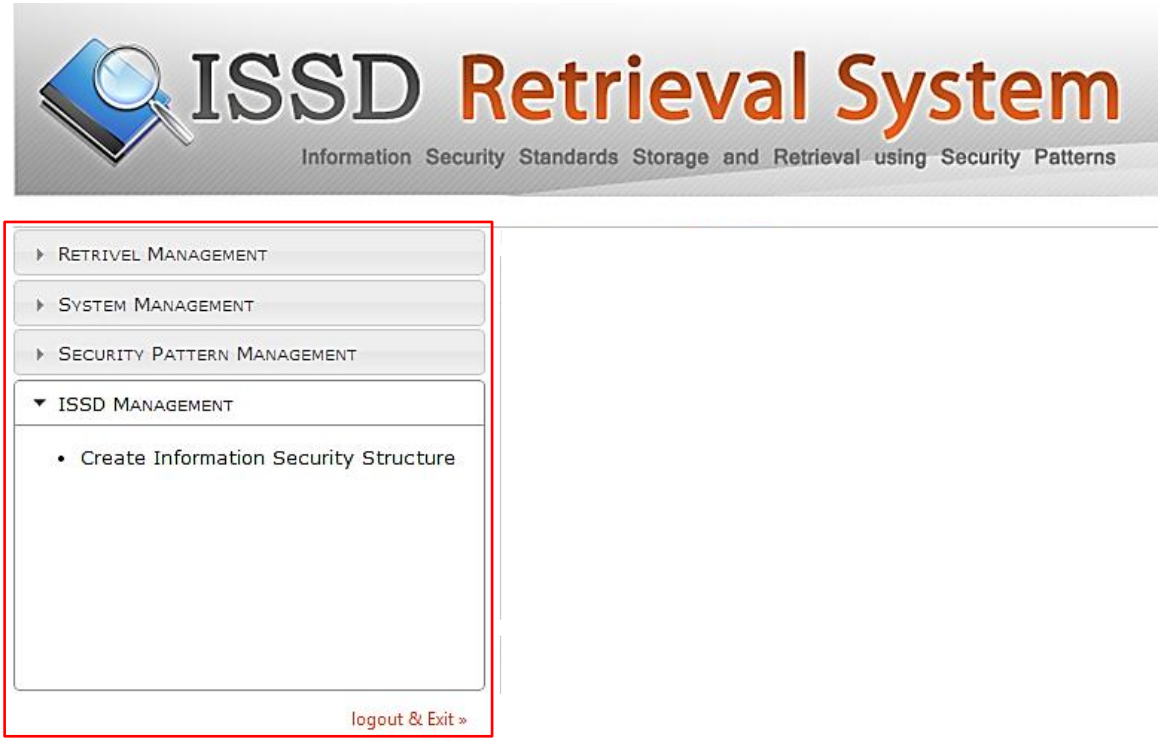
1) Security Pattern Management เป็นกลุ่มเมนูสำหรับการเพิ่ม ลบ แก้ไข แบบรูปความมั่นคง กลุ่มแบบรูปความมั่นคง รวมถึงคุณลักษณะด้านความมั่นคง

2) Retrieval System เป็นเมนูสำหรับการค้นคืน

3) System Management เป็นเมนูสำหรับผู้ดูแลระบบเท่านั้น โดยเป็นเมนูสำหรับการดูแลผู้ใช้ระบบ การนำเข้าเอกสารมาตรฐานความมั่นคงสารสนเทศ คำศัพท์และสัญลักษณ์ที่ไม่จำเป็นและการสั่งทำดัชนีของเอกสาร รวมทั้งส่วนจัดการกำหนดสิทธิ์การเข้าใช้ระบบ

4) ISSD Management เป็นเมนูสำหรับการสร้างโครงสร้างข้อมูลความมั่นคงสารสนเทศ

5) Logout & Exit เป็นเมนูสำหรับคำสั่งลงบันทึกออก หรือทำการออกจากโปรแกรม

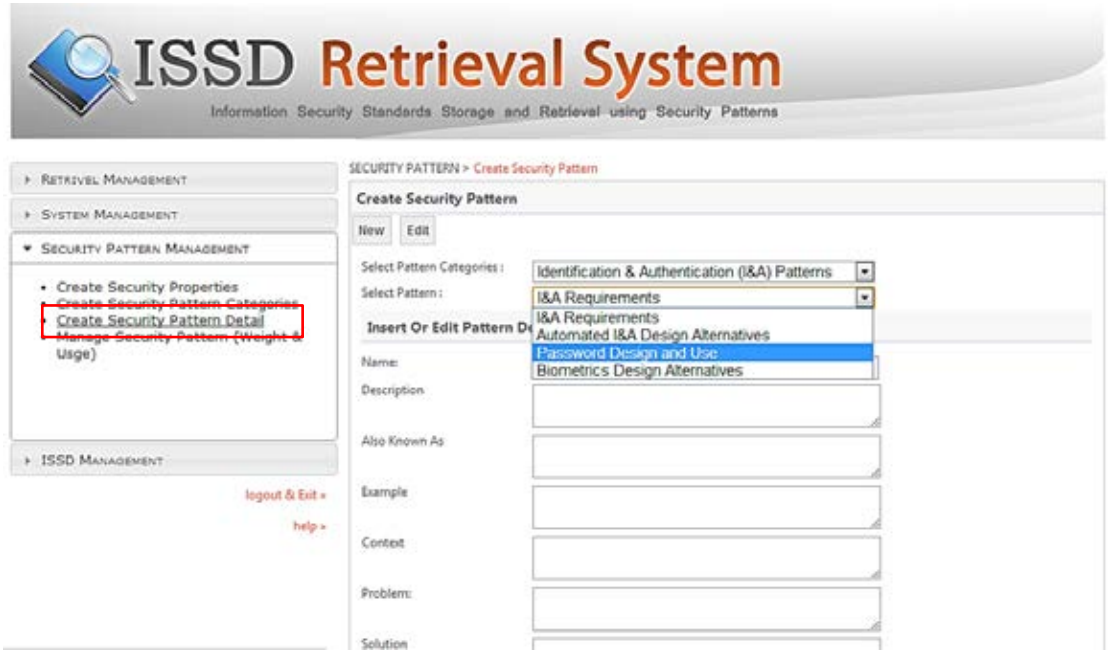


รูปที่ 4.4 เมนูหลักของเครื่องมือต้นแบบ

4.5.1 ส่วนการจัดเก็บแบบรูปความมั่นคง

ส่วนการจัดเก็บแบบรูปความมั่นคง ส่วนการเพิ่มแบบรูปความมั่นคงสู่ระบบสามารถทำได้โดย การเลือกที่เมนู “Security Pattern Management” และเลือก “Create Security Pattern Detail” ตามลำดับ โดยผู้ดูแลระบบจะสามารถเพิ่มแบบรูปความมั่นคงได้ ก็ต่อเมื่อมีการเพิ่มคุณลักษณะด้านความมั่นคง และกลุ่มของแบบรูปเข้าสู่ระบบแล้ว

หน้าจอการเพิ่มแบบรูปความมั่นคงจะมีตัวเลือกกลุ่มของแบบรูปความมั่นคง และช่องให้สำหรับใส่รายละเอียดแยกตามโครงสร้างของแบบรูปความมั่นคง โดยแสดงดังรูปที่ 4.5 หลังจากนั้นระบบจะนำข้อมูลที่ได้จากการบันทึกไปสร้างเป็นดัชนีของแบบรูปความมั่นคงต่อไป



รูปที่ 4.5 ส่วนการจัดเก็บแบบรูปความมั่นคง

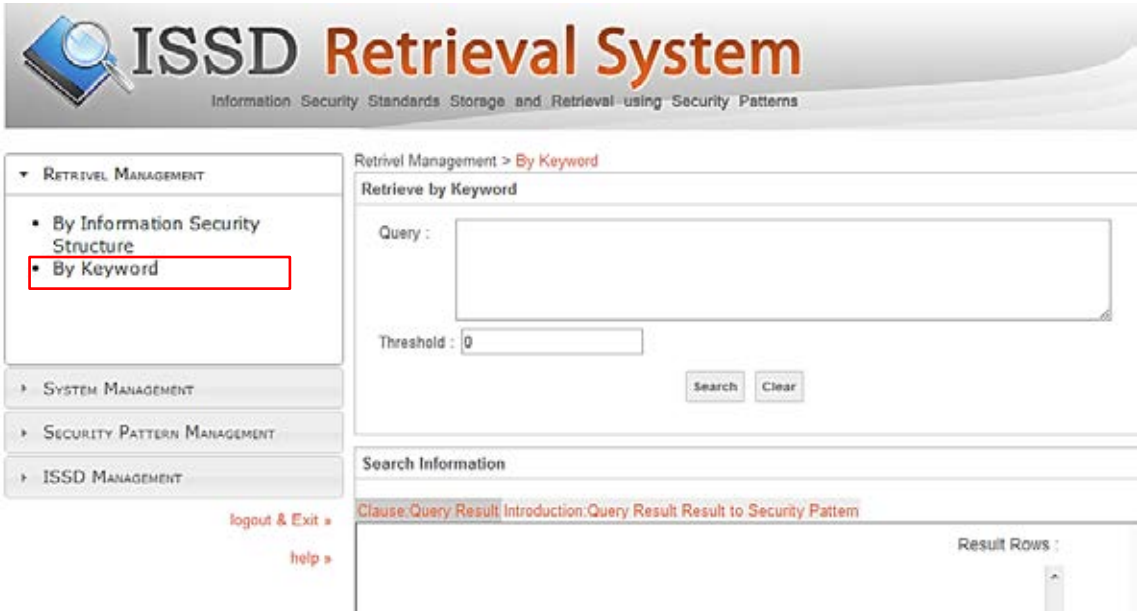
4.5.2 ส่วนการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง

ส่วนต่อประสานของในส่วนค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง โดยแบ่งออกเป็น 2 ส่วน คือส่วนการรับข้อคำถาม และส่วนการแสดงผล โดยแต่ละส่วนสามารถแบ่งออกเป็นส่วนต่าง ๆ ดังนี้

1) ส่วนรับข้อคำถาม ประกอบด้วย 2 แบบ ดังนี้

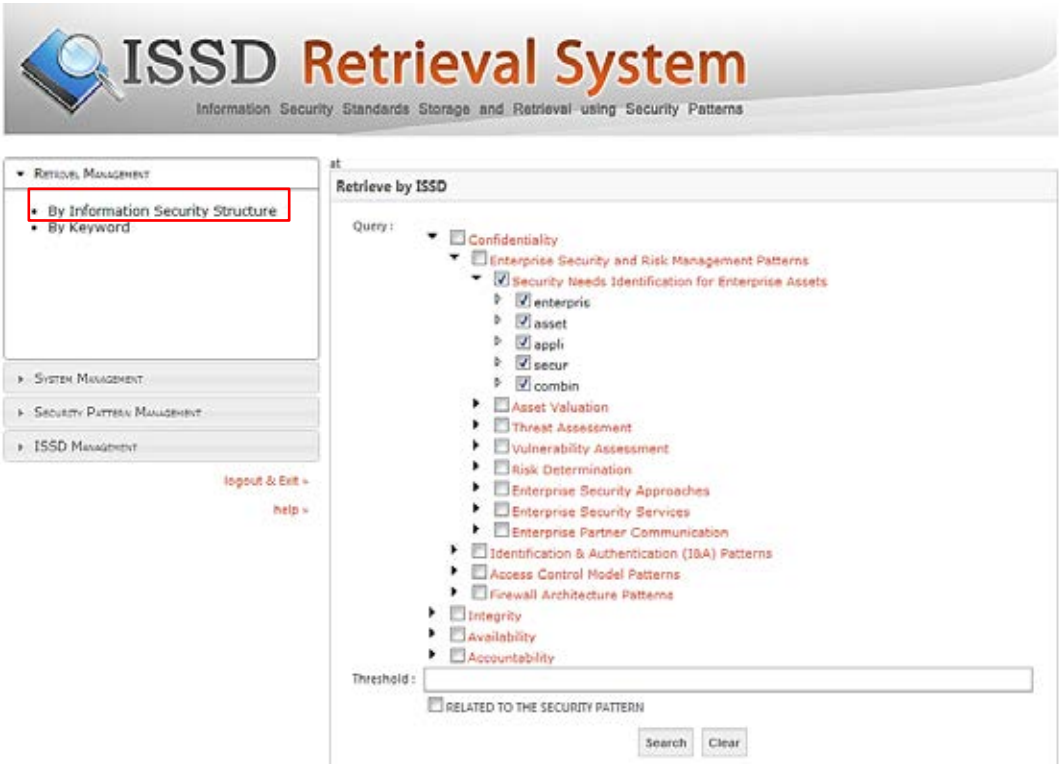
(1) ส่วนต่อประสานสำหรับค้นคืน

การค้นคืนส่วนเอกสารมาตรฐานโดยใช้คำสำคัญ สามารถทำได้โดย การเลือกที่เมนู “Retrieval System” และเลือก “By Keyword” ตามลำดับ โดยผู้ค้นคืนสามารถระบุข้อคำถามด้วยข้อความ หลังจากนั้นระบบจะจัดทำดัชนีข้อคำถามเพื่อใช้การค้นคืนต่อไป รวมทั้งผู้ใช้สามารถระบุค่าขีดแบ่งสำหรับแสดงคัดกรองผลลัพธ์ ดังรูปที่ 4.6



