การตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ สำหรับการปฏิบัติการแบบไม่มีการลงบันทึก

AUTOMATED SECURITY COMPLIANCE CHECKING FOR NON-LOGGED OPERATIONS

นันทา จันทร์พิทักษ์

NANTA JANPITAK

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาปรัชญาดุษฎีบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2559

KMITL-2016-IT-D-001-001

การตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ สำหรับการปฏิบัติการแบบไม่มีการลงบันทึก

AUTOMATED SECURITY COMPLIANCE CHECKING FOR NON-LOGGED OPERATIONS

นันทา จันทร์พิทักษ์

NANTA JANPITAK

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาปรัชญาดุษฎีบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2559

KMITL-2016-IT-D-001-001

AUTOMATED SECURITY COMPLIANCE CHECKING FOR NON-LOGGED OPERATIONS

NANTA JANPITAK

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2016

KMITL-2016-IT-D-001-001

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติสำหรับการปฏิบัติการแบบไม่มีการลงบันทึก

Automated Security Compliance Checking for Non-Logged Operations

นักศึกษา นางสาวนันทา จันทร์พิทักษ์

รหัสประจำตัว 51066303

ปริญญา ปรัชญาดุษฎีบัณฑิต

สาขาวิชา เทคโนโลยีสารสนเทศ

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รองศาสตราจารย์ ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

คณะกรรมการสอบวิทยานิพนธ์	ลายมือชื่อ
รองศาสตราจารย์ ดร.โชติพัชร์ ภรณวลัย	
ผู้ช่วยศาสตราจารย์ ดร.ทศพล สอตระกูล	
รองศาสตราจารย์ ดร.จันทร์บูรณ์ สถิตวิริยวงศ์	
ผู้ช่วยศาสตราจารย์ ดร.สุเมธ ประภาวัต	
ผู้ช่วยศาสตราจารย์ ดร.ปานวิทย์ ธุวะนุติ	

วัน / เดือน/ ปี ที่สอบ วันพฤหัสบดีที่ 21 เมษายน 2559 เวลา 09.30 น. เป็นต้นไป

สถานที่สอบ ณ ห้อง M23 คณะเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศรับรองแล้ว

(รองศาสตราจารย์ ดร.นพพร โชติกกำธร)

คณบดีคณะเทคโนโลยีสารสนเทศ

วันที่ 17 **เดือน** พ.ค. **พ.ศ.** 2559

หัวข้อวิทยานิพนธ์	การตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติสำหรับการปฏิบัติการแบบไม่มีการลงบันทึก
นักศึกษา	นางสาวนันทา จันทร์พิทักษ์
รหัสประจำตัว	51066303
ปริญญา	ดุษฎีบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
พ.ศ.	2559
อาจารย์ผู้ควบคุมวิทยานิพนธ์	รศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

บทคัดย่อ

ในปัจจุบัน ไม่ว่าการปฏิบัติการใด ๆ ล้วนมีระบบคอมพิวเตอร์มาช่วยลดภาระงานในการประมวลผล โดยเฉพาะภาระงานที่มีข้อมูลปริมาณสูง ๆ แต่ในบางภาระงานก็ยังคงเป็นเรื่องยากที่จะใช้ระบบคอมพิวเตอร์แทนแรงงานคน ทั้งนี้คอมพิวเตอร์กับคนนั้นมีความแตกต่างกันในด้านการประมวลผลข้อมูลคือ คนสามารถแยกแยะความกำกวมของภาษาได้ แต่มีความเร็วจำกัดในด้านการประมวลผลข้อความที่มีปริมาณสูง ส่วนระบบคอมพิวเตอร์โดยทั่วไปนั้นสามารถประมวลผลข้อมูลข้อความปริมาณสูง ๆ ได้ในเวลาที่รวดเร็วแต่ยังไม่สามารถจัดการกับความกำกวมของภาษาได้ดีนัก

การตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง (Security Compliance Checking) ก็เป็นภาระงานหนึ่งที่ยังคงต้องอาศัยการทำงานด้วยคนเป็นหลัก เนื่องจากกฎเกณฑ์ต่าง ๆ นั้นถูกเขียนขึ้นด้วยภาษาธรรมชาติซึ่งมีความกำกวมสูง จำเป็นต้องใช้การตีความด้วยคนที่มีความรู้ความชำนาญเฉพาะด้าน และยังเป็นเรื่องยากที่จะพัฒนาระบบคอมพิวเตอร์ให้ทำงานแทนคนได้ ดังนั้นเวลาและค่าแรงงานที่ต้องเสียไปกับกิจกรรมนี้จึงถือว่าเป็นค่าใช้จ่ายที่ค่อนข้างสูงมาก

วิทยานิพนธ์ฉบับนี้จัดทำขึ้นเพื่อนำเสนอกระบวนการที่สามารถทำให้การตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงมีความเป็นอัตโนมัติ โดยนำเทคโนโลยีที่สามารถประมวลผลกับข้อมูลที่เป็นรูปแบบของภาษาธรรมชาติ (Natural Language Processing) มาใช้เป็นเครื่องมือสำคัญ โดยเลือกตัวอย่างกระบวนการทำงานที่ปรกติแล้วไม่มีการบันทึกข้อมูลลงในระบบคอมพิวเตอร์ในรูปแบบที่สามารถประมวลผลได้ (Non-Logged Operations) และใช้หลักการของการถามตอบซึ่งเป็นกระบวนการของการตรวจสอบโดยทั่วไป วิธีการที่นำเสนอในงานวิจัยฉบับนี้สามารถช่วยให้บุคลากรที่ไม่ใช่ผู้ตรวจสอบสามารถทำการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงได้เอง สามารถรู้ได้ว่ากระบวนการควบคุมใด ๆ ที่ปฏิบัติอยู่ไม่ตรงตามข้อกำหนด ซึ่งจะทำให้รายจ่ายสำหรับการบริหารจัดการการปฏิบัติตามกฎเกณฑ์ (Compliance Management) ลดลงเป็นอย่างมาก

Thesis	Automated Security Compliance Checking for Non-Logged Operations
Student	Nanta Janpitak
Student ID.	51066303
Degree	Doctor of Philosophy
Program	Information Technology
Year	2016
Thesis Advisor	Assoc.Prof.Dr.Chanboon Sathitwiriyawong

ABSTRACT

Compliance Management (CM) is the management process that an organization implements to ensure organizational compliance with relevant requirements and expectations. The most complicate process, costly and time consuming in CM is compliance checking because it requires a person who has a good policy knowledge to examine whether the current operations meet the policy requirements or not. This thesis proposes a methodology to enable the automation of compliance checking by using tools that support natural language processing (NLP). We use GATE (General Architecture for Text Engineering) as a tool to extract only the essential compliance requirements from the legal documents which always embodied in natural language and cannot be understood by the traditional computer system. We use Protégé to develop ontology which is a kind of natural language database to store the compliance checking data. Then the Jena semantic web technology is used to retrieve data from ontology to present the compliance evaluation and suggest the solution if the control violations are found.

In this thesis, we use the sample case from the operations that have no log in computer systems by using questions and answers principle to cooperate with the semantic web technologies. Since there are some operations that cannot be understood by computer systems, so using questions is one of the ways to gather the answers as operation log to evaluate their compliance. The proposed methodology can help non-auditor to perform the compliance checking, so that the time and cost of CM would be greatly reduced.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้อย่างสมบูรณ์ โดยได้รับความกรุณาเป็นอย่างดียิ่งจากท่านรองศาสตราจารย์ ดร.จันทร์บูรณ์ สถิตวิริยวงศ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ข้าพเจ้ารู้สึกซาบซึ้งและขอขอบพระคุณเป็นอย่างสูงในความเมตตาของท่านที่ได้ให้คำแนะนำพร้อมทั้งข้อเสนอแนะที่เป็นประโยชน์ในการทำวิจัย จนกระทั่งงานวิจัยสำเร็จลุล่วง

ขอขอบพระคุณคณาจารย์คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ให้กับข้าพเจ้า

ขอขอบคุณผู้บริหารบริษัทออโต้อัลลายแอนซ์ (ประเทศไทย) จำกัดที่อนุมัติให้ข้าพเจ้าได้ลาศึกษาโดยยังคงจ่ายค่าจ้างให้เป็นระยะเวลาหลายปี

สุดท้ายต้องขอขอบคุณคู่สมรสของข้าพเจ้า คุณอิสระ รอดทอง ที่เป็นเสมือนคู่คิดและเป็นกำลังใจที่ดีเสมอมา อีกทั้งยังคอยสนับสนุนค่าใช้จ่ายตลอดเวลาที่ศึกษา จนส่งผลให้การทำวิจัยในครั้งนี้สำเร็จลุล่วงไปได้ด้วยดี

สำหรับคุณงามความดีอันใดที่เกิดจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบให้กับมารดา ซึ่งเป็นที่รักและเคารพยิ่ง ตลอดจนครูอาจารย์ที่เคารพทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้และถ่ายทอดประสพการณ์ที่ดีให้แก่ข้าพเจ้า

นันทา จันทร์พิทักษ์

สารบัญ

หน้า

บทคัดย่อภาษาไทย..... I

บทคัดย่อภาษาอังกฤษ..... II

กิตติกรรมประกาศ..... III

สารบัญ..... IV

สารบัญตาราง..... VI

สารบัญรูป..... VII

บทที่ 1 บทนำ..... 1

1.1 ความเป็นมาและความสำคัญของปัญหา..... 1

1.2 ความมุ่งหมายและจุดประสงค์ของการศึกษา..... 2

1.3 ขอบเขตการวิจัย..... 2

1.4 ขั้นตอนของการดำเนินงานวิจัย..... 2

1.5 คำจำกัดความต่าง ๆ ที่ใช้บ่อยในงานวิจัยฉบับนี้..... 3

บทที่ 2 ทฤษฎีพื้นฐานและงานวิจัยที่เกี่ยวข้อง..... 4

2.1 กฎข้อบังคับ (Regulations) และมาตรฐาน (Standards) สากลที่สำคัญต่าง ๆ ที่นิยมใช้อยู่ในปัจจุบัน..... 4

2.2 ส่วนประกอบและค่าใช้จ่ายสำหรับการปฏิบัติตามกฎเกณฑ์ (Compliance)..... 9

2.3 งานวิจัยที่เกี่ยวข้องกับการบริหารจัดการการปฏิบัติตามกฎเกณฑ์ (Compliance Management)..... 11

2.4 งานวิจัยเกี่ยวกับการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ และการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ..... 13

2.5 การประมวลผลภาษาธรรมชาติ (Natural Language Processing) และงานวิจัยที่เกี่ยวข้อง..... 32

บทที่ 3 การออกแบบสถาปัตยกรรมสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ..... 41

3.1 การจัดทำ Security Compliance Management Framework และ Security Compliance Checking..... 41

3.2 การวิเคราะห์ปัญหาและจุดอ่อนของ Automated Security Compliance Checking 44

3.3 การเสนอสถาปัตยกรรมการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ..... 46

สารบัญ (ต่อ)

หน้า

บทที่ 4 การทดลองพัฒนาระบบการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง
โดยอัตโนมัติ..... 50
4.1 การพัฒนาออนโทโลยีเพื่อแยกองค์ความรู้ออกจากนโยบายโดยอัตโนมัติ..... 50
4.2 ขั้นตอนการพัฒนาออนโทโลยีสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์
ความมั่นคงโดยอัตโนมัติ..... 51
4.3 การสกัดกฎระเบียบหรือข้อกำหนดออกจากเอกสารทางกฎหมาย
(Information Extraction from Regulatory Documents)..... 63
4.4 การสกัดประโยคที่มีข้อความสำคัญออกจากเอกสารทางด้านกฎหมาย
(Requirements Extraction from Legal Documents)..... 63
บทที่ 5 การประเมินผลการวิจัย..... 71
5.1 การประเมินผลการวิจัยในส่วนของการสกัดประโยคที่มีความสำคัญ
ออกจากเอกสารทางกฎหมายต่าง ๆ..... 71
5.2 การประเมินผลการวิจัยโดยรวมจากการพัฒนาระบบการตรวจสอบ
การปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ..... 76
บทที่ 6 บทสรุปและข้อเสนอแนะ..... 78
6.1 บทสรุป..... 78
6.2 ข้อเสนอแนะ..... 79
เอกสารอ้างอิง..... 80
ประวัติผู้เขียน..... 84
ภาคผนวก ก ผลงานวิจัยที่ได้รับการตีพิมพ์เผยแพร่..... 85

สารบัญตาราง

ตารางที่ **หน้า**

4.1 สถานการณ์สมมุติสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง..... 52
4.2 ตัวอย่างคำถามเพื่อตรวจสอบความสามารถของออนโทโลยี..... 53
4.3 คลาสหลักและคลาสย่อยที่สำคัญ..... 54
4.4 ตัวอย่างความสัมพันธ์ คุณลักษณะและคุณสมบัติของแต่ละคลาส..... 55
4.5 ตัวอย่างกฎเกณฑ์และข้อจำกัดของความสัมพันธ์และคุณสมบัติของแต่ละคลาส..... 56
4.6 ตัวอย่างของข้อมูลจริงที่บันทึกลงในแต่ละคลาส..... 57
4.7 ตัวอย่างการจับคู่นโยบายกับ Auditor Questions, Compliance Lists
และ Non-Compliance Lists 60

สารบัญรูป

รูปที่	หน้า
2.1 ค่าใช้จ่ายสำหรับการ Compliance แยกตาม Compliance Cost Model.....	10
2.2 A Layer Model for Compliance.....	13
2.3 Framework for Automating Compliance.....	17
2.4 ExPDT Codes the Modalities into the Ruling.....	18
2.5 Workflow Execution and Analysis Infrastructure.....	19
2.6 Active Enforcement of Controls.....	21
2.7 OLAP Anomaly Detector.....	22
2.8 The Workflow of Privacy Evidence.....	23
2.9 Policy Language for Dynamic Systems.....	25
2.10 Example of Policy Rules.....	25
2.11 Adding an Entry to the Log File.....	26
2.12 Frame Security for Web Service Based On Regulatory Compliance.....	29
2.13 Implement of Security for Web Service Based On Regulatory Compliance.....	31
2.14 GATE TeamWare with Low and High Level Factor Annotations.....	38
2.15 A Section of Eudralex Regulation Showing How the System Annotates the Document Structure and Concepts.....	39
2.16 An Example of Regulatory Concepts and Their Relationship in the SemReg Ontolog....	39
2.17 Mapping Regulations to Validation Tasks in the SemReg and OntoReg Ontologies.....	39
3.1 Security Compliance Management Framework.....	42
3.2 ตัวอย่างของนโยบายหรือมาตรฐานที่ประยุกต์ใช้ในองค์กร.....	43
3.3 Security Compliance Checking Framework.....	43
3.4 The Combination of Compliance Requirements and Current Operations Condition.....	45
3.5 Seven Major Components of IT Infrastructure.....	46
3.6 Proposed Automated Security Compliance Checking.....	48
3.7 ผังงานของ Proposed Security Compliance Checking System.....	49
4.1 กระบวนการพัฒนาออนโทโลยี.....	51
4.2 ออนโทโลยีสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง ที่พัฒนาโดย Protégé.....	58

สารบัญรูป (ต่อ)

รูปที่ **หน้า**

4.3 OWLViz แสดงภาพกราฟของออนโทโลยีสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง..... 59
4.4 OntoGraf แสดงภาพกราฟของออนโทโลยีสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง..... 59
4.5 ผลลัพธ์จากการ Query ด้วยคำสั่ง SPARQL..... 62
4.6 สถาปัตยกรรมของการสกัดข้อมูลออกจากเอกสารทางด้านกฎหมาย..... 64
4.7 เอกสารที่โหลดเป็น Language Resource ใน GATE..... 65
4.8 Gazetteer List ใน GATE..... 66
4.9 JAPE Grammar ที่จะทำการสร้างหมายเหตุประกอบ ของประโยคที่เป็น Obligation..... 67
4.10 Customized ANNIE..... 67
4.11 Annotations ที่สร้างขึ้นจาก Customized ANNIE..... 69
4.12 ผลของการค้นหาด้วย ANNIC..... 70
4.13 การเอ็กซ์พอร์ต ANNIC..... 70
5.1 ผลการประมวลผลก่อนทำการแก้ไขเพื่อเพิ่มความถูกต้องครั้งที่ 1..... 72
5.2 ผลการประมวลผลก่อนทำการแก้ไขเพื่อเพิ่มความถูกต้องครั้งที่ 2..... 73
5.3 ตัวอย่างของประโยคที่ไม่ถูกสกัดออกมาเนื่องจากการขึ้นหน้าใหม่..... 74
5.4 ตัวอย่างของประโยคที่ไม่ถูกสกัดออกมาเนื่องจากการขึ้นบรรทัดใหม่โดยที่ยังไม่จบประโยค..... 75
5.5 ผลการประมวลผลหลังจากทำการแก้ไขประโยคในเอกสารนำเข้า..... 76

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

คำว่า "Compliance" หมายถึง การปฏิบัติตามกฎระเบียบข้อบังคับและกฎหมาย ตลอดจนการปฏิบัติตามนโยบายด้านสารสนเทศและความมั่นคงปลอดภัยขององค์กรอย่างถูกต้องได้ตามมาตรฐาน

ในปัจจุบันนี้ กระแสของคำว่า "Compliance" กำลังมาแรงทั่วโลกรวมถึงประเทศไทยด้วย เพราะเรามีทั้งกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และกฎหมายเกี่ยวกับการกระทำผิดเกี่ยวกับคอมพิวเตอร์ที่ประกาศออกมาบังคับใช้กันแล้ว การที่ผู้บริหารขององค์กรใดมิได้ให้ความสำคัญกับเรื่องนี้ อาจก่อให้เกิดความเสี่ยงที่จะเกิดขึ้นกับองค์กรอย่างหลีกเลี่ยงไม่ได้ ยกตัวอย่างบริษัทที่ประสบปัญหาในสหรัฐอเมริกา เช่น บริษัท ENRON และ บริษัท WORLDCOM ก็ล้วนมีปัญหาเรื่องความไม่โปร่งใสและการไม่ปฏิบัติตามข้อกฎหมายต่าง ๆ จนเป็นเหตุให้บริษัทต้องล้มละลายในที่สุด

เหตุการณ์อื้อฉาวทางด้านการเงินดังกล่าวข้างต้น รวมทั้งเหตุการณ์หลังจากวันที่ 11 กันยายน 2001 กระตุ้นให้เกิดการบัญญัติกฎหมายขึ้นมาเพื่อป้องกัน ตรวจจับและแก้ไขความผิดปรกติที่อาจจะเกิดขึ้นเช่นเดียวกันนั้น เมื่อมีการบัญญัติกฎหมายขึ้นมา ก็เกิดการบังคับใช้ ดังนั้นองค์กรต่าง ๆ ก็ต้องปฏิบัติตามอย่างหลีกเลี่ยงไม่ได้ การปฏิบัติตามข้อกำหนดเรียกได้ว่าเป็นการ Compliance ดังที่ได้กล่าวมาข้างต้น ส่วนการปฏิบัติในทางตรงกันข้ามกันเรียกว่าเป็น Non-Compliance ซึ่งผลกระทบของการเป็นองค์กรที่ Non-Compliance นั้นอาจส่งผลให้นักลงทุนหรือผู้ถือหุ้นขาดความเชื่อมั่นและขาดความเชื่อถือในด้านการเงินของบริษัท หรือแม้แต่อาจถูกเบี้ยปรับจากรัฐบาล

การบริหารจัดการการปฏิบัติตามกฎเกณฑ์ (Compliance Management) โดยเฉพาะอย่างยิ่ง การตรวจสอบการปฏิบัติตามกฎเกณฑ์ (Compliance Checking) ได้กลายเป็นภาระงานที่สำคัญและยุ่งยาก รวมทั้งเป็นค่าใช้จ่ายก้อนใหญ่สำหรับองค์กร เนื่องจากเป็นกระบวนการที่สิ้นเปลืองเวลาเป็นอย่างสูงเพราะต้องใช้บุคลากรที่มีความรู้ความเชี่ยวชาญทางด้านกฎระเบียบนั้น ๆ ในการตรวจสอบ การใช้ระบบคอมพิวเตอร์แบบดั้งเดิมในการพัฒนาระบบงานคอมพิวเตอร์เพื่อรองรับการตรวจสอบให้เป็นไปอย่างอัตโนมัตินั้นค่อนข้างเป็นไปได้ยาก เนื่องจากกฎระเบียบข้อบังคับเหล่านี้ถูกเขียนขึ้นโดยภาษาธรรมชาติ (Natural Language) อีกทั้งต้องมีการปรับเปลี่ยนบ่อยและเพิ่มขึ้นเรื่อย ๆ เพื่อให้สอดคล้องกับกฎหมายที่ถูกบัญญัติโดยรัฐบาล ดังนั้นจึงถือว่าเป็นเรื่องท้าทายอย่างมากในการที่จะพัฒนาระบบงานที่ช่วยให้การตรวจสอบการปฏิบัติตามกฎเกณฑ์โดยอัตโนมัติ (Automated Compliance Checking)

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

1. เพื่อศึกษางานวิจัยที่อภิปรายถึงความสำคัญของการปฏิบัติตามกฎเกณฑ์ (Compliance) และปัญหาที่เกิดขึ้น

2. เพื่อศึกษางานวิจัยที่เกี่ยวข้องกับวิธีการลดภาระทางด้านการบริหารจัดการการปฏิบัติตามกฎเกณฑ์ (Compliance Management) โดยใช้เครื่องมือที่ช่วยให้การปฏิบัติตามกฎเกณฑ์โดยอัตโนมัติ (Automated Compliance) โดยมุ่งเน้นที่การปฏิบัติตามกฎเกณฑ์ความมั่นคงปลอดภัยของข้อมูลเป็นหลัก (Automated Security Compliance)

3. เพื่อศึกษางานวิจัยที่เกี่ยวข้องกับการพัฒนาเครื่องมือที่ใช้ในการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ (Automated Security Compliance Checking)

4. เพื่อศึกษางานวิจัยที่เกี่ยวข้องกับเครื่องมือที่ประมวลผลได้กับภาษาธรรมชาติ (Natural Language Processing)

5. เพื่อนำเสนอสถาปัตยกรรมสำหรับพัฒนาเครื่องมือที่ใช้ในการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ (Proposed Automated Security Compliance Checking Architecture)

1.3 ขอบเขตของการวิจัย

งานวิจัยนี้มีขอบเขตเพื่อศึกษาและนำเสนอเครื่องมือในการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติเพื่อช่วยประมวลผลในส่วนของกิจกรรมที่ปัจจุบันปฏิบัติงานด้วยคนเท่านั้น

1.4 ขั้นตอนของการดำเนินงานวิจัย

1. ศึกษางานวิจัยทางด้านแนวโน้มและผลกระทบของการปฏิบัติตามกฎเกณฑ์ (Compliance)

2. ศึกษาถึงส่วนประกอบ ต้นทุนหรือค่าใช้จ่ายของการปฏิบัติตามกฎเกณฑ์ (Compliance)

3. ศึกษางานวิจัยที่นำเสนอแนวคิดเกี่ยวกับการปฏิบัติตามกฎเกณฑ์โดยอัตโนมัติ (Automated Security Compliance)

4. ศึกษางานวิจัยที่นำเสนอผลงานที่เกี่ยวข้องกับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ (Automated Security Compliance Checking)

5. ศึกษางานวิจัยที่นำเสนอผลงานที่เกี่ยวข้องกับการประมวลผลภาษาธรรมชาติ (Natural Language Processing)

6. นำเสนอสถาปัตยกรรมเพื่อการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ (Automated Security Compliance Checking Architecture)

7. พัฒนาเครื่องมือตามสถาปัตยกรรมเพื่อการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ

8. จัดรูปแบบและเตรียมข้อมูลสำหรับการทดลองเพื่อวัดผลและประสิทธิภาพของเครื่องมือที่ได้นำเสนอ

9. สรุปผลการทดลอง

10. จัดทำรายงานการวิจัย

1.5 คำจำกัดความต่าง ๆ ที่ใช้บ่อยในงานวิจัยฉบับนี้

1. Compliance การปฏิบัติตามกฎเกณฑ์/ Non-Compliance การไม่ปฏิบัติตามกฎเกณฑ์
2. Compliance Management (CM) การบริหารจัดการการปฏิบัติตามกฎเกณฑ์
3. Compliance Checking การตรวจสอบการปฏิบัติตามกฎเกณฑ์
4. Security Compliance Checking การตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง
5. Law กฎหมาย
6. Regulation กฎข้อบังคับ
7. Standard มาตรฐาน
8. Best Practice วิธีการปฏิบัติที่เป็นเลิศ
9. IT Security Framework กรอบความมั่นคงปลอดภัยของไอที
10. Natural Language Processing การประมวลผลภาษาธรรมชาติ
11. Semantic เชิงความหมาย
12. Information Extraction การสกัดข้อความ
13. Ontology ออนโทโลยี
14. Logged การลงบันทึกผลการปฏิบัติงาน

บทที่ 2
ทฤษฎีพื้นฐานและงานวิจัยที่เกี่ยวข้อง

ในบทนี้เป็นการรวบรวมความรู้และข้อมูลพื้นฐานต่าง ๆ ที่เกี่ยวข้องกับกฎข้อบังคับ มาตรฐานสากลที่สำคัญในปัจจุบัน และหลักการของการปฏิบัติตามกฎเกณฑ์ (Compliance) รวมทั้งงานวิจัยที่เกี่ยวข้องกับการเครื่องมือและแนวคิดที่ใช้ในการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ

การรวบรวมข้อมูลจะแบ่งเป็นหัวข้อหลัก ๆ ดังนี้คือ

1. อธิบายอย่างย่อ ๆ ถึงกฎข้อบังคับ (Regulations) และมาตรฐาน (Standards) สากลที่สำคัญต่าง ๆ ที่นิยมใช้อยู่ในปัจจุบัน เช่น SOX, HIPAA, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 15408, ITIL, COBIT, PCI DSS เป็นต้น
2. ศึกษาถึงส่วนประกอบ และค่าใช้จ่ายสำหรับการ Compliance
3. ศึกษาค้นคว้างานวิจัยที่เกี่ยวข้องกับการจัดการด้าน Compliance
4. ศึกษาค้นคว้างานวิจัยที่เกี่ยวข้องกับ Automated Security Compliance และ Automated Security Compliance Checking
5. ศึกษาค้นคว้าเกี่ยวกับเครื่องมือที่ใช้ในการประมวลผลภาษาธรรมชาติ (Natural Language Processing)

2.1 กฎข้อบังคับ (Regulations) และมาตรฐาน (Standards) สากลที่สำคัญต่าง ๆ ที่นิยมใช้อยู่ในปัจจุบัน

2.1.1 SOX (Sarbanes-Oxley Act of 2002)

Sarbanes-Oxley Act of 2002 (หรือเรียกสั้นๆ ว่า SOX) เป็นกฎหมายที่ตราขึ้นบังคับใช้เพื่อป้องกันปัญหาด้านบัญชีการเงินที่ผิดพลาดและการฉ้อโกงภายในให้กับผู้ถือหุ้นและสาธารณชนทั่วไป หลังจากเกิดกรณีอื้อฉาวด้านการเงินของเอรอนและเวิลด์คอม โดยกฎหมายฉบับนี้ได้รับการร่างขึ้นจากคณะกรรมการ ตลาดหลักทรัพย์ของสหรัฐอเมริกา (SEC) ซึ่ง SOX นั้นไม่ใช่กฎหมายที่มีมาตรฐานที่ว่าด้วยเรื่องแนวทางการปฏิบัติของธุรกิจ หรือไม่ได้ระบุเจาะจงว่าองค์กรธุรกิจจะต้องจัดเก็บข้อมูลอย่างไร แต่เป็นการกำหนดว่าข้อมูลอะไรบ้างที่ต้องเก็บรักษาและจัดเก็บไว้นานเท่าไร โดยครอบคลุมชนิดข้อมูลทางธุรกิจทั้งหมด ไม่ว่าจะเป็นข้อมูลดิจิทัล ข้อมูลการแจ้งเตือนของระบบก็ตาม โดยทั้งหมดต้องจัดเก็บไว้ไม่น้อยกว่า 5 ปี และหากองค์กรใดไม่ปฏิบัติตามจะต้องถูกลงโทษปรับหรือจำคุก หรือทั้งสองอย่างรวมกัน

2.1.2 HIPAA (The United States Health Insurance Portability and Accountability Act of 1996)

HIPAA ย่อมาจาก The United States Health Insurance Portability and Accountability Act of 1996 เป็นกฎหมายที่มีสองมาตรา โดยมาตราแรกเกี่ยวเนื่องกับการปกป้องด้านประกันสุขภาพที่ครอบคลุมกลุ่ม บุคคลว่างงานหรือกำลังเปลี่ยนงาน และมาตราที่สองว่าด้วยเรื่องงานด้านธุรกรรมของโรงพยาบาล ซึ่งได้บัญญัติมาตรฐานที่เกี่ยวกับระบบงานข้อมูลสารสนเทศด้านสุขภาพ (Healthcare Information System) ไว้ โดยมาตรฐานดังกล่าวเกี่ยวข้องโดยตรงกับงานด้านเทคโนโลยีสารสนเทศ อันเนื่องมาจากการวางมาตรฐานตั้งแต่รูปแบบการจัดเก็บข้อมูล การรับส่งข้อมูลผ่านโพรโทคอล EDI การจัดการด้านความมั่นคงปลอดภัยของข้อมูลและการป้องกันข้อมูลส่วนบุคคลต่าง ๆ โดยมีรูปแบบข้อมูลที่ได้มาตรฐานเกี่ยวกับข้อมูลผู้ป่วย ข้อมูลการรักษาและข้อมูลด้านการเงิน และใช้หมายเลขรหัสส่วนตัวเพื่อแบ่งแยกหน่วยงาน หรือส่วนต่าง ๆ ที่เกี่ยวข้องออกจากกัน โดยมีจุดมุ่งหมายสูงสุดให้ทุกข้อมูลมีความเป็นส่วนตัวและความมั่นคงปลอดภัยจากการเข้าถึงของบุคคลที่ไม่ได้รับอนุญาต

มาตรฐาน HIPAA จะช่วยให้แต่ละโรงพยาบาลที่ได้รับการรับรอง สามารถดำเนินธุรกิจเชื่อมโยงถึงกันได้ ข้อมูลผู้ป่วยสามารถส่งผ่านเครือข่ายอินเทอร์เน็ตได้อย่างมั่นคงปลอดภัยบนมาตรฐานเดียวกัน ช่วยลดขั้นตอนพื้นฐานทางแพทย์ลง ให้ผู้ป่วยได้รับการรักษาที่รวดเร็วขึ้น มีความถูกต้องมากขึ้นและสร้างความมั่นใจด้านข้อมูลให้กับแพทย์ผู้รักษา

2.1.3 ISO/IEC 27001:2005 (Information Security Management System: ISMS)

ISO/IEC 27001:2005 (Information Security Management System : ISMS) เป็นมาตรฐานการจัดการข้อมูลที่มีความสำคัญเพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่อง กำหนดขึ้นโดยองค์กรที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศ คือ ISO (The International Organization for Standardization) และ IEC (The International Electrotechnical Commission) การประยุกต์ใช้ ISMS จะช่วยให้กิจกรรมทางธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง ช่วยป้องกันระบบข้อมูลสารสนเทศขององค์กรจากความเสี่ยงต่อภัยคุกคามต่าง ๆ เช่น การหลอกลวงทางคอมพิวเตอร์ การจารกรรมข้อมูล ไวรัสคอมพิวเตอร์ การเจาะเข้าโปรแกรมคอมพิวเตอร์และการโจมตีเข้าระบบ ฯลฯ นอกจากนี้ยังช่วยป้องกันกระบวนการทางธุรกิจจากความเสี่ยงหากเกิดภัยร้ายแรงต่าง ๆ เช่น แผ่นดินไหว วาตภัย อัคคีภัย อุทกภัย ฯลฯ

โครงสร้างระบบ ISO/IEC27001:2005 เป็นระบบพลวัตร (Dynamic System) ซึ่งอ้างอิงรูปแบบ PDCA Model (Plan Do Check Action) เป็นโครงสร้างระบบการบริหารที่เป็นสากลที่ใช้กันทั่วโลก โดย ISO/IEC27001:2005 เป็นระบบการจัดการความมั่นคงปลอดภัยของข้อมูล เพื่อให้ระบบข้อมูลสารสนเทศขององค์กรมีคุณสมบัติในด้านต่าง ๆ ดังต่อไปนี้

- Confidentiality เพื่อให้มั่นใจได้ว่าข้อมูลต่าง ๆ สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิเท่านั้น

- Integrity เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องครบถ้วนสมบูรณ์ โดยไม่ได้ถูกเปลี่ยนแปลงหรือแก้ไขจากผู้ที่ไม่ได้รับอนุญาต

- Availability เพื่อให้มั่นใจได้ว่าข้อมูลพร้อมที่จะใช้งานอยู่เสมอ โดยผู้ที่มีสิทธิในการเข้าถึงข้อมูลสามารถเข้าถึงได้ทุกเมื่อที่ต้องการ

2.1.4 ISO/IEC 27002:2013 (Code of Practice for Information Security Management)

ISO/IEC 27002:2013 (Code of Practice for Information Security Management) กล่าวถึงวิธีปฏิบัติที่จะนำไปสู่ ระบบบริหารจัดการความมั่นคงปลอดภัยที่องค์กรได้จัดทำขึ้น ซึ่งจะต้องเป็นไปตามข้อกำหนดในมาตรฐาน ISO/IEC 27001:2013 รายละเอียดของมาตรฐานนี้จะบอกถึงวิธีปฏิบัติในการลดความเสี่ยงที่เกิดจากจุดอ่อนของระบบโดยแบ่งเป็นหัวข้อหลักที่เกี่ยวข้องกับระบบ และให้แนวทางว่าผู้จัดทำควรปฏิบัติอย่างไร ซึ่งผู้ใช้สามารถเพิ่มเติมมาตรการหรือใช้วิธีการที่มีความมั่นคงปลอดภัยเพียงพอ หรือเหมาะสมตามที่องค์กรได้ประเมินไว้ ซึ่งจะมีทั้งหมด 133 หัวข้อ และแบ่งออกเป็น 11 หมวดหลัก

2.1.5 ISO/IEC 15408:2005/Common Criteria/ ITSEC

ISO/IEC 15408:2005/Common Criteria/ ITSEC มาตรฐานนี้ได้รับการพิมพ์เผยแพร่โดย ISO/IEC JTC1 กลุ่มองค์กรที่ให้ความร่วมมือกันจัดทำมาตรฐานกลางหรือข้อกำหนดร่วมกันที่เรียกว่า Common Criteria โดยส่วนใหญ่เป็นกลุ่มองค์กรในประเทศแถบยุโรป เป้าหมายในการร่างมาตรฐานกลางหรือข้อกำหนดร่วมนี้ จัดทำขึ้นเพื่อใช้เป็นเกณฑ์กลางในการวัดระดับความมั่นคงปลอดภัยว่าระบบต่าง ๆ ที่จัดทำขึ้น เมื่อนำมาเปรียบเทียบกับเกณฑ์นี้แล้วระบบนั้นจะมีความมั่นคงปลอดภัยอยู่ในระดับใด

2.1.6 COBIT

มาตรฐาน “COBIT” ย่อมาจาก “Control Objectives for Information and Related Technology” เริ่มพัฒนาโดยองค์กรระดับโลก คือ The Information Systems Audit and Control Association (ISACA) และ IT Governance Institute (ITGI) เป็นผู้ดูแลในปัจจุบัน (ISACA และ ITGI ตั้งอยู่ที่ประเทศสหรัฐอเมริกา) โดยมีวัตถุประสงค์เดิมเพื่อให้เป็นเครื่องมือ (Tools) หรือกรอบแนวทาง (Guideline) สำหรับการตรวจสอบภายในเทคโนโลยีสารสนเทศ อย่างไรก็ดี ต่อมาผู้บริหารธุรกิจ ผู้บริหารระบบสารสนเทศได้นำมาตรฐาน COBIT ไปประยุกต์ใช้กับองค์กร เพื่อกำกับดูแลระบบสารสนเทศด้วย

มาตรฐาน COBIT เป็นมาตรฐานหนึ่งที่อธิบายถึงรายละเอียดของกระบวนการทางเทคโนโลยีสารสนเทศ (Information Technology Process) ได้แก่ รายละเอียดของการเตรียมความพร้อมแต่ละ

ขั้นตอนว่าต้องทำอะไรบ้าง สิ่งไหนที่สำคัญ และมีทรัพยากรตัวใดบ้างที่ต้องพิจารณาเป็นพิเศษ รวมทั้งวัตถุประสงค์ของการควบคุมและแนวทางในการปฏิบัติ

มาตรฐาน COBIT เป็นทั้งแนวคิดและแนวทางการปฏิบัติ (Framework) เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสารสนเทศสำหรับองค์กรต่าง ๆ ที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดี (Best Practice) ซึ่งสามารถนำไปปรับใช้ได้ในทุกองค์กรสำหรับกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยโครงสร้างของมาตรฐาน COBIT ได้ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ (Business Process) สามารถแบ่งได้เป็น 4 กระบวนการหลัก (Domain) ได้แก่

- การวางแผนและการจัดการองค์กร (PO : Planning and Organisation)
- การจัดหาและติดตั้ง (AI : Acquisition and Implementation)
- การส่งมอบและบำรุงรักษา (DS : Delivery and Support)
- การติดตามผล (M : Monitoring)

ในแต่ละกระบวนการหลักข้างต้น มาตรฐาน COBIT แสดงวัตถุประสงค์ของการควบคุมหลัก (High-Level Control Objectives) รวมถึง 34 หัวข้อ และในแต่ละหัวข้อจะประกอบด้วยวัตถุประสงค์ของการควบคุมย่อยลงไปอีกขั้นหนึ่ง (Detailed Control Objectives) รวมถึง 318 หัวข้อย่อย พร้อมทั้งแนวทางการตรวจสอบ (Audit Guidelines) สำหรับแต่ละหัวข้ออีกด้วย

เวอร์ชั่นล่าสุดคือ COBIT 5 ซึ่งออกมาในปี ค.ศ. 2015

2.1.7 ITIL (IT Infrastructure Library)

มาตรฐาน ITIL นั้น เป็นมาตรฐานด้านความปลอดภัยจากประเทศอังกฤษ มีวัตถุประสงค์ในการสร้าง Best Practices สำหรับกระบวนการของ IT Service Delivery และ Support แต่ไม่ได้เป็นการกำหนด Framework ของการควบคุมในแนวกว้าง ITIL นั้นจะมุ่งไปทางการเสนอวิธีการในการปฏิบัติ แต่มีขอบเขตงานเพียงแค่ IT Service Management และมีความลึกในรายละเอียดของกระบวนการทำงาน ซึ่งมีวัตถุประสงค์ที่จะให้ทางฝ่ายระบบสารสนเทศ และ Service Management เป็นผู้นำไปใช้ ซึ่งได้จัดแบ่งกระบวนการเทคโนโลยีสารสนเทศ ดังนี้

- Security Management เป็นการบริหารไอทีโดยการสร้างข้อกำหนด ตรวจสอบผล และควบคุมรักษาความปลอดภัยของระบบด้านข้อมูล และบริการขององค์กรเมื่อมีผู้เกี่ยวข้องเข้าสู่ระบบเทคโนโลยีสารสนเทศ

- Change Management คือ การบริหารการเปลี่ยนแปลงเพื่อก่อให้เกิดความเชื่อมั่นในไอทีขององค์กร ซึ่งมีการใช้วิธีการปฏิบัติและกระบวนการที่มีมาตรฐานเพื่อที่จะจัดการกับการเปลี่ยนแปลงของสภาพแวดล้อมของระบบบนโปรดักชั่น เพื่อที่จะลดผลกระทบจากปัญหาเนื่องจากการเปลี่ยนแปลงเพื่อพัฒนาคุณภาพของบริการ

- Release Management เป็นการบริหารกระบวนการนำระบบออกให้ผู้ใช้สามารถใช้ระบบงานต่าง ๆ ได้ โดยเริ่มต้นจากการวางแผนเพื่อนำระบบออกใช้ เตรียมเอกสารของระบบเผยแพร่ และการจัดอบรมให้แก่ลูกค้า เพื่อให้เกิดความมั่นใจในระบบเทคโนโลยีสารสนเทศที่พัฒนาขึ้น

- Incident Management หรือเรียกว่า Help Desk หรือ Service Desk เป็นกระบวนการแก้ไขระบบให้สามารถกลับมาใช้งานได้ปกติ ซึ่งจะแก้ไขก็ต่อเมื่อมีการแจ้งปัญหาจากลูกค้า หรือผู้ใช้งาน โดยฝ่ายไอทีจะต้องจัดการแก้ไขปัญหาที่เกิดขึ้นดังกล่าวให้เสร็จสิ้นเร็วที่สุด เพื่อให้กระทบกับผู้เกี่ยวข้องน้อยที่สุด

- Problem Management เป็นการบริหารไอทีโดยการคิดเชิงรุก (Proactive) เพื่อลดปัญหาของระบบที่เกิดจากการแจ้งของผู้ใช้งาน มุ่งเน้นการวิเคราะห์ต้นเหตุของปัญหา รวมถึงการควบคุมความผิดพลาดที่อาจเกิดขึ้นในอนาคต ซึ่งมักจะเป็นการดำเนินการระยะยาว

- Service-Level Management คือการบริหารการให้บริการระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม และเป็นไปตามความต้องการของลูกค้า หรือผู้ที่มีส่วนเกี่ยวข้องในระบบด้านต่าง ๆ โดยฝ่ายไอทีสามารถให้คำมั่นในการดำเนินงานเพื่อการบริการที่มีศักยภาพแก่ลูกค้าได้

- Availability Management เป็นการบริหารระบบเทคโนโลยีสารสนเทศ เพื่อแสดงเปอร์เซ็นต์ความถูกต้องของข้อมูลจากระบบต่าง ๆ ที่องค์กรบริการแก่ลูกค้า โดยเจ้าหน้าที่เทคโนโลยีสารสนเทศมีหน้าที่ในการกำหนดลักษณะการใช้งาน ตรวจสอบการเข้าสู่ระบบของลูกค้าและควบคุมการบริการให้เกิดประสิทธิภาพสูงสุดแก่ลูกค้า

- Configuration Management เป็นกระบวนการของการวางแผนเพื่อรองรับการบริหารการเปลี่ยนแปลง ซึ่งจะเป็นการกำหนด ควบคุม และตรวจสอบความถูกต้องของ Configuration Item หรือ CI ให้มีความทันสมัยและถูกต้องอยู่เสมอ

2.1.8 GLBA/OCC

GLBA/OCC เป็นไกด์ไลน์ที่ออกแบบเพื่อช่วยธนาคารและสถาบันการเงินต่าง ๆ ให้สามารถปฏิบัติตามข้อกำหนด GLBA หรือ Gramm-Leach-Bliley Act ได้ง่ายขึ้น โดยได้ออกแนวทางที่ช่วยปกป้อง ตรวจสอบและตอบสนองต่อปัญหาการถูกโจมตีในระบบข้อมูลสารสนเทศสำหรับธุรกิจธนาคาร อีคอมเมิร์ซ โดยกำหนดให้ธนาคารต้องปกป้องข้อมูลส่วนบุคคลของลูกค้า ระบบต้องมีความสมบูรณ์พร้อมใช้งานและมีระบบตรวจสอบการโจมตี เพราะเมื่อเกิดข้อผิดพลาดด้านข้อมูลแม้เล็กน้อย แต่ก็เป็นผลให้ธุรกิจธนาคารต้องหยุดชะงัก กลายเป็นเพิ่มความเสี่ยง เพิ่มค่าใช้จ่ายในการแก้ไขปัญหา อาจถูกปรับจนทำให้รายได้ผลกำไรขององค์กรสูญหาย

2.1.9 PCI DSS (Payment Card Industry Data Security Standard)

มาตรฐาน PCI DSS ย่อมาจาก "Payment Card Industry Data Security Standard" เป็นมาตรฐานความมั่นคงปลอดภัยสารสนเทศที่แพร่หลายทั่วโลก รวบรวมโดยคณะกรรมการ Payment Card

Industry Security Standards Council (PCI SSC) มาตรฐานนี้ถูกกำหนดขึ้นเพื่อช่วยให้องค์กรต่าง ๆ ที่มีการรับชำระเงินด้วยบัตรเครดิต สามารถป้องกันการฉ้อโกงบัตรเครดิต โดยการควบคุมข้อมูลและช่องโหว่ต่าง ๆ ให้เข้มงวดมากยิ่งขึ้น และได้นำไปใช้กับทุกองค์กรที่เก็บรักษา ประมวลผล หรือรับส่งข้อมูลของผู้ถือบัตรเครดิต ไม่ว่าจะเป็นบัตรของค่ายใดก็ตาม

มาตรฐาน PCI DSS ได้เริ่มใช้ในโครงการรักษาความมั่นคงปลอดภัยข้อมูลของบัตรเครดิต 5 ค่ายยักษ์ คือ Visa, MasterCard, American Express, Discover และ JCB ซึ่งมีจุดหมายร่วมกันเพื่อยกระดับการคุ้มครองลูกค้า โดยสร้างความมั่นใจว่าผู้ขาย (ผู้รับชำระเงินด้วยบัตรเครดิต) มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมในการเก็บรักษา การประมวลผล และการรับส่งข้อมูลของผู้ถือบัตรเครดิต

2.2 ส่วนประกอบและค่าใช้จ่ายสำหรับการปฏิบัติตามกฎเกณฑ์ (Compliance)

ในหัวข้อนี้จะแสดงให้เห็นถึงค่าใช้จ่ายสำหรับในกรณีที่องค์กรใด ๆ ต้องการปรับกระบวนการและโครงสร้างพื้นฐาน (Infrastructure) ขององค์กรให้เป็นไปตามข้อกำหนดของกฎหมายหรือ Regulation ต่าง ๆ ซึ่งนั่นก็คือการทำให้เป็นองค์กรที่ปฏิบัติตามกฎเกณฑ์นั่นเอง

จากงานวิจัยชื่อว่า Understanding the Costs of Compliance [1] ขององค์กรที่ชื่อ Gartner โดย Bace J., Rozwell C., Feiman J. และ Kirwin B. ได้ทำการอ้างอิงถึงผลสำรวจและการวิเคราะห์ต่าง ๆ ที่สำคัญดังต่อไปนี้

- W. Mark Crain และ Thomas D. Hopkins นักวิจัยที่มีชื่อเสียงทางด้านนโยบายได้ประมาณการไว้ว่าการที่บริษัทจะทำให้ Compliance กับ Regulatory ต่าง ๆ ทำให้เกิดค่าใช้จ่ายได้ถึง $7000 ต่อปีต่อพนักงาน 1 คน

- ผลการสำรวจขององค์กรต่าง ๆ เช่น RHR International, องค์การที่ให้คำปรึกษาทางด้านการจัดการและองค์กรบริหารการเงินนานาชาติ (Financial Executives International) และสมาคมผู้เชี่ยวชาญของ CFO ได้ระบุไว้ว่าค่าใช้จ่ายสำหรับการ Compliance จะเป็นสองถึงสามเท่าของค่าใช้จ่ายที่ได้ประมาณการไว้ตั้งแต่เบื้องต้นเนื่องจากข้อกำหนดของ SOX Section 404

- บริษัทมหาชนต่าง ๆ ที่มีเงินรายได้ต่อปีน้อยกว่า $1 พันล้าน ต้องใช้เงินโดยเฉลี่ยประมาณ $1.8 ล้าน สำหรับการทำให้ Compliance กับ SOX Section 404

- จาก Foley & Lardner องค์กรทางด้านกฎหมายแห่งชาติ ระบุว่าบริษัทต่าง ๆ ที่มีเงินรายได้ต่อปีน้อยกว่า $1พันล้าน ต้องใช้เงินโดยเฉลี่ยประมาณ $2.9 ล้าน สำหรับการทำให้ Compliance กับ SOX

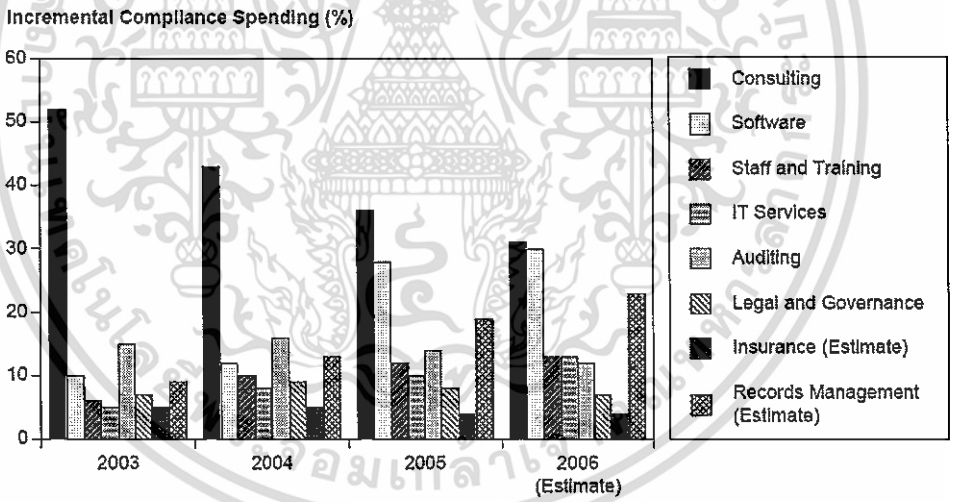
- จากการศึกษาโดย CRA International สำหรับ Big Four Accounting Companies พบว่าค่าใช้จ่ายในปีแรกสำหรับการ Compliance กับ SOX 404 สำหรับบริษัทมหาชนที่มีรายได้ต่อปีมากกว่า $7 พันล้านนั้นจะมากกว่า $8.5 ล้าน

- จากผลการสำรวจของ Gartner เองในปี 2005 พบว่าค่าใช้จ่ายสำหรับการจัดการด้าน IT Compliance นั้นเพิ่มขึ้น 10 – 15 % ของงบประมาณรายปีทางด้านไอที

นอกจากนี้ Gartner ได้ทำการวิเคราะห์โดยแบ่งออกเป็นส่วน ๆ ตาม Model ของ Compliance Cost ซึ่งประกอบไปด้วย

