ระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 กรมโรงงานอุตสาหกรรม

INFORMATION SECURITY MANAGEMENT SYSTEM ISO / IEC 27001 DEPARTMENT OF INDUSTRIAL WORKS

โดย

ธงชัย อุทัยจรัสรัศมี

THONGCHAI UTAIJARASRATSAMEE

อาจารย์ที่ปรึกษา

รศ.ดร. วรพจน์ กรีสุระเดช

รายงานนี้เป็นส่วนหนึ่งของวิชาการศึกษาอิสระ
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 1 ปีการศึกษา 2553

INFORMATION SECURITY MANAGEMENT SYSTEM ISO / IEC 27001

DEPARTMENT OF INDUSTRIAL WORKS

THONGCHAI UTAIJARASRATSAMEE

A REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

OF THE COURSE

INDEPENDENT STUDY

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

1/ 2010

ใบรับรองการศึกษาอิสระ (INDEPENDENT STUDY)

เรื่อง

ระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 กรมโรงงานอุตสาหกรรม

Information Security Management System ISO / IEC 27001 Department of Industrial Works

นายธงชัย อุทัยจรัสรัศมี

รหัสประจำตัว 51066616

ขอรับรองว่ารายงานฉบับนี้ ข้าพเจ้าไม่ได้คัดลอกมาจากที่ใด
รายงานฉบับนี้ได้รับการตรวจสอบและอนุมัติให้เป็นส่วนหนึ่งของ
การศึกษาวิชาการศึกษาอิสระ หลักสูตรวิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศ)
ภาคเรียนที่ 1 ปีการศึกษา 2553

.....อาจารย์ที่ปรึกษา

(รศ.ดร. วรพจน์ กรีสุระเดช)

.....กรรมการสอบ

(รศ.ดร. อาริต ธรรมโน)

หัวข้อ	ระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 กรมโรงงานอุตสาหกรรม
นักศึกษา	นายธงชัย อุทัยจรัสรัศมี
รหัสนักศึกษา	51066616
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2553
อาจารย์ที่ปรึกษา	รศ.ดร. วรพจน์ กรีสุระเดช

บทคัดย่อ

มาตรฐานความปลอดภัยสารสนเทศ ISO/IEC 27001 เป็นมาตรฐานสากลที่มีจุดประสงค์เพื่อจะทำให้องค์กรสามารถบริหารจัดการทางด้านความปลอดภัยของสารสนเทศได้อย่างมีระบบ และเพียงพอเหมาะสมต่อการดำเนินธุรกิจขององค์กร โดยเริ่มจากการวิเคราะห์ความเสี่ยงของระบบจากภัยคุกคามและจุดอ่อนต่างๆ ทั้งภายในและภายนอก จากนั้นจึงเลือกแนวทางและกำหนดวิธีการควบคุมและป้องกัน ระบบมาตรฐานความปลอดภัย ISO / IEC 27001 มีแนวทางที่เรียกว่า Code of Practice ให้ผู้ใช้ได้ใช้งาน เพื่อควบคุมความเสี่ยงต่างๆ ขณะเดียวกันมาตรฐานก็ยังกำหนดให้ต้องควบคุมดูแลระบบการรักษาความมั่นคงปลอดภัยและมีการพัฒนาระบบอย่างต่อเนื่องอีกด้วย โดยโครงการนี้เป็นการออกแบบระบบงาน สำหรับนำมาใช้ในการควบคุมตรวจสอบการปฏิบัติตามมาตรฐานความปลอดภัย ISO/IEC 27001 และยังใช้ในการติดตามผลการตรวจสอบ จัดทำผลสรุปรายงานต่างๆ ให้แก่ผู้บริหารอีกด้วย

Title	Information Security Management System ISO/IEC 27001 Department of Industrial Works
Student	Mr. Thongchai Utaijarasratsamee
Student ID.	51066616
Degree	Master of Science
Program	Information Technology
Major	Information Technology Management
Academic Year	2010
Advisor	Associate Professor Dr. Worapoj Kreesuradej

ABSTRACT

Information Security Management System ISO/IEC27001 is the international standard which refers to the standard of the management for information security. The purpose of this standard is to make the organization manage about the security systematically and properly for the organization's business. For the beginning, the organization has to analysis the risk of system from the harm and weakness in the system and then try to find and choose the best way to control and protect the system properly. There will be the method called Code of Practice to be used to control the risk and determine the organization to control the security system and develop it continually. The purpose of this project is to design an application used for the control, to monitor of the compliance with safety standard ISO / IEC 27001, to track the results of the audit and to prepare summary reports for executives.

กิตติกรรมประกาศ

โครงการศึกษากรณีพิเศษนี้ สำเร็จได้จากความรู้ที่ได้รับการถ่ายทอดจากอาจารย์ทุกท่าน โดยเฉพาะอย่างยิ่งขอขอบพระคุณ รศ.ดร. วรพจน์ กรีสุระเดช เป็นอย่างสูงสำหรับคำแนะนำและข้อคิดเห็นรวมถึงการชี้แนะแนวทางต่างๆ ที่เป็นประโยชน์ในการพัฒนาระบบงานนี้ทุกขั้นตอน

ผู้จัดทำขอขอบพระคุณผู้บริหารศูนย์สารสนเทศโรงงานอุตสาหกรรม กรมโรงงานอุตสาหกรรม และเพื่อนทุกท่าน สำหรับการสนับสนุนและให้กำลังใจในการศึกษาจัดทำโครงการศึกษากรณีพิเศษนี้ และขอพระขอบคุณ ผอ.เสรี อติภัทธะ เป็นอย่างสูงที่ช่วยให้คำปรึกษาแนะนำและสนับสนุนด้วยดีตลอดมา

ธงชัย อุทัยจรัสรัศมี

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญปัญหา

กรมโรงงานอุตสาหกรรม เป็นหน่วยงานภาครัฐที่มีภารกิจในการกำกับดูแล และสนับสนุนผู้ประกอบกิจการอุตสาหกรรม โดยมุ่งเน้นภารกิจด้านความปลอดภัยและสิ่งแวดล้อม ในขณะเดียวกันก็ส่งเสริมและสนับสนุนให้ผู้ประกอบการมีศักยภาพในการแข่งขันที่สูง กรมโรงงานอุตสาหกรรมได้นำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในภารกิจตามที่กล่าวมาแล้วข้างต้น โดยในปัจจุบันการทำงานต่างๆ ของเจ้าหน้าที่ เช่น การตรวจสอบโรงงาน รายงานผลการวิเคราะห์มลพิษ ระบบสารบรรณ ระบบการอนุญาตต่างๆ จะดำเนินการบนระบบคอมพิวเตอร์ ซึ่งเป็นที่มาของข้อมูล จากข้อมูลที่ได้มานี้ ศูนย์สารสนเทศโรงงานอุตสาหกรรมได้นำมาแปรเปลี่ยนเป็นสารสนเทศทางอุตสาหกรรมเพื่อให้บริการแก่เจ้าหน้าที่ ผู้ประกอบการ และประชาชนทั่วไป โดยการให้บริการนี้ในอดีตที่ผ่านมาได้มีอุปสรรคเกิดขึ้นจากระบบสารสนเทศมาโดยตลอด เช่น ระบบไม่สามารถตอบสนองผู้ใช้งานได้ตลอดเวลาเนื่องจากเซิร์ฟเวอร์ขัดข้อง ระบบถูกบุกรุกจากภายนอกหรือจากภายใน ดังนั้นกรมโรงงานอุตสาหกรรม จึงได้นำมาตรฐานความปลอดภัยของข้อมูล ISO/IEC 27001 มารองรับการให้บริการที่มีมาตรฐานอันเป็นการนำไปสู่การให้บริการที่มีความยั่งยืนและปลอดภัย

ในปี พ. ศ. 2552 กรมโรงงานอุตสาหกรรมได้จัดทำระบบมาตรฐานความปลอดภัยของข้อมูล ISO/IEC 27001 ที่ศูนย์สารสนเทศโรงงานอุตสาหกรรม เพื่อใช้เป็นกลไกในการพัฒนาระบบเทคโนโลยีสารสนเทศ อันนำไปสู่การบริการแก่ผู้ประกอบกิจการและประชาชนที่มีคุณภาพได้มาตรฐาน โดยจะมุ่งเน้นให้ความสำคัญด้านความปลอดภัยของข้อมูล ระบบการให้บริการ ระบบสำรองฉุกเฉิน รวมทั้งระบบการบำรุงรักษาอุปกรณ์ ฮาร์ดแวร์ ซอฟแวร์และระบบเครือข่าย โดยทั้งนี้ให้ตั้งอยู่บนพื้นฐานตามมาตรฐานความปลอดภัย ISO/IEC 27001

อย่างไรก็ตามแม้ว่ามาตรฐานความปลอดภัย ISO/IEC 27001 ได้ถูกจัดทำขึ้นแล้วเสร็จ หากขาดการดูแลอย่างต่อเนื่องจะทำให้ระบบขาดความมีเสถียรภาพ ดังนั้นจึงได้ออกแบบและจัดทำระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 กรมโรงงานอุตสาหกรรม เพื่อนำมาใช้ในการควบคุมตรวจสอบการปฏิบัติตามมาตรฐานความปลอดภัย ISO/IEC 27001 และใช้ในการติดตามผลการตรวจสอบ จัดทำผลสรุปรายงานต่างๆ ให้แก่ผู้บริหาร

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

การจัดทำระบบบริหารความปลอดภัยข้อมูลสารสนเทศ ISO/IEC 27001 มีวัตถุประสงค์ดังต่อไปนี้

- เพื่อออกแบบระบบต้นแบบระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 กรมโรงงานอุตสาหกรรม
- เพื่อนำระบบต้นแบบมาใช้ในการควบคุมตรวจสอบการปฏิบัติตามมาตรฐานความปลอดภัย ISO/IEC 27001 และยังใช้ในการติดตามผลการตรวจสอบ จัดทำผลสรุปรายงานต่างๆ

1.3 ขอบเขตของการศึกษา

- ระบบงานต้นแบบ ที่จะทำการออกแบบขึ้นจะตั้งอยู่บนข้อกำหนดตามมาตรฐานความปลอดภัยของข้อมูล ISO/IEC 27001

1.4 ขั้นตอนของการศึกษา

ขั้นตอนการศึกษาของโครงการได้กำหนดขั้นตอนการดำเนินการไว้ดังนี้

1. วางแผนโครงการ โดยในการวางแผนได้ทำการศึกษาถึงปัญหา ศึกษาความต้องการ และศึกษาวิเคราะห์ความเป็นไปได้ของระบบในแง่มุมต่างๆ เป็นการค้นหาข้อสรุปและขอบเขตของปัญหา จากนั้นจัดทำรายงานแผนโครงการข้อเสนอยื่นแก่ผู้บริหารเพื่อยืนยันถึงโครงการระบบงานใหม่
2. ศึกษาความเป็นไปได้ทางด้านเทคนิค เป็นการศึกษาเพื่อประเมินทรัพยากรขององค์กรที่มีอยู่ในปัจจุบันทั้งฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย บุคลากร รวมถึงด้านข้อมูล ซึ่งในปัจจุบันมีระบบอินเทอร์เน็ต ระบบเครือข่าย เซิร์ฟเวอร์และเว็บใช้งานอยู่แล้ว ส่วนเครื่องคอมพิวเตอร์ที่มีใช้งานอยู่ทุกเครื่องสามารถรองรับการใช้งานอินเทอร์เน็ตได้
3. ศึกษาความเป็นไปได้ด้านการดำเนินงาน เป็นการศึกษาความเป็นไปได้ของการปฏิบัติงานผ่านระบบใหม่ ซึ่งยังไม่มีการทำงานผ่านระบบคอมพิวเตอร์มาเป็นการทำงานผ่านเว็บ มีความเป็นไปได้สูง เนื่องจากเป็นการเปลี่ยนแปลงที่ก่อให้เกิดประโยชน์กับผู้ปฏิบัติงาน ให้สามารถปฏิบัติงานได้สะดวกรวดเร็ว สามารถใช้งานได้ง่าย และคาดว่าจะได้รับความร่วมมือจากเจ้าหน้าที่ภายในกรมโรงงานอุตสาหกรรมเป็นอย่างดีทำให้สามารถนำระบบมาใช้งานได้อย่างสมบูรณ์
4. ศึกษาวิเคราะห์รูปแบบข้อกำหนดต่างๆ ของมาตรฐาน ISO/IEC 27001 และสำรวจระบบเบื้องต้นเพื่อเก็บข้อมูลพื้นฐานขององค์กร เพื่อนำมาออกระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 กรมโรงงานอุตสาหกรรม
5. จัดสร้างและวิเคราะห์ออกแบบระบบงานต้นแบบ (Prototype)

1.5 แผนการดำเนินงาน

การจัดทำแผนการดำเนินงานของการออกแบบระบบงานกำหนดไว้ 4 เดือน ซึ่งมีรายละเอียดดังต่อไปนี้

ตารางที่ 1.1 แผนการดำเนินงานของระบบ

Project Plan																
Task	**เดือน1**				**เดือน2**				**เดือน3**				**เดือน4**			
	1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
1. วางแผน (Planning) - ระบุปัญหา (Identifying Problem) - ความต้องการของระบบ (System Request) -วิเคราะห์ความเป็นไปได้(Feasibility Analysis)																
2. วิเคราะห์ระบบ (System Analysis) - รวบรวมความต้องการ (Requirement Gathering) - แนวคิดการออกแบบระบบ (Design System Concepts) -สร้างแบบจำลองความต้องการ (Requirement Modeling) -สร้างแบบจำลองโครงสร้าง (Structural Modeling) -สร้างแบบจำลองพฟติกรรม (Behavioral Modeling)																
3. ออกแบบระบบ (System Design) - ออกแบบฐานข้อมูล (Database Design) - ออกแบบส่วนติดต่อผู้ใช้ (User Interface Design)																

1.6 ประโยชน์ที่คาดว่าจะได้รับ

ในการจัดทำระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 ผู้จัดทำคาดว่ากรมโรงงานอุตสาหกรรมจะได้รับดังนี้

- การให้บริการงานของศูนย์สารสนเทศโรงงานอุตสาหกรรมสามารถให้บริการได้อย่างต่อเนื่อง
- ผู้รับบริการมีความมั่นใจในความถูกต้องของข้อมูลและมั่นใจการเข้าใช้งานของระบบ
- กรมโรงงานอุตสาหกรรม สามารถดำเนินการตามพันธกิจได้อย่างต่อเนื่อง

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

ในการศึกษาและพัฒนาระบบงานจะต้องอาศัยทฤษฎีและเทคโนโลยีสารสนเทศต่างๆ มาประยุกต์ใช้ให้เหมาะสม เพื่อให้สามารถออกแบบและพัฒนาระบบใหม่ได้อย่างมีประสิทธิภาพตรงกับความต้องการของผู้ใช้ โดยสามารถนำไปใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพมากที่สุด ดังนั้นจึงได้นำทฤษฎีและเทคโนโลยีที่เกี่ยวข้องมาประยุกต์ใช้ในการพัฒนาระบบงาน โดยสรุปได้ดังนี้

2.1 ยูเอ็มแอล

ยูเอ็มแอล เป็นโมเดลมาตรฐานที่ใช้หลักการออกแบบเชิงวัตถุ รูปแบบของยูเอ็มแอลจะมีสัญลักษณ์ที่นำไปใช้ในโมเดลต่างๆ โดยมีข้อกำหนดในโปรแกรมและข้อกำหนดนั้นจะมีความหมายต่อการเขียนโปรแกรม ดังนั้นการใช้ ยูเอ็มแอลจะต้องทราบความหมายของสัญลักษณ์ต่างๆ เช่น Generalize, Association, Dependency, Class และ Package ซึ่งมีความจำเป็นอย่างยิ่งต่อการตีความในการออกแบบระบบก่อนนำไปใช้งานจริง ในปัจจุบันมีเครื่องมือมากมายที่สามารถแปลงโมเดลยูเอ็มแอลเป็นโค้ดภาษาต่างๆ ได้ เช่น ภาษาจาวา และ วิชวลเบสิก เป็นต้น
(บรรจง หะรังษี และญาณวรรณ สินธุภิญโญ . 2548)

ยูเอ็มแอล เป็นรูปแบบเสมือนโครงสร้าง ซึ่งจะทำหน้าที่ในการแสดงโครงสร้าง การทำงานของซอฟต์แวร์ให้ออกมาในรูปแบบที่สามารถมองเห็นได้ โดยการสื่อให้ออกมาในรูปของไดอะแกรมรูปภาพ ด้วยวิธีการแบบนี้จะทำให้การพัฒนารูปแบบและการเขียนโปรแกรมมีความสอดคล้องกันอย่างมีประสิทธิภาพ ซึ่งไดอะแกรมต่างๆ ประกอบด้วย

2.1.1 ยูสเคสไดอะแกรม เป็นไดอะแกรมที่ใช้แสดงเป็นแผนภาพที่อธิบายถึงการปฏิสัมพันธ์ระหว่างระบบงานกับสิ่งที่อยู่นอกระบบงาน เป็นเครื่องมือให้ผู้ใช้ระบบสามารถสื่อสารให้ผู้ออกแบบระบบได้รับรู้ว่าผู้ใช้ต้องการระบบในลักษณะไหน ข้อดีของยูสเคสไดอะแกรม คือทำให้เห็นชัดว่าขอบเขตของระบบมีอยู่แค่ไหน โดยยูสเคสไดอะแกรมประกอบด้วย

1. แอกเตอร์ ใช้สัญลักษณ์เป็นรูปคน หมายถึงผู้ที่ใช้งานระบบหรือระบบงานก็ได้

2. ยูสเคส ใช้สัญลักษณ์เป็นรูปวงรี หมายถึงกิจกรรมหลักของระบบที่จะเกิดขึ้นในระบบในมุมมองของผู้ใช้งาน

3. ความสัมพันธ์ ใช้สัญลักษณ์เป็นเส้นลูกศร ซึ่งแสดงถึงความสัมพันธ์ระหว่างยูสเคสกับยูสเคส หรือความสัมพันธ์ระหว่างยูสเคสกับแอกเตอร์

4. ขอบเขตระบบ ใช้สัญลักษณ์สี่เหลี่ยม หมายถึงเส้นแบ่งขอบเขตระหว่างระบบกับผู้กระทำต่อระบบ

2.1.2 แอกทิวิตีไดอะแกรม เป็นไดอะแกรมที่แสดงให้เห็นถึงลำดับการดำเนินกิจกรรม จากกิจกรรมหนึ่งไปอีกกิจกรรมหนึ่งภายในระบบ สัญลักษณ์ที่ใช้แสดงในแอกทิวิตีไดอะแกรม ประกอบด้วย

- จุดเริ่มต้น ใช้สัญลักษณ์วงกลมทึบ เป็นจุดเริ่มต้นของกิจกรรม
- กิจกรรม ใช้สัญลักษณ์สี่เหลี่ยมขอบมน โดยมีคำอธิบายกิจกรรมไว้ภายใน
- การตัดสินใจ ใช้สัญลักษณ์สี่เหลี่ยมข้าวหลามตัด ตัดสินใจใช่หรือไม่ใช่
- จุดสิ้นสุด ใช้สัญลักษณ์วงกลมโปร่งล้อมรอบวงกลมทึบ แสดงจุดสิ้นสุดของกิจกรรม

2.1.3 คลาสไดอะแกรม เป็นแผนภาพที่ใช้ในการแสดงกลุ่มของคลาส โครงสร้างของคลาส ตลอดจนความสัมพันธ์ระหว่างคลาส โดยการแสดงความสัมพันธ์จะใช้สัญลักษณ์เป็นเส้นตรงเชื่อมระหว่างคลาส มีการเขียนถึงบทบาทความสัมพันธ์ และมีการกำหนดตัวเลขความสัมพันธ์เป็นตัวเลขหรือช่วงของตัวเลขในรูปแบบค่าต่ำสุดและค่าสูงสุดไว้ที่ด้านปลายของเส้นแสดงความสัมพันธ์ ถ้าเป็นตัวเลขจำนวนเดียว หมายถึงค่าที่แน่นอน ถ้าเป็นช่วง หมายถึงค่าที่เป็นไปได้ ถ้าหมายถึงจำนวนใดๆ ใช้สัญลักษณ์ดอกจัน (*)

2.1.4 ซีเควนซ์ไดอะแกรม เป็นแผนภาพที่ใช้อธิบายปฏิสัมพันธ์ระหว่างอ็อบเจกต์ของคลาส ซึ่งส่งข้อความระหว่างอ็อบเจกต์ที่โต้ตอบกันตามลำดับ ซีเควนซ์ไดอะแกรมจะแสดงในรูปแบบ 2 มิติ โดยมีเส้นประแนวตั้งนำเสนอในด้านเวลา และด้านแนวนอนนำเสนอเกี่ยวกับการโต้ตอบระหว่างคลาสต่างๆ ซีเควนซ์ไดอะแกรมประกอบด้วย

- อ็อบเจกต์ ใช้สัญลักษณ์สี่เหลี่ยมผืนผ้า ซึ่งจะมีชื่อคลาสอยู่ภายใน และจะแสดงอยู่ส่วนบนสุดของซีเควนซ์ไดอะแกรม
- เส้นอายุขัย ใช้สัญลักษณ์เส้นประ แสดงช่วงเวลาตั้งแต่อ็อบเจกต์ของคลาสข้างบนมีปฏิสัมพันธ์กับอีกอ็อบเจกต์หนึ่ง
- จุดควบคุม ใช้สัญลักษณ์สี่เหลี่ยมผืนผ้าวางทับเส้นประ แสดงช่วงเวลาที่อ็อบเจกต์ มีการรับหรือส่งข้อความ
- เมสเสจหรือข้อความ ใช้สัญลักษณ์เส้นลูกศรที่มีข้อความหรือเมสเสจอยู่บนเส้นลูกศรเพื่ออธิบายคำสั่งสั้นๆ ระหว่างอ็อบเจกต์

2.1.5 สเตทชาร์ตไดอะแกรม เป็นแผนภาพที่แสดงการเปลี่ยนแปลงสถานะของอ็อบเจกต์หนึ่งตั้งแต่เริ่มต้นจนสิ้นสุด โดยสัญลักษณ์ต่างๆ ที่ใช้ในสเตทชาร์ตไดอะแกรมประกอบด้วย