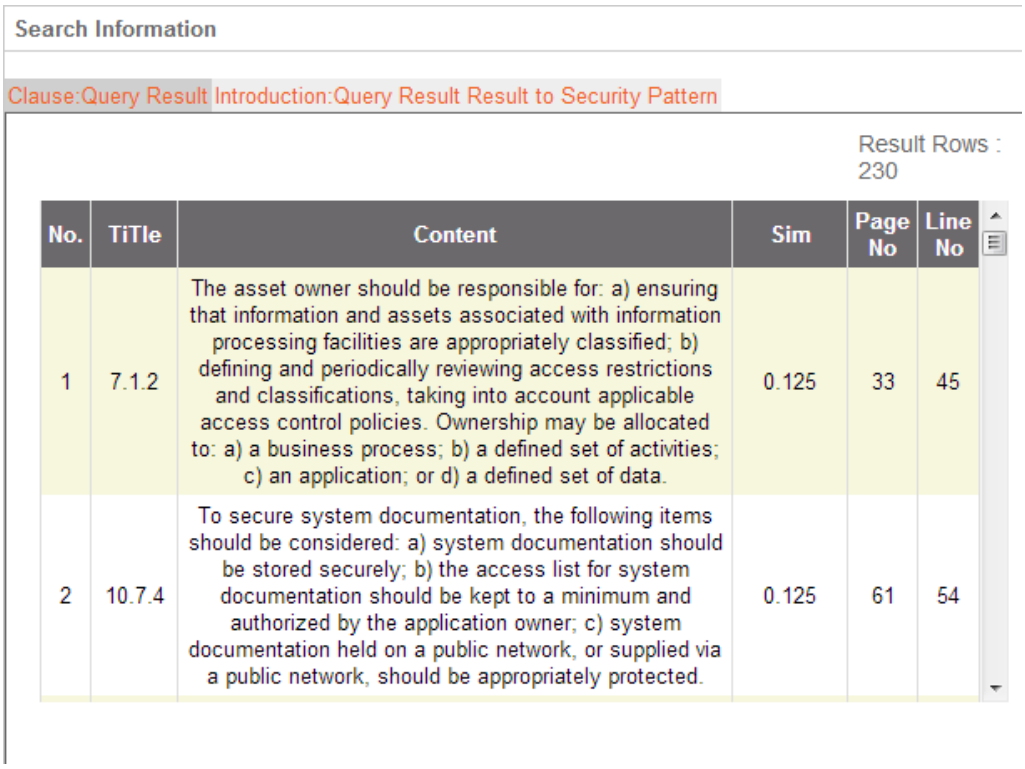
รูปที่ 4.6 ส่วนต่อประสานสำหรับค้นคืนส่วนเอกสารมาตรฐานโดยใช้คำสำคัญ

การค้นคืนส่วนเอกสารมาตรฐานโดยใช้แบบรูปความมั่นคงสามารถทำได้โดย การเลือกที่เมนู “Retrieval System” และเลือก “By Information Security Structure” ตามลำดับ โดยผู้ค้นคืนสามารถเลือกข้อคำถามตามหัวข้อของโครงสร้างด้วยข้อความ หลังจากนั้นระบบจะสร้างข้อคำถามจากโครงสร้างที่ผู้ใช้เลือกเพื่อนำไปหาดัชนีข้อคำถามเพื่อใช้การค้นคืนต่อไป รวมทั้งผู้ใช้สามารถระบุค่าขีดแบ่งสำหรับคัดกรองการแสดงผลลัพธ์ ดังรูปที่ 4.7



รูปที่ 4.7 ส่วนต่อประสานสำหรับการค้นคืนส่วนเอกสารมาตรฐานโดยใช้แบบรูปความมั่นคง

2) ส่วนแสดงผลลัพธ์ โดยส่วนแสดงผลลัพธ์จะสามารถเลือกดูส่วนของเอกสารความมั่นคงและแบบรูปความมั่นคง ที่มีความคล้ายคลึงกับผลลัพธ์ที่เลือกได้ รวมทั้งสามารถเลือกแสดงส่วนของเอกสารมาตรฐานความมั่นคงที่เกี่ยวเนื่องกับแบบรูปความมั่นคงแสดงในกระบวนการในหัวข้อที่ 3.1.1.2 ได้ ตัวอย่างผลลัพธ์แสดงดังรูปที่ 4.8



Search Information

Clause:Query Result Introduction:Query Result Result to Security Pattern

Result Rows : 230

No.	TiTle	Content	Sim	Page No	Line No
1	7.1.2	The asset owner should be responsible for: a) ensuring that information and assets associated with information processing facilities are appropriately classified; b) defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies. Ownership may be allocated to: a) a business process; b) a defined set of activities; c) an application; or d) a defined set of data.	0.125	33	45
2	10.7.4	To secure system documentation, the following items should be considered: a) system documentation should be stored securely; b) the access list for system documentation should be kept to a minimum and authorized by the application owner; c) system documentation held on a public network, or supplied via a public network, should be appropriately protected.	0.125	61	54

รูปที่ 4.8 ตัวอย่างผลลัพธ์ส่วนของเอกสารมาตรฐานความมั่นคงที่เกี่ยวข้อง

บทที่ 5

การทดสอบระบบและการประเมินผลการทำงานของระบบ

การทดสอบเครื่องมือต้นแบบในการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลสารสนเทศที่สร้างขึ้น มีเป้าหมายเพื่อจะทราบว่าเครื่องมือต้นแบบที่พัฒนาขึ้นมานั้นได้ถูกพัฒนาได้คุณภาพ กล่าวคือมีความถูกต้องและครบถ้วนตามที่ได้ระบุไว้ในขอบเขตและส่วนประกอบของแบบเครื่องมือหรือไม่ รวมถึงต้องการประเมินผลของการค้นคืนในวิธีต่าง ๆ ที่ได้นำเสนอไว้

5.1 การประเมินคุณภาพของเครื่องมือต้นแบบ

การประเมินคุณภาพของเครื่องมือต้นแบบ ในงานวิจัยนี้จะอ้างอิงปัจจัยจาก มาตรฐานไอเอสโอ 9126 [11] ซึ่งในงานวิจัยนี้จะใช้ทั้งสิ้น 2 ปัจจัย โดยระบุมาตรวัดของแต่ละปัจจัย ดังตารางที่ 5.1

ตารางที่ 5.1 มิติปัจจัยการประเมินคุณภาพและมาตรวัดที่ใช้

หน้าที่การทำงาน (Functionality)	ความเหมาะสม (Suitability)	ความครบถ้วนของฟังก์ชันการทำงานของเครื่องมือต้นแบบ รายละเอียดอยู่ในหัวข้อ 5.2
	ความถูกต้อง (Accuracy)	ความถูกต้องของฟังก์ชันการทำงานของเครื่องมือต้นแบบ ต้นแบบ รายละเอียดอยู่ในหัวข้อ 5.3

5.2 การทดสอบความครบถ้วนของฟังก์ชันการทำงานของเครื่องมือต้นแบบ

การทดสอบความครบถ้วนของฟังก์ชันการทำงานของเครื่องมือต้นแบบมีวัตถุประสงค์เพื่อทำการตรวจสอบเครื่องมือต้นที่ต้นแบบที่ผู้วิจัยพัฒนาขึ้น มีฟังก์ชันการทำงานถูกต้อง ครบถ้วนตามที่ได้

ออกแบบไว้ โดยจะทำการทดสอบฟังก์ชันงานต่าง ๆ แสดงรายการทดสอบฟังก์ชันงานดังตารางที่ 5.2

ตารางที่ 5.2 การทดสอบความครบถ้วนของฟังก์ชันการทำงานของเครื่องมือต้นแบบ

รายการทดสอบ	ผลการทดสอบ	หมายเหตุ
การเข้าใช้ระบบ		
กำหนดสิทธิ์การเข้าใช้ระบบ	ผ่าน	สำหรับผู้ดูแลระบบ
การจัดการแบบรูปความมั่นคง		
การจัดเก็บแบบรูปความมั่นคงตามโครงสร้าง	ผ่าน	สำหรับผู้ดูแลระบบ
การจัดเก็บลักษณะด้านความมั่นคง	ผ่าน	สำหรับผู้ดูแลระบบ
การจัดเก็บกลุ่มแบบรูปความมั่นคง	ผ่าน	สำหรับผู้ดูแลระบบ
แก้ไขแบบรูปความมั่นคง	ผ่าน	สำหรับผู้ดูแลระบบ
แก้ไขลักษณะความมั่นคง	ผ่าน	สำหรับผู้ดูแลระบบ
แก้ไขกลุ่มแบบรูปความมั่นคง	ผ่าน	สำหรับผู้ดูแลระบบ
ลบแบบรูปความมั่นคง	ผ่าน	สำหรับผู้ดูแลระบบ
ลบลักษณะความมั่นคง	ผ่าน	สำหรับผู้ดูแลระบบ
ลบกลุ่มแบบรูปความมั่นคง	ผ่าน	สำหรับผู้ดูแลระบบ
การจัดการส่วนของเอกสารมาตรฐาน		
การกำหนดค่าน้ำหนักของส่วนเอกสาร	ผ่าน	
การจัดเก็บและการค้นคืน		
การนำเข้าไฟล์คำและสัญลักษณ์คำละเว้น	ผ่าน	สำหรับผู้ดูแลระบบ
การจัดทำดัชนีของเอกสารมาตรฐาน	ผ่าน	สำหรับผู้ดูแลระบบ
การจัดการโครงสร้างข้อมูลสารสนเทศ	ผ่าน	

ตารางที่ 5.2 การทดสอบความครบถ้วนของฟังก์ชันการทำงานของเครื่องมือต้นแบบ (ต่อ)

รายการทดสอบ	ผลการทดสอบ	หมายเหตุ
การค้นคืนโดยใช้คำสำคัญ		ระบบแจ้งเตือนถ้ากรอกข้อมูลข้อคำถามและค่าขีดแบ่งไม่ครบ
การค้นคืนใช้โครงสร้างข้อมูลสารสนเทศ		ระบบแจ้งเตือนถ้าไม่เลือกหัวข้อข้อมูลข้อคำถามและกรอกค่าขีดแบ่งไม่ครบ

โดยผลจากการทดสอบความครบถ้วนดังที่ได้ทำการทดสอบฟังก์ชันงานในตารางที่ 5.1 โดยสรุปได้ว่าเครื่องมือต้นแบบในการจัดเก็บและรค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลสารสนเทศ ทำงานได้ถูกต้อง และครบถ้วนตามที่ได้ระบุไว้ในส่วนของการออกแบบโครงสร้างของเครื่องมือต้นแบบที่ได้กล่าวไว้ในบทที่ 4

5.3 การทดสอบความถูกต้องของฟังก์ชันการทำงานของเครื่องมือต้นแบบ

เป็นการตรวจสอบเครื่องมือต้นแบบได้ทำการออกแบบแล้วพัฒนามานั้น มีฟังก์ชันการทำงานถูกต้อง ครบถ้วนตามที่ได้ออกแบบและกำหนดความต้องการไว้หรือไม่ โดยในการทดสอบความถูกต้อง ในงานวิจัยนี้ใช้การทดสอบแบบกล่องดำ (Black Box Testing) ซึ่งแสดงตัวอย่างการทดสอบดังตารางที่ 5.3 -5.6

ตารางที่ 5.3 การทดสอบความถูกต้องของการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง

ชื่อระบบ	การค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง
ชื่อฟังก์ชัน	การค้นคืนส่วนของเอกสารมาตฐานความมั่นคงโดยใช้คำสำคัญ
รหัสกรณีทดสอบ	ISSDTC-01
ชื่อกรณีทดสอบ	ทดสอบการแสดงผลการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง
วัตถุประสงค์	เพื่อทดสอบการแสดงผลค้นคืนรายละเอียดส่วนของเอกสารที่ค้นคืนออกมาได้อย่างครบถ้วน
บทบาทผู้ใช้งานระบบ	กลุ่มผู้เชี่ยวชาญ และ กลุ่มผู้ใช้ทั่วไป
ข้อมูลนำเข้า	คำสำคัญในรูปแบบภาษาธรรมชาติ และ ค่าขีดแบ่งที่ผู้ใช้กำหนด
ผลลัพธ์ที่คาดหวัง	1) ผลลัพธ์ของระบบแบ่งเป็นสองกรณี 1.1) ค้นหาเจอผลลัพธ์ ระบบแสดงส่วนเอกสารความมั่นคงที่เรียงลำดับตามค่าความคล้ายคลึงจากมากไปน้อยโดยค่าที่แสดงต้องมีค่าความคล้ายคลึง

ตารางที่ 5.3 การทดสอบความถูกต้องของการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง (ต่อ)

	มากกว่าหรือเท่ากับค่าขีดแบ่งที่กำหนดไว้ 1.2) ค้นหาไม่เจอผลลัพธ์ ระบบแสดงข้อความเตือน “ไม่พบข้อมูลส่วนเอกสารความมั่นคง”
ผลการทดสอบ	การแสดงการค้นคืนรายละเอียดส่วนของเอกสารสามารถทำงานได้ถูกต้องครบถ้วน
สรุปผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน

ตารางที่ 5.4 การทดสอบความถูกต้องของการค้นคืนส่วนของเอกสารมาตฐานความมั่นคงโดยใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ

ชื่อระบบ	การค้นคืนส่วนของเอกสารมาตฐารความมั่นคง
ชื่อฟังก์ชัน	การค้นคืนส่วนของเอกสารมาตฐานความมั่นคงโดยใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ
รหัสกรณีทดสอบ	ISSDTC-02
ชื่อกรณีทดสอบ	ทดสอบการแสดงผลการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ
วัตถุประสงค์	เพื่อทดสอบการแสดงผลค้นคืนรายละเอียดส่วนของเอกสารที่ค้นคืนออกมาได้อย่างครบถ้วน
บทบาทผู้ใช้งานระบบ	กลุ่มผู้เชี่ยวชาญ และ กลุ่มผู้ใช้ทั่วไป
ข้อมูลนำเข้า	คำที่ได้จากการเลือกโครงสร้างข้อมูลสารสนเทศ และ ค่าขีดแบ่งที่ผู้ใช้กำหนด
ผลลัพธ์ที่คาดหวัง	1) ผลลัพธ์ของระบบแบ่งเป็นสองกรณี 1.1) ค้นหาเจอผลลัพธ์ ระบบแสดงส่วนเอกสารความมั่นคงที่เรียงลำดับตามค่าความคล้ายคลึงจากมากไปน้อยโดยค่าที่แสดงต้องมีค่าความคล้ายคลึงมากกว่าหรือเท่ากับค่าขีดแบ่งที่กำหนดไว้ 1.2) ค้นหาไม่เจอผลลัพธ์ ระบบแสดงข้อความเตือน “ไม่พบข้อมูลส่วนเอกสารความมั่นคง”

ตารางที่ 5.4 การทดสอบความถูกต้องของการค้นคืนส่วนของเอกสารมาตฐานความมั่นคงโดยใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ (ต่อ)

ผลการทดสอบ	การแสดงการค้นคืนรายละเอียดส่วนของเอกสารสามารถทำงานได้ถูกต้องครบถ้วน
สรุปผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน

ตารางที่ 5.5 การทดสอบความถูกต้องของการจัดทำดัชนีเอกสาร

ชื่อระบบ	การจัดทำดัชนีเอกสารมาตฐานความมั่นคง
ชื่อฟังก์ชัน	การจัดทำดัชนีเอกสารมาตฐานความมั่นคง
รหัสกรณีทดสอบ	ISSDTC-03
ชื่อกรณีทดสอบ	ทดสอบการผลการจัดทำดัชนีของเอกสารมาตฐานความมั่นคง
วัตถุประสงค์	เพื่อทดสอบการว่าระบบจัดทำดัชนีของคำที่ได้จากส่วนเอกสารที่นำเข้ามาได้อย่างถูกต้องและครบถ้วน
บทบาทผู้ใช้งานระบบ	ผู้ดูแลระบบ
ข้อมูลนำเข้า	ส่วนของเอกสารมาตรฐานความมั่นคงที่อยู่ในรูปแบบข้อความ
ผลลัพธ์ที่คาดหวัง	ดัชนีคำที่ผ่านการตัดคำและสัญลักษณ์ที่ไม่จำเป็นและการทำรากศัพท์ ความถี่ของดัชนี และค่าน้ำหนัก ที่สัมพันธ์กับส่วนของเอกสารมาตรฐานความมั่นคง
ผลการทดสอบ	ดัชนีที่ได้มีการตัดคำและทำรากศัพท์ที่ถูกต้อง และมีการคำนวณค่าความถี่และค่าน้ำหนักที่ถูกต้องตามสูตรการหาค่าน้ำหนักของ TF-IDF
สรุปผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน

ตารางที่ 5.6 การทดสอบความถูกต้องของการจัดเก็บแบบรูปความมั่นคง

ชื่อระบบ	การจัดเก็บแบบรูปความมั่นคง
ชื่อฟังก์ชัน	การบันทึกแบบรูปความมั่นคงตามโครงสร้างแบบรูปความมั่นคง
รหัสกรณีทดสอบ	ISSDTC-04
ชื่อกรณีทดสอบ	ทดสอบการบันทึกแบบรูปความมั่นคงตามโครงสร้างแบบรูปความมั่นคง
วัตถุประสงค์	เพื่อทดสอบว่าระบบบันทึกรายละเอียดแบบรูปความมั่นคงตามโครงสร้างแบบรูปความมั่นคงเข้าสู่ฐานข้อมูลเชิงสัมพันธ์ได้อยากถูกต้องและครบถ้วน

ตารางที่ 5.6 การทดสอบความถูกต้องของการจัดเก็บแบบรูปความมั่นคง (ต่อ)

บทบาทผู้ใช้งานระบบ	ผู้ดูแลระบบ
ข้อมูลนำเข้า	ชื่อกลุ่มของแบบรูปความมั่นคง รายละเอียดแบบรูปความมั่นคงที่อยู่ในรูปแบบข้อความ ที่ผู้ดูแลระบบกรอกตามโครงสร้าง
ผลลัพธ์ที่คาดหวัง	1) ผลลัพธ์ของระบบแบ่งเป็นสองกรณี 1.1) กรณีรายละเอียดแบบรูปความมั่นคงที่จำเป็นต้องระบุครบถ้วน ระบบแสดงข้อความเตือน “บันทึกข้อมูลแบบรูปความมั่นคงเรียบร้อยแล้ว” 1.2) กรณีรายละเอียดแบบรูปความมั่นคงที่จำเป็นต้องระบุไม่ครบถ้วน ระบบแสดงข้อความเตือน “ไม่สามารถบันทึกข้อมูลแบบรูปความมั่นคง กรุณากรอกข้อมูลให้ครบถ้วน”
ผลการทดสอบ	ระบบสามารถแบบรูปความมั่นคงตามโครงสร้างแบบรูปความมั่นคงได้อย่างถูกต้องครบถ้วน
สรุปผลการทดสอบ	☑ ผ่าน ☐ ไม่ผ่าน

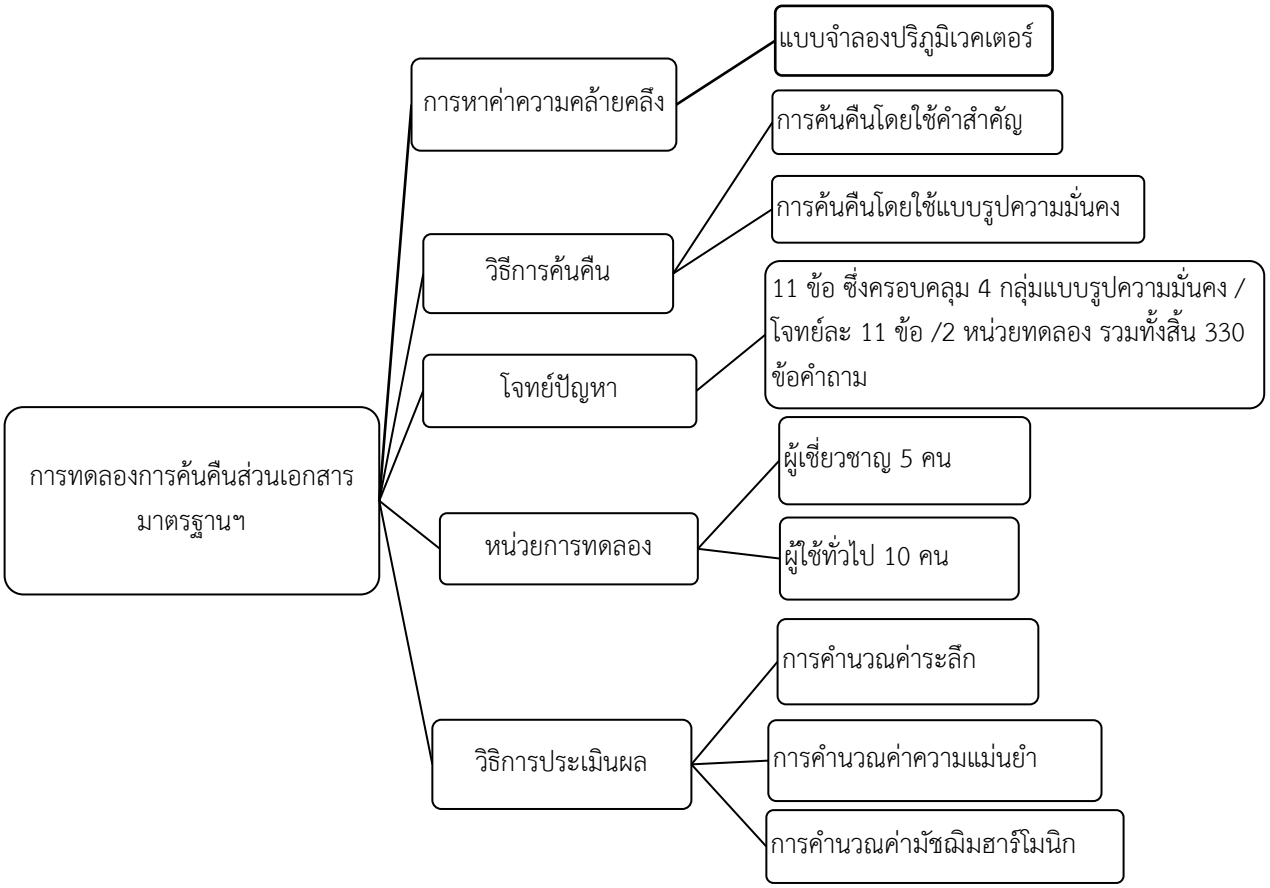
5.4 การทดลองเพื่อเปรียบเทียบผลจากการค้นคืน

5.4.1 วัตถุประสงค์ของการทดลอง

วัตถุประสงค์ของการทดลองนี้ เพื่อเปรียบเทียบผลการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ 2 วิธีการ โดยจะกล่าวถึงในหัวข้อ 5.2.4 โดยเปรียบเทียบหน่วยทดลองทั้งสิ้น 2 กลุ่ม คือผู้เชี่ยวชาญและผู้ใช้ทั่วไป ซึ่งจะอธิบายอย่างละเอียดในหัวข้อ 5.2.8 และจะใช้การคำนวณค่าระลึก ค่าความแม่นยำ และค่ามัชฌิมฮาร์โมนิก ในการเปรียบเทียบและสรุปผลการค้นคืน

5.4.2 วิธีการทดลอง

จากวัตถุประสงค์การทดลอง สามารถสร้างโครงสร้างการทดลองได้ดังรูปที่ 5.1



รูปที่ 5.1 แผนภาพกิจกรรมขั้นตอนการทดลอง

โดยในงานวิจัยนี้ได้กำหนดสิ่งแวดล้อมในการทดลองได้ดังต่อไปนี้

5.4.2.1 เอกสารมาตรฐานที่ทำมาใช้ในการทดลอง

เอกสารมาตรฐานที่ทำมาใช้ในการทดลอง คือส่วนเอกสารมาตรฐานไอเอสโอ/ไออีซี 27002 ที่ได้กล่าวไว้ในหัวข้อ การจัดเก็บส่วนเอกสารมาตรฐานความมั่นคง ในบทที่ 3 และ ส่วนของแบบรูปความมั่นคงได้นำมาจากหนังสือแบบรูปความมั่นคง การบูรณาการความมั่นคงและวิศวกรรมระบบของ M. Schumacher และคณะ โดยนำมาทั้งสิ้น 4 กลุ่ม แบบรูป จำนวน 20 แบบรูป ดังที่ได้กล่าวไว้ใน 1.3 ในหัวข้อขอบเขตของงานวิจัย รายละเอียดการรจัดเก็บที่ได้กล่าวไว้ในหัวข้อ การจัดเก็บแบบรูปความมั่นคง ในบทที่ 3

5.4.2.2 วิธีการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ

ในงานวิจัยนี้ผู้วิจัยได้ทำการพัฒนาเครื่องมือเพื่อใช้ในการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงตามความต้องการของผู้ใช้ โดยแบ่งเป็น 2 วิธีการ ได้แก่

1) วิธีการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้คำสำคัญ

2) วิธีการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ

5.4.2.3 โจทย์ปัญหาที่ใช้ในการทดลอง

โจทย์ปัญหาที่ใช้ในการทดลองเพื่อทำการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ งานวิจัยนี้ผู้วิจัยกำหนดโจทย์ปัญหาที่ใช้ในการทดลองสำหรับค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศมีทั้งหมด 11 ข้อ ดังแสดงดังตารางที่ ก.3 โดยออกแบบให้อยู่ในรูปแบบหัวข้อนโยบายหรือแนวปฏิบัติที่ต้องการศึกษาสำหรับมหาวิทยาลัย โดยการกำหนดโจทย์ครอบคลุมทั้งหมด 4 กลุ่มแบบรูปความมั่นคง ดังแสดงไว้ในตารางที่ ในภาคผนวก โดยผู้วิจัยได้เตรียมชุดคำตอบที่เกี่ยวข้องสำหรับแต่ละโจทย์จากกลุ่มผู้เชี่ยวชาญ เพื่อนำมาใช้ในการเปรียบเทียบกับชุดคำตอบที่ได้จากข้อคำถามที่ผู้ใช้ใช้ในการค้นคืนผ่านเครื่องมือต้นแบบที่ผู้วิจัยสร้างขึ้น เพื่อนำไปประเมินประสิทธิผลการค้นคืนต่อไป

5.4.2.4 ข้อคำถาม

ข้อคำถามที่ใช้ในการทดลองแบ่งออกเป็นสองกลุ่มคือข้อคำถามจากกลุ่มผู้ค้นคืนที่เป็นผู้เชี่ยวชาญและผู้ใช้ทั่วไป โดยข้อคำถามจะตอบโจทย์ข้อคำถามทั้ง 11 ข้อภายในแต่ละกลุ่ม

เมื่อนำข้อคำถามไปใช้ค้นคืนผ่านเครื่องมือที่ผู้วิจัยได้จัดทำขึ้น จะได้รายการของผลลัพธ์เพื่อนำไปเทียบกับชุดคำตอบของโจทย์ในแต่ละโจทย์ที่กำหนดไว้ เพื่อนำไปคำนวณค่าระลึก ค่าความแม่นยำ และค่ามัชฌิมฮาร์โมนิก รวมถึงทำการจัดเก็บลำดับที่พบเอกสารที่ตรงกับชุดคำตอบเพื่อใช้ในการประเมินต่อไป