- Consulting ค่าใช้จ่ายที่เกิดจากการจ้างผู้เชี่ยวชาญมาเป็นที่ปรึกษา
- Software ค่าใช้จ่ายที่เกิดจากการติดตั้งซอฟต์แวร์ที่ช่วยในการ Compliance
- Staff and Training ค่าใช้จ่ายที่เกิดจากการจ้างและอบรมพนักงานให้เรียนรู้และเข้าใจในกระบวนการที่เกี่ยวข้องกับการ Compliance
- IT Service ค่าใช้จ่ายในส่วนของฝ่ายไอทีสำหรับการ Compliance
- Auditing ค่าใช้จ่ายที่เกิดจากการจ้างผู้ตรวจสอบ
- Legal and Governance ค่าใช้จ่ายที่เกิดจากการติดต่อสื่อสารกับหน่วยงานราชการ
- Insurance ค่าใช้จ่ายที่เกิดจากการประกัน
- Record Management ค่าใช้จ่ายที่เกิดจากการจัดการทางด้านการบันทึกข้อมูลต่าง ๆ

ซึ่งจากการสำรวจค่าใช้จ่ายแยกตามส่วนประกอบตั้งแต่ปี 2003 ถึงปี 2006 แสดงได้ดังรูปที่ 2.1



รูปที่ 2.1 ค่าใช้จ่ายสำหรับการ Compliance แยกตาม Compliance Cost Model

จากรูปแสดงให้เห็นว่าค่าใช้จ่ายที่สูงสุดและสูงมากคือค่าใช้จ่ายของที่ปรึกษา (Consultant) เนื่องจากในระยะเริ่มแรกบริษัทต่าง ๆ ยังไม่มีความรู้ความชำนาญในการปฏิบัติว่าต้องทำอย่างไรบ้าง การตีความกฎหมายหรือ Regulations ต่าง ๆ ก็เป็นเรื่องยาก เพราะในเนื้อความของกฎหมายเหล่านั้นไม่ได้ระบุชัดเจนว่าต้องทำอย่างไรบ้างในการ Compliance จึงต้องมีการจ้างที่ปรึกษาที่เป็นผู้เชี่ยวชาญมาให้คำปรึกษา ค่าใช้จ่ายทางด้านที่ปรึกษาลดลงเรื่อย ๆ ซึ่งสวนทางกับค่าใช้จ่ายทางด้านซอฟต์แวร์ นั่นแสดงให้เห็นว่าในปีหลัง ๆ บริษัทเริ่มหันมาพึ่งซอฟต์แวร์ที่ช่วยในการ

Compliance มากขึ้น ทำให้ค่าใช้จ่ายในการจ้างที่ปรึกษาลดลง ถึงแม้แนวโน้มของค่าใช้จ่ายทางด้านที่ปรึกษาจะลดลง แต่ก็ยังไม่มากพอ เนื่องจากยังไม่มีซอฟต์แวร์หรือเครื่องมือใด ๆ ที่สามารถแทนที่ที่ปรึกษาได้แบบครบวงจร องค์กรยังคงต้องพึ่งพอความช่วยเหลือของที่ปรึกษาอย่างมากในการบรรลุสู่การเป็นบริษัทที่ Compliance

2.3 งานวิจัยที่เกี่ยวข้องกับการบริหารจัดการการปฏิบัติตามกฎเกณฑ์ (Compliance Management)

ในปัจจุบันพบว่าการบริหารจัดการการปฏิบัติตามกฎเกณฑ์ (Compliance Management: CM) ได้กลายเป็นภาระที่หนักหน่วงขึ้นเรื่อย ๆ สำหรับหลาย ๆ องค์กรเนื่องจากกระบวนการที่มีความยุ่งยาก ต้องใช้เวลา ค่าใช้จ่ายและแรงงานอย่างมากมาย จากผลของงานวิจัยที่ผ่านมา ผู้เชี่ยวชาญส่วนใหญ่ลงความเห็นว่ากระบวนการการปฏิบัติตามกฎเกณฑ์ ควรจะต้องเป็นแบบอัตโนมัติ (Automated) ให้มากที่สุดเท่าที่จะเป็นไปได้

2.3.1 การปฏิบัติตามกฎหมายหรือข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

จากบทความ Regulatory Compliance and Information Security [2] โดย Igli Tashi ได้ให้ความกระจ่างเกี่ยวกับความสัมพันธ์ระหว่าง Regulatory Compliance และระดับความปลอดภัยโดยรวมสำหรับองค์กร โดยได้อธิบายถึงความแตกต่างของคำว่า Compliance และ Conformity ไว้ดังนี้

Compliance มักจะถูกอ้างอิงถึงไปในเรื่องของกฎหมายหรือข้อกำหนดจากรัฐบาลซึ่งมักถือว่าเป็นข้อบังคับที่ต้องถือปฏิบัติ ในกรณีนี้ Compliance ถือเป็นภารกิจที่สำคัญสูงสุด

Conformity ถูกใช้มากในมุมมองของการปรับแต่งให้เหมาะสมเพื่อให้มั่นใจว่ามีการบริหารจัดการระบบความมั่นคงปลอดภัยด้านไอที และการควบคุมบริหารความเสี่ยงที่ดี

หรืออีกนัยหนึ่ง Compliance คือความสามารถขององค์กรที่จะปฏิบัติโดยตั้งมั่นอยู่บนกฎหมาย (Laws) กฎเกณฑ์ (Rules) มาตรฐาน (Standards) และกฎข้อบังคับ (Regulations) ในขณะที่ Conformity คือการกระทำที่มีความสอดคล้องกับบางมาตรฐานหรือ Authority ที่เฉพาะเจาะจง

ในบทความนี้ยังได้กล่าวถึงประโยชน์ที่จะได้รับจากการประเมินระดับของการ Compliance เป็นประจำคือ

- ปรับปรุงระดับของความปลอดภัยโดยการบังคับให้คนที่ไม่เคยทำอะไรเลยได้ทำอะไรบ้าง
- ได้รับผลในทางบวกด้านเศรษฐกิจโดยการเปิดเผยสถานะทางด้านความปลอดภัยที่สร้างความสบายใจและความเชื่อมั่นให้กับคู่ค้า
- สร้างความตระหนักรู้อย่างลึกซึ้งทางด้านความปลอดภัยเพราะ Regulations ต่าง ๆ ต้องเกี่ยวข้องกับผู้บริหารระดับสูงมากขึ้นเรื่อย ๆ

ผู้เขียนยังได้ทำการเชื่อมโยงความสัมพันธ์ของการ Compliance กับ Information Security โดยอ้างอิงจากรายงานการสำรวจ 2006 Global Security Survey พบว่า Regulatory Compliance เป็นลำดับหนึ่งของห้าสิ่งที่ได้รับความสนใจเป็นพิเศษ ประมาณ 70% ของผู้ตอบแบบสำรวจ แนวทางแบบเดียวกันพบได้ในการสำรวจของ Big Four's Security Survey ในปีเดียวกัน ซึ่งได้สรุปเกี่ยวกับแนวโน้มเอาไว้ว่า

- แนวโน้มที่ 4: ผลกระทบของการ Compliance จะสูงขึ้นเรื่อย ๆ

- แนวโน้มที่ 5: Compliance คือการสร้างทีมงานร่วมระหว่าง Information Security และฟังก์ชั่นทางธุรกิจอื่น ๆ

- แนวโน้มที่ 6: Compliance คือการปรับปรุง Information Security

2.3.2 ความเกี่ยวข้องของบุคลากรไอทีกับ Corporate Compliance

จากบทความ Corporate Compliance and Its Implications to IT Professionals [3] โดย Venkat N. และ Jagadeesh N. ได้ทำการวิเคราะห์ถึงความเกี่ยวพันระหว่าง Corporate Compliance ซึ่งหมายถึงความต้องการที่องค์กรจะทำตามข้อกำหนดต่าง ๆ ว่าเกี่ยวพันกับไอทีอย่างไร โดยมุ่งเน้นไปที่ความสำคัญของไอทีในการพัฒนาซอฟต์แวร์ที่ช่วยในการ Compliance ของบริษัท ผู้เขียนได้แนะนำว่าควรจะบรรจุบทเรียนเกี่ยวกับการ Compliance ไว้ในระหว่างการเรียนการสอนระดับวิทยาลัย และเนื่องจากการดำเนินการทางธุรกิจในปัจจุบันต้องพึ่งพาอาศัยระบบคอมพิวเตอร์เป็นอย่างมาก ดังนั้นบุคลากรไอทีจึงควรจะต้องมีบทบาทเป็นผู้นำในการจัดหาวิธีการที่จะทำให้องค์กรบรรลุตามข้อกำหนดของการ Compliance

ในปัจจุบันมีผลิตภัณฑ์ในตลาดอยู่บ้างที่ผลิตขึ้นมาช่วยในการปฏิบัติให้ตรงตามข้อกำหนดของ Regulations ต่าง ๆ ความสามารถของผลิตภัณฑ์เหล่านี้มีตั้งแต่การจัดการกับการเก็บข้อมูลแบบส่วนกลาง (Centralized Repository) เพื่อพิสูจน์ให้เห็นถึงการ Compliance, ผลิตภัณฑ์ที่เกี่ยวกับการรายงานสำหรับ Compliance Monitoring, การปกป้องข้อมูลส่วนบุคคลของลูกค้า หรือการป้องกันและตรวจจับการปฏิบัติที่ผิดกฎหมาย แต่ผลิตภัณฑ์เหล่านี้ยังอยู่ในขั้นของการวิวัฒนาการและเป็นที่คาดหวังว่าจะสมบูรณ์ในอีกไม่กี่ปีข้างหน้า ซึ่งบริษัทจะต้องรอบคอบในการที่จะเลือกใช้ผลิตภัณฑ์เหล่านี้

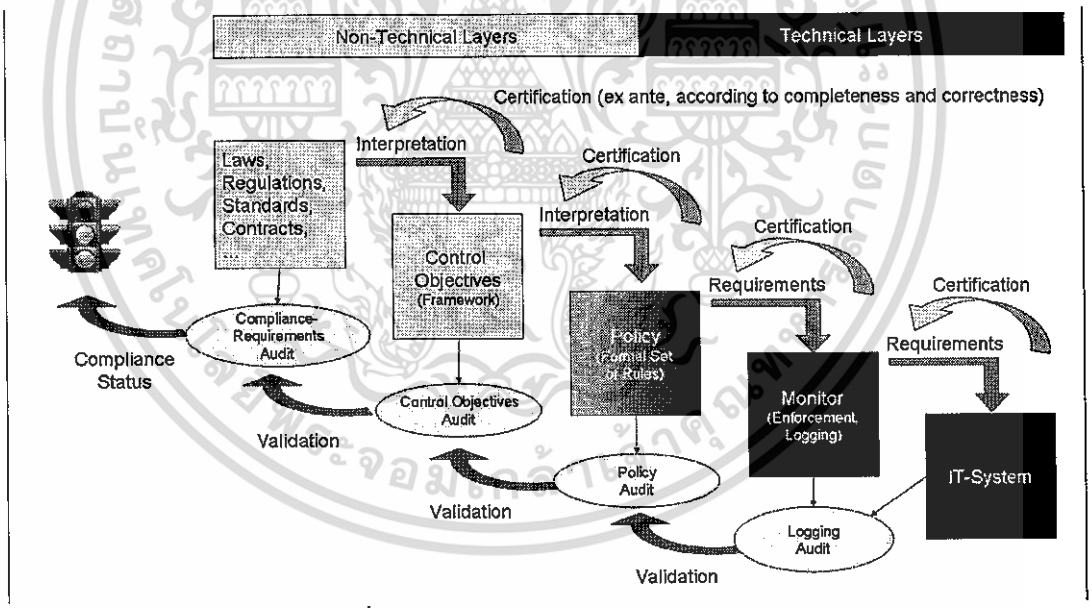
เนื่องจากผลกระทบทางด้านสังคมและการเงินจากการเป็นบริษัทที่ Non-Compliance ดังนั้นความรู้ทางด้านการ Compliance กับ Regulations จึงกลายมาเป็นส่วนที่ควบรวมเข้ากับการศึกษาของบุคลากรไอที ผู้เขียนแนะนำให้มีการควบรวมหัวข้อของการ Compliance เข้ากับวิชาทางด้าน Software Engineering โดยใช้กรณีศึกษาของการ Compliance หรือ Non-Compliance ในปัจจุบันเป็นบทเรียน

2.4 งานวิจัยเกี่ยวกับการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติและการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ

มีการนำเสนอวิธีการหลากหลายที่จะช่วยให้การปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ (Automated Security Compliance)

2.4.1 การแบ่งแยกประเภทของข้อกำหนดเพื่อการปฏิบัติตามแบบอัตโนมัติ

จากบทความ A Classification Model for Automating Compliance [4] โดย Sackmann S., Kähmer M., Gilliot M. และ Lowis L. ได้นำเสนอวิธีการจัดแบ่งประเภท (Classification Scheme) สำหรับวิธีการที่มีอยู่แล้ว ซึ่งทำให้เข้าใจมุมมองต่าง ๆ ของการทำให้เป็นอัตโนมัติของการปฏิบัติตามกฎเกณฑ์โดยการใช้รูปแบบเลเยอร์ (Layer Model) ดังแสดงในรูปที่ 2.2 ในการเชื่อมโยงความเกี่ยวพันระหว่างกฎหมายหรือข้อบังคับเข้ากับระบบสารสนเทศ ซึ่งจากโมเดลนี้ "Policy Layer" จะเป็นเหมือนการเชื่อมโยงระหว่างข้อกำหนดที่เป็น Non-Techical Compliance เข้ากับการนำระบบสารสนเทศไปใช้งานซึ่งเป็นแบบ Technical Compliance ระดับของการบรรลุผลสำเร็จของรูปแบบอัตโนมัตินี้ขึ้นอยู่กับลักษณะของภาษาของนโยบายที่สำคัญนั้น ๆ



รูปที่ 2.2 A Layer Model for Compliance

รูปที่ 2.2 ได้นำเสนอห้าเลเยอร์ที่ครอบคลุมทั้งประเด็นที่เป็น Technical และ Non-Technical

1. Laws and Regulations: Compliance Requirements กำหนดว่าอะไรบ้างที่จำเป็นต้องยึดติด เช่น กฎข้อบังคับของรัฐบาล (Government Regulations) เงื่อนไขของสัญญา (Contractual Terms) ข้อตกลงการค้า (Trading Agreements) มาตรฐานนโยบายภายใน (Internal Policies Standards)

2. Control Objectives: กลั่นกรองกฎหมายและกฎข้อบังคับให้เป็น Control Objective ของแต่ละองค์กร แต่ยังคงเป็นภาษาไม่มีรูปแบบ เป็นภาษาแบบธรรมชาติ

3. Policies: กลั่นกรอง Control Objectives ให้มาเป็นกฎเกณฑ์ที่เป็นทางการ โดยอธิบายว่าทำอย่างไรในการควบคุมเป้าหมายขององค์กรในสภาวะแวดล้อมของไอที

4. Monitors: กำหนดกลไกทางด้านไอทีที่จะบังคับและควบคุมให้ทำตามนโยบาย

5. IT-System: การนำกลไกการควบคุมที่เป็นระบบไอทีมาใช้งานจริง

2.4.1.1 Layer 1: Laws and Regulations

เลเยอร์สูงสุดที่ประกอบไปด้วยกฎหมาย ข้อบังคับ มาตรฐาน สัญญา เป็นต้น เพื่อโต้ตอบต่อเหตุการณ์อื้อฉาวทางการเงินที่เกิดขึ้นบ่อย ๆ การออกกฎหมายหรือพระราชบัญญัติกลายมาเป็นสิ่งที่ประยุกต์ใช้เป็นสำคัญในเร็ว ๆ นี้ กฎหมายที่โด่งดังที่สุดคือ SOX ซึ่งประกาศใช้เมื่อปี 2002 เพื่อปกป้องผู้ถือหุ้นหรือสังคมโดยรวมให้ปราศจากการกระทำที่ฉ้อโกงและความผิดพลาดทางด้านการบัญชีขององค์กร ผลที่ตามมาจากการเป็นองค์กรที่ Non-Compliance คือค่าปรับที่รุนแรงหรือแม้แต่การถูกจำคุก กฎหมายอื่น ๆ ที่สำคัญเช่น Graham-Leach-Bliley Act (GLBA) ซึ่งเป็นกฎหมายเพื่อปกป้องข้อมูลทางด้านการเงินของผู้บริโภคที่อยู่ในความดูแลของธนาคาร หน่วยงานทางด้านหลักทรัพย์ หรือบริษัทประกันชีวิต และบริษัทอื่น ๆ ที่ให้บริการทางด้านการเงิน หรือ Health Insurance Portability and Accountability Act (HIPAA) of 1996 ที่เป็นกฎหมายเกี่ยวกับการปกป้องข้อมูลส่วนบุคคลทางด้านสุขภาพที่อยู่ภายใต้การดูแลของหน่วยงานสุขภาพทั้งหลาย

ข้อกำหนดอื่น ๆ จากหน่วยงานกลางที่เกี่ยวกับมาตรฐานทางด้านความปลอดภัย เช่น NIST Handbook หรือ ISO Standard Code of Practice for Information Security Management (ISO 17799) (ในปัจจุบันคือ ISO 27000 Series) ซึ่งมาตรฐานเหล่านี้ให้แนวทางในการปกป้องดูแลสภาวะแวดล้อมทางด้านไอทีให้ปราศจากการฉ้อโกงและการจารกรรม เช่นการควบคุมและจำกัดการเข้าถึงข้อมูลที่สำคัญ หรือบังคับให้มีการกำหนดการแบ่งแยกหน้าที่ (Separation of Duty) สำหรับการทำธุรกรรมทางด้านการเงิน

กฎข้อบังคับ (Regulations) จะระบุข้อกำหนดที่ค่อนข้างคลุมเครือ โดยบอกว่า “what” ที่จะต้องทำในระดับที่ค่อนข้างเป็นนามธรรม ซึ่งเข้าใจยาก โดยที่ไม่ได้บอกแนวทางว่า “how” จึงจะบรรลุผลข้อกำหนดนั้น

2.4.1.2 Layer 2: Control Objectives

การเปลี่ยนรูปของข้อกำหนดระดับสูงสุดมาเป็นรูปแบบ Machine-Readable จำเป็นต้องใช้การตีความอย่างมาก เนื่องจากกฎหมายและกฎข้อบังคับเกือบทั้งหมดนั้นคลุมเครือและเป็นนามธรรม ดังนั้นขั้นตอนระหว่างกลางคือการเปลี่ยนรูปของข้อกำหนดระดับสูงสุดมาเป็น Control Objectives ซึ่งในระดับของ Control Objectives นั้นสามารถชี้แจงได้มากขึ้นในรายละเอียดว่าทำอย่างไรจึงจะ

บรรลุผลของข้อกำหนด ซึ่งสิ่งเหล่านี้ต้องการการตีความที่ถูกต้องและสมบูรณ์ จำเป็นอย่างยิ่งที่ต้องใช้ความรู้ที่ลึกซึ้งทางด้านกฎหมายในการกำหนด Control Objectives ที่ยังคงเป็นแบบไม่เป็นทางการและเป็นภาษาแบบธรรมชาติ การแปรรูปจากกฎหมายหรือกฎข้อบังคับไปเป็น Control Objectives นั้นก็ยังคงถือว่าห่างไกลจากคำว่าอัตโนมัติ (Automation)

ในขั้นเริ่มต้นได้ถูกนำเสนอโดย Breaux et al. [20] ในการใช้วิธีการของการแปลงข้อกำหนดในกฎหมายออกมาเป็นรูปแบบที่ระบุว่า "must" หรือ "must permit" แต่ผลของการแปลงเช่นนี้ก็ยังออกมาเป็นรูปแบบที่เป็นภาษาธรรมชาติและไม่เป็นนโยบายที่เป็นทางการ เช่นเดียวกันกับวิธีการของ Kabilan et al. [22] ที่นำเสนอศาสตร์ของการแบ่งกฎและข้อกำหนดออกมาเป็นบล็อก ซึ่งสามารถนำบล็อกดังกล่าวมาช่วยได้ด้วยระบบไอที แต่อย่างไรก็แล้วแต่ ยังคงต้องอาศัยความพยายามอย่างมากในการแปลความอย่างละเอียดด้วยคน

ในการปฏิบัติจริง บริษัทสามารถเชื่อมั่นได้กับมาตรฐานหรือเฟรมเวิร์กที่มีอยู่ในปัจจุบัน เช่น ITIL, COBIT หรือ COSO ที่ได้รับการยอมรับจากหน่วยงานที่ออกข้อกำหนดเหล่านั้นว่าเป็นมาตรฐานที่สามารถทำให้มีการควบคุมเพื่อการปฏิบัติตามกฎเกณฑ์ SOX ได้

ยกตัวอย่างแนวทางของ COSO ที่กำหนด 5 ส่วนประกอบสำหรับการควบคุมภายใน ซึ่งก็คือ Control Environment, Risk Assessment, Control Activities, Information and Communication, Monitoring ซึ่งการเป็นไปในทางเดียวกันกับ COSO ก็ถือว่าเป็นไปในแนวทางเดียวกับ SOX และเช่นเดียวกันกับ GRC Repository ของ SAP เขาใช้วิธีกำหนดกระบวนการว่าทำอย่างไรจึงจะบ่งชี้บัญชีที่สำคัญและกระบวนการที่เกี่ยวข้อง ทำอย่างไรจึงจะชี้วัดระดับความสำคัญของทรัพย์สินต่าง ๆ และทำอย่างไรจึงจะบ่งชี้ช่องโหว่และคำนวณความเสี่ยง จากการประเมินความเสี่ยงดังกล่าว ก็ทำการกำหนดกระบวนการขึ้นมาเพื่อให้มั่นใจว่าสามารถควบคุมให้ตรงตามข้อกำหนด ยกตัวอย่างการกำหนดการแบ่งแยกหน้าที่ (Separation of Duty) เพื่อป้องกันการออกคำสั่งซื้อโดยไม่ได้รับอนุญาตตามข้อบังคับใน SOX 404

- Regulation: ป้องกันการออก PO โดยไม่ได้รับอนุญาต
- Risk: การออก PO โดยไม่ได้รับอนุญาตและทำการชำระเงินกับซัพพลายเออร์ที่ไม่อยู่ในระบบอาจก่อให้เกิดความเสียหายทางด้านการเงิน
- Activity: การออก PO จะต้องได้รับการอนุมัติโดยพนักงานฝ่ายจัดซื้อสองคน

2.4.1.3 Layer3: Policies

เลเยอร์นโยบายถือเป็นสะพานที่เชื่อมต่อระหว่างเลเยอร์ที่เป็น Technical เข้ากับ Non-Technical ซึ่งต้องทำการแปลและเปลี่ยนรูปของ Control Objectives ซึ่งเป็นเลเยอร์ก่อนหน้านี้ให้เป็นรูปแบบที่เครื่องคอมพิวเตอร์เข้าใจได้ (Machine-Readable) ภาระงานสำคัญของเลเยอร์นี้คือการแมป Control Objective ให้เป็น System Component และ System Event

กิจกรรมที่ว่า "creation of purchase order" จากตัวอย่างที่ผ่านมาได้ถูกแมปไปเป็นกระบวนการทางธุรกิจในระบบงานจริงใน Term ที่ว่า "by two separate purchase officers" ซึ่งก็คือการแมปไปเป็นสอง Roles ใน IT-System

2.4.1.4 Layer 4: Monitor

เลเยอร์นี้เกี่ยวข้องกับการบังคับและควบคุมให้ระบบเป็นไปตามข้อกำหนดในนโยบาย จากประสพการณ์ของ Network and System Management แสดงให้เห็นว่าสามารถประสบผลสำเร็จโดยใช้กลไกของระบบปฏิบัติการ มิดเดิลแวร์ หรือแม้แต่ภายในโปรแกรมประยุกต์เอง

มีการจัดแบ่งกฎในนโยบายออกเป็นสามกลุ่มซึ่งต้องใช้กลไกทางด้านไอทีที่แตกต่างกันไปในการบังคับใช้ให้ตรงกับนโยบาย

- Enforceable Policy Rules: กฎที่สามารถบังคับใช้ได้โดยกลไกลการตรวจจับการฝ่าฝืน เช่น การตรวจสอบการขอเข้าใช้ข้อมูลก่อนที่จะ Grant Access ให้ว่าฝ่าฝืนต่อนโยบายหรือไม่

- Observable Policy Rules: กฎที่สามารถสังเกตุการณ์ได้ เช่นการกระทำใด ๆ ที่สามารถตรวจจับได้ในขณะปฏิบัติการ หรือตรวจสอบได้ภายหลังจากการตรวจสอบ Logs ของ Event Activities เช่น กฎที่ว่า "delete data before 9:00 p.m." ไม่สามารถบังคับใช้ได้ ณ เวลาปฏิบัติการ แต่สามารถตรวจจับได้โดยการตรวจสอบ ณ เวลา 9:01 p.m. ว่าข้อมูลได้ถูกลบแล้วหรือยัง

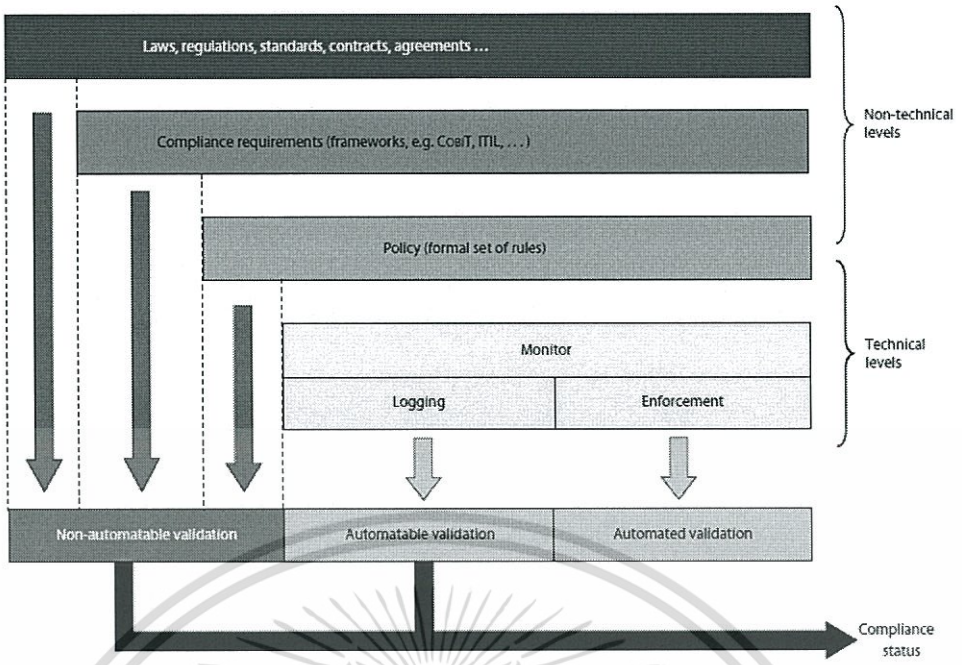
- Non-Observable Policy Rules: กฎที่ไม่สามารถสังเกตการณ์หรือตรวจสอบได้เลย เช่น "delete data after use" ไม่สามารถสังเกตุการณ์ได้ เหตุการณ์เช่นนี้จึงไม่สามารถตรวจสอบหรือสังเกตุการณ์ได้จนกว่าจะมีเหตุการณ์นั้น ๆ เกิดขึ้น

2.4.1.5 Layer 5: IT-System

เลเยอร์ที่ห้านี้เกี่ยวข้องกับระบบคอมพิวเตอร์ โดยในเลเยอร์นี้เป็นการนำกลไกที่ต้องการจากเลเยอร์ Monitor มาพัฒนาเป็นระบบที่ตอบสนองต่อการ Monitor ที่จำเป็น

2.4.2 เครื่องมือสำหรับการเปลี่ยนนโยบายเป็นภาษาที่เรียกว่า Machine-Readable

บทความก่อนหน้านี้เป็นการนำเสนอเชิงแนวความคิด หลังจากนั้นผู้เขียนบทความกลุ่มเดียวกันนี้ได้นำเสนอเครื่องมือที่พัฒนาจากแนวความคิดดังกล่าวในบทความที่ชื่อว่า ExPDT: A Policy-Based Approach for Automating Compliance [5] โดยเริ่มต้นจากการนำเสนอ Framework for Automating Compliance ดังรูปที่ 2.3 ซึ่งเป็นเฟรมเวิร์กที่เชื่อมโยงกับ Layer Model จากบทความที่ผ่านมา



รูปที่ 2.3 Framework for Automating Compliance

ผู้เขียนได้นำเสนอเครื่องมือที่ชื่อว่า The Extended Privacy Definition Tool (ExPDT) ซึ่งเป็นเครื่องมือสำหรับการดัดแปลงภาษานโยบายที่เป็นภาษาแบบทางการแต่ยังคงต้องใช้คนในการตีความมาเป็นภาษาแบบ Machine-Readable ซึ่งช่วยให้การ Monitor ซึ่งเป็นเลเยอร์ถัดไปมีความเป็นอัตโนมัติได้ง่ายยิ่งขึ้นโดยแบ่งเป็นส่วนประกอบดังนี้

2.4.2.1 Syntax

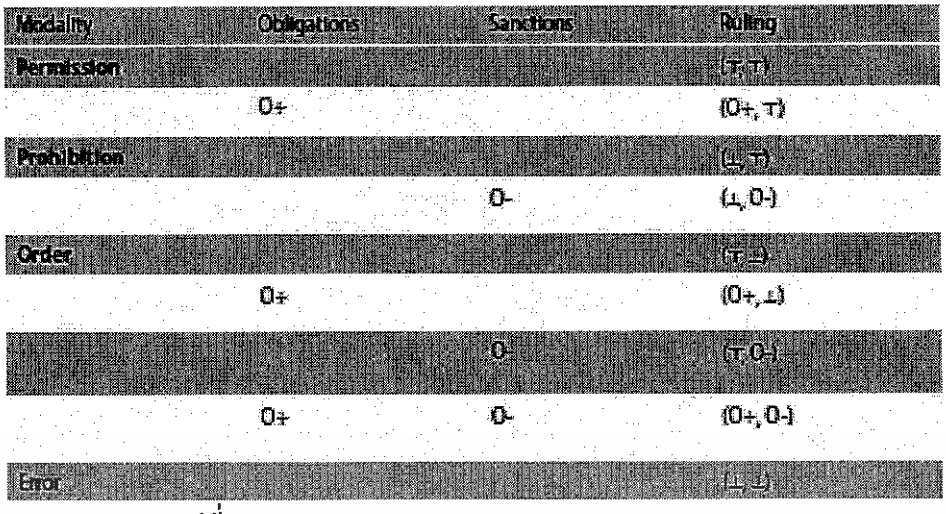
([¯](*User, Action, Data, Purpose*))+, *Conditions*, (*Ruling*)

ผู้เชี่ยวชาญทำการแปลงนโยบายให้อยู่ในรูปของ Machine-Readable โดยให้กำหนดตรงตาม Syntax

2.4.2.2 Semantic of Rule

ตัวอย่าง Semantic of Rule แสดงได้ดังรูปที่ 2.4

- Permission: พนักงานได้รับอนุญาตให้เปิด PO , Ruling: ($\top$, $\top$)
- Permission with Obligation: พนักงานได้รับอนุญาตให้เปิด PO แต่หัวหน้าจะได้รับการแจ้ง. Ruling: (notify, $\top$)
- Prohibition with Sanction: พนักงานไม่ได้รับอนุญาตให้เปิด PO ถ้าพวกเขาไม่ทำตามกฎ โดยทำการเปิด PO หัวหน้าจะได้รับการแจ้ง. Ruling: ($\perp$, notify)
- Compulsory Order: Administrator จะต้องทำการสำรองข้อมูลเป็นรายสัปดาห์. Ruling: ($\top$, $\perp$)



รูปที่ 2.4 ExPDT Codes the Modalities into the Ruling

2.4.2.3 Semantic of a Policy

1. เริ่มต้น result ด้วย $(\top, \top)$ และนำเสนอผล status ของการประเมินด้วย ν เป็นค่า default

2. ประเมินกฎแบบทีละหนึ่งตามลำดับความสำคัญ ถ้า rules's guard ถูกค้นหาพบโดย query และ

- ถ้าเงื่อนไขถูกประเมินผลเป็น 1 ผลของการประเมิน status ในขั้นสุดท้ายจะเป็น ν
- ถ้าเงื่อนไขถูกประเมินเป็น u ให้เพิ่ม rule's ruling ไปที่ result จากนั้นกำหนด status ν แล้วประมวลผลกฎต่อไป

3. ถ้า status ν นั้นใช้ได้ให้ส่ง result ตาม ruling และ status ν

4. ถ้า status ยังคงเป็นค่า default ไม่มี rule ใด ๆ ที่เข้ากันได้ ให้ส่งกลับค่า default ruling อีกครั้ง พร้อมกับ status ν

2.4.3 การช่วยให้การควบคุมภายในภายใต้ข้อกำหนดของ SOX แน่นหนายิ่งขึ้นโดยการใช้เทคโนโลยีทางด้านข้อมูล

Section 302 ของกฎหมาย SOX กำหนดให้ผู้บริหารระดับสูงต้องทำการรายงานงบการเงินของบริษัทเพื่อการรับรองความถูกต้องของข้อมูลทางด้านการเงินและมีการจัดการกระบวนการควบคุมภายในที่เกี่ยวข้องกับรายงานทางด้านการเงิน

ส่วน Section 404 กำหนดว่าในรายงานประจำปีของบริษัทจะต้องมีการรายงานเกี่ยวกับกระบวนการควบคุมภายใน ซึ่งจะต้องประกอบไปด้วย (i) โครงสร้างการบริหารสำหรับการประเมินผลการควบคุมภายใน (ii) การประเมินประสิทธิภาพของการควบคุมภายใน ณ ตอนสิ้นปีงบการเงิน (Fiscal Year) และ (iii) การรับรองระบบควบคุมภายในโดยผู้ตรวจสอบภายนอก

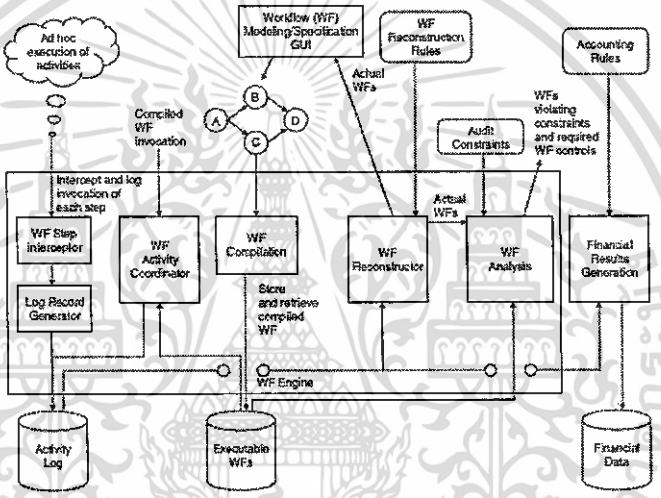
จากบทความ Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology [6] โดย Agrawal R., Johnson C., Kiernan J., และ Leymann, F. ได้ทำการนำเสนอ

วิธีการที่ใช้เทคโนโลยีทางด้านข้อมูลในการสนับสนุนให้เกิดการ Compliance ตามข้อกำหนดของ Section 302 และ Section 404 เพื่อช่วยสนับสนุนกระบวนการต่อไปนี้คือ

Management's Assessment of Controls หลังจากทำการกำหนดระบบการควบคุมภายในและปฏิบัติใช้จริงแล้ว ผู้บริหารจะต้องทำการประเมินผลของการปฏิบัติใช้และตรวจสอบว่ามีการควบคุมใดบ้างที่ล้มเหลวในการปฏิบัติ หรือมีจุดอ่อนใด ๆ บ้างในระบบควบคุมนั้น

Auditor's Evaluation of Controls จากการที่รายงานการควบคุมจะต้องมีการให้การรับรองจากผู้ตรวจสอบภายนอก ดังนั้นผู้ตรวจสอบจึงต้องทำการตรวจสอบเอกสารต่าง ๆ และทดสอบการควบคุมนั้นด้วยความเป็นอิสระ

สถาปัตยกรรมของแนวทางที่ผู้เขียนนำเสนอนี้แสดงได้ดังรูปที่ 2.5



รูปที่ 2.5 Workflow Execution and Analysis Infrastructure

ซึ่งประกอบไปด้วย 4 ส่วนประกอบหลักคือ

- Workflow Modeling
- Active Enforcement
- Workflow Auditing
- Financial Analytics for Anomaly Detection

2.4.3.1 Workflow Modeling

ส่วนประกอบแรกของสถาปัตยกรรมนี้คือ Workflow ("WF") Modeling ซึ่งเรามองกระบวนการควบคุมภายในเป็นกลุ่มของ Workflow แต่ละ Workflow ประกอบไปด้วยกิจกรรม (Activities) การควบคุมที่กำหนด เพื่อทำการกำหนดรูปแบบของ Workflow ในงานวิจัยฉบับนี้เน้นการใช้ Log ของ Activity ในอดีตมาเป็นตัวดำเนินการ

2.4.3.1.1 Activity Logging

เริ่มต้นด้วยการบันทึกข้อมูล Activity ทุก ๆ อย่างที่ทำกับ Transaction ไว้ใน Logs ซึ่งเก็บอยู่ในฐานข้อมูล ซึ่งเป็น Activity ทั้งหมดที่เกี่ยวข้องกับการสร้าง (Initiating) การอนุมัติสิทธิ์ (Authorizing) การบันทึก (Recording) การประมวลผล (Processing) การเปิดเผยข้อมูล (Disclosure) และการอ้างอิงสิทธิ์ต่าง ๆ (Related Assertion) ที่เกี่ยวข้องกับงบทางการเงิน ซึ่ง Logs ก็ต้องประกอบไปด้วยข้อมูลของ Activity ข้อมูลของผู้ที่ทำ Activity นั้น เวลาที่ดำเนินการ และข้อมูลอื่น ๆ ที่เกี่ยวข้อง

Activities ใด ๆ ที่ทำภายใน Workflow ระบบจะทำการบันทึกข้อมูลลงใน Logs

สำหรับ Activities ใด ๆ ที่กระทำนอกเหนือจาก Workflow System ระบบจะมีตัวสกัดจับที่ชื่อว่า WF Step Interceptor จะจับข้อมูลเหล่านี้แล้วส่งต่อไปยัง Log Record Generator

เช่นเดียวกัน เครื่องแม่ข่ายเองก็อาจตรวจจับ Activities ที่เรียกเข้ามาแล้วส่งต่อข้อมูลเหล่านั้นมายัง Log Record Generator

ระบบจัดการต่าง ๆ ภายในเครื่องแม่ข่ายก็อาจมีการตรวจจับ Activities ที่แยกตามชนิดของของเหตุการณ์เช่น Web Service Environment ก็อาจมีการส่ง Activities ผ่าน SOAP Header มายัง Log Record Generator

2.4.3.1.2 Modeling Required Workflows

ขั้นตอนต่อไปเราทำการคัดแยกข้อมูลของ Activity Logs เพื่อประกอบ Transaction ที่ผ่านมาเข้าเป็น Workflow แล้วใช้เป็นข้อมูล Baseline ในการกำหนดรูปแบบของ Workflow ที่เป็นแบบกิจวัตรประจำ (Routine)

ในแต่ละ Workflow ที่ต้องการต้องมีการกำหนดการควบคุมเกี่ยวกับการ Initiating, Authorizing, Documenting, Processing และ Reporting สำหรับแต่ละ Transaction เส้นทางของ Workflow จะถูกแปล (Compile) แล้วเก็บในฐานข้อมูล Executable WF ที่มีการปรับปรุงเพื่อการบังคับใช้และเพื่อจุดประสงค์ของการตรวจสอบ Workflow ที่ต้องการสามารถแก้ไขและปรับปรุงได้ตลอดเวลาแล้วส่งไปเพื่อทำการแปล (Compilation)

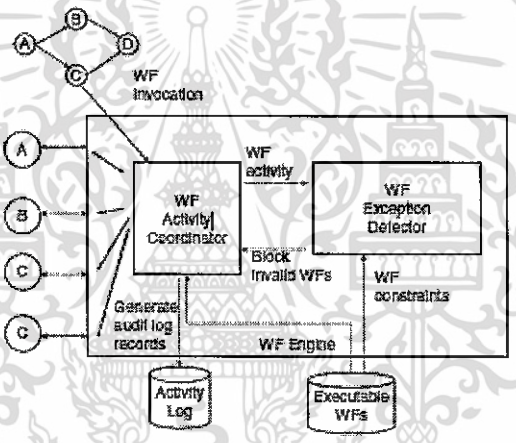
2.4.3.2 Active Enforcement

ส่วนประกอบที่สองเป็นการกำหนดควบคุม Workflow สำหรับกระบวนการทางธุรกิจที่เป็นไปตามข้อกำหนดหรือสิ่งที่บังคับใช้อยู่ในปัจจุบัน ส่วนนี้เป็นการสร้างความมั่นใจว่า Routine Transaction นั้นเป็นไปตาม Workflow ที่กำหนดไว้ ส่วนประกอบอื่น ๆ นั้น เราตั้งใจให้เป็นการจัดการกับ Non-Routine Transaction และการตรวจจับการกระทำที่เป็นการทุจริตต่าง ๆ ที่อยู่นอกเหนือจากระบบควบคุมภายใน

วิธีการหนึ่งของการบังคับใช้คือการนำข้อจำกัดของกระบวนการที่ไม่ยินยอมให้ Non-Compliant Transaction นั้นสามารถทำสำเร็จลงได้ เช่น Workflow ของการอนุมัติสิทธิ์ต่าง ๆ

วิธีการอื่น ๆ เช่นการยอมให้ Non-Compliant Transaction ประมวลผลได้สำเร็จแต่ทำการ Log ข้อยกเว้นต่าง ๆ ไว้

รูปที่ 2.6 แสดงถึงการจัดการระบบ Active Enforcement โดยที่ Workflow Engine ทำการจัดการและประสาน Activity ต่าง ๆ ใน Workflow เรียกว่า WF Coordinator ซึ่งจะทำการส่งผ่าน Activity ต่าง ๆ เข้าไปยัง WF Exception Detector ซึ่งทำการบ่งชี้ว่าแต่ละกิจกรรมนั้นเป็นไปตามข้อกำหนดใน Workflow หรือไม่ ถ้ากิจกรรมใดละเมิดกฎ Workflow Engine จะทำการสกัดกั้นเอาไว้ไม่ให้ดำเนินการต่อไป หรืออีกทางเลือกหนึ่งคือ Workflow Engine สามารถปล่อยให้ Activity นั้นผ่านไปได้แต่ทำการบันทึกข้อมูลการละเมิดนั้นไว้เพื่อจุดประสงค์ในการตรวจสอบในอนาคต



รูปที่ 2.6 Active Enforcement of Controls

2.4.3.3 Workflow Auditing

ส่วนประกอบที่สามนี้ทำการแบ่ง Workflow Auditing ออกเป็นสองชนิดคือ

- Compliance Verification
- Query-Based Auditing

ซึ่งส่วนประกอบนี้ทั้งผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอกสามารถใช้เพื่อประเมินความมีประสิทธิภาพของกระบวนการควบคุมภายใน

- Compliance Verification เป็นการ Workflow จากการปฏิบัติงานจริงมาประกอบกันแล้วเปรียบเทียบกับ Workflow ที่กำหนดเพื่อบ่งชี้ว่ามีการละเมิดการควบคุมหรือไม่

- Query-Based Auditing ทำให้บริษัทสามารถที่จะตรวจสอบ Activity Logs เพื่อสืบสวน Transaction ที่น่าสงสัยได้และเพื่อประเมินประสิทธิภาพของการควบคุมภายในอย่างเป็นระยะ ผลของการทำ Query-Based Auditing นี้จะส่งผลของ Workflow ที่ละเมิดกับกฎแบบเร่งด่วน

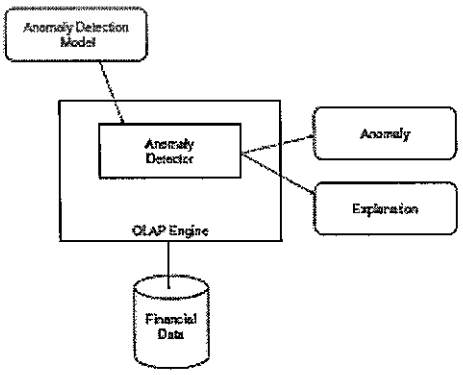
ผู้ตรวจสอบสามรรถวิเคราะห์ Workflow จากการปฏิบัติจริงโดยใช้ WF Analysis ในการค้นหา Workflow ที่ละเมิดกฎด้วยตัวผู้ตรวจสอบเอง ตัวอย่างเช่น ในระหว่างการประเมิน ผู้ตรวจสอบอาจต้องการที่จะสืบสวนผู้จัดการที่น่าสงสัยโดยร้องขอตรวจสอบการอนุมัติทุกรายการที่เกิดจากผู้จัดการคนนั้น หรือบางทีเธออาจจะร้องขอตรวจสอบทุก ๆ รายการในระหว่างช่วงเวลาใดเวลาหนึ่ง

2.4.3.4 Financial Analytics for Anomaly Detection

ส่วนประกอบสุดท้ายนี้เป็นการใช้วิธีการวิเคราะห์แบบ OLAP เพื่อค้นหาความผิดปรกติที่อาจจะเกิดขึ้นในข้อมูลทางด้านการเงินที่อาจก่อให้เกิดความผิดพลาดหรือความไม่เหมาะสมทางด้านการบัญชี ผู้ตรวจสอบภายนอกมักจะต้องค้นหาความผิดปรกติดังกล่าวนี้ในการตรวจสอบอย่างเป็นระยะ ซึ่งพวกเขาต้องทำการตรวจสอบรายงานที่มีความสำคัญต่าง ๆ ที่ไม่ถูกต้อง ซึ่งต้องการการตรวจสอบในเชิงลึกสำหรับรายการประจำวันต่าง ๆ และข้อมูลทางด้านบัญชีอื่น ๆ ที่เกี่ยวข้อง ระบบรายงานที่ใช้อยู่อาจไม่เพียงพอสำหรับการตรวจสอบความผิดปรกติดังกล่าว ผู้ตรวจสอบสามารถทำการวิเคราะห์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้นโดยการใช้เทคนิคของ OLAP ซึ่ง OLAP Cube สามารถจัดเตรียมความพร้อมสำหรับข้อมูลต่าง ๆ เช่น Drilldown, Roll-up และการคัดเลือกข้อมูลที่ผิดปรกติ อย่างไรก็ตาม วิธีการของ OLAP แบบมาตรฐานนั้นขึ้นอยู่กับการวิเคราะห์ข้อมูลที่ถูกเลือกค้นหาโดยการสมมุติฐานไว้ ซึ่งอาจไม่สามารถสดงผลได้อย่างที่ต้องการเนื่องมาจากขนาดของข้อมูล และการใช้เงื่อนไขการค้นหาที่ซับซ้อนอาจแสดงผลได้ไม่ถูกต้อง

ซึ่งแทนที่จะขึ้นอยู่กับนักวิเคราะห์ที่จะเป็นผู้เลือกค้นหา Cube View แต่สำหรับวิธีการนี้นำเสนอให้ใช้หลักการของ Discovery-Driven OLAP ซึ่งจะคัดเลือกความผิดปรกติให้หลายระดับแล้วชี้นำเพื่อการสำรวจในขั้นต่อ ๆ ไป

รูปที่ 2.7 แสดงถึงวิธีการตรวจจับความผิดปรกติโดย OLAP

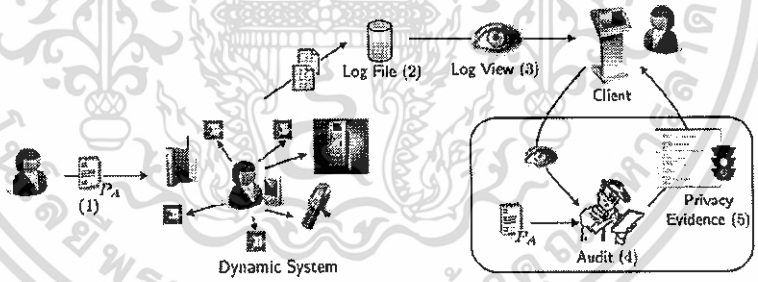


รูปที่ 2.7 OLAP Anomaly Detector

2.4.4 การตรวจสอบระบบจัดการข้อมูลความเป็นส่วนตัวแบบอัตโนมัติ

ระบบจัดการกับข้อมูลส่วนบุคคล (Identity Management Systems: IMS) เป็นสิ่งที่ขาดไม่ได้สำหรับระบบคอมพิวเตอร์ในเครือข่ายสมัยใหม่ เนื่องจากข้อมูลส่วนบุคคลส่วนใหญ่ในปัจจุบันจะอยู่ในความดูแลของคนกลางที่เราเรียกกันว่า Data Provider จึงมีการกำหนดระบบ IMS ขึ้นมาเพื่อให้ Data Provider ได้มีความตระหนักถึงความสำคัญของการควบคุม เพื่อป้องกันและปกป้องการเปิดเผยและการใช้งานข้อมูลส่วนบุคคล แต่อย่างไรก็แล้วแต่ Data Provider ในปัจจุบันซึ่งได้ให้คำสัญญาว่าจะปกป้องและดูแลข้อมูล โดยกำหนดนโยบายปกป้องความเป็นส่วนตัวขึ้นมา แต่ก็ยังไม่มีหลักฐานที่พิสูจน์ให้เชื่อถือได้ว่าพวกเขาได้ยึดถือปฏิบัติตามนโยบายนั้นจริง ดังนั้นผู้บริโภคจึงยังมีความหวั่นกลัวว่าข้อมูลความเป็นส่วนตัว (Privacy) ของพวกเขาอาจถูกเปิดเผยหรือแบ่งปันอย่างไม่ถูกต้องให้กับบุคคลที่สามหรือว่านำไปใช้ในวัตถุประสงค์อื่น ๆ นอกเหนือจากที่พวกเขาต้องการ

บทความ Automated Privacy Audits to Complement the Notion of Control for Identity Management [7] โดย Rafael Accorsi ได้นำเสนอถึงแนวความคิดที่เรียกว่า หลักฐานความเป็นส่วนตัว (Privacy Evidence) ซึ่งเป็นหลักการของเก็บข้อมูลทุกอย่างมาเป็นหลักฐานแล้วสร้างระบบการตรวจสอบแบบอัตโนมัติ โดยใช้เทคนิคที่เรียกว่า Building Block ซึ่งมี Workflow ของการทำงานดังรูปที่ 2.8