- จุดเริ่มต้นของสถานะใช้สัญลักษณ์วงกลมทึบ แสดงถึงจุดเริ่มต้นการเปลี่ยนแปลงสถานะ
- สถานะของการทำงานใช้สัญลักษณ์รูปสี่เหลี่ยมขอบมน แสดงถึงสถานะของทำงาน

- จุดสิ้นสุดของสถานะใช้สัญลักษณ์วงกลมโปร่งล้อมรอบวงกลมทึบแสดงจุดสิ้นสุดการเปลี่ยนแปลงของสถานะ

- เส้นกระตุ้นให้เปลี่ยนสถานะใช้สัญลักษณ์เส้นลูกศร ซึ่งจะมีเหตุการณ์บอกอยู่บนเส้นแสดงเหตุการณ์ต่างๆ ที่มากระทำให้อ็อบเจกต์นั้นมีการเปลี่ยนสถานะ

2.2 อี-อาร์โมเดล

ในการออกแบบฐานข้อมูลด้วย อี-อาร์โมเดล จำเป็นต้องศึกษาคุณสมบัติและความสัมพันธ์ระหว่างข้อมูลที่มีอยู่ในระบบ เพื่อให้ได้มาซึ่งโครงสร้างพื้นฐานของฐานข้อมูล ซึ่งโดยทั่วไปจะดำเนินการโดยการใช้แบบจำลองข้อมูล (วิเชียร เปรมชัยสวัสดิ์. 2547 : 61)

อี-อาร์โมเดล เป็นแบบจำลองข้อมูลที่ได้รับความนิยมมาก ในการใช้เป็นเครื่องมือสำหรับงานออกแบบฐานข้อมูล โดยอี-อาร์โมเดลจะเสนอโครงสร้างของฐานข้อมูลในระดับแนวคิดออกมาในรูปของแผนภาพที่มีโครงสร้างง่ายต่อการทำความเข้าใจ ทำให้เห็นภาพรวมของเอนทิตีทั้งหมดและความสัมพันธ์ระหว่างเอนทิตีในระบบฐานข้อมูล

ขั้นตอนการออกแบบฐานข้อมูลด้วยอี-อาร์โมเดล

การออกแบบฐานข้อมูลด้วยอี-อาร์โมเดลประกอบด้วยขั้นตอนต่างๆ ดังนี้คือ

1. การศึกษารายละเอียดและลักษณะหน้าที่งานของระบบ เป็นการศึกษาและรวบรวมรายละเอียดเกี่ยวกับลักษณะหน้าที่งานของระบบ ข้อมูลที่เกี่ยวข้อง ขั้นตอนในการทำงาน ตลอดจนข้อกำหนดและสมมติฐานต่างๆ ซึ่งอาจทำได้ด้วยการสัมภาษณ์หรือศึกษาจากแบบฟอร์มต่างๆ ที่มีการใช้งานอยู่ในระบบงานขณะนั้น

2. การกำหนดเอนทิตีที่ควรมีในระบบฐานข้อมูล เนื่องจากฐานข้อมูลหนึ่งๆ อาจประกอบด้วยเอนทิตีต่างๆ ได้จำนวนมาก ดังนั้นขั้นตอนนี้จึงเป็นการนำรายละเอียดในข้อ 1 มาทำการกำหนดเอนทิตีที่จำเป็นต้องมีอยู่ในระบบฐานข้อมูล โดยคำนึงถึงการเป็นเอนทิตีประเภทอ่อนแอ ตลอดจนซุปเปอร์ไทร์หรือซับไทร์ด้วย

3. การกำหนดความสัมพันธ์ระหว่างเอนทิตี เป็นการกำหนดประเภทของความสัมพันธ์ระหว่างเอนทิตี โดยพิจารณาจากข้อกำหนดและสมมติฐานต่างๆ ที่ได้ทำการศึกษามาในข้อ 1

- การกำหนดคุณลักษณะของเอนทิตีเป็นการกำหนดว่าแต่ละเอนทิตีควรประกอบด้วยพรอพเพอร์ตีใดบ้าง พรอพเพอร์ตีใดที่มีคุณสมบัติเป็นคีย์พรอพเพอร์ตีหรือคอมโพสิต พรอพเพอร์ตีหรือดีไรฟด์ พรอพเพอร์ตี

- การกำหนดคีย์หลักของแต่ละเอนทิตี เป็นการกำหนดคีย์พร็อพเพอร์ตีของแต่ละเอนทิตีเพื่อให้แต่ละสมาชิกในเอนทิตีสามารถมีคุณสมบัติเป็นเอกลักษณ์เฉพาะได้

- การนำสัญลักษณ์ที่ใช้ในอี-อาร์โมเดลมาอธิบายความสัมพันธ์ระหว่างข้อมูล การนำสัญลักษณ์ที่ใช้ในอี-อาร์โมเดลมาอธิบายความสัมพันธ์ระหว่างข้อมูล เป็นการนำรายละเอียดใน

ขั้นตอนต่างๆ มาพิจารณาทบทวนเพื่อเพิ่มหรือลดเอนทิตี พรอพเพอร์ตีและความสัมพันธ์ต่างๆ จากนั้นจึงนำข้อมูลที่ได้จากขั้นตอนทั้งหมดมาเขียนเป็นแบบจำลอง เพื่ออธิบายความสัมพันธ์ระหว่างข้อมูลด้วยสัญลักษณ์ต่างๆ หรืออี-อาร์ไดอะแกรม ดังนั้นแบบจำลองข้อมูลที่เกิดขึ้นจึงมีความชัดเจน สอดคล้อง ถูกต้องและเหมาะสมกับองค์ประกอบของงานที่กำลังศึกษาทำให้เป็นที่ยอมรับของทุกฝ่ายที่เกี่ยวข้อง

2.3 เอเอสพี

เอเอสพี ย่อมาจาก Active Server Page เป็นภาษาที่ใช้ในการพัฒนาโปรแกรม ที่คิดค้นโดยบริษัทไมโครซอฟต์ ซึ่งเป็นภาษาทางโปรแกรมที่ทำงานในฝั่งของเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์ที่ให้บริการเอกสารหรือสื่อต่างๆ ในอินเทอร์เน็ตหรืออินทราเน็ต

2.3.1 หลักการทำงานของเอเอสพี

เอเอสพี ทำงานบนเซิร์ฟเวอร์ร่วมกับโปรแกรมเว็บเซิร์ฟเวอร์ จะทำหน้าที่ประมวลข้อมูลที่ได้จากผู้เข้ามาเยี่ยมชมและแสดงผลออกมาทางเว็บบราวเซอร์เริ่มจากผู้ใช้เอเอสพีสร้างไฟล์ที่มีนามสกุลเป็น .ASP ขึ้นมา จากนั้นนำไฟล์นั้นไปไว้ในเครื่องคอมพิวเตอร์ ที่ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์ที่ติดตั้งโปรแกรมเอเอสพีไว้ และเชื่อมต่ออยู่กับเครือข่ายอินเทอร์เน็ต จากนั้นเมื่อมีผู้ใช้รายใดเรียกใช้ไฟล์นั้นผ่านโปรแกรมบราวเซอร์ โปรแกรมเอเอสพีในเว็บเซิร์ฟเวอร์ จะเรียกไฟล์นั้นขึ้นมาอ่านแล้วทำตามคำสั่งต่างๆ ที่ผู้สร้างไฟล์นั้นได้กำหนดขึ้น ส่งผลที่ได้กลับไปให้ผู้เรียกใช้โดยแสดงผลที่โปรแกรมบราวเซอร์ของผู้เรียก ซึ่งขั้นตอนข้างต้นเป็นหลักการทำงานโดยทั่วไปของเอเอสพี

2.3.2 ความสามารถและประโยชน์ของ เอเอสพี

1. เอเอสพี ทำให้เว็บเป็นแบบไดนามิก คือรูปแบบที่แสดงผลออกมานั้นสามารถเปลี่ยนแปลงได้ตามข้อมูลที่เอเอสพีได้รับ เช่น ตัวอย่างจากการค้นหาข้อมูลในเว็บไซต์ ผลลัพธ์ที่ได้จะเปลี่ยนไปตามที่ค้นหา

2. เพิ่มความเร็วในการดูเว็บ เนื่องจากการดูเว็บนั้น มักสูญเสียเวลาส่วนใหญ่กับการรอข้อมูลที่มาจากอินเทอร์เน็ต ยิ่งข้อมูลมากขึ้นยิ่งรอนาน ซึ่งเอเอสพีสามารถช่วยในจุดนี้ได้ กล่าวคือ เอเอสพีจะทำการคำนวณต่างๆ จะเสร็จและส่งเฉพาะผลลัพธ์ที่ต้องการเท่านั้น ทำให้ปริมาณการส่งข้อมูลน้อยลง จะเสียเวลารอข้อมูลน้อยลงและสามารถดูเว็บได้เร็วขึ้น

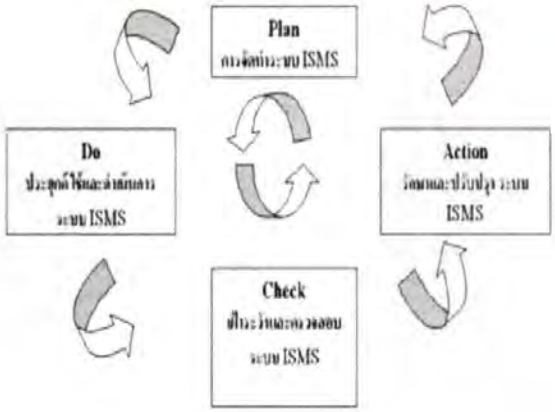
3. เพิ่มความปลอดภัยให้กับระบบในการเขียนโปรแกรมต่างๆ บางครั้งต้องอ้างถึงไดเร็กทอรีที่เก็บฐานข้อมูล อย่างเช่น เว็บไซต์ Yahoo เป็นต้น ซึ่งการใช้เอเอสพีไดเร็กทอรี่ต่างๆ จะไม่ถูกแสดงที่ฝั่งผู้ดูเว็บจะแสดงเฉพาะผลลัพธ์ที่เอามาจากฐานข้อมูลเท่านั้นทำให้ผู้ดูแลเว็บไม่สามารถรู้ถึงโครงสร้างของเว็บเราได้ง่าย และป้องกันผู้ไม่หวังดีมาเจาะระบบ

4. ลดปัญหาความสามารถของเครื่องที่ใช้ดูเว็บ เนื่องจากเอเอสพีจะส่งเฉพาะผลลัพธ์สุดท้ายมาแสดงผลเท่านั้น ดังนั้นไม่ว่าเครื่องคอมพิวเตอร์จะทันสมัยหรือล้าสมัยเพียงใดก็ไม่ทำให้เวลาที่ใช้เปิดดูเว็บแตกต่างกันมาก เพราะว่าการประมวลผลทั้งหมดเสร็จสิ้นที่ฝั่งเซิร์ฟเวอร์แล้ว

2.4 ระบบมาตรฐาน ISO/IEC 27001

ISO/IEC 27001 เป็นมาตรฐานการบริหารในการรักษาความมั่นคงและความปลอดภัยทางด้านสารสนเทศ ที่มีวัตถุประสงค์เพื่อให้การดำเนินงานธุรกิจเป็นไปอย่างต่อเนื่อง ซึ่งข้อกำหนดต่างๆ กำหนดขึ้น โดยองค์กรสากลที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศ คือ ISO (The International Organizationfor Standardization) และ IEC (The International Electrotechnical Commission) ในการที่หน่วยงานได้มีการประยุกต์ใช้จะช่วยให้กิจกรรมทางธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง ช่วยป้องกันระบบข้อมูลสารสนเทศขององค์กร จากความเสี่ยงต่อภัยคุกคามต่างๆ เช่น การหลอกลวงทางคอมพิวเตอร์ การจารกรรมข้อมูล ไวรัสจากคอมพิวเตอร์ การเจาะเข้าโปรแกรมคอมพิวเตอร์และการโจมตีเข้าระบบ เป็นต้น นอกจากนี้ยังช่วยป้องกันกระบวนการทางธุรกิจไม่ให้เสียหายจากความเสี่ยงที่เกิดจากภัยร้ายแรงต่างๆ เช่น แผ่นดินไหว วาตภัย อัคคีภัย อุทกภัย เป็นต้น

2.4.1 หลักการออกแบบโครงสร้างระบบ ISO/IEC 27001 เป็นระบบพลวัตร(Dynamic System) ซึ่งใช้อ้างอิงรูปแบบ PDCA Model (Plan Do Check Action) เป็นโครงสร้างเดียวกับ ระบบการบริหารที่เป็นสากลที่ใช้กันทั่วโลก เช่น ระบบการจัดการคุณภาพ ISO 9001:2000 ระบบการจัดการสิ่งแวดล้อม ISO 14001:2004 ระบบการจัดการคุณภาพสำหรับอุตสาหกรรมรถยนต์ ISO/TS 16949 ระบบการจัดคุณภาพสำหรับอุตสาหกรรมอาหาร ISO 21001 ซึ่งองค์กรที่มีการประยุกต์ระบบการจัดการต่างๆ นี้แล้ว จะสามารถต่อยอดระบบ ISO/IEC27001 ได้เร็วและง่ายขึ้น แต่สำหรับองค์กรที่ยังไม่มีระบบการจัดการใด ๆ ก็ใช่ว่าจะประยุกต์ใช้ยาก เพราะระบบมีการเขียนที่เข้าใจง่าย และแบ่งหมวดให้ง่ายต่อความเข้าใจตามPDCA อยู่แล้วเพียงแต่ต้องทำความเข้าใจกับระบบให้มากขึ้น ระบบ ISMS เป็นระบบ Dynamic system ที่ใช้โครงสร้าง PDCA ดังนั้นระบบจะมีการหมุนเพื่อปรับปรุงอย่างต่อเนื่องอยู่ตลอดเวลาไม่มีที่สิ้นสุด โดยโครงสร้างของข้อกำหนดจะถูกแบ่งตาม PDCA ดังนี้



รูปที่ 2.1 โครงสร้าง PDCA Model

Plan คือการวางแผน การกำหนดขอบเขตและส่วนงานที่เกี่ยวข้อง (Scope and Boundaries) การจัดตั้งทีมงานและกำหนดหน้าที่ความรับผิดชอบ

Do คือการดำเนินการระบบ การกำหนดนโยบายความมั่นคงปลอดภัยขององค์กร การบริหารจัดการความเสี่ยง ซึ่งประกอบด้วยการประเมินความเสี่ยง การวิเคราะห์และแก้ไขความเสี่ยง การเลือกใช้มาตรการความมั่นคงปลอดภัยและควบคุมตามมาตรฐาน การฝึกอบรมพนักงานเกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศในทุกๆ ระดับ

Check คือการเฝ้าระวัง การตรวจประเมินภายในของระบบบริหารความมั่นคงปลอดภัยของสารสนเทศ การทบทวนระบบบริหารความมั่นคงปลอดภัยของสารสนเทศโดยผู้บริหาร

Act คือการรักษาและปรับปรุงระบบ เป็นการดำเนินการปรับปรุงระบบบริหารความมั่นคงปลอดภัยของสารสนเทศตามสิ่งที่ได้ตรวจพบ การดำเนินการวิเคราะห์หาสาเหตุของปัญหาที่แท้จริง (Corrective Actions) การดำเนินการป้องกันไม่ให้ปัญหาเกิดซ้ำอีก (Preventive Actions)

อย่างไรก็ตาม ปัจจัยสำคัญในการจัดทำระบบบริหารความมั่นคงปลอดภัยของสารสนเทศให้ประสบผลสำเร็จต้องอาศัยความเข้าใจในขั้นตอนต่างๆ และความร่วมมือร่วมใจของทีมงานและการสนับสนุนจากผู้บริหารทุกระดับทั้งทางด้านทรัพยากร งบประมาณ และเวลา รวมทั้งระบบที่จัดทำขึ้นจะต้องตอบโจทย์วัตถุประสงค์ขององค์กรด้วย

การที่ระบบมาตรฐาน ISO/IEC 27001 ทำ PDCA Model เพื่อให้ระบบข้อมูลสารสนเทศขององค์กรมีคุณสมบัติในด้านต่าง ๆ ดังต่อไปนี้คือ

Confidentiality (ความลับ) เพื่อให้มั่นใจว่าข้อมูลต่างๆ สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิที่จะเข้าเท่านั้น

Integrity (ความถูกต้องและสมบูรณ์ครบถ้วน) เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องครบถ้วนสมบูรณ์ โดยไม่ได้ถูกเปลี่ยนแปลงหรือแก้ไขจากผู้ที่ไม่ได้รับอนุญาต

Availability (ความพร้อมใช้งาน) เพื่อให้มั่นใจได้ว่าข้อมูลพร้อมที่จะใช้งานอยู่เสมอ โดยผู้ที่มีสิทธิในการเข้าถึงข้อมูลสามารถเข้าถึงได้ทุกเมื่อหากต้องการ

2.4.2 ข้อกำหนด ISO/IEC 27001 ก่อนจะมาเป็นมาตรฐานสากลนี้ มาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799:2005 ได้รับการแก้ไขปรับปรุงมาจากมาตรฐานเดิมที่ชื่อว่า BS 7799-1 และ ISO/IEC 17799 : 2000 ตามลำดับ เนื้อหาของมาตรฐาน ISO 27001 จะเกี่ยวข้องกับการจัดตั้งและปฏิบัติงาน "ระบบบริหารความมั่นคงของข้อมูล" ขึ้นในองค์กร ซึ่งในแนวคิดของมาตรฐานส่วนนี้จะเป็นแนวทางสำคัญ

เนื้อหาของมาตรฐาน ISO/IEC 27001: 2005 แบ่งออกเป็น 8 ส่วน ดังต่อไปนี้

1. ขอบเขต (SCOPE) ข้อกำหนด ISO27001 จะต้องนำไปประยุกต์ใช้ให้มีการเฝ้าติดตามและบำรุงรักษาระบบให้มีความสมบูรณ์ครอบคลุมความเสี่ยงที่อาจจะเกิดขึ้นในองค์กร สามารถประยุกต์ใช้กับบางส่วนขององค์กรได้ องค์กรจะต้องปฏิบัติตามกฎหมายที่เกี่ยวข้อง

2. มาตรฐานอ้างอิง (Normative References) มาตรฐานอ้างอิงของ ISO/IEC 27001 ต้องอยู่บนมาตรฐานอ้างอิงดังนี้

- มาตรฐานเทคโนโลยีสารสนเทศ (Information technology)
- มาตรฐานเทคนิคการรักษาความปลอดภัย (Security techniques)
- มาตรฐานจรรยาบรรณในการปฏิบัติสำหรับการจัดการความปลอดภัยของข้อมูล (Code of practice for information security management)

3. คำจำกัดความและนิยาม (Term and Definitions) ต้องหาคำตอบ คำจำกัดความและนิยามในองค์กรดังนี้

- สิ่งที่มีมูลค่าสำหรับองค์กร
- ความพร้อมเข้าใช้งาน
- การจำกัดสิทธิในการเข้าถึงข้อมูล
- การรักษาไว้ซึ่ง CIA ของข้อมูล เพื่อให้ข้อมูลมีความปลอดภัย และน่าเชื่อถือ
- เหตุการณ์ไม่พึงประสงค์ที่เป็นภัยคุกคามต่อความปลอดภัยข้อมูล

4. ระบบบริหารความมั่นคงของข้อมูล (Information Security Management System) องค์กรต้องกำหนดขอบเขตของระบบ ISMS ให้ครอบคลุมลักษณะของธุรกิจองค์กร พื้นที่ ทรัพย์สิน และเทคโนโลยีรวมถึงระบุขอบเขตที่มีการยกเว้น กำหนดนโยบายการบริหารความปลอดภัยของข้อมูล กรอบการทำงาน วัตถุประสงค์และหลักการของกิจกรรมด้านความปลอดภัยของข้อมูล กำหนดความสอดคล้องกับกฎหมายหรือข้อบังคับต่างๆ ที่เกี่ยวข้องสอดคล้องตามกลยุทธ์ด้านการบริหารความเสี่ยงและบำรุงรักษาระบบ กำหนดเกณฑ์ในการประเมินความเสี่ยง กำหนดความเสี่ยงในองค์กร มีแผนของการดำเนินการกำจัดความเสี่ยงที่มีระบบบริหารจัดการที่เหมาะสม มีทรัพยากรและความรับผิดชอบตามลำดับความสำคัญของข้อมูลที่เป็นความเสี่ยง ต้องมีระเบียบปฏิบัติเรื่องการปฏิบัติการเฝ้าติดตาม

ทบทวนและการควบคุมในระบบ ISMS ระบุแนวทางการป้องกันความผิดพลาดของผลในกระบวนการ วิธีการแก้ไขเหตุการณ์ที่ส่งผลกระทบต่อความปลอดภัยของข้อมูล กำหนดตัวชี้วัดระบบที่ชัดเจน วัดประสิทธิภาพของการควบคุม และทวนสอบให้เห็นว่าการทำงานยังสอดคล้องกับข้อกำหนดด้านความปลอดภัยของข้อมูล มั่นใจได้ว่ากระบวนการในการปรับปรุงได้ประสบความสำเร็จ และเป็นไปตามเป้าหมายจริง ต้องควบคุมการจัดเก็บ การป้องกันข้อมูล การเรียกคืน ระยะเวลาจัดเก็บ และการทำลาย บันทึกที่มีใช้ในระบบ เช่น บันทึกการเข้าเยี่ยม รายงานผลการตรวจและเอกสารมอบอำนาจต่าง ๆ

5. หน้าที่ความรับผิดชอบของฝ่ายบริหาร (Management Responsibility) ผู้บริหารต้องกำหนดนโยบาย มีการกำหนดเป้าหมายและมีการวางแผน กำหนดกฎระเบียบและความรับผิดชอบในระบบรักษาความปลอดภัยของข้อมูล สื่อสารภายในองค์กรจัดประชุมเกี่ยวกับเป้าหมายระบบความปลอดภัยของข้อมูล การทำงานที่สอดคล้องกับนโยบาย การปรับปรุงอย่างต่อเนื่องจัดทรัพยากรให้เหมาะสมในการจัดเตรียมประยุกต์ใช้ปฏิบัติเฝ้าติดตาม ทบทวน บำรุงรักษาและปรับปรุง

6. การตรวจประเมินการบริหารความมั่งคงของข้อมูลภายใน (Internal ISMS Audit) องค์กรต้องจัดให้มีการตรวจติดตาม ISMS ภายในโดยมีการวางแผนและกำหนดวิธีการ วัตถุประสงค์การตรวจเป็นระเบียบปฏิบัติดังนี้