5.4.2.5 เส้นขีดแบ่งความคล้าย

ค่าเส้นขีดแบ่งความคล้าย (Similarity Threshold) ที่ใช้ในการทดลองนี้มาเพื่อคัดกรองผลลัพธ์ที่ต้องการ โดยทำการค้นคืนเอกสารออกมาได้ต้องค่าคล้ายคลึงมากกว่าหรือเท่ากับเส้นขีดแบ่ง

ความคล้าย โดยเส้นขีดแบ่งความคล้ายสามารถหาได้จากค่าเฉลี่ยของค่าคล้ายคลึงของเอกสารที่ได้จากข้อคำถาม ลบด้วยค่าเบี่ยงเบนมาตรฐาน ดังแสดงในสมการที่ 10

ค่าขีดแบ่งเริ่มต้นความคล้าย = ค่าเฉลี่ย – ค่าเบี่ยงเบนมาตรฐาน (10)

5.4.2.6 หน่วยทดลอง

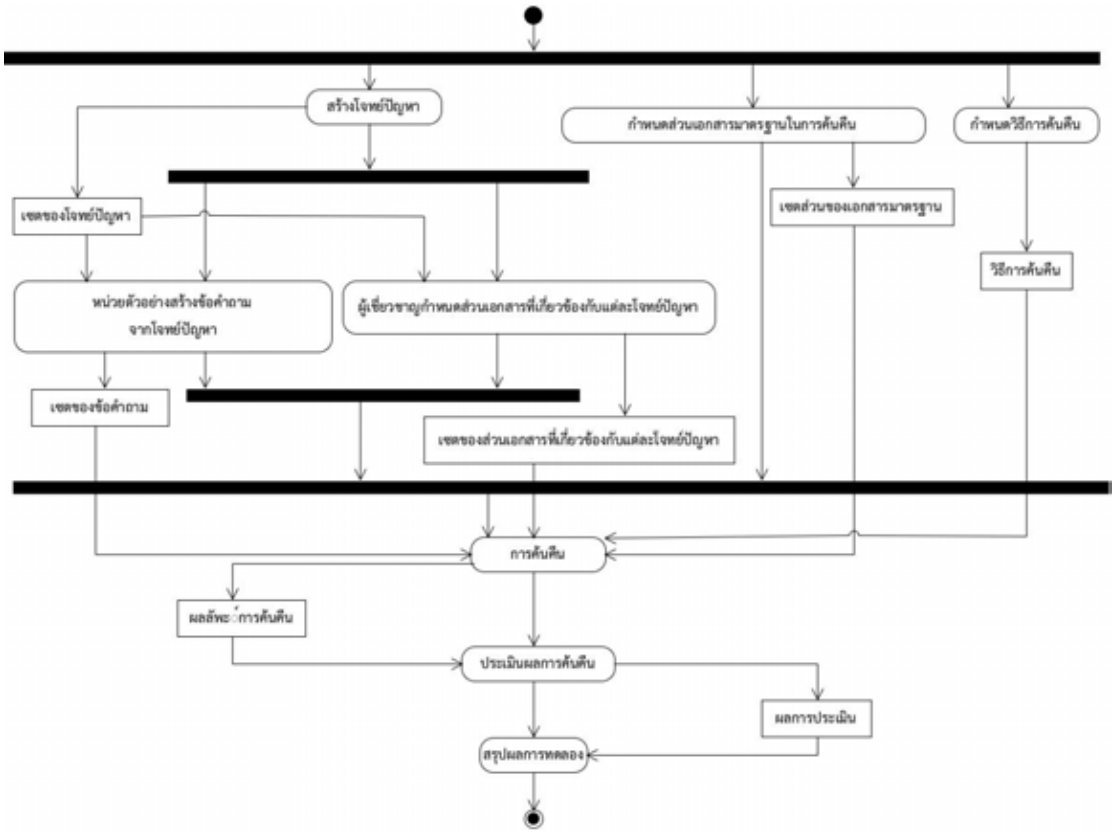
ในการเปรียบเทียบการค้นคืนเอกสารมาตรฐานความมั่นคงสารสนเทศ ในการทดลองนี้ทดลองผู้วิจัยแบ่งหน่วยเป็น 2 กลุ่ม ดังแสดงในตารางที่ 5.2 เพื่อเปรียบเทียบการค้นคืนจากสองวิธีการค้นคืน โดยทั้งสองกลุ่มทำโจทย์ปัญหาเดียวกันในทั้งสองวิธี

ตารางที่ 5.7 กลุ่มหน่วยทดลอง

หน่วยทดลอง	คุณสมบัติ	จำนวนคน
ผู้เชี่ยวชาญ	มีประสบการณ์ด้านการทำงานในด้านความมั่นคงมากกว่า 10 ปี หรือได้รับการรับรองประกาศนียบัตรวิชาชีพด้านความมั่นคงสารสนเทศ	5
ผู้ใช้ทั่วไป	บุคคลทั่วไปที่ทำงานที่มีการใช้เทคโนโลยีสารสนเทศในมหาวิทยาลัย	10

5.4.2.7 ขั้นตอนการทดลอง

ขั้นตอนการทดลองสำหรับค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ แสดงในแผนภาพกิจกรรมที่แสดงในรูปที่ 52



รูปที่ 5.2 แผนภาพกิจกรรมการทดลองสำหรับค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ

จากรูปที่ 5.2 แสดงขั้นตอนทดลองสำหรับค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ โดยมีรายละเอียดแต่ละขั้นตอนดังนี้

1) สร้างโจทย์ปัญหาเพื่อใช้ทดลองในการค้นคืน

2) ผู้เชี่ยวชาญกำหนดส่วนเอกสารที่เกี่ยวข้องกับโจทย์ปัญหาแต่ละข้อ

3) ให้แต่ละหน่วยทดลองทำการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดย ใช้คำสำคัญ)

4) ระบบแสดงผลลัพธ์การค้นคืนโดยไม่พิจารณาแบบรูปเพื่อนำไปเปรียบเทียบกับชุดคำตอบเพื่อนำไปใช้ในการคำนวณเปรียบเทียบเพื่อประเมินผลต่อไป

5) ให้หน่วยทดลองเดิมใช้โจทย์ปัญหาเดิม ในการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลสารสนเทศ

6) ระบบแสดงผลลัพธ์การค้นคืนโดยพิจารณาแบบรูปความมั่นคงที่ใช้ เพื่อนำไปเปรียบเทียบกับชุดคำตอบเพื่อนำไปใช้ในการคำนวณเปรียบเทียบเพื่อประเมินผลต่อไป

7) นำผลการประเมินมาสรุปผลการทดลอง

5.5 ตัวอย่างการทดลองและประเมินผลการทดลอง

ผู้วิจัยจะยกตัวอย่างเพื่อให้เห็นขั้นตอนการทดลองมายิ่งขึ้น โดยจะยกตัวอย่างจากการทำการทดลองจากหน่วยทดลองจำนวนหนึ่งในการค้นคืนส่วนเอกสารมาตรฐานความมั่นคง

1) โจทย์ปัญหา : แนวทางปฏิบัติการจัดการทรัพย์สินสารสนเทศ

2) คำอธิบายโจทย์ปัญหา : การจัดการทรัพย์สินสารสนเทศ (Information Asset Management) กำหนดขึ้นเพื่อป้องกันทรัพย์สินสารสนเทศของมหาวิทยาลัยให้เกิดความมั่นคง และสามารถใช้งานทรัพย์สินได้อย่างเหมาะสม

3) ตัวอย่างส่วนเอกสารที่เกี่ยวข้องจากผู้เชี่ยวชาญ แสดงดังตารางที่ 5.8

4) ข้อคำถามและการสร้างข้อคำถามใหม่ แสดงดังตารางที่ 5.9

ตารางที่ 5.8 ตัวอย่างส่วนเอกสารที่เกี่ยวข้องที่ระบุโดยผู้เชี่ยวชาญ

รหัสโครงสร้าง	ประเภทของส่วนของเอกสาร	ความเกี่ยวข้อง [เกี่ยว =1,ไม่เกี่ยว 0]
6	Chapter	1
6.1	TiTle	1
6.1	Objective	1
6.1.1	SubTiTlle	1
6.1.1	Control	1
:	:	:
:	:	:
:	:	:
10	Chapter	0
10.1	TiTle	0

ตารางที่ 5.9 ตัวอย่างข้อคำถามและการขยายข้อคำถาม

ลำดับ	ข้อคำถาม	วิธีการค้นคืน	คำสำคัญที่ได้จากข้อคำถาม
ข้อคำถาม 1	Information asset management protect security proper	คำสำคัญ	asset inform manag proper protect secur
ข้อคำถาม 2	Information asset management	คำสำคัญ	asset inform manage
ข้อคำถาม 3	Security Needs Identification for Enterprise Assets enterpris asset appli secur combin Asset Valuation enterpris control asset assess determin Risk Determination determin evalu risk	โครงสร้างข้อมูลความมั่นคงสารสนเทศ (ต่อ)	appli assess asset control determin enterpri enterpris evalu identif need risk secur valuat
ข้อคำถาม 4	Confidentiality Identification & Authentication (I&A) Patterns Password Design and Use design administr password 192 229 Biometrics Design Alternatives altern design addit 241 biometr I&A Requirements also authent determin appli altern	โครงสร้างข้อมูลความมั่นคงสารสนเทศ	addit administr also altern appli authent biometr confidenti design i&a identif password pattern requir us

ตารางที่ 5.9 ตัวอย่างข้อคำถามและการขยายข้อคำถาม (ต่อ)

ลำดับ	ข้อคำถาม	วิธีการค้นคืน	คำสำคัญที่ได้จากข้อคำถาม
	Biometrics Design		

เมื่อนำโจทย์ปัญหา ข้อคำถามและส่วนเอกสารที่เกี่ยวข้องจากผู้เชี่ยวชาญ มาทำการทดลองโดยใช้วิธีการค้นคืนจากหัวข้อที่ 5.2.2.7 ผลลัพธ์ที่ได้ทำการประเมินผลการทดลองโดยใช้มาตรวัดทั้ง 3 อันได้แก่ ค่าระลึก (R) ค่าความแม่นยำ (P) และค่ามัชฌิมฮาร์โมนิก (H) แสดงผลการประเมินดังแสดงในตารางที่ 5.6

ตารางที่ 5.10 ตัวอย่างผลการทดลองที่ได้จากการทดลอง

ข้อคำถาม	มาตรวัดประสิทธิผลการค้นคืน		
	R	P	H
1	0.490	0.912	0.638
2	0.572	0.933	0.706
3	0.2896	0.9186	0.440
4	0.593	0.914	0.720

5.6 การประเมินผลการทดลอง

ผลการทดลองจากการที่ได้ทำการทดลองการค้นคืนความต้องการความมั่นคงสำหรับค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศจาก 2 กลุ่มหน่วยทดลอง โดยใช้ข้อคำถามที่ได้ระบุไว้ใน ภาคผนวก ข ที่ได้นำผลที่ได้จากการทำการทดลองมาทำการคำนวณค่าระลึก (R) ค่าความแม่นยำ (P) ที่ได้จากแต่ละข้อคำถามไว้ในภาคผนวก ก ซึ่งค่าเฉลี่ยของผลการทดลองที่ได้ทำการทดลองสำหรับค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศของผู้ใช้ทั่วไปจะแสดงในตารางที่ 5.3 และค่าเฉลี่ยของผลการทดลองที่ได้ทำการทดลองสำหรับค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศของจะแสดงในตารางที่ 5.11

ตารางที่ 5.11 เปรียบเทียบผลการทดลองโดยใช้ ค่าระลึก ค่าความแม่นยำ และค่ามัชฌิมฮาร์โมนิกสำหรับผู้ใช้ทั่วไป

วิธีการ	ใช้คำสำคัญ			ใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ			อัตราการเปลี่ยนแปลง(%)		
โจทย์	R	P	H	R	P	H	R	P	H
Q1	0.192	0.946	0.301	0.710	0.920	0.800	**+269.866**	**-2.686**	**+165.993**
Q2	0.285	0.942	0.401	0.730	0.935	0.819	**+156.042**	**-0.745**	**+104.410**
Q3	0.123	0.568	0.191	0.710	0.501	0.587	**+478.743**	**-11.803**	**+207.465**
Q4	0.090	0.668	0.141	0.655	0.473	0.548	**+629.131**	**-29.250**	**+288.053**
Q5	0.089	0.747	0.147	0.527	0.639	0.553	**+492.838**	**-14.488**	**+275.720**
Q6	0.092	0.640	0.145	0.581	0.573	0.559	**+531.767**	**-10.506**	**+286.421**
Q7	0.100	0.386	0.139	0.813	0.461	0.580	**+713.199**	**19.186**	**+316.275**
Q8	0.161	0.388	0.204	0.604	0.278	0.357	**+275.236**	**-28.491**	**+74.881**
Q9	0.042	0.746	0.074	0.422	0.644	0.453	**+907.233**	**-**	**+513.046**

ตารางที่ 5.11 เปรียบเทียบผลการทดลองโดยใช้ ค่าระลึก ค่าความแม่นยำ และค่ามัชฌิมฮาร์โมนิก สำหรับผู้ใช้ทั่วไป (ต่อ)