รูปที่ 2.8 The Workflow of Privacy Evidence

การทำงานจากรูป อธิบายได้เป็นขั้นตอนดังนี้คือ

1. Data Provider A กำหนดนโยบาย PA ขึ้นมาแล้วส่งให้กับผู้บริโภค เนื่องจากเรามุ่งเน้นที่ระบบ Dynamic ดังนั้นเราจึงมั่นใจว่าระบบมีการสื่อสารกันแบบปฏิสัมพันธ์ (Interaction) เราตั้งสมมุติฐานว่านโยบายได้ถูกสื่อสารก่อนที่จะมีการร่วมใช้ระบบ เมื่อมีการปฏิสัมพันธ์กับระบบเหตุการณ์ต่าง ๆ จะถูกบันทึกลงสู่ Log Files

2. ในความเป็นจริง เราตั้งสมมุติฐานว่าทุก ๆ เหตุการณ์ได้ถูกบันทึก ดังนั้น Log Files จะถือว่าเป็นตัวแทนของข้อมูลแบบดิจิทัลที่เก็บ Activity ได้อย่างสมบูรณ์ในระบบแบบไดนามิก

3. ในบางเวลา ผู้บริโภคข้อมูลอาจจะเรียกดู SA ซึ่ง Log ที่ประกอบไปด้วยข้อมูลที่บันทึกเกี่ยวข้องกับ A

4. A สามารถเก็บรวบรวมข้อมูลแล้วเริ่มกระบวนการของการตรวจสอบแบบอัตโนมัติโดยฝ่ายที่สาม

5. ทำการสร้างหลักฐานที่สอดคล้องกัน เพื่อตรวจสอบว่านโยบาย PA ได้ถูกปฏิบัติตามหรือไม่

เพื่อให้หลักฐานความเป็นส่วนตัว (Privacy Evidence) มีความเป็นไปได้ สิ่งที่สำคัญยิ่งคือ

- Policy Language เพื่อแสดงออกถึงความต้องการทางด้านความเป็นส่วนตัว (Privacy) ในระบบไดนามิค

- Log Views คือสิ่งที่สร้างออกมาเพื่อให้สามารถมองเห็นข้อมูล Activities ที่บันทึกไว้

- Secure Logging คือสิ่งที่สร้างความมั่นใจว่าข้อมูลที่บันทึกไว้นั้นเชื่อถือได้ โดยเฉพาะเพื่อปรับปรุงความน่าเชื่อถือให้กับ Log Views

- Automated Audit Process เป็นกระบวนการเพื่อตรวจสอบว่านโยบายได้ถูกปฏิบัติตาม

2.4.4.1 A Policy Language for Dynamic Systems

Policy Language คือสิ่งที่ยินยอมให้ Data Provider สามารถกำหนดกลุ่มของกฎเกณฑ์ต่าง ๆ ขึ้นมา เช่น นโยบายสำหรับควบคุมการเข้าถึง ในขณะที่การทำการ Monitor ข้อมูลของผู้บริโภคก่อนให้เกิดการบันทึกข้อมูลการอนุญาตเพื่อใช้ตรวจสอบในภายหน้า อย่างไรก็ตามนโยบายสำหรับระบบไดนามิคควรจะยินยอมให้ Data Provider สามารถเลือกกำหนดคุณลักษณะว่าจะจัดเก็บหรือไม่จัดเก็บ Policy Language ที่นำเสนอในบทความนี้ จะอยู่บนสองแนวคิดคือ Access และ Collection เราจะเรียกง่าย ๆ ว่าเป็น Act

เราจะสร้างความเข้าใจให้มากขึ้นด้วยเงื่อนไขสำหรับ Usage Control ซึ่งเป็นเทคนิคในการควบคุมการเข้าถึงแบบดั้งเดิมโดยที่ยินยอมให้ Data Provider ได้ระบุว่าอะไรคือ ข้อกำหนด (Provision) และข้อผูกมัด (Obligation) ซึ่งตามความรู้สึกแล้ว Provision จะเป็นการแสดงออกถึงเงื่อนไขที่ต้องปฏิบัติเพื่อที่จะอนุญาตหรือปฏิเสธ Act นั้น ตัวอย่างเช่นการเข้าถึงข้อมูลโดยรวมของ Data Provider A จะอนุญาตให้เฉพาะจุดประสงค์ทางด้านบัญชีเท่านั้น ส่วน Obligation แสดงถึงเหตุการณ์ที่จะต้องเกิดขึ้นเมื่อ Act นั้นได้รับการยินยอมหรือปฏิเสธให้เข้าถึงข้อมูล ตัวอย่างเช่น Data Provider A ต้องการได้รับการแจ้งเมื่อมีการบันทึกข้อมูลผ่าน RFID เกิดขึ้น

รูปที่ 2.9 แสดงให้เห็นถึงตัวอย่างของ Policy Language

รูปที่ 2.10 แสดงให้เห็นตัวอย่างของ Policy Rules

```
1.  <Policy>      := (<Rule>) | (<Rule>), <Policy>
2.  <Rule>        := <Col_Ctrl> | <Col_Ctrl>, if (<Cond>) |
3.                   <Acc_Ctrl> | <Acc_Ctrl>, if (<Cond>)
4.  <Col_Ctrl>    := <Perm>, <Subj>, <Obj>, <Event>
5.  <Acc_Ctrl>    := <Perm>, <Subj>, <Obj>, <Right>
6.  <Cond>        := <Atom_Cond> | <Atom_Cond> && <Cond>
7.  <Atom_Cond>   := <Provision> | <Obligation>
8.  <Provision>   := role <Op> <Role> | purpose <Op> <Purpose>  |
9.                   <DataField> <Op> <Value>
10. <Obligation> := delete <DataField>  <Temp_mod> [<Sanction>] |
11.                  notify <DataProvider> <Temp_mod> [<Sanction>]
12. <Perm>        := allow | deny
13. <Right>       := read | write | exec <Cmd>
14. <Temp_mod>    := immediately | within <Nat_Number> days
15. <Sanction>    := otherwise <String>
16. <Op>          := > | < | >= | <= | == | !=
```

รูปที่ 2.9 Policy Language for Dynamic Systems

```
r1 := ( allow, *, *, read,
        if ( role == Marketing &&
             purpose == PersService &&
             delete * within 30 days otherwise Fine=$100$ ))
r2 := ( deny, RFID-Reader, *, * )
```

รูปที่ 2.10 Example of Policy Rules

2.4.4.2 Secure Logging and Log View

ข้อมูล Log ถือเป็นใจกลางของแหล่งข้อมูลในระบบคอมพิวเตอร์ ในทางตรงกันข้าม เป็นสิ่งที่เก็บสาระสำคัญของการทำงานในระบบคอมพิวเตอร์แบบไดนามิก ดังนั้น Log File จึงเป็นแหล่งข้อมูลที่ใช้สำหรับการตรวจสอบ อย่างไรก็ตาม เพื่อให้มีประโยชน์และมีความน่าเชื่อถือ ข้อมูล Log จะต้องคุณสมบัติที่เรียกว่าแท้จริง (Authentic) เช่น ต้องมีคุณสมบัติดังต่อไปนี้

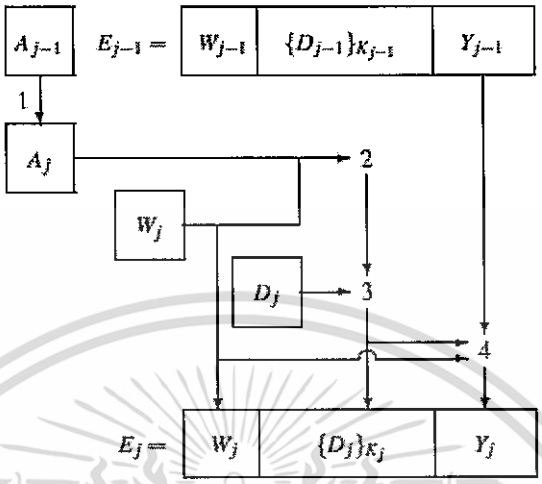
- Integrity กำหนดว่า Log Data จะต้องมีความถูกต้อง (ข้อมูลต้องไม่ถูกแก้ไข) สมบูรณ์ (ข้อมูลจะต้องไม่ถูกลบทิ้ง) และมีความกระชับ (ข้อมูลต้องไม่ถูกเพิ่มเติมอย่างผิดกฎ) ดังนั้น Log Data จะต้องไม่ถูกแก้ไข ลบ หรือเพิ่มในระหว่างการส่งผ่านและการจัดเก็บในหน่วยเก็บข้อมูล

- Confidentiality กำหนดว่าข้อมูล Log จะต้องไม่เก็บในลักษณะข้อมูลที่สามารถอ่านได้ (Clear Text) ซึ่งจะทำให้ Log นั้นสามารถเข้าถึงและทำซ้ำได้อย่างง่ายดาย

คุณสมบัติแท้จริงของ Log Data นั้น เกิดขึ้นได้ด้วยเทคนิคการเข้ารหัสลับโดยการตรวจจับความพยายามที่จะเข้ามาแก้ไข Log Data

แนวทางของงานวิจัยนี้ ได้นำเสนอวิธีการที่ปลอดภัยโดยทำการบันทึกข้อมูลและเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องโดยไม่แยกกระบวนการกัน แต่ละ Log E_j จะถูกเข้ารหัสลับด้วยกุญแจ K_j ซึ่งได้มาจากการคำนวณจาก secret master key A_j และ index W_j

กระบวนการ hash Y มีความเกี่ยวข้องกับข้อมูลก่อนหน้าคือ E_{j-1} และข้อมูลปัจจุบัน ซึ่งกระบวนการดังกล่าวนี้แสดงได้ดังรูปที่ 2.11



รูปที่ 2.11 Adding an Entry to the Log File

1. $A_j = \text{Hash}(A_{j-1})$ แทนกุญแจสำหรับการพิสูจน์ตัวตนสำหรับข้อมูล Log ลำดับที่ j การรักษาความลับของข้อมูลนี้มีความสำคัญอย่างมากเนื่องจากเป็นข้อมูลที่ใช้ในการเข้ารหัสลับ ดังนั้น เราจึงตั้งสมมุติฐานว่าการคำนวณค่าใหม่นั้นไม่สามารถทำให้ล่วงรู้ค่าก่อนหน้านี้ได้

2. $K_j = \text{Hash}(W_j, A_j)$ คือกุญแจในการเข้ารหัสลับสำหรับข้อมูล Log ลำดับที่ j ซึ่งกุญแจนี้ก็ขึ้นอยู่กับ index W_j ดังนั้นจะมีเฉพาะ Data Provider ที่สอดคล้องกันเท่านั้นที่จะสามารถได้รับอนุญาตให้เข้าถึงข้อมูลนี้ได้

3. $\{D_j\}K_j$ คือ Log ที่เข้ารหัสลับของข้อมูล D_j

4. $Y_j = \text{Hash}(Y_{j-1}, \{D_j\}K_j, W_j)$ คือค่าลำดับที่ j ของกระบวนการสร้างโซ่แฮช (hash chain) แต่ละการเชื่อมโยงในโซ่แฮชนี้ขึ้นอยู่กับค่าของข้อมูลที่ถูกเข้ารหัสลับที่สอดคล้องกัน

Log generator กำหนดด้วย $E_j = W_j, \{D_j\}K_j, Y_j$ ประกอบไปด้วย index W_j, Log ที่เข้ารหัสลับ $\{D_j\}K_j$, และ hash chain Y_j

2.4.4.3 Automated Audits and Digital Privacy Evidence

Data Provider สามารถเรียกดู Log View ของพวกเขาและสามารถตรวจสอบได้ว่านโยบายเกี่ยวกับข้อมูล Privacy ได้ถูกปฏิบัติตามหรือไม่ อย่างไรก็ตามดูเหมือนจะเป็นเรื่องที่ซับซ้อนเพราะ Log View อาจจะประกอบไปด้วยข้อมูลมากมายและความสัมพันธ์โยงใยระหว่างกันมักจะยากที่จะทำความเข้าใจและปะติดปะต่อกัน ซึ่งนั่นก็เป็นสิ่งที่เรากำลังพยายามจะปรับปรุงความสามารถในการอ่านได้ของ Log Review

ผู้เขียนได้พัฒนาวิธีการที่จะตรวจสอบ Log View ด้วยนโยบายของ Data Provider สมมุติให้นโยบาย $P := \{r_1, \ldots, r_n\}$ (P ประกอบไปด้วยเซ็ตของ r) และกำหนดให้ Log View S ทำการเปลี่ยนรูป V ซึ่งใช้ P และส่งกลับมาเป็น Set ของ กฎ $V_P = \{v_1, \ldots, v_n\}$ ซึ่ง $v_i \in V$ แสดงถึงการละเมิดกฎ r_i เพื่อแสดงให้เห็น ให้ดูกฎ r_2 ในรูปที่ 2.10 โดยใช้ตัวเปลี่ยนรูป V จะได้กฎการละเมิดดังนี้

$v_2 :=$ (allow, RFID-Reader, *, *)

ซึ่งแสดงให้เห็นว่าการเก็บข้อมูลผ่าน RFID Reader ถูกอนุญาต ซึ่งเป็นการขัดกับกฎเดิมที่กำหนดไว้โดย Data Provider

เมื่อได้กฎ V_P มาแล้ว เราก็ทำการค้นหาการละเมิดใน Log View จาก Data Provider ที่สอดคล้องกัน

เราใช้เครื่องแสดงสัญญาณไฟเพื่อให้แสดงผลของการตรวจสอบให้แก่ Data Provider ในกรณีนี้สัญญาณไฟแดงหมายถึงมีการละเมิดกฎข้อบังคับ ในขณะที่สัญญาณไฟเขียวหมายถึงการปฏิบัติตามกฎข้อบังคับอย่างถูกต้อง

2.4.5 ความมั่นคงปลอดภัยของเว็บเซอร์วิสบนพื้นฐานของ Regulatory Compliance

จากความแพร่หลายของระบบคอมพิวเตอร์บนเครือข่าย เว็บเซอร์วิสจึงเป็นส่วนสำคัญที่เชื่อมโยงระบบสารสนเทศและการบริการทางด้านคอมพิวเตอร์ ดังนั้นการรักษาความมั่นคงปลอดภัยของเว็บเซอร์วิสจึงมีความสำคัญมากขึ้นเรื่อย ๆ

เนื่องจากมีกฎหมายและข้อกำหนดเพื่อป้องกันข้อมูลบนเครือข่ายเหล่านั้น เช่น SOX และการบังคับใช้กฎหมายนั้นมีความเข้มงวดสูง ดังนั้นการทำให้เป็น Regulatory Compliance จึงกลายเป็นภารกิจที่สำคัญสำหรับ CIO และ CEO

Organization, Flow และ Technology เป็นพื้นฐานสามประการของ Regulatory Compliance

ซึ่งจากพื้นฐานทั้งสามประการดังกล่าว Gang Chen ได้นำเสนอบทความชื่อ Security for Web Service Based on Regulatory Compliance [8] โดยแบ่งเป็นกรอบสามมิติของการรักษาความมั่นคงปลอดภัยของเว็บเซอร์วิสบนพื้นฐานของ Regulatory Compliance คือ การป้องกัน (Protection) การเฝ้าดู (Monitor) และการตรวจสอบ (Audit) ซึ่งแบบแผน (Blueprint) ของการรักษาความมั่นคงปลอดภัยของเว็บเซอร์วิสจะต้องระบุให้ชัดเจนสำหรับสิทธิ หน้าที่ความรับผิดชอบของแต่ละบทบาท เสถียรภาพของโครงสร้างพื้นฐาน ความมั่นคงปลอดภัยสำหรับระบบการเงิน และระบบการตรวจสอบโดยรวม

2.4.5.1 พื้นฐานของ Regulatory Compliance

ต่อไปจะเป็นการกล่าวถึงรายละเอียดและพื้นฐานสำหรับ Regulatory Compliance ซึ่งประกอบด้วย 3 ส่วน ได้แก่

1. การจัดการอย่างเป็นระบบ (Organization)

Organization ของการรักษาความมั่นคงปลอดภัยคือกุญแจที่สำคัญ CIO และผู้บริหารระดับสูงจะต้องเป็นสมาชิกของทีมงานรักษาความมั่นคงปลอดภัย และพวกเขาจะต้องสร้างความเข้าใจที่ชัดเจนให้กับพนักงานเกี่ยวกับรายละเอียดของกฎหมายและกฎข้อบังคับ Organization จะต้องให้ความดูแลทางด้านเทคโนโลยีด้วย ดังนั้นวิศวกรจะต้องเป็นส่วนหนึ่งที่สำคัญ นักกฎหมายก็เป็นส่วนที่สำคัญเช่นเดียวกัน พวกเขาสามารถช่วยให้พนักงานของบริษัทเข้าใจกฎหมายได้ดีและช่วยให้บริษัทได้เปรียบถ้าหากว่าต้องมีการขึ้นศาล

2. โฟลว์ (Flow)

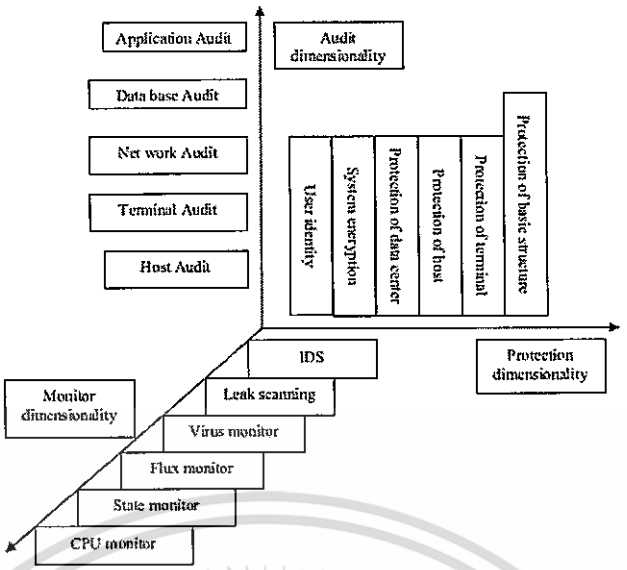
CIO จะต้องกำหนดโฟลว์ของการบริหารจัดการความมั่นคงปลอดภัยและกลยุทธการบันทึกการเข้าถึงข้อมูล ซึ่งบันทึกเหล่านี้ช่วยให้ CIO รู้ว่าระบบไอทีดำเนินงานอย่างไรซึ่งช่วยขยายความให้ได้รู้ถึงการดำเนินงานและเป้าหมายของบริษัท โฟลว์ของการบริหารจัดการความมั่นคงปลอดภัยจะต้องรวมถึงว่าจะเฝ้าดูข้อมูลและระบบสารสนเทศอย่างไร CIO จะต้องวิเคราะห์ถึงนโยบายทางด้านการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศที่ใช้อยู่และพัฒนาให้สอดคล้องกับกฎหมายและกฎข้อบังคับ

3. เทคโนโลยี (Technology)

เทคโนโลยีความมั่นคงปลอดภัยของ Regulatory Compliance นั้นหมายรวมถึงเทคโนโลยีที่ว่าทำอย่างไรจึงจะรับประกันความถูกต้องของข้อมูลและความสามารถในการเข้าถึงระบบสารสนเทศซึ่งแน่นอนว่าเทคโนโลยีความมั่นคงปลอดภัยนั้นคือกุญแจสำคัญ เช่น Firewall, IDS เป็นต้น CIO จะต้องรู้ว่าบางครั้งเทคโนโลยีไม่สามารถช่วยปรับปรุงความมั่นคงปลอดภัยของระบบสารสนเทศได้ถ้าหากไม่มีการบริหารจัดการ เช่นการบริหารความเสี่ยงและการตรวจสอบไอที ซึ่งควรต้องทำเป็นประจำเพื่อให้ค้นพบปัญหาได้ทันเวลา

2.4.5.2 Frame of Security for Web Service based on Regulatory Compliance

ผู้เขียนบทความได้แบ่งมิติของกรอบความมั่นคงปลอดภัยออกเป็น 3 มิติด้วยกันคือ การป้องกัน (Protection) การเฝ้าดู (Monitor) และการตรวจสอบ (Audit) ซึ่งแสดงได้ดังรูปที่ 2.12



รูปที่ 2.12 Frame Security for Web Service Based On Regulatory Compliance

1. Protection Dimensionality

มิติของการป้องกันนั้นรวมถึงการป้องกันระบบพื้นฐาน การป้องกันเทอร์มินัล การป้องกันเครื่องแม่ข่าย การป้องกันศูนย์ข้อมูล ระบบการเข้ารหัสลับและข้อมูลส่วนบุคคลของผู้ใช้ มิติของการป้องกันนี้เป็นการควบคุมและดูแลฮาร์ดแวร์และซอฟต์แวร์ในระบบสารสนเทศ ซึ่งถือว่าเป็นพื้นฐานในการสร้างความมั่นใจในเว็บเซอร์วิสและระบบสารสนเทศ

2. Monitor Dimensionality

มิติของการเฝ้าดู (Monitor) นี้รวมถึง IDS, Leak Scanning, Virus Monitor, Flux Monitor, State Monitor และ CPU Monitor มิติของการเฝ้าดูนี้ทำให้ระบบสามารถจัดเตรียมข้อมูลให้กับ CIO หรือผู้ตรวจสอบ เมื่อมีการตรวจพบปัญหาทางด้านความมั่นคงปลอดภัย ระบบจะแจ้งเตือนไปยังผู้จัดการและให้คำแนะนำในการที่จะแก้ปัญหาด้วยแผนและโฟลว์ของการกู้คืน

3. Audit Dimensionality

มิติของการตรวจสอบนั้นรวมถึงการตรวจสอบ Host, Terminal, Network, Database และ Application รายงานของการตรวจสอบจะต้องถูกเก็บและวิเคราะห์โดย CIO และผู้ตรวจสอบ ผลของการตรวจสอบจะต้องมีสาระสำคัญสำหรับการปรับปรุงและกลยุทธสำหรับสร้างความปลอดภัย

2.4.5.3 Blueprint of Security for Web Service Based On Regulatory Compliance

แบบแผน (Blueprint) ของการรักษาความมั่นคงปลอดภัยสำหรับเว็บเซอร์วิสจะต้องระบุให้ชัดเจนสำหรับสิทธิ หน้าที่ความรับผิดชอบของแต่ละบทบาท เสถียรภาพของโครงสร้างพื้นฐานความมั่นคงปลอดภัยสำหรับระบบการเงินและระบบการตรวจสอบโดยรวม และจะต้องมีคุณสมบัติต่อไปนี้คือ

1. Ascertain Range of Security

ขอบเขตของความปลอดภัยคือขอบเขตของระบบการเฝ้าดูความปลอดภัยตามข้อกำหนดของกฎหมาย ข้อกำหนดหรือนโยบายของบริษัท ขอบเขตนั้นหมายรวมถึงการบำรุงรักษาไอที การเข้าถึงระบบข้อมูลและเครือข่าย

สำหรับรัฐบาล มีการกำหนดระดับของความมั่นคงปลอดภัยของเว็บเซอร์วิส ระบบสารสนเทศของรัฐบาลมีความสำคัญและข้อมูลก็สำคัญมากและต้องมีระดับของความมั่นคงปลอดภัยสูง การตรวจสอบข้อมูลและระบบสารสนเทศจะต้องทำเป็นประจำ การเข้าถึงระบบสารสนเทศถือเป็นกุญแจสำคัญของระบบความมั่นคงปลอดภัย CIO จะต้องกำหนดนโยบายทางด้านความมั่นคงปลอดภัยและใช้เทคโนโลยีที่เหมาะสมสำหรับประกันความมั่นคงปลอดภัยของข้อมูลและหลีกเลี่ยงการเข้าถึงระบบสารสนเทศอย่างไม่ถูกต้อง CIO จะต้องหลีกเลี่ยงการเปิดเผยข้อมูลด้วยเช่นกัน

สำหรับบริษัทเอกชนทั่วไป การตรวจสอบการเข้าถึงของผู้ใช้งานถือเป็นกุญแจสำคัญสำหรับความมั่นคงปลอดภัยของเว็บเซอร์วิส เป็นการควบคุมและวิเคราะห์การกระทำของผู้ใช้งานและหลีกเลี่ยงการเปิดเผยข้อมูลที่ไม่ถูกต้องและเป็นการปรับปรุงระบบความมั่นคงปลอดภัย

สำหรับบริษัททางด้านการเงิน นอกจากการตรวจสอบระบบสารสนเทศแล้ว กุญแจสำคัญสำหรับระบบความมั่นคงปลอดภัยคือการตรวจสอบการปฏิบัติงานของพนักงานผู้ที่ทำงานทางด้านการบำรุงรักษา เพราะพนักงานเหล่านี้สามารถเข้าถึงระบบไอที และระบบไอทีก็เป็นเส้นทางดำเนินธุรกิจของบริษัท บริษัททางด้านการเงินอาจมีการจัดจ้างผู้ให้บริการภายนอกเพื่อการซ่อมบำรุง ซึ่งความสำคัญของการตรวจสอบก็ยิ่งสูงขึ้นในกรณีนี้

2. Value Risk and Monitor Security

Value Risk สามารถบอก CIO ถึงความเสี่ยงที่ซ่อนอยู่และร่องรอยของความเสี่ยงของ Regulatory Compliance ซึ่ง CIO ควรจะกำหนดระดับของความเสี่ยงและวางแผนเพื่อหลีกเลี่ยงความเสี่ยงในทุก ๆ ระดับ CIO จะต้องกำหนดโฟลว์ของการเฝ้าดูความมั่นคงปลอดภัยและทำการวิเคราะห์รายงานเพื่อสร้างความชัดเจนในระบบความมั่นคงปลอดภัยและเพื่อปรับปรุงระบบความมั่นคงปลอดภัย

3. Audit Security System

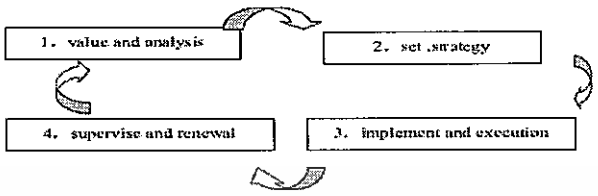
ทำการตรวจสอบโดยหน่วยงานตรวจสอบของรัฐบาลและสำนักงานบัญชีภายนอก เพื่อตรวจสอบระบบความมั่นคงปลอดภัยของเว็บเซอร์วิสบนพื้นฐานของกฎข้อบังคับ (Regulatory)

4. Report and Advice CIO about Security

มีรายงานทางด้านระบบความปลอดภัยอยู่ 3 ชนิดคือ รายงานที่ต้องส่งหน่วยงานตรวจสอบของรัฐบาลสำหรับ Regulatory Compliance รายงานสำหรับคณะกรรมการบริหารบริษัทและรายงานสำหรับ CIO และผู้จัดการระบบไอที

2.4.5.4 Implement of Security for Web Service Based On Regulatory Compliance

การปฏิบัติใช้ระบบความมั่นคงปลอดภัยสำหรับเว็บเซอร์วิสบนพื้นฐานของ Regulatory Compliance นั้นรวมถึง 4 กระบวนการดังรูปที่ 2.13



รูปที่ 2.13 Implement of Security for Web Service Based On Regulatory Compliance

1. Value and Analysis

ทำการวิเคราะห์และกำหนดมูลค่าสำหรับทุก ๆ นโยบายและโฟลว์ให้สอดคล้องกับ Regulatory Compliance ซึ่ง CEO จะต้องกำหนดคณะกรรมการของ Regulatory Compliance ในคณะกรรมการนั้นจะต้องประกอบไปด้วย CIO, CFO, นักกฎหมายของบริษัทและระดับผู้จัดการของบริษัท

ทุก ๆ คนที่อยู่ในคณะกรรมการจะต้องรู้ถึงกระบวนการของการดำเนินการและเป้าหมายของบริษัท และต้องรู้ข้อกำหนดในกกหมายรวมทั้งกฎเกณฑ์ของระบบสารสนเทศ

CIO จะต้องทำรายการของปัญหาของบริษัทให้สอดคล้องกับ Regulatory Compliance

2. Set Strategy

CIO จะต้องกำหนดกลยุทธทางด้านความมั่นคงปลอดภัยให้สอดคล้องกับ Regulatory Compliance กลยุทธนั้นจะต้องถูกส่งไปยังทุก ๆ คนที่อยู่ในคณะกรรมการความมั่นคงปลอดภัยและเก็บรวบรวมคำแนะนำต่าง ๆ เพื่อทำการปรับปรุงกลยุทธ ในขั้นตอนนี้ CFO จะต้องช่วย CIO ในแง่ของงบประมาณและ CTO จะต้องช่วย CIO ในการเลือกใช้เทคโนโลยีภายใต้งบประมาณนั้น

3. Implement and Execution

ในขั้นตอนของการปฏิบัติใช้จริง CIO จะต้องกำหนดทีมงานและกำหนดโครงสร้างของฮาร์ดแวร์และซอฟต์แวร์พื้นฐาน CIO จะต้องเป็นผู้นำทีมในการทดสอบในทุก ๆ ส่วนเพื่อประกันความสำเร็จของการปฏิบัติใช้

4. Supervise and Renewal

เนื่องจากการดำเนินกิจการทางด้านธุรกิจ กฎหมายและข้อกำหนดอาจมีการเปลี่ยนแปลงหรือเริ่มใช้ใหม่ ดังนั้นระบบความปลอดภัยจะต้องมีการเปลี่ยนแปลงด้วย และระบบความมั่นคงปลอดภัยควรจะต้องมีความยืดหยุ่น ไม่ว่าการเปลี่ยนแปลงหรือการเริ่มใช้ใด ๆ ผู้จัดการไอทีและ CIO จะต้องรายงานให้ผู้ตรวจสอบและคณะกรรมการของ Regulatory Compliance รับรู้

2.5 การประมวลผลภาษาธรรมชาติ (Natural Language Processing) และงานวิจัยที่เกี่ยวข้อง

เนื่องจากเอกสารทางด้านข้อกำหนดและกฎหมายส่วนใหญ่จะเขียนออกมาในรูปแบบของภาษาธรรมชาติซึ่งคนเราสามารถอ่านและเข้าใจได้ แต่เครื่องคอมพิวเตอร์ไม่สามารถเข้าใจได้หากไม่มีการตีความโดยคน ดังนั้นจึงเป็นความท้าทายอย่างสูงที่จะทำการสกัดหรือดึงข้อมูลออกจากเอกสารเหล่านี้แบบอัตโนมัติ มีนักวิจัยจำนวนมากพยายามที่จะหาวิธีการกำหนดโครงสร้างของข้อมูลเพื่อทำให้เครื่องคอมพิวเตอร์สามารถสกัดข้อมูลออกมาได้ ซึ่งแนวทางส่วนใหญ่คือการทำหมายเหตุประกอบลงในข้อมูล (Data Annotation) เพื่อทำการค้นหาและสรุปคำตอบแบบใช้หลักเหตุผล (Reasoning) โดยใช้การประมวลผลภาษาธรรมชาติ (Natural Language Processing) ซึ่งเครื่องมือหลัก ๆ ที่ใช้ในการประมวลผลภาษาธรรมชาตินั้นประกอบไปด้วยฐานข้อมูลที่รองรับภาษาธรรมชาติที่ชื่อว่าออนโทโลยี (Ontology) และเทคโนโลยีที่ใช้ในการสกัดข้อมูลออกจากสารสนเทศ (Information Extraction)

2.5.1 งานวิจัยที่นำเสนอการพัฒนาออนโทโลยีในขอบเขตที่เกี่ยวกับ Information Security

ออนโทโลยี (Ontology) มีผู้ให้คำจำกัดความไว้หลากหลายทั้งสาขาปรัชญาและเทคโนโลยีสารสนเทศ โดยความหมายของออนโทโลยีของสาขาเทคโนโลยีสารสนเทศ หมายถึง วิธีการบรรยายแนวความคิดตามขอบเขตที่สนใจ หรือข้อกำหนดที่เกี่ยวกับแนวคิด (The Specification of a Conceptualization) โดยที่ออนโทโลยีเป็นการสร้างโครงสร้างฐานความรู้ทางด้านใดด้านหนึ่ง หรือขอบเขต (Domain) ใดขอบเขตหนึ่ง ซึ่งมีแนวคิดและความเข้าใจตรงกัน ออนโทโลยีใช้ในการอธิบายความหมายของสิ่งต่าง ๆ และสามารถจัดหมวดหมู่เอกสารของข้อมูลได้ในขอบเขตความสนใจหนึ่ง ๆ ซึ่งในปัจจุบันออนโทโลยีได้ถูกนำมาประยุกต์ใช้งานมากยิ่งขึ้น สามารถประยุกต์กับงานหลาย ๆ ด้าน เช่น เว็บเชิงความหมาย (Semantic Web) การจัดการองค์ความรู้ (Knowledge Management) ธุรกิจอิเล็กทรอนิกส์ (e-Business) พาณิชย์อิเล็กทรอนิกส์ (e-Commerce) และการค้นคืนสารสนเทศ (Information Retrieval)

ออนโทโลยีถูกสร้างขึ้นมาเพื่อจำกัดองค์ความรู้ (Knowledge) ของขอบเขตข้อมูลนั้น ๆ โดยมีความสามารถในการใช้ข้อมูลร่วมกัน (Share) สามารถนำข้อมูลกลับมาใช้ได้ (Reuse) และมีความสามารถในการถ่ายทอดคุณสมบัติ (Inheritance) การนำออนโทโลยีมาใช้งานจึงเป็นทางเลือกหนึ่งในการใช้ข้อมูลร่วมกันและแยกองค์ความรู้ออกจากฐานข้อมูล

ออนโทโลยีเป็นลักษณะภาษาที่นำมาใช้บรรยายโครงสร้างและความสัมพันธ์ของระบบผ่านโหนดแบบลำดับชั้น (Hierarchies) ภาษาดังกล่าวถูกนำมาใช้ในงานหลายด้าน โดยเฉพาะด้านปัญญาประดิษฐ์ ในปัจจุบันได้กำหนดภาษามาตรฐานที่ใช้จำลองและออกแบบโครงสร้างของเอกสารเอกซ์เอ็มแอล (XML) โดยใช้นิยามแนวคิดให้อยู่ในรูปของกฎ (Role) คลาส (Class)

ความสัมพันธ์ระหว่างคลาส (Relation) และคุณสมบัติของคลาส (Properties) แล้วนำเสนอออกมาในรูปของโหนด และความสัมพันธ์แบบลำดับชั้น

เป้าหมายสำคัญสำหรับการพัฒนาออนโทโลยีของ Information Security คือการสร้างความเข้าใจที่ตรงกัน และลดความกำกวมของภาษาทางด้าน Information Security เพื่อใช้เป็นแนวทางสื่อสารระหว่างคนและซอฟต์แวร์

เนื่องด้วยงานวิจัยทางด้าน Information Security Ontologies นั้นมีเป็นจำนวนมาก เพื่อให้สามารถอ้างอิงได้มากที่สุด งานวิจัยฉบับนี้จึงขอสรุปแต่เพียงแนวคิดของแต่ละงานวิจัยไว้เท่านั้น

2.5.1.1 A Bootstrapping Approach for Developing a Cyber-Security Ontology Using Textbook Index [9]

ในบทความนี้ผู้เขียนนำเสนอวิธีการที่เรียกว่า Bootstrapping มาใช้ในการพัฒนาออนโทโลยีสำหรับการรักษาความมั่นคงปลอดภัยในโลกไซเบอร์ (Cyber Security Ontology) เพื่อเป็นพื้นฐานหรือดัชนีสำหรับรายการของคำ (Terms) ใน Security Domain วิธีการ Bootstrapping จะทำการสกัดคำศัพท์หรือแนวคิดออกมาจากดัชนีในตำรา แล้วสร้างเป็นความสัมพันธ์ของแต่ละรายการของคำตามแนวคิดของ Security Ontology ผลลัพธ์ของวิธีการนี้ สามารถนำมาใช้สำหรับการบันทึกและค้นหาสื่อสำหรับการเรียนรู้และการฝึกอบรมในด้านการรักษาความมั่นคงปลอดภัยในโลกไซเบอร์

2.5.1.2 A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations [10]

บทความนี้นำเสนอการสร้างออนโทโลยีโดยมุ่งเน้นไปที่ช่องโหว่ของความมั่นคงปลอดภัยซึ่งมีวัตถุประสงค์เพื่อบูรณาการความรู้เกี่ยวกับช่องโหว่ในขั้นตอนของการพัฒนาระบบ แนวคิดพื้นฐานของผู้เขียนคือการวิเคราะห์ช่องโหว่และผลกระทบของช่องโหว่นั้น ๆ ต่อระบบ ซึ่งเป็นแนวคิดสำหรับกรอบการรักษาความมั่นคงปลอดภัยของระบบโดยการเปรียบเทียบและประเมินผลกระทบของระบบโดยใช้ช่องโหว่เป็นพื้นฐาน

2.5.1.3 Qualitative Analysis of an Ontology Based Issue Resolution System for Cyber Attack Management [11]

ในงานวิจัยนี้ ผู้วิจัยได้เสนอ Ontology-Based Issue Resolution System (IRS) ซึ่งทำการแบ่งหมวดหมู่ของทิศทางของการโจมตีทางข้อมูลเพื่อช่วยในการสื่อสารภายในองค์กร ระบบ IRS จะใช้ส่วนขยายจากหมวดหมู่ของการโจมตีทางไซเบอร์ เป้าหมายของระบบ IRS คือการจัดเตรียมข้อมูลเกี่ยวกับทิศทางการโจมตีให้กับระบบป้องกัน รวมทั้งข้อมูลเกี่ยวกับผลกระทบหาก

ระบบเป้าหมายถูกโจมตี โครงสร้างของข้อมูลทิศทางการโจมตีอยู่ในรูปแบบของ Tree ซึ่งสร้างขึ้นโดยการทำเหมืองข้อมูลและสกัดข้อมูลเพื่อแสดงการโจมตีทั้งหมดใน IRS

2.5.1.4 A Security Audit Framework to Manage Information System Security [12]

ในบทความนี้เป็นการนำเสนอกรอบแนวคิดการจัดการระบบรักษาความมั่นคงปลอดภัยและการตรวจสอบระบบการรักษาความมั่นคงปลอดภัยของข้อมูล แนวคิดที่นำเสนอนี้ช่วยให้องค์กรเข้าใจว่าทรัพย์สินใดขององค์กรที่จะต้องปกป้องและมีช่องโหว่อะไรบ้าง ซึ่งทำให้องค์กรสามารถกำหนดวิธีการรักษาความมั่นคงปลอดภัยที่เหมาะสม

2.5.1.5 A Security Ontology for Incident Analysis [13]

ผู้เขียนได้มีการพัฒนาออนโทโลยีที่เกี่ยวข้องกับเหตุการณ์ที่ไม่พึงประสงค์ด้านความมั่นคงปลอดภัย (Security Incidents Ontology) ที่มีผลกับองค์กรและระบบโดยรวม ซึ่งมีการแนะนำการป้องกันที่เหมาะสม ซึ่งสถาปัตยกรรมของออนโทโลยีนี้ประกอบไปด้วยระดับความมั่นคงปลอดภัย 3 ระดับคือ ระดับ Social, Logical และ Physical ซึ่งแนวคิดนี้ได้ให้การวิเคราะห์เกี่ยวกับเรื่องของเหตุการณ์ที่ไม่พึงประสงค์ไม่เฉพาะจากปัจจัยด้านเทคนิค แต่รวมถึงปัจจัยด้านมนุษย์และธรรมชาติอีกด้วย ซึ่งทำให้เกิดการป้องกันในเชิงลึกที่ครอบคลุมทั้งทางด้านการป้องกัน การตรวจจับและการกู้คืนจากเหตุการณ์ที่เกิดขึ้น

2.5.1.6 A User-Oriented Ontology-Based Approach for Network Intrusion Detection [14]

ในบทความนี้ผู้เขียนได้นำเสนอวิธีการใหม่ในการออกแบบและการพัฒนาแอพพลิเคชันเพื่อตรวจจับการโจมตีระบบ โดยการรวบรวมข้อมูลความรู้จากผู้เชี่ยวชาญแล้วนำมาพัฒนามาเป็นออนโทโลยี ซึ่งออนโทโลยีนี้สามารถพัฒนาขึ้นมาใหม่ หรือสร้างขึ้นจากออนโทโลยีที่มีอยู่ โดยการใช้องค์ความรู้จากออนโทโลยีและแนวคิดระดับสูงในการสร้างแบบจำลองของระบบตรวจจับการบุกรุก ผู้ที่ไม่มีความรู้ความชำนาญในด้านนี้ก็สามารถปรับแต่งระบบตรวจจับการบุกรุกได้โดยการระบุ Instant ลงในออนโทโลยี วิธีการนี้มีข้อดีคือ (1) ตรงกับความต้องการของผู้ใช้และลูกค้า (2) ทำให้กระบวนการพัฒนาระบบสั้นลง (3) มีความเป็นไปได้ที่จะสร้างต้นแบบอย่างรวดเร็ว (4) มีความลงตัวด้านการสื่อสารกับผู้เชี่ยวชาญด้านการตรวจจับการบุกรุก และ (5) ใคร ๆ ก็ใช้ความรู้จากโดเมนนี้ได้

2.5.1.7 An Information Security Ontology Incorporating Human-Behavioral Implications [15]

ในบทความนี้ผู้เขียนพิจารณาถึงความจำเป็นที่ต้องทำความเข้าใจปัจจัยที่เกี่ยวกับพฤติกรรมของมนุษย์ในกระบวนการของการจัดการความปลอดภัยของข้อมูลในองค์กร พวกเขาพัฒนาออนโทโล

ยีด้านความมั่นคงปลอดภัยของข้อมูลที่เป็นการผสมผสานเนื้อหาของมาตรฐานด้านการรักษาความมั่นคงปลอดภัยข้อมูล (ในกรณีนี้ ISO 27002) ร่วมกับการพิจารณาปัญหาทางด้านความมั่นคงปลอดภัยของข้อมูลที่อาจเกิดจากพฤติกรรมของมนุษย์ ออนโทโลยีนี้ช่วยจัดเตรียมโครงสร้างเพื่อช่วยในการตัดสินใจของผู้บริหารในกระบวนการติดตั้งระบบควบคุมความมั่นคงปลอดภัยของข้อมูล

2.5.1.8 Ontological Approach Toward CyberSecurity in Cloud Computing [16]

บทความนี้ผู้เขียนได้นำเสนอออนโทโลยีสำหรับการรักษาความมั่นคงปลอดภัยในโลกไซเบอร์สำหรับ Cloud Computing โดยมุ่งเน้นที่ความมั่นคงปลอดภัยของข้อมูลที่จะทำการแลกเปลี่ยนบน Cloud Computing ซึ่งผู้เขียนมองว่ามีสิ่งที่มีความสำคัญคือการรักษาความมั่นคงปลอดภัยให้กับข้อมูลเมื่อมีการเปลี่ยนแปลงต่าง ๆ เช่น แหล่งที่มาของข้อมูล และข้อมูลเกี่ยวกับความเกี่ยวข้องกันของแต่ละทรัพยากร เป็นต้น

2.5.1.9 Ontology for Attack Detection: An Intelligent Approach to Web Application Security [17]

ในงานวิจัยฉบับนี้ ผู้เขียนได้นำเสนอออนโทโลยีสำหรับการตรวจจับการโจมตีแอพพลิเคชันบนเวปไซต์ ซึ่งประกอบไปด้วย Attacks Ontology และ Communication Protocol Ontology ที่ผู้เขียนระบุว่าแนวคิดนี้สามารถปรับปรุงความสามารถในการตรวจจับการโจมตีระดับแอพพลิเคชัน ซึ่งมีผลงานที่สำคัญดังต่อไปนี้

- Communication Ontology ซึ่งเน้นรูปแบบการสื่อสารของโปรโตคอล HTTP ซึ่งไม่เพียงแต่จะตรวจจับการโจมตี แต่ยังช่วยให้ระบบตรวจสอบการร้องขอ (Request) และการตอบสนอง (Response) ที่อาจจะมีสคริปต์ที่ประสงค์ร้ายบรรจุอยู่
- Attack Ontology ซึ่งประกอบไปด้วยรูปแบบของการโจมตีที่สำคัญบนเวปแอพพลิเคชัน รูปแบบการโจมตีที่แตกต่างกันโดยแฮกเกอร์ แหล่งที่มาและเป้าหมายของการโจมตี ผลกระทบต่อระบบจากการโจมตี สิ่งที่อาจจะเป็นช่องโหว่และนโยบายของการควบคุมเพื่อบรรเทาผลกระทบของการโจมตีดังกล่าว

2.5.1.10 The STAC (Security Toolbox: Attacks & Countermeasures) Ontology [18]

ผู้เขียนบทความนี้นำเสนอออนโทโลยีเกี่ยวกับการรักษาความปลอดภัย ซึ่งจะช่วยให้บุคคลที่ไม่มีความรู้ ความเชี่ยวชาญทางด้านความปลอดภัยสามารถที่จะ

(1) ออกแบบซอฟต์แวร์รักษาความปลอดภัย และ

(2) เข้าใจและตระหนักถึงแนวคิดการรักษาความปลอดภัยรวมทั้งปัญหาต่าง ๆ

ออนโทโลยีนี้พัฒนาโดยรวบรวมแนวคิดของการรักษาความมั่นคงปลอดภัยหลัก ๆ เช่นการโจมตี การรับมือกับการโจมตี คุณสมบัติด้านความมั่นคงปลอดภัยและความสัมพันธ์ต่าง ๆ การรับมือหรือการตอบโต้จากการถูกโจมตีอาจใช้แนวคิดการเข้ารหัสลับ (เช่น Encryption Algorithms, Key Management, Digital Signature, Hash Function)

2.5.2 Information Extraction

Information Extraction [19] หมายถึงกระบวนการในการสกัดสารสนเทศออกจากเอกสารที่เราสนใจ เป็นเทคโนโลยีที่อยู่บนพื้นฐานของการวิเคราะห์ภาษาธรรมชาติเช่นเอกสาร ตำรา หรือแม้แต่คำพูดมาสร้างรูปแบบที่เครื่องคอมพิวเตอร์สามารถเข้าใจได้ และได้ผลลัพธ์ออกมาในรูปแบบของภาษาที่ไม่คลุมเคลือ ซึ่งข้อมูลที่เป็นผลลัพธ์อาจถูกนำไปใช้โดยการแสดงให้ผู้ใช้เห็นโดยตรง หรืออาจเก็บไว้ในฐานข้อมูลเพื่อการวิเคราะห์ในภายหลัง หรือเพื่อใช้ในการทำดัชนีสำหรับระบบค้นคืนสารสนเทศ (Information Retrieval: IR) เช่นเครื่องมือค้นหาทางอินเทอร์เน็ตอย่าง Google

2.5.3 Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations [20]

เนื่องจากข้อมูลทางด้านสุขภาพของผู้ป่วยเป็นข้อมูลที่อาจเป็นเป้าหมายของการโจมตีและอาจถูกไปใช้ในทางที่ผิด รวมทั้งมีการละเมิดสิทธิ์ของข้อมูลมากขึ้น ทั้งนี้ข้อกำหนด หรือกฎหมายต่าง ๆ ที่ออกมาเพื่อปกป้องข้อมูลเหล่านี้ เช่นกฎหมาย HIPAA ก็ยังเป็นเอกสารที่เขียนออกมาแบบกำกวม ยากต่อการทำความเข้าใจหรือตีความ ทำให้การออกแบบซอฟต์แวร์เพื่อปกป้องข้อมูลเหล่านี้มีความยุ่งยากและซับซ้อน งานวิจัยฉบับนี้นำเสนอวิธีการสกัดข้อความที่มีความสำคัญเพื่อเป็นกลไกในการช่วยให้นักวิเคราะห์ระบบสามารถเข้าใจได้อย่างชัดเจนถึงข้อกำหนดที่มีความจำเป็นในการออกแบบซอฟต์แวร์ เพื่อให้มั่นใจว่าระบบนั้นสอดคล้องและตอบสนองต่อนโยบายต่าง ๆ ที่เกี่ยวข้อง โดยขั้นตอนที่งานวิจัยได้นำเสนอคือ

1. กำหนดคำศัพท์เฉพาะทาง (Terminology) ดังต่อไปนี้

- Stakeholder คือ ผู้ที่ได้รับ Right หรือ Obligation ตามที่กฎหมาย HIPAA กำหนด
- Right คือกิจกรรมที่ Stakeholder ได้รับการยินยอมให้ทำได้ โดยเป็นตามเงื่อนไข
- Obligation คือกิจกรรมที่ Stakeholder ได้รับการร้องขอให้ทำ โดยเป็นไปตามเงื่อนไข
- Delegation คือ Right หรือ Obligation ที่ทาง Stakeholder ได้ทำการมอบหมายต่อให้ Stakeholder อื่นปฏิบัติ
- Rule Statement คือ ข้อความที่ประกอบไปด้วย Right หรือ Obligation และเงื่อนไขต่าง ๆ
- Constraint Phase คือประโยคที่เป็นส่วนหนึ่งของ Rule Statement และอธิบายถึงเงื่อนไขหนึ่ง ๆ
- Normative Phase คือประโยคที่ระบุว่า "ought to be" เป็นเสมือน Right หรือ Obligation

2. ใช้กระบวนการที่เรียกว่า Semantic Parameterization โดยการนำข้อความที่เป็น UNLS (Unrestricted Natural Language Statement) ที่มีถ้อยคำ Right และ Obligation ประมวลผลใน RNLS (Restricted Natural Language Statement) ซึ่งเป็นรูปแบบหนึ่งของการประมวลผลภาษาธรรมชาติ ตัวอย่างของ RNLS ใน งานวิจัยนี้เช่น

UNLS1: A covered entity that agrees to a restriction ***may not*** use or disclose protected health Information, ***except if*** the individual who requested the restriction is in need of emergency treatment.
RNLS1: The covered entity who **(RNLS2)** ***may not*** disclose protected health Information, ***except if*** **(RNLS3)**.
RNLS2: The covered entity agrees to a restriction.
RNLS3: The individual who (RNLS4) needs emergency treatment.
RNLS4: The individual requests the restriction.