- ตรวจสอบความสอดคล้องกับมาตรฐานสากลและกฎหมายที่เกี่ยวข้อง
- ตรวจสอบความสอดคล้องกับข้อกำหนดของ ISMS
- ตรวจสอบประสิทธิภาพของการนำไปประยุกต์ใช้และบำรุงรักษา
- ตรวจสอบว่าผลเป็นไปตามเป้าหมายที่ทำไว้ หรือไม่

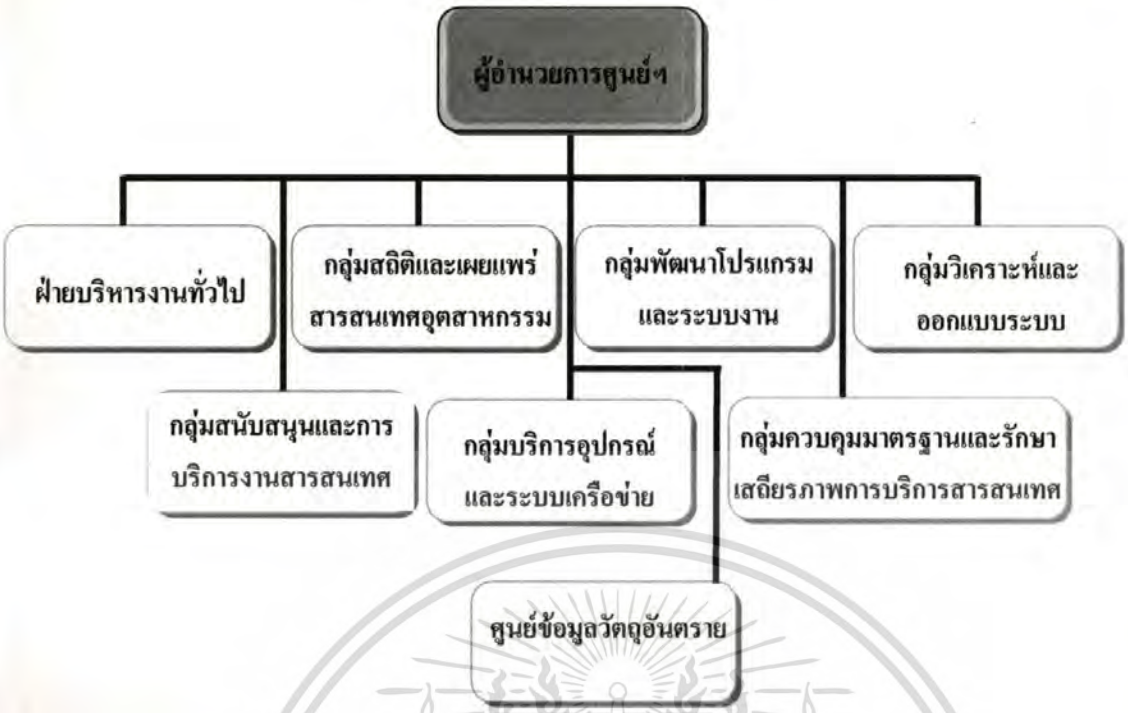
7. การทบทวนการบริหารความมั่นคงของข้อมูล (Management Review of ISMS) องค์กรต้องจัดให้มีการประชุมทบทวนฝ่ายบริหารในรายละเอียดของ ISMS อย่างน้อยปีละ 1 ครั้ง เพื่อเป็นการติดตามสถานะและประสิทธิภาพของ ISMS ผลการประชุมต้องบันทึกไว้เป็นบันทึกคุณภาพ มีการปรับระเบียบการควบคุม ซึ่งกระทบต่อความปลอดภัยของข้อมูลที่จำเป็น ทั้งส่วนที่เกิดจากภายในและภายนอก เช่น ข้อกำหนดทางธุรกิจ ข้อกำหนดด้านความปลอดภัย กระบวนการทางธุรกิจที่ส่งผลกระทบในปัจจุบัน ข้อกำหนดหรือกฎหมายที่เกี่ยวข้อง ความผิดปกติที่เกี่ยวข้อง

8. การปรับปรุงการบริหารความมั่นคงของข้อมูล (ISMS Improvement) องค์กรต้องมีกิจกรรมในการกำจัดต้นเหตุของความไม่สอดคล้องที่เกิดขึ้นในระบบ ISMS และมีการป้องกันการเกิดซ้ำ องค์กรต้องจัดให้มีกิจกรรมในการกำจัดแนวโน้มของความไม่สอดคล้องที่เกิดขึ้นในระบบ ISMS

บทที่ 3
ระบบงานปัจจุบัน

3.1 ความเป็นมาของธุรกิจและโครงสร้างองค์กร

ศูนย์สารสนเทศโรงงานอุตสาหกรรม มีหน้าที่ความรับผิดชอบการศึกษาและวิเคราะห์เทคโนโลยีสารสนเทศ ออกแบบระบบและชี้นำการประยุกต์ใช้เทคโนโลยีสารสนเทศกับงานด้านต่าง ๆ การวางแผนจัดการเทคโนโลยี (Management of technology) โดยคำนึงถึงประสิทธิผลและประสิทธิภาพการวางโครงการเกี่ยวกับระบบสารสนเทศ และการให้คำปรึกษา แนะนำหน่วยงานต่าง ๆ ในการแก้ไขปัญหาเกี่ยวกับระบบสารสนเทศ การส่งเสริม การสนับสนุน และจัดหาเทคโนโลยีสารสนเทศให้ทุกหน่วยงานของกรม บริหารระบบเครื่อง ให้เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ใช้งานได้อย่างมีประสิทธิภาพ ทำหน้าที่เป็นนายทะเบียนผู้ใช้ในระบบเครือข่าย (System Administrator) ทำหน้าที่เป็นผู้จัดการระบบเครือข่าย (Network Administrator) ฝึกอบรมให้คำปรึกษาแนะนำการใช้ระบบเครื่องคอมพิวเตอร์ การจัดระบบ (Configure) ปรับระบบ (Turn up) การจัดระบบฐานข้อมูล การให้คำปรึกษาแนะนำและประสานงานในการปรับปรุง และจัดทำโครงสร้างฐานข้อมูลด้านปฏิบัติการระบบสารสนเทศ เช่น การจัดการทดสอบระบบงาน รวบรวมปัญหาเกี่ยวกับการดำเนินการในระบบต่าง ๆ ให้บริการสารสนเทศระบบงานกับหน่วยงานของกรม กำหนดตัวชี้วัดและกรอบข้อมูล และงานมาตรฐานการบริการ (QA) จัดโครงการฝึกอบรมทางวิชาการด้านสารสนเทศ เผยแพร่สารสนเทศเกี่ยวกับสถิติโรงงาน ทะเบียนเครื่องจักร สารเคมี วัตถุอันตรายและสารระเหย วิเคราะห์รวบรวมผลเกี่ยวกับแนวโน้มด้านโรงงานและอื่น ๆ ที่เกี่ยวข้องกับภาคอุตสาหกรรม การวางแผน ออกแบบ และพัฒนาโปรแกรมระบบงานบนเครือข่ายอินเตอร์เน็ต (Internet) ของหน่วยงานเพื่อให้บริการข้อมูลแก่หน่วยงานภายนอก ประชาชน และผู้ประกอบการให้สามารถได้รับข้อมูลที่ถูกต้อง พร้อมนำไปใช้งานตามวัตถุประสงค์ (Front Office) พร้อมทั้งสนับสนุนการทำงานของหน่วยงานภายในเพื่อเพิ่มประสิทธิภาพการทำงานขององค์กร โปร่งใสและสามารถตรวจสอบได้ เป็นศูนย์กลางข้อมูลวัตถุอันตรายตามกฎหมายว่าด้วยวัตถุอันตราย เพื่อเป็นศูนย์กลางประสานในเรื่องข้อมูลของ วัตถุอันตรายกับส่วนราชการต่างๆ รวมทั้งเอกชนและปฏิบัติตามงานอื่นตามที่ได้รับมอบหมายแบ่งงานภายในออกเป็น 1 ฝ่าย 6 กลุ่ม และ 1 ศูนย์ ดังรูปที่ 3.1



รูปที่ 3.1 โครงสร้างของศูนย์สารสนเทศโรงงานอุตสาหกรรม

1) ฝ่ายบริหารงานทั่วไป มีหน้าที่รับผิดชอบการปฏิบัติงานสารบรรณ และงานธุรการทั่วไป ดำเนินการเกี่ยวกับการจัดทำแผนงาน งบประมาณ วัสดุ ครุภัณฑ์ งานบุคคล งานจัดประชุม จัดระบบงาน การให้บริการเครือข่ายห้องสมุด การจัดทำข้อมูลเกี่ยวกับงานในความรับผิดชอบของศูนย์และสนับสนุนการดำเนินงานของศูนย์ตามที่ได้รับมอบหมาย

2) กลุ่มสถิติและเผยแพร่สารสนเทศอุตสาหกรรม มีหน้าที่รับผิดชอบการจัดการและการบริการด้านสารสนเทศให้สอดคล้องกับความต้องการของผู้ใช้ ประสานงานด้านสารสนเทศกับหน่วยงานภายในและภายนอก การกำหนดหลักสูตรและจัดฝึกอบรมด้านสารสนเทศให้หน่วยงานภายใน ให้บริการสารสนเทศเกี่ยวกับสถิติโรงงานและเอกสารทางวิชาการ การพัฒนาสารสนเทศให้สอดคล้องกับความต้องการของผู้ใช้ เผยแพร่สารสนเทศเกี่ยวกับสถิติโรงงาน ทะเบียนเครื่องจักร สารเคมี วัตถุอันตรายและสารระเหย วิเคราะห์ รวบรวมผลเกี่ยวกับแนวโน้มด้านโรงงานและอื่น ๆ ที่เกี่ยวข้องกับอุตสาหกรรมและปฏิบัติงานอื่นตามที่ได้รับมอบหมาย

3) กลุ่มพัฒนาโปรแกรมและระบบงาน มีหน้าที่รับผิดชอบการวางแผน ออกแบบ และพัฒนาโปรแกรมระบบงานบนเครือข่ายอินเตอร์เน็ต (Internet) เพื่อให้บริการข้อมูลแก่หน่วยงานภายนอก ประชาชน และผู้ประกอบการให้สามารถได้รับข้อมูลที่ถูกต้องพร้อมนำไปใช้งานตามวัตถุประสงค์ (Front Office) พร้อมทั้งสนับสนุนการทำงานของหน่วยงานภายในเพื่อเพิ่มประสิทธิภาพการทำงานขององค์กร โปร่งใสและสามารถตรวจสอบได้ (Web Application) และ

ประสานงานกับหน่วยงานภายนอก เพื่อเชื่อมโยงแลกเปลี่ยนข้อมูลปฏิบัติการ เป็นผู้ดูแลระบบเครือข่ายการสื่อสารรวมทั้งรับจดหมายอิเล็กทรอนิกส์ (E-mail) ขององค์การและปฏิบัติงานอื่นตามที่ได้รับมอบหมาย

4) กลุ่มวิเคราะห์และออกแบบระบบ มีหน้าที่รับผิดชอบการศึกษาและวิเคราะห์ระบบงานสารสนเทศ การออกแบบระบบและชี้นำให้คำปรึกษาการประยุกต์ใช้งานเทคโนโลยีสารสนเทศกับงานด้านต่าง ๆ การทบทวนและปรับแต่งกระบวนงานทุกด้านตามสภาพแวดล้อมทางธุรกิจ การวางแผนจัดการเทคโนโลยี (Management of Technology) โดยคำนึงถึงประสิทธิผลและประสิทธิภาพ การวางโครงการเกี่ยวกับระบบสารสนเทศ และการให้คำปรึกษาแนะนำหน่วยงานต่าง ๆ ในการแก้ไขปัญหาเกี่ยวกับระบบสารสนเทศ และปฏิบัติงานอื่นตามที่ได้รับมอบหมาย

5) กลุ่มสนับสนุนและการบริการงานสารสนเทศ มีหน้าที่รับผิดชอบด้านระบบบริหารเพื่อการจัดการ จัดทำข้อมูลของศูนย์ปฏิบัติการขององค์กร (DOC) เพื่อสนับสนุนข้อมูลให้กับศูนย์ปฏิบัติการระดับกระทรวง ออกแบบและจัดทำรายงานระบบสารสนเทศภูมิศาสตร์ ให้บริการออกแบบและพัฒนาโปรแกรมบริการงานเร่งด่วน (Add hoc) บริหารฐานข้อมูล (Database Administrator) ปรับแต่งระบบฐานข้อมูลกลาง รวมทั้งเป็นนายทะเบียนควบคุมสิทธิการใช้งาน การจัดระบบ (Configure) ปรับระบบ (Turn up) การจัดระบบฐานข้อมูล และปฏิบัติงานอื่นตามที่ได้รับมอบหมาย

6) กลุ่มบริการอุปกรณ์และระบบเครือข่าย มีหน้าที่รับผิดชอบการส่งเสริม การสนับสนุนและจัดหาเทคโนโลยีสารสนเทศให้ทุกหน่วยงานของกรม ด้านบริหารระบบเครื่อง ให้เครื่องคอมพิวเตอร์และระบบงานต่าง ๆ ใช้งานได้อย่างมีประสิทธิภาพ ฝึกอบรม ให้คำปรึกษาแนะนำใช้ระบบเครื่องคอมพิวเตอร์บริหารระบบเครื่องคอมพิวเตอร์ (System Administrator) บริหารระบบเครือข่าย (Network Administrator) บริหารโปรแกรมสำเร็จรูป (Software) เช่น ศึกษาและจัดหาโปรแกรมให้หน่วยงานของกรมใช้งานร่วมกัน ด้านการขยายระบบเครือข่าย (Network) เป็นต้น และปฏิบัติงานอื่นที่ได้รับมอบหมาย

7) กลุ่มควบคุมมาตรฐานและรักษาเสถียรภาพการบริการสารสนเทศ มีหน้าที่รับผิดชอบการให้คำแนะนำและประสานงานในการปรับปรุง และจัดการรับสารสนเทศ เช่น การจัดการทดสอบระบบงาน รวบรวมปัญหาเกี่ยวกับการดำเนินการในระบบต่าง ๆ วางแผนและพัฒนาระบบตรวจสอบและกำกับดูแลความถูกต้องของข้อมูลและความถูกต้องของการใช้ระบบ ออกแบบและพัฒนาระบบตรวจสอบความผิดพลาดของระบบงาน รวมทั้งการวิเคราะห์และการกำหนดแนวทางการป้องกันแก้ไขความผิดพลาดที่เกิดขึ้น กำหนดตัวชี้วัดและกรอบข้อมูล และงานมาตรฐานการบริการ (QA) และปฏิบัติงานอื่นที่ได้รับมอบหมาย

8) ศูนย์ข้อมูลวัตถุอันตราย มีหน้าที่รับผิดชอบการทำหน้าที่เป็นศูนย์กลางข้อมูลวัตถุอันตรายตามกฎหมายว่าด้วยวัตถุอันตราย เพื่อเป็นศูนย์กลางประสานในเรื่องข้อมูลของวัตถุอันตรายกับส่วนราชการต่าง ๆ รวมทั้งภาคเอกชน เพื่อรวบรวมข้อมูลและให้บริการข้อมูลทุกชนิดเกี่ยวกับวัตถุอันตราย ตั้งแต่กรณีอยู่ในต่างประเทศ การนำเข้าหรือการผลิตภายในประเทศ การเคลื่อนย้าย การใช้สอย การทำลายและการอื่นใดที่เกี่ยวเนื่อง จัดสร้างและพัฒนาระบบข้อมูลวัตถุอันตราย จัดทำฐานข้อมูลเกี่ยวกับวัตถุอันตราย เพื่อสนับสนุนแผนงานนโยบายด้านการควบคุมวัตถุอันตรายของประเทศ และทำหน้าที่เป็นศูนย์ข้อมูลวัตถุอันตรายแห่งชาติ พัฒนาข้อมูลสารสนเทศด้านสารเคมีและวัตถุอันตรายให้ถูกต้องและทันสมัย เป็นศูนย์ประสานเครือข่ายข้อมูลสารเคมีแห่งชาติ พัฒนาให้มีระบบเครือข่ายข้อมูลเพื่อสนับสนุนมาตรการในการดำเนินงานตามแผนแม่บทพัฒนาความปลอดภัยด้านเคมีวัตถุแห่งชาติ เป็นศูนย์ข้อมูลเครื่องจักรของประเทศ ทั้งในด้านการใช้เครื่องจักรเป็นหลักทรัพย์ ด้านรายละเอียดข้อมูลและเทคนิค รวมทั้งการแลกเปลี่ยนข้อมูล ซื้อขายและปฏิบัติงานอื่นที่ได้รับมอบหมาย

3.2 ปัญหาที่พบจากการดำเนินงานในปัจจุบัน

จากการศึกษาและวิเคราะห์กระบวนการปฏิบัติงานของหน่วยงานในแต่ละขั้นตอนการทำงาน พบว่า ปัญหาที่เกิดขึ้นในปัจจุบันสามารถสรุปได้ดังนี้

1. การจัดเก็บข้อมูลหรือเอกสารหลักฐานประกอบการตรวจสอบต่างๆ มีทั้งเป็นไฟล์คอมพิวเตอร์และเป็นเอกสาร ซึ่งมีการจัดเก็บกระจัดกระจายไปตามผู้ตรวจสอบแต่ละคนรวมทั้งมีรูปแบบและวิธีการจัดเก็บที่แตกต่างกัน

2. การกำหนดเลขที่เอกสาร เช่น บันทึกแจ้งกำหนดการตรวจสอบ ร่างรายงานการตรวจสอบ รายงานการตรวจสอบ บันทึกการติดตามผลการดำเนินการจากการตอบคำชี้แจง เป็นต้น มีการกำหนดเองทำให้มีโอกาสเกิดความผิดพลาดจากการกำหนดเลขที่เอกสารได้ เช่น เลขที่เอกสารซ้ำกัน หรือรูปแบบของเลขที่เอกสารแตกต่างกัน เป็นต้น

3. การจัดทำเอกสาร เช่น บันทึกแจ้งกำหนดการตรวจสอบ รายงานการตรวจสอบ การติดตามผลการดำเนินประเมินผลการตรวจ เป็นต้น มีการจัดทำโดยวิธีแมนนวล (Manual) ทำให้เสียเวลาในการปฏิบัติงานและผู้ตรวจสอบบางคนจะจัดทำโดยนำเอาสำเนาไฟล์เอกสารฉบับเก่ามาทำการแก้ไขซึ่งทำให้มีโอกาสเกิดความผิดพลาดจากการจัดทำได้

4. การติดตามผลการดำเนินการตามข้อเสนอแนะที่ผู้รับการตรวจสอบและครบกำหนดระยะเวลาที่ดำเนินการแล้วเสร็จ ทำได้ล่าช้าหรือไม่ครบถ้วน เนื่องจากไม่มีระบบติดตามและช่วยเตือนให้ดำเนินการติดตาม

5. ผู้บริหารไม่มีข้อมูลการปฏิบัติงานของเจ้าหน้าที่ เพื่อใช้ในการวิเคราะห์ประเมินผลการปฏิบัติงาน เนื่องจากข้อมูลการปฏิบัติงานตรวจสอบของผู้ตรวจสอบแต่ละคนมีการจัดเก็บที่ไม่เป็นระบบ ทำให้มีข้อมูลไม่เพียงพอในการประเมินผลการปฏิบัติงาน

6. ไม่สามารถใช้ข้อมูลการตรวจสอบร่วมกันภายในหน่วยงานได้อย่างมีประสิทธิภาพ เนื่องจากไม่มีระบบที่ช่วยเก็บรวบรวมข้อมูลงานตรวจสอบทั้งหมดไว้ในฐานข้อมูลเดียวกัน

7. การค้นหาข้อมูลการตรวจสอบ ที่จัดเก็บเป็นไฟล์คอมพิวเตอร์ หรือเป็นเอกสารทำได้ไม่สะดวก เนื่องจากข้อมูลมีเป็นจำนวนมากต้องใช้เวลาในการค้นหา

8. ไม่มีการป้องกันความปลอดภัยให้กับข้อมูลงานตรวจสอบ เนื่องจากผู้ตรวจสอบแต่ละคนจะจัดเก็บข้อมูลไว้ในเครื่องคอมพิวเตอร์ส่วนกลาง หรือคอมพิวเตอร์ส่วนบุคคล ซึ่งแต่ละเครื่องจะเปิดแชร์ไดร์ฟผ่านระบบเครือข่ายทำให้ไม่มีความปลอดภัยในการใช้งานข้อมูล

3.3 แนวทางในการแก้ไขปัญหา

จากการศึกษาข้อมูลด้านการตรวจสอบ และวิเคราะห์กระบวนการทำงานในปัจจุบัน รวมทั้งรวบรวมปัญหาและความต้องการต่างๆ ของเจ้าหน้าที่ สามารถวิเคราะห์แนวทางการแก้ไขปัญหาได้ดังนี้

1. นำเทคโนโลยีสารสนเทศเข้ามาใช้ โดยการพัฒนาระบบบริหารจัดการเอกสารงานตรวจสอบภายใน เพื่อควบคุมการบันทึก การจัดทำเอกสารด้านการตรวจสอบให้เป็นระบบ มีรูปแบบและมีมาตรฐานเดียวกัน ลดการทำงานด้านเอกสารและลดความผิดพลาดจากการบันทึกข้อมูลรวมทั้งเป็นการเพิ่มประสิทธิภาพในการปฏิบัติงาน

2. จัดเก็บข้อมูลไว้ในฐานข้อมูลเดียวกันโดยใช้ฐานข้อมูลเชิงสัมพันธ์ เพื่อให้สามารถจัดเก็บเอกสารได้อย่างเป็นระเบียบเป็นหมวดหมู่ง่ายต่อการเพิ่มเติมหรือแก้ไขข้อมูล ช่วยแก้ไขปัญหาไม่ให้เกิดความซ้ำซ้อนของข้อมูล ช่วยลดเวลาและให้ความสะดวกรวดเร็วในการค้นหาข้อมูล ป้องกันความเสี่ยงต่อการสูญหายของข้อมูล และสามารถใช้ข้อมูลร่วมกันได้อย่างมีประสิทธิภาพ