วิธีการ	ใช้คำสำคัญ			ใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ			อัตราการเปลี่ยนแปลง(%)		
โจทย์	R	P	H	R	P	H	R	P	H
								13.609	
Q10	0.233	0.666	0.316	0.777	0.610	0.680	**+233.228**	**-8.395**	**+115.027**
Q11	0.171	0.681	0.265	0.639	0.661	0.585	**272.651**	**-2.906**	**+120.894**
ค่าเฉลี่ย	**0.143**	**0.671**	**0.211**	**0.652**	**0.609**	**0.593**	**+354.260**	**-9.270**	**+180.620**

R = ค่าระลึก, P = ค่าความแม่นยำ,H=ค่ามัชฌิมฮาร์โมนิก ,โจทย์ปัญหาอ้างอิงจากตารางที่ ก.2

ตารางที่ 5.12 เปรียบเทียบผลการทดลองโดยใช้ ค่าระลึก ค่าความแม่นยำ และค่ามัชฌิมฮาร์โมนิก สำหรับผู้เชี่ยวชาญ

วิธีการ	ใช้คำสำคัญ			ใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ			อัตราการเปลี่ยนแปลง(%)		
โจทย์	R	P	H	R	P	H	R	P	H
Q1	0.374	0.918	0.527	0.598	0.925	0.725	**+59.725**	**+0.692**	**+37.527**
Q2	0.284	0.934	0.429	0.594	0.942	0.693	**+109.242**	**+0.869**	**+61.501**
Q3	0.214	0.536	0.302	0.573	0.502	0.503	**+168.102**	**-6.353**	**+66.443**
Q4	0.189	0.549	0.278	0.554	0.464	0.497	**+192.404**	**-15.487**	**78.667**
Q5	0.263	0.668	0.374	0.531	0.636	0.559	**+101.893**	**-4.897**	**+49.719**
Q6	0.247	0.717	0.363	0.464	0.578	0.477	**+88.410**	**-19.415**	**+31.468**
Q7	0.287	0.384	0.327	0.788	0.472	0.560	**+174.207**	**23.036**	**71.255**
Q8	0.287	0.355	0.317	0.573	0.278	0.362	**+99.475**	**-21.639**	**14.180**
Q9	0.219	0.689	0.329	0.567	0.585	0.574	**+158.793**	**-15.104**	**+74.323**

ตารางที่ 5.12 เปรียบเทียบผลการทดลองโดยใช้ ค่าระลึก ค่าความแม่นยำ และค่ามัชฌิมฮาร์โมนิก สำหรับผู้เชี่ยวชาญ (ต่อ)

วิธีการ	ใช้คำสำคัญ			ใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ			อัตราการเปลี่ยนแปลง(%)		
โจทย์	R	P	H	R	P	H	R	P	H
Q10	0.489	0.689	0.559	0.807	0.610	0.693	**+64.933**	**-11.478**	**+24.121**
Q11	0.300	0.663	0.409	0.734	0.662	0.641	**+144.391**	**-0.289**	**+56.688**
ค่าเฉลี่ย	**0.287**	**0.646**	**0.383**	**0.617**	**0.605**	**0.571**	**+115.051**	**-6.334**	**+49.138**

R = ค่าระลึก, P = ค่าความแม่นยำ, H=ค่ามัชฌิมฮาร์โมนิก ,โจทย์ปัญหาอ้างอิงจากตารางที่ ก.2

จากตารางที่ 5.3 และ 5.4 จากผลการเปรียบเทียบจาการค้นคืนทั้งสองวิธี จาก 2 กลุ่มหน่วยทดลอง พบว่า ทั้งสองกลุ่มมีแนวโน้มการเพิ่มขึ้นและลดลงของค่าระลึก ค่าความแม่นยำ และค่าฮาร์โมนิค ไปในทิศทางเดียวกัน คือการค้นคืนโดยใช้แบบรูปความมั่นคง ได้ค่าเฉลี่ยค่าระลึกและค่ามัชฌิมฮาร์โมนิกที่เพิ่มมากขึ้นในข้อโจทย์ปัญหาส่วนใหญ่ เนื่องจาก การใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศที่สร้างขึ้น ทำให้ได้ข้อคำถามที่สร้างจากความสัมพันธ์ระหว่างคำศัพท์ควบคุม ลักษณะของความมั่นคง และชื่อกลุ่มแบบรูป เมื่อผ่านกระบวนการจัดทำดัชนีข้อคำถามจึงได้คำสำคัญใช้ในการค้นคืนที่เยอะมากขึ้น ทำให้ได้ผลลัพธ์ที่ครอบคลุมมากขึ้น แต่ขณะเดียวกันค่าเฉลี่ยความแม่นยำกลับมีอัตราการลดลง เนื่องจากการค้นคืนด้วยคำสำคัญทำให้ได้ใชดัชนีข้อคำถามที่มีความเจาะจงสูงกว่าการใช้โครงสร้าง ทำให้ส่วนเอกสารที่ถูกดึงออกมาสวนใหญ มักจะเปนเอกสารที่เกี่ยวข้องกับข้อคำถาม ซึ่งจากโจทย์ปัญหาทั้ง 11 ข้อ การค้นคืนด้วยการใช้แบบรูปความมั่นคงให้ค่าระลึกและค่ามัชฌิมฮาร์โมนิกของการค้นคืนเพิ่มมากขึ้น แต่จะเสียความแม่นยำไปเล็กน้อย และค่าระลึก ความแม่นยำเฉลี่ย และค่ามัชฌิมฮาร์โมนิกที่ได้จากทั้งสองกลุ่มหน่วยทดลองมีค่ามากกว่า 0.6 ซึ่งถือว่าการค้นคืนมีประสิทธิผลดี

ตารางที่ 5.13 เปรียบเทียบผลการทดลองโดยใช้ ค่าระลึก ค่าความแม่นยำและค่ามัชฌิมฮาร์โมนิกจาก 2 กลุ่มหน่วยทดลอง

วิธีการ	ใช้คำสำคัญ			ใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ			อัตราการเปลี่ยนแปลง(%)		
มาตรวัด	R	P	H	R	P	H	R	P	H
1.กลุ่มผู้ใช้ทั่วไป	0.143	0.671	0.211	0.652	0.609	0.593	**+354.3**	**-9.27**	**+180.62**
2.กลุ่มผู้เชี่ยวชาญ	0.287	0.646	0.383	0.617	0.605	0.571	**+115.1**	**-6.33**	**+49.14**
อัตราความแตกต่างของการเพิ่มลด	**+100.7**	**-3.726**	**+81.517**	**-5.368**	**-0.657**	**-3.710**	**-239.21**	**-2.94**	**-131.49**

จากการเปรียบเทียบผลระหว่างสองหน่วยทดลอง จากตาราง 5.6 พบว่า กลุ่มผู้เชี่ยวชาญ มีค่าเฉลี่ยค่าระลึก และค่ามัชฌิมฮาร์โมนิกการค้นคืนโดยใช้คำสำคัญที่มากกว่ากลุ่มผู้ใช้ทั่วไป เนื่องจากมีประสบการณ์ด้านการกำหนดนโยบายหรือมีความรู้เกี่ยวกับความมั่นคงสารสนเทศมากกว่า ทำให้ได้ข้อคำถามมีความครอบคลุมโจทย์ปัญหามากกว่า แต่ค่าเฉลี่ยความแม่นยำกลับน้อยกว่า อาจเพราะผู้ใช้ทั่วไปใช้ข้อคำถามที่กระชับและเจาะจงสูงกว่า

บทที่ 6

สรุปผลการวิจัย

บทนี้จะกล่าวถึงบทสรุปของงานวิจัย งานวิจัยในอนาคต และ บทความวิชาการที่ได้รับการตีพิมพ์ โดยมีรายละเอียดดังนี้

6.2 สรุปผลการวิจัย

งานวิจัยนี้ได้ทำการวิเคราะห์ ออกแบบ และสร้างเครื่องมือสนับสนุนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงโดยใช้แบบรูปความมั่นคง เครื่องมือได้เสนอส่วนการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคง โดยใช้โครงสร้างข้อมูลสารสนเทศ ซึ่งได้จากการวิเคราะห์แบบรูปความมั่นคงที่นำเสนอไว้โดย M.Schumacher และคณะ [1] สำหรับผู้ใช้ทั่วไปที่มีพื้นฐานด้านความมั่นคงสารสนเทศไม่มากนัก เพื่อให้การกำหนดนโยบายมีความเหมาะสม ครอบคลุมและสอดคล้องกับมาตรฐานที่ได้รับการยอมรับ โดยเสนอใช้วิธีการค้นคืน 3 วิธีการ คือการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลสารสนเทศ การค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้คำสำคัญ และการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยพิจารณาความสัมพันธ์ระหว่างแบบรูปความมั่นคงเพื่อเพิ่มความสมบูรณ์ในการกำหนดนโยบาย งานวิจัยนี้แบ่งออกเป็น 5 กระบวนการสำคัญ โดยมีรายละเอียด ดังต่อไปนี้

1) การจัดเก็บส่วนของเอกสารมาตรฐานด้านความมั่นคงและแบบรูปความมั่นคง

ส่วนจัดเก็บส่วนของเอกสารมาตรฐานด้านความมั่นคง งานวิจัยนี้ใช้เอกสารมาตรฐานไอเอสโอ/ไออีซี 27002 ในการค้นคืน ครอบคลุม 11 หัวข้อใหญ่ รวมทั้งสิ้น 185 ส่วนเอกสาร เพื่อนำมาจัดดัชนี และค่าน้ำหนักของแต่ละส่วนเอกสารต่อไป และจัดเก็บส่วนแบบรูปความมั่นคงทั้งสิ้น 20 แบบรูป มาเป็นกรณีศึกษา โดยนำมาจากหนังสือแบบรูปความมั่นคงการบูรณาการความมั่นคงและวิศวกรรมระบบของ M. Schumacher และคณะ เพื่อนำมาจัดจัดทำดัชนี และค่าน้ำหนักแต่นำไปสร้างโครงสร้างข้อมูลสารสนเทศเพื่อช่วยในเพิ่มประสิทธิผลในการค้นคืน

2) การออกแบบวิธีการและพัฒนาระบบต้นแบบสนับสนุนการจัดเก็บและค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศ

การค้นคืนในงานวิจัยนี้มุ่งเน้นค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงโดยใช้แบบจำลองปริภูมิเวคเตอร์ โดยทำการเปรียบเทียบ ประสิทธิผลการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้โครงสร้างข้อมูลสารสนเทศ และการค้นคืนส่วนของเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้คำสำคัญ จากกลุ่มผู้ใช้ 2 กลุ่ม คือกลุ่มผู้ใช้ทั่วไปและผู้เชี่ยวชาญ

3) การพัฒนาเครื่องมือ

หลังจากได้ทำการออกแบบวิธีการจัดเก็บและการค้นคืนเรียบร้อยแล้ว จึงทำการพัฒนาเครื่องมือต้นแบบเพื่อใช้ในการจัดเก็บและค้นคืน เพื่อให้สนับสนุนแนวความคิดในงานวิจัยนี้ โดยแบ่งออกเป็น 5 ส่วนหลัก ๆ

(1) ส่วนจัดเก็บส่วนของเอกสารมาตรฐานด้านความมั่นคง ผู้วิจัยได้ทำการพัฒนาส่วนการทำงานเพื่อตัดส่วนของเอกสารที่ต้องการ เพื่อจัดเก็บเข้าสู่ฐานข้อมูลเชิงสัมพันธ์ตามการออกแบบจำลองข้อมูลที่ได้ออกแบบไว้

(2) ส่วนจัดเก็บส่วนแบบรูปความมั่นคง ผู้วิจัยได้ทำการพัฒนาส่วนต่อประสานสำหรับจัดเก็บแบบรูปความมั่นคง รวมถึง แก้ไข ลบแบบรูปความมั่นคง

(3) ส่วนจัดทำดัชนีและน้ำหนักของเอกสาร ผู้วิจัยได้ทำการพัฒนาส่วนต่อประสานเพื่อช่วยในการจัดทำดัชนี มีส่วนสำหรับนำเข้าคำเอกสารคำและสัญลักษณ์ที่ควรละเว้นในรูปแบบข้อความ

(4) ส่วนการสร้างโครงสร้างข้อมูลสารสนเทศ ผู้วิจัยได้ทำการพัฒนาส่วนต่อประสานสำหรับจัดการโคงสร้างข้อมูลสารสนเทศ ผู้ใช้สามารถคัดเลือกส่วนแสดงผล ตามที่ต้องการได้

(5) ส่วนค้นคืนส่วนของเอกสารมาตรฐานด้านความมั่นคง ผู้วิจัยได้ทำการพัฒนาส่วนต่อประสานสำหรับการค้นคืน ทั้ง 2 วิธีคือค้นคืนโดยใช้คำสำคัญและใช้โครงสร้างข้อมูลสารสนเทศ ผู้ใช้สามารถคัดกรองผลลัพธ์โดยกำหนดค่าขีดแบ่งความคล้ายคลึงได้

4) ทำการทดลองและประเมินผลการทดลอง

ภายหลังจากพัฒนาเครื่องมือในการค้นคืนเสร็จสิ้นผู้วิจัยได้ทำการทดลองเพื่อเปรียบเทียบการค้นคืนทั้ง 2 วิธี จากสองกลุ่มผู้ใช้ โดยใช้โจทย์ปัญหาทั้งสิ้น 11 ข้อ จากกลุ่มผู้ใช้ 2 กลุ่มทดลอง คือกลุ่มผู้ใช้ทั่วไปและผู้เชี่ยวชาญ โดยใช้ ค่าระลึก ค่าความแม่นยำ และค่ามัชฌิมฮาร์โมนิก เป็นมาตรวัดเพื่อหาค่าของผลการค้นคืนในแต่ละวิธี เพื่อนำมาเปรียบเทียบวิธีค้นคืนแต่ละวิธีต่อไป