ถึงแม้ว่ากระบวนการนี้จะสามารถดึงประโยคหรือย่อหน้าที่มีถ้อยคำ Right และ Obligation ออกมาได้ แต่ต้องใช้ขั้นตอนและผู้ที่มีความรู้ในการกำหนด RNLS ซึ่งเป็นกระบวนการที่ต้องใช้เวลาเป็นอย่างสูง ผู้วิจัยจึงมองว่าวิธีการนี้จึงยังไม่เหมาะสมสำหรับการสกัดข้อมูล แต่อย่างไรก็ตามเราได้ปรับใช้ Terminology ในด้านของ Right และ Obligation รวมทั้งคีย์เวิร์ดต่าง ๆ ที่เป็น Condition เช่นคำว่า “except if”, “unless” จากงานวิจัยฉบับนี้

2.5.4 Using a Text Engineering Framework to Build an Extendable and Portable IE-Based Summarisation System [21]

งานวิจัยนี้เป็นการนำเสนอระบบที่ให้บริการข้อมูลทางด้านสุขภาพและความปลอดภัยที่ชื่อว่า HaSIE (Health and Safety Information Extraction) โดยใช้เครื่องมือ GATE เป็นเครื่องมือสำคัญ ซึ่ง GATE เป็นเครื่องมือเดียวกันกับงานวิจัยนี้ ซึ่งรายละเอียดของ GATE จะได้อธิบายในบทที่ 4 จุดประสงค์ของงานวิจัยนี้คือการสร้างรายงานประจำปีเกี่ยวกับผลการจัดการด้านสุขภาพและความปลอดภัยของบริษัท โดยการสกัดข้อมูลออกมาเพื่อสร้างรายงานทางสถิติที่บ่งชี้ถึงระดับของการ Compliance กับข้อกำหนดทางด้านสุขภาพและความปลอดภัย รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยระบบจะทำการตรวจสอบว่าเอกสารที่เป็นข้อมูลนำเข้ามีข้อมูลที่เกี่ยวข้องกับเรื่องสุขภาพและความปลอดภัย รวมทั้งข้อมูลในแนวนี้เช่น อัตราการเกิดอุบัติเหตุ อัตราการเกิดเหตุการณ์ไม่พึงประสงค์ และจำนวนพนักงาน เป็นต้น ถ้าพบจะทำการสกัดย่อหน้านั้นออกมา ซึ่งขั้นตอนการสกัดข้อมูลของระบบนี้คือ

1. กำหนดคำที่เกี่ยวข้องกับ Health and Safety เพื่อสร้างเป็น Gazetteer list เช่นคำว่า “HSE”, “Occupational Health”, “accident”, “injury”, “death” เป็นต้น

2. สกัดประโยคและย่อหน้าที่มีคำตรงกับ Gazetteer ออกมาด้วย JAPE grammar

3. ทำหมายเหตุประกอบ (Annotation) ในประโยคหรือย่อหน้าที่สกัดออกมา

4. ส่งออกข้อมูลลงฐานข้อมูล Microsoft Access เพื่อสร้างรายงาน

ถึงแม้ว่าในงานวิจัยนี้จะไม่ได้แสดงถึงรายงานที่สำเร็จรูป แต่ก็เป็นแนวความคิดของการสกัดเฉพาะข้อมูลที่สนใจออกจากเอกสารได้เป็นอย่างดี

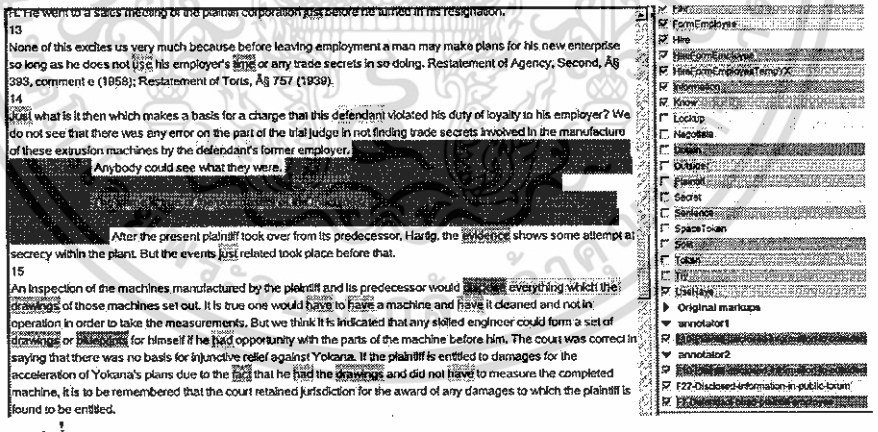
2.5.5 Towards Annotating and Extracting Textual Legal Case Factors [22]

ในบทความนี้ ผู้เขียนได้นำเสนอการสกัดข้อความที่เป็นปัจจัยสำคัญจากคดีความที่เกิดขึ้นในอดีต เพื่อเป็นประโยชน์สำหรับทนายความที่จะค้นหาข้อมูลประกอบการว่าความ โดยใช้ GATE เป็นเครื่องมือในการสกัดข้อมูล ซึ่งกระบวนการในการสกัดข้อมูลก็คือ

1. กำหนดคำที่เกี่ยวข้องกับปัจจัยที่ก่อให้เกิดคดีความต่าง ๆ เพื่อสร้างเป็น Gazetteer list เช่นคำต่าง ๆ เหล่านี้: announce, betray, break, bring out, communicate, confide, disclose, discover, divulge, expose, give away, impart, inform, leak, let on, let out, make known, pass on, reveal, tell, announcement, betrayal, communication, confidence, disclosure, divulgance, exposure

2. สกัดประโยคและย่อหน้าที่มีคำตรงกับ Gazetteer ออกมาด้วย JAPE Grammar

3. ทำหมายเหตุประกอบ (Annotation) ในประโยคหรือย่อหน้าที่สกัดออกมา ซึ่งตัวอย่างของผลลัพธ์แสดงได้ดังรูปที่ 2.14

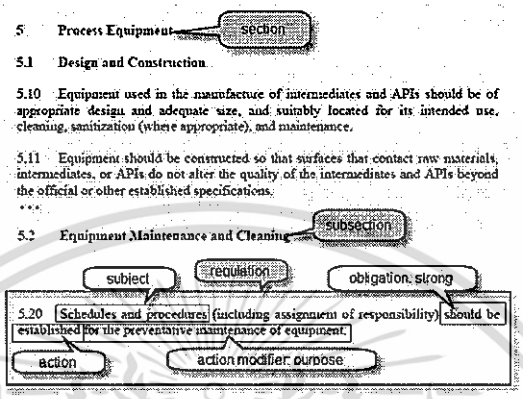


รูปที่ 2.14 GATE Team Ware with Low and High Level Factor Annotations

2.5.6 Towards Semantic Methodologies for Automatic Regulatory Compliance Support [23]

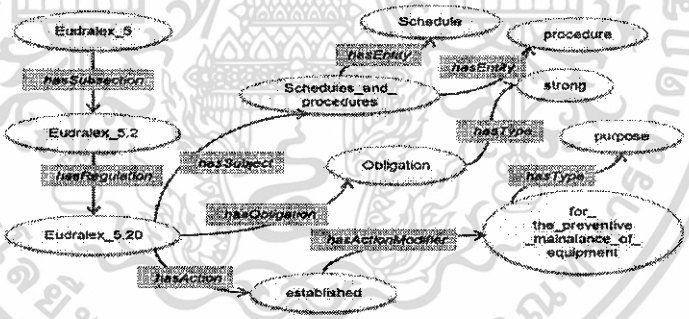
ในงานวิจัยนี้ผู้วิจัยได้นำเสนอออนโทโลยีร่วมกับการใช้ GATE ในการสกัดข้อมูล โดยใช้ตัวอย่างข้อมูลจากอุตสาหกรรมยาและกฎหมายควบคุมที่ชื่อว่า Eudralex EU ซึ่งกระบวนการที่นำเสนอประกอบไปด้วย 4 ขั้นตอนหลัก ๆ คือ

1. การสกัดข้อความจากกฎหมาย Eudralex EU โดยการสร้าง Gazetteer เพื่อทำหมายเหตุประกอบ (Annotate) ข้อความที่เป็นข้อกำหนดของกฎหมายและระบุความสัมพันธ์ต่าง ๆ เช่น Subject, Object และ Action เป็นต้น โดยใช้หลักการของ Obligation ในการสกัดข้อมูลออกมา ดังรูปที่ 2.15



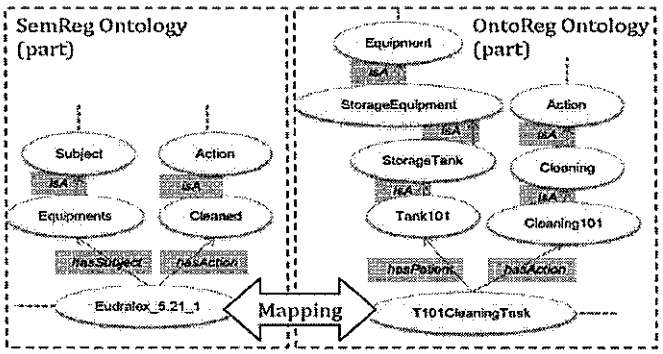
รูปที่ 2.15 A Section of Eudralex Regulation Showing How the System Annotates the Document Structure and Concepts

2. การ Formalize โครงสร้างของกฎหมายที่สกัดออกมาโดยการนำข้อมูลที่สกัดออกมาได้มาสร้างเป็นความสัมพันธ์ในออนโทโลยี ดังรูปที่ 2.16



รูปที่ 2.16 An Example of Regulatory Concepts and Their Relationship in the SemReg Ontology

3. การ Mapping กฎหมายเข้ากับกิจกรรมการตรวจสอบ ดังรูปที่ 2.17



รูปที่ 2.17 Mapping Regulations to Validation Tasks in the SemReg and OntoReg Ontologies

4. การสร้าง Semantic Rule ดังตัวอย่าง

Axiom 1: The validation task must have at least one approved written procedure.

ValidationTask hasWrittenProcedure
some (TaskProcedure **and** (hasValidationStatus **has** Approved).

Rule 1: If there is a written procedure in place for the Regulation, this Regulation is said to be compliant.

Regulations(r) ^ TaskProcedure(p) ^ hasWrittenProcedure(r,p) => compliant(r).

2.5.7 NLP and e-Government : Crime Information Extraction from Heterogeneous Data Sources [24]

งานวิจัยนี้นำเสนอการพัฒนาระบบเก็บข้อมูลการสัมภาษณ์ผู้ตกเป็นเหยื่อและพยานในคดีอาชญากรรมต่าง ๆ เพื่อเป็นการช่วยป้องกันและแก้ปัญหาการก่ออาชญากรรมแบบเดิม โดยการสกัดข้อมูลจากข่าวอาชญากรรม จากรายงานของตำรวจ บทความในหนังสือพิมพ์ หรือจากคำสัมภาษณ์ของเหยื่อและพยาน โดยระบบจะทำการสกัดข้อมูลที่เกี่ยวข้องกับอาชญากรรมนั้น ๆ เช่น รายชื่อบุคคล อาวุธ ยานพาหนะ ช่วงเวลา เสื้อผ้าและสถานที่ เป็นต้น เครื่องมือที่ใช้ในงานวิจัยนี้คือ GATE เช่นเดียวกัน โดยมีกระบวนการหลัก ๆ ดังนี้คือ

1. พัฒนา Lexicon เพื่อเก็บข้อมูลรายการของสิ่งที่เกี่ยวข้องกับอาชญากรรมเช่น อาวุธ ยานพาหนะ ฉาก เสื้อผ้า รองเท้า และลักษณะทางกายภาพต่าง ๆ โดยรวบรวมข้อมูลจากแหล่งต่าง ๆ เช่น Uniform Crime Report (UCR) และข้อมูลจาก FBI (Federal Bureau of Investigation) แล้วนำข้อมูลใน Lexicon ไปสร้างเป็น Gazetteer list แบ่งเป็นหมวดหมู่ต่าง ๆ เช่น 'Act', 'Scene', 'People', 'Personal Property', 'Vehicle', 'Weapon', 'Body Part', 'Time', และ 'Clothing' โดยที่ตัวอย่างของ list ในหมวดหมู่ Act เช่น assault/ attack / fight / kill / massacre / murder / rape / shoot / slay / stab / torture / steal / rob / burgle / lunder / ransack / grab / …

2. สกัดประโยคและย่อหน้าที่มีคำตรงกับ Gazetteer ออกมาด้วย JAPE grammar

3. Export ข้อมูลที่สกัดได้ไปยังฐานข้อมูลต่าง ๆ เช่น Excel หรือ Access เพื่อการสร้างระบบรายงาน

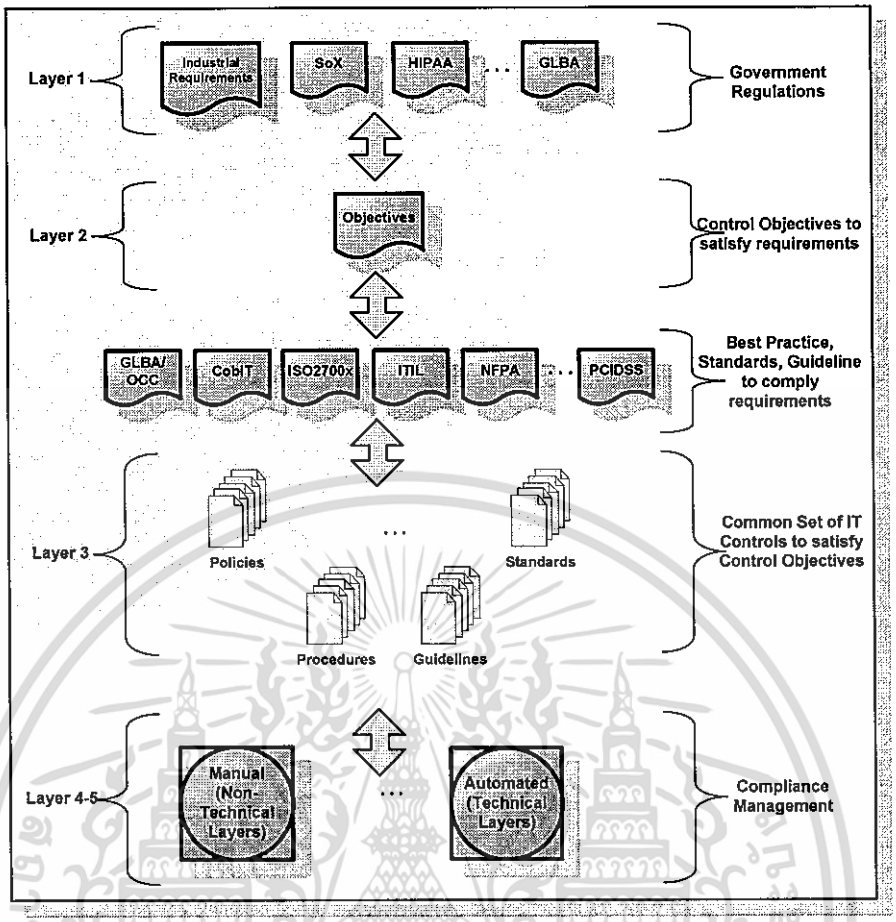
ในบทถัดไปจะเป็นการประมวลองค์ความรู้จากทฤษฎีและงานวิจัยที่เกี่ยวข้องเพื่อนำเสนอเป็นกระบวนการที่ทำให้การตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง (Security Compliance Checking) มีความเป็นอัตโนมัติ

บทที่ 3
การออกแบบสถาปัตยกรรมสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ

การศึกษาในครั้งนี้เป็นการประมวลองค์ความรู้ที่ใช้ในการควบคุมความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและองค์ความรู้ในการตรวจสอบระบบเทคโนโลยีสารสนเทศ มาออกแบบและนำเสนอเป็นสถาปัตยกรรมที่ทำให้การตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง (Security Compliance Checking) มีความเป็นอัตโนมัติ โดยนำเทคโนโลยีที่สามารถประมวลผลกับข้อมูลที่เป็นรูปแบบของภาษาธรรมชาติ (Natural Language Processing) มาใช้เป็นเครื่องมือสำคัญ

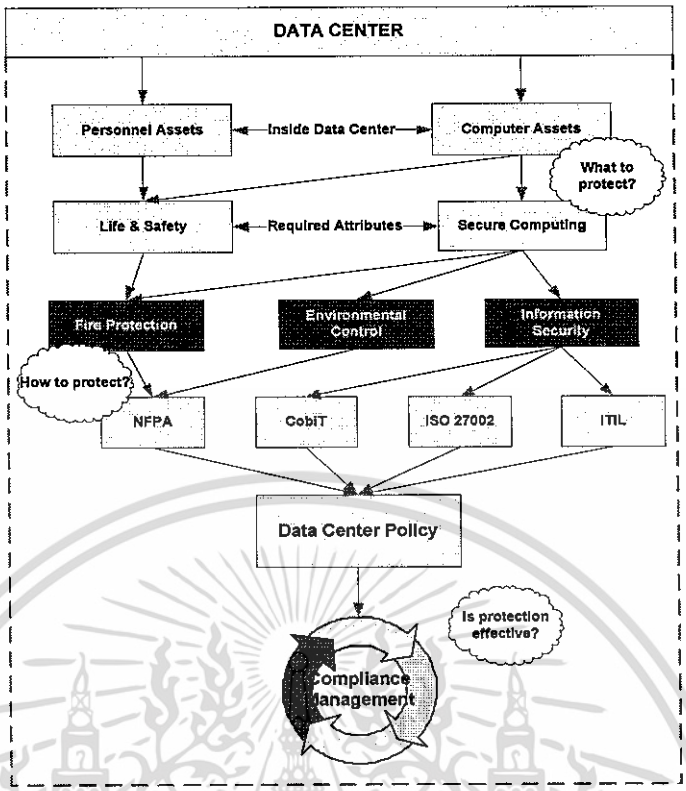
3.1 การจัดทำ Security Compliance Management Framework และ Security Compliance Checking Framework

การบริหารจัดการการปฏิบัติตามกฎเกณฑ์ (Compliance Management) เป็นกระบวนการในการจัดการบริหารองค์กรเพื่อให้มั่นใจว่าองค์กรจะปฏิบัติตามข้อหนดและกฎหมายที่เกี่ยวข้อง เนื่องจากกฎหมายต่าง ๆ นั้นได้ถูกบัญญัติขึ้นมากมายแยกตามขอบเขตที่ต้องการควบคุม ดังนั้นการที่องค์กรหนึ่ง ๆ จะถือว่าเป็นองค์กรที่ปฏิบัติตามกฎเกณฑ์ (Compliance) หรือไม่นั้น ไม่จำเป็นต้องยึดถือทุกกฎหมายมาปฏิบัติ แต่ต้องมีกระบวนการที่เลือกว่ากฎหมายใดบ้างที่เกี่ยวข้องและต้องนำมาปฏิบัติ โดยหลักการวิเคราะห์ความเสี่ยงว่าองค์กรนั้นมีความเสี่ยงอะไรบ้าง และความเสี่ยงนั้นใช้กฎหมายอะไรในการควบคุม ในงานวิจัยนี้ เรามุ่งเน้นที่การควบคุมความเสี่ยงทางด้านเทคโนโลยีสารสนเทศเป็นหลัก เพื่อให้เข้าใจถึงที่มาที่ไปของมาตรฐานหรือกฎระเบียบข้อบังคับในขั้นสุดท้ายที่องค์กรถือปฏิบัติเพื่อควบคุมการดำเนินงานทางด้านเทคโนโลยีสารสนเทศ โดยอ้างอิงจาก “A Layer Model for Compliance” จากรูปที่ 2.2 และจัดทำออกมาเป็นโครงร่างการบริหารจัดการการปฏิบัติตามกฎเกณฑ์ความมั่นคง (Security Compliance Management Framework) ดังรูปที่ 3.1



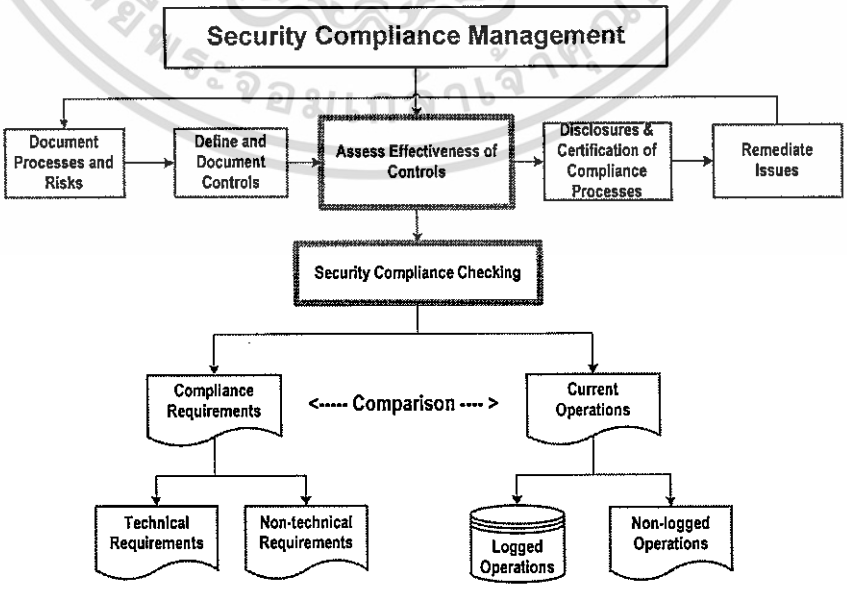
รูปที่ 3.1 Security Compliance Management Framework

จากรูปที่ 3.1 ใน Layer 3 คือการที่องค์กรได้ทำการประเมินความเสี่ยงของ Scope หรือ Area ที่จะควบคุมแล้วเลือกใช้ Best Practice, Standard หรือ Guideline มาประยุกต์ใช้และ Mapping เพื่อจัดทำเป็นนโยบายหรือมาตรฐานเพื่อใช้ในองค์กรนั้น ๆ ยกตัวอย่างเช่นในกรณีที่องค์กรหนึ่งมี Data Center ที่จะต้องควบคุม แทนที่องค์กรจะควบคุมการปฏิบัติงานโดยการอ้างอิงมาตรฐานหลาย ๆ ฉบับ องค์กรอาจทำการรวบรวมมาตรฐานหรือ Best Practice ที่เกี่ยวข้องแล้วจัดทำเป็นกฎระเบียบฉบับเดียวขึ้นมาเพื่อบังคับใช้ ดังรูปที่ 3.2



รูปที่ 3.2 ตัวอย่างของนโยบายหรือมาตรฐานที่ประยุกต์ใช้ในองค์กร

Security Compliance Checking เป็นกระบวนการย่อยของ Security Compliance Management ซึ่งเป็นกระบวนการในการประเมินผลว่าการปฏิบัติขององค์กรเป็นไปตามเอกสารควบคุมหรือนโยบายที่ได้กำหนดไว้หรือไม่ ซึ่งโครงร่าง Security Compliance Checking Framework แสดงดังรูปที่ 3.3



รูปที่ 3.3 Security Compliance Checking Framework

จากรูปที่ 3.3 กระบวนการ Security Compliance Checking ต้องการข้อมูลสองส่วนมาเปรียบเทียบกันและทำการประเมิน ส่วนแรกคือข้อมูลเกี่ยวกับ Compliance Requirements ซึ่งก็คือข้อกำหนดต่าง ๆ นั่นเอง ซึ่งข้อกำหนดแบ่งออกได้เป็นสองประเภทคือ Technical Requirements และ Non-Technical Requirements ข้อมูลส่วนที่สองคือข้อมูลการปฏิบัติการขององค์กรในปัจจุบัน ซึ่งแบ่งออกเป็น Logged Operations และ Non-Logged Operations ข้อมูลแต่ละประเภทสามารถอธิบายได้ดังนี้

1. Technical Requirements คือข้อกำหนดที่สามารถเข้าใจและประมวลผลได้โดยระบบคอมพิวเตอร์ แต่อย่างไรก็ตามยังต้องการการเขียนโปรแกรมที่เฉพาะเจาะจงสำหรับแต่ละข้อกำหนด ข้อกำหนดประเภทนี้มักจะเกี่ยวข้องกับตัวเลข รวมทั้งข้อมูล วันและเวลา ตัวอย่างเช่น ข้อกำหนด “Minimum password length=7” สามารถใช้ระบบคอมพิวเตอร์เพื่อคำนวณว่าความยาวของรหัสผ่านที่เก็บอยู่ในฐานข้อมูลนั้นตรงตามข้อกำหนดหรือไม่

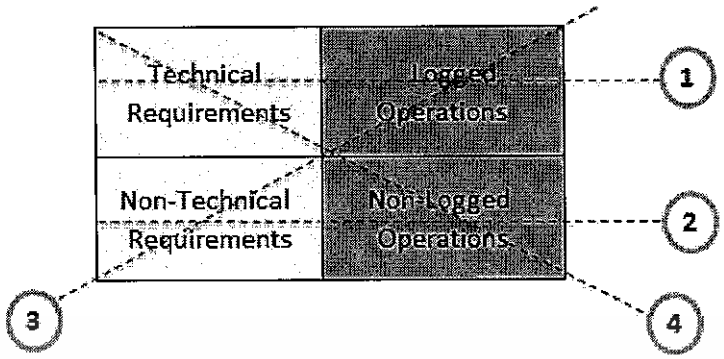
2. Non-Technical Requirements คือข้อกำหนดที่ระบบคอมพิวเตอร์แบบดั้งเดิมไม่สามารถเข้าใจได้ นอกจากใช้การ hard coding เท่านั้น ตัวอย่างเช่นข้อกำหนด “Smoke detector must be installed in the data center.” ระบบคอมพิวเตอร์แบบดั้งเดิมจะไม่เข้าใจคำว่า “smoke detector”, “must be”, “install”, or “data center” และไม่สามารถดึงคำเหล่านี้มาประมวลผลได้

3. Logged Operations คือกระบวนการทำงานใด ๆ ที่เกี่ยวข้องกับข้อกำหนดและมีการบันทึกข้อมูลในรูปแบบที่สามารถประมวลผลได้โดยระบบคอมพิวเตอร์ ตัวอย่างเช่น การเปลี่ยนรหัสผ่านครั้งล่าสุด เป็นหนึ่งในข้อกำหนดของการควบคุม มีการบันทึกข้อมูลและสามารถประมวลผลได้โดยระบบคอมพิวเตอร์ ดังนั้นจึงถือเป็น Logged Operations

4. Non-Logged Operations คือกระบวนการทำงานใด ๆ ที่เกี่ยวข้องกับข้อกำหนดแต่ไม่มีการบันทึกข้อมูลในรูปแบบที่สามารถประมวลผลได้โดยระบบคอมพิวเตอร์ ตัวอย่างเช่น การติดตั้ง Smoke Detector ไม่สามารถบันทึกข้อมูลในรูปแบบที่สามารถประมวลผลได้โดยระบบคอมพิวเตอร์ (การบันทึกด้วยมือลงใน Spreadsheet ต่าง ๆ ไม่ถือว่าเป็น Logged Operations)

3.2 การวิเคราะห์ปัญหาและจุดอ่อนของ Automated Security Compliance Checking

ผู้วิจัยได้ทำการรวบรวมและจัดหมวดหมู่ของงานวิจัยที่เกี่ยวข้องกับ Automated Security Compliance Checking ที่ใช้อยู่ในปัจจุบันเพื่อนำเสนอเป็นแนวคิดสำหรับงานวิจัย โดยอ้างอิงจากข้อมูล 4 ประเภทในหัวข้อที่ผ่านมา ออกเป็น 4 เงื่อนไขดังรูปที่ 3.4



รูปที่ 3.4 The Combination of Compliance Requirement and Current Operations Conditions

1. งานวิจัยที่เกี่ยวข้องกับ Technical Requirements และ Logged Operations จากการรวบรวมข้อมูลพบว่าระบบคอมพิวเตอร์แบบดั้งเดิมสามารถช่วยให้การตรวจสอบกับข้อมูลในเงื่อนไขนี้มีความเป็นอัตโนมัติได้ แต่ยังต้องอาศัยการตีความจากผู้เชี่ยวชาญด้านนโยบายในการติดตั้งข้อกำหนด การเพิ่มระดับของความอัตโนมัติจึงอยู่ที่การตีความข้อกำหนดให้มีความเป็นอัตโนมัติมากขึ้นโดยการใช้เครื่องมือที่สามารถทำงานกับภาษาธรรมชาติได้

2. งานวิจัยที่เกี่ยวข้องกับ Non-Technical Requirements และ Non-Logged Operations จากการรวบรวมข้อมูลพบว่าระบบคอมพิวเตอร์แบบดั้งเดิมไม่เหมาะสำหรับการตรวจสอบข้อมูลในเงื่อนไขนี้ และนักวิจัยส่วนใหญ่ยังมองข้าม ระดับความเป็นอัตโนมัติของการตรวจสอบจึงค่อนข้างต่ำ

3. งานวิจัยที่เกี่ยวข้องกับ Non-Technical Requirements และ Logged Operations จากการรวบรวมข้อมูลพบว่าระบบคอมพิวเตอร์ในปัจจุบันไม่เหมาะสำหรับการตรวจสอบข้อมูลในเงื่อนไขนี้ แต่มีนักวิจัยจำนวนมากกำลังทำงานอยู่ จึงทำให้ระดับความเป็นอัตโนมัติของการตรวจสอบกำลังเพิ่มสูงขึ้น

4. งานวิจัยที่เกี่ยวข้องกับ Technical Requirements และ Non-Logged Operations จากการรวบรวมข้อมูลพบว่าระบบคอมพิวเตอร์แบบดั้งเดิมนั้นสามารถตรวจสอบข้อมูลในเงื่อนไขนี้ แต่ไม่มีข้อมูลพร้อมสำหรับการตรวจสอบ และนักวิจัยส่วนใหญ่ยังมองข้าม ระดับความเป็นอัตโนมัติของการตรวจสอบจึงยังค่อนข้างต่ำ

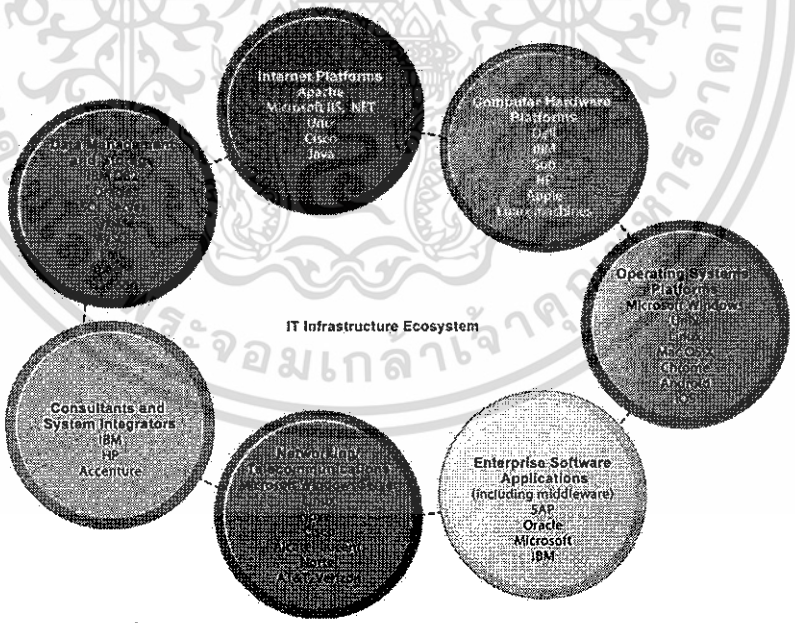
จากข้อมูลข้างต้น พบว่านักวิจัยส่วนใหญ่ที่วิจัยในเรื่องของ Automated Security Compliance Checking มักจะมุ่งเน้นไปที่การทำงานกับข้อมูลที่มีการบันทึกในรูปแบบที่สามารถประมวลผลได้โดยระบบคอมพิวเตอร์ หรือ Logged Operations งานวิจัยฉบับนี้จึงต้องการที่จะเพิ่มระดับของ Automated Security Compliance Checking โดยการนำเสนอ Automated Security Compliance Checking Architecture ที่จะอธิบายในหัวข้อถัดไป

3.3 การเสนอสถาปัตยกรรมการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ

การตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยทั่วไปมักจะมีขั้นตอนหลัก ๆ ดังต่อไปนี้

1. กำหนด Scope และ Area ที่ต้องการตรวจสอบ
2. กำหนดช่วงเวลาของการตรวจสอบ
3. สื่อสารกำหนดการต่าง ๆ กับผู้ที่รับผิดชอบส่วนงานที่ต้องการตรวจสอบ
4. การเตรียม Checklist สำหรับการตรวจสอบ (ปฏิบัติได้โดยผู้เชี่ยวชาญ)
5. การลงมือตรวจสอบจริง (ปฏิบัติได้โดยผู้เชี่ยวชาญ)
6. บันทึกผลของการตรวจสอบ (ปฏิบัติได้โดยผู้เชี่ยวชาญ)
7. การประเมินผลการตรวจสอบ (ปฏิบัติได้โดยผู้เชี่ยวชาญ)
8. การทำรายงานสรุปผลการตรวจสอบและการแนะนำการปรับปรุง (ปฏิบัติได้โดยผู้เชี่ยวชาญ)
9. การติดตามผลหลังการตรวจสอบ

ในที่นี้ Scope และ Area ที่ต้องการตรวจสอบในงานวิจัยนี้มุ่งเน้นไปที่หน่วยงานไอที ซึ่งจะอ้างอิงเป้าหมายที่จะต้องถูกตรวจสอบตาม Seven Major Components of IT Infrastructure ดังรูปที่ 3.5



รูปที่ 3.5 Seven Major Components of IT Infrastructure

รูปที่ 3.5 คือ Seven Major Components of IT Infrastructure จากหนังสือ Management Information Systems: Managing the Digital Firm [25] ซึ่งประกอบด้วย

1. Computer Hardware Platforms คือ เครื่องคอมพิวเตอร์ทั้งหมดไม่ว่าจะเป็นเซิร์ฟเวอร์หรือไคลเอ็นต์ ซึ่งรวมทั้งเครื่องคอมพิวเตอร์ที่เป็นเมนเฟรมด้วย ตัวอย่างเครื่องคอมพิวเตอร์ในปัจจุบันที่ใช้กันอย่างแพร่หลายเช่น IBM, HP, Dell, และ Sun Microsystems

2. Operating System Platforms คือระบบปฏิบัติการสำหรับคอมพิวเตอร์ทั้งหมด สำหรับระบบปฏิบัติการที่เป็นเซิร์ฟเวอร์ ในปัจจุบันมี 3 ระบบหลัก ๆ คือ Microsoft Windows Server มีการใช้ประมาณ 35% ส่วนอีก 65% เป็นระบบปฏิบัติการ Unix หรือ Linux ส่วนระบบปฏิบัติการสำหรับไคลเอ็นต์นั้น 90% เป็นระบบ Microsoft Windows ระบบอื่น ๆ สำหรับไคลเอ็นต์ก็เช่น Chrome OS สำหรับ Cloud Computing ที่ใช้ Netbook และ Android และ iOS สำหรับอุปกรณ์พกพา

3. Enterprise and Other Software Applications คือระบบงานที่ใช้สำหรับบริหารงานและประมวลผลในองค์กร ไม่ว่าจะเป็นระบบบริหารงานบุคคล ระบบบัญชี หรือระบบบริหารฝ่ายผลิต ซึ่งระบบเหล่านี้อาจเป็นระบบที่องค์กรพัฒนาขึ้นเองหรือเป็นระบบที่ใช้กันอย่างแพร่หลายเช่น SAP, Oracle หรือ PeopleSoft เป็นต้น

4. Data Management and Storage คือระบบเก็บข้อมูลขององค์กรเพื่อการประมวลผลและการเข้าใช้งาน เช่น IBM DB2, Oracle, Microsoft SQL Server และ Sybase เป็นต้น

5. Networking and Telecommunications Platforms คือการบริหารเครือข่ายหรือการเชื่อมต่อทั้งหมด ไม่ว่าจะเป็น LAN, WAN, TCP/IP protocol, Voice เป็นต้น รวมถึงอุปกรณ์คู่ค้าที่เกี่ยวข้องกับการบริหารเครือข่ายขององค์กร เช่น Cisco, Alcatel-Lucent, Nortel, และ Juniper Networks เป็นต้น

6. Internet Platforms คือระบบต่าง ๆ ที่เกี่ยวข้องกับ Web Hosting Service ขององค์กร

7. Consulting and System Integration Services คือผู้ให้บริการภายนอกองค์กร เช่น IBM, HP เป็นต้น

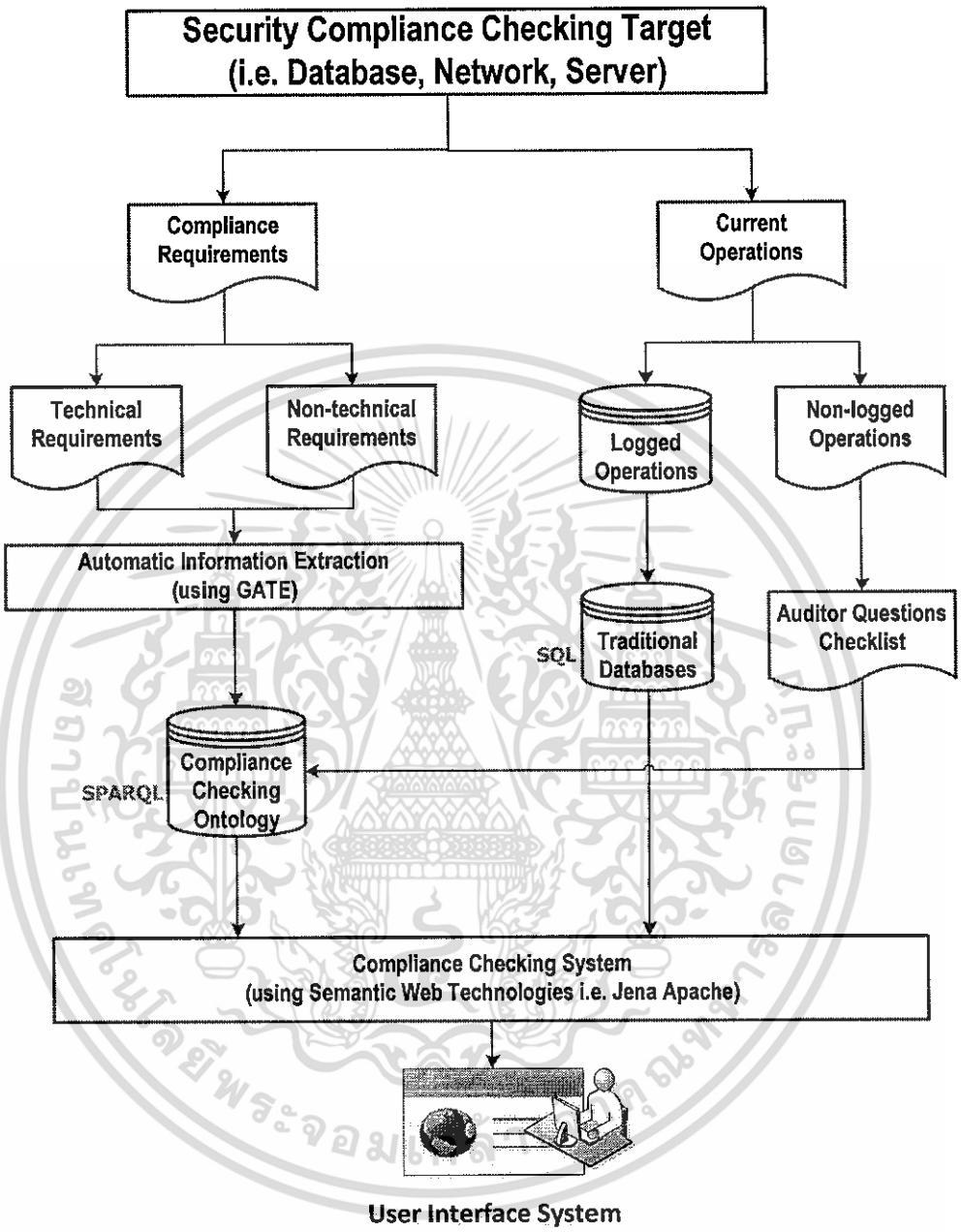
ซึ่งข้อมูลรายละเอียดของ Seven Major Components of IT Infrastructure จะถูกนำไปใช้ในการออกแบบและพัฒนาออนโทโลยีในขั้นตอนถัดไป

จะเห็นว่า ขั้นตอนที่ 4-8 ของการตรวจสอบนั้นสามารถปฏิบัติได้โดยผู้ตรวจสอบหรือผู้เชี่ยวชาญเท่านั้น ซึ่งรูปที่ 3.6 จะเป็นการนำเสนอสถาปัตยกรรมที่สามารถนำระบบคอมพิวเตอร์มาช่วยประมวลผลแทนผู้เชี่ยวชาญในขั้นตอนที่ 4-8

สถาปัตยกรรมในรูปที่ 3.6 สามารถอธิบายได้ดังนี้

1. Security Compliance Checking Target คือการกำหนดว่า Component ใดที่ต้องการตรวจสอบ ซึ่งเทียบได้กับการกำหนด Scope หรือ Area ที่ต้องการตรวจสอบ สำหรับ โดยการ

กำหนด Scope อ้างอิงมาจาก Seven Major Components of IT Infrastructure ตามที่ได้กล่าวมาแล้วในข้างต้น

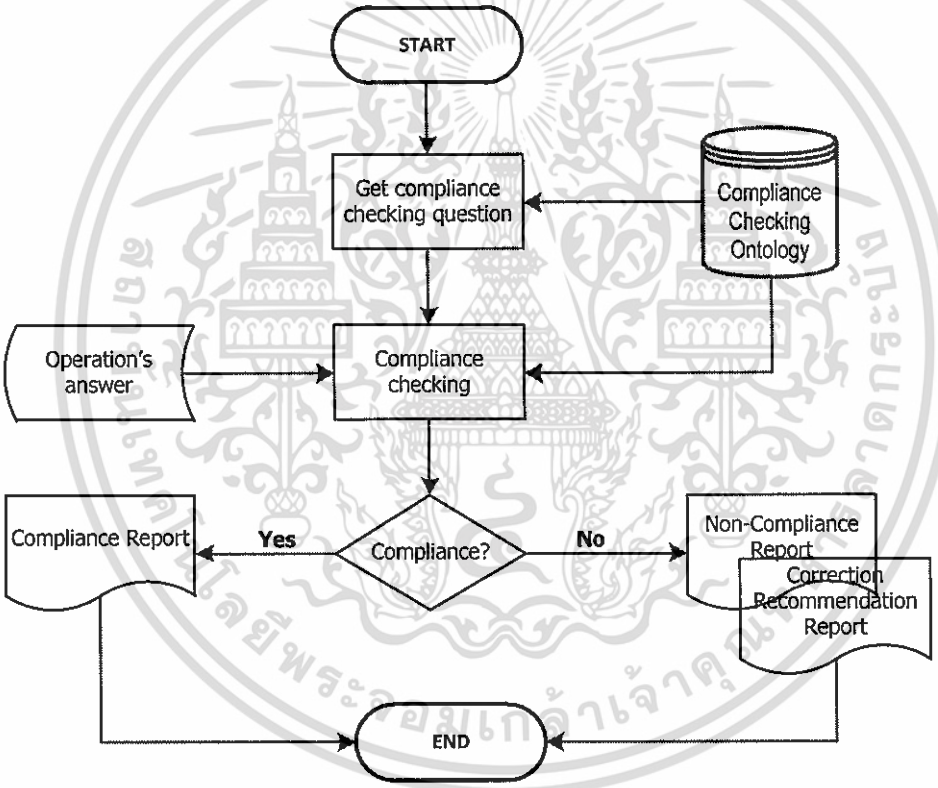


รูปที่ 3.6 Proposed Automated Security Compliance Checking

2. นำออนโทโลยี (Ontology) มาช่วยในการปรับเปลี่ยนรูปแบบของข้อมูลนโยบายหรือข้อกำหนดต่าง ๆ จากเอกสารภาษาธรรมชาติให้มาอยู่ในรูปแบบของข้อมูลที่สามารถประมวลผลได้ และออกแบบฐานข้อมูลเพื่อบันทึกข้อมูลของการปฏิบัติการที่เป็นแบบ Non-Logged Operations โดยใช้หลักการของการถามตอบตามขั้นตอนโดยทั่วไปของการตรวจสอบ

3. เพิ่มความเป็นอัตโนมัติเข้าไปในขั้นตอนของการสกัดข้อความจากเอกสารลงสู่ออนโทโลยี ด้วย GATE (General Architecture for Text Engineering) ซึ่ง GATE เป็นเครื่องมือที่ใช้กันอย่างแพร่หลายทางด้าน Information Extraction การใช้ GATE ในการสกัดข้อมูลลงในออนโทโลยีนั้น ก็เพื่อลดระยะเวลาและขั้นตอนการออกแบบระบบ (System Design) ในขั้นตอนการสร้าง User Interface System และสามารถช่วยในการจัดเตรียมรายการตรวจสอบ (Checklist) ของการตรวจสอบได้อีกด้วย

4. ใช้ Semantic Web Technologies เช่น Jena Apache ซึ่งสามารถเชื่อมต่อกับออนโทโลยี เพื่อพัฒนา User Interface System สำหรับการบันทึกผลและทำรายงานการประเมินผลและการแนะนำเพื่อปรับปรุงในกรณีที่พบว่ามีการปฏิบัติที่ไม่เป็นไปตามข้อกำหนด โดยมีผังงานของระบบที่ถูกเสนอดังรูปที่ 3.7



รูปที่ 3.7 ผังงานของ Proposed Security Compliance Checking System

วิธีการที่นำเสนอนี้จะสามารถช่วยให้ผู้ที่ไม่มีความเชี่ยวชาญทางด้านกฎระเบียบข้อบังคับสามารถตรวจสอบการปฏิบัติการของตนเองได้ว่าเป็นไปตามกฎระเบียบข้อบังคับหรือไม่ ทั้งนี้วิธีดำเนินการทดลองตามสถาปัตยกรรมที่นำเสนอ รวมทั้งผลการทดลองจะอธิบายในบทถัดไป

บทที่ 4
การทดลองพัฒนาระบบการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ

ในบทนี้จะเป็นการทดลองพัฒนาระบบการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ ตามกระบวนการที่ได้ออกแบบเอาไว้ในบทที่ 3 ซึ่งเนื้อหาหลัก ๆ ในบทนี้จะประกอบไปด้วย

1. กระบวนการออกแบบฐานข้อมูลออนโทโลยีที่รองรับภาษาธรรมชาติสำหรับนำเข้าข้อมูลนโยบายที่เกี่ยวข้องและข้อมูลการตรวจสอบ การเชื่อมโยงคำถามคำตอบสำหรับประเมินผลการตรวจสอบ การสร้าง Query เพื่อตรวจสอบว่าฐานข้อมูลสามารถใช้งานได้จริง เครื่องมือที่ใช้คือ Protégé ซึ่งเป็นเครื่องมือที่ใช้กันอย่างแพร่หลายในการพัฒนาออนโทโลยี

2. กระบวนการสกัดกฎระเบียบข้อบังคับออกจากเอกสารทางกฎหมายต่าง ๆ ที่ส่วนใหญ่อยู่ในรูปแบบของภาษาธรรมชาติ และนำเข้าข้อมูลไปยังฐานข้อมูลออนโทโลยีที่ได้พัฒนาในขั้นตอนก่อนหน้า เครื่องมือที่ใช้คือ GATE (General Architecture for Text Engineering) ซึ่งเป็นเครื่องมือที่ใช้กันอย่างแพร่หลายทางด้าน IE (Information Extraction)

4.1 การพัฒนาออนโทโลยีเพื่อแยกองค์ความรู้ออกจากนโยบายโดยอัตโนมัติ

เนื่องจากนโยบายต่าง ๆ ของระบบเทคโนโลยีสารสนเทศมักอยู่ในรูปแบบของภาษาธรรมชาติ (Natural Language) ซึ่งเป็นเรื่องยากที่จะใช้ระบบประมวลผลคอมพิวเตอร์ในรูปแบบทั่วไปดึงข้อมูลออกมาเพื่อประมวลผลต่อ ดังนั้น ในปัจจุบันจึงยังมีความจำเป็นอย่างยิ่งยวดที่ต้องพึ่งพาความสามารถของผู้เชี่ยวชาญทางด้านนโยบาย ซึ่งส่วนใหญ่ก็คือผู้ตรวจสอบความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ในการที่จะตีความนโยบาย แล้วนำมาเปรียบเทียบกับการควบคุมที่เป็นอยู่ว่าเป็นไปตามข้อกำหนดหรือไม่ จากกรณีนี้ทำให้ค่าใช้จ่ายในการตรวจสอบความปลอดภัยของระบบเทคโนโลยีสารสนเทศยังคงสูง เนื่องจากไม่มีระบบอัตโนมัติเข้ามาแทนที่การใช้แรงงานคนนั่นเอง การศึกษาค้นคว้าในเรื่องนี้จึงเกี่ยวข้องกับคำตอบที่ว่า ทำอย่างไรจึงจะสามารถดึงองค์ความรู้จากนโยบายออกมาสู่ระบบเทคโนโลยีสารสนเทศแบบอัตโนมัติเพื่อการตรวจสอบแบบอัตโนมัติในขั้นตอนถัด ๆ ไป

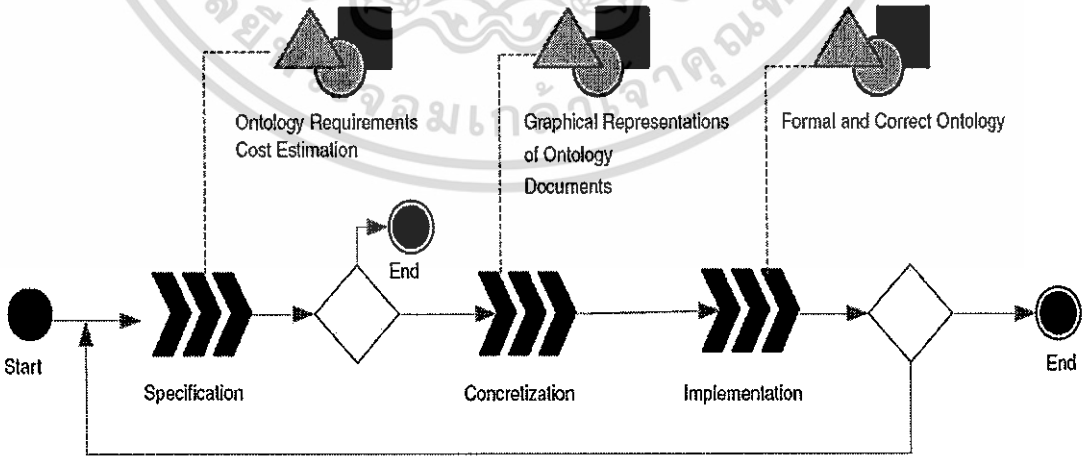
จากที่ได้กล่าวเอาไว้ในบทต้น ๆ นั้น ออนโทโลยี (Ontology) ถูกสร้างขึ้นมาเพื่อจำกัดองค์ความรู้ (Knowledge) ของขอบเขตข้อมูลนั้น ๆ โดยมีความสามารถในการใช้ข้อมูลร่วมกัน (Share) สามารถนำข้อมูลกลับมาใช้ได้ (Reuse) และมีความสามารถในการถ่ายทอดคุณสมบัติ (Inheritance)

การนำออนโทโลยีมาใช้งานจึงเป็นทางเลือกหนึ่งในการแชร์ข้อมูล และแยกองค์ความรู้ออกจากฐานข้อมูล การพัฒนาออนโทโลยีมีเป้าหมายเพื่อการแยกองค์ความรู้ของข้อมูลแบบอัตโนมัติจากแหล่งข้อมูลหลาย ๆ รูปแบบเช่น Word Document, PDF Document และ/หรือโดยเฉพาะอย่างยิ่งข้อมูลที่มาจากอินเทอร์เน็ต แล้วจัดเก็บเป็นฐานข้อมูลเพื่อใช้ในการแชร์ข้อมูลในขั้นตอนถัดไป

การพัฒนาออนโทโลยีในแต่ละโดเมนจะประสบความสำเร็จหรือไม่ขึ้นอยู่กับความถูกต้องของคำศัพท์และความเชื่อมโยงที่กำหนดว่าสามารถรองรับข้อมูลนำเข้าที่จะเกิดขึ้นจริงได้มากน้อยเพียงใด ดังนั้นผู้ที่พัฒนาออนโทโลยีในแต่ละโดเมน นอกจากต้องมีความเชี่ยวชาญในการพัฒนาออนโทโลยีแล้วต้องมีความเชี่ยวชาญในองค์ความรู้ของโดเมนนั้น ๆ อย่างแท้จริง และต้องสามารถ Mapping ได้จริงระหว่างออนโทโลยีที่พัฒนาขึ้นและเอกสารนำเข้าที่เกิดขึ้นจริง ถ้าหากการพัฒนาออนโทโลยีเป็นไปอย่างไม่ถูกต้อง จะเกิดความผิดพลาดของการคัดแยกข้อมูลจากเอกสารนำเข้าและทำให้ไม่สามารถนำไปใช้ประโยชน์ได้จริง

4.2 ขั้นตอนการพัฒนาออนโทโลยีสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ

ขั้นตอนการพัฒนาออนโทโลยีในงานวิจัยฉบับนี้ดำเนินไปตามคำแนะนำจากงานวิจัยชื่อ "Towards Ontological Engineering: a Process for Building a Domain Ontology from Scratch in Public Administration" [26] ร่วมกับ "Ontology Development 101: A Guide to Creating Your First Ontology" [27] โดยใช้ Protégé [30] ซึ่งเป็นเครื่องมือที่ใช้กันอย่างแพร่หลายในการพัฒนาออนโทโลยี ขั้นตอนต่าง ๆ ในรูปที่ 4.1 สามารถอธิบายได้ดังต่อไปนี้



รูปที่ 4.1 กระบวนการพัฒนาออนโทโลยี

4.2.1 การกำหนดขอบข่ายของโดเมน (Specification Subprocess)

ขั้นตอนที่ 1: อธิบายคุณลักษณะของโดเมน

ออนโทโลยีสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัตินี้เป็นการประมวลองค์ความรู้ของผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศในแต่ละส่วนหรือองค์ประกอบเข้ามารวบรวมเป็นออนโทโลยีที่สามารถนำไปประมวลผลได้โดยระบบคอมพิวเตอร์ เช่น กำลังจะตรวจสอบอะไร มีนโยบายอะไรบ้างที่เกี่ยวข้อง มีคำถามใดบ้างที่จะถามกับผู้ถูกตรวจสอบ คำตอบใดบ้างที่ถือว่าเป็นคำตอบที่เข้าข่ายการละเมิดกฎระเบียบข้อบังคับ เป็นต้น

ขั้นตอนที่ 2: การสมมุติสถานการณ์และคำถามตรวจสอบประสิทธิภาพของออนโทโลยี

ในขั้นตอนนี้จะมีการสมมุติสถานการณ์ขึ้นมาเพื่อช่วยให้การสร้างออนโทโลยีมีเป้าหมายที่ชัดเจนมากขึ้น รวมทั้งมีการกำหนดคำถามเพื่อใช้ตรวจสอบประสิทธิภาพของออนโทโลยีที่พัฒนาขึ้นมาว่าสามารถตอบคำถามเหล่านี้ได้หรือไม่ สถานการณ์สมมุติและคำถามตรวจสอบแสดงได้ดังตารางที่ 4.1 และ ตารางที่ 4.2 ตามลำดับ

ตารางที่ 4.1 สถานการณ์สมมุติสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง

ชื่อสถานการณ์	**การตรวจสอบ Data Center**
Site	DEMO
คำอธิบาย	DEMO เป็นบริษัทผลิตรถยนต์ เพื่อป้องกับทรัพย์สินทางด้านข้อมูลของบริษัท ฝ่ายไอทีของบริษัทจะต้องปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศที่กำหนดโดยสำนักงานใหญ่ ทุก ๆ 2 ปีจะมีการตรวจสอบ Data Center โดยผู้ตรวจสอบจากสำนักงานใหญ่ ซึ่งโดยปรกติแล้วทางบริษัท DEMO จะต้องจ่ายค่าบริการสำหรับการตรวจสอบให้กับผู้ตรวจสอบจากสำนักงานใหญ่เป็นมูลค่า 2 สัปดาห์ ทางบริษัทต้องการที่จะลดต้นทุนในครั้งนี้ให้เหลือเพียงแค่ 1 สัปดาห์ ดังนั้น ทางผู้จัดการฝ่ายไอทีจึงต้องมอบหมายให้ผู้ชำนาญการด้านนโยบายทำการตรวจสอบเบื้องต้นก่อนที่จะมีการตรวจสอบจริง
บุคลากร	- IT Manager - Information Security Expert
ความต้องการเบื้องต้น	- IT Policy - Data Center Related Policies

ตารางที่ 4.1 (ต่อ)

ขั้นตอนปรกติ	1. IT Infrastructure Supervisor จะร้องขอให้ Information Security Expert มาตรวจสอบประเมินความปลอดภัยของ Data Center 2. Information Security Expert จะร้องขอเอกสารและรวบรวมข้อมูลที่เกี่ยวข้องจาก IT Infrastructure Supervisor 4. Information Security Expert ทำการตรวจสอบเอกสารและตรวจพื้นที่จริง 4. กรณีที่เจอข้อบกพร่องของการควบคุม IT Security Expert จะแจ้งต่อ IT Infrastructure Supervisor 5. IT Infrastructure Supervisor หารือเพื่อแก้ไขข้อบกพร่องกับ IT Manager 6. ฝ่ายไอทีทำการแก้ไขข้อบกพร่องตามที่ Information Security Expert ระบุมา
Main problems	- กระบวนการตรวจสอบนั้นต้องพึ่งพา Information Security Expert อย่างสูง

ตารางที่ 4.2 ตัวอย่างคำถามเพื่อตรวจสอบความสามารถของออนโทโลยี

1. What are questions that auditors always ask when they perform the audit?
2. What are responses that might be the audit finding for each auditor questions?
3. What should be the valid control that comply to auditors questions?
4. If auditors found the control gaps, what should be done to correct a control?

ขั้นตอนที่ 3: กำหนดเป้าหมายและขอบเขตของการพัฒนาออนโทโลยี

ออนโทโลยีนี้พัฒนาขึ้นมาเพื่อจำลองกิจกรรมที่ผู้ตรวจสอบกระทำเมื่อทำการตรวจสอบระบบเทคโนโลยีสารสนเทศ

4.2.2 การออกแบบออนโทโลยี (Concretization Subprocess)

ขั้นตอนที่ 1: กำหนดคลาสและลำดับชั้นของคลาส

ในขั้นตอนนี้จะเป็นการกำหนดคำศัพท์ หรือ Term ที่สำคัญของโดเมน ซึ่งแสดงได้ดังตารางที่ 4.3

ตารางที่ 4.3 คลาสหลักและคลาสย่อยที่สำคัญ

Class	Subclass
Main Component	Computer hardware platforms
	Operating system platforms
	Enterprise and other software applications
	Data management and storage
	Networking and telecommunications platforms
	Internet platforms
	Consulting and system integration services
Sub Component	Activity
	Document
	Environment
	Equipment
	Personnel
	Event
Policy	-
Auditor Question	-
Global Standard	-

- คลาส "Main Component" ถูกกำหนดมาเป็นคลาสระดับสูงสุดของโดเมนนี้เพื่อบรรจุข้อมูลเกี่ยวกับส่วนประกอบต่าง ๆ ที่จะถูกตรวจสอบ เช่น "Data Center", "Database", "Network", "Business Application" เป็นต้น ซึ่งส่วนประกอบเหล่านี้จะอยู่ภายใต้ subclass ที่อ้างอิงมาจาก "Seven Major Components of IT Infrastructure" [25] ซึ่งประกอบด้วย "Computer hardware platforms", "Operating system platforms", "Enterprise and other software applications", "Data management and storage", "Networking and telecommunications platforms", "Internet platforms", "Consulting and system integration services" ตามที่ได้อธิบายมาแล้วในบทที่ 3

- คลาส "Sub Component" ถูกกำหนดเพื่อบรรจุข้อมูลที่มีความเกี่ยวพันกับ Main Component หรือ Component ที่จะถูกตรวจสอบ แบ่งเป็น Subclass ย่อย ๆ ได้คือ "Activity", "Document", "Environment", "Equipment", "Personnel" และ "Event"

- คลาส "Policy" ถูกกำหนดมาเพื่อบรรจุข้อมูลที่เป็นนโยบายที่เกี่ยวข้องกับ Audited Component ตัวอย่างเช่น สมมุติว่า Data Center กำลังจะถูกตรวจสอบ หนึ่งในนโยบายที่เกี่ยวข้องก็คือ นโยบายด้านความปลอดภัยของ Data Center ตัวอย่างนโยบายที่จะบันทึกอยู่ในคลาสนี้เช่น "Smoking is not permitted in data center", "Entry and exiting doors must be secured utilizing the Card Access System."

- คลาส "Global Standard" ถูกกำหนดมาเพื่อบรรจุข้อมูลของมาตรฐานต่างๆ ที่นโยบายได้อ้างอิงถึง ตัวอย่างเช่น "NFPA", "SOX", "ISO27001", "ITIL", "COBIT" เป็นต้น

- คลาส "Auditor Question" ถูกกำหนดมาเพื่อบรรจุคำถามที่ถูกถามบ่อย ๆ โดยผู้ตรวจสอบ คลาสนี้ต้องการผู้เชี่ยวชาญทางด้านนโยบายหรือผู้ตรวจสอบเป็นผู้กำหนดรายการของคำถามขึ้นมา ตัวอย่างเช่น คำถามที่เกี่ยวข้องกับ Data Center คือ "What kind of access control at entry door?"

ขั้นตอนที่ 2: กำหนดความสัมพันธ์ คุณลักษณะและ คุณสมบัติของแต่ละคลาส

การกำหนดแต่คลาสเพียงอย่างเดียวไม่สามารถจะให้ข้อมูลที่เพียงพอได้ จึงต้องมีการกำหนดความสัมพันธ์ คุณลักษณะและคุณสมบัติของแต่ละคลาสดังแสดงได้ในตารางที่ 4.4

ตารางที่ 4.4 ตัวอย่างความสัมพันธ์ คุณลักษณะและ คุณสมบัติของแต่ละคลาส

Class Name #1	Relation	Class Name #2	Inverse relation
Main Component	hasPolicy	Policy	relatedTo
Sub Component	hasPolicy	Policy	relatedTo
Main Component	hasSubComponent	Sub Component	isSubComponentOf
Policy	hasReference	Global Standard	none
Auditor Question	askAbout	Main Component	hasQuestion
Auditor Question	askAbout	Sub Component	hasQuestion

ขั้นตอนที่ 3: กำหนดกฎเกณฑ์และข้อจำกัดของความสัมพันธ์และคุณสมบัติของแต่ละคลาส

ขั้นตอนนี้เป็นการกำหนดขอบเขตของความสัมพันธ์และคุณสมบัติของแต่ละคลาส ดังแสดงในตารางที่ 4.5

ตารางที่ 4.5 ตัวอย่างกฎเกณฑ์และข้อจำกัดของความสัมพันธ์และคุณสมบัติของแต่ละคลาส

Class	**Property**	**Type**	**Restrictions**
Main Component	hasDescription	String	
	hasSubComponent	Instant	class{Sub Component}
	hasPolicy	Instant	class{Policy}
Sub Component	hasDescription	String	
	isComponentOf	Instant	class{Main Component}
	hasPolicy	Instant	class{Policy}
Policy	hasTopic	String	
	hasSubTopic	String	
	hasContent	String	
	hasRemark	String	
	hasSubject	String	
	hasObject	String	
	hasCompliance_List	String	
	hasNonCompliance_List	String	
	hasReference	Instant	class{Global Standard}
	relatedTo	Instant	class{Main Component, Sub Component}
Auditor Question	hasContent	String	
	askAbout	Instant	class{Main Component, Sub Component}

ขั้นตอนที่ 4: กำหนดข้อมูลจริงเพื่อบันทึกลงในแต่ละคลาส

ขั้นตอนนี้เป็นการกำหนดข้อมูลจริงสำหรับแต่ละคลาส ดังแสดงได้ในตารางที่ 4.6

ตารางที่ 4.6 ตัวอย่างของข้อมูลจริงที่บันทึกลงในแต่ละคลาส

Class/SubClass	Instance Name	Property Name	Property Value
Main Component/Data management and storage	Data Center	hasDescription	Data center is a facility used for housing a large amount of computer and communications …
Sub Component /Activity	Smoking	hasDescription	Smoking is activity that may create fire.
		isSubComponentOf	Data Center
Sub Component /Equipment	Fire Extinguisher	hasDescription	A portable device for extinguishing fires, usually consisting ...
		isSubComponentOf	Data Center
Global Standard	NFPA	hasDescription	NFPA (National Fire Protection Association) is the world's leading advocate of fire prevention …
	ISO27002	hasDescription	ISO27002 is a detailed security standard organized into 10 major sections….
	ITIL	hasDescription	ITIL (IT Infrastructure Library) features seven sets of processes..
Policy (Dynamic)	To be dynamic	hasTopic	To be dynamic extracted
Auditor Question	DCQ1.1	hasContent	Is non-smoking sigh put in data center?
		askAbout	Smoking
			Data center

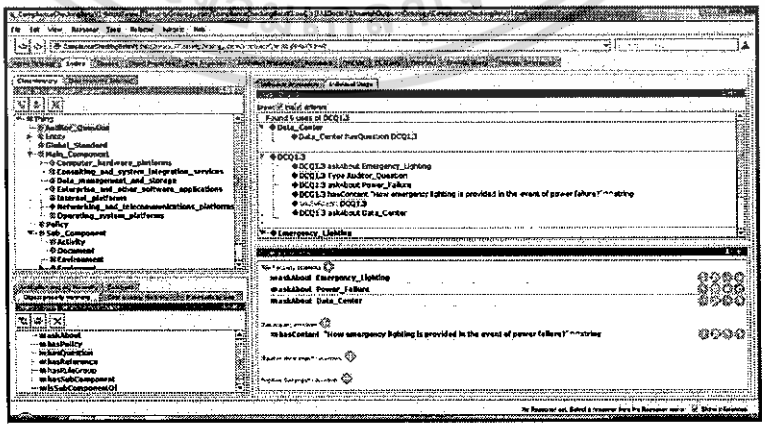
ตารางที่ 4.6 (ต่อ)

Class/SubClass	Instance Name	Property Name	Property Value
	DCQ1.2	hasContent	What kinds of fire extinguishers are provided in data center?
		askAbout	Fire extinguisher
			Data Center
	DCQ1.3	hasContent	How emergency lighting is provided in the event of power failure?
		askAbout	Emengency Lighting
			Power failure
			Data Center

4.2.3 การนำไปใช้งานจริง (Implementation Subprocess)

ขั้นตอนที่ 1: สร้างออนโทโลยีที่สามารถประมวลผลได้

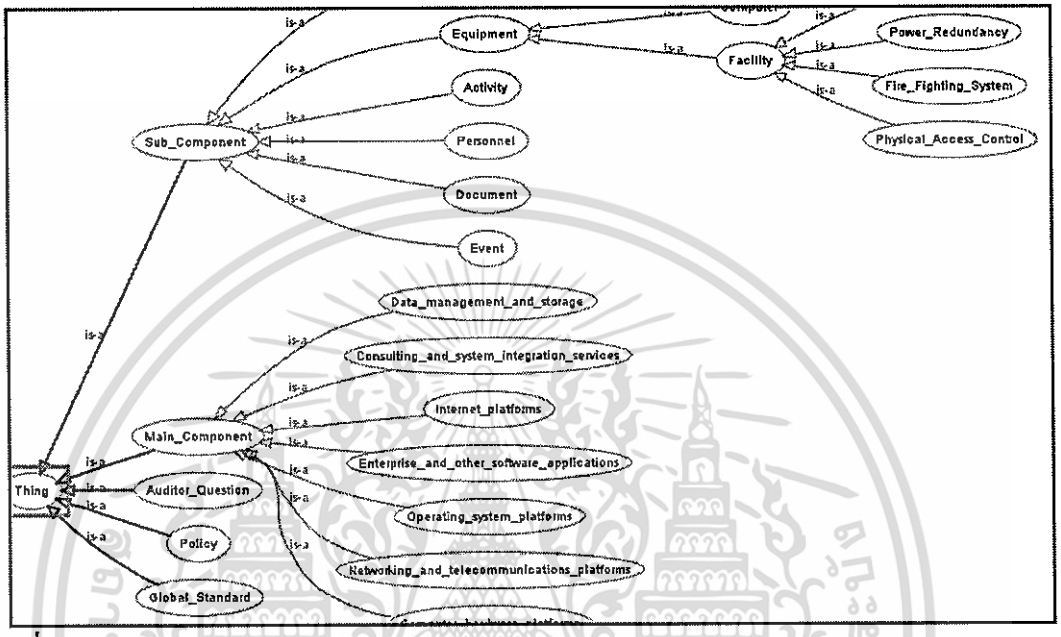
ขั้นตอนนี้เป็นการนำสิ่งที่ออกแบบในขั้นตอนก่อนหน้าไปพัฒนาเป็นออนโทโลยีที่สามารถประมวลผลได้โดยระบบคอมพิวเตอร์ โดยการใช้โปรแกรมภาษาที่เหมาะสม ซึ่งมีหลายรูปแบบ แต่ที่มีความเกี่ยวข้องและเหมาะสมมากที่สุดสำหรับงานนี้คือภาษา RDF(Resource Description Framework) และ OWL (Web Ontology Language) ในกระบวนการนี้ได้นำ Protege ซึ่งเป็นโปรแกรมพัฒนาออนโทโลยีที่แพร่หลายมาเป็นเครื่องมือในการพัฒนาออนโทโลยี ซึ่งแสดงได้ดังรูปที่ 4.2



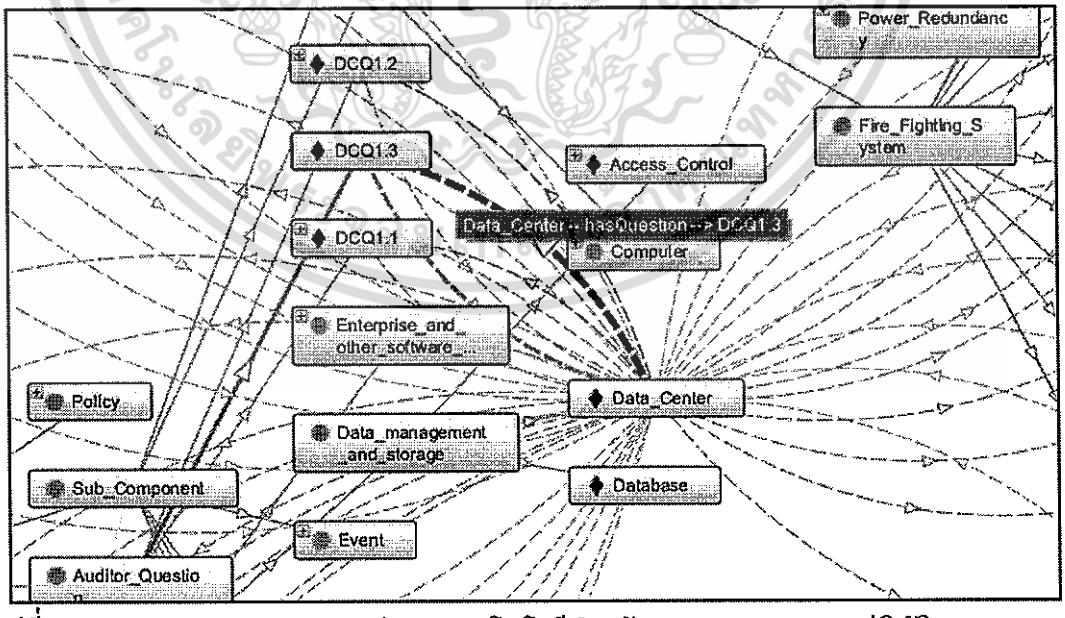
รูปที่ 4.2 ออนโทโลยีสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงที่พัฒนาโดย Protégé

ขั้นตอนที่ 2: การตรวจสอบข้อผิดพลาดของออนโทโลยี

เป้าหมายของขั้นตอนนี้เพื่อหลีกเลี่ยงการเกิดข้อผิดพลาดในอนาคต เราใช้ OWLViz และ OntoGraf แสดงออกมาเป็นรูปแบบกราฟเพื่อเปรียบเทียบออนโทโลยีที่พัฒนาขึ้นกับสิ่งที่ได้ออกแบบไว้ในกระบวนการก่อนหน้านี้ ดังแสดงได้ในรูปที่ 4.3 และรูปที่ 4.4



รูปที่ 4.3 OWLViz แสดงภาพกราฟของออนโทโลยีสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง



รูปที่ 4.4 OntoGraf แสดงภาพกราฟของออนโทโลยีสำหรับการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง

ขั้นตอนที่ 3: การตรวจสอบว่าออนโทโลยีสามารถใช้งานได้จริง

เพื่อตรวจสอบว่าออนโทโลยีสามารถใช้งานได้จริง จำเป็นอย่างยิ่งที่ต้องตรวจสอบว่าออนโทโลยีนั้นสามารถตอบคำถามที่ได้กำหนดไว้เป็นคำถามตรวจสอบความสามารถ (Competency Question) ในขั้นตอนต้นได้หรือไม่ เราต้องทำการตรวจสอบโดยใช้ Semantic Queries ด้วยภาษา SPARQL เพื่อให้ง่ายต่อการความเข้าใจก่อนการตรวจสอบ เราได้ทำการรวบรวมข้อมูลทั้งหมดไว้ในรูปของตารางดังแสดงในตารางที่ 4.7 โดยการจับคู่นโยบาย (Policy Mapping) กับ Auditor Questions, Compliance Lists และ Non-Compliance Lists แล้วใช้ SPARQL แสดงผลออกมา ดังรูปที่ 4.5

ตารางที่ 4.7 ตัวอย่างการจับคู่นโยบายกับ Auditor Questions, Compliance Lists และ Non-Compliance Lists

No.	Policy Content	Related To (extracted)	Auditor Questions	Compliance Lists (extracted)	Non-Compliance Lists (extracted)
1.	Smoking is not permitted in data center.	Smoking/ Data center	Is non-smoking sign put in data center?	Yes (Smoking is not permitted)	No (Smoking is permitted)
2.	Emergency lighting shall be installed in all data centers. The lighting shall operate automatically in the event of a power failure.	Emergency lighting/ Power failure.	Has emergency lighting been installed in data center?	Emergency lighting immediately provided.	No emergency lighting is provided.
			How emergency lighting is provided in the event of power failure?	Automatically	Manual
4.	Type of Fire Extinguishers Pressurized water fire extinguisher. Carbon dioxide (CO2) fire extinguishers Clean agent (ABC type rated) Dry chemical fire extinguishers are prohibited	Fire extinguisher	What kinds of fire extinguishers are provided in data center?	Pressurized water fire extinguisher. Carbon dioxide (CO2) fire extinguisher. Clean agent (ABC type rated).	No water fire extinguisher. No carbon dioxide (CO2) fire extinguisher. Dry chemical fire extinguishers.
4.	Entry and exiting doors must be secured utilizing the Card Access System.	Physical Access	What kind of access control at entry door?	Card Access System.	Others
5.	Provide emergency power disconnect switches located inside the computer room at main exit doors.	Emergency power disconnect	Does data center install emergency power disconnect switch?	Yes	No emergency power disconnect switch.
			Where is emergency power disconnect switch located?	Main exit doors	Others

Competency Question 1.

What are questions that auditors always ask when they perform the audit?

Query

```
PREFIX CC: <http://www.ITSecurityOntology.com/ComplianceCheckingBetaV1.owl#>
SELECT ?MainComponent ?SubComponent ?Question
WHERE {
?SubComponent CC:isSubComponentOf ?MainComponent .
?SubComponent  CC:hasQuestion ?Q.
?Q CC:hasContent ?Question
}
order by ?MainComponent?SubComponent
```

Results

MainComponent	SubComponent	Question
Data_Center	Emergency_Lighting	How emergency lighting is provided in the event of power failure?
Data_Center	Fire_Extinguisher	What kinds of fire extinguishers are provided in data center?
Data_Center	Power_Failure	How emergency lighting is provided in the event of power failure?
Data_Center	Smoking	How smoking prohibit in data center?

Competency Question 2.

What are responses that might be the audit finding for each auditor questions?

Query

```
PREFIX CC: <http://www.ITSecurityOntology.com/ComplianceCheckingBetaV1.owl#>
SELECT ?MainComponent ?SubComponent ?Question ?NonCompliance
WHERE {
   ?SubComponent CC:isSubComponentOf ?MainComponent.
   ?SubComponent CC:hasQuestion ?Q .
   ?Q CC:hasContent ?Question .
  ?y  CC:hasNonCompliance_List ?NonCompliance
   FILTER REGEX(?Question,"fire ex")
}
```

Results

MainComponent	SubComponent	Question	NonCompliance
Data_Center	Fire_Extinguisher	What kinds of fire extinguishers are provi...	Dry chemical fire extinguishers

Competency Question 3.

What should be the valid control that comply to auditors questions?

Query

```
PREFIX CC: <http://www.ITSecurityOntology.com/ComplianceCheckingBetaV1.owl#>
SELECT ?MainComponent ?SubComponent ?Question ?Compliance
WHERE {
   ?SubComponent CC:isSubComponentOf ?MainComponent.
   ?SubComponent CC:hasQuestion ?Q .
   ?Q CC:hasContent ?Question .
  ?y  CC:hasCompliance_List ?Compliance
   FILTER REGEX(?Question,"fire ex")
}
```

Results

MainComponent	SubComponent	Question	Compliance
Data_Center	Fire_Extinguisher	What kinds of fire extinguishers are p...	Clean agent (ABC type rated)
Data_Center	Fire_Extinguisher	What kinds of fire extinguishers are p...	Carbon dioxide (CO2) fire extinguisher
Data_Center	Fire_Extinguisher	What kinds of fire extinguishers are p...	Water fire extinguisher

Competency Question 4.

If auditors found the control gaps, what should be done to correct a control?

Query

```
PREFIX CC: <http://www.ITSecurityOntology.com/ComplianceCheckingBetaV1.owl#>
SELECT ?SubComponent ?Question ?NonCompliance ?Policy
WHERE {
   ?SubComponent CC:isSubComponentOf ?MainComponent.
   ?SubComponent CC:hasQuestion ?Q .
   ?Q CC:hasContent ?Question .
  ?y  CC:hasNonCompliance_List ?NonCompliance.
  ?SubComponent CC:hasPolicy ?P.
  ?P CC:hasContent ?Policy
   FILTER REGEX(?Question,"fire ex")
}
```

Results

SubComponent	Question	NonCompliance	Policy
Fire_Extinguisher	What kinds of fire extinguishers are provi...	Dry chemical fire extinguishers	Type of Fire Extinguishers;a) 9.5 liter (21/2 gallon) pr

รูปที่ 4.5 ผลลัพธ์จากการ Query ด้วยคำสั่ง SPARQL

จากตัวอย่างข้างต้น แสดงให้เห็นว่าออนโทโลยีที่พัฒนาขึ้นมาสามารถจัดเตรียมผลลัพธ์สำหรับขั้นตอนถัดไปเพื่อรอรับคำตอบจากผู้ที่ถูกตรวจสอบแล้วนำไปประมวลผลเพื่อให้ได้เป็นผลการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติได้

4.3 การสกัดกฎระเบียบหรือข้อกำหนดออกจากเอกสารทางกฎหมาย (Information Extraction from Regulatory Documents)

ในการประเมินผลว่าการปฏิบัติขององค์กรเป็นไปตามเอกสารควบคุมหรือนโยบายที่ได้กำหนดไว้หรือไม่ กระบวนการนี้ต้องการข้อมูล 2 ส่วนมาเปรียบเทียบกันและทำการประเมิน ข้อมูลส่วนแรกที่สำคัญคือข้อมูลเกี่ยวกับ Compliance Requirements ซึ่งก็คือข้อกำหนดต่าง ๆ นั่นเอง (อ้างอิงจาก Security Compliance Checking Framework ที่ได้อธิบายในบทที่ 2) การที่จะทำให้ระบบ Security Compliance Checking เป็นไปอย่างอัตโนมัติ จะต้องมีการสกัดกฎระเบียบหรือข้อกำหนดออกจากเอกสารทางกฎหมายแบบอัตโนมัติ เพื่อเป็นข้อมูลนำเข้าสู่ฐานข้อมูลออนโทโลยีที่ได้พัฒนาไว้แล้วในหัวข้อที่ผ่านมา

เนื่องจากเอกสารทางด้านข้อกำหนดและกฎหมายส่วนใหญ่จะเขียนออกมาในรูปแบบของภาษาธรรมชาติซึ่งคนเราสามารถอ่านและเข้าใจได้ แต่เครื่องคอมพิวเตอร์ไม่สามารถเข้าใจได้หากไม่มีการตีความโดยคน ดังนั้นจึงเป็นความท้าทายอย่างสูงที่จะทำการสกัดหรือดึงข้อมูลออกจากเอกสารเหล่านี้แบบอัตโนมัติ มีนักวิจัยจำนวนมากพยายามที่จะหาวิธีการกำหนดโครงสร้างของข้อมูลเพื่อทำให้เครื่องคอมพิวเตอร์สามารถสกัดข้อมูลออกมาได้ ซึ่งแนวทางส่วนใหญ่คือการทำหมายเหตุประกอบลงในข้อมูล (Data Annotation) เพื่อทำการค้นหาและสรุปคำตอบแบบใช้หลักเหตุผล (Reasoning) โดยใช้เครื่องมือการประมวลผลภาษาธรรมชาติ (Natural Language Processing) อย่างไรก็ตามเอกสารทางด้านกฎหมายนั้นมักจะประกอบไปด้วยถ้อยคำหลายร้อยหลายพันคำ ไม่ใช่ทุกคำที่จำเป็นสำหรับระบบตรวจสอบแบบอัตโนมัติ การสกัดออกมาเฉพาะประโยคที่มีใจความสำคัญจึงเป็นการลดเวลาและภาระการทำงานของกระบวนการสกัดข้อกำหนด ในหัวข้อถัดไปจะนำเสนอกระบวนการสกัดข้อกำหนดออกจากเอกสารทางกฎหมายในรูปแบบของ Goal หรือ SOTA (Subject, Object, Target, Action) โดยใช้เครื่องมือที่ชื่อว่า GATE

4.4 การสกัดประโยคที่มีข้อความสำคัญออกจากเอกสารทางด้านกฎหมาย (Requirements Extraction from Legal Documents)

ในหัวข้อนี้ จะอธิบายถึงกระบวนการของการสกัดประโยคที่มีข้อความสำคัญจากเอกสารทางด้านกฎหมาย โดยอ้างอิงจากหลักการ GBRAM (Goal-Based Requirements Analysis Method) [28] ซึ่งเป็นกระบวนการในการระบุเป้าหมายและความต้องการขององค์กร ซึ่งมีประโยชน์ในการบ่งชี้และกรั่นกรองเป้าหมายที่ระบบจะต้องทำให้สำเร็จโดยทำการเปลี่ยนแปลงเป้าหมายให้เป็นสิ่งที่องค์กรจะต้องปฏิบัติ GBRAM นั้น เป็นการอิมพลีเมนต์ในรูปแบบความสัมพันธ์ของ Subject, Object, Target, Action (SOTA) ซึ่งเป็นการแสดงให้เห็นถึงเป้าหมายนั่นเอง ซึ่งเครื่องมือที่ใช้คือ GATE

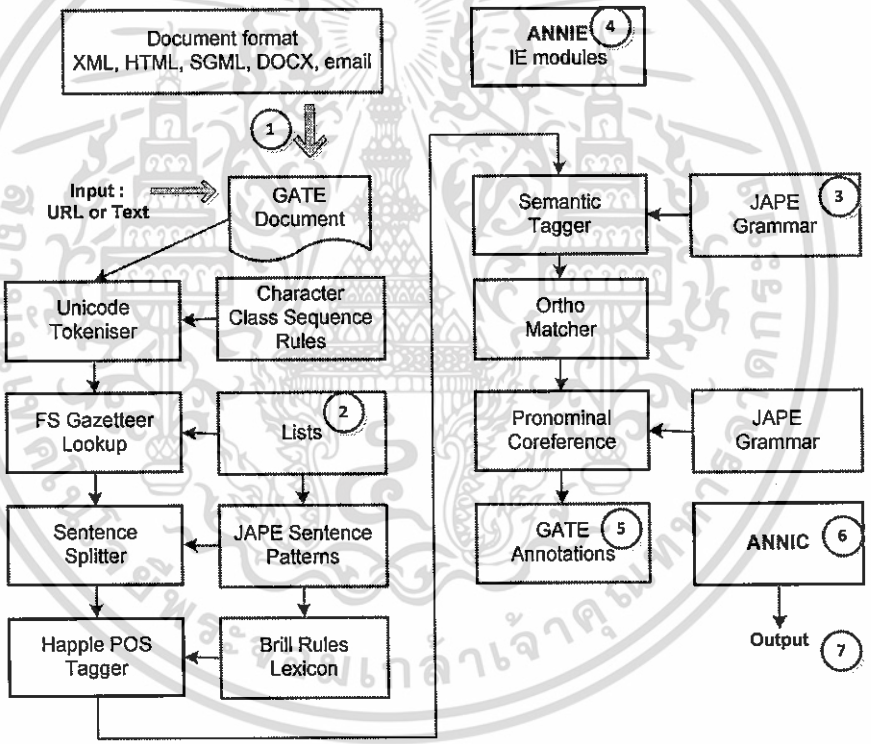
GATE (General Architecture for Text Engineering) เป็นสถาปัตยกรรมสำหรับประมวลผลภาษาธรรมชาติ โดยเฉพาะอย่างยิ่งเป็นเครื่องมือที่ใช้กันอย่างแพร่หลายทางด้านการสกัดข้อมูล ใน GATE จะประกอบไปด้วยองค์ประกอบที่สำคัญ 3 ส่วนหลัก ๆ คือ

1. Language Resource (LR) – องค์ประกอบด้านข้อมูลภาษา เช่น พจนานุกรม (Lexicons), คลังข้อมูลภาษา (Corpus) และ ออนโทโลยี เป็นต้น

2. Processing Resource (PR) – องค์ประกอบที่เป็นชุดของคำสั่งพื้นฐานที่สร้างไว้ (Algorithm)

3. Visual Resource (VR) – องค์ประกอบที่เป็นสถาปัตยกรรมสำหรับการพัฒนาในรูปแบบของ GUIs

เพื่อเป็นการสาธิตสถาปัตยกรรมของงานนี้ เราได้ใช้เอกสาร ISO27002 ซึ่งเป็นมาตรฐานควบคุมความมั่นคงปลอดภัยทางด้านสารสนเทศมาเป็นเอกสารตัวอย่าง



รูปที่ 4.6 สถาปัตยกรรมของการสกัดข้อมูลออกจากเอกสารทางด้านกฎหมาย

จากรูปที่ 4.6 เราใช้ GATE Developer เป็นเสมือน Visual Resource (VR) ในการพัฒนา ใช้เอกสาร ISO27002 เป็นเสมือน Language Resource (LR) และใช้ Processing Resource (PR) ต่าง ๆ ใน GATE เพื่อสกัดข้อมูลที่ต้องการ ซึ่ง Processing Resource ที่สำคัญใน GATE มีดังนี้

1. Gazetteer คือ Plaintext ที่ประกอบไปด้วยรายการของชื่อหรือคำต่าง ๆ ที่สามารถนำมาใช้ร่วมกันในหลาย ๆ โดเมน (Domain)

2. JAPE (Java Annotation Pattern Engine) คือโปรแกรมที่พัฒนาขึ้นเพื่อทำการสร้างหมายเหตุประกอบในเอกสาร ซึ่งไวยกรณ์ใน JAPE rule นั้นจะประกอบไปด้วย ภาษา 2 ส่วนคือ

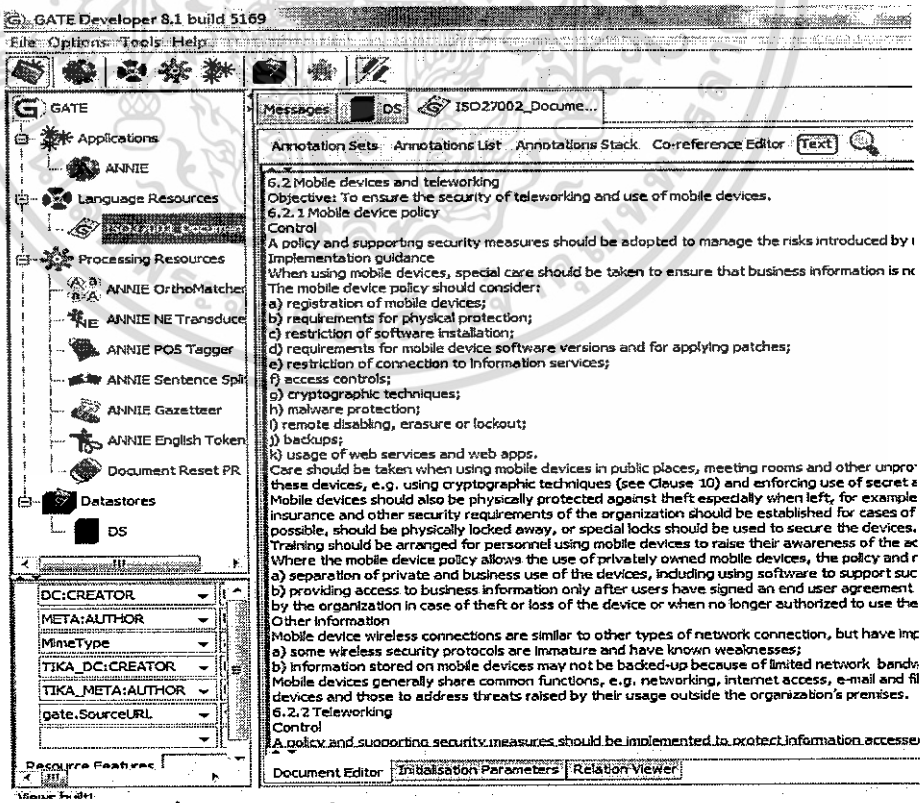
- LHS (Left Hand Side) คือกฎที่ต้องการค้นหาเพื่อสร้างหมายเหตุประกอบ
- RHS (Right Hand Side) คือหมายเหตุประกอบที่ต้องการให้สร้างขึ้นเมื่อกฎของ LHS ถูกค้นพบ

3. ANNIE (A Nearly-New Information Extraction System) เป็นอัลการิทึมที่สร้างมาพร้อมใช้ (Ready-Made) สำหรับการสกัดข้อมูลในเอกสารที่ไร้โครงสร้าง ใน ANNIE ประกอบไปด้วย PR ที่สำคัญซึ่งจะอธิบายในส่วนของรายละเอียดของขั้นตอน

4. ANNIC (Annotations in Context) เป็น plug-in ใน GATE ที่ช่วยในการสืบค้น Annotations ในเอกสารได้โดยการใช้ Query

ต่อไปจะเป็นการอธิบายถึงขั้นตอนการปรับใช้ Processing Resource ต่าง ๆ ใน GATE เพื่อทำการสกัดสิ่งที่จะต้องถูกควบคุมออกจากเอกสารทางด้านกฎหมาย

1. โหลดตัวอย่างเอกสาร ISO27002 เพื่อเป็น LR เอกสารสามารถจัดเก็บในรูปแบบของ “Serial Data Store” หรือ “Lucene Based Searchable Datastore” ในกรณีนี้เราจัดเก็บในรูปแบบของ Lucene Based Searchable Datastore เพื่อจะใช้ค้นหาใน ANNIC ในขั้นตอนหลัง ๆ ตัวอย่างเอกสารที่โหลดใน GATE แสดงได้ดังรูปที่ 4.7



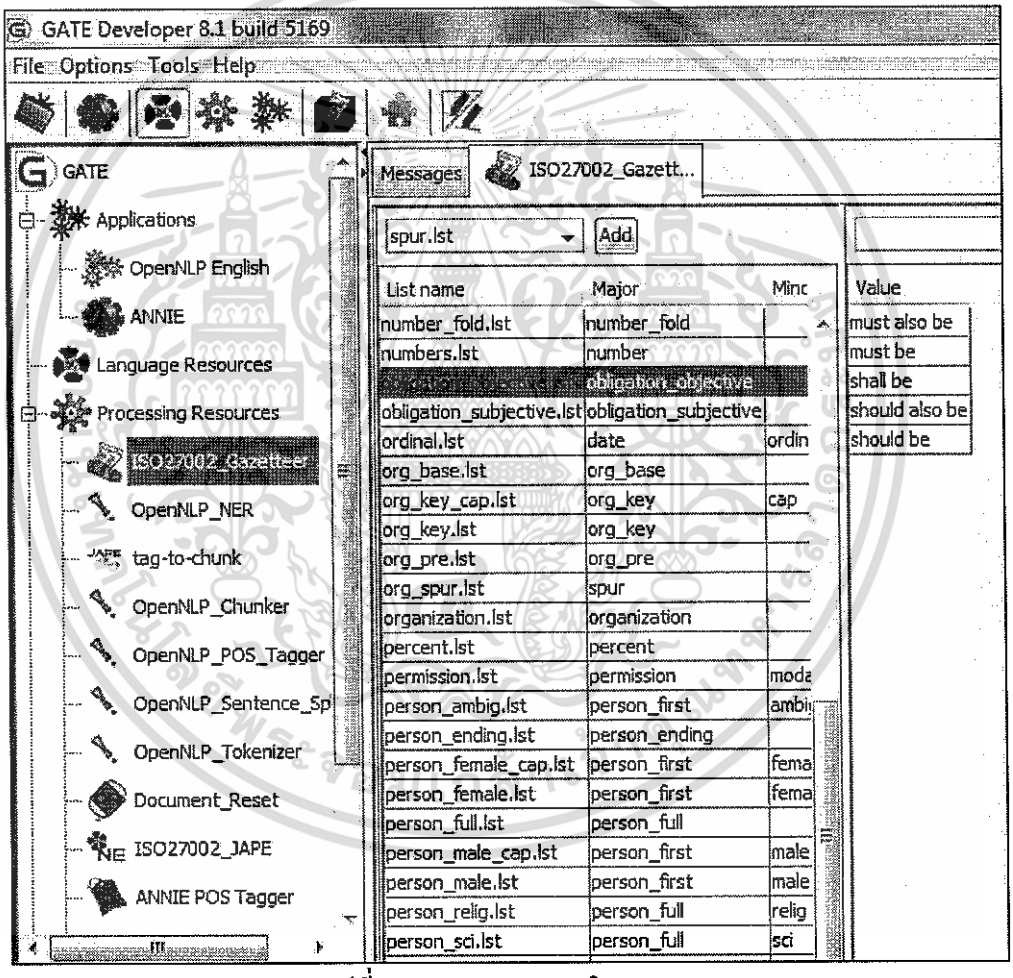
รูปที่ 4.7 เอกสารที่โหลดเป็น Language Resource ใน GATE

2. พัฒนา Gazetteer ซึ่งประกอบไปด้วยรายการของประโยคดัง Terminologies เหล่านี้

- Right – คือกิจกรรมที่ Stakeholder ได้รับการยินยอมให้ทำได้ โดยเป็นตามเงื่อนไข ซึ่งประโยคที่อยู่ในกลุ่มของ "Right" จะมีคำเหล่านี้อยู่ในประโยค เช่น "can be", "could be", "may", "might", "might be", "may deny", "may require", เป็นต้น

- Obligation – คือกิจกรรมที่ Stakeholder ได้รับการร้องขอให้ทำ โดยเป็นไปตามเงื่อนไข ประโยคที่อยู่ในกลุ่มของ "Obligation" จะมีคำเหล่านี้อยู่ในประโยค เช่น "may not", "must", "should", "should be", "should also be", "must be", "required to", เป็นต้น

Gazetteer ที่พัฒนาใน GATE แสดงได้ดังรูปที่ 4.8



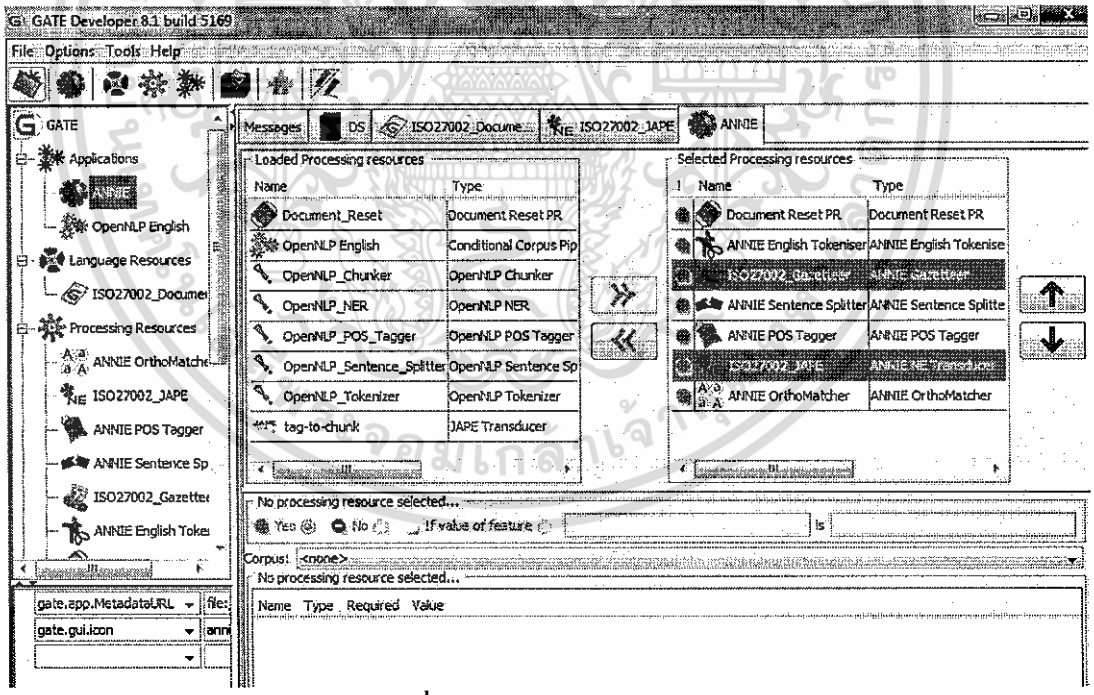
รูปที่ 4.8 Gazetteer List ใน GATE

3. พัฒนา JAPE Grammars ที่ช่วยในการบ่งชี้ว่าประโยคใดที่เป็นประโยคควบคุม ตัวอย่าง JAPE Grammar ที่แสดงในรูปที่ 4.9 จะค้นหาประโยคที่ตรงกันกับ Gazetteer List ซึ่งมีคำที่เป็น Obligation แล้วสร้าง Annotations ที่ชื่อว่า "ObligationObjectSentence"

```
Phase: thing2control
Input: Lookup Sentence
Options: control = appelt

Rule: ObligationObjectvieSentence01
Priority: 5
(
{Sentence contains {Lookup.majorType ==
"obligation_objective"}
}
):ObligationObjectiveSentence
                                    -->
 :ObligationObjectiveSentence.ObligationObjectiveSentence =
{rule = "ObligationObjectiveSentence01"}
```

รูปที่ 4.9 JAPE Grammar ที่จะทำการสร้างหมายเหตุประกอบ ของประโยคที่เป็น Obligation

4. Run ANNIE โดยใช้เอกสารที่โหลดในขั้นตอนที่ 1 ใช้ Gazetteer จากขั้นตอนที่ 2 และใช้ JAPE จากขั้นตอนที่ 3 ซึ่งหน้าตาของ ANNIE ที่ถูกแก้ไขจะแสดงได้ดังรูปที่ 4.10



รูปที่ 4.10 Customized ANNIE

จากรูปจะเห็นว่า ANNIE ประกอบด้วยหลาย Processing Resource มารันต่อ ๆ กัน ซึ่งการทำงานของแต่ละ Processing Resource ใน ANNIE สามารถอธิบายได้คร่าว ๆ ดังนี้

4.1. Document Reset PR: เป็นการรีเซ็ต Annotations ที่สร้างก่อนหน้าเพื่อป้องกันการสร้างใหม่ที่ซ้ำซ้อน

4.2. ANNIE English Tokeniser: เป็นการตัดคำภาษาอังกฤษ ซึ่งคำที่ตัดออกมาจะมีการจัดแบ่งประเภทออกเป็น 5 ประเภทดังนี้คือ

- Word: คือตัวอักษรที่เรียงต่อเนื่องกันเป็นชุด
- Number: คือตัวเลขที่เรียงต่อเนื่องกันเป็นชุด
- Symbol: สัญลักษณ์ต่างๆ เช่น $, ^, +, =, เป็นต้น
- Punctuation: เครื่องหมายวรรคตอน เครื่องหมายเริ่มคำ หรือจบคำ
- SpaceTokens: ช่องว่างหรืออักขระอื่น ๆ ที่นอกเหนือการควบคุม

4.3. ANNIE Gazetteer: Plaintext ที่ประกอบไปด้วยรายการของชื่อหรือคำต่าง ๆ ที่สามารถนำมาใช้ร่วมกันในหลาย ๆ โดเมน ซึ่ง ANNIE ได้รวบรวมรายการต่าง ๆ ไว้มากมาย เช่น รายการชื่อคน รายการชื่อเมือง รายการชื่อองค์กร รายการชื่อเดือน รายการชื่อวันในสัปดาห์

4.4. ANNIE Sentence Splitter: สร้าง Annotations ในรูปแบบประโยค โดยใช้จุดจบประโยคเป็นตัวแบ่งประโยค

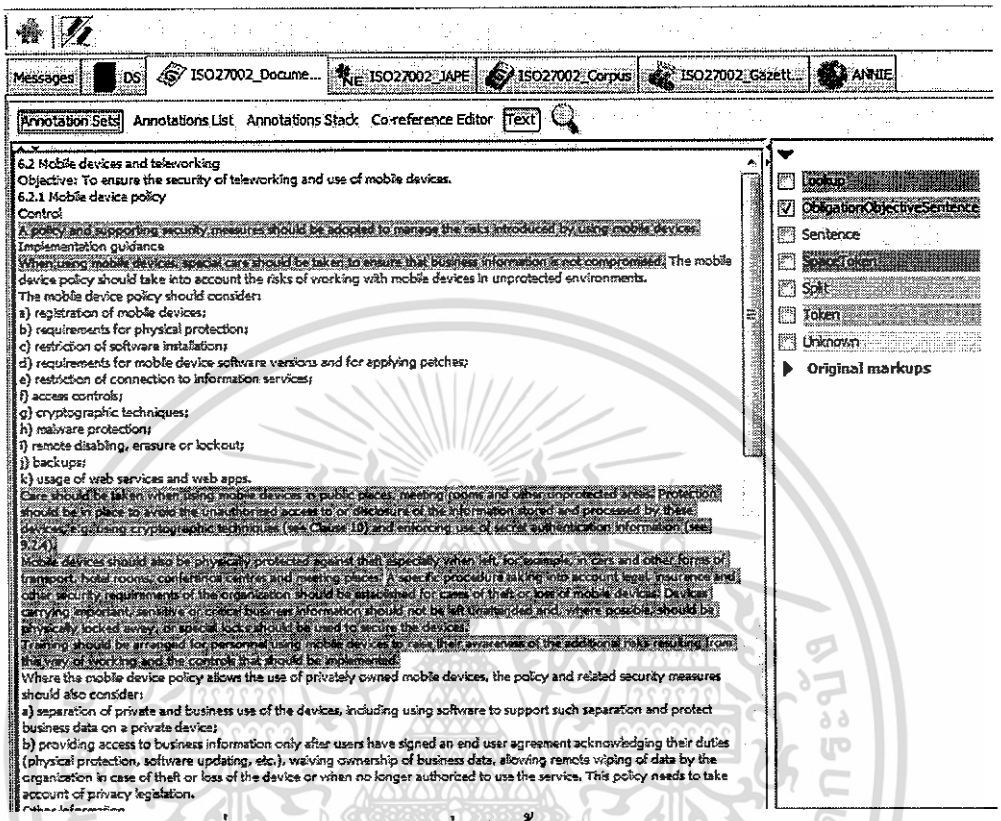
4.5. ANNIE POS Tagger: แบ่งกลุ่มให้กับ Token ที่ได้แบ่งคำออกมา เช่น

- CC – กลุ่มของคำเชื่อม (Coordinating Conjunction) เช่นคำว่า ‘and’, ‘but’, ‘nor’, ‘or’, ‘yet’, ‘plus’, ‘minus’, ‘less’
- CD – กลุ่มของจำนวนนับ (Cardinal Number)
- NN – กลุ่มของคำนาม (Noun - Singular or Mass)
- อื่น ๆ

4.6. ANNIE NE Transducer: สร้าง Annotations อื่น ๆ ที่นอกเหนือจาก Annotations ที่ได้จากหัวข้อก่อนหน้านี้ โดยการสร้างจาก JAPE Rules

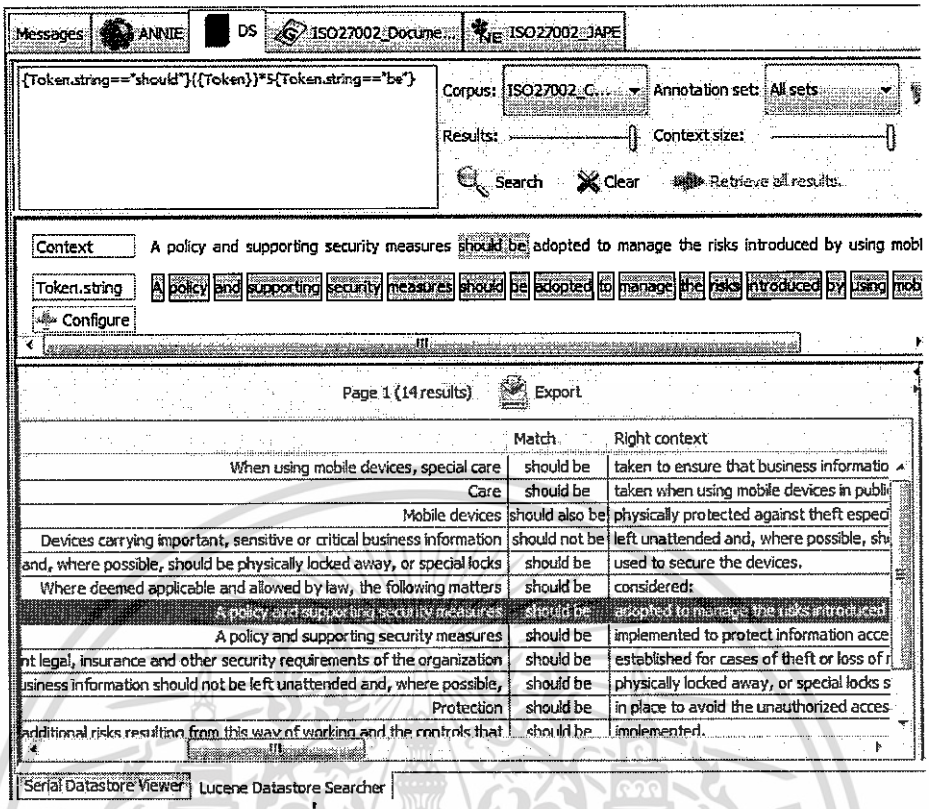
4.7. ANNIE OrthoMatcher: ทำการจับคู่คำที่มีความหมายเดียวกัน แต่อาจเขียนต่างกัน เช่น do not = don’t เป็นต้น

5. หลังจากที่ Run ANNIE ที่ได้รับการปรับแต่งแล้ว ประโยคที่มีข้อความควบคุมจะถูกทำหมายเหตุ (Annotate) เป็น “ObligationObjectiveSentences” ดังรูปที่ 4.11



รูปที่ 4.11 Annotations ที่สร้างขึ้นจาก Customized ANNIE

6. จากรูปที่ 4.11 ประโยคที่มีข้อความควบคุมได้ถูกสกัดออกมาจากเอกสารทั้งหมด แต่ยังคงอยู่ในรูปข้อความ เพื่อสกัดข้อความให้แตกย่อยกว่านั้น เราใช้ ANNIC (Annotations in Context) ซึ่งเป็นเครื่องมือ Plug-in ใช้ร่วมกับ GATE ช่วยในการค้นหา Annotations ซึ่ง ANNIC สามารถแบ่งข้อความจากขั้นตอนก่อนหน้านี้ออกเป็น “left context”, “match” และ “right context” ซึ่งในตัวอย่างนี้เป็น ประโยคที่สกัดออกมาเป็นแบบ Obligation Objects ดังนั้น Left Context ก็คือ Thing to be Controlled หรือสิ่งที่จะต้องถูกควบคุม ส่วน Right Context ก็คือ How to Control หรือวิธีการควบคุม จากตัวอย่างนี้จะเห็นได้ว่า ANNIC สามารถสกัด Thing to be Controlled และ How to Control ออกมาจากประโยคที่สกัดออกมาในขั้นตอนก่อนหน้านี้ ดังรูปที่ 4.12 ซึ่งผลจาก ANNIC สามารถ Export ออกไปเพื่อใช้ในฐานข้อมูลที่เหมาะสมสำหรับการเขียนโปรแกรมในขั้นถัด ๆ ไป ดังรูปที่ 4.13



รูปที่ 4.12 ผลการค้นหาด้วย ANNIC

Annic Results and Statistics

Parameters

- Corpus: ISO27002_Corpus
- Annotation set: All sets
- Query Issued: {Token.string=="should"}({Token})*5{Token.string=="be"}
- Context Window: 50

Results

Left context	Match	Right context	Features	Query	
When using mobile devices, special care	should be	taken to ensure that business information is not compromised.	Token.string=should, be	{Token.string=="should"} {Token.string=="be"}	ISO27002_Docur
Care	should be	taken when using mobile devices in public places, meeting rooms and other unprotected areas.	Token.string=should, be	{Token.string=="should"} {Token.string=="be"}	ISO27002_Docur

รูปที่ 4.13 การเอ็กซ์พอร์ต ANNIC

ในบทถัดไปจะเป็นการประเมินผลการทดลองและให้ข้อเสนอแนะเพื่อการนำไปประยุกต์ใช้งานจริง

บทที่ 5
การประเมินผลการวิจัย

ในบทที่ผ่านมา ผู้วิจัยได้ทำการรวบรวมองค์ความรู้ที่เกี่ยวข้อง ออกแบบ และนำเสนอกระบวนการในการพัฒนาระบบคอมพิวเตอร์เพื่อช่วยในการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง โดยมีจุดมุ่งหมายที่จะให้ระบบคอมพิวเตอร์เข้ามาช่วยลดเวลาและภาระงานที่ปัจจุบันปฏิบัติการด้วยคน โดยเลือกกรณีศึกษาจาก Non-Logged Operations ซึ่งเป็นกระบวนการทำงานที่ปรกติแล้วไม่มีการบันทึกข้อมูลลงในระบบคอมพิวเตอร์ในรูปแบบที่สามารถประมวลผลได้ โดยนำเทคโนโลยีที่สามารถประมวลผลกับข้อมูลที่เป็นรูปแบบของภาษาธรรมชาติ (Natural Language Processing) มาใช้เป็นเครื่องมือ ซึ่งเครื่องมือสำคัญหลัก ๆ คือออนโทโลยี (Ontology) และการสกัดข้อความจากสารสนเทศ (Information Extraction) ในบทนี้จะเป็นการประเมินจากการทดลองในบทที่ผ่านมา

5.1 การประเมินผลการวิจัยในส่วนของการสกัดประโยคที่มีความสำคัญออกจากเอกสารทางกฎหมายต่าง ๆ

ในส่วนนี้จะเป็นการประเมินผลการวิจัยจากการทดลองสกัดประโยคที่มีความสำคัญออกจากเอกสารทางกฎหมายต่าง ๆ ตามที่ได้อธิบายไว้ในบทที่ 4 ซึ่งในงานวิจัยนี้ใช้ตัวอย่างจากมาตรฐาน ISO/IEC 27002:2013 การประเมินผลความถูกต้องในการสกัดประโยคนั้นคิดเปรียบเทียบจากการสกัดประโยคโดยคน โดยตั้งสมมุติฐานว่าคนสามารถสกัดข้อความได้ถูกต้อง 100% จากมาตรฐาน ISO/IEC 27002:2013 ซึ่งมีทั้งหมด 114 Controls ตามโครงสร้างของเอกสารนี้ ที่ระบุว่า "This standard contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls"

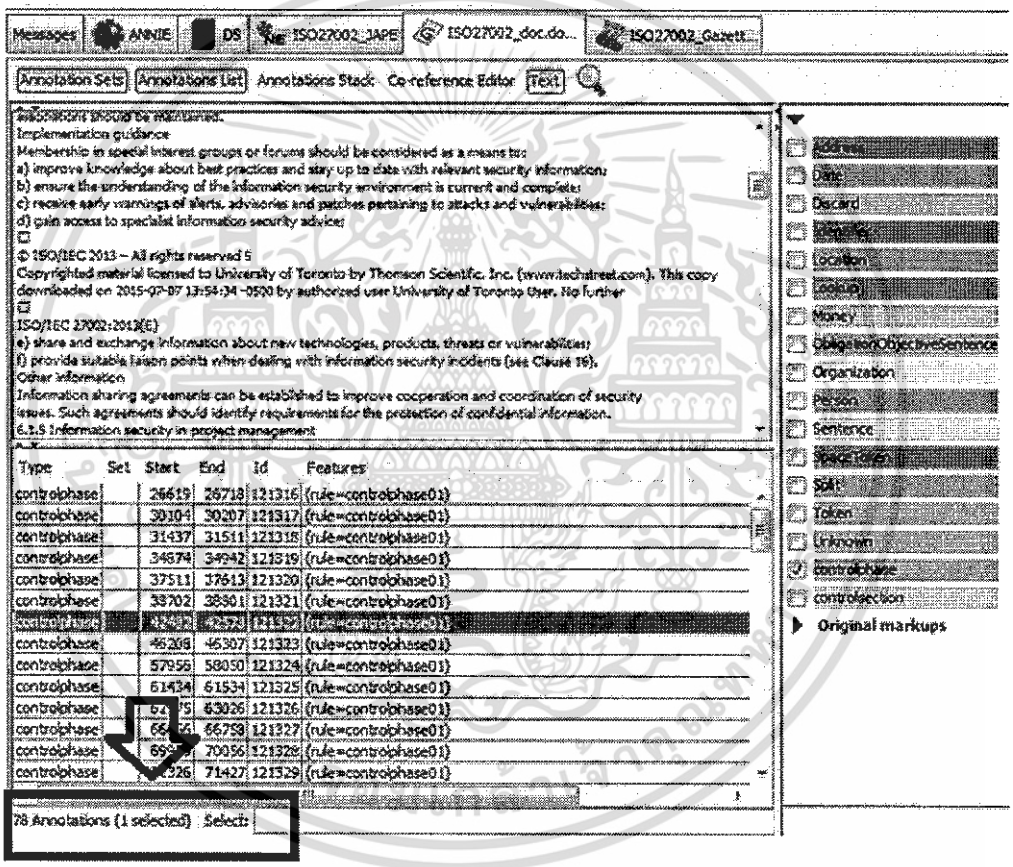
ในครั้งแรกของการประมวลผล เราทดลองใช้ JAPE Grammar ดังนี้

```
Phase: controlphase
Input: Token Lookup Sentence
Options: control = appelt

Rule: controlphase01
Priority: 5
( {Token.string == "Control"})
( {Sentence contains {Lookup.majorType ==
"obligation_objective"} } ):controlphase
-->
:controlphase.controlphase = {rule = "controlphase01"}
```

ร่วมกับ Gazetteer List ดังนี้

must also be must be shall be should also be

ซึ่งหลังจากประมวลผล โปรแกรมสามารถดึงประโยคที่เป็น Control มาได้เพียง 78 Controls ดังรูปที่ 5.1 ซึ่งถือเป็นความถูกต้องเพียง 68%



รูปที่ 5.1 ผลการประมวลผลก่อนทำการแก้ไขเพื่อเพิ่มความถูกต้องครั้งที่ 1

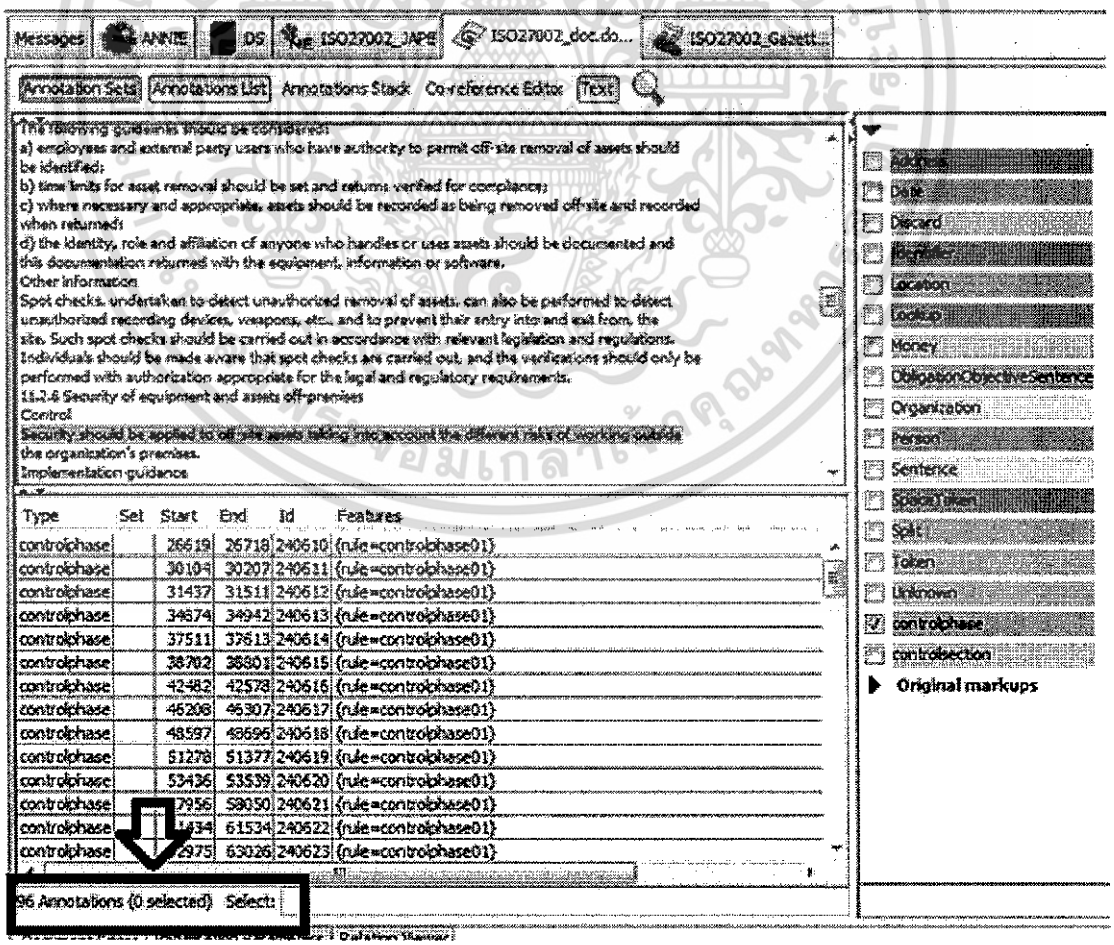
ผู้วิจัยจึงทำการปรับปรุง Gazetteer List เพิ่มขึ้นดังนี้

must also be must be shall be should also be should be	และ	may may also must must also shall should should also

โดยใช้ JAPE Grammar ดังนี้

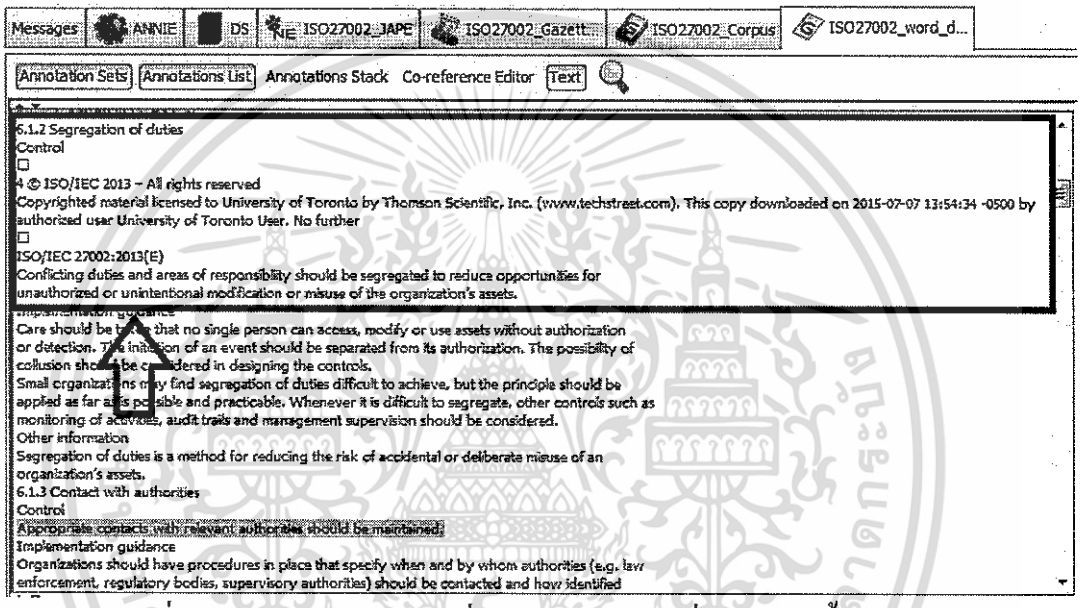
```
Phase: controlphase
Input: Token Lookup Sentence
Options: control = appelt

Rule: controlphase01
Priority: 5
( {Token.string == "Control"})
( {Sentence contains {Lookup.majorType ==
"obligation_objective"} }|
 {Sentence contains {Lookup.majorType ==
"obligation_subjective"} }
):controlphase
-->
:controlphase.controlphase = {rule = "controlphase01"}
```

ซึ่งหลังจากประมวลผลอีกรอบ โปรแกรมสามารถดึงประโยคที่เป็น Control เพิ่มมาได้เป็น 96 Controls ดังรูปที่ 5.2 ซึ่งถือเป็นความถูกต้อง 84%



รูปที่ 5.2 ผลการประมวลผลก่อนทำการแก้ไขเพื่อเพิ่มความถูกต้องครั้งที่ 2

เมื่อได้ทำการตรวจสอบอีกครั้งพบว่า JAPE Grammar ยังมีจุดอ่อนที่การเจาะจงรูปแบบของประโยค เนื่องจากประโยคบางประโยคถูกคั่นด้วยรูปแบบ (Format) ของเอกสารต่าง ๆ เช่น การเปลี่ยนหน้า การเริ่มต้นหน้าใหม่ด้วยข้อความที่ไม่เกี่ยวกับ Control ทำให้บาง Control ไม่ตรงตามเงื่อนไขของ JAPE Grammar จึงไม่ถูกสกัดออกมา ตัวอย่างเช่นกรณีของรูปที่ 5.3 ประโยค Control ใน Section ที่ 6.1.2 ไม่ถูกสกัดออกมาเนื่องจากมีการขึ้นหน้าใหม่และมีคำอื่นที่ไม่เกี่ยวข้องมาคั่นระหว่างคำว่า Control ซึ่งคำสำคัญ (Keyword)ในการสกัดข้อความกับประโยคที่เป็น Control ซึ่งเป็นเงื่อนไขของ JAPE Grammar

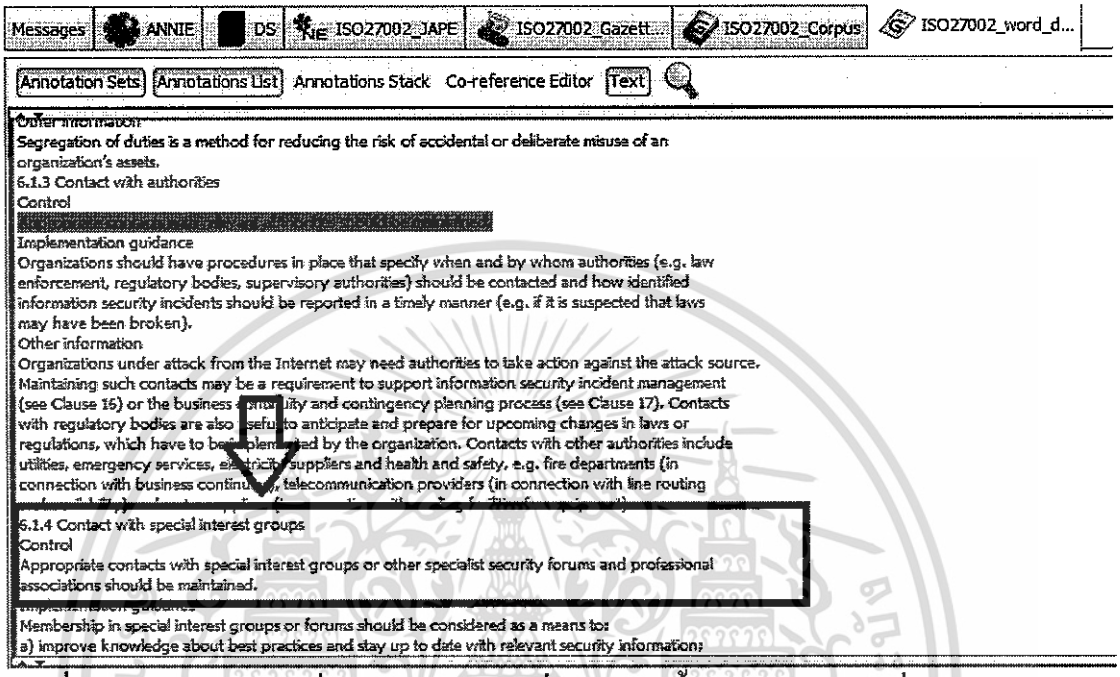


รูปที่ 5.3 ตัวอย่างของประโยคที่ไม่ถูกสกัดออกมาเนื่องจากการขึ้นหน้าใหม่

อีกกรณีหนึ่งที่เป็นสาเหตุของความผิดพลาดคือเอกสารนำเข้ามีความไม่ถูกต้องในเรื่องของการตัดคำ เช่น การเว้นวรรค การขึ้นบรรทัดใหม่ เป็นต้น เนื่องจาก JAPE Grammar ในกรณีตัวอย่างดึงข้อมูลจากประโยค (Sentence) หากเอกสารนำเข้ามีการตัดคำขึ้นบรรทัดใหม่โดยที่ยังไม่จบประโยคอาจเป็นสาเหตุที่ประโยคไม่ถูกสกัดออกมาตามเงื่อนไข ยกตัวอย่างเช่น

> 6.1.4 Contact with special interest groups
> Control
> Appropriate contacts with special interest groups or other specialist security forums and professional
> associations should be maintained.

เอกสารนำเข้ามีการตัดคำขึ้นบรรทัดใหม่โดยที่ยังไม่จบประโยค ทำให้ประโยคที่เป็นคำสำคัญ (Keyword) ของการสกัดคำไม่ตรงไปตามเงื่อนไข ประโยคดังกล่าวจึงไม่ถูกสกัดออกมาตามรูปที่ 5.4

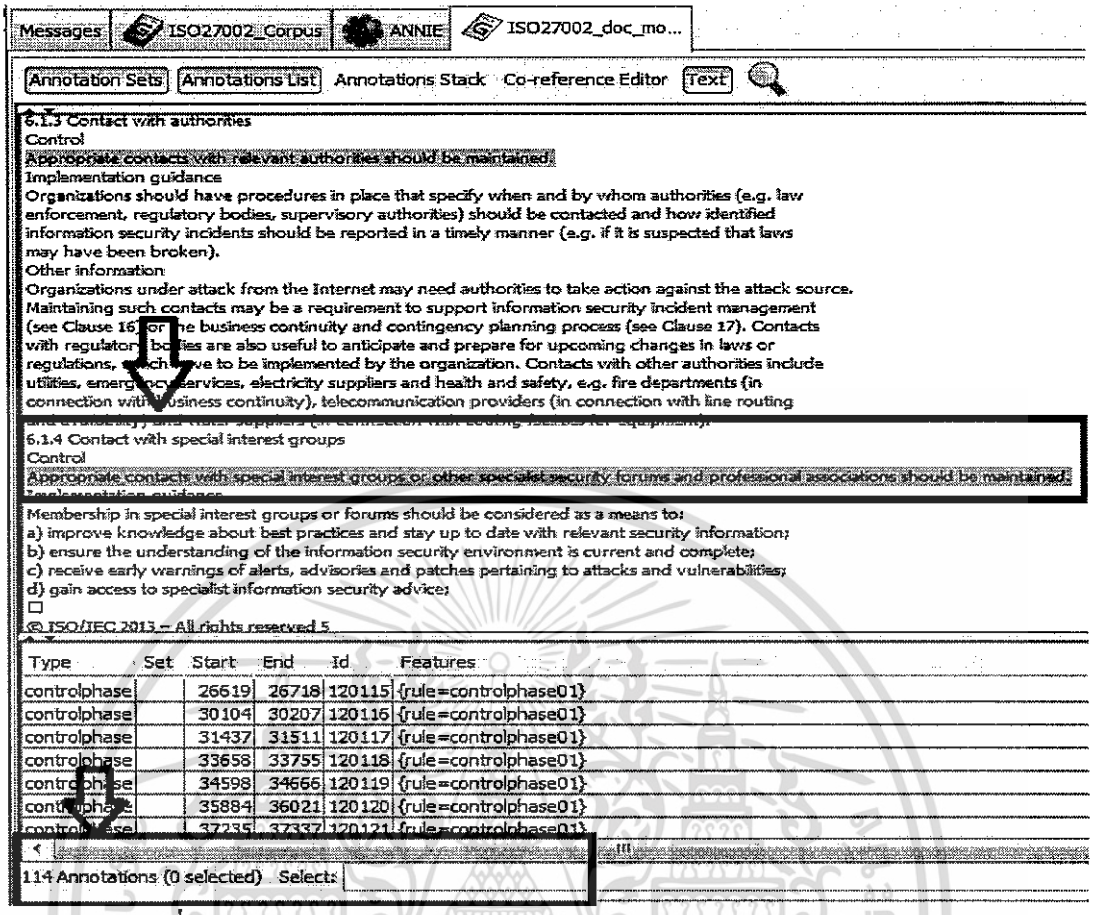


รูปที่ 5.4 ตัวอย่างประโยคที่ไม่ถูกสกัดออกมาเนื่องจากการขึ้นบรรทัดใหม่โดยที่ยังไม่จบประโยค

เมื่อทำการทดลองใหม่ โดยการแก้ไขเอกสารนำเข้าให้มีการตัดคำขึ้นประโยคใหม่อย่างถูกต้อง ดังนี้

> 6.1.4 Contact with special interest groups
> Control
> Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

เมื่อทดลองประมวลผลอีกรอบโดยไม่เปลี่ยนแปลงเงื่อนไขอื่น ๆ นอกจากเอกสารนำเข้าที่ได้ทำการปรับปรุง พบว่าประโยคที่ถูกแก้ไขในเอกสารนำเข้าได้ถูกสกัดออกมาและทำให้จำนวนประโยคทั้งหมดเพิ่มเป็น 114 ประโยค ซึ่งถือเป็นความถูกต้อง 100% ดังรูปที่ 5.5



รูปที่ 5.5 ผลการประมวลผลหลังจากทำการแก้ไขประโยคในเอกสารนำเข้า

จากข้อมูลดังกล่าวข้างต้นจึงสรุปได้ว่า การสกัดข้อความจะมีความถูกต้องมากน้อยเพียงใดนั้นขึ้นอยู่กับความสามารถในการระบุคำที่เป็นกุญแจสำคัญในการสกัดข้อความมาพัฒนาลงใน Gazeteer List และความสามารถในการพัฒนา JAPE Grammar เพื่อสกัดข้อความที่สัมพันธ์กันกับ Gazetteer List และรูปแบบเอกสารของเอกสารนำเข้าก็ถือเป็นเงื่อนไขหนึ่งของความถูกต้องในการสกัดประโยคที่มีความสำคัญออกมา เมื่อทุกอย่างมีความถูกต้อง ความถูกต้องจะเข้าใกล้ 100% มากขึ้น

5.2 การประเมินผลการวิจัยโดยรวมจากการพัฒนาระบบการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติ

เนื่องจาก Non-Logged Operations คือการปฏิบัติงานที่ไม่มีการบันทึกผลการปฏิบัติงานในรูปแบบที่คอมพิวเตอร์สามารถเข้าใจได้ ดังนั้นการตรวจสอบการปฏิบัติงานจึงยังคงต้องใช้กิจกรรมที่ผู้ปฏิบัติงานต้องตอบคำถามเพื่อให้เกิดการประเมิน ในการวิจัยนี้ เราตั้งสมมุติฐานว่าผู้ตอบคำถามหรือเจ้าของส่วนงานที่ถูกตรวจสอบไม่มีความรู้ทางด้านความมั่นคงปลอดภัยหรือนโยบายที่เกี่ยวข้อง ดังนั้นในการปฏิบัติงานจริง พวกเขาจะไม่สามารถประเมินได้ว่าการปฏิบัติงานที่เป็นอยู่

สอดคล้องกับนโยบายที่เกี่ยวข้องหรือไม่ จึงหลีกเลี่ยงไม่ได้ที่ต้องใช้บริการจากผู้เชี่ยวชาญหรือผู้ตรวจสอบ ซึ่งผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยสารสนเทศหรือผู้ตรวจสอบนั้นมีค่อนข้างจำกัดและค่าตัวค่อนข้างสูง ถ้ามีการพัฒนาและใช้ระบบที่นำเสนอจากงานวิจัยนี้ เจ้าของส่วนงานจะสามารถประเมินผลการปฏิบัติการของตนเองได้โดยไม่ต้องอาศัยผู้เชี่ยวชาญเหล่านั้น ทำให้สามารถลดกระบวนการ เวลา และค่าใช้จ่ายได้ค่อนข้างสูง นอกจากนั้นยังสามารถเพิ่มความถูกต้องของการลงความเห็นจากการประเมินได้อีกด้วย เพราะระบบนี้สามารถหลีกเลี่ยงความผิดพลาดจากการลงความเห็นที่เอนเอียง (Biased Judgment) ค่าใช้จ่ายที่สามารถลดได้จากระบบที่นำเสนอนี้สามารถประมาณการได้จากสมการต่อไปนี้

Manual Labor Time = $\sum_{i=1}^{n}(A_i + T_i)$

Proposed Solution Labor Time = $\sum_{i=1}^{n}(T_i)$

Reduced Labor Time = $\sum_{i=1}^{n}(A_i)$

โดยที่

n = Number of Questions (จำนวนคำถาม)

A_i = Assessor Labor Time of Question i (เวลาที่ใช้ในส่วนของผู้ประเมิน)

T_i = Operation Owner Labor Time of Question i (เวลาที่ใช้ในการหาคำตอบและตอบคำถามโดยเจ้าของส่วนงาน)

กล่าวโดยสรุปได้คือ การประยุกต์ใช้ระบบที่นำเสนอจะสามารถลดเวลาและค่าใช้จ่ายที่เกิดขึ้นจากผู้ตรวจสอบหรือผู้ประเมิน ซึ่งทั้งนี้จะสามารถลดค่าใช้จ่ายได้มากเพียงใด ขึ้นอยู่กับจำนวนของคำถามและค่าตัวของผู้ประเมิน

บทที่ 6
บทสรุปและข้อเสนอแนะ

6.1 บทสรุป

ในกระบวนการของบริหารจัดการการปฏิบัติตามกฎเกณฑ์ความมั่นคง (Security Compliance Management) นั้น กิจกรรมการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคง (Security Compliance Checking) คือกิจกรรมที่ต้องปฏิบัติแบบต่อเนื่อง ซึ่งในปัจจุบันยังต้องพึ่งพาผู้เชี่ยวชาญด้าน IT Security เป็นผู้ตรวจสอบ แต่เนื่องจากผู้เชี่ยวชาญด้าน IT Security มีจำนวนน้อยและค่าตัวแพง กิจกรรมนี้จึงกลายเป็นกิจกรรมที่มีค่าใช้จ่ายสูง หลายองค์กรจึงมีความต้องการในการลดการพึ่งพาผู้เชี่ยวชาญ ซึ่งในกรณีนี้ การลดการพึ่งพาผู้เชี่ยวชาญคือการเพิ่มความสามารถในการตรวจสอบตัวเอง (Self Assessment) ซึ่งทำได้โดยการพัฒนา Automated Security Compliance Checking นั่นเอง

เนื่องจากกฎเกณฑ์ความมั่นคงต่าง ๆ นั้นถูกเขียนขึ้นด้วยภาษาธรรมชาติซึ่งมีความกำกวมสูง จำเป็นต้องใช้การตีความด้วยบุคคลที่มีความรู้ความชำนาญเฉพาะด้าน จึงกลายเป็นอุปสรรคสำคัญในการพัฒนา Automated Security Compliance Checking อุปสรรคที่สำคัญอีกประการหนึ่งคือการที่ข้อมูลสำคัญที่ใช้สำหรับการตรวจสอบนั้นไม่มีการบันทึกลงในระบบคอมพิวเตอร์ในรูปแบบที่สามารถประมวลผลได้ (Non-Logged Operations) หรือไม่มีความพร้อมของข้อมูลนั่นเอง

งานวิจัยนี้ได้นำเสนอสถาปัตยกรรมสำหรับการพัฒนาระบบการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงโดยอัตโนมัติโดยนำเทคโนโลยีที่สามารถประมวลผลกับข้อมูลที่เป็นรูปแบบของภาษาธรรมชาติ (Natural Language Processing) มาใช้เป็นเครื่องมือสำคัญในการเปลี่ยนกฎเกณฑ์ความมั่นคงต่าง ๆ ให้มาอยู่ในลักษณะของ Machine-Readable และใช้หลักการของการถามตอบซึ่งเป็นกระบวนการของการตรวจสอบโดยทั่วไปเพื่อเปลี่ยนข้อมูลที่เป็นแบบ Non-Logged Operations ให้มาเป็นข้อมูลนำเข้าในรูปแบบของ Machine-Readable เช่นเดียวกัน

การเปลี่ยนการเปลี่ยนกฎเกณฑ์ความมั่นคงต่าง ๆ ที่อยู่ในรูปภาษาธรรมชาติให้มาอยู่ในลักษณะของ Machine-Readable ทำได้โดยการสร้างฐานข้อมูลในรูปแบบของออนโทโลยีโดยนำองค์ความรู้ของกฎเกณฑ์ต่าง ๆ มาสร้างความสัมพันธ์เชื่อมโยงกัน สร้างเงื่อนไขต่าง ๆ ในรูปแบบของ Database และใช้ GATE เป็นเครื่องมือในการสกัดกฎเกณฑ์ต่าง ๆ แบบอัตโนมัติลงในฐานข้อมูลออนโนโลยีที่พัฒนาไว้แล้ว ซึ่งวิธีการที่นำเสนอสามารถสกัดข้อความได้ถูกต้องสูงสุดถึง 100%

การเปลี่ยนข้อมูลที่เป็นแบบ Non-Logged Operations ให้มาเป็นข้อมูลนำเข้าในรูปแบบของ Machine-Readable ทำได้โดยการนำ Checklist ที่เป็นคำถามที่ผู้ตรวจสอบส่วนใหญ่ใช้ มาพัฒนาร่วมกับออนโทโลยีข้างต้นเพื่อนำไปสู่การรับข้อมูลนำเข้าสำหรับการประเมินผลการตรวจสอบตาม

กฎเกณฑ์ความมั่นคงแบบอัตโนมัติ วิธีการนี้เพิ่มความสามารถของ Automated Security Compliance Checking จากวิธีการอื่น ๆ ที่นำเสนอในปัจจุบันได้มากกว่า 50% เนื่องจากข้อมูลแบบ Non-Logged Operations นั้นมีจำนวนมากกว่า 50% ของข้อมูล Opearations ทั้งหมด แต่ที่ผ่านมายังไม่มีการนำเสนอแนวทางแก้ไขสำหรับทำงานร่วมกับ Non-Logged Operations

วิธีการที่นำเสนอในงานวิจัยฉบับนี้ช่วยให้บุคลากรที่ไม่ใช่ผู้ตรวจสอบสามารถทำการตรวจสอบการปฏิบัติตามกฎเกณฑ์ความมั่นคงได้เอง สามารถลดการพึ่งพาผู้เชี่ยวชาญด้าน IT Security ซึ่งจะทำให้รายจ่ายสำหรับการบริหารจัดการการปฏิบัติตามกฎเกณฑ์ความมั่นคงลดลงเป็นอย่างมาก

6.2 ข้อเสนอแนะ

ถึงแม้ว่ากรณีตัวอย่างที่นำมาปรับใช้ในงานวิจัยนี้จะเป็นเพียง Non-Logged Operations แต่เนื่องจากกิจกรรมการตรวจสอบโดยส่วนใหญ่ของผู้ตรวจสอบจะใช้หลักการถามตอบในการประเมิน ดังนั้น งานวิจัยนี้จึงไม่ได้มีประโยชน์แต่เพียง Non-Logged Operations เท่านั้นแต่ยังสามารถนำไปปรับใช้กับการปฏิบัติงานที่เป็น Logged Operations อีกด้วย

การพัฒนาออนโทโลยี ถือเป็นขั้นตอนสำคัญที่ต้องมีการพัฒนาโดยผู้เชี่ยวชาญเฉพาะทางในด้านนั้น ๆ และต้องมีการตรวจสอบความสมเหตุสมผล (Validation) ว่าออนโทโลยีที่พัฒนามาแล้วนั้นสามารถใช้งานได้จริงโดยผู้เชี่ยวชาญอีกเช่นกัน ออนโทโลยีในโดเมนเดียวกันอาจมีการนำเสนอได้หลายรูปแบบ ซึ่งไม่สามารถมีคำตอบที่ชัดเจนว่ารูปแบบใดคือออนโทโลยีที่ถูกต้อง เพราะการพัฒนาออนโทโลยีของแต่ละรูปแบบอาจมีสมมุติฐานที่ต่างกันไป แต่รูปแบบที่ถือว่าประสบความสำเร็จคือรูปแบบที่สามารถนำกลับมาใช้ได้ใหม่ในหลาย ๆ สถานการณ์ ซึ่งนั่นหมายความว่าออนโทโลยีถูกพัฒนาโดยผู้ที่มีความเชี่ยวชาญในโดเมนนั้นอย่างครอบคลุมนั่นเอง

การสกัดข้อความสำคัญในการพัฒนาระบบเพื่อใช้งานจริงนั้นต้องเพิ่มขั้นตอนที่ครอบคลุมการสกัดข้อความที่กำกวมต่าง ๆ ออกจากเอกสารก่อนนำข้อมูลไปใช้งานจริงในฐานข้อมูล เพราะในรูปแบบข้อความในภาษาธรรมชาตินิได้มีข้อจำกัดของการเขียนที่ถูกต้องเพียงรูปแบบเดียว เช่น ในบางประโยค Subject มาก่อน Object แต่บางประโยค Object อาจมาก่อน Subject ขึ้นอยู่กับว่าประโยคนั้นเป็น Tense แบบใด หรือแม้แต่คำที่มีความหมายเดียวกันอาจเขียนได้ต่างกัน เช่น do not หรือ don't ก็คือคำที่มีความหมายเดียวกัน คำว่า May อาจเป็นได้ทั้งชื่อคน (May Jones) ชื่อเดือน (May 2010) หรือความหมายอื่น ๆ เช่น May I come in? ซึ่งทั้งนี้ทั้งนั้น การจะแยกแยะคำเหล่านี้ได้ต้องใช้องค์ความรู้ด้านภาษามาพัฒนาเป็นแอปพลิเคชัน ด้านภาษาเพื่อสกัดคำเหล่านี้ ซึ่งใน GATE ก็มีเครื่องมือค่อนข้างครอบคลุมการพัฒนาแอปพลิเคชัน ที่แก้ไขความกำกวมเหล่านี้ได้

เอกสารอ้างอิง

[1] Bace J., Rozwell C., Feiman J. and Kiwin B. "Understanding the Costs of Compliance." **Gartner Report G00138098**, 2006.

[2] Tashi I. "Regulatory Compliance and Information Security." **In Proceedings of 2009 International Conference on Availability, Reliability and Security, Fukuoka, Japan,** 2009. pp. 670-674.

[3] Venkat N. and Jagadeesh N. "Corporate Compliance and Its Implications to IT Professionals." **In Proceedings of 6th International Conference on Information Technology: New Generations, Las Vegas, NV,** April 27-29, 2009. pp. 725-729.

[4] Sackmann S., Kähmer M., Gilliot M. and Lowis L. "A Classification Model for Automating Compliance." **In Proceedings of Tenth IEEE Conference on E-Commerce Technology (CEC08). Washington, USA**, 2008. p. 79-86.

[5] Sackmann S. and Kähmer M. "ExPDT: A Policy-Based Approach for Automating Compliance." **Wirtschaftsinformatik**, Vol. 50(8), October 2008. pp. 366–374.

[6] Agrawal R., Johnson C., Kiernan J. and Leymann F. "Taming Compliance with Sarbanes-Oxley Internal Controls Using Database Technology." **In Proceedings of the 22nd International Conference on Data Engineering (ICDE'06), IEEE Computer Society, Washington, DC**, 2006. pp. 92-101.

[7] Accorsi R. "Automated Privacy Audits to Complement the Notion of Control for Identity Management." **In Proceedings of the IFIP Conference on Policies and Research in Identity Management, Springer, Berlin,** 2008. pp. 39–48.

[8] Gang C. "Security for Web Service Based On Regulatory Compliance." **In Proceedings of the 2009 International Symposium on Computer Network and Multimedia Technology,** 2009. pp. 1-4.

.[9] Wali A., Chun S. A. and Geller J. "A Bootstrapping Approach for Developing a Cyber Security Ontology Using Textbook Index Terms." **In Proceedings of the 2013 International Conference on Availability, Reliability and Security, Regensburg, Germany,** 2013. pp. 569–576.

[10] Elahi G., Yu E. and Zannone N. "A Modeling Ontology for Integrating Vulnerabilities into Security Requirements Conceptual Foundations." **In Proceedings of the 28th International Conference on Conceptual Modeling, Brazil,** 2009. pp. 99-114.

[11] Simmons C. B., Shiva S. G. and Simmons L. L. "A Qualitative Analysis of an Ontology Based Issue Resolution System for Cyber Attack Management." **In Proceedings of the International Conference on Cyber Technology in Automation Control and Intelligent Systems (IEEE Cyber), Hong Kong, China,** 2014. pp. 323-329.

[12] Pereira T. and Santos H. "A Security Audit Framework to Manage Information System Security." **In Proceedings of the 6th International Conference, ICGS3 2010, Braga, Portugal,** 2010. pp. 9-18.

[13] Blackwell C. "A Security Ontology for Incident Analysis." **In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW'10, Oak Ridge, Tennessee,** 2010. pp. 46-49.

[14] Hung S. and Shing-Min Liu D. "A User-Oriented Ontology-Based Approach for Network Intrusion Detection." **Computer Standards & Interfaces,** vol.30, 2008. pp. 78–88.

[15] Parkin S. E. and Van Moorsel A. "An Information Security Ontology Incorporating Human-Behavioral Implications." **In Proceedings of the 2nd International Conference on Security of Information and Networks, Famagusta, Cyprus,** 2009. pp. 46-55.

[16] Takahashi T., Kadobayashi Y, and Fujiwara H. "Ontological Approach Toward Cyber Security in Cloud Computing Categories and Subject Descriptors." **In Proceedings of the 3rd International Conference on Security of Information and Networks, Taganrog, Russian Federation,** 2010. pp. 100–109.

[17] Razzaq A., Anwar Z., Ahmad H. F., Latif K. and Munir F. "Ontology for Attack Detection: An Intelligent Approach to Web Application Security." **Computers & Security,** vol.45, 2014. pp. 124–146.

[18] Gyrard A., Bonnet C. and Boudaoud K. "The STAC (Security Toolbox: Attacks & Countermeasures) Ontology." **In Proceedings of the 22nd International Conference on World Wide Web Companion, Rio de Janeiro, Brazil,** 2013. pp. 165–166.

[19] Cunningham H. "Information Extraction, Automatic." **Encyclopedia of Language & Linguistics, Second Edition,** vol. 5, 2006. pp. 665-677.

[20] Breaux T. D., Vail M. W. and Anton A. I. "Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations." **In Proceedings of 14th IEEE International Requirements Engineering Conference (RE'06), Minneapolis: IEEE Computer Society**, 2006. pp. 49-58.

[21] Maynard D., Bontcheva K., Saggion H., Cunningham H. and Hamza O. "Using a Text Engineering Framework to Build an Extendable and Portable IE-Based Summarisation System." **In Proceedings of the ACL Workshop on Text Summarisation,** 2002. pp. 19-26.

[22] Wyner A. and Peters W. "Towards Annotating and Extracting Textual Legal Case Factors." **In Proceedings of the 3rd Workshop on Semantic Processing of Legal Texts (SPLeT 2010)**, 2010. pp. 36–45.

[23] Sapkota K., Aldea A., Duce D., Younas M. and Banares-Alcantara R. "Towards Semantic Methodologies for Automatic Regulatory Compliance Support." **In Proceedings of the 4th Workshop on Workshop for Ph.D. Students in Information & Knowledge Management,** 2011. pp. 83-86.

[24] Ku C., Iriberri A. and Leroy G. "Natural Language Processing and e-Government: Crime Information Extraction from Heterogeneous Data Sources." **The Proceedings of the 9th Annual International Digital Government Research Conference,** 2008. pp. 162-170.

[25] Kenneth C. L. and Jane P. L. "Infrastructure Components." **Management Information Systems: Managing the Digital Firm,** Edition 13, 2014. pp. 203-209.

[26] Brusa G., Caliusco M. L. and Chiotti O. "Towards Ontological Engineering: a Process for Building a Domain Ontology from Scratch in Public Administration." **Expert Systems: The Journal of Knowledge Engineering,** Vol. 25, 2008, pp. 484–503.

[27] Noy N. F. and McGuinness D. L. "Ontology Development 101: A Guide to Creating Your First Ontology." **Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880**, 2001.

[28] Antón A.I. "Goal-Based Requirements Analysis." **In Proceedings of the International Conference on Requirements Engineering (ICRE `96), Colorado Springs, Colorado, USA**, April 1996. pp. 136-144.

[29] Kabilan V., Johannesson P., Rugaimukamu D.M. "Business Contract Obligation Monitoring through Use of Multi Tier Contract Ontology." **In Proceedings of the Workshop on**

Regulatory Ontologies and the Modelling of Complaint Regulations (WORM CoRe), Springer, 2003. pp. 690-702.

[30] Stanford Center for Biomedical Informatics Research. **"The Protégé Ontology Editor and Knowledge Acquisition System."** [Online]. Available: http://protege.stanford.edu. 2016.

ประวัติผู้เขียน

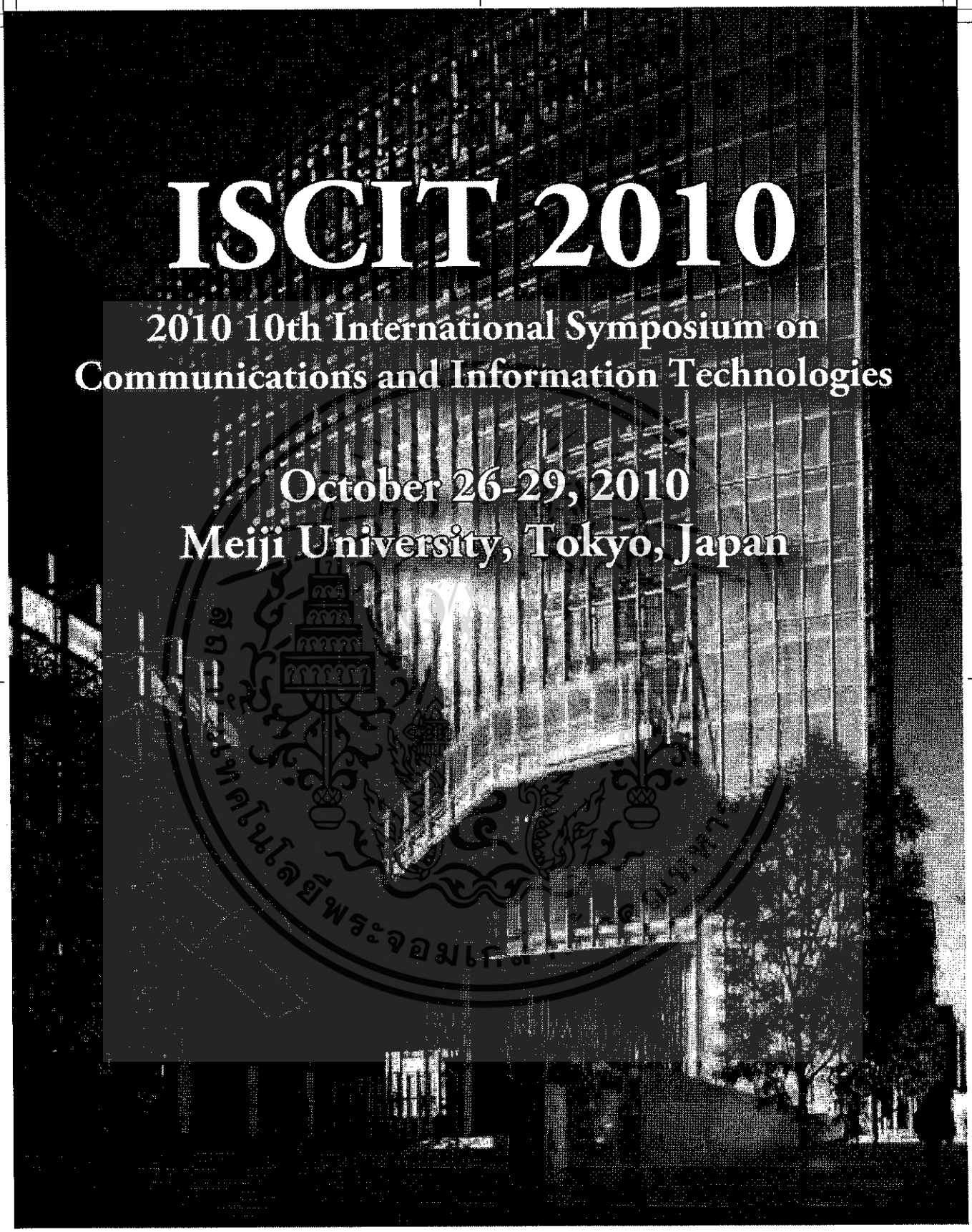
ชื่อ-นามสกุล	นางสาวนันทา จันทร์พิทักษ์
วัน เดือน ปีเกิด	8 ธันวาคม 2514 จังหวัดระยอง
ที่อยู่	72/6 หมู่ 1 ต.แกลง อ.เมือง จ.ระยอง 21160
	โทรศัพท์ : 0810016767
ประวัติการศึกษา	2535 วิทยาศาสตรบัณฑิต สาขาคณิตศาสตร์
	มหาวิทยาลัยบูรพา
	2550 วิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ
	มหาวิทยาลัยเทคโนโลยีมหานคร
ความชำนาญเฉพาะด้าน	1. การบริหารงานด้านเทคโนโลยีสารสนเทศ
	2. การตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ
	3. การออกแบบและบริหาร Data Center
ประสพการณ์การทำงาน	
2540-2556	บริษัทออโต้อัลลายแอนซ์ (ประเทศไทย) จำกัด
	ตำแหน่ง IT Manager บริหารงานด้าน enterprise system
	ตำแหน่ง Security Control Champion
	ดูแลและควบคุมด้านความมั่นคงปลอดภัยของสารสนเทศ
2551	CISA (Certified Information System Auditor)
2553	Certified ITIL

ภาคผนวก ก
ผลงานวิจัยที่ได้รับการเผยแพร่

[1] Janpitak N. and Sathitwiriyawong C. "Run-time Enforcement Model for Dynamic Separation of Duty." in **2010 International Symposium on Communications and Information Technologies (ISCIT)**, Japan, 2010. pp. 115-120.

[2] Janpitak N. and Sathitwiriyawong C. "Data Center Physical Security Ontology for Automated Evaluation." in **The 2011 International Conference on Security and Management (SAM2011)**, USA, 2011, pp. 78-84.

[3] Janpitak N. and Sathitwiriyawong C. "Automated Compliance Checking Methodology for Non-Log Operations." **Information Security Journal: A Global Perspective**, vol. 24, 2015, pp. 98-108.



ISCIT 2010

2010 10th International Symposium on Communications and Information Technologies

October 26-29, 2010
Meiji University, Tokyo, Japan

Supported by The Telecommunications Advancement Foundation / SCAT / Headquarters of International Collaboration, Meiji University

Run-time Enforcement Model for Dynamic Separation of Duty

Nanta Janpitak and Chanboon Sathitwiriyawong
Faculty of Information Technology,
King Mongkut's Institute of Technology Ladkrabang,
Bangkok 10520, Thailand
E-mail: njanpita@hotmail.com, chanboon@it.kmitl.ac.th

***Abstract*— Separation of duty (SoD) is a primary internal control in many businesses including information systems intended to prevent frauds and errors due to the conflict of interest. To enforce the separation of duty in the information systems, Role-Based Access Control (RBAC) has been proposed and been the most popular access control model in today's security management. This paper focuses on the Dynamic Separation of Duty (DSD) which is one of the four components of the ANSI RBAC standard. To maximize the utilization of human resources, one user is allowed to have multiple mutually exclusive roles but can activate only one role at a time. The DSD does not only provide more flexibility for business system but also create more vulnerability in the separation of duty compliance because of the complication in checking the conflict of interest. This paper proposes a very simple but effective model to solve the problem of the DSD by integrating the workflow sequence to the concept of mutually exclusive roles (MER) constraint. From the proposed model, the conflict of interest can be verified at run time. The system will not allow the continuity of any process if the activation of conflicting users has been found.**

Keywords—Separation of duty (SoD); Role-Based Access Control (RBAC); the Constrained RBAC; Static Separation of Duty (SSD); Dynamic Separation of Duty (DSD); Mutually Exclusive Roles (MER); Workflow

I. INTRODUCTION

Separation of duty is a primary internal control intended to reduce the risk of errors or irregularities, identify problems, and ensure that no single person can completely compromise information system resources. It ensures that a concentration of responsibilities does not occur in one person or activity that will allow accidental or deliberate errors to go undetected.

To enforce the separation of duty, the information systems should be integrated with access control mechanisms. Role-Based Access Control (RBAC) which was proposed by Ferriaiolo and Kuhn in 1992 [1] and was adopted as ANSI Standard in 2004 [2] is the most popular security access control model in today's security management. The ANSI standard for RBAC model is defined in terms of four model components: Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations, and Dynamic Separation of Duty Relations. Core RBAC is required as a minimum in any RBAC system, the basic concept is that permissions are assigned to roles and individual users obtaining such permissions by being assigned to roles. The other components are independent of each other and may be implemented separately.

This paper focuses on the implementation of Dynamic Separation of Duty (DSD). The DSD is part of the Constrained RBAC which is realized by mutually exclusive roles (MER). More detail will be explained in section II.

A Workflow as defined by Georgakopoulos et al. [3] is a computer system used to increase efficiency by concentrating on the routine aspects of work activities. Workflow typically separates work activities into well-defined tasks, roles, rules, and procedures which regulate most of the work in manufacturing and the office. Initially, processes were carried out entirely by humans who manipulated physical objects. With the introduction of information technology, processes in the work place are partially or totally automated by information systems, i.e., computer programs performing tasks and enforcing rules which were previously implemented by humans.

The rest of this paper is organized as follows. Section II explains the overview of Constrained RBAC. Section III expresses the motivation of the research by utilizing the purchase order (PO) issuing scenario. Section IV discusses some related works. Section V describes the proposed model and algorithm and also demonstrates how this model can work with PO issuing scenario. Finally in section VI summarization and conclusions of this paper will be provided.

II. OVERVIEW OF CONSTRAINED RBAC

The basic concept of RBAC is that permissions are assigned to roles and individual users obtaining such permissions by being assigned to roles. The Constrained RBAC adds separation of duty relations to enforce the conflict of interest.

One means of implementing separation of duty relations is with mutually exclusive roles (MER). MER is defined as a set of roles of which any sensitive business process comprising of at least two steps requires the cooperation of at least two different users to complete the task. The common example for MER is that in a bank, a user who is authorized for the role Teller may not be authorized for the role Auditor. That is the roles Teller and Auditor are mutually exclusive. The set of MER expresses for this case is defined as {Teller, Auditor}.

Fig. 1 illustrates the Constrained RBAC that allows for both static and dynamic separation of duty as defined within the next two subsections.

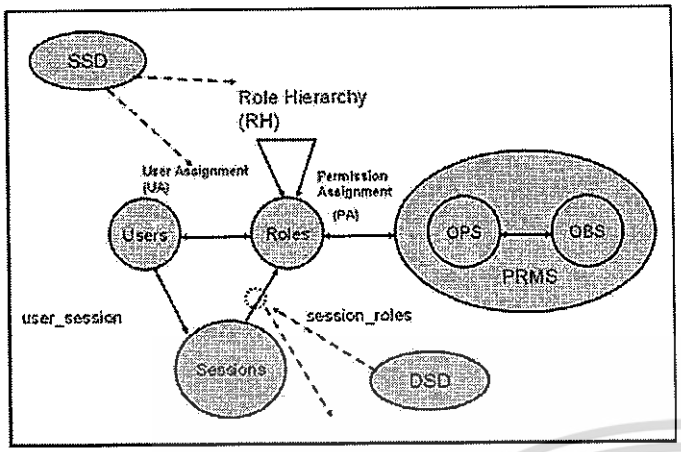


Fig. 1 Constrained RBAC

A. *Static Separation of Duty Relations (SSD)*

The definition of SSD is given in ANSI Standard as "A user is authorized as a member of a role only if that role is not mutually exclusive with any of the other roles for which the user already possesses membership".

SSD is defined as a pair (*role set*, *n*), where $n \geq 2$ and no user is assigned to n or more roles from the role set. Suppose that the mention role set is the set of mutually exclusive roles (MER) so that the SSD constraint can be illustrated by MER($\{r_1, r_2, \ldots, r_m\}$, n), where each r_i is a role, m and n are integers, $1 < n \leq m$.

B. *Dynamic Separation of Duty Relations (DSD)*

The definition of DSD is given in ANSI Standard as "A user can be authorized for multiple mutually exclusive roles and the user can exercise these roles independently but not at the same time or simultaneously".

Similar to SSD relations, DSD relations define constraints as a pair (*role set*, *n*), where $n \geq 2$, with the property that no user session may activate n or more roles from the role set. Suppose that the mention role set is the set of mutually exclusive roles (MER) so that the DSD constraint can be illustrated by MER($\{r_1, r_2, \ldots, r_m\}$, n), where each r_i is a role, m and n are integers, $1 < n \leq m$.

III. Scenario

In this paper, the motivation of the research will be expressed by using purchase order (PO) issuing scenario. A policy is defined in purchasing department as "In order to issue the POs to suppliers, the POs need to be involved by at least 3 roles in the purchasing system". Each buyer cannot create POs by themselves. The POs have to be originated by purchasing clerk with initial request information such as requestor, request items, request quantity then pass to buyer to input supplier information and item prices, etc. and then finally approved by purchasing manager. It can be supposed in this scenario that in some period there is no real purchasing clerk available in purchasing department. Each buyer has to act as purchasing clerk to originate POs for other buyers so that each buyer has to be assigned as both role "Clerk" and "Buyer". From this scenario, the DSD constraint in RBAC is the most appropriate access control system. By applying the proposed model, this scenario will demonstrate that how to protect one buyer from activating both "Clerk" and "Buyer" to perform the task for one PO.

In this scenario, there is the case of policy changing. The policy is changed to "In order to issue the POs to suppliers, the POs need to be involved by at least 3 roles in purchasing system and require at least 2 persons". From the policy changing, one person can perform 2 roles out of 3 roles. This paper will present that by applying this model, there is no need to change the system coding; the policy changing can be easily deployed by changing to DSD rule.

IV. Related Works

Since RBAC is an open-ended concept which ranges from very simple at one extreme to fairly complex and sophisticated at the other. Organizations can select to implement the RBAC level which is the most fit to their business environment. Each level has its own advantage and disadvantage. For example, the implementation of first level, Core RBAC will give the strictest and the most secure model but does not provide the flexibility to the resource utilization. Some organizations select to implement the Constrained RBAC to maximize the utilization of resources, but the chance of fraud increases due to the complexity in checking the conflicts of interest.

The implementation of RBAC has been widely studied by many researchers to cover the vulnerabilities or weak points of each level. This paper discusses only the related works which was proposed about the Constrained RBAC.

Sandhu [4] proposed a notation and model based on transaction control expressions for specifying and enforcing separation of duty by maintaining a history which included information on who performed each step. His idea has been adopted to use in the proposed model in this paper by maintaining a history on who performed each step in the workflow.

Bertino et al. [5] proposed the specification and enforcement of authorization constraints in workflow by referring to the association of roles with tasks in a workflow and specify the rules by encoding the constraint of each task and then compute the set of all possible roles and user assignments. When the user requests to activate the role, the algorithm will check whether the user is satisfied a given constraint or not. If the user is allowed to do the task, after the task is finished, the rule will be pruned from workflow specification to make the subsequent task evaluations faster. Some part of their workflow role specification has been adopted to use for workflow specification in the proposed model.

Chadwick et al. [6] proposed the multi-session Separation of Duty (MSoD) to support the role-based SoD constraint in

dynamic virtual organizations (VOs) via Multi-session mutually exclusive roles (MMER) constraint. A MMER constraint can be denoted as an m-out-of-n constraint, which contains n MSoD roles in which m or more roles are conflicting with each other and cannot be activated by a user in a particular business context. A MMER constraint is in a form of MMER($\{r_1, r_2, \ldots, r_n\}$, m, BC), where BC identifies the particular business context to which the m mutually exclusive roles apply, in which each $r_i (i = 1, 2, \ldots, n, n \geq 2)$ is a role, and $1 < m \leq n$. In this case, a user is forbidden to activate m or more roles among $\{r_1, r_2, \ldots, r_n\}$ in the same business context, so as to enforce an MSoD policy.

Chadwick et al.'s model might work if different business contexts can be specified, e.g., branch or period. In the PO issuing scenario, the different business contexts cannot be specified because those mutually exclusive roles are in the same environment and period, so that Chadwick et al.'s model is not applicable for PO issuing scenario.

Thipse and Hewett [7, 8] proposed an algorithm for constraint checking of simple dynamic SoD that works in a form of mutually exclusive roles pair. Their proposed model integrates MER into the business workflow. The proposed model in this paper uses the same approach. The differentiation is that their approach works by verifying separation of duty at build time (when roles are assigned to users but not activated), whereas the approach in this paper works by enforcing separation of duty at run time. Their algorithm uses the complete list of user assignments for each business process in the workflow to verify whether the given user role assignments are satisfied with the dynamic separation of duty constraint or not. The argument is that their approach should be used for roles assignment in Static Separation of Duty (SSD) because the Dynamic Separation of Duty (DSD) requires verification at role activations rather than at role assignments. For example in banking firm, one user can be assigned as Teller and Auditor simultaneously in DSD. Their proposed model may verify that a given user role assignments can perform an operation in a safe manner in case the workflow is composed of only two activities, starting with Teller and ending with Auditor. The suspicion is how they can guarantee that one user will not activate as Teller, then quit and later activated as Auditor to perform the operation of the same transaction. Another argument is that their work may only work if the assignment of all roles is completely taken place before the operation starts. Since in the real world business operations, some operations may take place before the assignment of all roles is completed, therefore the verification at roles assignment may not be effective.

Habib and Praher [9] recently proposed the new definition of dynamic separation of duty which is contrary to the definition given in [2] as "A user can be assigned to all mutually exclusive roles and is allowed to activate all mutually exclusive roles at the same time but not for the same object and also the user is not allowed to activate two successive dependent roles for the same object". They also gave a number of examples of different possibilities of role activation with respect to different scenarios. Finally, there was no enforcement or implementation mechanism of SoD in RBAC discussed in their work. Their proposed definition does not meet the concept of least privilege in separation of duty. They should maintain the word "multiple mutually exclusive roles" rather than using the word "all mutually exclusive roles". Another argument is that their definition is too much restricted, not as flexible as the DSD intention. The DSD rational in ANSI Standard defined as "DSD relations define constraints as a pair (*role set*, n) where n is a natural number ≥ 2, with the property that no user session may activate n or more roles from the role set". This rational does not forbid users to perform the task by more than one role for one object but forbids users to perform the task by m or more roles from the role set depending on the DSD rules enforced.

Most previous researches for DSD had concentrated on the user activations of one object. They always put the restriction that one user can activate only one role within the set of mutually exclusive roles for each object. The proposed model in this paper provides the restriction based on the DSD rule by allowing user to activate more than one role within the set of mutually exclusive roles depending on the policy requirement. This flexibility provides more convenient for policy deployment.

Although the workflow integration has been used in some researches, none of them used the workflow sequence for computational benefit. The proposed model in this paper used workflow sequence to compute the conflicts of interest at run time and provide run-time enforcement with low computational cost.

Some researches had provided the ability for run-time enforcement, e.g., the multi-session Separation of Duty (MSoD). The MSoD needs the specific business context to be identified in its constraint while the proposed model in this paper does not need any specific business context to provide more convenient for implementation.

V. DSD Enforcement Based on Workflow Sequence Model

The assumption in this paper is that the organization has implemented the access control system with Constrained RBAC including the level of Core RBAC, so that some users may have more than one role and may activate different roles at different times. The security management system has already assigned the appropriate permissions to the appropriate roles. The security management system will be the function to ensure that the tasks will be performed only by authorized users with the access control system. This paper will focus only on the activation of users into the roles to ensure that the authorized users who have already gained the access from security management system will not perform the conflicting tasks.

Fig. 2 illustrates the proposed model architecture and the detail of each entity will be described in the next subsections as follows. Subsection A describes the workflow specification. Subsection B presents DSD rule generation. Subsection C presents algorithms for run-time enforcement of user

activation based on DSD rule. Subsection D demonstrates how the proposed model and algorithm work with PO issuing scenario.

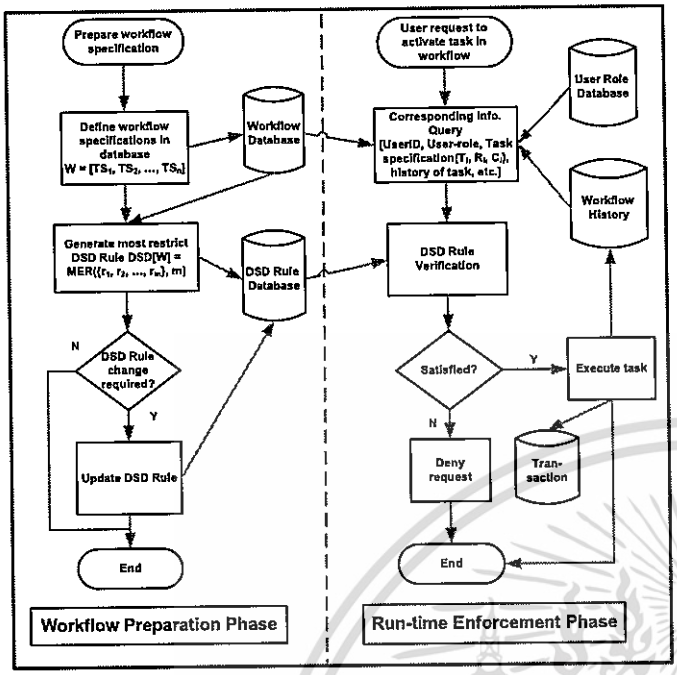


Fig. 2 DSD Enforcement Based on Workflow Sequence Model Architecture

A. *Workflow specification*

The limitation of this workflow specification is that each task in workflow allows only one role to perform the task and this workflow specification does not support the Hierarchical RBAC.

The workflow specification is the list of task specification sequence from start to end denoted by $W = [TS_1, TS_2, \ldots, TS_n]$, where n is the sequence of the ending task, $n > 1$. Each TS_i is a tuple of task specification (T_i, R_i, C_i) where

- T_i is the task of step i in the workflow. T_i is composed of operations, objects, and some other instances, as required. The specification of T_i will not be described in detail because it will not be used for the enforcement algorithm.
- R_i is the role which has been authorized to execute T_i.
- C_i is the criticality of T_i in the workflow denoted by a Boolean *true* or *false*. If C_i is *true*, it means that the task is a critical task, and then the R_i for this task will be considered as mutually exclusive role. If the task does not require integrity, C_i will be set to *false* and the R_i for this task will not be considered as mutually exclusive role.

B. *DSD Rule Generation Algorithm*

With a given workflow specification from the previous subsection, the algorithm as illustrated in Fig. 3 computes a set of mutually exclusive roles and generates the DSD rule in a form of $DSD[W] = \text{MER}(\{r_1, r_2, \ldots, r_m\}, k)$, where each r_i is a role, m is the number of roles defined as mutually exclusive roles and k is the number of minimum required persons, m and k are integers, $1 < k \leq m$. The algorithm generates the default DSD rule with the most restricted constraint. The most restricted constraint is that the number of minimum required persons and the number of roles in the role set are the same, so that the default DSD rule generated from this algorithm will result as $DSD[W] = \text{MER}(\{r_1, r_2, \ldots, r_m\}, m)$. The DSD rule can be changed by modifying the cardinal numbers k from m to be any integer number, where $1 < k \leq m$, depending on the company policy.

```
INPUT:   A workflow
         W = [TS1, TS2, ..., TSn],
         TSi = (Ti, Ri, Ci),
         i = 1, ..., n, n > 1
OUTPUT:  DSD Rule DSD[W] =
         MER({r1, r2, ..., rm}, m)
         1 < m ≤ n
Begin
  MER = {empty set}
  for each TSi in W do
    if Ci is true then
      MER = Ri union MER
    Endif
  DSD[W]=(MER, m)
  DSD[W]= MER({r1, r2, ..., rm}, m)
  return(DSD[W])
End
```

Fig. 3 DSD Rule Generation Algorithm

C. *DSD Run-time Enforcement Algorithm*

An algorithm for run-time enforcement of user activation based on DSD rule is illustrated in Fig. 4. When the user requests to activate the task within the workflow, the corresponding information, such as UserID, User-role, task specification (T_i, R_i, C_i), history of task, will be collected and sent as input to DSD run-time enforcement algorithm. At the first step, if it is found that a user role does not satisfy the role in the task specification, the algorithm will immediately deny the activation. For the next step, the algorithm checks whether the task is critical or not. If the task is not critical, the activation of user is allowed to perform the task and maintain the workflow history. If the task is critical, the algorithm uses the history of the corresponding transaction to compute the number of user activations in the previous steps of workflow and computes the possible total number of users by using the sequence of the current task. If the possible total number of users does not satisfy the DSD rule, the algorithm will deny the activation. On the contrary result, the algorithm will allow activation to perform the task and maintain the workflow history.

```
INPUT:  1) A workflow
           W = [TS1, TS2, ..., TSn],
           TSi = (Ti, Ri, Ci),
           i = 1, ..., n, n > 1
        2) UserID, User-role, task
           specification (Ti, Ri, Ci),HUW
           where HUW = history(set) of
           users in previous critical steps
        3) DSD Rule DSD[W] =
           MER({r1, r2, ..., rm}, k);
           where 1 < k ≤ m, k is the number
           of minimum   required users
        4) j = sequence of the request task
OUTPUT: deny if algorithm return true
        otherwise allow

Begin
  declare lou as set,
          cnu,ptn,k as integer
    '--lou = list of user
    '--cnu = current number of user
    '--ptn = possible total number of user
  if User-role ≠ Ri then return false
  else if Ci is false then return true
  else
     lou = HUW union UserID
     cnu = count(lou)
     ptn = Comp_Poss_Num_of_U(cnu,W,j)
     if ptn < k then return false
     else
          return true
     endif
  endif
End

Function Comp_Poss_Num_of_U(cnu,W,j)
  W = [TS1, TS2, ..., TSn], i = 1,..., n, n > 1
  n = last sequence of W
  TSi = (Ti, Ri, Ci)
  ptn = cnu
  for i = j to n do
    if Ci is true then
       add 1 to ptn
    endif
  endfor
return ptn
```

Fig. 4 DSD Run-time Enforcement Algorithm

D. *Work with PO Issuing Scenario*

This subsection presents how the proposed model and algorithm work with the PO issuing scenario.

In case Alice has been assigned as only purchasing clerk, Bob has been assigned as only buyer, and Dave has been assigned as only purchasing manager. There is no need to apply this algorithm because the assignments of users just fall into the Core RBAC.

Suppose that both Alice and Bob are buyers but they also have been assigned as purchasing clerk to originate POs for each other. By applying this proposed model, Bob and Alice cannot originate POs and act as buyer for the same POs.

For the first step, the workflow specification in the database can be defined as follows:

POW = [TS_1, TS_2, TS_3], where

TS_1 = (Create_PO, Pur_Clerk, True) ← Create PO by purchasing clerk, critical task

TS_2 = (Input_Price, Buyer, True) ← Input price by buyer, critical task

TS_3 = (Approve_PO, Pur_Manager, True) ← Approve PO by purchasing manager, critical task

For the next step, the DSD rule is generated by using DSD rule generation algorithm in subsection B, so the DSD rule will be given as DSD[POW] = MER({Pur_Clerk, Buyer, Pur_Manager}, 3). This DSD rule can be translated as "The workflow for PO needs role Pur_Clerk, Buyer, Pur_Manager and requires at least 3 persons to perform the task".

The next paragraph demonstrates possible events for various cases:

1. Bob is activated as Pur_Clerk and is requested to execute task TS_1. Bob is allowed to perform the task because the role is satisfied and the possible total number of users computed from the algorithm is 3, which is equal to the number of minimum required users. PO1 is created by Bob. History of Bob in the workflow is maintained.

2. Bob is activated as Buyer and is requested to execute task TS_2 for PO1. Bob is not allowed to perform the task because the possible total number of users computed from the algorithm is 2, which is less than the number of minimum required users. Therefore, the request is denied.

3. Alice is activated as Buyer and is requested to execute task TS_2 for PO1. Alice is allowed to perform the task because the possible total number of users computed from the algorithm is 3, which is equal to the number of minimum required users. History of Alice in the workflow is maintained.

4. Dave is activated as Pur_Manager and is requested to execute task TS_3 for PO1. Dave is allowed to perform the task because the role is satisfied and the possible total number of users computed from the algorithm is 3, which is equal to the number of minimum required users. History of Dave in the workflow is maintained.

Suppose that the policy has been changed to require at least two persons to perform the PO issuing, so that the DSD rule has to be revised as

DSD[POW] = MER({Pur_Clerk, Buyer, Pur_Manager}, 2)

5. Bob is activated as Pur_Clerk and is requested to execute task TS_1. Bob is allowed to perform the task because the role is satisfied and the possible total number of users computed from the algorithm is 3, which is more than the number of minimum required users. PO2 is created by Bob. History of Bob in the workflow is maintained.
6. Bob is activated as Buyer and is requested to execute task TS_2 for PO2. Bob is allowed to perform the task because the possible total number of users computed from the algorithm is 2, which is equal to the number of minimum required users. History of Bob in the workflow is maintained.
7. Dave is activated as Pur_Manager and is requested to execute task TS_3 for PO2. Dave is allowed to perform the task because the role is satisfied and the possible total number of users computed from the algorithm is 2, which is equal to the number of minimum required users. History of Dave in the workflow is maintained.

VI. CONCLUSIONS

This paper presents a very simple but effective model to verify the conflicts of interest at run time for dynamic separation of duty. This model provides the restriction based on the DSD rule by allowing user to activate more than one role within the set of mutually exclusive roles depending on the policy requirement. This flexibility provides more convenient for policy deployment. The integration with workflow in this model uses the workflow sequence to compute the conflicts of interest and provide run-time enforcement with low computational cost. This model can be implemented without any particular business context to be specified as some other researches to make more convenient for implementation.

For the future work, we have planned to include the verification of Hierarchical RBAC and support the concurrent case. The concurrent case is the case that needs more than one person of the same role to perform the same task. For example, in the case of PO issuing, two purchasing managers may be needed for the concurrent approval. This would require a more complexity model to verify the conflicts of interest.

REFERENCES

[1] D. F. Ferraiolo and D. R. Kuhn, "Role-based access control," *In Proceedings of the 15th National Computer Security Conference*, pp. 554-563, 1992.

[2] ANSI. *American national standard for information technology – role based access control.* ANSI INCITS 359-2004, February 2004.

[3] D. Georgakopoulos, M. Hornick, and A. Sheth, "An overview of workflow management: from process modeling to workflow automation infrastructure," *Distributed and Parallel Databases*, 3, pp. 119-153, 1995.

[4] R. S. Sandhu, "Transaction control expressions for separation of duties," *In Proceedings of the Fourth Annual Computer Security Applications Conference*, pp. 282-286, 1988.

[5] E. Bertino, E. Ferrari, and V. Atluri. "The specification and enforcement of authorization constraints in workflow management systems," *ACM Trans. on Information and System Security*, Vol.2, No.1, pp. 65-104, February 1999.

[6] D. W. Chadwick, Wensheng Xu, S. Otenko, R. Laborde, and B. Nasser, "Multi-session separation of duties (MSoD) for RBAC," *In Proceedings of the IEEE 23rd International Conference on Data Engineering*, pp. 744-753, 2007.

[7] R. Hewett, A. Thipse, and P. Kijsanayothin, "Security analysis of role-based separation of duty with workflow," *In Proceedings of the 3rd International Conference on Availability, Reliability and Security*, pp. 765-770, 2008.

[8] A. Thipse and R. Hewett, "Verification of dynamic separation of duty policy for role-based business processes," *In Proceedings of the 2008 IEEE Region 5 Conference*, pp. 1-6, 2008.

[9] M. A. Habib and C. Praher, "Object based dynamic separation of duty in RBAC," *In Proceedings of the 4th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 512-516, 2009.

PROCEEDINGS OF
THE 2011 INTERNATIONAL CONFERENCE ON
SECURITY & MANAGEMENT

SAM'11

Volume I

Editors

Hamid R. Arabnia
Michael R. Grimaila, George Markowsky
Selim Aissi

Associate Editors

Leonidas Deligiannidis
Ashu M. G. Solo

WORLDCOMP'11
July 18-21, 2011
Las Vegas Nevada, USA
www.world-academy-of-science.org

Data Center Physical Security Ontology for Automated Evaluation

Nanta Janpitak and Chanboon Sathitwiriyawong
Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang,
Bangkok 10520, Thailand

Abstract - *Nowadays, most business operations are supported by IT systems. Therefore, their availability is critical to keep business running smoothly and continuously. In order to provide high quality IT services, a well-managed data center is required to house computer servers, storage systems, network devices, and their associated components. Downtime of the data center can be costly resulting in production and business losses so that the high availability requirement of the data center is needed. Apart from availability, the data center also requires a dependable and secure computing including such attributes as confidentiality, reliability, safety, integrity, maintainability, etc. This paper introduces an ontology-based framework for data center physical security by gathering and mapping the requirement from well-known information security standards such as COBIT, ISO/IEC 27002, and ITIL. In order to fulfill the safety requirement of the data center, this ontology-based framework is also designed to be applicable with National Fire Protection Association (NFPA) code and standard for protecting all data center occupants and for limiting data center property loss from fire. The completion of this ontology will be used for the knowledge sharing and also as an input for data center physical security evaluation tool.*

Keywords: Ontology; Data Center; Dependable Computing; Information Security; Automated Evaluation

1 Introduction

Data Center is a facility used for housing a large amount of computer and communications equipment maintained by an organization for the purpose of handling the data necessary for its operations [1]. Since data center contains many sensitive organization's data, the access to these data by authorized person is one of the mandatory feature of data center. The access control of data can be done physically and logically. This paper focuses on physical access control by referring to section DS12-Manage the Physical Environment from the mapping of CoBiT 4.1, ITIL V3 and ISO/IEC 27002 [2]. This publication is the new ITGI/OGC guide intended to help companies achieve maximum governance and value in a down economy.

Data center always requires a non-stopped service or 24x7 availability. The availability of data center mainly requires the protection of computer equipment and personnel. There are some potential hazards which may occur and impact the availability of data center. Fire is the most potential hazard which can create severe effects on data center. Fire can occur in a data center by mechanical failure, intentional arson, or natural causes. This paper focuses on how to deal with fire for protection of computer equipment and personnel by designing the data center to comply with National Fire Protection Association (NFPA) code and standard [3].

Most large organizations have defined their information security policy to protect their information asset by interpreting multiple requirements such as laws, regulations, well-known standards, and some other requirements. IT personnel including IT managers are well aware that information security policy is important to follow but they do not take much effort to understand and remember what the rules or policies said. They always leave this responsibility to Information Security Expert, which is a rare personnel in each organization. In order to evaluate the policy compliance, the Information Security Expert has to do the evaluation manually using their information security expertise. The manual evaluation is always time consuming, complex and requires expert knowledge. Once the Information Security Expert leaves the company, other personnel cannot evaluate their policy compliance because of the lack of information security knowledge.

Another major problem in managing data center is that most facilities in the data center are normally installed and supported by other departments rather than IT department. For instance, Production Engineering department is responsible for the planning and design of overall facilities, Maintenance department is responsible for preventive maintenance, and Safety department is responsible for supporting and monitoring the fire protection system. This makes more complexity to data center facilities management. IT department must provides a clear communication to those departments to make sure that the data center related policies are met, so that IT personnel should have a good understanding and knowledge in data center policy requirement.

As mentioned above, various approaches to organize the information security knowledge and automate the evaluation process of policy compliance have been proposed. Ontology is one of the tools which many researchers have recently

proposed to support the knowledge sharing and enhance the automated evaluation process. The overview of ontology will be provided in section 3.

The overall proposal of this paper is the ontology-based framework for data center physical security. This ontology is designed by gathering many sources of requirement in order to develop a single source of knowledge and prepare for a future automated evaluation process.

The rest of this paper is organized as follows. Section 2 explains the overview of data center and discusses some related works. Section 3 explains the overview of ontology and discusses some information security related works. Section 4 describes the proposed ontology-based framework for data center physical security. Finally in section 5 summarization and conclusions of this paper are provided.

2 Overview of data center and related works

A data center is a facility used to house computer servers, storage systems, network devices, and their associated components. Downtime of data center can be costly resulting in production and business losses. In order to reduce business interruptions, an effective management with a comprehensive design of data center is required.

As data center becomes more and more central in the present age of internet communication, both research and operations communities have begun to explore how to better design and manage them. There are some materials providing guideline for data center design such as Sun Microsystems provides "Enterprise Data Center Design and Methodology" [4], Cisco Systems provides "Data Center Fundamentals" [5]. Those materials provide a comprehensive design guideline to cover the different areas of data center requirements such as cable management, network infrastructure, environmental controls, power management, physical security, etc. The data center ontology-based framework designed in this paper is based on the guideline in "Enterprise Data Center Design and Methodology" from Sun Microsystems.

Thomas [6] discussed an idea that computer security should be improved through environmental controls. An environment which is constantly varying will produce unreliable equipment operation. Humidity has to be controlled as well as temperature. For instance, the temperature in data center should not be adjusted by human comfort but rather machine, the relative humidity should not exceed 80 percent, the maximum number of people allowed in a data center at any one time should be determined, etc. Working space is also an important element when designing the data center. Since the computing equipment has a very heavy load, so floor selection process should be carefully done. As Thomas's main point, the environmental controls have been put an attention as one main component in the proposed ontology which will be discussed in section 4.

Robert [7] presented an overview of some technical and managerial of protecting the data center resources including personnel from any accidental damage. This paper focuses on the engineering management aspects of 6 major areas of concern regarding operational data security: personnel, facilities, computer hardware, computer software, communications, and procedures. In addition to the many important design considerations such as temperature, humidity, cooling water and fire fighting system, the interference of electro-magnetic to computer hardware is also examined in this paper.

In order to protect the information asset, the information security policy is defined by interpreting multiple requirements such as laws and regulations. To ensure that the information security policy is followed, the evaluation process is required. The policies or any related requirements regarding to the data center physical security are considered as a non-technical requirement which is hard to be interpreted and transformed to a machine-readable form. This makes an evaluation or validation process hard to be performed. In order to enable the automated process, an ontology technology has been selected to transform the non-technical requirement into machine-readable form. The overview of ontology will be described in the next section.

3 Overview of ontology and information security related works

Ontology is an explicit specification of a conceptualization [8]. A conceptualization is the objects, concepts, and other entities that are assumed to exist in some areas of interest and the relationships that hold among them. A conceptualization is an abstract, simplified view of the world that we wish to represent for some purposes. Ontology represents knowledge in a formal and structured form as well as provides a better communication, reusability and organization of knowledge and a better computational inference.

From the previous section, information security needs a better knowledge sharing method for better communication. It also requires automating any related processes such as evaluation and monitoring. Ontology has been studied and proposed by many researchers to cover those requirements. Since the area of interest and the relationships that hold among them is considered as a domain, so that from now, the information security area will be called as information security domain in this paper.

A study of Carlos et al. [9] is useful to shorten the review of previous works in information security domain. They used OntoMetric [10] to compare various security ontologies proposed by many researchers. Finally, they have concluded that the existing ontologies in this domain are not prepared for being reused and extended. They suggested that the community should put efforts to join and improve the developed ontologies. Besides combining different terms from

different creators looks impossible despite being a domain expert.

Stefan et al. [11, 12] proposed a security ontology based on the security relationship model described in the National Institute of Standards and Technology Special Publication 800-12 [15]. Their security ontology was also developed based on the basic concepts and taxonomy of dependable and secure computing [16] which will be used and discussed later in the proposed ontology section. The core concepts of their security ontology were grouped in three sub-ontologies: security sub-ontology, enterprise sub-ontology, and location sub-ontology. Security sub-ontology consists of attribute, control, threat, vulnerability, and rating, derived from well established information security standard. Enterprise sub-ontology consists of asset, person, and organization. Location sub-ontology only stores a list of locations. Finally they have given the relations between these concepts such as each *threat* has been connected to *asset* concepts by the *threatens* relation, organization concept has been connected to its assets by the *ownedBy* relation. In [11] they presented a tool called "SecOntManager" by using their security ontology to simulate threats. From the simulation example, it shows the impact of fire on the infrastructure, what countermeasures exist and how the outage costs for each simulation of countermeasure.

Stefan et al. also proposed other ontologies related to information security domain such as ontology-based framework to improve the preparation of ISO/IEC 27001 audits [13] by mapping with the security ontology which they had earlier proposed. A Common Criteria (CC) ontology [14] comprising the entire CC domain with special focus on security assurance requirements is relevant for the evaluation.

Ju and Minzhe proposed an ontology for vulnerability management called OVM [17]. The top level concepts in this ontology are Vulnerability, IT_Product, Attacker, Attack, Consequence, and Countermeasure. At the earlier steps, the OVM retrieves the common vulnerabilities from the National Vulnerability Database (NVD) which is the US government repository of standard-based vulnerability data. The OVM then links the *Vulnerability* concept to *IT_Product* concept by *hassAffectedProduct* and *hasVulnerability* relations. By retrieving vulnerability data from OVM, the information can then be served as the knowledge base for vulnerability management.

From many information security ontologies that we had reviewed, we found that the ontologies developed for a full information security domain are not easy to be used in the future. We support an idea that the information security domain should be split into subdomains and each subdomain should have a connection point to link each other. Then a full information security domain can be created by linking all subdomains. This makes it easier to be implemented in the next steps. The ontology-based framework for data center physical security is one of the information security subdomains that will be explained in the next section.

4 Ontology-based framework for data center physical security

To ensure that the protection of data center is effective, the IT department should have an effective compliance management. To support the compliance management, the ontology-based framework for data center physical security has been developed in details as follows subsections.

4.1 Overview of data center physical security framework

In order to support the compliance management, the ontology-based framework for data center physical security has been developed the same as the data center policy by consolidating the requirements from various well-known standards for computer security, fire protection and environmental control as depicted in figure 1.

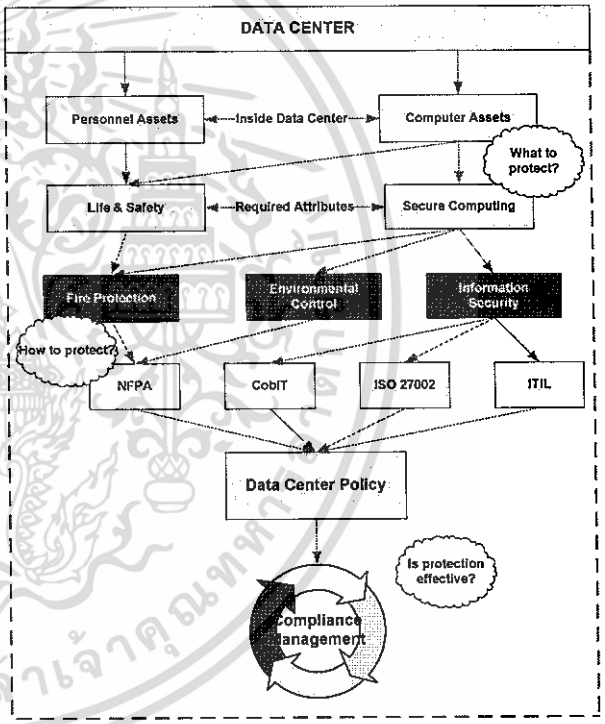


Figure 1. Data Center Physical Security Framework

4.2 Overview of ontology development methodology

To increase the ontology efficiency and ensure the consistency of ontology structure, during development we followed the guidelines from many sources. First we studied how to build the ontology by using a guideline from [18]. The guide was built using Protégé ontology editor [19] which is the same tool that we have used for our ontology development. To develop ontology by using Protégé we followed the guideline from [20]. There is no single correct ontology-design methodology [18] so that we studied a few ontology

development methodologies and finally we decided to follow a recently defined methodology from [21] incorporating with the guide in [18]. This ontology development methodology covers the steps from the initiation stage to the maintenance stage of ontology. The methodology consists of three main subprocesses: specification, concretization and implementation. Each subprocess consists of a set of activities that will be described along the ontology development in the next subsection.

4.3 Ontology for data center physical security

The ontology for data center physical security has been developed by following the methodology in [21] as the following processes.

1. *Specification subprocess (Equivalent to step 1 in [18])*

   1.1 Activity 1: Describing the domain. The ontology for data center physical security is a subdomain of the information security domain. This ontology is the consolidation of requirements from various well-known standards for computer security, fire protection and environmental control to protect information asset and ensure that data center can provide a continuous service with a minimum downtime. The completion of this ontology will be used for the knowledge sharing and also as an input for data center physical security evaluation tool.

   1.2 Activity 2: Elaborating motivating scenarios and competency questions. Due to page constraint, the complete scenario and competency questions will not be presented in this paper. The example of competency question is "How to prevent fire in data center?" which will be used as example in the validation activity (*subprocess 3.3*).

   1.3 Activity 3: Determining the ontology goal and scope. This ontology goal is to represent the set of data center physical security requirements as reusable knowledge for preparing either manual or automated evaluation process. This ontology is limit to the physical security which does not include the logical security. This ontology covers only fire hazard which is the most potential occurrence at all parts of the world. The other natural disasters such as flood or storm can be included in the future.

2. *Concretization subprocess*

   2.1 Activity 1: Defining classes and class hierarchy (Equivalent to step 3-4 in [18]. In this task, a list of terms that represent the most important entities in data center physical security domain has been enumerated as classes. The list of important classes and subclasses is shown in table 1. Definitions of important classes are provided after table.

TABLE 1. Key Item List as Class and Subclass

Class	Subclass
DataCenter	
Safeguard	
DataCenterDesignGuideline	Physical_LogicalSecurity
	AvoidingHazards
	HVACandEnvironmentalControls
Reference	ISO2700x
	COBIT
	ITIL
	NFPA
Facility	PhysicalAccessControl
	FireDetectionSystem
	FireSuppressionSystem
	PowerRedundancy
	HVAC
Threat	Hazard:Fire
	PowerLoss
	UnstableEnvironment
	UnauthorizedAccess

- The class "*DataCenter*" is defined as the highest level class in this domain.
- The class *"Safeguard"* is defined to contain the countermeasure that use to deal with each threats which impact to the availability of data center.
- The class *"DataCenterDesignGuideline"* is defined to contain the contents of guideline retrieved from [4] that will be referred by each safeguard.
- The class *"Reference"* is defined to contain the contents of requirements from various well-known standards. The reference is divided into 4 subclasses as "ISO2700x", "COBIT", "ITIL", and "NFPA".
- The class *"Facility"* is defined to contain the facilities that have to be used in accordance with the guidelines or references. The facility is divided into a few main subclasses such as "PhysicalAccessControl", "PowerRedundancy", and "FireSuppressionSystem".

2.2 Activity 2: Identifying class relations, attributes and properties (Equivalent to step 5 in [18]). Only the classes will not provide enough information. In this task, the main relations, attributes and properties were created. The example of class relations is shown in table 2.

2.3 Activity 3: Representing rules and restrictions (Equivalent to step 6 in [18]). This task is to analyze the *restrictions* represented in the class relations, attributes and properties. On the other hand, in general usage a restriction is a specific type of rule that sets a finite boundary defined for a type of process or function. The example of class attributes, properties, rules and restriction is shown in table 3. Then, the classes, class hierarchy with relations have been captured in a graphical diagram to represent the

linkage and relation between each component as shown in figure 2.

2.4 Activity 4: Representing individuals (Equivalent to step 7 in [18]). This task is to define individual instances of each class. The instances of data center physical security were created as shown in table 4.

3. The implementation subprocess

3.1 *Activity 1: Creating a computational ontology.* The goal of this activity is to convert the ontology which was designed in the prior subprocesses into a formalized representation interpretable by a machine, using an appropriate language with formal semantics. There are different languages to be used for this task. The most relevant ones are RDF (Resource Description Framework) and OWL (Web Ontology Language). In order to carry out this activity, the Protégé ontology editor [19] which is the most popular ontology development tool has been used. The ontology was built in OWL by using the Protégé as shown in figure 3.

3.2 *Activity 2: Verifying the ontology.* The goal of verification process is to avoid future propagation of errors. To compare with ontology which was designed in the prior subprocesses, the graphical view of class hierarchies were generated by using OWLViz plug-ins. The consistency checking was done by using a Reasoner plug-ins.

Activity 3: Validating the ontology. In order to validate the ontology, it is necessary to verity whether the ontology can answer the competency questions. We have to do some semantic queries by using the semantic web query language SPARQL [22] and Jena API [23]. Hereunder is an example result of SPARQL query to answer the competency question "How to prevent fire in data center?"

```
SELECT ?x WHERE { ?x rdf:type
<#Guideline_FirePrevention> }
Result:
...
Guideline_FP_NoSmoking
Guideline_FP_NoCombustibleMaterials
...
SELECT ?x WHERE
{ <#Guideline_FP_NoSmoking>
rdfs:comment ?x }
Result:
Smoking should never be allowed in the data center.
Signs should be posted at entryways and inside.
```

The example query result shows how this ontology answers the competency questions. In the future steps, the query result will be used in semantic web technology for user friendly mode.

TABLE 2. An excerpt of the relation table of the data center physical security

Class Name	Relation	Class Name	Inverse Relation
DataCenter	required	SecurityAttribute	requiredBy
SecurityAttribute	impactedBy	Threat	impactTo
Fire	detectedBy	FireDetection System	toDetect
	Suppressed By	FireSuppression System	toSuppress
PowerLoss	preventedBy	Power Redundancy	toPrevent
Unstable Environment	controlledBy	HVAC	toControl
Unauthorized Access	preventedBy	PhysicalAccess Control	toPrevent
FireDetection System	followedTo	DataCenter Guideline	followedBy
DataCenter Guideline	referredTo	Reference	referredBy

TABLE 3. An excerpt of the class attributes and properties of the data center physical security

Class	Property	Type	Restrictions
DataCenter	has Component	Instant	class{RoomComponent}
	required	Instant	class{SecurityAttribute}
	threathenBy	Instant	class{Hazard:Fire}
Hazard:Fire	detectedBy	Instant	class{Guideline_FireDetection}
	preventedBy	Instant	class{ Guideline_FirePrevention }
	Suppressed By	Instant	class{ Guideline_FireSuppression}
Unstable Environment	controlledBy	Instant	classes={HVACandEviromentalControls}
Unauthorized Access	preventedBy	Instant	classes={PhysicalAccess Control}

TABLE 4. An excerpt of the class attributes and properties of the data center physical security

Class	Instance Name	Property Name	Property Value
DataCenter	PirmaryDC	required	Availability
		threathenBy	Threat_Fire
		hasComponent	DCRoof
		hasComponent	EgressDoor
		hasComponent	DoorSideWall
		hasComponent	DCFloor
Room Component :Door	EgressDoor	madeBy	Steal
		hasFireRating	1
		isSwingOut	true
Room Component :Wall	DoorSideWall	equippedTo	Facility_FireExtinguisher_Co2
		hasFireRating	1
Facility:FireSuppressionSystem	Facility_FireExtinguisher_Water	isMandatory	true
	Facility_FireExtinguisher_CO2	isMandatory	true

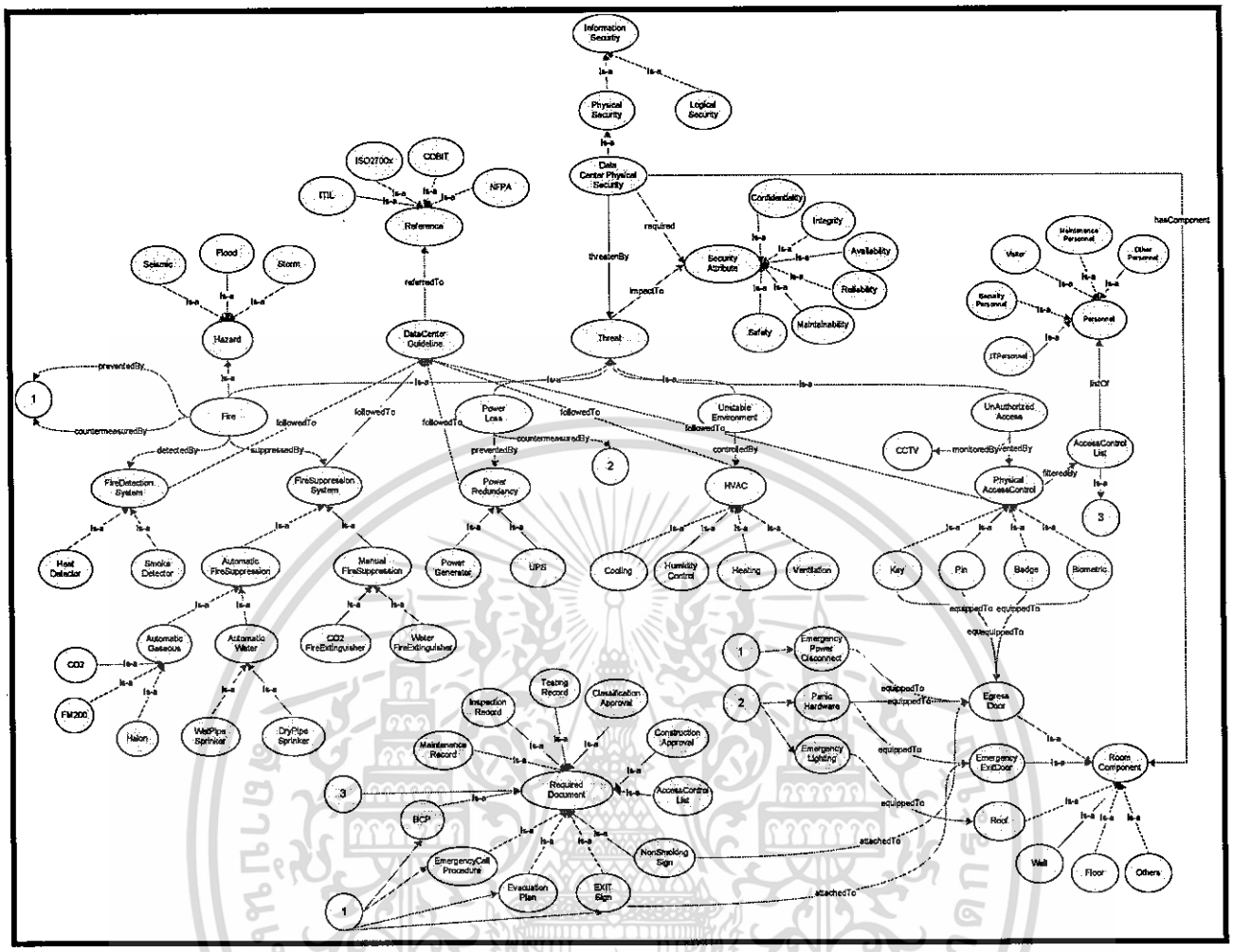


Figure 2. Components Linkage Diagram

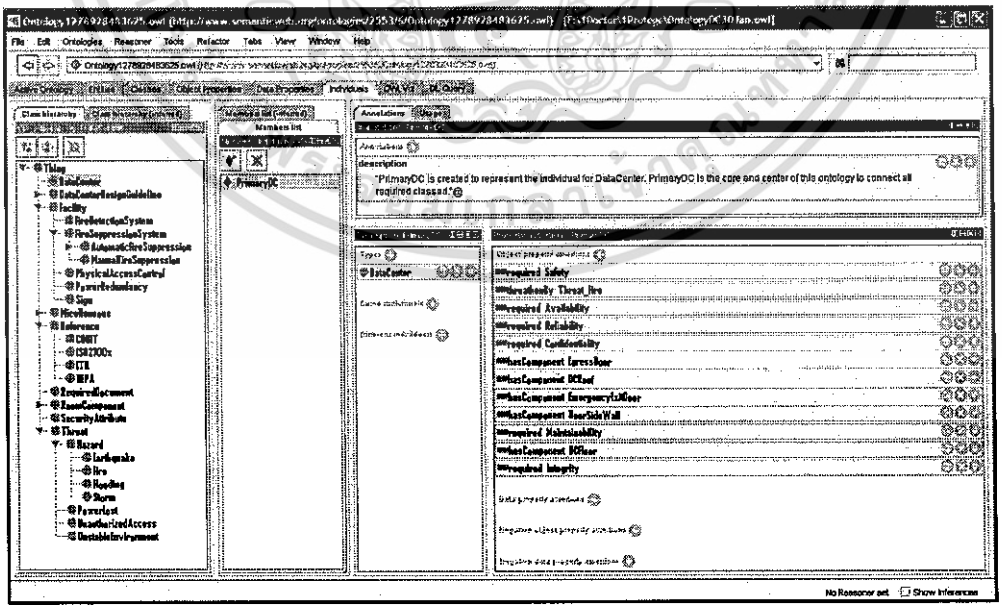


Figure 3. Protégé logical view window

5 Conclusions

This paper presents an ontology developed for information security knowledge sharing by focusing on data center physical security. The data center physical security ontology can be used for an automated evaluation in the future to enhance the automated compliance process. This ontology also provides the connection point to the information security domain. Since the information systems can be accessed by either physical or logical so that the information security should be split into physical security and logical security. Then the data center physical security is linked to the main information security domain under physical security section. Apart from data center, there are other physical entities such as a client, a telecommunication asset, etc. The controls of those entities can be developed as ontology and linked into information security domain under physical security section. The ontology proposed and developed that is presented in this paper would be continuing improved and used for our work in progress (Data Center Physical Security Evaluation Tool).

6 References

[1] Glossary of MMC Terminology. Available: http://msdn.microsoft.com/en-us/library/bb246417(VS.85).aspx.

[2] ITGI/OGC. "Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for business benefit". A management briefing from ITGI and OGC. Available: http://www.isaca.org.

[3] National Electric Code, National Fire Protection Association International, Boston, Mass., U.S.A.

[4] R. Snevely. "Enterprise data center design and methodology". Palo Alto, California: Sun Microsystems Press, A Prentice Hall Title, 2002.

[5] M.Portolani. "Data center fundamentals". Indianapolis, Indiana: Cisco Press, 2004.

[6] T. C. Richards. "Improving computer security through environmental controls"; Security Audit and Control Review, Vol. 1, No. 3, Fall 1982, pp. 18-24.

[7] R. J. Wilk. "Engineering management considerations in data center security"; Proceedings of the 4th annual symposium on SIGCOSIM: management and evalution of computer technologym, 1973, pp. 11-22.

[8] T. R. Gruber. "Towards principles for the design of ontologies used for knowledge sharing"; International Journal of Human-Computer Studies, Vol.43, 1995, pp. 907-928.

[9] C.Blanco et al. "A systematic review and comparison of security ontologies"; International Conference on Availability, Reliability and Security (ARES). Barcelona, 2008, pp. 813-820.

[10] A. Lozano-Tello, A. Gómez-Pérez. "ONTOMETRIC: A method to choose the appropriate ontology"; Journal of Database Management. Special Issue on Ontological analysis, Evaluation, and Engineering of Business Systems Analysis Methods, Vol.15, 2004, pp.1-18.

[11] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl. "Security ontology: Simulating threats to corporate assets"; In A. Bagchi and V. Atluri, editors, Information Systems Security, volume 4332 of Lecture Notes in Computer Science, Springer, 2006, pp. 249–259.

[12] S. Fenz, A. Ekelhart. "Formalizing information security knowledge"; In 4th International Symposium on Information, Computer, and Communications Security (ASIACCS '09), 2009, pp. 183-194.

[13] S. Fenz, G.Goluch, A. Ekelhart, B. Riedl, and E. Weippl. "Information security fortification by ontological mapping of the ISO/IEC 27001 standard"; In 13th IEEE International Symposium on Pacific Rim, 2007, pp. 381-388.

[14] A. Ekelhart, S. Fenz, G. Goluch, and E.Weippl. "Ontological mapping of common criteria's security assurance requirements"; In 22nd IFIP TC-11 International Information Security Conference (IFIPSEC'07), 2007, pp. 85-95.

[15] NIST. An Introduction to Computer Security – The NIST Handbook. Technical report, NIST (National Institute of Standards and Technology), October 1995. Special Publication 800-12.

[16] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr. "Basic concepts and taxonomy of dependable and secure computing"; IEEE Trans. Dependable and Secure Computing, vol. 1, no. 1, 2004, pp. 11-33.

[17] J. A. Wang and M. Guo. "OVM: an ontology for vulnerability management"; Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, 2009, pp. 1-4.

[18] N. F. Noy and D. L. McGuinness. "Ontology development 101: A guide to creating your first ontology"; Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, 2001.

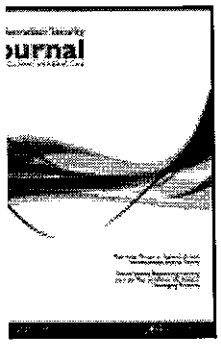
[19] Stanford Center for Biomedical Informatics Research. "The Prot´eg´e ontology editor and knowledge acquisition system". Available: http://protege.stanford.edu.

[20] M. Horridge, H. Knublauch, A. Rector, R. Stevens, and C. Wroe. "A practical guide to building OWL ontologies using the Prote´ge´-OWL plugin and CO-ODE tools edition 1.2"; University of Manchester, 2009.

[21] G. Brusa, M. L. Caliusco, and O. Chiotti. "Towards ontological engineering: a process for building a domain ontology from scratch in public administration"; Expert Systems: The Journal of Knowledge Engineering, Vol. 25, Issue 5, 2008, pp. 484–503.

[22] SPARQL Query Language for RDF. Available: http://www.w3.org/TR/rdf-sparql-query/.

[23] Jena – A Semantic Web Framework for Java. Available: http://jena.sourceforge.net/index.html



Information Security Journal: A Global Perspective

ISSN: 1939-3555 (Print) 1939-3547 (Online) Journal homepage: http://www.tandfonline.com/loi/uiss20

Automated Compliance Checking Methodology for Non-Log Operations

Nanta Janpitak & Chanboon Sathitwiriyawong

To cite this article: Nanta Janpitak & Chanboon Sathitwiriyawong (2015) Automated Compliance Checking Methodology for Non-Log Operations, Information Security Journal: A Global Perspective, 24:4-6, 98-108, DOI: 10.1080/19393555.2015.1067340

To link to this article: http://dx.doi.org/10.1080/19393555.2015.1067340

Accepted author version posted online: 16 Jul 2015.
Published online: 18 Aug 2015.

Information Security Journal: A Global Perspective, 24:98–108, 2015

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393555.2015.1067340

Taylor & Francis
Taylor & Francis Group

Automated Compliance Checking Methodology for Non-Log Operations

Nanta Janpitak and Chanboon Sathitwiriyawong
Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand

ABSTRACT Compliance Management (CM) is the management process that an organization implements to ensure organizational compliance with relevant requirements and expectations. The most complicated, time-consuming, and costly process in CM is compliance checking because it requires a person who has a good knowledge in policy to examine whether the current operations meet the policy requirements. Many researchers have tried to study better ways to automate the compliance checking process, but most of them require the operation logs in to the computer systems. This paper proposes a methodology to enable the automation of compliance checking for those operations that have no log in computer systems by using questions and answers principle to cooperate with the semantic web technologies. Since there are some operations that cannot be understood by computer systems, using questions is one way to gather the answers, such as operation log to evaluate their compliance. The proposed methodology can help noncertified auditors perform the compliance checking so that the time and cost of compliance checking would be greatly reduced.

KEYWORDS compliance checking, Compliance Management (CM), data center, ontology, semantic web technology

1. INTRODUCTION

The financial scandals in many major companies such as WorldCom, Enron, and Siemens have resulted in a decline of public trust in accounting and reporting practices (John, 2009). This makes it necessary to create laws, regulations, standards, and guidelines to protect, detect, and correct such events. The most well-known law is Sarbanes-Oxley Act (SOX) (Congress of the United States, 2002), which was enacted in 2002. The intent of SOX is to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. Other examples of well-known laws, regulations, and standards are the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Control Objectives for Information and Related Technology (COBIT), ISO/IEC 27000 series, and Information Technology Infrastructure Library (ITIL). To maintain and increase a public trust in accounting and reporting practices, companies try to help investors feel more confident by certification audits that they are compliant with such laws, regulations and standards.

Address correspondence to Nanta Janpitak, Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang, 1 Soi Chalongkrung 1, Ladkrabang, Bangkok 10520,Thailand. E-mail: njanpita@hotmail.com

Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/uiss.

Compliance is a concept of acting in accordance with established laws, regulations, and so forth. It is part of Governance, Risk, and Compliance (GRC) (Tarantino, 2008) which is an important term in the world of business and information technology. Compliance is usually a term referring to laws and governmental regulations, which are considered mandatory by definition. The mistaken or misunderstanding interaction can be defined as noncompliance activities, which can result in high business risk such as fines and brand reputation. The cost of noncompliance could run into millions of dollars (Bace, Rozwell, Feiman, & Kiwin, 2006; Greengard, 2004). Instead of responding to regulatory compliance issue as ad-hoc, one-off manner, businesses should be devising effective ways to measure the effectiveness of compliance efforts and creating a compliance governance structure that allows planning for the future.

Compliance Management (CM) is the management process that an organization implements to ensure organizational compliance with relevant requirements and expectations (Frederick, Nandan, & Pradeep, 2007). The requirements are referred to as the compliance standard or compliance benchmark, while the process is what manages their compliance. Compliance management has become a significant concern for organization due to the increasing number and changing of rules in accordance with laws and regulations. Companies need to be able to easily ensure compliance with revised laws and regulations. Since today's businesses are complex, organization rules are often branched across numerous departments. It is quite impossible for a single manager to understand all of the rules, which can lead to noncompliance activities, so many organizations choose to have an effective compliance management. An effective compliance management not only protects organization from the adverse affects of noncompliance but also helps organization achieve better operational control.

However, compliance management, especially compliance checking (or compliance auditing or compliance measurement), is a costly and time-consuming task that is performed manually by auditors or information security experts. Some organizations developed their computerized compliance checking systems, but these systems were developed in specific programming codes and platforms which are difficult to update and reuse. Regulations in their original form are abstract specifications to ensure more independence from implementation and more flexibility in adapting regulations to different business problems (Kharbili, Stein, Markovic, & Pulvermüller, 2008). The writers and users of regulations are generally business people and lawyers. Their instrument of works is natural language and is nonformalized. The information extraction process is carried out manually, so the traditional programming codes are not suitable to manage such kind of changes. Presently, the level of automation in compliance checking is still low.

There have been many researchers who have studied an effective way to automate compliance management. Many of them proposed the use of semantic web technologies, which are the same technologies we used in our proposal.

The overall proposal of this paper is a methodology for developing an automated compliance checking tool. The main tool is an ontology that is part of semantic web technologies.

The rest of this paper is organized as follows. Section 2 explains the research motivation. Section 3 discusses some related works about compliance checking and ontology. Section 4 describes the proposed automated compliance checking methodology for non-log operations. Section 5 provides the performance evaluation. Finally, section 6 concludes this paper.

2. RESEARCH MOTIVATION

Compliance is part of GRC, which is important for business and information technology. Compliance checking is a subprocess in compliance management usually handled manually by auditors. Our research motivation is to replace the manual activities of auditors with computerized systems.

For more understanding, we drafted the compliance management framework and drilled down into the compliance checking framework as shown in Figure 1 and Figure 2 respectively.

As shown in Figure 2, compliance checking is a process to assess the effectiveness of controls. It requires two portions of information to be compared and evaluated. One portion comprises the compliance requirements that are separated into two types: technical requirements and nontechnical requirements. Another portion is information of current operations that are separated into log operations and nonlog operations.

Each type of information can be explained as follows.

1. Technical requirements are requirements that can be understood and computed by traditional computerized systems. However, it requires specific programming for each requirement. This kind of requirement is usually relevant to numeric assessment including date and time.

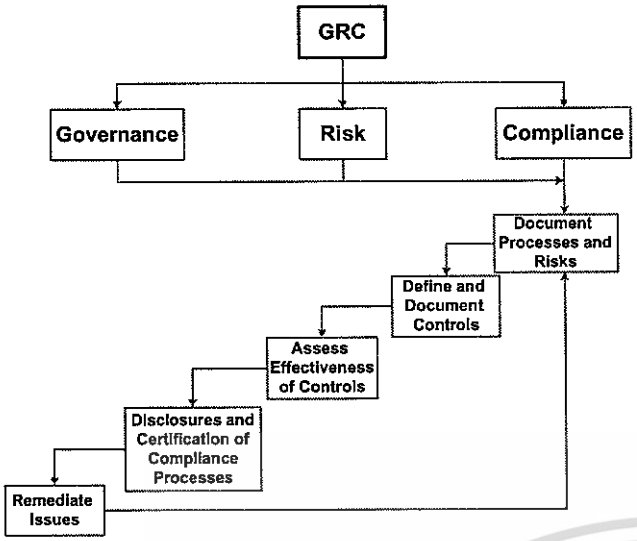


FIGURE 1 Compliance management framework.

For example, the compliance requirement is "Minimum password length=7." We can use computerized systems to count the length of user passwords that are stored in user databases. The company will be evaluated as noncompliant to this requirement if the computerized systems find that some user passwords are less than 7 characters in length.

2. Nontechnical requirements are requirements that cannot be understood by computerized systems. Without hard coding, such requirements cannot be evaluated.

For example, the compliance requirement is "Smoke detector must be installed in the data center." Since the traditional computerized systems do not understand the terms "smoke detector," "must be," "install", or "data center," we cannot use computerized systems to evaluate this requirement without manual interpretation by human.

3. Log operations are operations that have records of events or changes in computerized systems.

For example, the last password change date can be understood by computerized systems, so that it is considered as a log operation.

4. Non-log operations are operations that have no record of events or changes that can be understood by computerized systems.

For example, smoke detector installation has no record of events that can be understood by computerized systems because the computerized systems do not understand the terms "smoke detector" and "installation," so it is considered as a non-log operation.

In order to achieve the automation of compliance checking, the automated processing of compliance requirements and operation logs is required.

From our study and literature reviews, we combined the condition of compliance requirements and current operations as shown in Figure 3.

The combinations can be explained as follows.

1. Compliance requirements are in technical form and current operations are log operations. The automation is mostly adhered to by traditional computerized systems.
2. Compliance requirements are in nontechnical form and current operations are nonlog operations. The

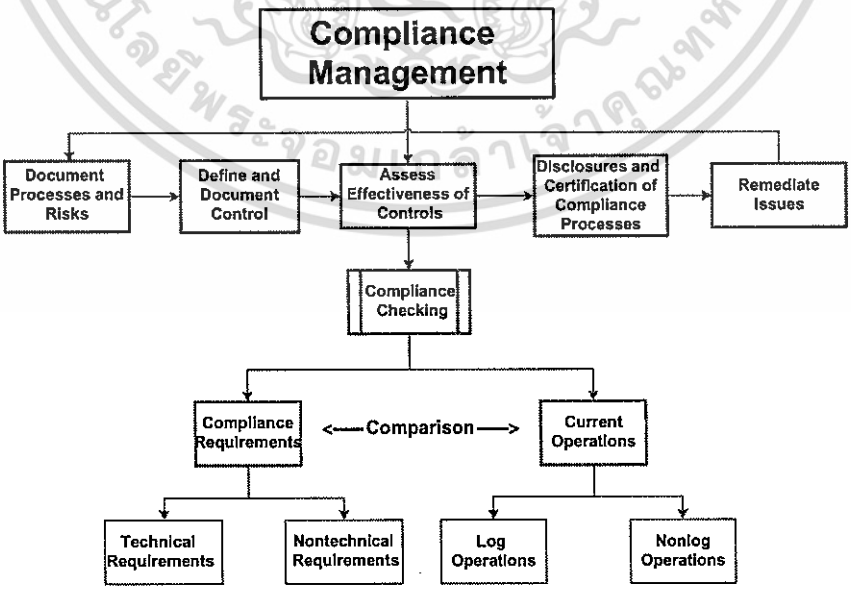


FIGURE 2 Compliance checking framework.

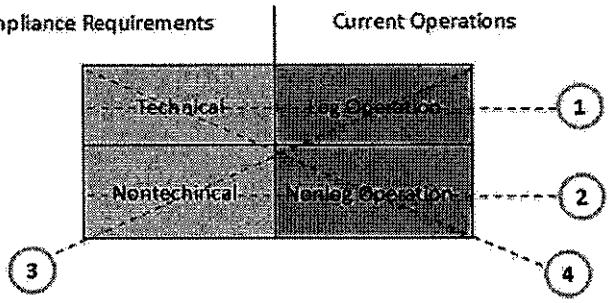


FIGURE 3 The combination of compliance requirements and current operations condition.

traditional computerized systems are not suitable to support such combination and current research generally overlooks this condition. So, the automation level of this condition is still very low.

3. Compliance requirements are in nontechnical form and current operations are log operations. There are many researchers in this condition at this moment, so the automation level of this condition is increasing.
4. Compliance requirements are in technical form and current operations are nonlog operations. This condition is generally overlooked by current research, so the automation level of this condition is still very low.

The approach of this paper is to increase the automation level of combination numbers 2 and 4 which are related to nonlog operations.

Since the compliance requirements are frequently changed and always in human language, the traditional programming codes are not suitable to manage such kind of changes. Therefore, the information extraction process is still carried out manually. The next section discusses about ontology which is a semantic web technology that many researchers have utilized as a tool to improve the automation of information extraction process.

3. ONTOLOGY AND RELATED WORKS

An ontology is an explicit specification of a conceptualization (Gruber, 1995). A conceptualization is the objects, concepts, and other entities that are assumed to exist in some areas of interest and the relationships that hold among them. It is an abstract, simplified view of the world that we wish to represent for some purposes. Ontology represents knowledge in a formal and structured form as well as provides a better communication, reusability and organization of knowledge and a better computational inference.

Ontologies became a famous tool to solve a problem that concern about human language in internet resource especially the e-commerce data. Ali and Maseud (2011) proposed an ontology-based approach for generating virtual catalogs by extracting the product information and product prices from the vendor's website. This approach can help the buyer generate automatic product catalogs from the vendor's website.

Frederick et al. (2007) proposed compliance management methodology using ontology and semantic web rules to encode and formalize linguistic information into machine readable form. The compliance requirements are converted into terms of the domain concepts in OWL ontology and also translated into SWRL rules. This proposal can improve the automated compliance requirement extraction only.

Sapkota, Aldea, Duce, Younas, & Banares-Alcantara (2011) proposed the methodology named RegCMantic by using an ontology to automate the extraction and modelling of regulatory information from various formats and structures such as PDF, text, and HTML into semantic web rules. In their later works, Sapkota, Aldea, Younas, Duce, and Banares-Alcantara (2012, 2011) introduced the Semantic-ART framework, designed to increase the automation of overall CM by extracting regulatory information from text and converting them into a semantic model. We have followed their works and hope that this framework works well to support our part of research that requires the automate extraction of regulation.

Kharbili et al. (2008) introduced the reason why automated compliance checking becomes a necessity for organizations. They proposed the framework for compliance management using a policy-based semantic business process. The framework had been designed to support the transformation of the various levels of policies, and the designed algorithm for compliance checking was executed by the semantic compliance checking engine. In their later

work, Kharbili and Stein (2008) discussed the semantic compliance checking by introducing an ontology for policies and rules. They showed how the ontology for policies and rules look alike, but they had not shown how these ontologies worked in compliance checking.

Schmidt, Bartsch, and Oberhauser (2007) proposed the ontology-based representation of compliance requirements for service processes by defining and comparing two ontologies to discover noncompliant configurations and behavior of business processes. A process ontology is mainly developed to define the activities, resources, and information to cope with problems or incidents found from services that are provided to customers. Another ontology is a compliance ontology that defines objectives that have to be fulfilled by the service process to assure a certain quality of the services provided. From their application scenario, they compared these two ontologies by using the reasoner to discover the noncompliance. We argue that this scenario only discovers the noncompliant configurations in ontology but not yet the noncompliant behavior because there was no service database found in their scenario.

Jiansong and Nora (2011) proposed the automatic information extraction by using ontological feature. In order to extract the information from the sentence, the matching pattern "noun + verb + noun" has been identified. Then, a set of information extraction rules was developed. For example, "Put the first noun as the subject, put the verb as the action, and put the second noun as the object." Then, the rules would extract and put the corresponding parts of sentence into the following classes: subject, action, and object.

Nash et al. (2011) presented the analysis of whether the automation of the compliance checking is possible in agricultural production standards or not. They determined the four criteria to enable automated compliance checking as follows.

1. The rule must be encoded in machine-readable form. It means the wording must be able to be extracted by computerized systems.
2. The rule, and all terms used in defining it, must be capable of being interpreted by the software. It means the wording in rules must exist in the computer dictionary, such as "length," "age," "range," and so forth.
3. Each rule must have a discrete outcome which can be determined by a computer. It means each rule must have data that can be evaluated by computerized systems such as "true/false," numeric, and date/time data.
4. The required data inputs for assessment must be available in digital form at the point of assessment. It means the operation logs should exist in the computerized system.

They proposed the ontologies for agricultural standards and found that the availability of data would be the largest technical problem for automated compliance checking. This motivates us to improve the availability of data that are necessary for the assessment.

Since most of the past researches have already proposed solutions to automate the extraction of regulation into semantic model which fulfil the first three criteria of compliance checking. Therefore, we will focus on the last criteria of compliance checking. However, we still require the success of regulation extraction to accomplish our work.

4. PROPOSED AUTOMATED COMPLIANCE CHECKING METHODOLOGY FOR NONLOG OPERATIONS

In this section we propose a methodology to enable the automation of compliance checking for nonlog operations, which was generally overlooked by past research. Since the nonlog operations are operations that cannot automatically obtain data from computer systems, using questions is one way to gather answers as input to evaluate their compliance. This proposal aims to fulfill all criteria of automated compliance checking especially the fourth criteria that involves availability of data for assessment.

The main concept of our approach is to develop the ontology for automatic extraction of the information from policies and the common questions that auditors ask when performing an audit. Then we map these policies and questions to get the users' answers for compliance evaluation.

From this point onward, the words "policy" and "policies" in this paper will include but not be limited to rules, laws, regulations, procedures, standards, and the like that are used as compliance requirements with auditors' knowledge.

The proposed automated compliance checking methodology for nonlog operations is composed of six main steps. Each step will be explained along with an example as follows.

1. Define the audit component and identify policies. In relation to our previous work (Janpitak & Sathitwiriyawong, 2011), we have selected "Data Center" as an example of audited component. The data center policy which had been developed by consolidating many regulations such as NFPA, ITIL, and ISO/IEC 27000 series are then identified. In order to demonstrate the next step, we would use the example of policy contents in Data Center as follow.
   a. Smoking is not permitted in Data Center.
   b. Emergency lighting shall be installed in all Data Centers.
   c. Type of fire extinguishers
      a. Pressurized water fire extinguisher.
      b. Carbon dioxide (CO_2) fire extinguishers
      c. Clean agent (ABC type rated)
      d. Dry chemical fire extinguishers are prohibited.
   d. Entry and exit doors must be secured by utilizing the Card Access System.
   e. Provide emergency power disconnect switches located inside the computer room at main exit doors.
2. Develop the compliance checking ontology for the audit component domain based on the competency questions as shown in Table 1. In order to carry out this activity, the Protégé ontology editor (Stanford Center for Biomedical Informatics Research, 2015) has been used. The ontology was built in OWL (Web Ontology Language) as shown in Figure 4 and Figure 5. We have to skip the explanation of the process to develop this ontology due to the limitation of page.
3. Develop auditor questions and link to correspondence entities in the compliance checking ontology. The frequent question that is always asked by auditors related to data center had been added into the ontology as shown in Figure 6.
4. Load policy contents into the compliance checking ontology as the initial database. Insert policy contents as defined in step 1 into the compliance checking ontology.
5. Extract policy contents as the knowledge bases. In this step, we would use ontology features and text processing tools to extract information from policy contents that have been loaded in the earlier step. To facilitate an easy understanding, the results from the previous steps have been mapped into the table for each relevant auditor questions as depicted in Table 2.
6. Develop a user-friendly application using semantic web technologies. Since the policy contents, auditor questions, and other information in this knowledge are always constructed in human language, traditional programming codes are not suitable to manage this kind of knowledge. This step is used to develop the semantic queries by using SPARQL (2015) to retrieve data from the ontology. In the later step, semantic web technologies that can connect with ontology such as Jena API should be developed in the user-friendly mode. The completeness of the application depends on the capability of the development team.

TABLE 1 Competency questions

Examples of competency questions
1. What are the questions that auditors always ask when they audit the data center?
2. What are the responses that might be the audit finding for each auditors questions?
3. What should be the valid control that comply to auditors questions?
4. If auditors found the control gaps, what should be done to correct a control?

5. PERFORMANCE EVALUATION

Proof of Concept

To prove that the proposed solution is able to work in the real-world audit environment, following are examples of SPARQL queries that answer the competency questions mentioned in step 6a. The consequence queries and results to reach the compliance checking can be presented as follows.

Competency Question 1. What are questions that auditors always ask when they perform the audit? (Please see the example query in Figure 7)

Competency Question 2. What are responses that might be the audit finding for each auditor questions? (Please see the example query in Figure 8)

Competency Question 3. What should be the valid control that comply to auditors questions? (Please see the example query in Figure 9)

Competency Question 4. If auditors found the control gaps, what should be done to correct a control? (Please see the example query in Figure 10)

The example queries can prove that our ontology can provide the result for the next step to get the answer from auditees. They can also evaluate the answers from auditees then suggest the right policies if the gaps are found.

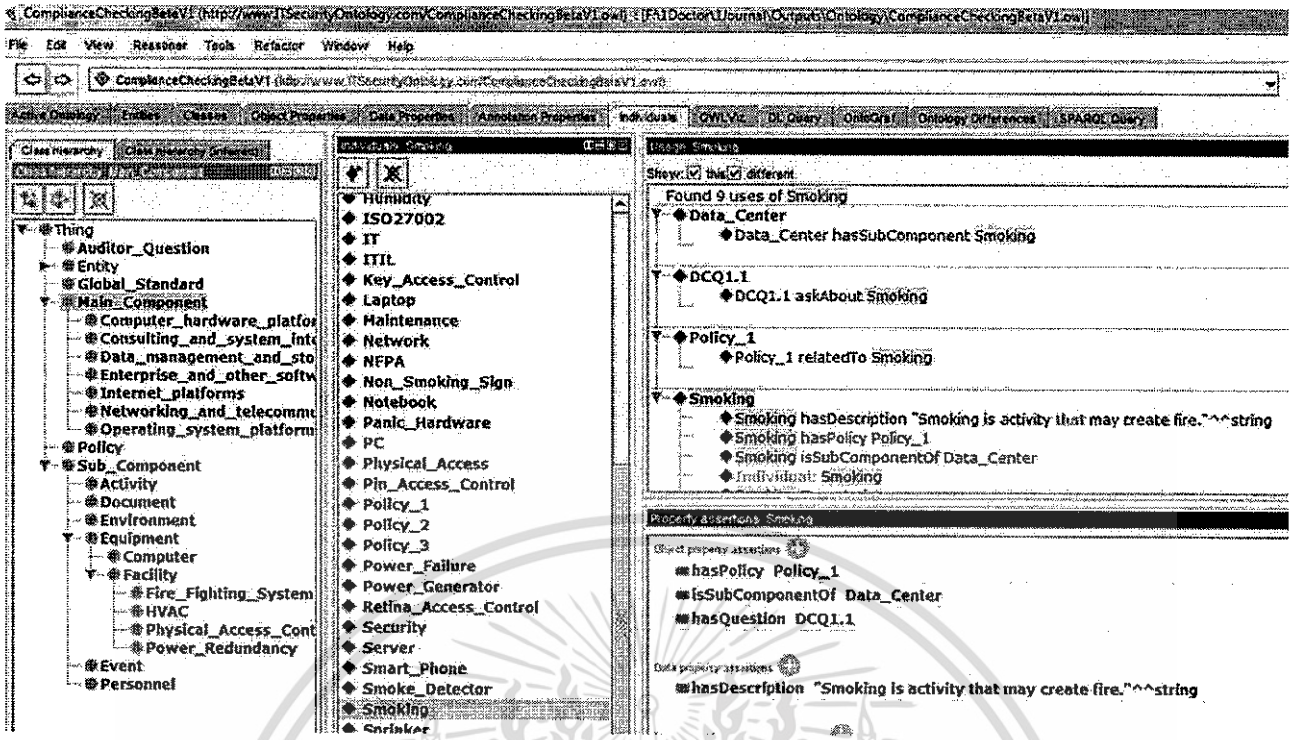


FIGURE 4 Ontology for compliance checking built by protégé.

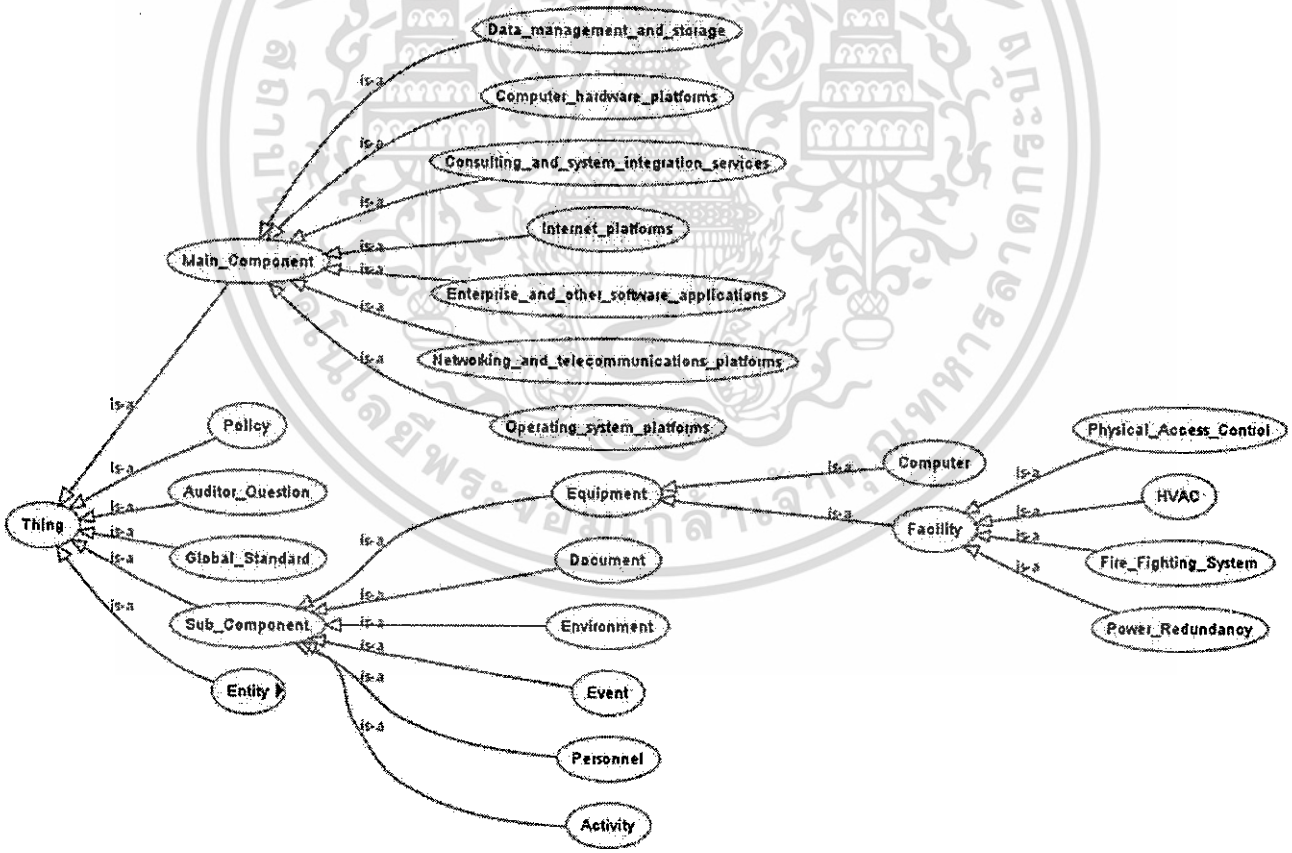


FIGURE 5 OWLviz for compliance checking ontology.

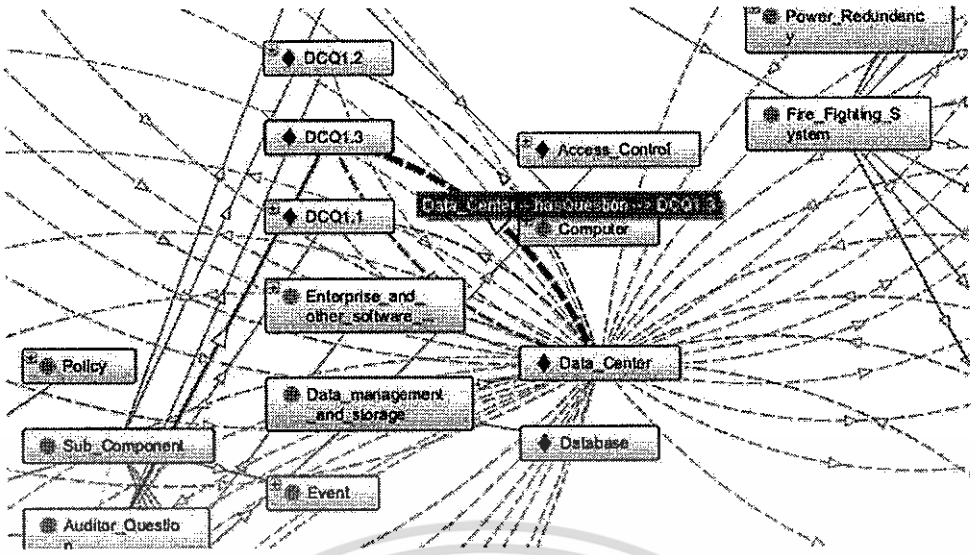


FIGURE 6 OntoGraf for compliance checking ontology.

TABLE 2 Example of policy mapping with auditor questions, compliance lists and non-compliance lists

No.	Policy content	Related to (extracted)	Auditor questions	Compliance lists (extracted)	Noncompliance lists (extracted)
1.	Smoking is not permitted in Data Center.	Smoking/ Data Center	Is a nonsmoking sign put in Data Center?	Yes (Smoking is not permitted)	No (Smoking is permitted)
2.	Emergency lighting shall be installed in all Data Centers. The lighting shall operate automatically in the event of a power failure.	Emergency lighting/ Power failure	Has emergency lighting been installed in Data Center?	Emergency lighting immediately provided	No emergency lighting is provided.
			How is emergency lighting provided in the event of power failure?	Automatically	Manual
3.	Type of Fire Extinguishers Pressurized water fire extinguisher. Carbon dioxide (CO_2) fire extinguishers Clean agent (ABC type rated) Dry chemical fire extinguishers are prohibited	Fire extinguisher	What kinds of fire extinguishers are provided in Data Center?	Pressurized water fire extinguisher Carbon dioxide (CO_2) fire extinguisher Clean agent (ABC type rated)	No water fire extinguisher. No carbon dioxide (CO_2) fire extinguisher. Dry chemical fire extinguishers.
4.	Entry and exiting doors must be secured utilizing the Card Access System	Physical Access	What kind of access control is used at entry door?	Card Access System	Others
5.	Provide emergency power disconnect switches located inside the computer room at main exit doors.	Emergency power disconnect	Does Data Center install emergency power disconnect switch?	Yes	No emergency power disconnect switch.
			Where is emergency power disconnect switch located?	Main exit doors	Others

Query

```
PREFIX CC: <http://www.ITSecurityOntology.com/ComplianceCheckingBetaV1.owl#>
SELECT ?MainComponent ?SubComponent ?Question
WHERE {
?SubComponent CC:isSubComponentOf ?MainComponent.
?SubComponent  CC:hasQuestion ?Q.
?Q CC:hasContent ?Question
}
order by ?MainComponent?SubComponent
```

Results

MainComponent	SubComponent	Question
Data_Center	Emergency_Lighting	How emergency lighting is provided in the event of power failure?
Data_Center	Fire_Extinguisher	What kinds of fire extinguishers are provided in data center?
Data_Center	Power_Failure	How emergency lighting is provided in the event of power failure?
Data_Center	Smoking	How smoking prohibit in data center?

FIGURE 7 Competency question 1.

Query

```
PREFIX CC: <http://www.ITSecurityOntology.com/ComplianceCheckingBetaV1.owl#>
SELECT ?MainComponent ?SubComponent ?Question ?NonCompliance
WHERE {
   ?SubComponent CC:isSubComponentOf ?MainComponent.
   ?SubComponent CC:hasQuestion ?Q .
   ?Q CC:hasContent ?Question .
  ?y  CC:hasNonCompliance_List ?NonCompliance
   FILTER REGEX(?Question,"fire ex")
}
```

Results

MainComponent	SubComponent	Question	NonCompliance
Data_Center	Fire_Extinguisher	What kinds of fire extinguishers are provi...	Dry chemical fire extinguishers

FIGURE 8 Competency question 2.

Query

```
PREFIX CC: <http://www.ITSecurityOntology.com/ComplianceCheckingBetaV1.owl#>
SELECT ?MainComponent ?SubComponent ?Question ?Compliance
WHERE {
   ?SubComponent CC:isSubComponentOf ?MainComponent.
   ?SubComponent CC:hasQuestion ?Q .
   ?Q CC:hasContent ?Question .
  ?y  CC:hasCompliance_List ?Compliance
   FILTER REGEX(?Question,"fire ex")
}
```

Results

MainComponent	SubComponent	Question	Compliance
Data_Center	Fire_Extinguisher	What kinds of fire extinguishers are p...	Clean agent (ABC type rated)
Data_Center	Fire_Extinguisher	What kinds of fire extinguishers are p...	Carbon dioxide (CO_2) fire extinguisher
Data_Center	Fire_Extinguisher	What kinds of fire extinguishers are p...	Water fire extinguisher

FIGURE 9 Competency question 3.

```
Query
PREFIX CC: <http://www.ITSecurityOntology.com/ComplianceCheckingBetaV1.owl#>
SELECT ?SubComponent ?Question ?NonCompliance ?Policy
WHERE {
   ?SubComponent CC:isSubComponentOf ?MainComponent.
   ?SubComponent CC:hasQuestion ?Q .
   ?Q CC:hasContent ?Question .
  ?y  CC:hasNonCompliance_List ?NonCompliance.
  ?SubComponent CC:hasPolicy ?P.
  ?P CC:hasContent ?Policy
   FILTER REGEX(?Question,"fire ex")
}
```

Results

SubComponent	Question	NonCompliance	Policy
Fire_Extinguisher	What kinds of fire extinguishers are provi...	Dry chemical fire extinguishers	Type of Fire Extinguishers:a) 9.5 liter (21/2 gallon) pr...

FIGURE 10 Competency question 4.

Calculation

For easy understanding, we will scope the example calculation of compliance checking in the self-auditing exercise only.

Since the nonlog operations are operations that have no log that can be understood by a computerized system, the compliance checking process requires that operation owners provide answers for the evaluation. It is assumed that the operation owners have no skill in security and control, so they cannot perform the compliance checking without the assessors. An assessor is a person who is an expert in security control including but not limited to internal auditor, external auditor, internal control team, and security control expert. By applying our proposed solution, the operation owners can perform compliance checking without the assessors so that the labor time and cost used to perform the compliance checking is reduced. Moreover, the accuracy of compliance judgment will be improved because this solution can avoid human errors and biased judgments. The labor time reduced by the proposed solution can be estimated by the following equation.

$$\text{Manual labor time} = \sum_{i=0}^{n} (A_i + T_i)$$

$$\text{Proposed solution labor time} = \sum_{i=0}^{n} (T_i)$$

$$\text{Reduced labor time} = \sum_{i=0}^{n} (A_i)$$

when

n = Number of questions

A_i = Assessor labor time of question i

T_i = Operation owner labor time of question i

For the wider scope such as the certified auditing, the operation owners would be called auditees. The assessors would be called auditors.

CONCLUSION

Our proposed solution aims to replace any manual activities that involve the gathering of the audit questions and also the evaluation of answers from the auditees. Since compliance checking is commonly implemented as a standards-based question-answering process, relevant standards and best practices are employed to generate sets of compliance checklist items (questions) to benchmark an organizational adherence (answers) to applicable requirements and expectations (Gruber, 1995). According to this definition, our approach benefits not only the nonlog operations but also the log operations.

REFERENCES

Ali, G., & Maseud, R. (2011). An ontology-based semantic extraction approach for B2C eCommerce. *The International Arab Journal of Information Technology (IAJIT)*, *8*(2), 163–170.

Bace, J., Rozwell, C., Feiman, J., & Kiwin, B. (2006). *Understanding the Costs of Compliance* (Report G00138098). Stamford, CT, USA: Gartner, Inc.

Congress of the United States. (2002). Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley Act). Pub. L. No. 107-204, 116 Stat. 745. Washington DC: U.S. Government Publishing Office.

Frederick, Y., Nandan, P., & Pradeep, R. (2007, October). Rules and ontology in compliance management. In *11th IEEE International Enterprise Distributed Object Computing Conference (EDOC 2007)* (pp. 435–442). Los Alamitos, CA: IEEE.

Greengard, S. (2004). Compliance software's bonus benefits. *Business Finance Magazine*. Retrieved from http://businessfinancemag.com/technology/compliance-softwares-bonus-benefits

Gruber, T. R. (1995). Toward principles for the design of ontologies used for knowledge sharing? *International Journal of Human-Computer Studies, 43*, 907–928. doi:10.1006/ijhc.1995.1081

Janpitak, N., & Sathitwiriyawong, C. (2011, July). Data center physical security ontology for automated evaluation. *The 2011 International Conference on Security and Management (SAM2011)*, 78–84. Las Vegas, NV, USA: WORLDCOMP.

Jiansong, Z., & Nora, E. (2011, October). Automated information extraction from construction-related regulatory documents for automated compliance checking. In *Proceedings of the CIB W78-W102*. Washington, USA: International Council for Research and Innovation in Building and Construction.

John, R. (2009). *Computer and information security handbook*. Atlanta, GA, USA: Elsevier.

Kharbili, M., Stein, S., Markovic, I., & Pulvermüller, E. (2008, June). Towards a framework for semantic business process compliance management. *Proceedings of the GRCIS, Caise Workshop on Governance, Risk and Compliance of Information Systems*. Phoenix, AZ, USA: CEUR Workshop.

Kharbili, M., & Stein, S. (2008, November). Policy-based semantic compliance checking for business process management. *Proceedings of the MobIS Workshops*, 178–192. Aachen, Germany: CEUR Workshop Proceedings.

Nash, E., Wiebensohn, J., Nikkilä, R., Vatsanidou, A., Fountas, S., & Bill, R. (2011). Towards automated compliance checking based on a formal representation of agricultural production standards. *Computers and Electronics in Agriculture, 78*, 28–37. doi:10.1016/j.compag.2011.05.009

Sapkota, K., Aldea, A., Duce, D., Younas, M., & Banares-Alcantara, R. (2011, October). Towards semantic methodologies for automatic regulatory compliance support. *PKM'11 Proceedings of the 4th Workshop on Workshop for Ph.D. Students in Information & Knowledge Management*, 83–86. New York: ACM.

Sapkota, K., Aldea, A., Younas, M., Duce, D., & Banares-Alcantara, R. (2012). Extracting meaningful entities from regulatory text: Towards automating regulatory compliance. *Proceedings of the 5th International Workshop on Requirements Engineering and Law*, pp. 29–32.

Sapkota, K., Aldea, A., Younas, M., Duce, D., & Banares-Alcantara, R. (2011, October). Semantic-ART: A framework for semantic annotation of regulatory text. *ESAIR'11 Proceedings of the 4th Workshop on Exploiting Semantic Annotations in Information Retrieval*, 23–24. New York: ACM.

Schmidt, R., Bartsch, C., & Oberhauser, R. (2007, April). Ontology-based representation of compliance requirements for service processes. *Proceedings of the Workshop on Semantic Business Process and Product Lifecycle Management*. Phoenix, AZ, USA: CEUR Workshop.

SPARQL. (2015). *SPARQL Query Language for RDF*. Retrieved from http://www.w3.org/TR/rdf-sparql-query/

Stanford Center for Biomedical Informatics Research. (2015). *The Protégé Ontology Editor and Knowledge Acquisition System*. Retrieved from http://protege.stanford.edu

Tarantino, A. (2008). *Governance, risk, and compliance handbook*. New Jersey, USA: Wiley.

BIOGRAPHIES

Nanta Janpitak got her BSc in Mathematics from Burapha University in 1993 and her MSc in Information Technology from Mahanakorn University of Technology, Thailand in 2007. She is currently pursuing her PhD in Information Technology at King Mongkut's Institute of Technology Ladkrabang. Her research interests are in information security, audit, and compliance.

Chanboon Sathitwiriyawong got his Bachelor Degree in Electrical Engineering from Prince of Songkla University, Thailand in 1986. He earned his MSc in Data Tele-communications and Networks in 1993 and his PhD in Electronic and Electrical Engineering from the University of Salford, United Kingdom in 1996. He is an associate professor of Information Technology and the Dean of the Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang. His current research interests are in the area of computer network, and network and system security. He is a member of the IEEE Communication Society.