3. การอนุมัติเอกสารของหน่วยงานควรดำเนินการผ่านระบบโดยส่งผ่านตามลำดับขั้นตอนการอนุมัติ เพื่อความสะดวกรวดเร็วในการปฏิบัติงาน ลดการทำงานด้านเอกสาร ช่วยให้การอนุมัติเอกสารต่างๆ มีประสิทธิภาพ

4. มีระบบรักษาความปลอดภัยในการเข้าถึงข้อมูล ซึ่งผู้ใช้ที่ Login เข้าใช้งานจะสามารถเปิดดูเอกสารได้ตามสิทธิของตนเองที่ถูกกำหนดไว้แล้วเท่านั้น

บทที่ 4
การวิเคราะห์ และออกแบบระบบงานใหม่

จากการศึกษาขั้นตอนการทำงานของระบบงานในปัจจุบัน และได้เก็บรวบรวมข้อมูลของระบบงานต่างๆ ทำให้ทราบถึงปัญหาที่เกิดขึ้นในระบบงานปัจจุบัน รวมถึงเห็นความต้องการใหม่ของผู้ใช้งาน หลังจากนั้นจึงได้นำมาทำการวิเคราะห์และออกแบบระบบงานใหม่ เพื่อให้ได้ระบบสารสนเทศที่สามารถทำงานได้อย่างมีประสิทธิภาพ สามารถตอบสนองต่อความต้องการของผู้ใช้งานได้ โดยได้นำเอาหลักการวิเคราะห์และออกแบบเชิงวัตถุซึ่งใช้ UML (Unified Modeling Language) เป็นเครื่องมือในการจำลองแบบระบบ

4.1 ความต้องการของระบบงานใหม่

การดำเนินงานในปัจจุบันไม่มีการนำเทคโนโลยีสารสนเทศเข้ามาช่วยในด้านการจัดการตรวจประเมิน การติดตามสถานะการตรวจประเมิน การตรวจสอบผลการตรวจประเมิน ทำให้การดำเนินงานไม่มีประสิทธิภาพ ดังนั้นในการวิเคราะห์และออกแบบระบบงานใหม่ จึงได้นำเทคโนโลยีสารสนเทศเข้ามาช่วยในการดำเนินงานและระบบงานใหม่ที่จะพัฒนาขึ้นจะมีความสามารถทำงานได้ดังนี้

4.1.1 Functional Requirements

- สามารถเพิ่ม ลบ แก้ไข และค้นหาผู้ตรวจประเมินได้
- สามารถเพิ่ม ลบ แก้ไข และค้นหาการตรวจประเมินได้
- สามารถติดตามสถานะการตรวจประเมินได้
- สามารถดูรายงานผลการตรวจประเมินได้
- สามารถพิมพ์รายงานผลการประเมินได้
- สามารถพิมพ์รายงานสรุปผลการตรวจประเมินทั้งหมดได้

4.1.2 Non-functional Requirements

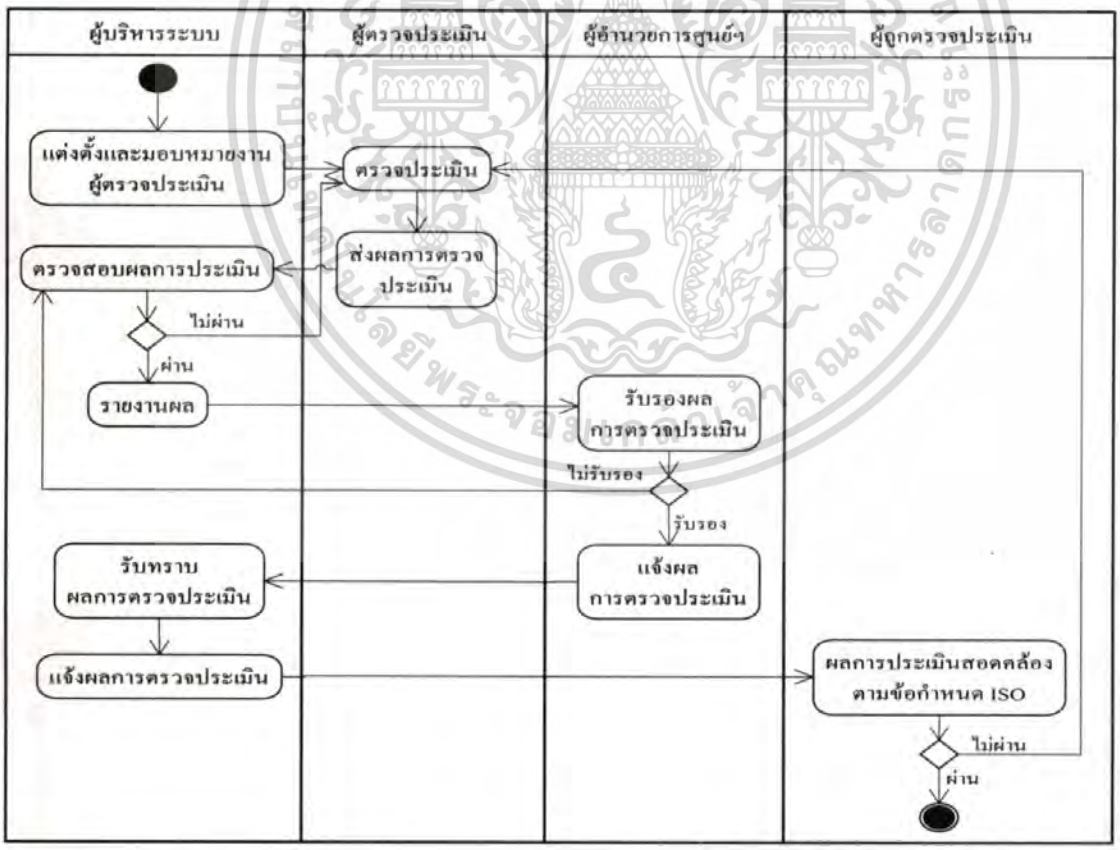
- สามารถทำงาน โดยผ่านช่องทางอินเทอร์เน็ต
- สามารถป้องกัน และรักษาความปลอดภัยของข้อมูลจากการตรวจประเมิน ของแต่ละหน่วยงานได้
- ระบบสามารถรองรับการทำงานได้ตลอดเวลา

4.2 การวิเคราะห์และออกแบบระบบงานใหม่

ในการวิเคราะห์ปัญหาและข้อจำกัดของระบบงานในปัจจุบันพบว่า การทำงานในปัจจุบันยังเป็นการทำงานด้วยระบบเอกสารด้วยมือ ทำให้การสืบค้นข้อมูลและการจัดทำรายงานทำได้ยากและล่าช้าไม่ทันต่อความต้องการใช้งาน บางครั้งยังได้ข้อมูลที่ไม่ถูกต้องและครบถ้วน จึงได้มีการออกแบบและพัฒนาระบบสารสนเทศเข้ามาใช้ เพื่อแก้ไขปัญหาและข้อกำจัดต่างๆ ที่เกิดขึ้น โดยได้มีการปรับปรุงในการทำงานที่ซ้ำซ้อน และเพิ่มความสะดวกในการทำงานมากขึ้น ทำให้การทำงานรวดเร็วและมีประสิทธิภาพมากขึ้น

กระบวนการทำงานของระบบงานใหม่

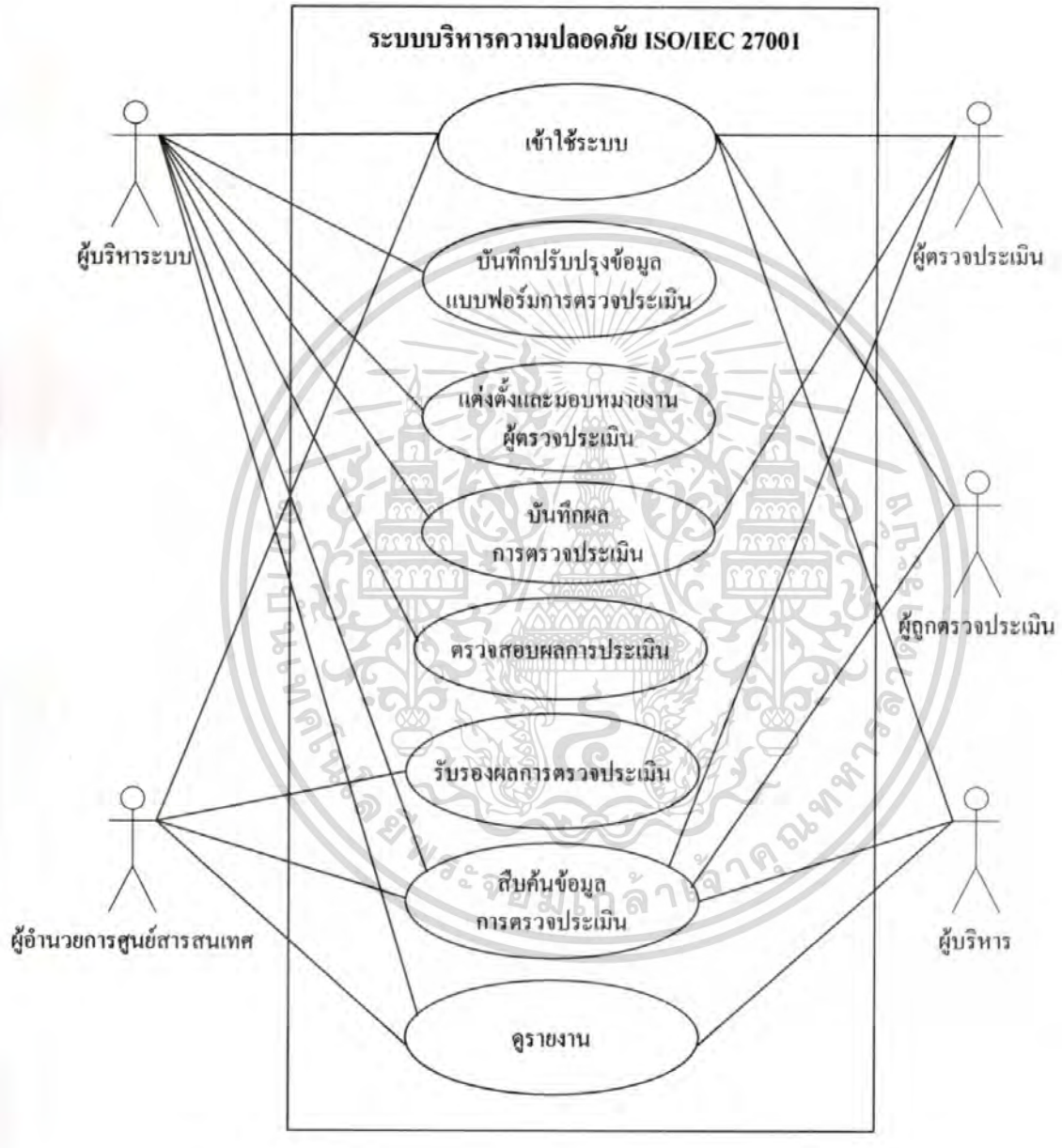
ในการรวบรวมข้อเท็จจริงและความต้องการของระบบ สรุปได้ว่าลักษณะของระบบงานใหม่ต้องการกระบวนการทำงานในรูปแบบเดิม แต่จะนำระบบคอมพิวเตอร์มาช่วยเพิ่มประสิทธิภาพในการทำงานให้ดีขึ้นและทำให้สามารถติดตามงานตรวจประเมินได้ตลอดเวลา แต่ทั้งนี้โปรแกรมระบบงานจะต้องมีความคล่องตัวและง่ายต่อการใช้งาน ซึ่งสามารถเขียนแอกทิวิตีไดอะแกรมอธิบายขั้นตอนการทำงานของระบบได้ ดังรูปที่ 4.1



รูปที่ 4.1 แอกทิวิตีไดอะแกรมอธิบายกระบวนการทำงานของระบบงานใหม่

4.3 ยูสเคสไดอะแกรมระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศISO/IEC 27001

เป็นยูสเคสทำหน้าที่สร้างแบบจำลองเพื่อใช้อธิบายภาพรวมของระบบ ตามความต้องการของลูกค้าหรือผู้ใช้งานและผู้พัฒนาระบบ ซึ่งประกอบด้วยยูสเคส แอกเตอร์ ความสัมพันธ์ของยูสเคสและระบบบริหารความปลอดภัยสำหรับ ISO/IEC 27001 แสดงได้ดังรูปที่ 4.2



รูปที่ 4.2 ยูสเคสไดอะแกรมของระบบบริหารความปลอดภัย ISO/IEC 27001

จากการวิเคราะห์ความต้องการของระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 สามารถกำหนดยูสเคส และแอกเตอร์ได้ดังนี้

4.3.1 แอกเตอร์ ประกอบด้วย

1. ผู้บริหารระบบ หมายถึงผู้ดูแลระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 ในกรมโรงงานอุตสาหกรรมมีหน้าที่แต่งตั้งผู้ตรวจประเมินและตรวจสอบผลการประเมิน

2. ผู้ตรวจประเมิน หมายถึงเจ้าหน้าที่ที่ได้รับมอบหมายของแต่ละหน่วยงานต่างๆ ในระดับสำนัก ศูนย์ กอง ของกรมโรงงานอุตสาหกรรมในการตรวจประเมิน

3. ผู้ถูกตรวจประเมิน หมายถึงหน่วยงานระดับสำนัก ศูนย์ กอง ของกรมโรงงานอุตสาหกรรมที่ถูกตรวจประเมิน สามารถติดตามดูสถานะผลการตรวจประเมินได้

4. ผู้อำนวยการศูนย์สารสนเทศโรงงานอุตสาหกรรม หมายถึงผู้มีหน้าที่ในการพิจารณาตรวจสอบและรับรองผลการตรวจประเมิน

5. ผู้บริหาร หมายถึงผู้บังคับบัญชาระดับสูงได้แก่ อธิบดี รองอธิบดี ผู้อำนวยการ สามารถสืบค้นข้อมูลผลการตรวจประเมินย้อนหลังได้และดูรายงานสรุปต่างๆ ได้

4.3.2 ยูสเคส ประกอบด้วย

1. ยูสเคสเข้าใช้ระบบ หมายถึงการตรวจสอบสิทธิ์การเข้าใช้งานของผู้ใช้ระบบ โดยต้องพิมพ์ชื่อผู้ใช้และรหัสผ่าน จากนั้นระบบจะตรวจสอบชื่อผู้ใช้และรหัสผ่านจากฐานข้อมูลว่าถูกต้องหรือไม่ และมีสิทธิ์ในการใช้ระบบในระดับใด รายละเอียดของยูสเคสแสดงได้ดังตารางที่ 4.1

2. ยูสเคสบันทึกปรับปรุงข้อมูลแบบฟอร์มการตรวจประเมิน เป็นยูสเคสที่เกี่ยวข้องกับผู้บริหารระบบ ซึ่งมีหน้าที่ปรับปรุงข้อมูล คือ แก้ไข เพิ่ม ลบ ข้อมูลแบบฟอร์มการตรวจประเมินได้ รายละเอียดของยูสเคสแสดงได้ดังตารางที่ 4.2

3. ยูสเคสแต่งตั้งและมอบหมายงานผู้ตรวจประเมิน เป็นยูสเคสที่ผู้บริหารระบบพิจารณาแต่งตั้งและมอบหมายงานให้เจ้าหน้าที่ในการตรวจประเมินในแต่ละระดับ ซึ่งเจ้าหน้าที่หนึ่งคนสามารถตรวจประเมินได้หลายระดับ รายละเอียดของยูสเคสแสดงได้ดังตารางที่ 4.3

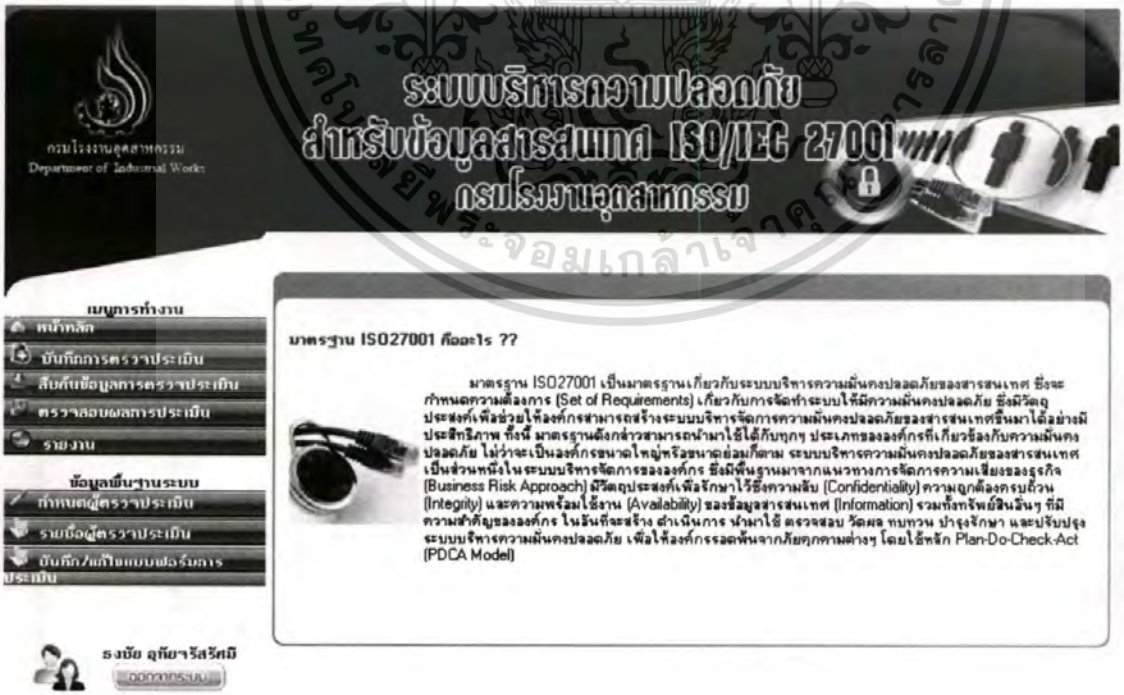
4. ยูสเคสบันทึกผลการตรวจประเมิน เป็นยูสเคสที่เกี่ยวข้องกับผู้ตรวจประเมินและผู้บริหารระบบ เมื่อไปตรวจประเมินเรียบร้อยแล้วต้องนำผลการประเมินมาบันทึกข้อมูลในระบบ รายละเอียดของยูสเคสแสดงได้ดังตารางที่ 4.4

5. ยูสเคสตรวจสอบผลการตรวจประเมิน เป็นยูสเคสที่เจ้าหน้าที่ตรวจประเมินติดตามดูสถานะการตรวจประเมินการดำเนินการอยู่ในขั้นตอนใดแล้ว ซึ่งจะทำหลังจากที่เจ้าหน้าที่ได้ยืนยันส่งผลการตรวจประเมินเรียบร้อยแล้ว รายละเอียดของยูสเคสแสดงได้ดังตารางที่ 4.5

ตารางที่ 4.1 รายละเอียดยูสเคสเข้าใช้ระบบ

Use Case Name	เข้าใช้ระบบ	
Scenario	เข้าใช้ระบบ	
Triggering Event	ผู้ใช้งานกรอกชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าใช้งานระบบ	
Brief Description	ผู้ใช้งานพิมพ์ชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าใช้งานระบบ ระบบตรวจสอบรายชื่อผู้ใช้และรหัสผ่านจากฐานข้อมูลว่าถูกต้องหรือไม่ และมีสิทธิ์ในการใช้งานในระดับใด	
Actors	ผู้บริหารระบบ ผู้ตรวจประเมิน ผู้ถูกตรวจประเมิน ผู้อำนวยการศูนย์สารสนเทศ ผู้บริหาร	
Related Use Case	-	
Stakeholders	-	
Preconditions	มีข้อมูลผู้ใช้งานอยู่ในระบบ	
Post conditions	แสดงเมนูการใช้งานตามสิทธิ์การใช้งานของผู้ใช้งานแต่ละคน	
Flow of Activities	**Actor**	**System**
	1. ผู้ใช้งานพิมพ์ชื่อผู้ใช้งานและรหัสผ่าน ดังรูปที่ 4.3 2. เข้าใช้งานระบบตามสิทธิ์ที่ได้รับ ดังรูปที่ 4.4	1.1 ระบบตรวจสอบรายชื่อผู้ใช้และรหัสผ่าน 1.2 ระบบแสดงเมนูการใช้งานตามสิทธิ์การใช้งานของผู้ใช้งานแต่ละคน
Exception Conditions	1.1 กรณีพิมพ์ชื่อผู้ใช้งานและรหัสผ่านไม่ถูกต้องหรือไม่มีอยู่ในระบบ ระบบให้กรอกชื่อผู้ใช้งานและรหัสผ่านใหม่	

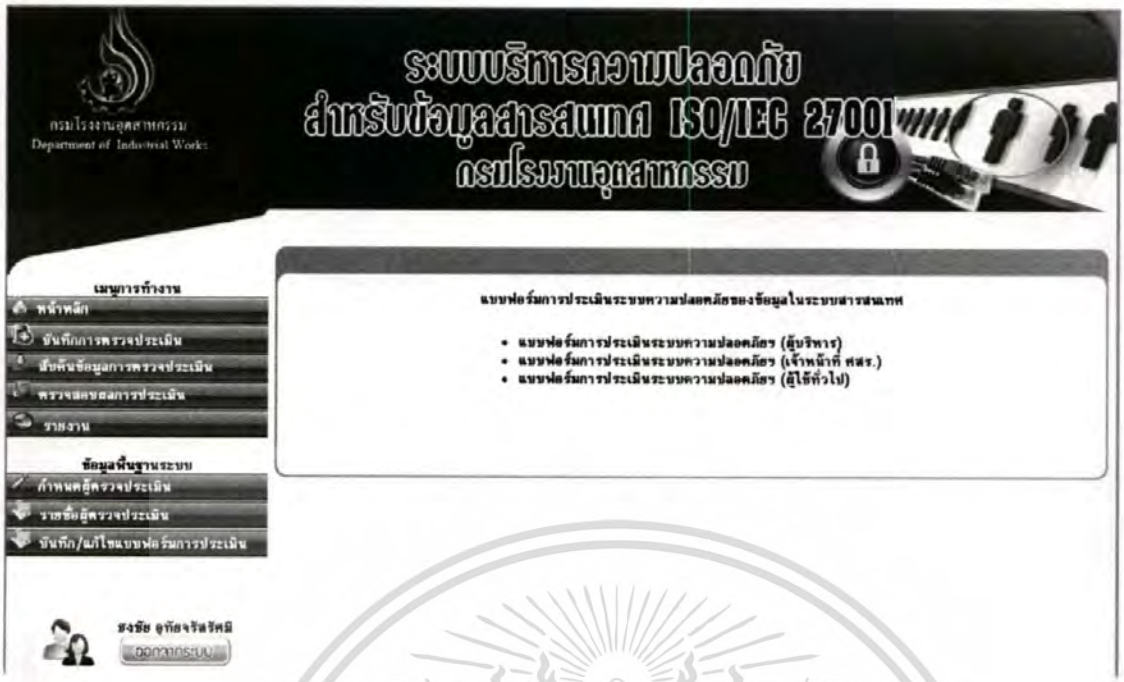
รูปที่ 4.3 หน้าจอตรวจสอบผู้ใช้ระบบ



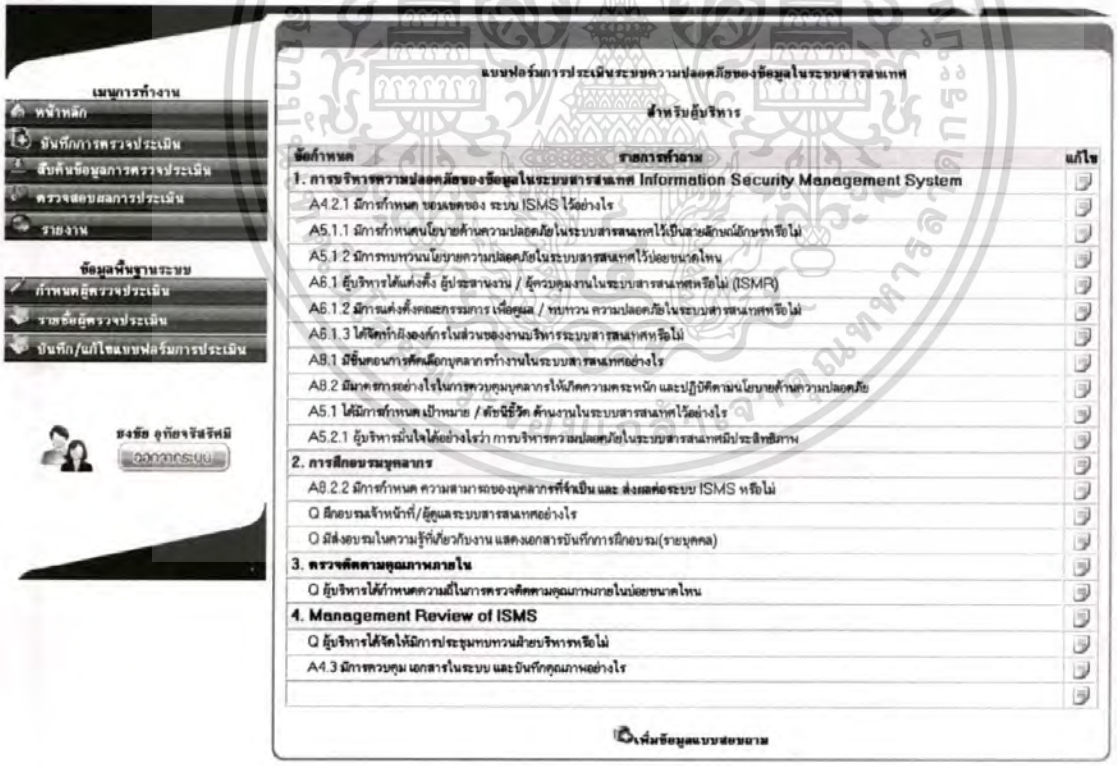
รูปที่ 4.4 หน้าจอแสดงเมื่อเข้าสู่ระบบเรียบร้อยแล้ว

ตารางที่ 4.2 รายละเอียดยูสเคสบันทึกปรับปรุงข้อมูลแบบฟอร์มการตรวจประเมิน

Use Case Name	บันทึกปรับปรุงข้อมูลแบบฟอร์มการตรวจประเมิน	
Scenario	บันทึกปรับปรุงข้อมูลแบบฟอร์มการตรวจประเมิน	
Triggering Event	ผู้บริหารระบบเลือกแบบฟอร์ม	
Brief Description	ผู้บริหารระบบเลือกแบบฟอร์มแต่ละระดับ ระบบแสดงรายการคำถามของแต่ละแบบฟอร์ม ผู้บริหารระบบสามารถแก้ไข เพิ่ม หรือลบรายการคำถามของแต่ละแบบฟอร์มได้	
Actors	ผู้บริหารระบบ	
Related Use Case	-	
Stakeholders	-	
Preconditions	มีข้อมูลแบบฟอร์มที่ผ่านการพิจารณาเรียบร้อยแล้ว	
Post conditions	รายการคำถามในแบบฟอร์มถูกปรับปรุงข้อมูล	
Flow of Activities	**Actor**	**System**
	1. ผู้บริหารระบบเลือกแบบฟอร์ม ดังรูป ที่ 4.5 2. ผู้บริหารระบบเลือก แก้ไข เพิ่ม ลบ รายการคำถามของแบบฟอร์ม ดังรูป ที่ 4.6	1.1 ระบบแสดงรายการคำถามของแต่ละแบบฟอร์ม 2.1 ระบบทำการแก้ไข เพิ่ม หรือลบรายการคำถามตามที่ผู้บริหารระบบเลือก
Exception Conditions	2.1 กรณีผู้บริหารระบบเลือกเพิ่มข้อมูลและไม่พิมพ์ข้อมูลในช่องรายละเอียดคำถามระบบจะแสดงข้อความเตือนให้พิมพ์ข้อมูล	



รูปที่ 4.5 หน้าจอเมนูแบบฟอร์ม



รูปที่ 4.6 หน้าจอแสดงการปรับปรุงข้อมูลแบบฟอร์ม

ตารางที่ 4.3 รายละเอียดยูสเคสแต่งตั้งและมอบหมายงานผู้ตรวจประเมิน

Use Case Name	แต่งตั้งและมอบหมายงานผู้ตรวจประเมิน	
Scenario	แต่งตั้งและมอบหมายงานผู้ตรวจประเมิน	
Triggering Event	ผู้บริหารระบบเลือกเมนูกำหนดผู้ตรวจประเมิน	
Brief Description	ผู้บริหารระบบเลือกหน่วยงานของเจ้าหน้าที่ ระบบจะแสดงรายชื่อเจ้าหน้าที่ที่สังกัดหน่วยงานดังกล่าว ผู้บริหารระบบเลือกระดับการตรวจประเมิน	
Actors	ผู้บริหารระบบ	
Related Use Case	-	
Stakeholders	เจ้าหน้าที่ในกรมโรงงานอุตสาหกรรม	
Preconditions	มีข้อมูลเจ้าหน้าที่ในระบบ	
Post conditions	เจ้าหน้าที่ที่ถูกแต่งตั้งมีสถานะเป็นผู้ตรวจประเมิน	
Flow of Activities	**Actor**	**System**
	1. ผู้บริหารระบบเลือกหน่วยงาน ดังรูปที่ 4.7 2. อัพโหลดไฟล์เอกสารแต่งตั้งผู้ประเมิน 3. ผู้บริหารระบบเลือกเจ้าหน้าที่และเลือกระดับการตรวจประเมิน 4. ผู้บริหารระบบบันทึกข้อมูล	1.1 ระบบแสดงรายชื่อเจ้าหน้าที่ของหน่วยงานที่ถูกเลือก ดังรูปที่ 4.8 2.1 ระบบจัดเก็บไฟล์ไว้ในเครื่องแม่ข่าย(Server)ในโฟลเดอร์ DOCAUDITOR 4.1 ระบบบันทึกข้อมูลสถานะให้กับเจ้าหน้าที่ที่ถูกแต่งตั้งและแสดงข้อความจัดเก็บข้อมูลเรียบร้อยแล้ว ดังรูปที่ 4.9
Exception Conditions		

รูปที่ 4.7 หน้าจอแสดงเลือกหน่วยงานที่ต้องการแต่งตั้งผู้ตรวจประเมิน

รูปที่ 4.8 หน้าจอแสดงรายชื่อเจ้าหน้าที่และระดับการตรวจประเมิน

รูปที่ 4.9 หน้าจอแสดงข้อความจากระบบหลังจากผู้บริหารระบบกดปุ่มบันทึกข้อมูล

ตารางที่ 4.4 รายละเอียดยูสเคสบันทึกผลการตรวจประเมิน

Use Case Name	บันทึกผลการตรวจประเมิน	
Scenario	บันทึกผลการตรวจประเมิน	
Triggering Event	ผู้ตรวจประเมินหรือผู้บริหารระบบ เลือกเมนูบันทึกการตรวจประเมิน	
Brief Description	ผู้ตรวจประเมินหรือผู้บริหารระบบ เมื่อตรวจประเมินเรียบร้อยแล้วต้องนำผลการตรวจประเมินมาบันทึกเข้าระบบ โดยระบบจะตรวจสอบสิทธิ์ของผู้ตรวจประเมินว่าอยู่ในระดับใด เมื่อตรวจสอบเรียบร้อยแล้วจะแสดงแบบฟอร์มตามสิทธิ์ของผู้ตรวจประเมิน กรณีที่สิทธิ์ของผู้ประเมินสามารถประเมินได้หลายระดับ ระบบจะให้เลือกระดับและเลือกหน่วยงานที่ถูกตรวจประเมินได้	
Actors	ผู้ตรวจประเมิน ผู้บริหารระบบ	
Related Use Case	-	
Stakeholders		
Preconditions	ผู้ตรวจประเมินตรวจประเมินเรียบร้อยแล้ว	
Post conditions		
Flow of Activities	**Actor**	**System**
	1. ผู้ตรวจประเมินเลือกเมนูบันทึกการตรวจประเมิน 2. ผู้ตรวจประเมินบันทึกผลการตรวจประเมิน 3. ผู้ตรวจประเมินกดปุ่มบันทึกข้อมูล	1.1 ระบบตรวจสอบสิทธิ์ของผู้ตรวจประเมิน 1.2 ระบบแสดงแบบฟอร์มตามสิทธิ์ผู้ตรวจประเมิน ดังรูปที่ 4.10 3.1 ระบบตรวจสอบความครบถ้วนของข้อมูล 3.2 ระบบบันทึกข้อมูลการตรวจประเมินลงฐานข้อมูลและแสดงข้อความ ดังรูปที่ 4.11
Exception Conditions	3.2 กรณีผู้ตรวจประเมินพิมพ์ข้อมูลไม่ครบระบบแสดงข้อความเตือนให้พิมพ์ข้อมูลให้ครบถ้วน	

รูปที่ 4.10 หน้าจอแสดงแบบฟอร์มการประเมิน

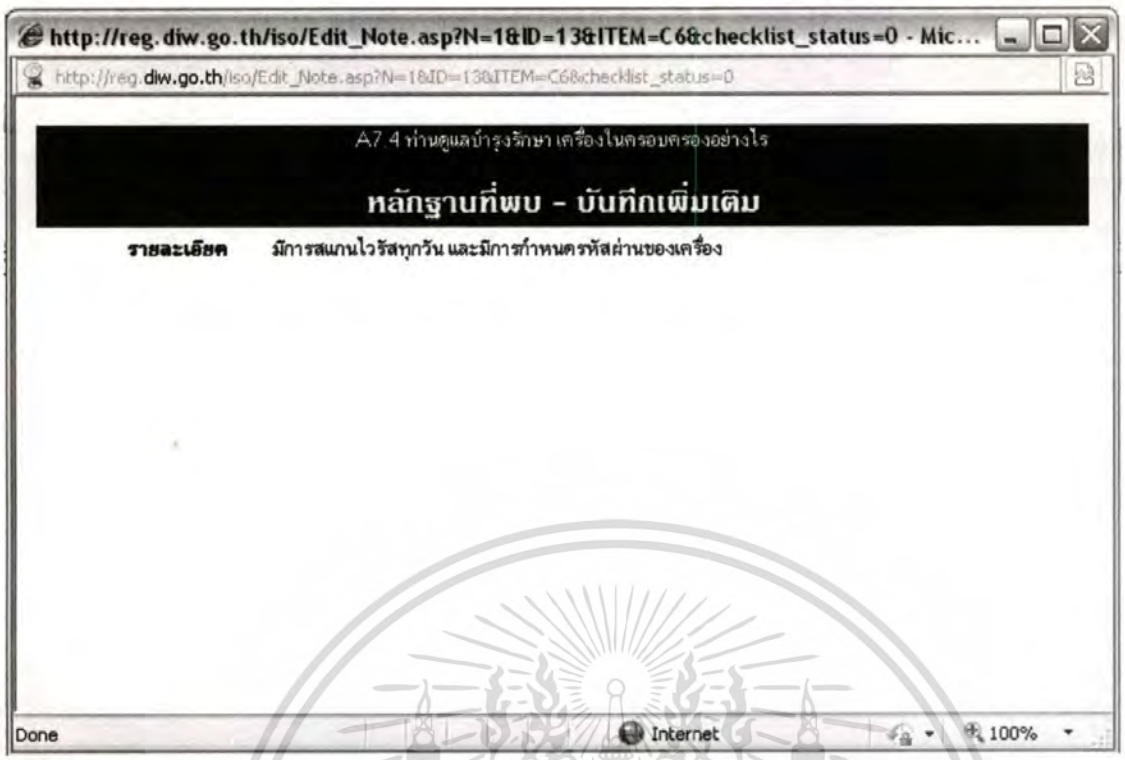
รูปที่ 4.11 หน้าจอแสดงข้อความหลังจากผู้ตรวจประเมินกดปุ่มบันทึกข้อมูล

ตารางที่ 4.5 รายละเอียดยูสเคสตรวจสอบผลการตรวจประเมิน

Use Case Name	ตรวจสอบผลการตรวจประเมิน	
Scenario	ตรวจสอบผลการตรวจประเมิน	
Triggering Event	ผู้บริหารระบบ เลือกเมนูตรวจสอบผลการตรวจประเมิน	
Brief Description	เมื่อผู้ตรวจประเมินยืนยันส่งผลการตรวจประเมิน รายการตรวจประเมินจะแสดงในเมนูตรวจสอบผลการประเมินของผู้บริหารระบบ ซึ่งผู้บริหารระบบตรวจสอบผลการตรวจประเมินเรียบร้อยแล้วจะเลือกผลการตรวจสอบผ่านหรือไม่ผ่าน กรณีไม่ผ่านต้องระบุเหตุผลที่ไม่ผ่านการตรวจสอบให้ผู้ตรวจประเมินทราบ	
Actors	ผู้บริหารระบบ	
Related Use Case	-	
Stakeholders	ผู้ตรวจประเมิน	
Preconditions	มีข้อมูลการตรวจประเมินที่ผู้ตรวจประเมินยืนยันส่งผลการตรวจประเมินเรียบร้อยแล้ว	
Post conditions	สถานะการตรวจประเมินถูกเปลี่ยนเป็นผ่านการตรวจสอบหรือไม่ผ่านการตรวจสอบ	
Flow of Activities	**Actor**	**System**
	1. ผู้บริหารระบบเลือกรายการผลการตรวจประเมิน 2. ผู้บริหารระบบพิจารณาผลการตรวจประเมิน ดังรูปที่ 4.13 และสามารถคลิกดูหลักฐานเพิ่มเติมที่ผู้ตรวจประเมินบันทึกรายละเอียดไว้ ดังรูปที่ 4.14 3. ผู้บริหารระบบเลือกผลการตรวจสอบ ดังรูปที่ 4.15 4. ผู้บริหารระบบบันทึกข้อมูล	1.1 ระบบแสดงผลการตรวจประเมินตามแบบฟอร์มที่ตรวจประเมิน ดังรูปที่ 4.12 4.1 ระบบตรวจสอบความครบถ้วนของข้อมูล 4.2 ระบบบันทึกข้อมูลลงฐานข้อมูลและส่งอีเมล์แจ้งผู้ตรวจประเมิน ดังรูปที่ 4.16
Exception Conditions	4.1 กรณีผู้บริหารระบบเลือกผลการตรวจสอบไม่ผ่านและไม่ได้พิมพ์ข้อมูลในช่องหมายเหตุระบบจะแสดงข้อความเตือนให้พิมพ์ข้อมูลเหตุผลการไม่ผ่านการตรวจสอบ	

รูปที่ 4.12 หน้าจอแสดงรายการประเมินที่รอตรวจสอบผลการประเมิน

รูปที่ 4.13 หน้าจอแสดงการตรวจสอบผลการประเมินที่รอตรวจสอบผลการประเมิน



รูปที่ 4.14 หน้าจอแสดงรายละเอียดหลักฐานเพิ่มเติมที่ผู้ตรวจประเมินบันทึกไว้

รูปที่ 4.15 หน้าจอแสดงการตรวจสอบผลการประเมิน

รูปที่ 4.16 หน้าจอแสดงเมื่อบันทึกข้อมูลและส่งผลการตรวจสอบถึงผู้ตรวจประเมินทางอีเมล์

6. ยูสเคสรับรองผลการตรวจประเมิน เป็นยูสเคสที่ผู้อำนวยการศูนย์สารสนเทศโรงงานอุตสาหกรรม พิจารณาผลการตรวจประเมินต่อจากผู้บริหารระบบหากผลการตรวจประเมินอยู่ในช่วงของการยอมรับได้จะรับรองผลการตรวจประเมิน ซึ่งถือว่าผลการตรวจประเมินเสร็จสมบูรณ์ และผู้บริหารระบบสามารถนำผลการประเมินไปประกาศตามขั้นตอนต่อไป รายละเอียดของยูสเคสแสดงได้ดังตารางที่ 4.6

7. ยูสเคสสืบค้นข้อมูลการตรวจประเมิน เป็นยูสเคสที่ใช้ในการค้นหาข้อมูลผลการตรวจประเมินย้อนหลังได้ โดยระบุเงื่อนไขต่างๆ เช่น วันที่ตรวจ ผู้ถูกตรวจประเมิน ระดับการตรวจ รายละเอียดของยูสเคสแสดงได้ดังตารางที่ 4.7

8. ยูสเคสดูรายงาน เป็นยูสเคสที่ใช้ออกรายงาน และจัดทำรายงานสรุปผลการตรวจประเมินในภาพรวมของข้อมูลโดยในรูปแบบที่จัดเตรียมไว้ซึ่งมีหลายรูปแบบ และจะแสดงผลออกมาตามเงื่อนไขที่กำหนด ได้แก่

- รายงานสรุปผลการตรวจประเมินแยกตามผู้ตรวจประเมิน เป็นการรายงานสรุปแยกตามผู้ตรวจประเมิน
- รายงานสรุปผลการตรวจประเมินแยกตามหน่วยงาน เป็นการรายงานสรุปแยกตามหน่วยงานที่ถูกตรวจประเมิน
- รายงานผลการตรวจประเมินปัจจุบัน เป็นรายงานตามแบบฟอร์มของการตรวจประเมินเป็นข้อมูลที่ตรวจประเมินครั้งล่าสุด ซึ่งผู้บริหารสามารถเข้ามาดูรายงานในแต่ละระดับได้โดยไม่เสียเวลาในการสืบค้นข้อมูล
- สถิติการไม่สอดคล้องตามข้อกำหนดเป็นรายงานสรุปสถิติการประเมินที่ไม่สอดคล้องตามข้อกำหนด ซึ่งข้อมูลจะเป็นประโยชน์ในพิจารณาแนวทางการแก้ไขหรือป้องกันการปฏิบัติไม่สอดคล้องตามข้อกำหนดในอนาคตได้ รายละเอียดของยูสเคสแสดงได้ดังตารางที่ 4.8

ตารางที่ 4.6 รายละเอียดยูสเคสรับรองผลการตรวจประเมิน

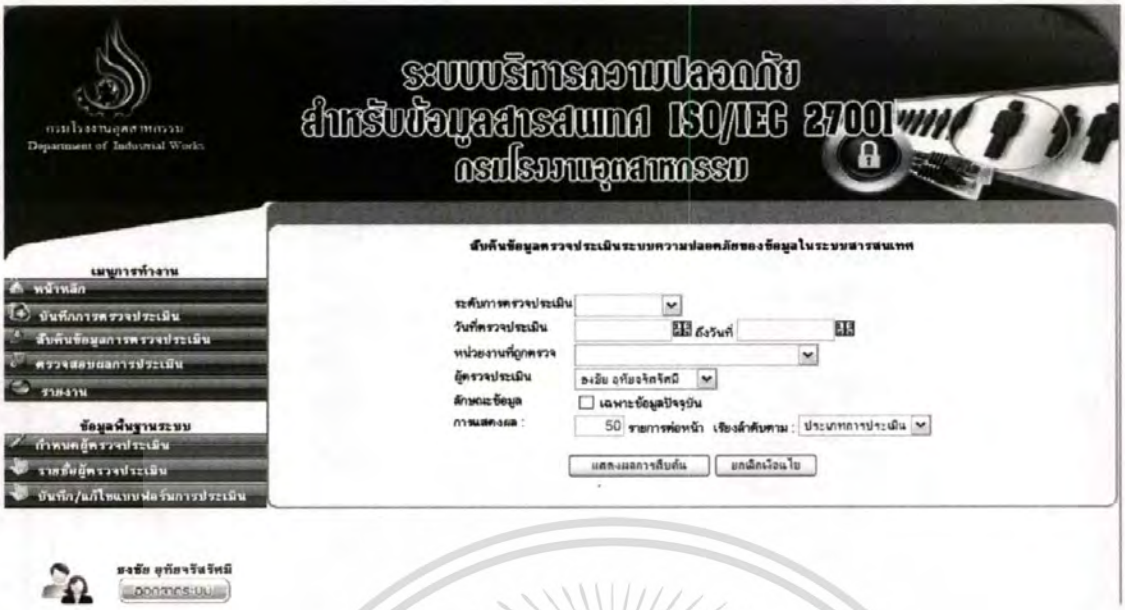
Use Case Name	รับรองผลการตรวจประเมิน	
Scenario	รับรองผลการตรวจประเมิน	
Triggering Event	ผู้อำนวยการศูนย์สารสนเทศโรงงานอุตสาหกรรมเลือกเมนูรับรองผลการตรวจประเมิน	
Brief Description	เมื่อผู้บริหารระบบตรวจสอบผลการตรวจประเมินเรียบร้อยแล้ว รายการที่ผ่านการตรวจสอบจะมาแสดงในเมนูรับรองผลการตรวจประเมินของผู้อำนวยการศูนย์สารสนเทศโรงงานอุตสาหกรรม ซึ่งผู้อำนวยการศูนย์ ฯ ตรวจสอบผลการตรวจประเมินเรียบร้อยแล้วเลือกรับรองผลหรือไม่รับรองผลการตรวจประเมิน กรณีที่ไม่รับรองผลต้องระบุเหตุผลที่ไม่รับรองผลการตรวจประเมินให้ผู้บริหารระบบ และผู้ตรวจประเมินทราบ	
Actors	ผู้อำนวยการศูนย์สารสนเทศโรงงานอุตสาหกรรม	
Related Use Case	-	
Stakeholders	ผู้ตรวจประเมิน ผู้บริหารระบบ	
Preconditions	มีข้อมูลการตรวจประเมินผ่านการตรวจสอบของผู้บริหารระบบเรียบร้อยแล้ว	
Post conditions	สถานะการตรวจประเมินถูกเปลี่ยนเป็นรับรองผลหรือไม่รับรองผลการตรวจประเมิน	
Flow of Activities	**Actor**	**System**
	1. ผู้อำนวยการศูนย์ฯ เลือกรายการรับรองการตรวจประเมิน ดังรูปที่ 4.17 2. ผู้อำนวยการศูนย์ฯ พิจารณาผลการตรวจประเมินและดูรายละเอียดหลักฐานเพิ่มเติมที่ผู้ตรวจประเมินบันทึกมา 3. ผู้อำนวยการศูนย์ฯ เลือกผลการพิจารณา ดังรูปที่ 4.18 4. ผู้อำนวยการศูนย์ฯ บันทึกข้อมูล	1.1 ระบบแสดงผลการตรวจประเมินตามแบบฟอร์มที่ตรวจประเมิน 4.1 ระบบตรวจสอบความครบถ้วนของข้อมูล 4.2 ระบบบันทึกข้อมูลลงฐานข้อมูลและส่งอีเมล์แจ้งผู้ตรวจประเมิน
Exception Conditions	4.1 กรณีผู้อำนวยการศูนย์ฯ เลือกไม่รับรองผลการประเมินและไม่ระบุเหตุผลในช่องหมายเหตุ ระบบจะแสดงข้อความเตือนให้พิมพ์ข้อมูล	

รูปที่ 4.17 หน้าจอแสดงรายการที่รอรับรองผลการตรวจประเมิน

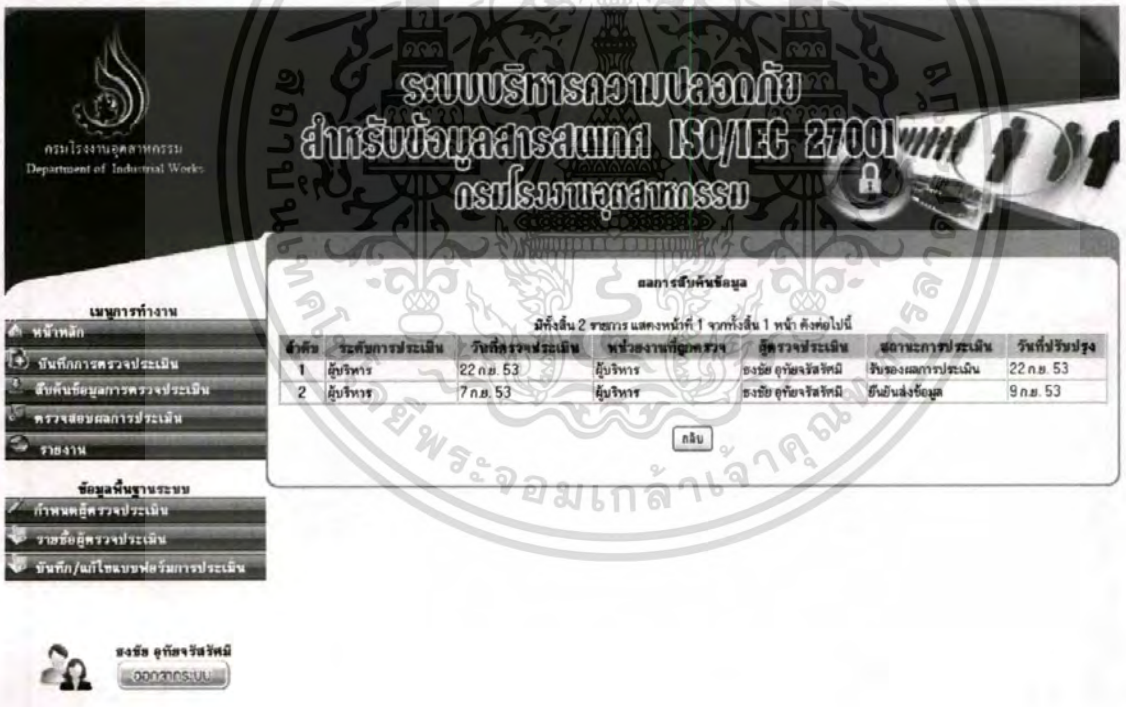
รูปที่ 4.18 หน้าจอแสดงการรับรองผลการตรวจประเมินของผู้อำนวยการศูนย์สารสนเทศ

ตารางที่ 4.7 รายละเอียดยูสเคสสืบค้นข้อมูลการตรวจประเมิน

Use Case Name	สืบค้นข้อมูลการตรวจประเมิน	
Scenario	สืบค้นข้อมูลการตรวจประเมิน	
Triggering Event	ผู้ใช้ระบบเลือกเมนูสืบค้นข้อมูลการตรวจประเมิน	
Brief Description	การสืบค้นข้อมูลการตรวจประเมินของระบบเป็นกระบวนการสืบค้นและแสดงข้อมูลบนหน้าจอ โดยเจ้าหน้าที่ที่เกี่ยวข้องใช้ในการค้นหาข้อมูลการตรวจประเมินต่างๆ ย้อนหลังได้ โดยระบุเงื่อนไขที่กำหนด	
Actors	ผู้บริหารระบบ ผู้ตรวจประเมิน ผู้ถูกตรวจประเมิน ผู้อำนวยการศูนย์สารสนเทศ ผู้บริหาร	
Related Use Case	-	
Stakeholders	ผู้บริหารระบบ ผู้ตรวจประเมิน ผู้ถูกตรวจประเมิน ผู้อำนวยการศูนย์สารสนเทศ ผู้บริหาร	
Preconditions	มีข้อมูลการตรวจประเมินในระบบ	
Post conditions	แสดงผลการค้นหาข้อมูลการตรวจประเมิน	
Flow of Activities	**Actor**	**System**
	1. ผู้ใช้ระบบเลือกเมนูการสืบค้นข้อมูลการตรวจประเมิน 2. กำหนดเงื่อนไขในการสืบค้นข้อมูล 3. กดปุ่มแสดงผลการสืบค้น	1.1 ระบบแสดงสืบค้นข้อมูลการตรวจประเมิน ดังรูปที่ 4.19 3.1 ระบบสืบค้นข้อมูลในฐานข้อมูลตามเงื่อนไขที่ผู้ใช้ระบบกำหนด 3.2 แสดงผลการสืบค้นข้อมูล ดังรูปที่ 4.20
Exception Conditions		



รูปที่ 4.19 หน้าจอแสดงหน้าสืบค้นข้อมูลการตรวจประเมิน



รูปที่ 4.20 หน้าจอแสดงผลการสืบค้นข้อมูลตามเงื่อนไขที่กำหนด

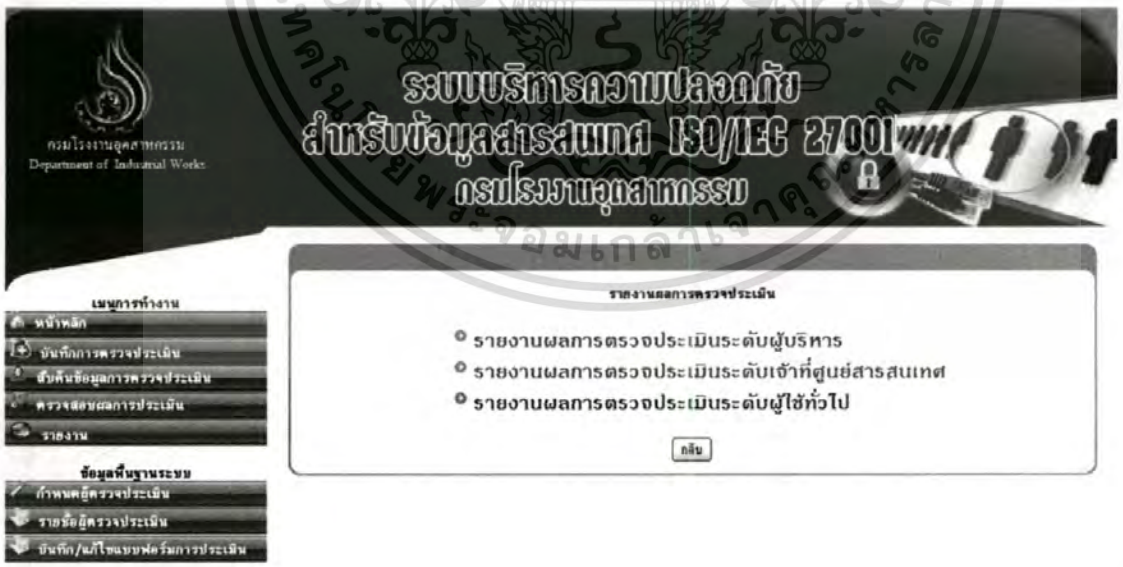
ตารางที่ 4.8 รายละเอียดยูสเคสดูรายงาน

Use Case Name	ดูรายงาน	
Scenario	ดูรายงาน	
Triggering Event	ผู้ใช้ระบบเลือกเมนูรายงาน	
Brief Description	การเรียกดูรายงานและการออกรายงานเกี่ยวกับผลการตรวจประเมิน โดยการจัดทำรายงานจะสรุปผลการตรวจประเมินในภาพรวมของข้อมูล ซึ่งจะแสดงผลรายงานออกมาตามเงื่อนไขที่กำหนด ในรูปแบบที่จัดเตรียมไว้ ได้แก่ รายงานสรุปผลการตรวจประเมินแยกตามผู้ตรวจประเมิน รายงานสรุปผลการตรวจประเมินแยกตามหน่วยงาน รายงานผลการตรวจประเมิน และรายงานสถิติการไม่สอดคล้องตามข้อกำหนด	
Actors	ผู้บริหารระบบ ผู้อำนวยการศูนย์ฯ ผู้บริหาร	
Related Use Case	-	
Stakeholders	ผู้ตรวจประเมิน ผู้ถูกตรวจประเมิน ผู้บริหารระบบ ผู้อำนวยการศูนย์ฯ ผู้บริหาร	
Preconditions	มีข้อมูลการตรวจประเมินในระบบ	
Post conditions	แสดงรายงานผลการประเมิน	
Flow of Activities	**Actor**	**System**
	1. ผู้ใช้ระบบเลือกเมนูรายงาน 2. เลือกเมนูรายงาน	1.1 ระบบแสดงเมนูรายงาน ดังรูปที่ 4.21 2.1 ระบบแสดงรายงานตามหัวข้อที่เลือก ดังรูปที่ 4.22 ถึงรูปที่ 4.26
Exception Conditions		

รูปที่ 4.21 หน้าจอแสดงเมนูรายงานการตรวจประเมิน

รูปที่ 4.22 หน้าจอแสดงรายงานสรุปผลการตรวจประเมินแยกตามผู้ตรวจประเมิน

รูปที่ 4.23 หน้าจอแสดงรายงานสรุปผลการตรวจประเมินแยกตามหน่วยงาน



รูปที่ 4.24 หน้าจอแสดงรายงานผลการตรวจประเมิน ณ ปัจจุบัน

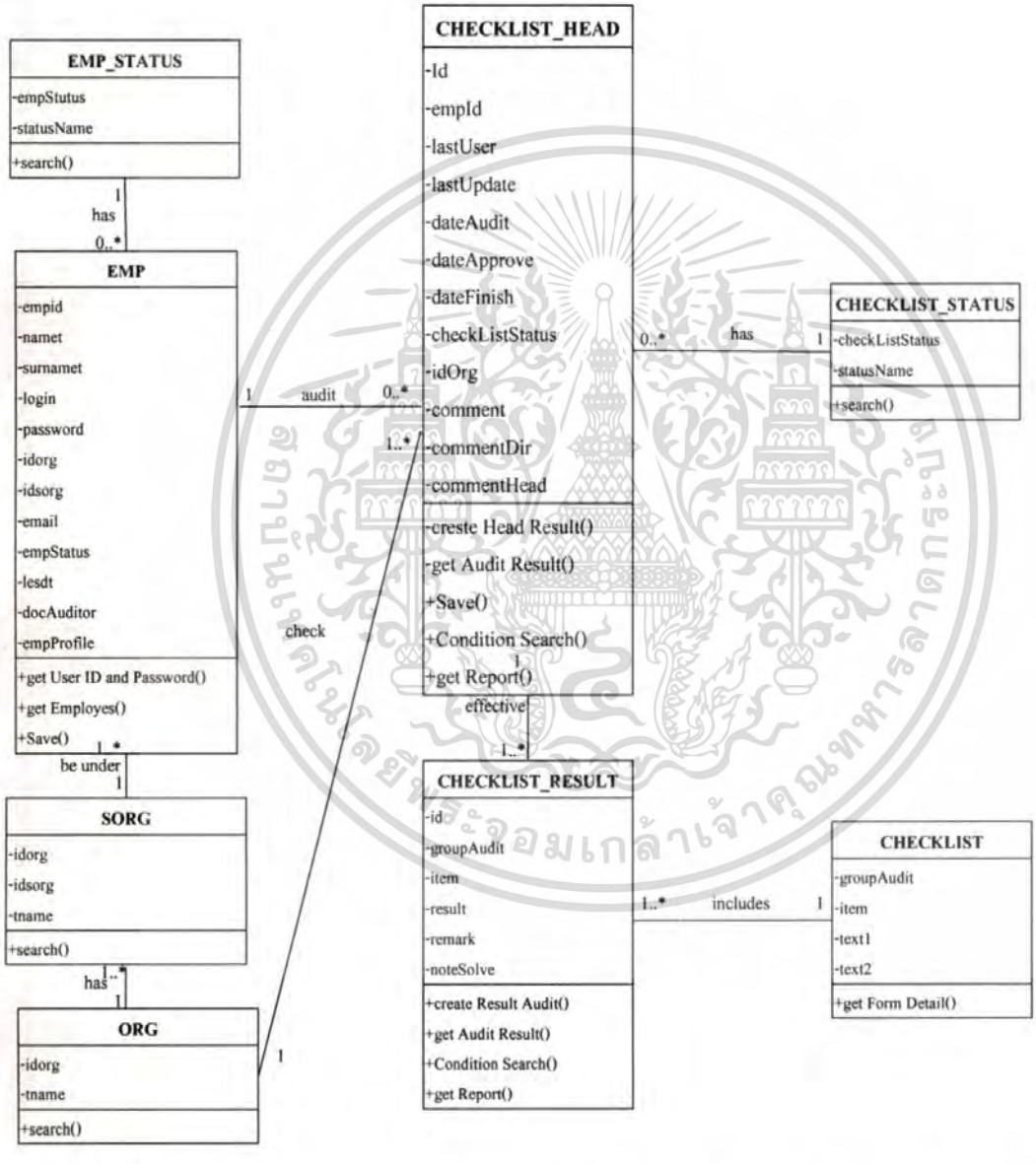
รูปที่ 4.25 หน้าจอแสดงเมนูรายงานสถิติผลการตรวจประเมินที่ไม่สอดคล้องกับ ISO/IEC 27001

ลำดับ	ชื่อผู้ตรวจประเมิน	จำนวนที่ไม่สอดคล้องตามข้อกำหนด (ครั้ง)
1	A5.2.1 ผู้บริหารมั่นใจได้อย่างไรว่า การบริหารความปลอดภัยในระบบสารสนเทศมีประสิทธิภาพ	2
2	A8.2.2 มีการกำหนด ความสามารถของบุคลากรที่จำเป็น และ ส่งผลต่อระบบ ISMS หรือไม่	2
3	Q มีกอบรมให้พนักงาน/ผู้ดูแลระบบสารสนเทศอย่างไร	2
4	Q มีส่งอบรมในความรู้ที่เกี่ยวกับงาน แสดงเอกสารบันทึกการฝึกอบรม(รายบุคคล)	3
5	A4.3 มีการควบคุม เอกสารในระบบ และบันทึกคุณภาพอย่างไร	3
6	A5.1.1 มีการกำหนดนโยบายด้านความปลอดภัยในระบบสารสนเทศไว้เป็นลายลักษณ์อักษรหรือไม่	2
7	A5.1.2 มีการทบทวนนโยบายความปลอดภัยในระบบสารสนเทศไว้บ่อยขนาดไหน	2
8	A6.1 ผู้บริหารได้แต่งตั้ง ผู้ประสานงาน / ผู้ควบคุมงานในระบบสารสนเทศหรือไม่ (ISMR)	1
9	A6.1.2 มีการแต่งตั้งคณะกรรมการ เพื่อดูแล / ทบทวน ความปลอดภัยในระบบสารสนเทศหรือไม่	2
10	A6.1.3 ได้จัดทำผังองค์กรในส่วนของงานบริหารระบบสารสนเทศหรือไม่	2
11	A8.1 มีขั้นตอนการคัดเลือกบุคลากรทำงานในระบบสารสนเทศอย่างไร	2
12	A5.1 ได้มีการกำหนด เป้าหมาย / ดัชนีชี้วัด ด้านงานในระบบสารสนเทศไว้อย่างไร	2

รูปที่ 4.26 หน้าจอแสดงเมนูรายงานสถิติผลการตรวจประเมินที่ไม่สอดคล้องระดับผู้บริหาร

4.4 คลาสไดอะแกรม

จากการที่ได้วิเคราะห์ภาพรวมของการทำงานของระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 ของกรมโรงงานอุตสาหกรรม โดยใช้ยูสเคสไดอะแกรมแล้ว สามารถนำมาสร้างคลาสไดอะแกรมของระบบได้ โดยคลาสต่างๆ จะแสดงโครงสร้างความสัมพันธ์ระหว่างคลาสที่จำเป็นในระบบ ซึ่งประกอบด้วยคลาสต่างๆ ดังรูปที่ 4.27

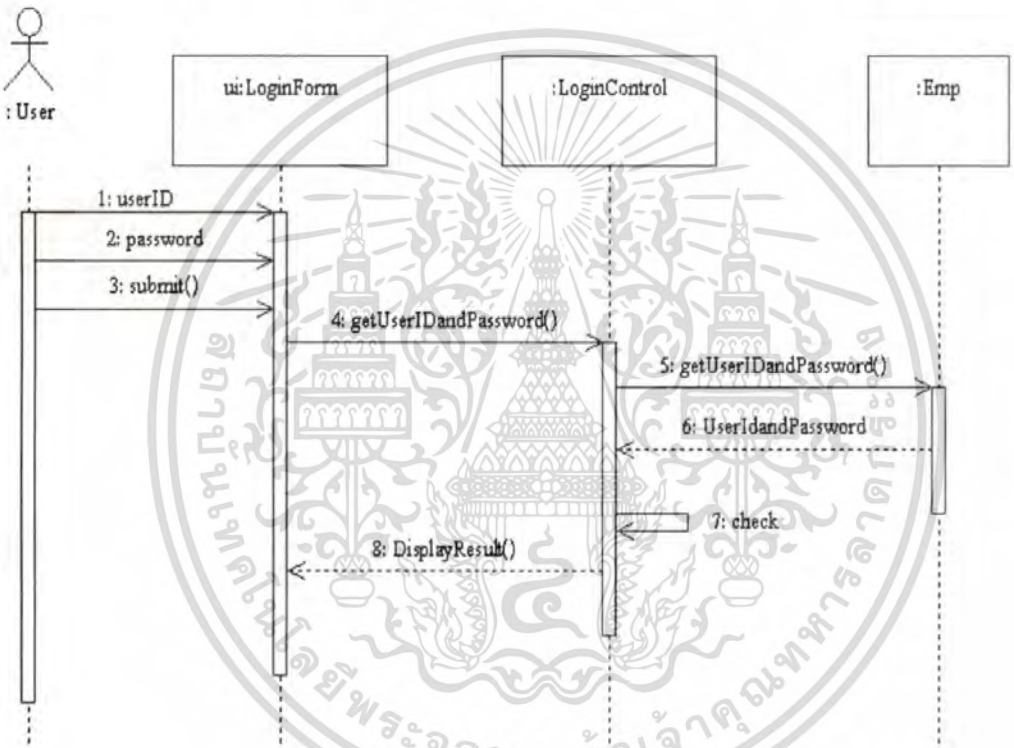


รูปที่ 4.27 คลาสไดอะแกรมของระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001

4.5 ซีเควนซ์ไดอะแกรม

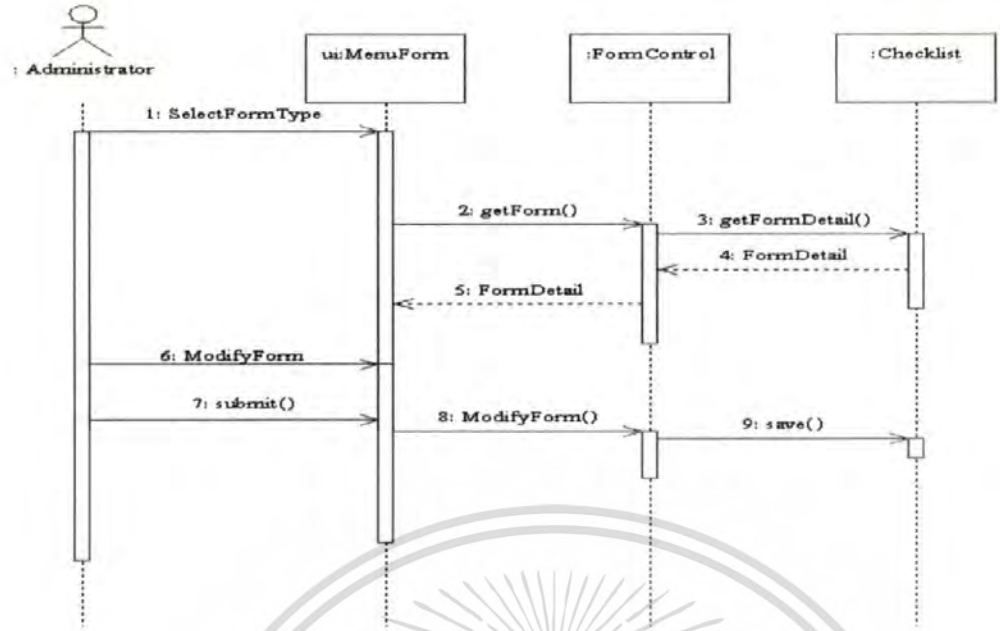
ซีเควนซ์ไดอะแกรม เป็นไดอะแกรมที่ใช้อธิบายการทำงานของ ยูสเคส เพื่อแสดงถึงขั้นตอนการทำงานและแสดงลำดับของเมสเสจที่ส่งผ่านระหว่างคลาสที่โต้ตอบกัน นอกจากนี้แล้ว ซีเควนซ์ไดอะแกรม ยังรวมถึงเงื่อนไขเวลาที่ใช้ในการทำงานด้วย

4.5.1 ซีเควนซ์ไดอะแกรมการเข้าใช้ระบบ เป็นการอธิบายกิจกรรมการเข้าใช้ระบบของผู้ใช้งาน คือผู้ใช้งานพิมพ์ชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าใช้งานระบบ ระบบตรวจสอบรายชื่อผู้ใช้และรหัสผ่านจากฐานข้อมูลว่าถูกต้องหรือไม่ และมีสิทธิ์ในการใช้งานในระดับใด ดังรูปที่ 4.28



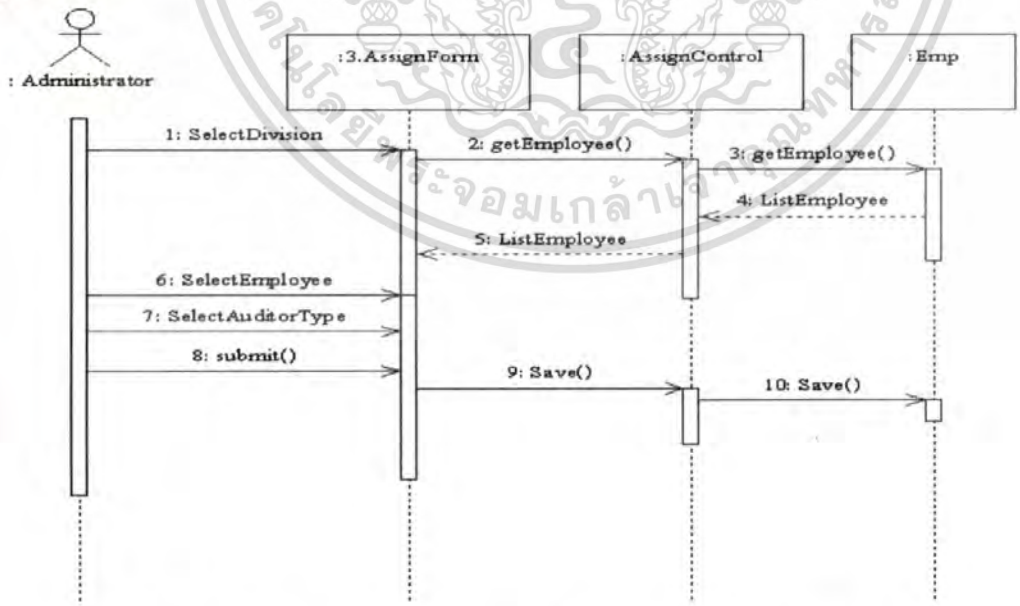
รูปที่ 4.28 ซีเควนซ์ไดอะแกรมการเข้าใช้ระบบ

4.5.2 ซีเควนซ์ไดอะแกรมการบันทึกปรับปรุงข้อมูลแบบฟอร์มการตรวจประเมิน เป็นการอธิบายกิจกรรมการบันทึกปรับปรุงข้อมูลแบบฟอร์มการตรวจประเมิน คือผู้บริหารระบบเลือกแบบฟอร์มแต่ละระดับ ระบบแสดงรายการคำถามของแต่ละแบบฟอร์ม ผู้บริหารระบบสามารถแก้ไข เพิ่ม หรือลบรายการคำถามของแต่ละแบบฟอร์มได้ ดังรูปที่ 4.29



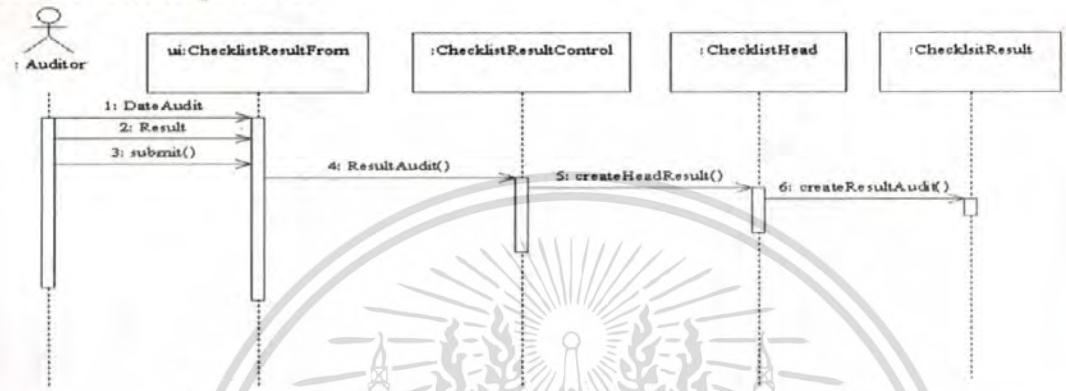
รูปที่ 4.29 ซีเควนซ์ไดอะแกรมการบันทึกปรับปรุงข้อมูลแบบฟอร์มการตรวจประเมิน

4.5.3 ซีเควนซ์ไดอะแกรมการแต่งตั้งและมอบหมายงานผู้ตรวจประเมิน เป็นการอธิบายกิจกรรมการแต่งตั้งและมอบหมายงานผู้ตรวจประเมิน คือผู้บริหารระบบเลือกหน่วยงานของเจ้าหน้าที่ระบบจะแสดงรายชื่อเจ้าหน้าที่ที่สังกัดหน่วยงานดังกล่าว ผู้บริหารระบบเลือกระดับการตรวจประเมิน ดังรูปที่ 4.30



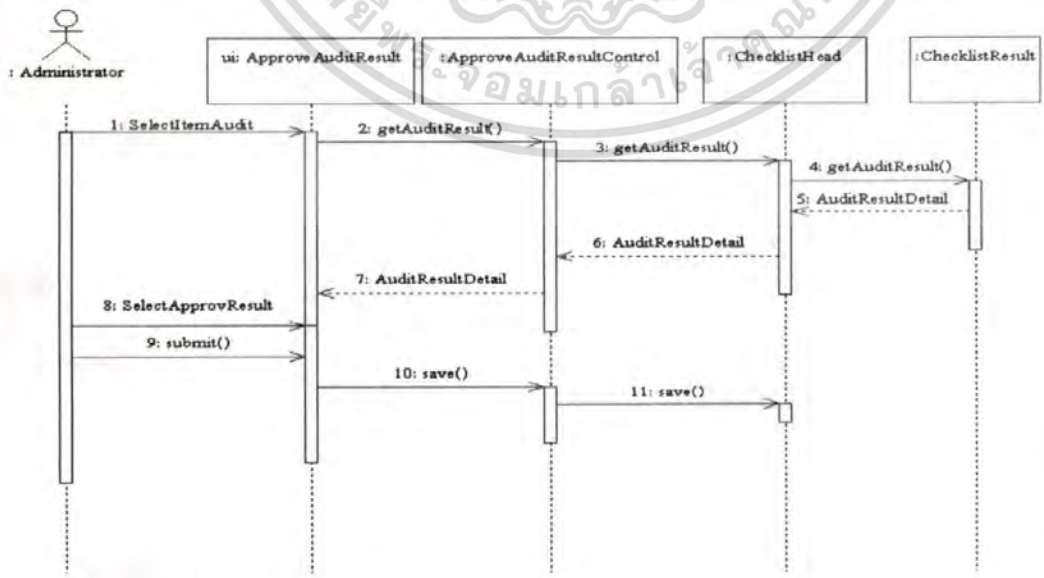
รูปที่ 4.30 ซีเควนซ์ไดอะแกรมการแต่งตั้งและมอบหมายงานผู้ตรวจประเมิน

4.5.4 ซีเควนซ์ไดอะแกรมการบันทึกผลการตรวจประเมิน เป็นการอธิบายกิจกรรมการบันทึกผลการตรวจประเมิน คือผู้ตรวจประเมินหรือผู้บริหารระบบ เมื่อตรวจประเมินเรียบร้อยแล้วต้องนำผลการตรวจประเมินมาบันทึกเข้าระบบ โดยระบบจะตรวจสอบสิทธิ์ของผู้ตรวจประเมินว่าอยู่ในระดับใด เมื่อตรวจสอบเรียบร้อยแล้วจะแสดงแบบฟอร์มตามสิทธิ์ของผู้ตรวจประเมิน กรณีที่สิทธิ์ของผู้ประเมินสามารถประเมินได้หลายระดับ ระบบจะให้เลือกระดับและเลือกหน่วยงานที่ถูกตรวจประเมินได้ ดังรูปที่ 4.31



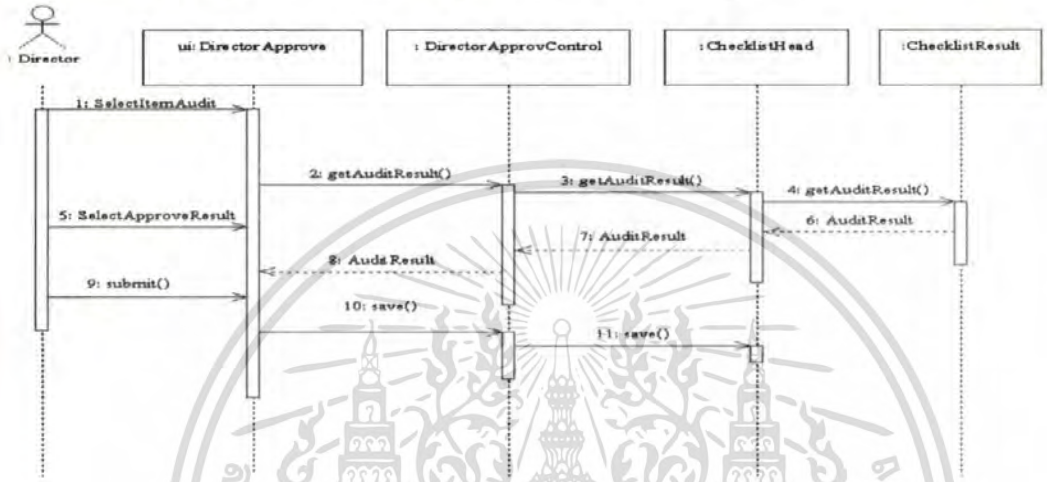
รูปที่ 4.31 ซีเควนซ์ไดอะแกรมการบันทึกผลการตรวจประเมิน

4.5.5 ซีเควนซ์ไดอะแกรมการตรวจสอบผลการตรวจประเมิน เป็นการอธิบายกิจกรรมการตรวจสอบผลการตรวจประเมิน คือเมื่อผู้ตรวจประเมินยืนยันส่งผลการตรวจประเมิน รายการตรวจประเมินจะแสดงในเมนูตรวจสอบผลการประเมินของผู้บริหารระบบ ซึ่งผู้บริหารระบบตรวจสอบผลการตรวจประเมินเรียบร้อยแล้ว จะเลือกผลการตรวจสอบผ่านหรือไม่ผ่าน กรณีไม่ผ่านต้องระบุเหตุผลที่ไม่ผ่านการตรวจสอบให้ผู้ตรวจประเมินทราบ ดังรูปที่ 4.32



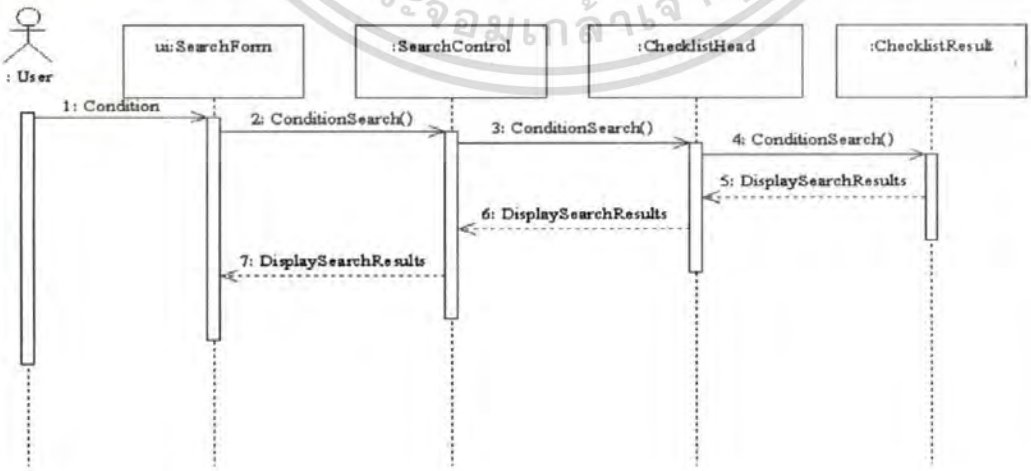
รูปที่4.32 ซีเควนซ์ไดอะแกรมการตรวจสอบผลการตรวจประเมิน

4.5.6 ซีเควนซ์ไดอะแกรมการรับรองผลการตรวจประเมิน เป็นการอธิบายกิจกรรมการรับรองผลการตรวจประเมิน คือเมื่อผู้บริหารระบบตรวจสอบผลการตรวจประเมินเรียบร้อยแล้ว รายการที่ผ่านการตรวจสอบจะมาแสดงในเมนูรับรองผลการตรวจประเมินของผู้อำนวยการศูนย์สารสนเทศโรงงานอุตสาหกรรม ซึ่งผู้อำนวยการศูนย์ตรวจสอบผลการตรวจประเมินเรียบร้อยแล้ว เลือกรับรองผลหรือไม่รับรองผลการตรวจประเมิน กรณีที่ไม่รับรองผลต้องระบุเหตุผลที่ไม่รับรองผลการตรวจประเมินให้ผู้บริหารระบบ และผู้ตรวจประเมินทราบ ดังรูปที่ 4.33



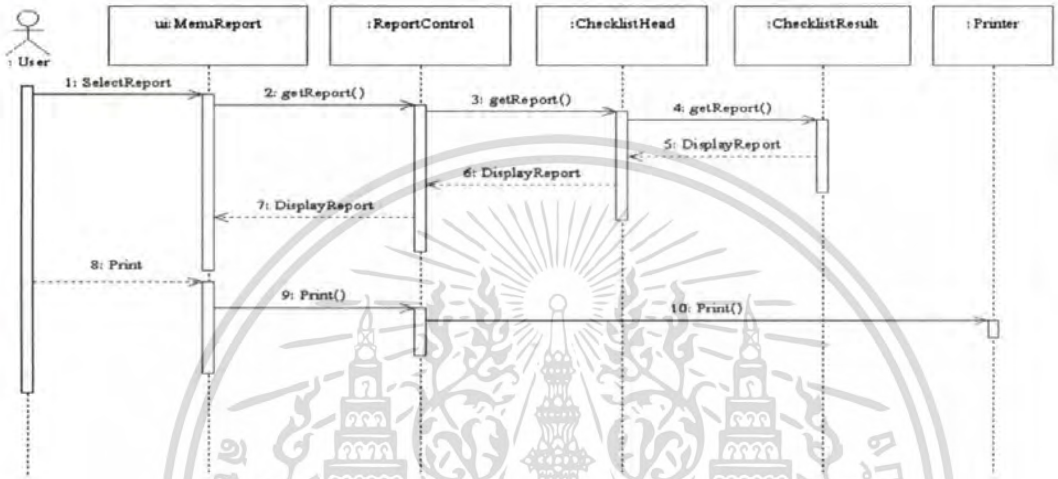
รูปที่ 4.33 ซีเควนซ์ไดอะแกรมการรับรองผลการตรวจประเมิน

4.5.7 ซีเควนซ์ไดอะแกรมการสืบค้นข้อมูลการตรวจประเมิน เป็นการอธิบายกิจกรรมการสืบค้นข้อมูลการตรวจประเมิน คือการสืบค้นข้อมูลการตรวจประเมินของระบบเป็นกระบวนการสืบค้นและแสดงข้อมูลบนหน้าจอ โดยเจ้าหน้าที่ที่เกี่ยวข้องใช้ในการค้นหาข้อมูลการตรวจประเมินต่างๆ ย้อนหลังได้ โดยระบุเงื่อนไขที่กำหนด ดังรูปที่ 4.34



รูปที่ 4.34 ซีเควนซ์ไดอะแกรมการสืบค้นข้อมูลการตรวจประเมิน

4.5.8 ซีเควนซ์ไดอะแกรมการดูรายงาน เป็นการอธิบายกิจกรรมการดูรายงาน คือการเรียกดูรายงาน และการออกรายงานเกี่ยวกับผลการตรวจประเมิน โดยการจัดทำรายงานจะสรุปผลการตรวจประเมินในภาพรวมของข้อมูล ซึ่งจะแสดงผลรายงานออกมาตามเงื่อนไขที่กำหนดในรูปแบบที่จัดเตรียมไว้ได้แก่ รายงานสรุปผลการตรวจประเมินแยกตามผู้ตรวจประเมิน รายงานสรุปผลการตรวจประเมินแยกตามหน่วยงาน รายงานผลการตรวจประเมิน และรายงานสถิติการไม่สอดคล้องตามข้อกำหนด ดังรูปที่ 4.35



รูปที่ 4.35 ซีเควนซ์ไดอะแกรมการดูรายงาน

4.6 สเตทชาร์ตไดอะแกรม

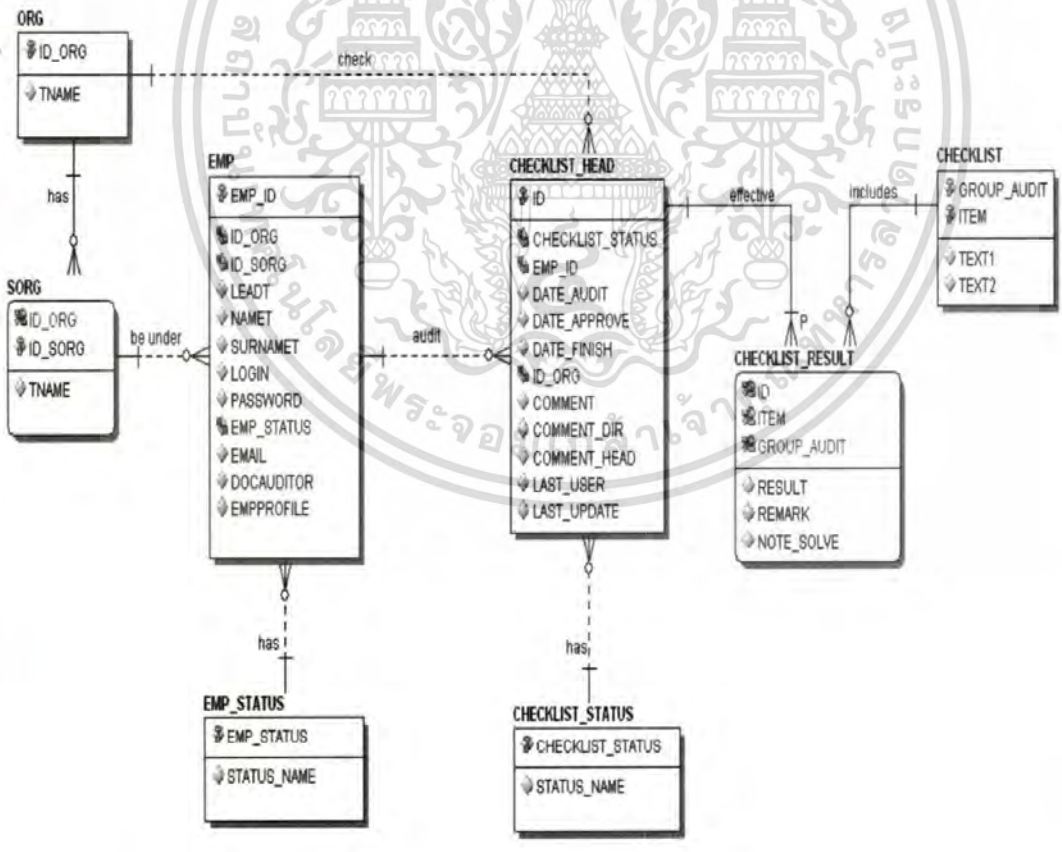
การทำงานของระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 เกี่ยวข้องกับการยืนยันส่งผลการตรวจประเมิน การตรวจสอบผลการตรวจประเมิน การรับรองผลการตรวจประเมิน ข้อมูลต่างๆ ซึ่งรอการรับรองผลการตรวจประเมิน จะต้องได้รับรองผลจากผู้อำนวยการศูนย์ฯ ซึ่งสามารถจำลองสถานะได้โดยใช้สเตทชาร์ตไดอะแกรมได้ดังรูปที่ 4.36

รูปที่ 4.36 สเตทชาร์ตไดอะแกรมการตรวจประเมิน

จากรูปสามารถอธิบายการเปลี่ยนสถานะของการประเมินตามข้อกำหนด ISO/IEC 27001 ได้ คือเริ่มจากผู้ตรวจประเมินบันทึกผลการตรวจประเมินโดยใช้ยูสเคส " บันทึกผลการตรวจประเมิน" เมื่อกดบันทึกข้อมูล สถานะผลการประเมินเป็นรอการยืนยันส่งผลข้อมูล เมื่อผู้ตรวจประเมินกดปุ่มยืนยันข้อมูล สถานะผลการประเมินจะเปลี่ยนเป็นรอตรวจสอบผลการประเมิน ซึ่งผู้บริหารระบบจะใช้ยูสเคส "ตรวจสอบผลการประเมิน" เพื่อตรวจสอบผลการประเมินที่ผู้ตรวจประเมินส่งมา และเมื่อผู้บริหารระบบตรวจสอบผลการประเมินผ่าน สถานะการประเมินจะเป็นการรอรับรองผลการตรวจประเมิน ซึ่งผู้อำนวยการศูนย์จะใช้ยูสเคส "รับรองผลการประเมิน" เมื่อผู้อำนวยการศูนย์รับรองผลการตรวจประเมิน สถานะผลการประเมินจะสิ้นสุด

4.7 การออกแบบระบบฐานข้อมูล

จากการวิเคราะห์โครงสร้างและคลาสไดอะแกรมของระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 ที่ได้กล่าวไว้ในข้อที่แล้วมา สามารถนำมาออกแบบฐานข้อมูลเชิงสัมพันธ์ โดยใช้แผนภาพความสัมพันธ์ระหว่างเอนทิตี ดังรูปที่ 4.37



รูปที่ 4.37 อีอาร์ไดอะแกรมของระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001

ประกอบด้วยตารางเอนทิตีสำหรับจัดเก็บข้อมูลต่างๆ ดังนี้

1. เอนทิตีพนักงาน (EMP) เก็บข้อมูลเกี่ยวกับเจ้าหน้าที่กรมโรงงานอุตสาหกรรม ได้แก่ รหัสพนักงาน รหัสสำนัก รหัสกอง คำนำหน้าชื่อ ชื่อ นามสกุล ชื่อผู้ใช้ รหัสผ่าน รหัสสถานะผู้ตรวจประเมิน อีเมลล์ ชื่อไฟล์เอกสารแต่งตั้งผู้ตรวจประเมิน และข้อมูลส่วนตัวของผู้ตรวจประเมิน

2. เอนทิตีสำนัก (ORG) เก็บข้อมูลเกี่ยวกับ รหัสสำนัก ชื่อสำนัก

3. เอนทิตีกอง (SORG) เก็บข้อมูลเกี่ยวกับ รหัสสำนัก รหัสกอง ชื่อกองภายในสำนัก

4. เอนทิตีแบบฟอร์มการประเมิน (CHECKLIST) เก็บข้อมูลเกี่ยวกับแบบฟอร์มการประเมิน ได้แก่ รหัสกลุ่มคำถาม รหัสคำถาม รายละเอียดข้อกำหนด รายละเอียดคำถาม

5. เอนทิตีผลการตรวจประเมิน (CHECKLIST_HEAD) เก็บข้อมูลเกี่ยวกับการตรวจประเมิน ได้แก่ เลขที่การตรวจประเมิน รหัสสถานการณ์ตรวจประเมิน รหัสพนักงาน วันที่ตรวจประเมิน วันที่ตรวจสอบผลการตรวจประเมิน วันที่รับรองผลการตรวจประเมิน รหัสสำนัก หมายเหตุ ข้อคิดเห็นของผู้อำนวยการศูนย์ฯ ข้อคิดเห็นของผู้บริหารระบบ เจ้าหน้าที่ปรับปรุงข้อมูล วันที่ปรับปรุงข้อมูล

6. เอนทิตีรายละเอียดผลการตรวจประเมิน (CHECKLIST_RESULT) เก็บข้อมูลเกี่ยวกับรายการคำถามตามแบบฟอร์ม ได้แก่ เลขที่การตรวจประเมิน รหัสกลุ่มคำถาม รหัสคำถาม ผลการตรวจประเมิน หลักฐานที่พบ แนวทางการแก้ไขข้อที่ไม่สอดคล้องตาม ISO/IEC 27001

7. เอนทิตีสถานะแบบประเมิน (CHECKLIST_STATUS) เก็บข้อมูลเกี่ยวกับ รหัสสถานะการตรวจประเมิน และชื่อสถานะการตรวจปประเมิน โดยค่าสถานะแบบประเมินมีดังนี้

0 - ยังไม่ได้ยืนส่งข้อมูล

1 - ยืนยันส่งข้อมูล

2 - ผลการตรวจสอบผ่าน

3 - ผลการตรวจสอบไม่ผ่าน

4 - รับรองผลการประเมิน

5 - ไม่รับรองผลการประเมิน

8. เอนทิตีสถานะผู้ตรวจประเมิน (EMP_STATUS) เก็บข้อมูลเกี่ยวกับ รหัสสถานะผู้ตรวจประเมิน และชื่อสถานะผู้ตรวจประเมิน โดยมีสถานะดังนี้

0 - สถานะเป็นผู้บริหารระบบ

1 - สถานะผู้ตรวจประเมินระดับผู้บริหาร

2 - สถานะผู้ตรวจประเมินระดับเจ้าหน้าที่ศูนย์สารสนเทศ

3 - สถานะผู้ตรวจประเมินระดับผู้ใช้ทั่วไป

พจนานุกรมข้อมูล (Data Dictionary) มีตารางเอนทิตีทั้งหมด 8 เอนทิตี ซึ่งแสดงไว้ในตารางที่ 4.9 ถึงตารางที่ 4.17

ตารางที่ 4.9 พจนานุกรมข้อมูล EMP

แอตทริบิวต์	ความหมาย	ชนิดของข้อมูล	ขอบเขต	คีย์	ตารางที่อ้างอิง
EMP_ID	รหัสพนักงาน	Text	10	PK	
ID_ORG	รหัสสำนัก	Number		FK	SORG
ID_SORG	รหัสกอง	Number		FK	SORG
LEADT	คำนำหน้าชื่อ	Text	50		
NAMET	ชื่อ	Text	100		
SURNAMET	นามสกุล	Text	100		
LOGIN	ชื่อผู้ใช้	Text	10		
PASSWORD	รหัสผ่าน	Text	10		
EMP_STATUS	รหัสสถานะผู้ตรวจประเมิน	Number		FK	EMP_STATUS
EMAIL	อีเมล์	Text	30		
DOCAUDITOR	ชื่อไฟล์เอกสารแต่งตั้งผู้ตรวจประเมิน	Text	50		
EMPPROFILE	ข้อมูลส่วนตัวของผู้ตรวจประเมิน	Text	200		

ตารางที่ 4.10 พจนานุกรมข้อมูล ORG

แอตทริบิวต์	ความหมาย	ชนิดของข้อมูล	ขอบเขต	คีย์	ตารางที่อ้างอิง
ID_ORG	รหัสสำนัก	Number		PK	
TNAME	ชื่อสำนัก	Text	80		

ตารางที่ 4.11 พจนานุกรมข้อมูล SORG

แอตทริบิวต์	ความหมาย	ชนิดของข้อมูล	ขอบเขต	คีย์	ตารางที่อ้างอิง
ID_ORG	รหัสสำนัก	Number		PK,FK	ORG
ID_SORG	รหัสกอง	Number		PK	
TNAME	ชื่อกอง	Text	80		

ตารางที่ 4.12 พจนานุกรมข้อมูล CHECKLIST

แอตทริบิวต์	ความหมาย	ชนิดของข้อมูล	ขอบเขต	คีย์	ตารางที่ อ้างอิง
GROUP_AUDIT	รหัสกลุ่มคำถาม	Number		PK	
ITEM	รหัสคำถาม	Text	10	PK	
TEXT 1	รายละเอียดข้อกำหนด	Text	200		
TEXT 2	รายละเอียดคำถาม	Text	200		

ตารางที่ 4.13 พจนานุกรมข้อมูล CHECKLIST_HEAD

แอตทริบิวต์	ความหมาย	ชนิดของข้อมูล	ขอบเขต	คีย์	ตารางที่อ้างอิง
ID	เลขที่การตรวจประเมิน	Number		PK	
CHECKLIST_ STATUS	รหัสสถานะการตรวจประเมิน	Number		FK	CHECKLIST _STATUS
EMP_ID	รหัสพนักงาน	Text	10	FK	EMP
DATE_AUDIT	วันที่ตรวจประเมิน	Date			
DATE_APPROVE	วันที่ตรวจสอบผลการตรวจประเมิน	Date			
DATE_FINISH	วันที่รับรองผลการตรวจประเมิน	Date			
ID_ORG	รหัสสำนัก	Number		FK	ORG
COMMENT	หมายเหตุ	Text	200		
COMMENT_ DIR	ข้อคิดเห็นของผู้อำนวยการศูนย์ฯ	Text	200		
COMMENT_ HEAD	ข้อคิดเห็นของผู้บริหารระบบ	Text	200		
LAST_USER	เจ้าหน้าที่ปรับปรุงข้อมูล	Text	50		
LAST_UPDATE	วันที่ปรับปรุงข้อมูล	Date/Time			

ตารางที่ 4.14 พจนานุกรมข้อมูล CHECKLIST_RESULT

แอตทริบิวต์	ความหมาย	ชนิดของข้อมูล	ขอบเขต	คีย์	ตารางที่อ้างอิง
ID	เลขที่การตรวจประเมิน	Number		PK,FK	CHECKLIST_HEAD
GROUP_AUDIT	รหัสกลุ่มคำถาม	Number		PK,FK	CHECKLIST
ITEM	รหัสคำถาม	Text	10	PK,FK	CHECKLIST
RESULT	ผลการตรวจประเมิน	Text	1		
REMARK	หลักฐานที่พบ	Text	200		
NOTE_SOLVE	แนวทางการแก้ไขข้อที่ไม่สอดคล้องตาม ISO/IEC 27001	Text	200		

ตารางที่ 4.15 พจนานุกรมข้อมูล CHECKLIST_STATUS

แอตทริบิวต์	ความหมาย	ชนิดของข้อมูล	ขอบเขต	คีย์	ตารางที่อ้างอิง
CHECKLIST_STATUS	รหัสสถานะการตรวจประเมิน	Number		PK	
STATUS_NAME	ชื่อสถานะการตรวจประเมิน	Text	50		

ตารางที่ 4.16 พจนานุกรมข้อมูล EMP_STATUS

แอตทริบิวต์	ความหมาย	ชนิดของข้อมูล	ขอบเขต	คีย์	ตารางที่อ้างอิง
EMP _STATUS	รหัสสถานะผู้ตรวจประเมิน	Number		PK	
STATUS_NAME	ชื่อสถานะผู้ตรวจประเมิน	Text	50		

บทที่ 5

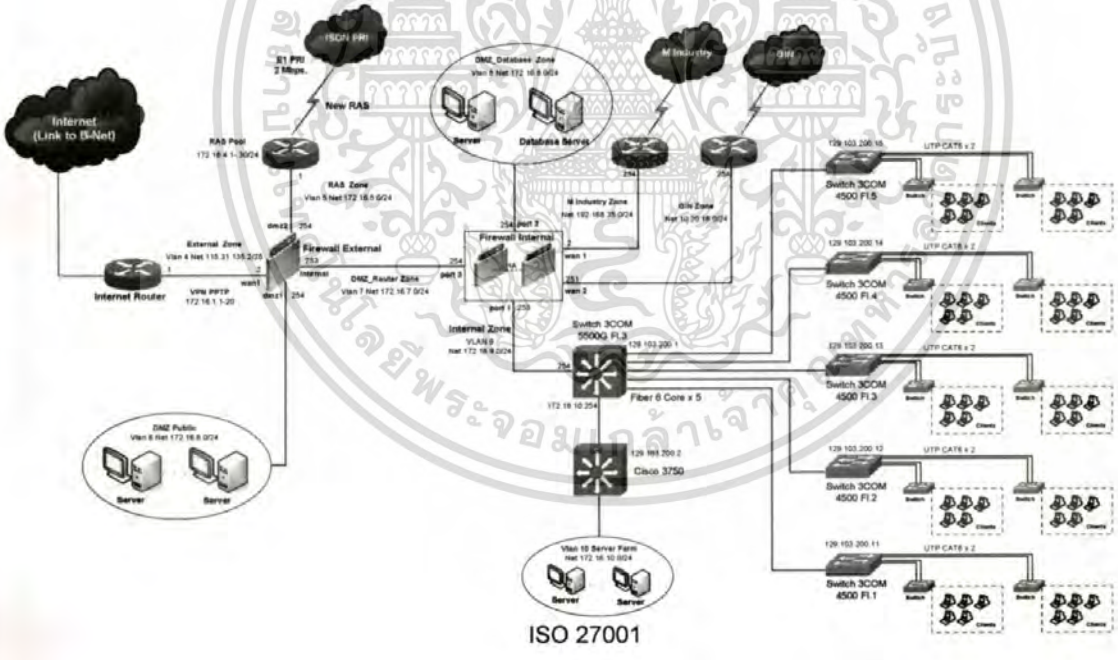
การออกแบบระบบ

จากการวิเคราะห์และออกแบบระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 ดังที่ผ่านมาในตอนต้นนั้น ทำให้สามารถออกแบบระบบออกมาได้ในลักษณะของเว็บแอพพลิเคชัน เพื่อให้ผู้ใช้งานสามารถใช้งานระบบผ่านเว็บบราวเซอร์ โดยอาศัยเครือข่ายอินเทอร์เน็ต ซึ่งในบทนี้จะแสดงให้เห็นถึงภาพรวมของระบบ ซึ่งจะทำให้ผู้ใช้งานระบบสามารถเข้าใจขั้นตอนในการทำงานมากยิ่งขึ้น

5.1 แบบจำลองเชิงกายภาพของระบบงานใหม่

5.1.1 สถาปัตยกรรมของระบบ

ระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 ได้ออกแบบสถาปัตยกรรมแบบ Three Tier ดังรูปที่ 5.1



รูปที่ 5.1 สถาปัตยกรรมระบบของกรมโรงงานอุตสาหกรรม

เนื่องจากกรมโรงงานอุตสาหกรรมมีเครื่องแม่ข่ายที่ให้บริการข้อมูล website อยู่แล้ว และเครื่องดังกล่าวสามารถที่จะรองรับการทำงานของระบบบริหารความปลอดภัย ISO/IEC 27001 ได้จึงใช้เครื่องแม่ข่ายที่มีอยู่เดิม โดยเครื่องมีคุณสมบัติดังนี้

- หน่วยประมวลผลแบบ Xeon จำนวน 2 CPU ความเร็วสัญญาณนาฬิกา 2.4 GHz
- หน่วยความจำหลัก (Main Memory) ขนาด 512 MB
- หน่วยความจำสำรอง (Hard Disk) แบบ SCSI ขนาด 36 GB จำนวน 2 ชุด
- อุปกรณ์สำรองข้อมูล (Tape Backup) แบบ DDS4 ชนิดติดตั้งภายใน
- ระบบปฏิบัติการ Windows 2000 Server พร้อมด้วยโปรแกรม IIS (Internet Information Server)

สำหรับเครื่องแม่ข่ายที่ให้บริการระบบจัดการฐานข้อมูลจะใช้กับเครื่องเดิมคือ เครื่อง SUN 5500 ซึ่งใช้ระบบปฏิบัติการ Solaris version 2.7 และเครื่องคอมพิวเตอร์ที่ใช้พัฒนาระบบงานจะใช้เครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Windows XP และใช้โปรแกรม Internet Explorer 6 ในการทดลองเรียกใช้ โดยตั้งความละเอียดหน้าจอ 800x600 pixels และ 1024x768 pixels

5.1.2 โปรแกรมสำหรับออกแบบและพัฒนาระบบ

ภาษาที่ใช้ในการพัฒนาแบ่งเป็น 2 ส่วน คือ

1. HTML (Hyper Text Markup Language) เป็นภาษามาตรฐานสำหรับติดต่อกันบนอินเทอร์เน็ต โดยใช้โปรโตคอล HTTP ภาษา HTML นั้นเป็นส่วนที่ตัดมาจากภาษา GHTML ซึ่ง GHTML นั้นจะมี Code และวิธีเขียนที่ซับซ้อนมากกว่า แต่ก็มีเป้าหมายเดิม คือเครื่องที่ใช้โปรแกรมระบบทุกตัวสามารถดูใช้งาน ศึกษาร่วมกันใช้ข้อมูลต่าง ๆ ได้อย่างไม่มีปัญหาและเพื่อให้เข้าสู่ยุคโลกไร้พรมแดนในการจัดการรูปแบบหน้าจอสำหรับระบบทั้งหมดเสียก่อน

2. ASP (Active Server Pages) ซึ่งคิดค้นโดยบริษัทไมโครซอฟต์ ASP เป็นโปรแกรมคอมพิวเตอร์ชนิดที่เป็น "Server side scripting" ซึ่งหมายถึงภาษาทางโปรแกรมที่ทำงานในฝั่งของเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์ที่ให้บริการเอกสารหรือสื่อต่างๆ ในอินเทอร์เน็ตหรืออินทราเน็ต ASP จะทำงานบนเซิร์ฟเวอร์และทำงานร่วมกับโปรแกรมเว็บเซิร์ฟเวอร์ทำหน้าที่ประมวลข้อมูลที่ได้จากผู้เข้ามาใช้งานและแสดงผลออกมาทาง Web browser โดยส่วนใหญ่แล้วขบวนการจะประกอบไปด้วยการสืบค้นข้อมูล การแสดงรายการ ผลการสืบค้น การแสดงแบบฟอร์มเพื่อให้ผู้ใช้งานบันทึกข้อมูลหรือทำการแก้ไข และการดำเนินการประมวลผลพร้อมจัดเก็บข้อมูล

5.2 การออกแบบระบบ

หลังจากที่ได้ออกแบบระบบงานใหม่แล้ว จะต้องมีการพัฒนาระบบทางกายภาพเพื่อสร้างระบบให้สามารถใช้งานได้จริง ซึ่งมีรายละเอียดดังต่อไปนี้

1 จัดเตรียมอุปกรณ์และโปรแกรมสำหรับเครื่องแม่ข่ายสำหรับบริการ World Wide Web (เว็บเซิร์ฟเวอร์)

- ระบบปฏิบัติการ (Operating System) คือ Microsoft Window 2000 Server

2 เครื่องแม่ข่ายสำหรับบริการฐานข้อมูล (Database Server)

- ระบบปฏิบัติการ (Operating System) คือ Microsoft Window 2000 Server
- ระบบบริหารฐานข้อมูล (Database Management System) คือ MS SQL Server 2000

3 เครื่องลูกข่าย (Client)

- ระบบปฏิบัติการ (Operating System) คือ Window 98 Window Me Window 2000 Window XP
- โปรแกรมประยุกต์ (Application Program) คือ Internet Explorer version 5 ขึ้นไป

บทที่ 6
บทสรุป

6.1 สรุปผลการออกแบบระบบ

โครงการนี้ได้เสนอแนวคิดการวิเคราะห์ ออกแบบระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 ของศูนย์สารสนเทศโรงงานอุตสาหกรรม กรมโรงงานอุตสาหกรรม โดยผ่านเครือข่ายอินเทอร์เน็ต ทำให้เป็นการเพิ่มช่องทางในการให้บริการแก่ผู้ใช้ภายในองค์กร ช่วยให้การบริการเกิดความสะดวกรวดเร็วโปร่งใสและสามารถตอบสนองความต้องการของผู้ใช้งานได้เป็นอย่างดี ผู้จัดทำได้ใช้ Unified Modeling Language (UML) เป็นเครื่องมือช่วยในขั้นตอนการออกแบบระบบไดอะแกรมต่างๆ ของระบบประกอบด้วยยูสเคสไดอะแกรม แอกทิวิตีไดอะแกรม คลาสไดอะแกรมและสเตทชาร์ตไดอะแกรม ซึ่งสามารถนำไปออกแบบเป็นระบบที่สมบูรณ์และสามารถใช้งานได้จริงต่อไปในอนาคต

6.2 ข้อจำกัดของระบบ

ระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 มีข้อจำกัดคือ

- ให้บริการผ่านระบบเครือข่ายอินเทอร์เน็ตเท่านั้น หากระบบเครือข่ายมีปัญหาจะทำให้ไม่สามารถใช้งานระบบได้
- ผู้ใช้ระบบต้องมีความรู้พื้นฐานด้านคอมพิวเตอร์

6.3 ข้อเสนอแนะในการพัฒนาต่อ

ระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 นี้ได้มีการพัฒนา และทดสอบระบบเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพแล้วในระดับหนึ่ง โดยได้ทดสอบตามขั้นตอนการใช้งานเท่านั้น ซึ่งหากมีการนำไปใช้งานจริงอาจพบว่ามีบางหัวข้อที่ควรเพิ่มเติมเพื่อสนับสนุนการดำเนินงานให้ดียิ่งขึ้น หรือมีบางหัวข้อหากไม่ได้รับการใช้งานอาจต้องตัดออก เพื่อให้ระบบเกิดความคล่องตัวให้การให้บริการระบบบริหารความปลอดภัยสำหรับข้อมูลสารสนเทศ ISO/IEC 27001 นี้จะดำเนินการต่อไปได้ต้องได้รับการสนับสนุนจากผู้บริหารและผู้ใช้งานให้การสนับสนุนเพื่อที่จะมาพัฒนาระบบให้ใช้งานได้ตรงตามต้องการและเหมาะสมต่อไป

บรรณานุกรม

กิตติ ภักดีวัฒนะกุล และกิตติพงษ์ กลมกล่อม. 2547. **UML วิเคราะห์และออกแบบเชิงวัตถุ**. กรุงเทพฯ : เคทีพี คอมพ์ แอนด์ คอนซัลท์.

บรรจง หะรังสี และญาณวรรณ สินธุภิญโญ. 2548. **โปรแกรมเชิงวัตถุและยูเอ็มแอล**. [ออนไลน์]. เข้าถึงได้จาก: http://www.thaiall.com/uml

วิเชียร เปรมชัยสวัสดิ์. 2546. **ระบบฐานข้อมูล.** กรุงเทพฯ: สมาคมส่งเสริมเทคโนโลยี (ไทย-ญี่ปุ่น).

สุนทริน วงศ์ศิริกุล. 2545. **พัฒนาโมเดลยุคใหม่ UML มาตรฐานการสร้างโมเดลระบบงาน.** กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

โอภาส เอี่ยมสิริวงศ์. 2547. **การวิเคราะห์และออกแบบระบบ.** กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

ประวัติผู้เขียน

ผู้เขียน	นายธงชัย อุทัยจรัสรัศมี
วันเดือนปีเกิด	25 มกราคม 2504
สถานที่เกิด	กรุงเทพมหานคร
ประวัติการศึกษา	ปริญญาวิศวกรรมศาสตรบัณฑิต (วิศวกรรมอุตสาหการ) คณะวิศวกรรมเทคโนโลยี สถาบันเทคโนโลยีราชมงคล
ประวัติการทำงาน	กรมโรงงานอุตสาหกรรม ศูนย์สารสนเทศโรงงานอุตสาหกรรม ตำแหน่ง ผู้อำนวยการกลุ่มบริการอุปกรณ์และระบบเครือข่าย