5) การสรุปผลการทดลอง

สำหรับผู้เชี่ยวชาญการค้นคืนส่วนของเอกสารมาตรฐานด้านความมั่นคงโดยใช้โครงสร้างข้อมูลความมั่นคงสารสนเทศ นั้นทำให้ค่าระลึกเฉลี่ยและค่ามัชฌิมฮาร์โมนิกเพิ่มขึ้น 115.05% และ 49.14% ตามลำดับ แต่ทำให้ค่าความแม่นยำ ลดลง 6.33%

สำหรับผู้ใช้ทั่วไปการค้นคืนส่วนของเอกสารมาตรฐานด้านความมั่นคงโดยใช้โครงสร้างข้อมูลสารสนเทศ ทำให้ค่าระลึกเฉลี่ยและค่ามัชฌิมฮาร์โมนิกเพิ่มขึ้น 354.26% และ 180.62% ตามลำดับ แต่ทำให้ค่าความแม่นยำ ลดลง 9.27%

จะเห็นได้ว่า สำหรับผู้ใช้ทั่วไปที่มีพื้นฐานด้านความมั่นคงสารสนเทศไม่มากนัก วิธีการการค้นคืนส่วนของเอกสารมาตรฐานด้านความมั่นคงโดยใช้โครงสร้างข้อมูลสารสนเทศ ช่วยให้การค้นคืนส่วนเอกสารความมั่นคงสารสนเทศเพื่อกำหนดนโยบาย มีความเหมาะสม ครอบคลุมและสอดคล้องกับมาตรฐานมากขึ้น

อย่างไรก็ตามผู้วิจัยมีความคิดเห็นว่า ยังมีอีกหลายปัจจัยที่สามารถทำให้ค่าประสิทธิผลในการค้นคืนนั้นเพิ่มมากขึ้นได้อีก เช่น ทักษะด้านภาษาอังกฤษของผู้ค้นคืน ทำให้ได้ข้อคำถามที่ถูกต้องมากยิ่งขึ้น เป็นต้น

จากการทดสอบคุณภาพของเครื่องมือ คือความครบถ้วนและถูกต้องของเครื่องมือต้นแบบสามารถสรุปได้ว่าเครื่องมือต้นแบบที่สร้างขึ้นมีความถูกต้องและครบถ้วนอยู่ในระดับที่สามารถนำไปใช้งานได้จริง

6.3 ข้อจำกัดของงานวิจัย

1) ในงานวิจัยนี้เอกสารที่ใช้ในการค้นคืน คือเอกสาร ไอเอสโอ/ไออีซี 27002 และแบบรูปความมั่นคง จำนวน 20 แบบรูป จาก 4 กลุ่มแบบรูปความมั่นคง ซึ่งเป็นเพียงส่วนหนึ่งของหนังสือแบบรูปความมั่นคงการบูรณาการความมั่นคงและวิศวกรรมระบบของ M. Schumacherและคณะ [1] เท่านั้น

2) เอกสารที่ใช้ทั้งหมดในการค้นคืน รวมทั้งข้อคำถามทั้งหมด ต้องเป็นภาษาอังกฤษเท่านั้น

6.4 งานวิจัยในอนาคต

1) งานวิจัยนี้ได้ใช้แบบรูปความมั่นคง จำนวน 20 แบบรูป จาก 4 กลุ่มแบบรูปความมั่นคง เพื่อนำมาสร้างโครงสร้างข้อมูลความมั่นคงสารสนเทศ ซึ่งเป็นเพียงส่วนหนึ่งของหนังสือแบบรูปความมั่นคงการบูรณาการความมั่นคงและวิศวกรรมระบบของ M. Schumacher และคณะ [1] เท่านั้น

หากสามารถจัดเก็บครอบคลุมในทุกกลุ่มแบบรูปความมั่นคง ผู้วิจัยคาดว่าจะช่วยปรับปรุงการค้นคืนแบบส่วนของเอกสารมาตรฐานความมั่นคงให้มีความสมบูรณ์มากยิ่งขึ้น

2) งานวิจัยนี้ใช้หลักการจัดทำดัชนีเอกสารโดยวิธีการ กำจัดคำที่ไม่จำเป็น การทำรากศัพท์โดยวิธีการของพอร์ตเตอร์ ถ้านำหลักการต่างๆ เช่น การค้นหาจากคำที่มีความหมายเหมือนกัน หรือการจัดทำดัชนีแบบสองคำ หรือสามคำ จะสามารถค้นคืนมีความครอบคลุมและเพิ่มประสิทธิผลมากยิ่งขึ้น

6.4 ผลงานตีพิมพ์จากวิทยานิพนธ์

ผู้วิจัยได้จัดทำผลงานวิชาการร่วมกับคณะผู้วิจัย เป็นบทความวิชาการระดับนานาชาติ คือ บทความวิชาการเรื่อง “กรอบงานการจัดเก็บและค้นคืนส่วนเอกสารมาตรฐานความมั่นคงสารสนเทศโดยใช้แบบรูปความมั่นคง (Framework for Information Security Standards Storage and Retrieval using Security Patterns)” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการทางวิศวกรรมคอมพิวเตอร์และวิทยาศาสตร์บริการระดับชาติ ครั้งที่ 4 (The 4th IEEE International Conference on Software Engineering and Service Science :ICSESS 2013) ระหว่างวันที่ 23 – 25 พฤษภาคม พ.ศ 2556 ณ กรุงปักกิ่ง ประเทศจีน

รายการอ้างอิง

[1] Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., and Sommerlad, P. Security Patterns Integrating Security and Systems Engineering.John Wiley & Sons, 2006.

[2] Nobukazu YOSHIOKA, H.W., and Katsuhisa MARUYAMA. A Survey on Security Patterns,in Proceeding in Informatics ,2008.

[3] mattord., M.E.W.a.H.J.. Principles of Information Security 4th Edition. Course Technology ,2003

[4] International Organization for Standarization.ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management,2005.

[5] กวิน สุภาพร. การกำหนดความต้องการความมั่นคงโดยใช้ไวยากรณ์ของแบบรูปความมั่นคง. วิทยานิพนธ์ปริญญามหาบัณฑิต, ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550.

[6] Baeza-Yates, R. and Ribeiro-Neto, B. Modern Information Retrieval. Addison Wesley, ACM, 1999.

[7] Morgan Kaufmann.Porter, M.F.An algorithm for suffix stripping,pp. 313 – 316. 1980.

[8] Manwar, A. B. A Vector Space Model For Information Retrieval: A Matlab Apporch. Indian Journal of Computer Science and Engineering (IJCSE), 2012.

[9] Munawar Hafiz, P.A., Ralph E. Johnson.Towards an Organization of SecurityPatterns ,University of Illinois,2010.

[10] Lucia, A. D., Fasano, F.,Oliveto, R., and Tortora, G. Recovering traceability links in software artifact management systems using information retrieval methods, ACM Transactions on Software Engineering and Methodology (TOSEM). 16, 2007.

[11] International Organization for Standarization. ISO Standard 9126: Software Engineering – Product Quality, parts 1, 2 and 3, International Organization for Standarization, Geneve, 2001.

ภาคผนวก

ภาคผนวก ก
แบบรูปความมั่นคงที่ใช้ในการทดลอง

ในภาคผนวก ก จะกล่าวถึงแบบรูปความมั่นคง การจำแนกแบบรูปความมั่นคงตามหลักของซี.ไอ.เอ.เอ และความสัมพันธ์ระหว่างแบบรูปความมั่นคงที่ใช้ในการทดลอง

ตารางที่ ก.1 แสดงแบบรูปความมั่นคงที่ใช้ในงานวิจัย [1]

กลุ่มแบบรูปความมั่นคง	ชื่อแบบรูปความมั่นคง	รหัสแบบรูป
กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง	การระบุความมั่นคงสำหรับสินทรัพย์ขององค์กร	SP1
	การประเมินค่าสินทรัพย์	SP2
	การประเมินภัยคุกคาม	SP3
	การประเมินจุดอ่อน	SP4
	การกำหนดความเสี่ยง	SP5
	แนวคิดความมั่นคงองค์กร	SP6
	บริการความมั่นคงองค์กร	SP7
	การสื่อสารของผู้เป็นหุ้นส่วนองค์กร	SP8
กลุ่มแบบรูปการระบุตัวตนและการพิสูจน์ตัวจริง	ความต้องการด้านการระบุและการพิสูจน์ตัวตน	SP9
	ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนแบบอัตโนมัติ	SP10
	การออกแบบและใช้รหัสผ่าน	SP11
	ทางเลือกการออกแบบชีวมิติ	SP12
กลุ่มแบบรูปแบบจำลองควบคุมการเข้าถึง	การให้อำนาจ	SP13
	การควบคุมการเข้าถึงเชิงบทบาท	SP14
	ความมั่นคงหลายระดับ	SP15
	การตรวจสอบการเข้าถึง	SP16
	การกำหนดสิทธิ์ให้กับบทบาท	SP17

ตารางที่ ก.1 แสดงแบบรูปความมั่นคงที่ใช้ในงานวิจัย [1] (ต่อ)

กลุ่มแบบรูปความมั่นคง	ชื่อแบบรูปความมั่นคง	รหัสแบบรูป
กลุ่มแบบรูปสถาปัตยกรรมไฟร์วอลล์	ไฟร์วอลล์สำหรับการกรองแพ็คเกจ	SP18
	ไฟร์วอลล์เชิงตัวแทน	SP19
	ไฟร์วอลล์เชิงสถานะ	SP20

ตารางที่ ก.2 การจำแนกแบบรูปความมั่นคงตามหลักของ ซี.ไอ.เอ.เอ

รหัสแบบรูป	คุณลักษณะด้านความปลอดภัย			
	ความลับของข้อมูล	ความบูรณภาพ	สภาพพร้อมใช้งานของข้อมูล	ความรับผิดชอบต่อข้อมูล
SP1	✓	✓	✓	✗
SP2	✓	✓	✓	✗
SP3	✓	✓	✓	✗
SP4	✓	✓	✓	✗
SP5	✓	✓	✓	✓
SP6	✓	✓	✓	✓
SP7	✓	✗	✗	✗
SP8	✓	✓	✓	✓
SP9	✓	✗	✗	✓
SP10	✓	✗	✗	✓
SP11	✓	✗	✗	✗
SP12	✓	✗	✗	✗
SP13	✓	✗	✗	✓
SP14	✓	✗	✗	✗
SP15	✓	✓	✗	✗
SP16	✓	✗	✗	✗
SP17	✓	✗	✗	✗
SP18	✓	✗	✗	✗

ตารางที่ ก.2 การจำแนกแบบรูปความมั่นคงตามหลักของ ซี.ไอ.เอ.เอ (ต่อ)

รหัสแบบรูป	คุณลักษณะด้านความปลอดภัย			
	ความลับของข้อมูล	ความบูรณภาพ	สภาพพร้อมใช้งานของข้อมูล	ความรับผิดชอบต่อข้อมูล
SP19	✓	×	×	×
SP20	✓	×	×	×

ตารางที่ ก.3 ตารางแสดงเงื่อนไขระหว่างแบบรูป [5]

ชื่อแบบรูปความมั่นคง	เงื่อนไขก่อนการใช้งานแบบรูปความมั่นคง
การระบุความมั่นคงสำหรับสินขององค์กร	-
การประเมินค่าสินทรัพย์	- ผ่านการกำหนดสินทรัพย์ขององค์กร
การประเมินภัยคุกคาม	- ผ่านการกำหนดสินทรัพย์ขององค์กร-
การประเมินจุดอ่อน	- ผ่านการกำหนดสินทรัพย์ขององค์กร - ผ่านการกำหนดภัยคุกคามให้กับสินทรัพย์
การกำหนดความเสี่ยง	- ผ่านการกำหนดสินทรัพย์ขององค์กร - ผ่านการประเมินค่าสินทรัพย์ - ผ่านการประเมินความถี่ที่จะเกิดภัยคุกคามให้กับ สินทรัพย์ - ผ่านการประเมินระดับความรุนแรงของจุดอ่อนที่เกิดจาก ภัยคุกคาม
แนวคิดความมั่นคงองค์กร	- ผ่านการกำหนดสินทรัพย์ขององค์กร

ตารางที่ ก.3 ตารางแสดงเงื่อนไขระหว่างแบบรูป [5] (ต่อ)

ชื่อแบบรูปความมั่นคง	เงื่อนไขก่อนการใช้งานแบบรูปความมั่นคง
บริการความมั่นคงองค์กร	- ผ่านการกำหนดภัยคุกคามให้กับสินทรัพย์
การสื่อสารของผู้เป็นหุ้นส่วนองค์กร	- ผ่านการกำหนดสินทรัพย์ขององค์กร - ผ่านการกำหนดการระบุและพิสูจน์ตัวตน
ความต้องการด้านการระบุและการพิสูจน์ตัวตน	-
ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนแบบอัตโนมัติ	- ผ่านการกำหนดชื่อตัวบริการในการระบุและพิสูจน์ตัวตน
การออกแบบและใช้รหัสผ่าน	- ผ่านการกำหนดชื่อตัวบริการในการระบุและพิสูจน์ตัวตน - ผ่านการเลือกวิธีในการพิสูจน์ตัวตน (เลือกแบบใช้ รหัสผ่าน)
ทางเลือกการออกแบบชีวมิติ	- ผ่านการกำหนดชื่อตัวบริการในการระบุและพิสูจน์ตัวตน - ผ่านการเลือกวิธีในการพิสูจน์ตัวตน (เลือกแบบใช้ชีวมิติ)
การให้อำนาจ	- ผ่านการกำหนดสินทรัพย์ขององค์กร
การควบคุมการเข้าถึงเชิงบทบาท	- ผ่านการกำหนดสินทรัพย์ขององค์กร - ผ่านการกำหนดบทบาทให้กับองค์กร
ความมั่นคงหลายระดับ	- ผ่านการกำหนดสินทรัพย์ขององค์กร - ผ่านการกำหนดบทบาทให้กับองค์กร
การตรวจสอบการเข้าถึง	- ผ่านการกำหนดสินทรัพย์ขององค์กร - ผ่านการกำหนดบทบาทให้กับองค์กร

ตารางที่ ก.3 ตารางแสดงเงื่อนไขระหว่างแบบรูป [5] (ต่อ)

ชื่อแบบรูปความมั่นคง	เงื่อนไขก่อนการใช้งานแบบรูปความมั่นคง
	- ผ่านการกำหนดสิทธิ์ให้กับบทบาท
การกำหนดสิทธิ์ให้กับบทบาท	- ผ่านการกำหนดสินทรัพย์ขององค์กร - ผ่านการกำหนดบทบาทให้กับองค์กร
ไฟร์วอลล์สำหรับการกรองแพ็คเกจ	- ผ่านการกำหนดสินทรัพย์ (บริการ) ขององค์กร
ไฟร์วอลล์เชิงตัวแทน	- ผ่านการกำหนดสินทรัพย์ (บริการ) ขององค์กร
ไฟร์วอลล์เชิงสถานะ	- ผ่านการกำหนดสินทรัพย์ (บริการ) ขององค์กร

ตารางที่ ก.4 ตารางแสดงความสัมพันธ์ระหว่างแบบรูป [5]

	SP1	SP2	SP3	SP4	SP5	SP6	SP7	SP8	SP9	SP10	SP11	SP12	SP13	SP14	SP15	SP16	SP17	SP18	SP19	SP20
SP1																				
SP2	✓																			
SP3	✓																			
SP4			✓																	
SP5	✓	✓	✓	✓																
SP6	✓				✓		✓													
SP7	✓																			
SP8	✓								✓											
SP9											✓	✓								
SP10									✓											
SP11										✓										
SP12																				
SP13	✓									✓										
SP14	✓									✓						✓				
SP15	✓																			
SP16	✓															✓				

SP17	✓																		
SP18	✓																	✓	✓
SP19	✓																		
SP20	✓																		

ภาคผนวก ข

โจทย์ปัญหาและข้อคำถามที่ใช้ในการทดลอง

สำหรับโจทย์ปัญหาในการทดลองเปรียบเทียบการค้นคืนส่วนเอกสารความมั่นคงสารสนเทศมีทั้งสิ้น 11 โจทย์ โดยการกำหนดโจทย์ปัญหาจะอยู่ภายใต้แบบรูปความมั่นคง 20 แบบรูป โดยมีรายละเอียดแสดงในตารางที่ ข.1 หน่วยทดลองทั้ง 2 กลุ่ม จะสร้างข้อคำถามจากแต่ละโจทย์ปัญหา โดยตัวอย่างข้อคำถามแสดงดังตารางที่ ข.2

ตารางที่ ข.1 โจทย์ปัญหาที่ใช้ในการทดลอง

เนื้อหา	คำอธิบาย	รหัสโจทย์ปัญหา	รหัสแบบรูปที่เกี่ยวข้อง
แนวทางปฏิบัติการจัดการทรัพย์สินสารสนเทศ	การจัดการทรัพย์สินสารสนเทศ (Information Asset Management) กำหนดขึ้นเพื่อป้องกันทรัพย์สินสารสนเทศของมหาวิทยาลัยให้เกิดความมั่นคงและสามารถใช้งานทรัพย์สินได้อย่างเหมาะสม	Q1	SP1,SP2,SP4,SP5 - 8,SP13
แนวทางปฏิบัติการตรวจสอบและประเมินความเสี่ยง	เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัย ด้านสารสนเทศ	Q2	SP1,SP8,SP14-15
แนวทางปฏิบัติการควบคุมการเข้าออกหองควบคุมระบบคอมพิวเตอร์(ห้อง Server)	เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงที่เกี่ยวข้องกับการเขาใช้งาน หรือการเขาถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่ายและระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยี	Q3	SP1,SP8-14

ตารางที่ ข.1 โจทย์ปัญหาที่ใช้ในการทดลอง (ต่อ)

เนื้อหา	คำอธิบาย	รหัสโจทย์ปัญหา	รหัสแบบรูปที่เกี่ยวข้อง
	สารสนเทศ ข้อมูลซึ่งเปนทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับโดยมาตรการนี้จะมีผลบังคับใช้กับผู้มีสวนเกี่ยวของกับการใช้งานระบบเทคโนโลยีสารสนเทศ		
แนวทางปฏิบัติความมั่นคงของอีเมล	เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวน สิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงของการใช้งานระบบเครือข่ายไร้สาย	Q4	SP5-SP7,SP9,SP13,SP18
แนวทางปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ	เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตเขาถึงระบบสารสนเทศและ ป้องกันการบุกรุกผ่านระบบเครือขายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไมพึงประสงคที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้	Q5	SP1, SP3-7, SP9, SP10-11,SP13-15

ตารางที่ ข.1 โจทย์ปัญหาที่ใช้ในการทดลอง (ต่อ)

เนื้อหา	คำอธิบาย	รหัสโจทย์ปัญหา	รหัสแบบรูปที่เกี่ยวข้อง
	หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เขาใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ได้อย่างถูกต้อง		
แนวทางปฏิบัติการรักษาความปลอดภัยของเครือข่ายไร้สาย	เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงของการใช้งานระบบเครือข่ายไร้สาย	Q6	SP9, SP11, SP15, SP18, SP20
แนวทางปฏิบัติการควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย		Q7	SP8-12
แนวทางปฏิบัติการใช้งานอินเตอร์เน็ต	เพื่อให้ผู้ใชรับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอรเน็ตอย่างปลอดภัยและเป็นการ ป้องกันไม่ให้ละเมิด	Q8	SP3-8, SP18, SP20

ตารางที่ ข.1 โจทย์ปัญหาที่ใช้ในการทดลอง

เนื้อหา	คำอธิบาย	รหัสโจทย์ปัญหา	รหัสแบบรูปที่เกี่ยวข้อง
	พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอรแก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบ คอมพิวเตอร์ของบุคคลอื่นโดยปกติ ทำใหระบบคอมพิวเตอร์ของมหาวิทยาลัยถูกระงับชะลอขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้		
แนวทางปฏิบัติการรักษาความมั่นคงของไฟรวอลล		Q9	SP14-16, SP18-20
แนวทางปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน	เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่กี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้ง จำกัดสิทธิ์ในการใช้งานระบบเทคโนโลยีสารสนเทศ	Q10	SP1, SP3-7, SP9-11, SP13-17

*หมายเหตุ รหัสแบบรูปที่เกี่ยวข้องอ้างอิงจาก ตารางที่ ก.1

ตารางที่ ข.2 ตัวอย่างข้อคำถามที่ใช้ในการทดลอง

ข้อคำถามที่	ข้อคำถาม	รหัสข้อคำถาม	ข้อคำถามที่
Q1	1	information asset management protect security proper	[K,E,Q1,1]
Q2	2	Risk Assessment & Management	[K,E,Q2,2]
Q3	3	Information security regarding physical conditions	[K,E,Q3,3]
Q4	4	E-mail Policy	[K,E,Q4,4]
Q5	5	permission policy application	[K,E,Q5,5]
Q6	6	wireless security policy authentication	[K,E,Q6,6]
Q7	7	internet policy message program	[K,E,Q7,7]
Q8	8	Firewall Policy	[K,E,Q8,8]
Q9	9	security access user management standard	[K,E,Q9,9]
Q10	10	Computer Operation	[K,E,Q10,10]
Q11	11	information asset management protect security proper	[K,E,Q10,11]
Q1	1	information asset Management	[K,U,Q1,1]
Q2	2	IT risk management control	[K,U,Q2,2]
Q3	3	security asset accessibility	[K,U,Q3,3]
Q4	4	email security encryption business rule	[K,U,Q4,4]
Q5	5	security encryption application accessibility	[K,U,Q5,5]
Q6	6	security wireless accessibility IEEE ISO standard	[K,U,Q6,6]
Q7	7	Security rule Computer center	[K,U,Q7,7]
Q8	8	internet policy	[K,U,Q8,8]
Q9	9	firewall security standard	[K,U,Q9,9]
Q10	10	(AAA) Authentication Authorization Accounting	[K,U,Q10,10]
Q11	11	security personal computer	[K,U,Q10,11]
Q1	1	Security Needs Identification for Enterprise	[SP,E,Q1,1]

ตารางที่ ข.2 ตัวอย่างข้อคำถามที่ใช้ในการทดลอง (ต่อ)

ข้อคำถามที่	ข้อคำถาม	รหัสข้อคำถาม	ข้อคำถามที่
		Assets enterpris asset appli secur combin Asset Valuation enterpris control asset assess determin Risk Determination determin evalu risk	
Q2	2	Security Needs Identification for Enterprise Assets enterpris asset appli secur combin Asset Valuation enterpris control asset assess determin Risk Determination determin evalu risk Enterprise Security and Risk Management Patterns Security Needs Identific	[SP,E,Q2,2]
Q3	3	Security Needs Identification for Enterprise Assets enterpris asset appli secur combin Asset Valuation enterpris control asset assess determin Risk Determination determin evalu risk Enterprise Security and Risk Management Patterns Security Needs Identific	[SP,E,Q3,3]
Q4	4	I&A Requirements also authent determin appli altern Multilevel Security access control check applic 287 Role-Based Access Control access control can appli assess Access Control Model Patterns Authorization access control asset check 287 Role-Based Access	[SP,E,Q4,4]
Q5	5	I&A Requirements also authent determin appli altern Multilevel Security access control check applic 287 Role-Based Access Control access control can appli assess	[SP,E,Q5,5]

ตารางที่ ข.2 ตัวอย่างข้อคำถามที่ใช้ในการทดลอง (ต่อ)

ข้อคำถามที่	ข้อคำถาม	รหัสข้อคำถาม	ข้อคำถามที่
		Access Control Model Patterns Authorization access control asset check 287 Role-Based Access	
Q6	6	I&A Requirements also authent determin appli altern Multilevel Security access control check applic 287 Role-Based Access Control access control can appli assess Access Control Model Patterns	[SP,E,Q6,6]
Q7	7	Security Needs Identification for Enterprise Assets enterpris asset appli secur approach Asset Valuation enterpris asset control assess determin Enterprise Partner Communication access enterpris applic busi commun Biometrics Design Alternatives design alt	[SP,E,Q7,7]
Q8	8	Proxy-Based Firewall access firewal can control base Identification & Authentication (I&A) Patterns Automated I&A Design Alternatives altern i&a strategi appropri factor Password Design and Use design administr password 192 229 Biometrics Design Alternati	[SP,E,Q8,8]
Q9	9	Security Needs Identification for Enterprise Assets enterpris asset appli secur combin Threat Assessment can assess enterpris asset determin Vulnerability Assessment access assess enterpris asset also Risk Determination determin evalu risk Firewall	[SP,E,Q9,9]

ตารางที่ ข.2 ตัวอย่างข้อคำถามที่ใช้ในการทดลอง (ต่อ)

ข้อคำถามที่	ข้อคำถาม	รหัสข้อคำถาม	ข้อคำถามที่
		Archit	
Q10	10	Access Control Model Patterns Authorization access control asset check 287 Role-Based Access Control access control can appli assess Multilevel Security access control check applic 287 Reference Monitor access can secur 287 authent Role Rights Definition	[SP,E,Q10,10]
Q11	11	Identification & Authentication (I&A) Patterns Automated I&A Design Alternatives altern i&a strategi appropri factor Password Design and Use design administr password 192 229 Biometrics Design Alternatives altern design addit 241 biometr I&A Requirements	[SP,E,Q10,11]
Q1	1	Enterprise Security and Risk Management Patterns Security Needs Identification for Enterprise Assets enterpris asset appli secur approach Asset Valuation enterpris asset control assess determin Threat Assessment can assess enterpris asset determin Vulnera	[SP,U,Q1,1]
Q2	2	Accountability Enterprise Security and Risk Management Patterns Security Needs Identification for Enterprise Assets enterpris asset appli secur combin Asset Valuation enterpris control asset assess determin Threat Assessment can assess enterpris asset det	[SP,U,Q2,2]
Q3	3	Accountability Enterprise Security and Risk	[SP,U,Q3,3]

ตารางที่ ข.2 ตัวอย่างข้อคำถามที่ใช้ในการทดลอง (ต่อ)

ข้อคำถามที่	ข้อคำถาม	รหัสข้อคำถาม	ข้อคำถามที่
		Management Patterns Security Needs Identification for Enterprise Assets enterpris asset appli secur combin Asset Valuation enterpris control asset assess determin Threat Assessment can assess enterpris asset det	
Q4	4	Enterprise Security and Risk Management Patterns Security Needs Identification for Enterprise Assets enterpris asset appli secur combin Asset Valuation enterpris control asset assess determin Threat Assessment can assess enterpris asset determin Vulnerabi	[SP,U,Q4,4]
Q5	5	Firewall Architecture Patterns Stateful Firewall firewal base filter combin 405 Packet Filter Firewall access firewal can base filter Proxy-Based Firewall access firewal can control base Access Control Model Patterns Authorization access control asset che	[SP,U,Q5,5]
Q6	6	Confidentiality Identification & Authentication (I&A) Patterns Automated I&A Design Alternatives altern i&a strategi appropri factor Password Design and Use design administr password 192 229 Biometrics Design Alternatives altern design addit 241 biometr I	[SP,U,Q6,6]

ตารางที่ ข.2 ตัวอย่างข้อคำถามที่ใช้ในการทดลอง (ต่อ)

ข้อคำถามที่	ข้อคำถาม	รหัสข้อคำถาม	ข้อคำถามที่
Q7	7	Asset Valuation enterpris asset control assess determin Enterprise Partner Communication access enterpris applic busi commun Identification & Authentication (I&A) Patterns Automated I&A Design Alternatives altern i&a appropri 02 factor Password Design and	[SP,U,Q7,7]
Q8	8	Identification & Authentication (I&A) Patterns Automated I&A Design Alternatives altern i&a strategi appropri factor Password Design and Use design administr password 192 229 Biometrics Design Alternatives altern design addit 241 biometr I&A Requirements	[SP,U,Q8,8]
Q9	9	Identification & Authentication (I&A) Patterns Automated I&A Design Alternatives altern i&a strategi appropri factor Password Design and Use design administr password 192 229 Biometrics Design Alternatives altern design addit 241 biometr I&A Requirements	[SP,U,Q9,9]
Q10	10	Access Control Model Patterns Authorization access control asset check 287 Role-Based Access Control access control can appli assess Multilevel Security access control check applic 287 Reference Monitor access can secur 287 authent Role Rights Definition	[SP,U,Q10,10]

ตารางที่ ข.2 ตัวอย่างข้อคำถามที่ใช้ในการทดลอง (ต่อ)

ข้อคำถามที่	ข้อคำถาม	รหัสข้อคำถาม	ข้อคำถามที่
Q11	11	Access Control Model Patterns Authorization access control asset check 287 Role-Based Access Control access control can appli assess Multilevel Security access control check applic 287 Reference Monitor access can secur 287 authent Role Rights Definition	[SP,E,Q10,11]

ภาคผนวก ค

ตัวอย่างค่าระลึก ค่าความแม่นยำและค่ามัชฌิมฮาร์โมนิก ที่ได้จากการทดลอง

ในบทนี้ จะกล่าวถึงตัวอย่างผลลัพธ์ที่ได้จากการทดลองเครื่องมือต้นแบบ โดยใช้มาตรวัดประสิทธิผลการค้นคืนทั้งสิ้น 3 มาตรวัด ได้แก่ ค่าเรียกคืน (R) ค่าความแม่นยำ (P) และค่ามัชฌิมฮาร์โมนิก (H) โดยทำการเปรียบเทียบกันทั้งสิ้น 2 กลุ่มหน่วยทดลอง จาก 2 วิธีการค้นคืนแบบดังนี้

1) การค้นคืนส่วนของเอกสารความมั่นคงสารสนเทศโดยใช้คำสำคัญ

2) การค้นคืนส่วนของเอกสารความมั่นคงสารสนเทศโดยใช้แบบรูป

โดยจะแสดงผลของการค้นคืนดังตารางที่ ค.1 ซึ่งรหัสข้อคำถามอ้างอิงจากภาคผนวก ข ตารางที่ ข.2

ตารางที่ ค.1 ตัวอย่างผลการทดลองของแต่ละข้อคำถามที่ใช้

วิธีการค้นคืน		มาตราวัดประสิทธิผล		
ลำดับที่	รหัสข้อคคำถาม	R	P	H
1	[K,E,Q1,1]	0.401691332	0.931372549	0.561299852
2	[K,E,Q2,2]	0.176245211	0.666666667	0.278787879
3	[K,E,Q3,3]	0.189393939	0.574712644	0.284900285
4	[K,E,Q4,4]	0.290858726	0.734265734	0.416666667
5	[K,E,Q5,5]	0.265780731	0.689655172	0.383693046
6	[K,E,Q6,6]	0.323308271	0.387387387	0.352459016
7	[K,E,Q7,7]	0.192771084	0.780487805	0.309178744
8	[K,E,Q8,8]	0.534545455	0.628205128	0.577603143
9	[K,E,Q9,9]	0.241758242	0.66	0.353887399
10	[K,E,Q10,10]	0.401691332	0.931372549	0.561299852
11	[K,E,Q10,11]	0.176245211	0.666666667	0.278787879
12	[K,U,Q1,1]	0.289079229	0.918367347	0.439739414

ตารางที่ ค.1 ตัวอย่างผลการทดลองของแต่ละข้อคำถามที่ใช้ (ต่อ)

วิธีการค้นคืน		มาตราวัดประสิทธิผล		
13	[K,U,Q2,2]	0.353065539	0.927777778	0.511485452
14	[K,U,Q3,3]	0.114942529	0.731707317	0.198675497
15	[K,U,Q4,4]	0.170454545	0.478723404	0.251396648
16	[K,U,Q5,5]	0.152354571	0.733333333	0.252293578
17	[K,U,Q6,6]	0.215946844	0.546218487	0.30952381
18	[K,U,Q7,7]	0.091370558	0.310344828	0.141176471
19	[K,U,Q8,8]	0.240601504	0.380952381	0.294930876
20	[K,U,Q9,9]	0.051204819	0.53125	0.093406593
21	[K,U,Q10,10]	0.181818182	0.625	0.281690141
22	[K,U,Q10,11]	0.172161172	0.643835616	0.271676301
23	[SP,E,Q1,1]	0.77589852	0.93622449	0.848554913
24	[SP,E,Q2,2]	0.770114943	0.512755102	0.615620214
25	[SP,E,Q3,3]	0.537878788	0.416422287	0.469421488
26	[SP,E,Q4,4]	0.606648199	0.642228739	0.623931624
27	[SP,E,Q5,5]	0.631229236	0.557184751	0.591900312
28	[SP,E,Q6,6]	0.918781726	0.468911917	0.620926244
29	[SP,E,Q7,7]	0.639097744	0.287162162	0.396270396
30	[SP,E,Q8,8]	0.512048193	0.53125	0.521472393
31	[SP,E,Q9,9]	0.821818182	0.624309392	0.709576138
32	[SP,E,Q10,10]	0.860805861	0.635135135	0.730948678
33	[SP,E,Q10,11]	0.77589852	0.93622449	0.848554913
34	[SP,U,Q1,1]	0.706638116	0.919220056	0.799031477
35	[SP,U,Q2,2]	0.78858351	0.927860697	0.852571429
36	[SP,U,Q3,3]	0.804597701	0.52238806	0.633484163

ตารางที่ ค.1 ตัวอย่างผลการทดลองของแต่ละข้อคำถามที่ใช้ (ต่อ)

วิธีการค้นคืน		มาตราวัดประสิทธิผล		
37	[SP,U,Q4,4]	0.651515152	0.479108635	0.552166934
38	[SP,U,Q5,5]	0.155124654	0.571428571	0.244008715
39	[SP,U,Q6,6]	0.558139535	0.589473684	0.57337884
40	[SP,U,Q7,7]	1.025380711	0.427061311	0.602985075
41	[SP,U,Q8,8]	0.736842105	0.264864865	0.389662028
42	[SP,U,Q9,9]	0.680722892	0.610810811	0.643874644
43	[SP,U,Q10,10]	0.821818182	0.624309392	0.709576138
44	[SP,E,Q10,11]	0.846153846	0.638121547	0.727559055

*หมายเหตุ รหัสข้อคำถาม อ้างอิงจาก ตารางที่ ก.2

ภาคผนวก ง

รายละเอียดโครงสร้างตารางที่ทำการจัดเก็บในฐานข้อมูล

ตารางอธิบายโครงสร้างข้อมูลในงานวิจัยนี้มีทั้งสิ้น 14 ตาราง โดยมีรายละเอียด โครงสร้างของแต่ละตารางดังแสดงต่อไปนี้

ตารางที่ ง.1 โครงสร้างข้อมูลของตาราง spProperties

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
spPropID	รหัสคุณลักษณะด้านความมั่นคง	Varchar(5)	PK
spPropNm	ชื่อคุณลักษณะด้านความมั่นคง	Varchar(50)	
IsUse	สถานะการใช้งาน	Int	

ตารางที่ ง.2 โครงสร้างข้อมูลของตาราง SpCategories

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
spCat_ID	รหัสกลุ่มแบบรูป	Varchar(5)	PK
spCatNm	ชื่อกลุ่มแบบรูป	Varchar(255)	
IsUse	สถานะการใช้	Int	

ตารางที่ ง.3 โครงสร้างข้อมูลของตาราง securityPatterns

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
Spid	รหัสแบบรูป	Varchar(5)	PK
spCat_ID	รหัสกลุ่มแบบรูป	Varchar(5)	FK

ตารางที่ ง.4 โครงสร้างข้อมูลของตาราง spDetails

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
spDetailID	รหัสรายละเอียดแบบรูป	Int	PK
SPID	รหัสแบบรูป	Varchar(5)	FK
spStructureID	รหัสโครงสร้างของแบบรูป	Varchar(5)	FK
content	เนื้อหาของแบบรูป	Text	

ตารางที่ ง.5 โครงสร้างข้อมูลของตาราง spRelationships

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
relationID	รหัสความสัมพันธ์ระหว่างแบบรูป	Varchar(5)	PK
spid1	รหัสแบบรูป	Varchar(5)	FK
spid2	รหัสแบบรูป	Varchar(5)	FK

ตารางที่ ง.6 โครงสร้างข้อมูลของตาราง spStructures

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
spStructureID	รหัสโครงสร้างของแบบรูป	Varchar(5)	PK
spStructureNm	ชื่อโครงสร้างของแบบรูป	Varchar(100)	
Weight	ค่าน้ำหนัก	int	

ตารางที่ ง.7 โครงสร้างข้อมูลของตาราง sdStructures

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
sdStructureID	รหัสโครงสร้างของเอกสาร	Varchar(5)	PK
sdStructureNm	ชื่อโครงสร้างของเอกสาร	Varchar(100)	
weight	ค่าน้ำหนัก	Int	

ตารางที่ ง.8 โครงสร้างข้อมูลของตาราง sdDetails

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
SDStructure_Detail_ID	รหัสรายละเอียดโครงสร้างเอกสาร	Int	PK
sdStructureID	รหัสโครงสร้างของเอกสาร	Varchar(5)	
ContentType	ประเภทของโครงสร้าง	Varchar(20)	
sdStructureCode	รหัสหัวข้อของโครงสร้าง	Varchar(20)	
size	ขนาด	Int	
Content	รายละเอียด	Text	
PageNo	เลขหน้า	Int	
LineNo	เลขบรรทัด	Int	

ตารางที่ ง.9 โครงสร้างข้อมูลของตาราง spPropRelationships

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
relationID	รหัสความสัมพันธ์	Int	PK
spid	รหัสแบบรูป	Varchar(5)	FK
spPropID	รหัสคุณลักษณะด้านความมั่นคง	Int	FK

ตารางที่ ง.10 โครงสร้างข้อมูลของตาราง Term

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
termID	รหัสดัชนี	Int	PK
termNm	ดัชนี	Varchar(255)	

ตารางที่ ง.11 โครงสร้างข้อมูลของตาราง spInvertedfile

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
termID	รหัสดัชนี	Int	PK,FK
spDetailID	รหัสรายละเอียดแบบรูป	Int	PK,FK
Frequency	ความถี่ของดัชนีที่ปรากฏ	Int	
Weight	ค่าน้ำหนักของดัชนี	Decimal(5,2)	

ตารางที่ ง.12 โครงสร้างข้อมูลของตาราง sdInvertedfile

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
termID	รหัสดัชนี	Int	PK,FK
sdStructure_Detail_ID	รหัสรายละเอียดโครงสร้างเอกสาร	Int	PK,FK
Frequency	ความถี่ของดัชนีที่ปรากฏ	Int	
Weight	ค่าน้ำหนักของดัชนี	Decimal(5,2)	

ตารางที่ ง.13 โครงสร้างข้อมูลของตาราง sdInvertedfile

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
sdStructure_Detail_ID		Int	PK,FK
spDetailID		Int	PK,FK
simValue	ค่าความคล้ายคลึงระหว่างส่วนของเอกสารและแบบรูปความมั่นคง	Decimal(5,2)	

ตารางที่ ง. 14 โครงสร้างข้อมูลของตาราง role

คุณลักษณะ	คำอธิบาย	ชนิด	คีย์
roleID	รหัสบทบาท	Int	PK
roleNm	ชื่อบทบาท	Varchar(50)	

ประวัติผู้เขียนวิทยานิพนธ์

นางสาวปรมาภรณ์ ร่วมจินดา ชื่อเล่นกิ่ง เกิดเมื่อวันที่ 6 ตุลาคม พ.ศ. 2528 ที่จังหวัดปัตตานี สำเร็จการศึกษาระดับปริญญาตรี หลักสูตรวิทยาศาสตร์ สาขาวิทยาการคอมพิวเตอร์ จากมหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ ในปีการศึกษา 2550 ปัจจุบันได้ทำงานในตำแหน่งนักพัฒนาระบบ (Developer) ที่มหาวิทยาลัยกรุงเทพ กรุงเทพมหานคร ตั้งแต่ปี 2551 จนถึงปัจจุบัน ในปี 2554 ได้เข้าศึกษาต่อในหลักสูตรวิทยาศาตรมหาบัณฑิต สาขาวิศวกรรมซอฟต์แวร์ ภาคนอกเวลาราชการ ที่ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย