การพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิต

นายกวิน บุญทวี

การศึกษาค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
เขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2559

Prototype Development of IT Audit and Quality Control for Truck Dealer Business Based on IT Governance and COBIT Framework

Mr. Kawin Boonthavee

An Independent Study Submitted in Partial Fulfillment of the Requirements for
the Degree of Master of Science in Information and Communication Technology
School of Science and Technology
Sukhothai Thammathirat Open University
2016

หัวข้อการศึกษาค้นคว้าอิสระ การพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิต

ชื่อและนามสกุล นายกวิน บุญทวี

แขนงวิชา เทคโนโลยีสารสนเทศและการสื่อสาร

สาขาวิชา วิทยาศาสตร์และเทคโนโลยีมหาวิทยาลัยสุโขทัยธรรมาธิราช

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร. วิภา เจริญภัณฑารักษ์

การศึกษาค้นคว้าอิสระนี้ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 31 ตุลาคม 2559

คณะกรรมการสอบการศึกษาค้นคว้าอิสระ

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร. วิภา เจริญภัณฑารักษ์)

..... กรรมการ
(อาจารย์ ดร. ดวงดาว วิชาดากุล)

.....
(รองศาสตราจารย์วรัญญา ปุณณวัฒน์)
ประธานกรรมการประจำสาขาวิชาวิทยาศาสตร์และเทคโนโลยี

ชื่อการศึกษาค้นคว้าอิสระ การพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิต

ผู้ศึกษา นายกวิน บุญทวี **รหัสนักศึกษา** 2579600194

ปริญญา วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร)

อาจารย์ที่ปรึกษา รองศาสตราจารย์ ดร. วิภา เจริญภัณฑารักษ์ **ปีการศึกษา** 2559

บทคัดย่อ

การศึกษาครั้งนี้จึงมีวัตถุประสงค์เพื่อ 1) ออกแบบและพัฒนาระบบควบคุมภาพงานสารสนเทศสำหรับธุรกิจจำหน่ายรถบรรทุก 2) สร้างและประเมินต้นแบบเพื่อรับการตรวจสอบระบบสารสนเทศจากผู้ตรวจสอบภายนอกโดยใช้แนวคิดวงจรควบคุมคุณภาพได้แก่ 1) วางแผนการดำเนินงาน (Plan) โดยรวบรวมรายการตรวจคุณภาพด้านสารสนเทศ วางแผนนำข้อมูลเข้าสู่ระบบ 2) ปฏิบัติตามแผน (DO)คือ พัฒนาระบบตรวจสอบมาตรฐานระบบสารสนเทศ 3) ตรวจสอบ (CHECK) คือ ทดสอบความปลอดภัยของระบบ และทดสอบสิทธิการใช้งาน เป็นการทดสอบการกำหนดสิทธิต่างๆ 4) ปรับปรุงการดำเนินการอย่างเหมาะสม (ACT) ได้แก่ ความเหมาะสมในการให้คะแนนการประเมินมาตรฐาน ปรับปรุงหน้าจอ การบันทึกข้อมูลลงระบบ ข้อมูลที่ใช้ในการพัฒนาประกอบด้วย รายการการตรวจคุณภาพด้านสารสนเทศ เอกสารหลักฐานที่ใช้ในการควบคุมระบบสารสนเทศของบริษัทและข้อมูลต่างๆ ของแผนกสารสนเทศ โดยใช้โปรแกรมไมโครซอฟเอกเซล และโปรแกรมไมโครซอฟแอกเซส สร้างเครื่องมือช่วยประเมินคุณภาพด้านสารสนเทศขององค์กร

ผลการศึกษาพบว่าระบบสารสนเทศที่พัฒนาขึ้นสามารถลดข้อบกพร่อง และควบคุมคุณภาพงานสารสนเทศได้ดีขึ้น เป็นที่ยอมรับจากผู้ตรวจสอบระบบสารสนเทศภายนอกตามหลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิตมากยิ่งขึ้นเช่น ความปลอดภัยในการเข้าถึงข้อมูล การปฏิบัติตามนโยบายด้านสารสนเทศ ฯลฯ และหลังจากที่ทดสอบเครื่องควบคุมคุณภาพระบบสารสนเทศที่พัฒนาขึ้นมา สามารถช่วยในการลดจุดบกพร่องควบคุมคุณภาพได้ดีขึ้น ทำให้เกิดการยอมรับจากผู้ตรวจสอบระบบสารสนเทศในการควบคุมคุณภาพงานด้านสารสนเทศโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิตมากยิ่งขึ้น

คำสำคัญ ต้นแบบระบบตรวจสอบ, ควบคุมคุณภาพงานไอที, ธุรกิจจำหน่ายรถบรรทุก, โคบิตเวอร์ชั่น 5, หลักธรรมาภิบาลไอที

Independent Study title: Prototype Development of IT Audit and Quality Control for Truck Dealer Business Based on IT Governance and COBIT Framework
Author: Mr. Kawin Boonthavee; **ID**: 2579600723;
Degree: Master of Science (Information and Communication Technology);
Independent Study advisor: Dr. VipaJaroenpuntaruk, Associate Professor;
Academic year: 2016

Abstract

This study aims at these 2 objectives :1 . To design and develop an IT quality control system for truck dealing business 2. To generate and assess prototype of an IT system for external audition based on the following Deming Cycles 1 . Planning: Information and report gathering , data integration into the system. 2. Do: Developing the IT system standardization. 3 . Checking : the system security and permission. 4. Act: Improving appropriate operation which includes standard scoring , improving user interface, data entry. The data used for system development include IT quality check list , document control and evidence used in IT system control , Using Microsoft Excel and Microsoft Access application in order to generate assessment tools for the IT department.

It has been found that the developed quality control tool can decrease some deficiencies and can better control the quality of the IT system. Acceptance by external auditor based on IT governance and IT Cobit frame work has been achieved.

Keywords: Prototype development, Quality control IT audit, Truck dealer business based, COBIT 5, IT Governance

กิตติกรรมประกาศ

การค้นคว้าแบบอิสระเรื่อง การพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิต ฉบับนี้สำเร็จลุล่วงได้ด้วยความกรุณาจากบุคลากรและผู้ทรงคุณวุฒิหลายท่านที่ได้อนุเคราะห์ให้ความช่วยเหลืออย่างดียิ่ง โดยเฉพาะรองศาสตราจารย์ดร. วิภา เจริญภัณฑารักษ์ ที่ได้ให้ความกรุณาให้คำแนะนำและติดตามการทำการค้นคว้าแบบอิสระครั้งนี้อย่างใกล้ชิดตลอดมา นับตั้งแต่เริ่มต้นจนกระทั่งสำเร็จเรียบร้อยสมบูรณ์ และอาจารย์ ดร. ดวงดาว วิชาดากุล ที่กรุณาให้ข้อคิดเห็นเพื่อปรับปรุงให้การค้นคว้าแบบอิสระเล่มนี้มีความสมบูรณ์มากยิ่งขึ้น ผู้วิจัยรู้สึกซาบซึ้งในความกรุณาของท่านทั้งสองเป็นอย่างยิ่ง

ขอขอบคุณเจ้าหน้าที่แผนกสารสนเทศ บริษัท มิตซุย บุซซัน ออโตโมทีฟ (ประเทศไทย) จำกัดที่ได้ให้ความร่วมมือในการจัดเตรียมข้อมูลในการวิจัยในครั้งนี้เป็นไปด้วยความเรียบร้อยอย่างดียิ่ง

สุดท้ายนี้ ประโยชน์ของการศึกษาครั้งนี้ ขอมอบเป็นเครื่องบูชาพระคุณบิดา คุณมารดา บรรดาคณาจารย์ และผู้มีพระคุณทุกท่านที่มีส่วนช่วยให้การศึกษาค้นคว้าอิสระครั้งนี้สำเร็จได้ด้วยดี

กวิน บุญทวี

ตุลาคม 2559

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง

บทคัดย่อภาษาอังกฤษ ..... จ

กิตติกรรมประกาศ ..... ฉ

สารบัญตาราง ..... ฌ

สารบัญภาพ ..... ญ

บทที่ 1 บทนำ 1

ความเป็นมาและความสำคัญของปัญหา 1

วัตถุประสงค์การวิจัย 3

ขอบเขตของการวิจัย 3

เครื่องมือที่ใช้ในการวิจัย 4

นิยามศัพท์เฉพาะ 4

ประโยชน์ที่คาดว่าจะได้รับ 6

บทที่ 2 วรรณกรรมที่เกี่ยวข้อง 7

แนวคิดธรรมาภิบาลด้านไอที (IT Governance) 7

กรอบมาตรฐานโคบิต (Cobit) 11

กรอบการดำเนินงานมาตรฐาน ISO/IEC 27001 19

กรอบงานไอทิล (ITIL Framework) 24

แนวคิดโคโซ (COSO) 30

ไมโครซอฟท์แอคเซส (Microsoft Access) 38

วงจรการบริหารงานคุณภาพ (PDCA) 39

งานวิจัยที่เกี่ยวข้อง 40

บทที่ 3 วิธีดำเนินการวิจัย 43

ขั้นตอนการดำเนินการวิจัย 43

อุปกรณ์และเครื่องมือที่ใช้ในการวิจัย 66

สารบัญ (ต่อ)

หน้า

บทที่ 4 ผลการวิเคราะห์ข้อมูล 67
ผลลัพธ์ของการออกแบบและพัฒนาระบบ 67
ผลลัพธ์ของการประเมินประสิทธิภาพของระบบ 81
บทที่ 5 สรุปการวิจัย อภิปราย และข้อเสนอแนะ 83
สรุปผลการวิจัย 83
อภิปรายผล 86
ข้อเสนอแนะ 88
บรรณานุกรม 89
ประวัติผู้ศึกษา 93

สารบัญตาราง

หน้า

ตารางที่ 3.1 วงจรเดมิง 43
ตารางที่ 3.2 ตารางแสดงรายการการตรวจสอบคุณภาพของระบบสารสนเทศทั้ง 8 ด้าน 74 รายการ จากผู้ตรวจสอบด้านสารสนเทศ 46
ตารางที่ 3.3 แสดงประเมินสถานะความพร้อมระบบตรวจสอบมาตรฐานระบบสารสนเทศ โดยโปรแกรม Microsoft Access 59
ตารางที่ 3.4 ตารางหัวข้อหลักในการตรวจสอบด้านต่างๆ ของระบบสารสนเทศ 60
ตารางที่ 3.5 ตารางเอกสารและข้อมูลที่ทางผู้ตรวจสอบต้องการ 60
ตารางที่ 3.6 ตารางสถานะคุณภาพ 61
ตารางที่ 3.7 ตารางผู้ใช้งาน 61
ตารางที่ 3.8 กลุ่ม “Admin” สามารถกำหนดสิทธิการทดสอบ 64
ตารางที่ 3.9 กลุ่ม “General user” สามารถกำหนดสิทธิการทดสอบ 64
ตารางที่ 4.1 แสดงสถานะของรายการตรวจสอบและเกณฑ์การให้คะแนน เพื่อนำไปใช้ในการวิเคราะห์คุณภาพงานด้านไอที 78
ตารางที่ 4.2 แสดงสถานะทำการบันทึกข้อมูลลงในระบบโดยการให้คะแนน ในแต่ละด้านตามเกณฑ์ 81

สารบัญภาพ

หน้า

ภาพที่ 2.1 กรอบแนวคิดของธรรมาภิบาลด้านไอที 8
ภาพที่ 2.2 องค์ประกอบของกรอบแนวคิดธรรมาภิบาลด้านไอที 9
ภาพที่ 2.3 กรอบมาตรฐานโคบิต 15
ภาพที่ 2.4 COBIT 5 Enablers 16
ภาพที่ 2.5 หลักการ Goal Cascade ของ COBIT 4.1 17
ภาพที่ 2.6 แสดงวงจรบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act (P-C-D-A) 20
ภาพที่ 2.7 ส่วนประกอบหลักของไอทิลเวอร์ชัน 3 25
ภาพที่ 2.8 กรอบแนวคิดโคโซ (COSO) 31
ภาพที่ 2.9 หน้าต่างโปรแกรม Microsoft Access 39
ภาพที่ 2.10 วงจรคุณภาพ PDCA 40
ภาพที่ 3.1 วงจรคุณภาพ PDCA 44
ภาพที่ 3.2 ตารางหัวข้อการตรวจสอบใน 8 ด้าน จากทางผู้ตรวจสอบระบบสารสนเทศในรูปแบบไฟล์เอ็กเซล 52
ภาพที่ 3.3 หัวข้อการตรวจสอบ 8 ด้านและหัวข้อย่อย 74 หัวข้อ ในระบบตรวจสอบมาตรฐานระบบสารสนเทศ โดยโปรแกรม Microsoft Access 56
ภาพที่ 3.4 สถานะต่างๆ ที่กำหนดไว้ในระบบตรวจสอบมาตรฐานระบบสารสนเทศโดยโปรแกรม Microsoft Access 58
ภาพที่ 3.5 หน้าจอสำหรับการบันทึกข้อมูลเข้าสู่ระบบตรวจสอบมาตรฐานระบบสารสนเทศโดยโปรแกรม Microsoft Access 59
ภาพที่ 3.6 Use Case ระบบตรวจสอบและควบคุมคุณภาพงานไอที 62
ภาพที่ 4.1 แสดงหน้าจอ login ชื่อผู้ใช้และรหัสผ่าน 68
ภาพที่ 4.2 แสดงหน้าจอการสร้างผู้ใช้งาน (User) และกลุ่ม (GROUP) การใช้งาน 68
ภาพที่ 4.3 แสดงตัวอย่างการสั่งพิมพ์รายชื่อผู้ใช้งาน (User) และกลุ่มการใช้งาน (Group) 69
ภาพที่ 4.4 แสดงแถบการทำงาน Groups 70
ภาพที่ 4.5 แถบการทำงาน Change Logon Password 71

สารบัญภาพ (ต่อ)

หน้า

ภาพที่ 4.6 รูปแสดงหน้าจอการกำหนดสิทธิในการใช้งานระบบของ Admin 72
ภาพที่ 4.7 รูปแสดงหน้าจอการกำหนดสิทธิในการใช้งานระบบของ Auditor 73
ภาพที่ 4.8 รูปแสดงหน้าจอการเปลี่ยนแปลงสิทธิการใช้งาน 74
ภาพที่ 4.9 แสดงหน้าจอการใช้งานระบบตรวจสอบและควบคุมคุณภาพงานไอที 75
ภาพที่ 4.10 รายละเอียดหัวข้อต่างๆ ในการตรวจสอบระบบสารสนเทศของ File Excel 76
ภาพที่ 4.11 แสดงหน้าจอรายละเอียดระบบตรวจสอบและควบคุมคุณภาพงานไอทีเพื่อใช้สำหรับการนำข้อมูลจากผู้ตรวจสอบทางสารสนเทศที่อยู่ในรูปแบบของ File Excel 77
ภาพที่ 4.12 ภาพหน้าต่างการทำงานของ Setup Audit Group 79
ภาพที่ 4.13 แสดงตัวอย่างภาพกราฟแสดงสถานะคุณภาพด้านเทคโนโลยีจากการประเมิน 80
ภาพที่ 4.14 แสดงสถานะด้วยการใช้สีในช่อง indicator ในการสื่อความหมายของคุณภาพด้านต่างๆ ของระบบสารสนเทศ 80
ภาพที่ 4.15 แสดงของทำงานของ IT Audit List Requirement โดยใช้สีเป็นตัววัดคุณภาพ สีเขียวเข้ม 100 / สีเขียวอ่อน / สีเหลือง 81
ภาพที่ 4.16 แสดงของทำงานของ IT Audit List Requirement 82

บรรณานุกรม

บรรณานุกรม

กัลยา ใจรักษ์ และประสงค์ ปราณีตพลกรัง. (2555: น.4). IT Governance: A Tutorial ธรรมาภิบาลด้านไอทีเข้าถึงได้จาก: http://www.spu.ac.th/graduate/files/2011/03/IT-Governance-Tutorial_kallaya.pdf (วันที่ค้นข้อมูล: 9 กันยายน 2559).

การจัดการความรู้ประจำปี. (2557). *การเขียนผังการปฏิบัติงาน (Flow chart) ด้วยวงจรคุณภาพ PDCA เพื่อการจัดทำคู่มือการปฏิบัติงาน (Work manual) ของบุคลากรสายสนับสนุนในวิทยาเขตจันทบุรี มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกวิทยาเขตจันทบุรี* เข้าถึงได้จาก: http://www.chan.rmutto.ac.th/ckeditor/userfiles/files/km/km57.pdf (วันที่ค้นข้อมูล: 9 กันยายน2559).

กำพล ศรธนะรัตน์. (2553). *IT governance: How to success?*.เอกสารประกอบการสัมมนา IT governance: How to success?เขตอุตสาหกรรมซอฟต์แวร์แห่งประเทศไทย.

กิติมาสุราชและ วิภาเจริญภัณฑารักษ์. (2557). *การประยุกต์ธุรกิจอัจฉริยะในการบริหารงานจัดซื้อจัดจ้างในธุรกิจซ่อมเรือ : กรณีของ บริษัท อู่เรือ มารีน แอ็คมี ไทย จำกัด*. การจัดประชุมเสนอผลงานวิจัยระดับบัณฑิตศึกษา มหาวิทยาลัยสุโขทัยธรรมาธิราช ครั้งที่ 4.

จิณห์ระพีร์ พุ่มสงวน. (ไม่ปรากฏปีพิมพ์). *การควบคุมภายในตามแนวทางของ COSO* เข้าถึงได้จาก: http://rama4.mahidol.ac.th/risk_mgt/?q=article/05252014-1648 (วันที่ค้นข้อมูล: 9 กันยายน2559).

ชุติกาญจน์ เพชรรักษ์. (2556). *กรอบงานโคบิต (CoBIT Framework)*.เข้าถึงได้จาก: http://chutikan220.blogspot.com/2013/01/cobit-framework_28.html (วันที่ค้นข้อมูล: 9 กันยายน 2559).

ทวีศักดิ์ กออนันตกูล, ชฎามาศ ธุระเศรษฐ, พันธศักดิ์ ศิริรัชตพงษ์, กุสุรางคณา วายุภาพและ ศิวรักษ์ ศิวโมกษธรรม. (2550). *มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์*. ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี.

เทพฤทธิ์ ฤทธิ์ทองพิทักษ์. (2551). *IT Infrastructure Library (ITIL)*. เข้าถึงได้จาก: http://www.tmi.or.th/index.php?option=com_content&view=article&id=282&catid=27:it-infrastructure&Itemid=49 (วันที่ค้นข้อมูล: 9 กันยายน2559).

นงลักษณ์ กอศรีลบุตร. (2549). *การนำมาตรฐาน COBIT มาประยุกต์ใช้ในองค์กร เพื่อปรับปรุงกระบวนการตรวจสอบระบบสารสนเทศ กรณีศึกษา: ผู้ประกอบการธุรกิจทางการเงินที่ไม่ใช่สถาบันการเงิน (Non-bank) แห่งหนึ่ง*. (วิทยานิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

บรรจง หะรังษีและภัทราวดี เหมทานนท์. (2555). *COBIT 5 กับการนำไปใช้งาน*.เข้าถึงได้จาก: http://www.tnetsecurity.com/content_audit/cobit5_implementation_step.php (วันที่ค้นข้อมูล: 22พฤศจิกายน2559).

มาตรฐาน IEEE. (2559). *IT Governance*.เข้าถึงได้จาก:http://omo57.blogspot.com/2016/03/blog-post.html. (วันที่ค้นข้อมูล: 9 กันยายน 2559).

โรลลิ่ง มีโดวส์, อิลลินอยส์บิสิเนสไวร์. (2550). *กรอบมาตรฐาน COBIT ใหม่ช่วยลดความเสี่ยงด้านไอที พร้อมปรับปรุงการปฏิบัติตามกฎเกณฑ์*.เข้าถึงได้จาก: https://www.google.co.th/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiL7fTnsLnQAhWMvI8KHawuBIUQFggbMAA&url=http%3A%2F%2Fwww.isaca.org%2FAboutISACA%2FPressroom%2FNewsReleases%2FThai%2FDocuments%2FITGIReleasesCOBIT4.1THAI.doc&usg=AFQjCNGVUc8ICzMjAFK86ZEtxSPeAZkRA&cad=rja (วันที่ค้นข้อมูล: 9 กันยายน 2559).

ศศิธร แซ่คูและ ผศ.ดร.สุรศักดิ์ มังสิงห์. (2556). การนำกรอบแนวคิด ITIL เข้ามาประยุกต์ใช้ในองค์กรให้ประสบความสำเร็จกรณีศึกษา บริษัทแอดอิน คอมพิวเตอร์กรุ๊ป จำกัด. หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม.

เศรษฐพงศ์ มะลิสุวรรณ. (2552). *มาตรฐานการรักษาความมั่นคงปลอดภัย ISO/IEC 27001 และ ISO/IEC 17799 ฉบับประเทศไทย*.เข้าถึงได้จาก:http://oknation.nationtv.tv/blog/weblog/2009/02/27/entry-4(วันที่ค้นข้อมูล: 9 กันยายน 2559).

สันติพัฒน์ อรุณธารี. (2555).*ธรรมาภิบาลด้านไอที*.ใน *ประมวลสาระชุดวิชาการจัดการเทคโนโลยีสารสนเทศและการสื่อสารเชิงกลยุทธ์* หน่วยที่ 10 หน้า 1–64 มหาวิทยาลัยสุโขทัยธรรมาธิราช บัณฑิตศึกษาสาขาวิชาวิทยาศาสตร์และเทคโนโลยี.นนทบุรี.

GunthimaChamnoiphrom.(2556).*การนำ COBIT Framework มาใช้ในการควบคุมภายในสำหรับงานเทคโนโลยีสารสนเทศ*.เข้าถึงได้จาก: http://chamnoiphrom-it.blogspot.com/2013/01/cobit-framework.html.(วันที่ค้นข้อมูล: 9 กันยายน2559).

It genius. (2558). ความรู้พื้นฐานและการใช้งานโปรแกรม Microsoft Access เบื้องต้น เข้าถึงได้จาก: http://itgenius.co.th/webboard/index.php?topic=256.0 (วันที่ค้นข้อมูล: 9 กันยายน 2559).

The 27000.org directory. (2007). *The ISO27001 Certification Process.* เข้าถึงได้จาก: http://www.27000.org/ismsprocess.htm. (วันที่ค้นข้อมูล: 9 กันยายน2559).

บทที่1
บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

บริษัท มิตซุย บุซซัน ออโตโมทีฟ (ประเทศไทย) จำกัด ได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายอย่างเป็นทางการจาก บริษัท ฮีโน่ มอเตอร์สเซลส์ (ประเทศไทย) จำกัด ในปี พ.ศ. 2524 ปัจจุบัน มีโชว์รูม 3 แห่ง คือ 1. สำนักงานใหญ่บนถนนกิ่งแก้ว จังหวัดสมุทรปราการ 2. ชลบุรี (ใกล้นิคมอมตะนคร) 3. แหลมฉบัง โดยยังให้บริการครอบคลุมพื้นที่กรุงเทพมหานครปริมณฑล รวมทั้งพื้นที่จังหวัดชลบุรีและจังหวัดใกล้เคียงอีกด้วย รวมถึงมีการจำหน่ายรถบรรทุกทั้งรูปแบบเงินสดหรือผ่อนชำระด้วยระบบเช่าซื้อหรือระบบลิสซิ่ง พร้อมบริการหลังการจำหน่าย ทั้งงานซ่อมบำรุงรถบรรทุกที่มีประสิทธิภาพและรวดเร็ว รวมถึงอะไหล่ต่างๆ ที่ไว้คอยบริการลูกค้าอย่างครบครัน ซึ่งสถานที่ตั้งของบริษัททั้ง 3 แห่งเป็นที่รู้จักกันดีในกลุ่มผู้ใช้รถบรรทุกว่าเป็นผู้นำในเรื่องศูนย์บริการมาตรฐานรถบรรทุกครบวงจร

โดยบริษัทจะมีระบบสารสนเทศเพื่อสนับสนุนการดำเนินธุรกิจในด้านต่างๆ เช่น ระบบบัญชีลูกค้าการให้บริการระบบเครือข่ายและบริการอินเทอร์เน็ตเพื่อเชื่อมโยงสาขาในการให้บริการ ฯลฯ ซึ่งที่กล่าวมานั้นถือเป็นหัวใจในการขับเคลื่อนธุรกิจในการต่อสู่กับคู่แข่งเพื่อก้าวสู่การเป็นผู้นำในธุรกิจรถบรรทุกโดยแท้จริง ระบบสารสนเทศจึงถือเป็นทรัพยากรที่มีคุณค่าของแต่ละองค์กรจึงทำให้เข้ามามีบทบาทในการพัฒนางานภายในองค์กรธุรกิจเพิ่มมากขึ้นเพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการทำงาน ซึ่งโดยส่วนใหญ่จะมุ่งเน้นงานด้านบริหารจัดการด้านคุณภาพของระบบและการพัฒนากระบวนการด้านเทคโนโลยีสารสนเทศ โดยองค์กรมักให้ความสำคัญกับมาตรฐานเพื่อเป็นแนวทางในการเตรียมระบบสารสนเทศ เพื่อสร้างความโปร่งใสในการบริหารในรูปแบบของหลักธรรมาภิบาลที่จะสามารถทำให้องค์กรปฏิบัติตามได้อย่างถูกต้อง เกิดข้อผิดพลาดน้อยที่สุด ป้องกันการทุจริตในกระบวนการต่างๆ ที่อาจเกิดขึ้น เพื่อสนับสนุนเป้าหมายทางธุรกิจและสามารถตรวจสอบการใช้งานเทคโนโลยีสารสนเทศภายในองค์กรได้ เพราะฉะนั้นองค์กรมีความจำเป็นที่จะต้องสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กรทั้งในแง่ของความลับ ความถูกต้อง และความพร้อมใช้งานของสารสนเทศ ตามหลักการของ CIA (Confidentiality , Integrity, Availability) ดังนั้นองค์กรจึงมีความจำเป็นต้องประเมินระบบสารสนเทศ

ตามหลักการดังกล่าว เพื่อกำหนดแนวทางในการบริหารจัดการเพื่อให้องค์กรสามารถดำเนินงานต่อไปได้อย่างต่อเนื่องและมีประสิทธิภาพซึ่งปัจจุบันจะมีการตรวจสอบด้านไอทีโดยผู้ตรวจสอบด้านสารสนเทศในการประเมินความมั่นคงปลอดภัยด้านสารสนเทศซึ่งจะก่อให้เกิดข้อได้เปรียบทางด้านการแข่งขัน สร้างความเชื่อมั่นต่อคู่ค้าทางธุรกิจและหน่วยงานภายนอกที่เกี่ยวข้อง รวมทั้งรักษาภาพลักษณ์และชื่อเสียงที่ดีขององค์กร

จากความสำคัญของระบบสารสนเทศดังที่ได้กล่าวมาข้างต้น บริษัท มิตซุย ประเทศญี่ปุ่นที่ควบคุมดูแลกิจการบริษัทในเครือจึงมีความต้องการให้ระบบสารสนเทศของบริษัทในเครือมีความเป็นมาตรฐานในด้านเทคโนโลยีสารสนเทศ จึงได้มีการว่าจ้างผู้ตรวจสอบทางด้านเทคโนโลยีสารสนเทศ (IT Auditor) ของบริษัท ดีลอยต์ทูชโทมัตสุ (Deloitte Touche Tohmatsu) คือหนึ่งในบริษัทตรวจสอบบัญชีสี่แห่งที่ใหญ่ที่สุดในโลกควบคู่กับไพรซ์วอเทอร์เฮาส์คูเปอส์ เคพีเอ็มจีและเอินส์ท แอนด์ ที่มีการให้บริการทั้งด้านการบัญชีและที่ปรึกษาต่างๆ เช่น การวางแผนยุทธศาสตร์เทคโนโลยีสารสนเทศ การควบคุมประสิทธิภาพ ฯลฯ เพื่อมาตรวจสอบระบบสารสนเทศเพื่อรับรองว่าระบบสารสนเทศของบริษัท มิตซุย บุซซัน ออโตโมทีฟ (ประเทศไทย) จำกัด มีความเป็นมาตรฐานสากลที่ได้รับการยอมรับทั่วโลก ซึ่งเป็นการรับประกันว่าระบบสารสนเทศจะเป็นไปตามเป้าหมายของธุรกิจ ทรัพยากรจะถูกใช้อย่างรับผิดชอบและมีการจัดการความเสี่ยงอย่างเหมาะสม โดยจะมีการตรวจสอบเป็นประจำทุกปี ซึ่งในการตรวจระบบสารสนเทศทุกๆ ปี ทางแผนกสารสนเทศมักจะประสบกับปัญหาเนื่องจากยังไม่มีการบริหารจัดการระบบบริการต่างๆ ที่ดีซึ่งจะเป็นไปในรูปแบบเดิมๆ คือ

2.1 ใช้เวลานานเพื่อจัดเตรียมเอกสารและข้อมูล กล่าวคือ โดยหัวข้อที่ทางผู้ตรวจสอบทางด้านเทคโนโลยีสารสนเทศต้องการมี 8 หัวข้อ 74 รายการ ทางแผนกสารสนเทศจำเป็นต้องรวบรวมจากแหล่งต่างๆ ที่กระจัดกระจายอยู่ตามแฟ้มของแผนกสารสนเทศซึ่งมีอยู่ประมาณ 43 แฟ้ม

2.2 ข้อมูลที่จัดเตรียมให้ผู้ตรวจสอบทางด้านเทคโนโลยีสารสนเทศ โดยส่วนใหญ่จะเป็นหลักฐานในรูปแบบเอกสารทั้งหมดซึ่งมีจำนวนมาก ทำให้ต้องใช้เวลานานเพื่อทำสำเนาส่งให้ผู้ตรวจสอบฯ เนื่องจากทางบริษัทต้องเก็บต้นฉบับไว้เพื่อเป็นหลักฐานไว้เช่นกัน

2.3 ข้อมูลรายละเอียดของการผู้ตรวจสอบทางด้านเทคโนโลยีสารสนเทศย้อนหลังที่ผ่านมาได้ทำการจัดเก็บในรูปแบบเอกสาร โดยการแยกแฟ้มเอกสารตามรอบปีของการตรวจสอบทำให้เวลาที่ต้องการทราบข้อมูลการตรวจสอบทางด้านเทคโนโลยีสารสนเทศย้อนหลังเป็นไปอย่างยุ่งยากและล่าช้าเพราะต้องใช้เวลาในการค้นหา

จากปัญหาดังกล่าวทำให้ผู้วิจัยเล็งเห็นถึงความสำคัญในการพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิตเข้ามาใช้เพื่อบริหารจัดการระบบเทคโนโลยีสารสนเทศของธุรกิจจำหน่ายรถบรรทุก

2. วัตถุประสงค์การวิจัย

การพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิตนั้น ผู้วิจัยได้กำหนดวัตถุประสงค์ในการศึกษา ดังนี้

2.1 ออกแบบและพัฒนาระบบควบคุมภาพงานสารสนเทศสำหรับธุรกิจจำหน่ายรถบรรทุก

2.2 ประเมินต้นแบบในการรับการตรวจสอบระบบสารสนเทศจากผู้ตรวจสอบทางด้านเทคโนโลยีสารสนเทศภายนอก

3. ขอบเขตของการวิจัย

3.1 ขอบเขตด้านพื้นที่

บริษัท มิตซุย บุซซัน ออโตโมทีฟ (ประเทศไทย) จำกัด ได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายอย่างเป็นทางการจาก บริษัท ฮีโน่ มอเตอร์สเซลส์ (ประเทศไทย) จำกัด ในปี พ.ศ. 2524 ปัจจุบัน มีโชว์รูม 3 แห่ง คือ 1. สำนักงานใหญ่บนถนนกิ่งแก้ว จังหวัดสมุทรปราการ 2. ชลบุรี (ใกล้นิคมอมตะนคร) 3. แหลมฉบัง

3.2 ขอบเขตด้านข้อมูล

โดยครอบคลุมข้อมูลงานของระบบเทคโนโลยีสารสนเทศสารสนเทศทั้ง 8 ด้านของบริษัท มิตซุย บุซซัน ออโตโมทีฟดังนี้

3.2.1 ระบบปฏิบัติการ (Operation System) ระบบฐานข้อมูลในเรื่องของการ Setup ค่าต่างๆ

3.2.2 ระเบียบปฏิบัติ และนโยบายต่างๆ ด้านสารสนเทศ โครงสร้างแผนกสารสนเทศและการควบคุมทั่วไปด้านสารสนเทศ

3.2.3 การปฏิบัติงานด้านต่างๆ ของแผนกสารสนเทศ

3.2.4 ความมั่นคงปลอดภัยทางกายภาพของระบบสารสนเทศ

3.2.5 ความมั่นคงปลอดภัยด้านสารสนเทศ

3.2.6 การควบคุมในด้านการเปลี่ยนแปลงระบบสารสนเทศ (System Change Control)

3.2.7 การควบคุมระบบการทำงานของโปรแกรมประยุกต์

3.2.8 การทดสอบรายความถูกต้องของรายการการบันทึกข้อมูลทางบัญชี

3.3 ขอบเขตของระบบ

โปรแกรมประยุกต์ที่ใช้ในการประเมินคุณภาพทางด้านสารสนเทศนั้นมีขอบเขตการใช้งานเพื่อการประเมินความพร้อมจากการตรวจสอบคุณภาพ ด้านสารสนเทศจาก IT Auditor เท่านั้น ฟังชั้นหลักๆ ของระบบดังนี้

3.3.1 ระบบความปลอดภัยในการใช้โปรแกรม และสิทธิการใช้งานและการเข้าถึงข้อมูล

3.3.2 ระบบการบันทึกข้อมูลลงในฐานข้อมูล

3.3.3 รายงานและการแสดงผลด้วยกราฟจากการวิเคราะห์ข้อมูลในระบบฐานข้อมูล

3.3.4 ฟังชั่นการนำข้อมูลออกมาในรูปแบบ File Excel

4. เครื่องมือที่ใช้ในการวิจัย

4.1 รายการการตรวจคุณภาพด้านสารสนเทศจากผู้ตรวจระบบสารสนเทศ (IT Auditor)

4.2 โปรแกรมประยุกต์ระบบฐานข้อมูลเพื่อใช้เตรียมความพร้อมและประเมินระบบสารสนเทศรองรับการตรวจระบบจากผู้ตรวจสอบทางด้านเทคโนโลยีสารสนเทศ

4.3 เอกสารหลักฐานที่ใช้ในการควบคุมระบบสารสนเทศของบริษัทและข้อมูลต่างๆ ของแผนกสารสนเทศ

5. นิยามศัพท์เฉพาะ

5.1 ธรรมาภิบาลไอที (IT Governance) หมายถึง กรอบแนวคิดในการบริหารจัดการงานทางด้านไอที โดยมุ่งหวังให้การทำงานทางด้านไอทีไม่ว่าจะเป็นงานทางด้านโครงการหรืองานบริการ มีการบริหารจัดการที่ดี มีการใช้ทรัพยากรไอทีต่างๆ ให้เกิดประโยชน์สูงสุด ส่งมอบงานให้กับผู้ใช้ได้ตามกำหนด โดยเป้าหมายในการบริหารงานทางด้านไอทีจะต้องมีความสอดคล้องกับเป้าหมายขององค์กรโดยมีกรอบมาตรฐานหลักๆ ดังนี้

5.1.1 มาตรฐาน COBIT ถูกพัฒนาขึ้นโดย ISACA และ IT Governance Institute เพื่อองค์กรที่ต้องการมุ่งสู่การเป็น “ไอทีภิบาล” หรือ “IT Governance”มาตรฐาน COBIT เป็นแนวคิดและแนวทางปฏิบัติของผู้บริหารระบบสารสนเทศ และขณะเดียวกันก็เป็นแนวทางปฏิบัติสำหรับผู้ตรวจสอบระบบสารสนเทศด้วย โครงสร้างของมาตรฐาน COBIT นั้นแบ่งออกเป็น 4 กระบวนการหลัก ประกอบด้วย High-level Control Objective ทั้งหมด 34 หัวข้อ และ Detail Control Objective แบ่งย่อยอีกทั้งหมด 318 หัวข้อย่อย

5.1.2 กรอบงาน ITIL (IT Infrastructure Library)/BS15000 มีต้นเกิดมาจากประเทศอังกฤษ ซึ่งทางรัฐบาลประเทศอังกฤษ โดย OGC (Office of Government Commerce) พัฒนาร่วมกับ BSI (British Standard Institute) มีวัตถุประสงค์ในการสร้าง Best Practice สำหรับกระบวนการบริหารงานบริการด้านสารสนเทศ (IT Service Management)

5.1.3 กรอบการดำเนินงานมาตรฐาน ISO 27001 เน้นเรื่องรายละเอียดเชิงเทคนิคมาตรฐานสำหรับการบริหารความปลอดภัยด้านสารสนเทศ ISMS (Information Security Management System) โดยเป็นรายละเอียดแบบมุ่งเน้นกระบวนการตามหลักการ PDCA (Plan-Do-Check-Act Process focused) สามารถใช้เป็นเกณฑ์เพื่อนำไปใช้งานจริง (Implement) และขอการรับรองได้

5.1.4 แนวคิด COSO คือ กรอบแนวคิดการควบคุมเพื่อช่วยให้ผู้ปฏิบัติงานบรรลุเป้าหมายทั้งเรื่องของการปฏิบัติงานอย่างมีประสิทธิภาพ ประสิทธิผล ความถูกต้องครบถ้วนของรายงาน และการปฏิบัติตามกฎเกณฑ์ที่กำหนด COSO ย่อมาจาก Committee of Sponsoring of the Treadway Commission เป็นคณะทำงานที่ก่อตั้งขึ้น โดยคณะกรรมาธิการของประเทศสหรัฐอเมริกาที่ชื่อว่า Treadway Commission ในปี 1985 โดยจัดตั้งขึ้นเพื่อศึกษาและพัฒนาแนวทางการบริหารความเสี่ยง รูปแบบการควบคุมภายในที่มีประสิทธิผล และป้องกันการทุจริตของรายงานทางการเงิน

5.2 ผู้ตรวจสอบด้านระบบเทคโนโลยีสารสนเทศ (IT Auditor) หมายถึงผู้ที่มีหน้าที่ในการตรวจระบบสารสนเทศและองค์ประกอบต่างๆ ที่เกี่ยวข้องกับระบบงานสารสนเทศรวมถึงเจ้าหน้าที่เครื่องคอมพิวเตอร์ (Hardware และ Software) และ เอกสารต่างๆ ที่เกี่ยวข้องกับจุดประสงค์ เพื่อให้แน่ใจว่าระบบสารสนเทศที่ใช้งานอยู่นั้นมีการทำงานที่ถูกต้องเป็นไปตามแนวทางและ มาตรฐานที่เหมาะสม รวมถึงการทำงานอย่างมีประสิทธิภาพ โดยหน่วยงานสารสนเทศขององค์กรมีหน้าที่ให้การสนับสนุนและประสานงานในการตรวจสอบ

5.3 โปรแกรมประยุกต์ระบบฐานข้อมูลใช้เพื่อเตรียมความพร้อมและประเมินระบบสารสนเทศรองรับการตรวจระบบจากผู้ตรวจสอบทางด้านเทคโนโลยีสารสนเทศ หมายถึงโปรแกรมที่พัฒนาขึ้นโดยใช้ Microsoft Access ซึ่งเป็นโปรแกรมระบบฐานข้อมูลใช้ในการ

รวบรวมจัดกลุ่มเอกสารที่ใช้สนับสนุนการตรวจสอบรวมทั้งการประเมินผลความมีมาตรฐานของระบบสารสนเทศของบริษัท มิตซุย บุซซัน ออโตโมทีฟ (ประเทศไทย) จำกัด

6. ประโยชน์ที่คาดว่าจะได้รับ

6.1 สร้างต้นแบบการพัฒนามาตรฐานระบบธรรมาภิบาลด้านสารสนเทศขององค์กร

6.2 พัฒนาโปรแกรมประยุกต์ระบบฐานข้อมูลเพื่อใช้เตรียมความพร้อมและประเมินระบบสารสนเทศรองรับการตรวจระบบจากผู้ตรวจสอบ

6.3 ลดปัญหาด้านการจัดเก็บเอกสารและการแยกหมวดหมู่แต่ละประเภทในการตรวจสอบให้ชัดเจน

6.4 สามารถตรวจสอบประวัติการตรวจสอบระบบสารสนเทศได้อย่างรวดเร็วมีประสิทธิภาพมากขึ้น

บทที่ 2
การทบทวนวรรณกรรมที่เกี่ยวข้อง

การพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิต โดยผู้วิจัยได้ศึกษาค้นคว้าเอกสารและงานทฤษฎีที่เกี่ยวข้องเพื่อมาใช้เป็นแนวทางในการพัฒนาประกอบโดยประกอบด้วยหัวข้อดังต่อไปนี้

1. แนวคิดธรรมาภิบาลด้านไอที (IT Governance)
2. กรอบมาตรฐานโคบิต (Cobit)
3. กรอบการดำเนินงานมาตรฐาน ISO/IEC 27001
4. กรอบงานไอทิล (ITIL Framework)
5. แนวคิดโคโซ (COSO)
6. ไมโครซอฟท์แอคเซส (Microsoft Access)
7. วงจรการบริหารงานคุณภาพ (PDCA)
8. งานวิจัยที่เกี่ยวข้อง

1. แนวคิดธรรมาภิบาลด้านไอที (IT Governance)

1.1 ความหมายของธรรมาภิบาลด้านไอที

Brisebois Boyd and Shadid (2011) ได้ให้ความหมายของธรรมาภิบาลด้านไอทีว่า ระบบการดำเนินการขององค์กรที่พิจารณาการบริหารจัดการองค์กรที่เกี่ยวข้องกับความถูกต้องของการบริหารงานประสิทธิผลทางเศรษฐศาสตร์ และประสิทธิผลทางกลยุทธ์ รวมถึงบทบาทของผู้เกี่ยวข้องที่มุ่งเน้นการดำเนินงานและความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ

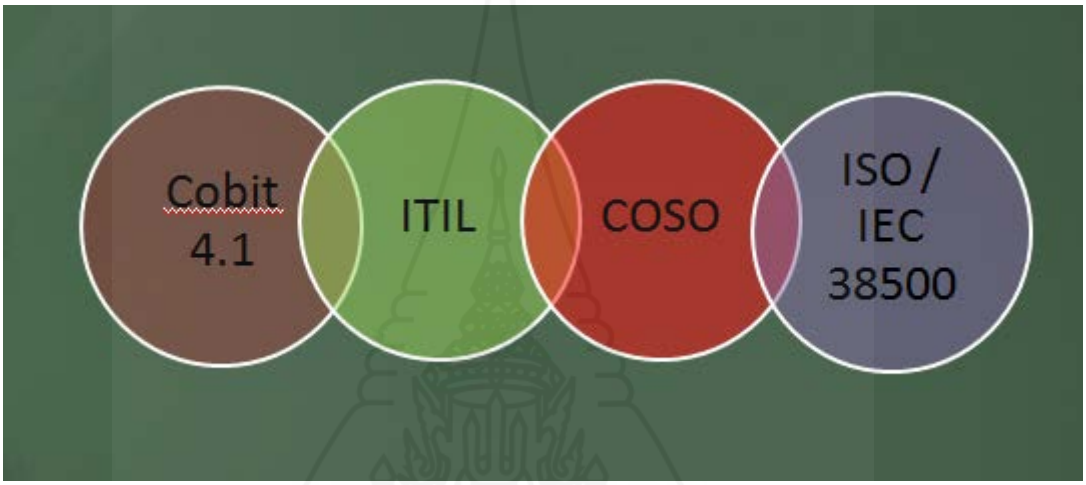
กัลยา ใจรักษ์ และประสงค์ ประณีต พลกรัง (2555: 4) ได้สรุปความหมายธรรมาภิบาลว่าด้านไอทีว่ากลไกเพื่อให้บรรลุถึงการใช้ไอทีที่เต็มความสามารถเพื่อช่วยสนับสนุนองค์กรและช่วยขยายกลยุทธ์และวัตถุประสงค์ขององค์กร

สันติพัฒน์ อรุณธารี (2555: 1-64) ได้ให้ความหมายไว้ว่า คือ การนำไอทีเพื่อนำมาใช้ในองค์การธุรกิจโดยมุ่งหวังให้เกิดการใช้ทรัพยากรไอทีอย่างคุ้มค่ากับการลงทุน ตอบสนองความ

ต้องการของธุรกิจได้อย่างถูกต้องเหมาะสมและสร้างคุณค่าให้กับธุรกิจ เช่น กระบวนการทำงานมีความโปร่งใสตรวจสอบได้ ฯลฯ

จากความหมายดังกล่าวสรุปได้ว่า คือ กระบวนการบริหารจัดการทางด้านไอทีต่างๆ ให้เกิดประโยชน์สูงสุดต่อองค์กร โปร่งใส สามารถตรวจสอบ ติดตามการทำงานได้ และต้องมีความสอดคล้องกับธรรมาภิบาลขององค์กร

1.2 กรอบแนวคิดของธรรมาภิบาลด้านไอที (IT Governance Frameworks)



ภาพที่ 2.1 กรอบแนวคิดของธรรมาภิบาลด้านไอที

จากภาพที่ 2.1 จะเห็นได้ว่ากรอบแนวคิดของธรรมาภิบาลด้านไอทีนั้นมีหลายแบบ ซึ่งมีรายละเอียดเบื้องต้นดังต่อไปนี้

1.2.1 COBIT (Control Objectives for information and Relate Technology) โดยกรอบโคบิต 5 (COBIT5) เป็นกรอบที่เน้นรายละเอียดเกี่ยวกับกระบวนการควบคุมการบริหารงานทางด้านไอที มีการกำหนดทรัพยากรทางด้านไอทีที่ มีการตั้งเป้าหมายของกระบวนการทางด้านไอทีให้สอดคล้องกับเป้าหมายของธุรกิจที่ได้วางไว้

1.2.2 ITIL (Information Technology Infrastructure Library) เน้นการบริหารจัดการทางด้านการบริการและการส่งมอบโดยใน Version 3 ที่พัฒนามาล่าสุดมีการออกแบบให้ใกล้เคียงกับมาตรฐาน ISO/IEC 20000 เน้นเรื่องการ Alignment ระหว่าง “IT” กับ “Business” ต้องไปในทิศทางเดียวกันและให้ความสำคัญในเรื่องการสร้าง “Business Value” มากกว่า “Process Execution”

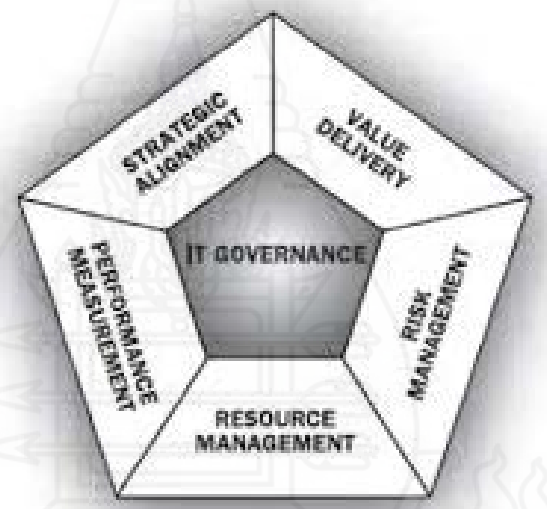
1.2.3 COSO (Committee of Sponsoring Organizations) เป็นกระบวนการปฏิบัติงานที่ถูกกำหนดร่วมกันโดยคณะกรรมการ ผู้บริหาร ในองค์กรซึ่งเป็นการออกแบบในระดับที่สมเหตุสมผล

และเพื่อให้บรรลุวัตถุประสงค์ของการควบคุม จะต้องประกอบไปด้วย 1. ด้านการดำเนินงาน (Operation) 2. ด้านรายงานการเงิน (Financial Reporting) 3. ด้านการปฏิบัติให้เป็นไปตามกฎระเบียบและนโยบาย (Compliance with application laws and regulations)

1.2.4 ISO / IEC 38500 (2008) เป็นมาตรฐานการกำกับดูแลเพื่อเป็นกรอบแนวคิดในการประเมินทิศทางและการตรวจสอบการใช้เทคโนโลยีสารสนเทศของแต่ละองค์กร

1.3 องค์ประกอบของกรอบแนวคิดธรรมาภิบาลด้านไอที (IT Governance Necessary Components)

กำพล ศรธนะรัตน์ (2553) องค์ประกอบของธรรมาภิบาลด้านไอทีประกอบด้วย 5 กิจกรรมดังภาพที่ 2



ภาพที่ 2.2 องค์ประกอบของกรอบแนวคิดธรรมาภิบาลด้านไอที
ที่มา: กำพล สนธนรัชต์ (2553)

1.3.1 การกำหนดกลยุทธ์ (Strategic Alignment) การนำแผนกลยุทธ์ขององค์กรมากำหนดแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ โดยผู้บริหารสูงสุดขององค์กรและผู้บริหารสูงสุดด้านเทคโนโลยีสารสนเทศต้องทำงานร่วมกันเพื่อสร้างความมั่นใจในการลงทุนในเรื่องทรัพยากรเทคโนโลยีสารสนเทศที่สามารถสร้างประโยชน์สูงสุดให้กับองค์กร

1.3.2 การบริหารจัดการทรัพยากร (Resource Management) การลงทุนและจัดสรรทรัพยากรเทคโนโลยีสารสนเทศให้กับองค์กรตามความต้องการและความเหมาะสม

1.3.3 การสร้างระบบเทคโนโลยีสารสนเทศให้กิจกรรม (Value delivery) การลงทุนพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อสร้างผลประโยชน์ให้องค์กร ทั้งการพัฒนาระบบเทคโนโลยีสารสนเทศขึ้นเองในองค์กรและการใช้บริการภายนอกองค์กร

1.3.4 การวัดผลการดำเนินการ (Performance measurement) การวัดผลสำเร็จและการบรรลุวัตถุประสงค์โครงการพัฒนาระบบเทคโนโลยีสารสนเทศที่ได้สร้างขึ้นแบ่งได้เป็น 2 ส่วน คือ

1) วัดการพัฒนาโครงการด้านเทคโนโลยีสารสนเทศ (Development metrics)

2) วัดการให้บริการ (Services metrics)

1.3.5 การบริหารความเสี่ยง (Risk management) การประมาณความเสี่ยงที่จะเกิดขึ้นและแนวทางลดความเสียหายที่อาจจะเกิดขึ้น

1.4 ความสำคัญของธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศทำให้องค์กรมีการบริหารงานที่เป็นระบบระเบียบมีขั้นตอนที่แน่นอนลดความซ้ำซ้อนและลดความเสี่ยงทำให้องค์กรสามารใช้สารสนเทศได้อย่างเต็มประสิทธิภาพส่งผลให้เกิดประโยชน์สูงสุดแก่องค์กรช่วยป้องกันการทุจริตของผู้บริหารหรือผู้ปฏิบัติงานได้เนื่องจากมีการบริหารงานที่โปร่งใส สามารถตรวจสอบได้ส่งเสริมภาพลักษณ์ที่ดีต่อองค์กรทำให้ผู้ที่มีส่วนเกี่ยวข้องกับองค์กรเกิดความเชื่อมั่นและความไว้วางใจในองค์กรมากยิ่งขึ้น

1.4.1 ผู้บริหารระดับสูงและคณะกรรมการผู้จัดการ (Executive and Broad of Director) ต้องการทราบว่าสามารถกำหนดเป้าหมายทางธุรกิจอย่างไรให้สามารถบรรลุเป้าหมายดังกล่าวได้โดยก่อให้เกิดประโยชน์สูงสุดแก่องค์กรและจะนำแนวทางปฏิบัติของธรรมาภิบาลด้านเทคโนโลยีสารสนเทศมาปรับใช้กับองค์กรให้เหมาะสมได้อย่างไรเพื่อให้สามารถแน่ใจได้ว่าความเสี่ยงต่างๆ ที่เกี่ยวข้องกับสารสนเทศที่มีความสำคัญต่อองค์กรจะได้รับการจัดการอย่างเหมาะสม

1.4.2 ผู้บริหารด้านธุรกิจ (Business Manager) ต้องการทราบว่าฝ่ายบริหารสามารถกำหนดความต้องการทางด้านธุรกิจที่เกี่ยวข้องกับธรรมาภิบาลด้านเทคโนโลยีสารสนเทศได้อย่างไรเพื่อให้มั่นใจได้ว่าโอกาสที่จะเกิดความเสี่ยงต่างๆ ที่เกี่ยวข้องจะลดน้อยลง

1.4.3 ผู้บริหารด้านเทคโนโลยีสารสนเทศ (IT Manager) ต้องการทราบว่าต้องทำอย่างไรเพื่อให้การให้บริการทางด้านเทคโนโลยีสารสนเทศสามารถตอบสนองได้ตรงตามความต้องการของธุรกิจอยู่ตลอดเวลา

1.4.4 ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Auditor) ต้องการทราบว่าต้องทำอย่างไรในการที่จะนำเนื้อหาต่างๆ ของโคบิตมาปรับใช้ในกระบวนการตรวจสอบด้านเทคโนโลยี

สารสนเทศ เพื่อให้มั่นใจได้ว่ากระบวนการตรวจสอบจะมีประสิทธิภาพและมีความเป็นอิสระจากฝ่ายงานอื่นความเสี่ยง

1.4.5 พนักงานทั่วไป (compliance officer) ต้องการทราบว่าผู้จัดการด้านความเสี่ยง (risk manager) และ พนักงานทั่วไป จะสามารถนำโคบิตมาใช้ในเรื่องที่เกี่ยวกับกิจกรรมด้านความเสี่ยงและการปฏิบัติตามกฎระเบียบข้อบังคับได้อย่างไรเพื่อให้สามารถแน่ใจได้ว่าความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศใหม่ๆ จะถูกค้นพบได้อย่างรวดเร็ว และ พนักงานที่จำเป็นต้องปฏิบัติตามกฎ (IT complies) มีการปฏิบัติตามนโยบาย ระเบียบข้อบังคับ และกฎหมายหรือไม่

2. กรอบมาตรฐานโคบิต (Cobit Framework)

2.1 ประวัติความเป็นมา

โคบิตได้รับการพัฒนาขึ้นในปี 1992 โดยสมาคมการควบคุมและการตรวจสอบระบบสารสนเทศหรือ The Information Systems Audit and Control Association (ISACA) และสถาบันเทคโนโลยีสารสนเทศาภิบาล หรือInformation Technology Governance Institute (ITGI) เป็นผู้ดูแลในปัจจุบัน (ซึ่ง ISACA และ ITGI เป็นองค์กรชั้นนำในด้านของการตรวจสอบและการควบคุมด้านเทคโนโลยีสารสนเทศระดับโลกที่ตั้งอยู่ในประเทศสหรัฐอเมริกา) โคบิตเวอร์ชันแรก (CoBIT1st Edition) ได้รับการตีพิมพ์และเผยแพร่ในปี 1996 จากนั้นได้มีการปรับปรุงเป็นเวอร์ชันที่ 2 (CoBIT 2rd Edition) ในปี 1998 โดยในเวอร์ชันที่ 2 มีการเพิ่มเติมแหล่งข้อมูลและมีการทบทวนเนื้อหาในส่วนของวัตถุประสงค์การควบคุมหลักและเนื้อหาอื่นๆ บางส่วน ต่อมาได้มีการพัฒนาเป็นเวอร์ชันที่ 3 (CoBIT 3 Edition) ในปี 2000 (ส่วนที่เป็น on-line edition ได้รับการเผยแพร่ในปี 2003) และเวอร์ชันที่ 4 (CoBIT 4.0) ซึ่งเป็นเวอร์ชันล่าสุดโดยได้มีการเผยแพร่ในเดือนธันวาคมปี 2005 โดยเป็นการปรับปรุงเนื้อหาให้มีความใกล้เคียงกับมาตรฐานสากลต่างๆ เช่น Sarbanes-Oxley Act. เป็นต้น

สถาบันเทคโนโลยีสารสนเทศภิบาล (ITGI) จัดตั้งขึ้นเมื่อ ปี ค.ศ. 1998 โดยสมาคมการควบคุมและตรวจสอบระบบสารสนเทศ (ISACA) และสมาคมอื่นๆ ที่เกี่ยวข้อง โดยมีวัตถุประสงค์เพื่อเสริมสร้างความเข้าใจและนำหลักการด้านการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศมาใช้งานโดยมีการเพิ่มเติมแนวทางในการบริหารหรือแนวทางสำหรับผู้บริหาร (Management Guideline) เข้ามาในโคบิตเวอร์ชันที่ 3 รวมถึงการเสริมสร้างและยกระดับการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (ชุติกาญจน์ เพชรรักษ์. 2556)

2.2 ความสำคัญของกรอบมาตรฐานโคบิต

โคบิตเป็นทั้งแนวคิดและแนวทางการปฏิบัติ (Framework) เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่างๆ ที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดี (Best Practice) ซึ่งสามารถนำไปปรับใช้ได้ในทุกองค์กรสำหรับกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยโครงสร้างของมาตรฐาน COBIT ได้ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ Business Process

โคบิตจึงเป็นบทสรุปรวมของความรู้หรือข้อมูลต่างๆ ที่องค์กรต้องการสำหรับการนำไปปรับใช้เพื่อให้องค์กรมีการควบคุมภายในด้านเทคโนโลยีสารสนเทศที่ดีและเพื่อพัฒนาองค์กรให้เข้าสู่การเป็นองค์กรที่มี “ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ” หรือ IT Governance กล่าวคือ สามารถบริหารจัดการระบบสารสนเทศขององค์กรให้สามารถใช้งานได้อย่างมีประสิทธิภาพ มีความคุ้มค่ากับการลงทุน และมีการบริหารจัดการที่โปร่งใสสามารถตรวจสอบได้ โดยโคบิตจะรวบรวมตัววัด (Measures) เครื่องบ่งชี้ (Indicators) ขั้นตอนการปฏิบัติงาน (Processes) และแนวทางการปฏิบัติที่ดีที่สุด (Best Practices) ซึ่งเป็นข้อมูลที่มีโครงสร้างสามารถเข้าใจและนำไปใช้ได้ง่ายอีกทั้งเป็นที่ยอมรับกันโดยทั่วไป ผู้ที่นำโคบิตไปใช้ได้แก่ ผู้บริหารธุรกิจ ผู้บริหารระบบสารสนเทศ และผู้ตรวจสอบ สามารถนำสิ่งต่างๆ ไปใช้เป็นเครื่องมือเพื่อสร้างประโยชน์สูงสุดจากการนำเทคโนโลยีสารสนเทศเข้ามาใช้งานภายในองค์กรและช่วยให้การลงทุนทางด้านเทคโนโลยีสารสนเทศประสบความสำเร็จอย่างตรงตามความต้องการทางด้านธุรกิจ เนื่องจากการนำโคบิตเข้ามาใช้จะช่วยให้ผู้ที่ปฏิบัติงานต่างๆ มีความเข้าใจในระบบเทคโนโลยีสารสนเทศที่ตนเองเกี่ยวข้องมากยิ่งขึ้น แล้วยังช่วยในเรื่องของการยกระดับของการควบคุมด้านความปลอดภัยที่จำเป็นสำหรับการป้องกันสินทรัพย์ต่างๆ ขององค์กร

2.3 กระบวนการของกรอบมาตรฐานโคบิต

สามารถแบ่งเป็น 4 กระบวนการหลัก (Domain) ได้แก่

2.3.1 การวางแผนและการจัดการองค์กร (PO: Planning and Organization) ครอบคลุมในเรื่องของกลยุทธ์และวิธีการที่นำมาใช้ในองค์กร โดยจะเน้นเรื่องของการกำหนดวิธีที่ทำให้เทคโนโลยีสารสนเทศมีบทบาทสำคัญ เพื่อให้สารสนเทศนั้นสามารถตอบสนองความต้องการทางด้านธุรกิจขององค์กรได้

2.3.2 การจัดหาและติดตั้ง (AI: Acquisition and Implementation) การทำให้กลยุทธ์ที่ได้กำหนดไว้ประสบผลสำเร็จ ซึ่งการดำเนินงานตามกลยุทธ์ที่ได้วางไว้นั้นจะต้องมีการระบุพัฒนาหรือจัดซื้อจัดหา นำไปติดตั้งใช้งาน รวมถึงการผนวกรวมเทคโนโลยีสารสนเทศเข้าเป็นส่วนหนึ่งของกระบวนการทางธุรกิจ และการเปลี่ยนแปลงและการดูแลรักษาระบบงานที่องค์กรมีอยู่

2.3.3 การส่งมอบและบำรุงรักษา (DS: Delivery and Support) รวมตั้งแต่การส่งมอบบริการการดำเนินงานด้านการรักษาความปลอดภัยและความต่อเนื่องของการให้บริการการบริหารจัดการสารสนเทศและอุปกรณ์อำนวยความสะดวกต่างๆ ที่ใช้ในการปฏิบัติงาน

2.3.4 การติดตามผล (M: Monitoring) กระบวนการด้านเทคโนโลยีสารสนเทศทั้งหมดจะต้องได้รับการประเมินอยู่เสมอเพื่อรับประกันได้ถึงคุณภาพและการปฏิบัติตามข้อบังคับของการควบคุมในโดเมนนี้จะเป็นการระบุถึงการบริหารจัดการในด้านของประสิทธิภาพของระบบสารสนเทศ ซึ่งจะต้องได้รับการประเมินจากผู้ตรวจสอบทั้งภายในและภายนอกองค์กร (Gunthima Chamnoiphrom. 2556)

ในแต่ละกระบวนการหลักข้างต้น โคบิตยังได้แสดงถึงวัตถุประสงค์การควบคุมหลัก (High-Level Control Objectives) รวมทั้งหมด 34 หัวข้อ และในแต่ละหัวข้อจะประกอบไปด้วยวัตถุประสงค์การควบคุมย่อย (Detailed Control Objectives) รวมทั้งหมดถึง 318 หัวข้อย่อย พร้อมทั้งยังมีแนวทางการตรวจสอบ (Audit Guideline) สำหรับแต่ละหัวข้อการควบคุมอีกด้วย ในแต่ละหัวข้อของวัตถุประสงค์การควบคุม มาตรฐาน COBIT แสดงถึงความสัมพันธ์ต่อปัจจัย 2 ประการ ได้แก่

1) คุณภาพของสารสนเทศ (Information Criteria) มี 7 ประการ

(1) ประสิทธิภาพ (Effectiveness) หมายถึง มีการจัดการกับข้อมูลที่ใช้หรือเกี่ยวข้องกับกระบวนการทางธุรกิจ โดยเฉพาะการส่งมอบสารสนเทศต่างๆ ให้แก่ผู้ใช้ได้อย่างถูกต้องทันเวลาและสามารถใช้ประโยชน์ได้

(2) ประสิทธิผล (Efficiency) หมายถึงมีการใช้ประโยชน์จากทรัพยากรอย่างเต็มที่ (คือให้ผลตอบแทนสูงสุดในขณะที่ใช้ต้นทุนที่ต่ำที่สุด) เพื่อให้ได้มาซึ่งสารสนเทศที่ผู้ใช้ต้องการ

(3) การรักษาความลับ (Confidentiality) หมายถึงมีการป้องกันการเปิดเผยข้อมูลที่มีความสำคัญต่อบุคคลหรือหน่วยงานที่ไม่ได้รับอนุญาต

(4) ความสมบูรณ์ของข้อมูล (Integrity) หมายถึงความถูกต้องตรงกันและความครบถ้วนสมบูรณ์ของสารสนเทศที่มีอยู่ในองค์กร

(5) ความพร้อมใช้งานของข้อมูล (Availability) หมายถึงการที่สามารถเรียกใช้ข้อมูลสารสนเทศได้ตลอดเวลาเมื่อผู้ใช้ต้องการรวมถึงการป้องกันและรักษาความปลอดภัยให้กับทรัพยากรที่จำเป็นต่างๆ และการรักษาระดับความสามารถในการทำงานของทรัพยากรเหล่านั้น ให้สามารถทำงานได้อย่างมีประสิทธิภาพอยู่ตลอดเวลา

(6) การปฏิบัติตามระเบียบ (Compliance) หมายถึงการที่องค์กรปฏิบัติตามกฎ ระเบียบ ข้อบังคับ หลักเกณฑ์ ข้อตกลง หรือกฎหมายที่เกี่ยวข้องกับกระบวนการทางธุรกิจที่มีขึ้นเพื่อบังคับใช้ทั้งจากหน่วยงานภายในและภายนอกองค์กร

(7) ความน่าเชื่อถือของข้อมูล (Reliability) หมายถึงความสามรถในการหาข้อมูลที่เหมาะสมและเชื่อถือได้ให้แก่ผู้บริหารเพื่อใช้ในการดำเนินธุรกิจและให้สามารถจัดทำรายงานทางการเงินหรือรายงานอื่นๆที่จำเป็น

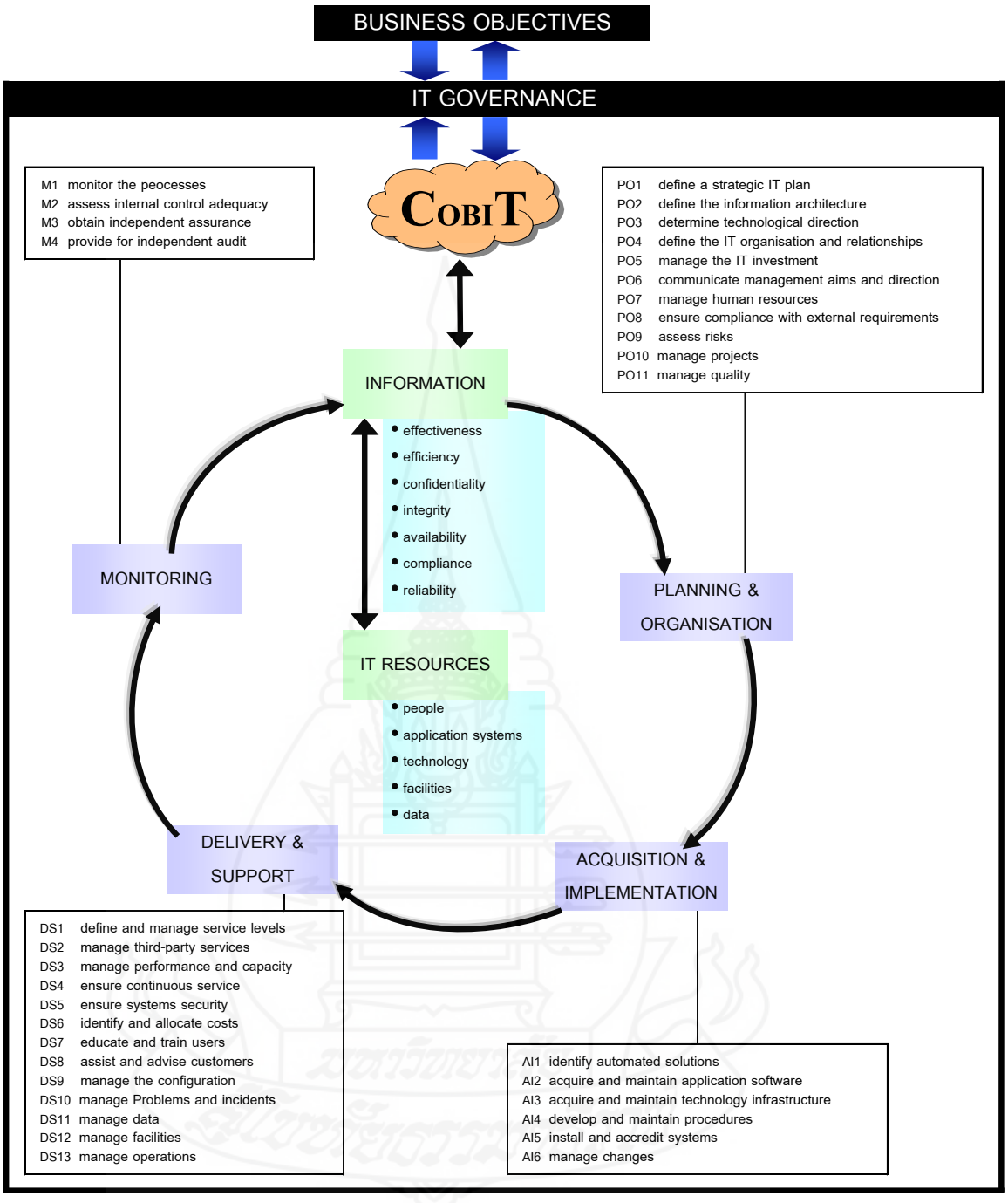
2) ทรัพยากรด้านเทคโนโลยีสารสนเทศ (IT Resources) มี 4 ประเภท

(1) ระบบงานประยุกต์ (Application Systems) ขั้นตอนและกระบวนการที่ใช้ในการปฏิบัติงานทั้งแบบที่ปฏิบัติเองด้วยมือและแบบที่ทำด้วยโปรแกรมคอมพิวเตอร์

(2) สารสนเทศ (Information) ข้อมูลหรือสารสนเทศในรูปแบบต่างๆ ทั้งที่เป็นรูปภาพ ข้อมูลเสียง เป็นต้น โดยสามารถเป็นได้ทั้งข้อมูลที่มีโครงสร้างและที่ไม่มีโครงสร้าง ที่องค์กรนำมาใช้ในการปฏิบัติงาน

(3) โครงสร้างพื้นฐาน (Infrastructure) โครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศขององค์กรที่ใช้ในการปฏิบัติงานต่างๆ ภายในองค์กร ซึ่งรวมตั้ง hardware software ระบบปฏิบัติการ ระบบบริหารฐานข้อมูล ระบบเครือข่าย และยังรวมไปถึงทรัพยากรต่างๆ ที่ใช้ในสนับสนุนการปฏิบัติงานขององค์กร เช่น อาคาร สถานที่ และสาธารณูปโภคต่างๆ

(4) บุคลากร (People) บุคลากรที่มีความรู้ความชำนาญในการบริหารและการปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถมั่นใจได้ว่าระบบสารสนเทศจะได้รับการดูแลที่ดีจากบุคลากรที่มีความสามารถ

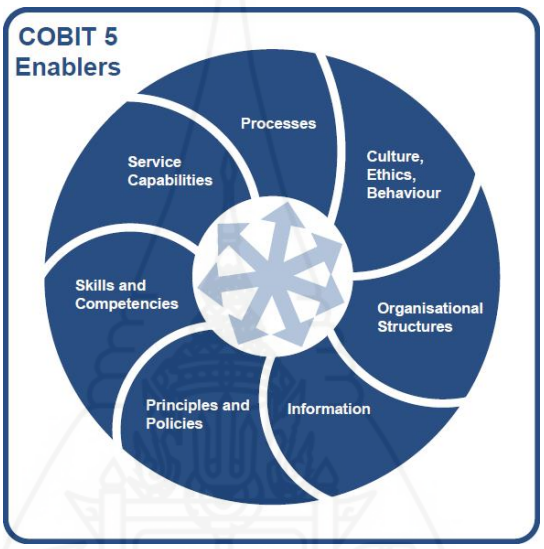


ภาพที่ 2.3 กรอบมาตรฐานโคบิต

ที่มา: www.isaca.org

2.4 โคบิต 5.0

หลักการของ COBIT เป็นหลักการที่ต้องการให้เกิดการบรรลุเป้าหมายระดับองค์กร (Enterprise Goals) ที่กำหนดไว้ โดยอาศัยปัจจัยก่อเกิด (Enablers) 7 ปัจจัยดังภาพที่ 2.4 ที่เป็นสิ่งที่ทำให้เป้าหมายที่กำหนดไว้สามารถบรรลุได้ โดยปัจจัยก่อเกิดเหล่านี้ต้องทำงานผสานกันหรือร่วมกัน ซึ่งในรูปแสดงเป็นสัญลักษณ์ลูกศรที่อยู่ตรงกลางและชี้โยงไปมาในทิศทางและมิติต่างๆ จึงจะทำให้เกิดความสำเร็จได้



ภาพที่ 2.4 COBIT 5 Enablers

ที่มา: http://www.tnetsecurity.com/content_audit/cobit5_implementation_step.php

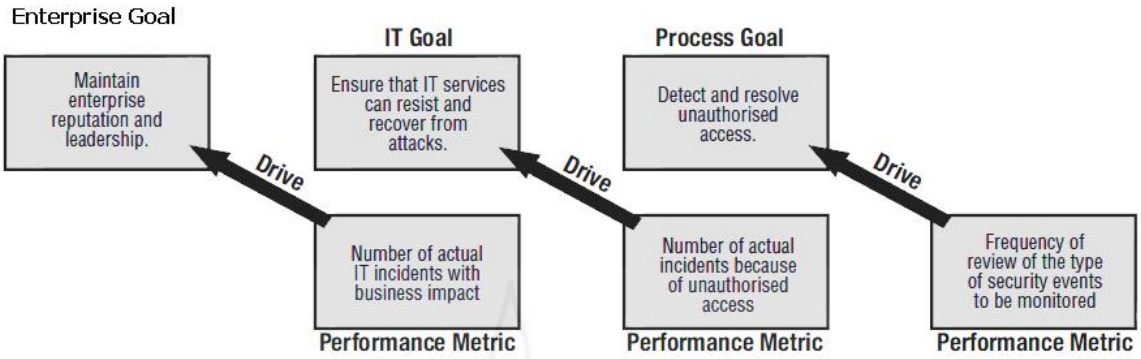
ปัจจัยก่อเกิดประกอบด้วย

2.4.1 กระบวนการ (Processes) องค์กรต้องมีกระบวนการเพื่อให้งานได้ผลลัพธ์หรือบรรลุเป้าหมายของกระบวนการ ซึ่งจะนำไปสู่การบรรลุซึ่งเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและเป้าหมายระดับองค์กรได้

หลักการ Goal Cascade ของ COBIT 5 ดังภาพที่ 2.5 ได้กำหนดไว้ว่า

1) การบรรลุเป้าหมายระดับองค์กร (Enterprise Goals) ต้องได้รับการสนับสนุนจากการบรรลุเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related Goals)

2) การบรรลุเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ต้องได้รับการสนับสนุนจากการบรรลุเป้าหมายของกระบวนการ (Process Goals)



ภาพที่ 2.5 หลักการ Goal Cascade ของ COBIT 5

ที่มา: http://www.tnetsecurity.com/content_audit/cobit5_implementation_step.php

ซึ่งทำให้เห็นภาพว่าเป้าหมายในระดับสูงกว่า จะถูกขับเคลื่อนด้วยเป้าหมายในระดับต่ำกว่า เป็นทอดๆ ต่อๆ กันไปตามลำดับ ในรูป Performance Metric หมายถึงตัวชี้วัดสำหรับเป้าหมายซึ่งจะมีตัวชี้วัดในแต่ละระดับตั้งแต่ระดับกระบวนการ ระดับเทคโนโลยีสารสนเทศ และระดับองค์กร COBIT 5 ก็ยังคงใช้หลักการ Goal Cascade ในข้างต้นด้วยเช่นกัน แต่ขยายเป้าหมายเพิ่มเติมให้ครอบคลุมทั้ง 7 ปัจจัย ไม่เฉพาะแต่ปัจจัยด้านกระบวนการเท่านั้น องค์กรต้องบรรลุเป้าหมายเพิ่มเติมเหล่านั้นด้วยให้ได้ จึงจะสามารถบรรลุเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และเป้าหมายระดับองค์กรได้

2.4.2 วัฒนธรรม จริยธรรม และความประพฤติ (Culture, ethics, behavior) หากวัฒนธรรม จริยธรรม และความประพฤติของบุคลากรขององค์กร ไม่ได้รับการปลูกฝัง อบรม บ่มเพาะ หรือบ่มนิสัย ในทิศทางที่เหมาะสมที่องค์กรต้องการแล้ว อาจส่งผลต่อการบรรลุเป้าหมายระดับองค์กรได้ เช่น หากองค์กรขาดการปลูกฝังเรื่องการมีวินัยที่ดีหรือการรู้จักหน้าที่ความรับผิดชอบของตนเองแล้ว ก็ยากที่จะทำให้การ ปฏิบัติตามกระบวนการที่สร้างขึ้นมาสำเร็จได้ ซึ่งอาจเป็นเพราะคนขาดวินัย ก็เลยปฏิบัติตามบ้าง ไม่ปฏิบัติตามบ้าง เป้าหมายของกระบวนการ เป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และตามด้วยเป้าหมายระดับองค์กร จึงไม่สามารถบรรลุได้

2.4.3 โครงสร้างบุคลากร (Organizational structures) องค์กรต้องกำหนดโครงสร้างด้านบุคลากรขึ้นมาเพื่อให้มีหน้าที่ความรับผิดชอบที่ชัดเจนว่าต้องทำอะไรบ้าง หน้าที่ความรับผิดชอบส่วนหนึ่งคือการปฏิบัติตามบทบาทในกระบวนการที่กำหนดไว้ หากขาดโครงสร้างนี้ การปฏิบัติหน้าที่ของตนเองตามบทบาทในกระบวนการ จะไม่สามารถเกิดขึ้นได้ ซึ่งอาจส่งผลต่อการบรรลุเป้าหมายในระดับองค์กรได้

2.4.4 ข้อมูล (Information) ข้อมูลเป็นหัวใจสำคัญขององค์กร หลายๆ กระบวนการมีข้อมูลเป็น Input หรือ Output เข้าสู่หรือออกจากกระบวนการก็ตาม ข้อมูลถูกนำไปใช้ในหลายๆ เรื่อง เช่น เพื่อเป็นข้อมูลพื้นฐาน เพื่อใช้ในการตัดสินใจ เพื่อการวางแผน เพื่อการพยากรณ์ หรืออื่นๆ ดังนั้นหากปราศจากข้อมูลที่ต้องการแล้ว อาจทำให้งานหรือกระบวนการขององค์กรไม่สามารถทำได้เลย หรือทำได้อย่างไม่ได้ผลหรือสัมฤทธิ์ผลเท่าที่ควร

2.4.5 หลักการและนโยบายองค์กร (Principles and policies) หลักการและนโยบายองค์กรที่กำหนดไว้โดยทั่วไปจะสะท้อนให้เห็นถึงภาพรวม ทิศทาง กรอบแนวคิด หรือกรอบการปฏิบัติที่องค์กรต้องการให้บรรลุเพื่อบังเกิดความสำเร็จตามที่ต้องการ บุคลากรขององค์กรควรยึดตามหลักการและนโยบายที่กำหนดไว้และปฏิบัติตามอย่างสอดคล้อง เพื่อให้เกิดผลตามที่องค์กรต้องการ ดังนั้นหากปราศจากหลักการและนโยบายกำหนดไว้อย่างชัดเจนแล้ว ภาพรวม ทิศทาง กรอบแนวคิด หรือกรอบการปฏิบัติที่ต้องการอาจไม่บังเกิดผลตามที่ต้องการได้ เช่น หลักการ “ขยัน ซื่อสัตย์ และอดทน” ขององค์กร อาจมีผลต่อการทำงานตามหน้าที่และกระบวนการที่ตนเองต้องรับผิดชอบ ซึ่งสามารถส่งผลต่อการบรรลุเป้าหมายในระดับองค์กรได้

2.4.6 ทักษะ ความรู้ และความสามารถของบุคลากร (Skills and competences) องค์กรต้องอาศัยบุคลากรเป็นกุญแจสำคัญไปสู่ความสำเร็จของงานและกระบวนการ ซึ่งโดยทั่วไปจำเป็นอย่างยิ่งที่จะต้องให้หรือต้องสร้างให้บุคลากรมีทักษะ ความรู้ และความสามารถที่จำเป็นสำหรับงานหรือกระบวนการที่ปฏิบัติ ถ้าไม่เช่นนั้นแล้ว อาจจะเป็นอุปสรรคสำคัญต่องานหรือกระบวนการที่ทำและต่อความสำเร็จของงานที่จะเกิดขึ้น

2.4.7 โครงสร้างพื้นฐานของการให้บริการสารสนเทศ (Service capabilities) โครงสร้างพื้นฐานของการให้บริการสารสนเทศ หมายรวมถึงฮาร์ดแวร์ ซอฟต์แวร์ แอพพลิเคชัน และเทคโนโลยีอื่นๆ ที่ทำหน้าที่เป็นพื้นฐานในการให้บริการด้านระบบงานและข้อมูลแก่ผู้ใช้งานขององค์กร หากปราศจากโครงสร้างพื้นฐานนี้ จะเป็นอุปสรรคต่อการทำงานซึ่งอาจทำให้งาน กระบวนการหรือข้อมูลที่จำเป็นต้องใช้ เกิดความล่าช้าจนธุรกิจไม่สามารถยอมรับได้

สรุปได้ว่าปัจจัยก่อเกิดทั้ง 7 ประการในข้างต้น จะใช้ “กระบวนการเป็นศูนย์กลาง” ซึ่งมีจุดประสงค์ให้เห็นว่าแต่ละปัจจัยก่อเกิดมีความเกี่ยวข้องกับกระบวนการในลักษณะใดลักษณะหนึ่งกล่าวคือ

1) องค์กรต้องมีกระบวนการเพื่อให้งานได้ผลลัพธ์หรือบรรลุเป้าหมายของกระบวนการ

2) องค์กรต้องมีการบ่มเพาะวัฒนธรรม จริยธรรมและความประพฤติของบุคลากรในทิศทางที่เหมาะสมเพื่อให้บุคลากรเห็นความสำคัญของการปฏิบัติตามกระบวนการที่กำหนดไว้

3) องค์กรต้องกำหนดโครงสร้างด้านบุคลากรขึ้นมาเพื่อให้มีหน้าที่ความรับผิดชอบที่ชัดเจนว่าต้องทำอะไรบ้างหน้าที่ความรับผิดชอบส่วนหนึ่งคือการปฏิบัติตามบทบาทในกระบวนการที่กำหนดไว้

4) กระบวนการมีข้อมูลเป็น Input หรือ Output เข้าสู่หรือออกจากกระบวนการก็ตาม

5) หลักการและนโยบายองค์กรส่งผลต่อการทำงานตามหน้าที่และกระบวนการที่ตนเองต้องรับผิดชอบ

6) บุคลากรต้องมีทักษะ ความรู้ และความสามารถที่จำเป็นสำหรับงานหรือกระบวนการที่ตนเองต้องรับผิดชอบ

7) โครงสร้างพื้นฐานของการให้บริการสารสนเทศเป็นส่วนที่ทำให้กระบวนการต่างๆ ขององค์กรดำเนินไปได้อย่างง่ายและรวดเร็วขึ้นเช่นในการปฏิบัติงานตามกระบวนการหนึ่งสามารถใช้ประโยชน์จากระบบงานเพื่อช่วยในการปฏิบัติงานตามกระบวนการนั้น

3. กรอบการดำเนินงานมาตรฐาน ISO/IEC 27001

3.1 มาตรฐาน ISO/IEC27001

ข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยให้กับองค์กรได้รับการพัฒนามาจาก Information Security Management Standard BS7799 ออกโดย British Standardm Institute (BSI) เพื่อให้สามารถบริหารจัดการทางด้านความปลอดภัยได้อย่างมีระบบและเพียงพอเหมาะสมต่อการดำเนินธุรกิจ (ทวีศักดิ์ กออนันตกูล, ชฎามาศ ธุระเศรษฐ, พันธศักดิ์ ศิริรัชตพงษ์,กุสุรางคณา วายุภาพ และ ศิวรักษ์ ศิวโฆกษธรรม : 2550)

ซึ่งสามารถแบ่งเนื้อหาของข้อกำหนดออกเป็น 2 ส่วนประกอบด้วย 1. ส่วนของการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ 2. ส่วนของรายการควบคุมและวัตถุประสงค์ของการควบคุมแนวทางการบริหารความมั่นคงปลอดภัยสารสนเทศในการบริหารจัดการระบบบริหารความมั่นคงปลอดภัยสารสนเทศจะขับเคลื่อนผ่านวงจร PDCA ประกอบด้วยการวางแผน (Plan) การลงมือทำ (Do) การตรวจสอบ (Check) และการปรับปรุงแก้ไข (Act)

ภาพที่ 2.6 แสดงวงจรบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act (P-C-D-A)
ที่มา: http://ict.surinpho.go.th/files/WWIH1Z.pdf

นอกจากมาตรฐาน ISO/IEC 27001 แล้ว ยังได้มีการพัฒนามาตรฐานขึ้นมาอีกฉบับหนึ่งคือมาตรฐาน ISO/IEC 17799 (Information technology - Security techniques - Code of practices for information security management) ซึ่งเป็นมาตรฐานที่ระบุถึงแนวปฏิบัติสำหรับการประเมินและจัดการความเสี่ยง รวมถึงแนวทางในการควบคุมตามมาตรฐานISO/IEC 27001ประกอบด้วย 11 หมวดดังนี้

3.1.1 นโยบายความมั่นคงปลอดภัยขององค์กร (Security policy) ประกอบด้วยนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ ซึ่งมีวัตถุประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง โดยผู้บริหารองค์กรจะต้องมีการจัดทำนโยบายที่เป็นลายลักษณ์อักษร รวมถึงการทบทวนนโยบายตามระยะเวลาที่กำหนดหรือมีการเปลี่ยนแปลงที่สำคัญขององค์กร

3.1.2 โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security) โดยได้กล่าวถึงบทบาทของผู้บริหารองค์กรและหัวหน้างานสารสนเทศ ในด้านต่างๆ ดังต่อไปนี้

1) โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กรเพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

2) โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

3.1.3 การบริหารจัดการทรัพย์สินขององค์กร (Asset management) กล่าวถึงบทบาทของหัวหน้างานสารสนเทศและหัวหน้างานพัสดุในด้านต่างๆ ดังต่อไปนี้หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจขึ้นได้การจัดหมวดหมู่สารสนเทศ เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

3.1.4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security) โดยได้กล่าวถึงบทบาทของผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ หัวหน้างานบุคคลและหัวหน้างานที่เกี่ยวข้องในต่างๆ ดังนี้

1) การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอก เข้าใจถึงบทบาทและหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์

2) การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบและทำความเข้าใจกับนโยบาย เพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

3) การสิ้นสุดและการเปลี่ยนการจ้างงาน เพื่อให้พนักงานและผู้เกี่ยวข้องจากหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

3.1.5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security) กล่าวถึงบทบาทของหัวหน้างานสารสนเทศและหัวหน้างานอาคารในด้านต่างๆ ดังต่อไปนี้บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กรความมั่นคงปลอดภัยของอุปกรณ์ เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และทำให้กิจกรรมการดำเนินงานต่างๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

3.1.6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ (Communication and operations management) โดยได้กล่าวถึงบทบาทของผู้บริหารองค์กร ผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ ผู้ที่เป็นเจ้าของกระบวนการทางธุรกิจและพนักงานสารสนเทศในด้านต่างๆ ดังต่อไปนี้

1) การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

2) การบริหารจัดการการให้บริการของหน่วยงานภายนอก เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

3) การวางแผนและการตรวจรับทรัพยากรสารสนเทศ เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

4) การป้องกันโปรแกรมที่ไม่ประสงค์ดี เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

5) การสำรองข้อมูล เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

6) การบริหารจัดการทางด้านความปลอดภัยสำหรับเครือข่ายขององค์กร เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

7) การจัดการสื่อที่ใช้ในการบันทึกข้อมูล เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ

8) การแลกเปลี่ยนสารสนเทศ เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

9) การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และในการใช้งาน

10) การเฝ้าระวังทางด้านความมั่นคงปลอดภัย เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

3.1.7 การควบคุมการเข้าถึง (Access Control) โดยได้กล่าวถึงบทบาทของผู้บริหารสารสนเทศ หัวหน้างานสารสนเทศ ผู้ดูแลระบบและพนักงานในด้านต่างๆ ดังนี้

1) ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ เพื่อควบคุมการเข้าถึงสารสนเทศ

2) การบริหารจัดการการเข้าถึงของผู้ใช้ เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

3) หน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยหรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

4) การควบคุมการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาต

5) การควบคุมการเข้าถึงระบบปฏิบัติการที่ไม่ได้รับอนุญาต

6) การควบคุมการเข้าถึง Application และสารสนเทศที่ไม่ได้รับอนุญาต

7) การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกเพื่อสร้างความมั่นคงปลอดภัยให้กับอุปกรณ์และการปฏิบัติงานที่เกี่ยวข้อง

3.1.8 การจัดหา การพัฒนาและบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance) โดยได้กล่าวถึงบทบาทของหัวหน้างานสารสนเทศ ผู้พัฒนาระบบ และผู้เป็นเจ้าของระบบในด้านต่างๆ ดังนี้

1) ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ เพื่อให้การจัดหาและพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

2) การประมวลผลสารสนเทศใน Application เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์

3) มาตรการการเข้ารหัสข้อมูล เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการทางการเข้ารหัสข้อมูล

4) การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ

5) การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ

6) การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

3.1.9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management) โดยได้กล่าวถึงบทบาทของหัวหน้างานสารสนเทศ หัวหน้างานนิติกร ผู้ดูแลระบบและพนักงานในด้านต่างๆ ดังนี้

1) การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

2) การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

3.1.10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management) โดยได้กล่าวถึงบทบาทของผู้บริหารสารสนเทศ และหัวหน้างานสารสนเทศ ที่เกี่ยวกับหัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

3.1.11 การปฏิบัติตามข้อกำหนด (Compliance) โดยได้กล่าวถึงบทบาทของหัวหน้างานสารสนเทศและหัวหน้างานนิติกร ในด้านต่างๆ ดังต่อไปนี้

1) การปฏิบัติตามข้อกำหนดทางกฎหมาย เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ

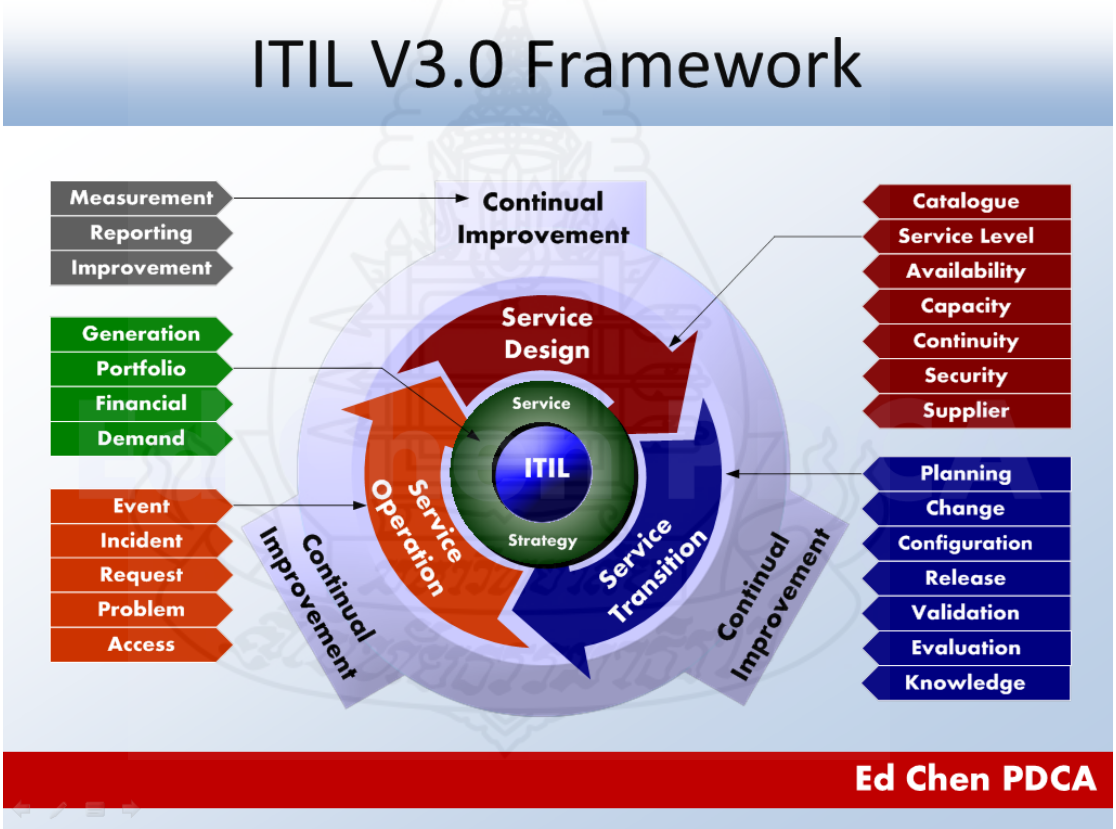
2) การปฏิบัติตามนโยบาย มาตรฐานความปลอดภัยและข้อกำหนดทางเทคนิค เพื่อให้ระบบเป็นตามนโยบายและมาตรฐานความมั่นคงปลอดภัยตามที่องค์กรกำหนดไว้

3) การตรวจประเมินระบบสารสนเทศ เพื่อตรวจประเมินระบบสารสนเทศให้ได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

4. กรอบงานไอทิล (ITIL Framework)

หลักการในการทำงานที่เป็นแบบอย่างที่ดีที่สุดในการที่องค์กรจะจัดการและควบคุมการให้บริการของ IT โดยจะประกอบ ด้วยแบบแผนการทำงานที่มีประสิทธิภาพ การนำไปปฏิบัติในองค์กร และการประเมิน หรือกำหนดเครื่องมือที่จะนาไปใช้ในองค์กร ซึ่งในแต่ละองค์กรจะมีสิ่งแวดล้อมที่ต่างกัน จึงเป็นข้อจำกัดที่ไม่สามารถนำวิธีการจัดการจากองค์กรหนึ่งไปยังอีกองค์กรหนึ่งได้ (เทพฤทธิ์ ฤทธิ์ทองพิทักษ์, 2551: ออนไลน์)

ไอทิลได้ถูกพัฒนาขึ้นในช่วงปลายยุค 1980 โดยซีซีทีเอ - CCTA (Central Computer and Telecommunication Agency)หรือในปัจจุบันได้กลายเป็น OGC (Office of Government Commerce) เมื่อปี2000 ซึ่งเป็นหน่วยงานรัฐบาลของสหราชอาณาจักรเพื่อต้องการใช้เป็นแนวทางกำหนดกระบวนการจัดการงานบริการด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ และได้สรุปรายละเอียดต่างๆ ออกมาเป็นชุดหนังสือที่เรียกว่า IT Infrastructure Library ที่เรียกว่าไอทิล (ITIL) ซึ่งได้ถูกนำไปประยุกต์ใช้ในหลายองค์กรชั้นนำ อย่างแพร่หลาย ภายหลังจึงได้มีการประกาศมาตรฐานของกระบวนการจัดการงานด้านเทคโนโลยีสารสนเทศ (IT Service Management) หรือ ITSM ขึ้นมา ชื่อว่า The British Standard 15000 (BS-150000) และต่อมาได้มีการประกาศเป็นมาตรฐานสากลชื่อว่า ISO-20000:2005 โดยมีการปรับปรุงและพัฒนาอย่างต่อเนื่องจากความร่วมมือจากหลายภาคส่วน และในปี 2011 ก็ได้มีการประกาศเปิดตัว ITIL 2011 ขึ้นมา



ภาพที่ 2.7 ส่วนประกอบหลักของไอทิลเวอร์ชัน 3

ที่มา: http://pdca.edchen.org/2014/07/itil-v30-framework-illustrated.html

ปัจจุบัน ITILv3 ถูกการพัฒนาขึ้นมาจาก ITILv1 และ ITILv2 ได้กำหนดมาตรฐานหลักออกเป็น 5 มาตรฐาน ส่วนข้อแตกต่างระหว่าง v2 กับ v3 ได้แก่ การเปลี่ยนแปลงโครงสร้างการทำงานที่แต่เดิมเน้นวงจรชีวิตของกระบวนการและปรับแต่งให้ไอทีสามารถเข้ากันได้กับธุรกิจทุกประเภทเป็นการบริหารจัดการวงจรชีวิตของกระบวนการบริการที่แผนกไอทีให้สามารถเข้ากับหน่วยงานได้ โดยมีการบริหารการให้บริการเชิงปฏิบัติที่มีประสิทธิภาพ โดยเน้นคำว่า “แนวทางปฏิบัติอันเป็นเลิศหรือ “Best Practice” หรือวิธีการทำงานเชิงปฏิบัติที่ดีที่สุดเพื่อให้เข้าใจถึงความสัมพันธ์ของแต่ละองค์ประกอบ โดยประกอบด้วย 5 หมวดหมู่หลักและกระบวนการย่อยๆ ดังนี้

4.1 กลยุทธ์ด้านการบริการ (Service Strategy) คือ กลยุทธ์และการวางแผนที่สร้างคุณค่าหน้าที่และความรับผิดชอบการวางแผนและพัฒนากลยุทธ์ แผนงานธุรกิจที่เชื่อมโยงกับระบบไอที ปัจจัยที่เป็นโอกาสในการประสบความสำเร็จ และความเสี่ยงที่อาจจะเกิดขึ้นมี 4 กระบวนการได้แก่

4.1.1 การจัดการด้านการเงิน (Financial Management) การจัดการด้านการเงินกับการให้บริการทางด้านไอที และจัดการงบประมาณทางด้านการบัญชี เพื่อรองรับการจัดการทางการเงินที่มีประสิทธิภาพ และสามารถช่วยวางแผนทางการเงินให้กับองค์กรได้ เช่น การวางแผนการสั่งซื้ออุปกรณ์ การบริหารทรัพย์สินทางด้านไอที และ ทรัพยากรที่ถูกใช้ในการให้บริการเพื่อสร้างความมั่นใจให้บุคลากรในองค์กรหรือลูกค้าได้ และ เพื่อให้มีการวางแผนการลงทุนอย่างแม่นยำและมีประสิทธิภาพมากยิ่งขึ้น

4.1.2 การจัดการด้านกลุ่มผลงานจากการบริการ (Service Portfolio Management) เป็นกระบวนการที่รับผิดชอบในการบริหารจัดการงานบริการด้านต่างๆ เช่น บริการที่มีการวางแผนการให้บริการไว้และได้รับการอนุมัติจากผู้บริหารแล้ว (Service Pipeline) บริการที่ให้บริการอยู่ในปัจจุบัน (Service Catalogue) และบริการที่หยุดให้บริการไปแล้ว (Retired Services) อาจรวมถึงการดูแลทางด้านการลงทุนในการจัดการบริการที่มีรูปแบบไม่คงที่ตามโครงสร้างภายในองค์กรและการจัดการมูลค่า จะทำให้เกิดประโยชน์เพิ่มขึ้น

4.1.3 การสร้างกลยุทธ์ (Strategy Generation) โดยในกระบวนการนี้เป็นการมุ่งเน้นไปที่การหาโอกาสทางการตลาดหรือช่องทางในการให้บริการโดยปรับปรุงบริการที่มีอยู่เดิมหรือทำความเข้าใจวิเคราะห์ถึงปัญหาที่ธุรกิจกาลังประสบอยู่และนาเสนอบริการใหม่ที่สามารถตอบสนองความต้องการและสามารถแก้ไขปัญหาให้กับธุรกิจได้ เพื่อให้ฝ่ายบริการทราบเหตุผลต่างๆ ที่จำเป็นต่อการบริการงานด้านไอทีมีการสำรวจยุทธศาสตร์การกำหนดวัตถุประสงค์ วิเคราะห์คู่แข่ง เป็นต้น

4.1.4 การจัดการด้านความต้องการ (Demand Management) เป็นกระบวนการในการวิเคราะห์ความต้องการของผู้ใช้บริการที่มีผลต่อความต้องการของงานบริการและยังรับผิดชอบในการบริหารจัดการทรัพยากรทางด้านไอทีให้สามารถตอบสนองต่อความต้องการที่เกิดขึ้นได้อย่างมีประสิทธิภาพมากที่สุด

4.2 การออกแบบงานบริการ (Service Design) คือวงจรของการบริการ หน้าที่และความรับผิดชอบ การออกแบบวัตถุประสงค์ของการบริการและส่วนประกอบต่างๆ การคัดเลือกและการจัดสรรรูปแบบงานบริการ ค่าใช้จ่ายของงานบริการ การวิเคราะห์ผลประโยชน์และความเสี่ยง การพัฒนางานบริการ การวัดผลและควบคุม รวมถึงปัจจัยการประสบความสำเร็จและความเสี่ยงมี 7 กระบวนการ ได้แก่

4.2.1 การจัดการด้านระดับของการบริการ (Service Level Management) ในกระบวนการนี้มีหน้าที่เพื่อการเจรจาข้อตกลงระดับการบริการระหว่างผู้ให้บริการกับผู้ขอใช้บริการและเป็นตรวจสอบว่ารูปแบบของการบริการที่ออกแบบไว้เป็นไปตามเป้าหมายที่ตกลงกันไว้หรือไม่โดยในการให้บริการจะจัดทาข้อตกลงระดับการให้บริการ (Service Level Agreement, SLA) และตรวจสอบการให้บริการให้เป็นไปตามนั้น และเอกสารข้อตกลงระดับการปฏิบัติการ (Operation Level Agreement, OLAs) ที่ใช้แสดงข้อตกลงระหว่างหน่วยงานภายในที่มีหน้าที่สนับสนุนระดับการให้บริการที่ได้ตกลงไว้กับลูกค้า

4.2.2 การจัดการด้านบัญชีการบริการ (Service Catalogue Management) เป็นกระบวนการที่ทาหน้าที่จัดทาและดูแลบัญชีการบริการให้มีความถูกต้องและทันสมัยอยู่เสมอ โดยจะเป็นการให้บริการเตรียมการเพื่อให้สามารถใช้งานการจัดการด้านบัญชีการให้บริการได้และเป็นการให้ข้อมูลสำคัญสาหรับทุกๆ บริการ รวมถึงการจัดการกระบวนการรายละเอียดการบริการต่างๆ ให้อยู่ในสถานะปัจจุบันและข้อมูลที่ให้บริการเป็นปัจจุบันในด้านต่างๆ ให้มีประสิทธิภาพมากที่สุด

4.2.3 การจัดการความมั่นคงของสารสนเทศ (Information Security Management) เป็นกระบวนการใหม่ที่มีใน ITIL V.3 เพื่อให้งานบริการมีความมั่งคงและปลอดภัยตามหลัก CIA โดยมีการจัดทานโยบาย มาตรฐานและขั้น ตอนการปฏิบัติเพื่อทราบถึงความเสี่ยงในปัจจุบัน ลดช่องโหว่จากภัยคุกคามต่างๆ

4.2.4 การจัดการด้านความพร้อมใช้งาน (Availability Management) เป็นกระบวนการที่ทาหน้าที่เพื่อรักษาความพร้อมใช้งานให้อยู่ในระดับที่ตกลงกันไว้ในการทา SLA โดยต้องมีการจัดทาแผนความพร้อมใช้งาน การเฝ้าตรวจสอบความพร้อมใช้งานและการประเมินความเสี่ยงและการจัดการกลยุทธ์เพื่อให้การบริการมีความพร้อมใช้อยู่ตลอดเวลา ซึ่งเป้า หมายหลักก็เพื่อการเตรียม

ความพร้อมในทุกด้านของงานบริการทางด้านไอทีและทาให้ทราบถึงการออกแบบโครงสร้างเพื่อรองรับความพร้อม ความเชื่อถือ ความถูกต้อง และ ความปลอดภัย

4.2.5 การจัดการด้านขีดความสามารถ (Capacity Management) เพื่อให้มั่นใจว่าผู้ให้บริการดาเนินการได้ตามที่ต้องการหรือมีหน้าที่ในการรักษาขีดความสามารถของธุรกิจและขีดความสามารถขององค์ประกอบต่างๆ ให้เพียงพอตามที่ได้ทาข้อตกลงกันไว้เช่น พื้นที่ที่ให้บริการในการแชร์ข้อมูลจะต้องเพียงพอต่อการใช้งาน เป็นต้น

4.2.6 การจัดการด้านความต่อเนื่องในการบริการด้าน IT (IT Service Continuity Management) จะเป็นกระบวนการรองรับการจัดการแผนธุรกิจต่อเนื่องโดยรวม และมั่นใจได้ว่าโครงสร้างพื้นฐาน และ บริการสามารถครอบคลุมความต้องการ และ ตอบรับกับข้อตกลงของเวลาในการดาเนินการของธุรกิจ และจัดทาการวิเคราะห์ผลกระทบต่อธุรกิจ (Business Impact Analysis, BIA) เพื่อให้ธุรกิจที่ใช้ระบบสารสนเทศสามารถดาเนินการได้อย่างต่อเนื่องจากภัยพิบัติ และเหตุการณ์ผิดปกติ ลดความเสี่ยงทางธุรกิจ มีแผนรับมือความเสี่ยงที่จะเกิด และ สร้างความพร้อมของทีมงานเมื่อเกิดภัยพิบัติขึ้น

4.2.7 การจัดการด้านซัพพลายเออร์ (Supplier Management) เป็นกระบวนการที่เกี่ยวการบริหารจัดการผู้ให้บริการจากภายนอกที่มีหน้าที่สนับสนุนองค์กรและเพื่อให้มั่นใจว่าทุกสัญญาที่ทากับซัพพลายเออร์จะสนับสนุนความต้องการของธุรกิจ และซัพพลายเออร์ทั้งหมดจะต้องทาตามสัญญาข้อผูกพันของบริษัท ให้ได้รับบริการที่มีคุณภาพจากผู้ให้บริการที่มีความพร้อมและเหมาะสมกับความต้องการขององค์กรเพื่อประสิทธิภาพการติดต่อกับผู้ให้บริการ เพิ่มประสิทธิภาพของระบบงานเนื่องจากได้ผู้ให้บริการที่มีความเหมาะสม

4.3 การส่งมอบงานบริการ (Service Transition) คือ การจัดการความเปลี่ยนแปลง ต่างๆ ที่จะเกิดขึ้น ไม่ว่าจะเป็นรูปแบบองค์กร หรือวัฒนธรรมองค์กร การบริหารจัดการความรู้ การวิเคราะห์ความเสี่ยง ข้อควรปฏิบัติในการบริการ สถานการณ์ การงานบริการ แนวทางการฝึกฝน เครื่องมือในการบริการการวัดผลและควบคุม มี 7 กระบวนการได้แก่

4.3.1 การจัดการด้านการเปลี่ยนแปลง (Change Management) เป็นกระบวนการ ซึ่งมีหน้าที่ความรับผิดชอบในการตรวจสอบและควบคุมการเปลี่ยนแปลง และเพื่อมั่นใจว่ามีวิธีการดาเนินการเป็นมาตรฐานและขั้นตอนปฏิบัติได้ถูกใช้อย่างมีประสิทธิภาพและพร้อมกับการรับมือกับการเปลี่ยนแปลงโดยต้องได้รับผลกระทบต่อคุณภาพน้อยที่สุด

4.3.2 การวางแผนการส่งมอบและให้การสนับสนุน (Transition Planning and support) เพื่อการวางแผนและประสานงานทรัพยากร รวมถึงการปรับใช้หลักการปล่อยผ่าน (Release)

เข้ามาภายใต้ต้นทุนที่คาดการณ์ไว้ที่เวลาและการประเมินคุณภาพไว้แล้ว ได้แผนงานที่มีประสิทธิภาพก่อนที่จะดาเนินการ

4.3.3 การจัดการด้านการปรับตั้งและสินทรัพย์ที่เกี่ยวกับการบริการ (Service Asset and Configuration Management) ในส่วนของการจัดการด้านการปรับตั้งนั้นเป็นกระบวนการที่มีอยู่แล้วใน ITIL V.2 แต่ใน ITIL V.3 ได้เพิ่มการจัดการด้านทรัพย์สินการบริการเข้ามาเพื่อทาหน้าที่บริหารจัดการเกี่ยวกับทรัพย์สินที่เกี่ยวข้องในการให้บริการส่วน Configuration Management เป็นกระบวนการเพื่อกำหนดและควบคุมส่วนประกอบของบริการและโครงสร้างพื้นฐาน ทั้งจัดทาเวอร์ชันในการกำหนดการติดตั้งต่างๆ และการจัดการเรื่องหรือรายการที่ต้องปรับตั้ง (Configuration Item, CI) เพื่อให้มีความสัมพันธ์กับกระบวนการอื่นๆ ได้

4.3.4 การจัดการด้านการปล่อยผ่านและการนาไปใช้งาน (Release and Deployment Management) เป็นกระบวนการที่มีอยู่แล้วใน ITIL V.2 แต่ในเวอร์ชัน 2 จะถูกเรียกว่า การจัดด้านการปล่อยผ่าน (Release Management) แต่ในเวอร์ชัน 3 จะเพิ่มกระบวนการนาไปใช้งานขึ้นมาโดยในกระบวนการนี้จัดทาเพื่อวางแผนตารางเวลาและการควบคุมการเคลื่อนไหวของเวอร์ชันที่จะใช้ทดสอบและการนาไปใช้งานจริงและกระบวนการ นาไปใช้งานจะรับผิดชอบในการขนย้าย ไปยังสภาวะการทำงานจริง

4.3.5 การทดสอบและการทวนสอบการบริการ (Service Validation and Testing) เป็นกระบวนการใหม่ใน ITIL V.3 ที่มีหน้าที่ในการทดสอบและตรวจสอบผลลัพธ์ที่ได้จากชุดการออกแบบงานบริการและการปล่อยผ่าน เพื่อให้แน่ใจว่าการติดตั้งและบริการมีผลตามความคาดหวังของผู้ใช้บริการและยืนยันว่าการดาเนินงานไอทีสามารถรองรับบริการใหม่ที่เกิดขึ้นมาได้

4.3.6 การประเมินผล (Evaluation) เป็นกระบวนการใหม่ในไอทิลเวอร์ชัน 3 โดยเน้นไปที่ประสิทธิภาพของการให้บริการว่าเป็นไปตามกฎเกณฑ์ที่ได้กำหนดไว้หรือไม่

4.3.7 การจัดการความรู้ (Knowledge Management) เป็นกระบวนการที่มีหน้าที่ในการสร้างฐานข้อมูลเกี่ยวกับการให้บริการทั้งหมด เพื่อรวบรวมวิเคราะห์จัดเก็บและแบ่งปันความรู้และข้อมูลภายในองค์กร หรือ เป็นการจัดการความรู้เพื่อปรับปรุงประสิทธิภาพโดยการลดความจาเป็นในการที่จะต้องทาการค้นหาความรู้อีกครั้ง ซึ่งให้เป็นศูนย์รวมความรู้ทั้งหมดให้ทุกคนในองค์กรเข้ามาหาความรู้กันซึ่งจะเป็นประโยชน์ในการตอบปัญหาของ Service ที่ได้เปิดให้บริการอีกทางด้วย

4.4 การปฏิบัติงานบริการ (Service Operation) เน้นไปงานทางด้านกิจกรรมที่จำเป็นต่อการปฏิบัติงานในลักษณะแบบวันต่อวันเพื่อให้บรรลุผลสำเร็จในการดูแลรักษาหน้าที่การทำงาน

หรือบริการที่เป็นไปตามข้อตกลงว่าด้วยข้อตกลงใน SLA ที่มีต่อผู้ใช้บริการ รวมไปถึงการเฝ้าตรวจสอบ เหตุการณ์และปัญหาต่างๆ ที่อาจเกิดขึ้นกับบริการได้ โดยมีกระบวนการดังนี้

4.4.1 การจัดการสถานการณ์ (Event Management) กระบวนการที่ช่วยติดตามเหตุการณ์ต่างๆ ทีมีผลกับการให้บริการ ซึ่งอาจจะใช้ระบบการเฝ้าดู (Monitoring) ช่วยตรวจสอบฮาร์ดแวร์ ซอฟต์แวร์ และโครงข่าย เป็นต้น

4.4.2 การดำเนินการเกี่ยวกับการร้องขอ (Request Fulfillment) คือ กระบวนการทีช่วยรับเรื่องความต้องการต่างๆ ของผู้ใช้งานที่ไม่เกี่ยวข้องกับปัญหาการใช้บริการ หรืออาจจะเป็นลักษณะขอคาปรึกษาเกี่ยวกับการใช้บริการ

4.4.3 การจัดการด้านเหตุการณ์ที่ผิดปกติ (Incident Management) กระบวนการที่ช่วยในการสนับสนุนการแก้ไขเหตุการณ์ผิดปกติที่ทาให้การบริการต้องหยุดชะงักโดยมุ่งหมายไปที่การแก้ไขปัญหาให้เร็วที่สุดโดยไม่ต้องสนใจสาเหตุที่แท้จริงก่อน

4.4.4 การจัดการด้านการแก้ไขปัญหา (Problem Management) กระบวนการที่ช่วยในการแก้ไขปัญหาจากสาเหตุทีแท้จริง ซึ่งต่างกับการจัดการด้านเหตุการณ์ผิดปกติที่มุ่งเน้นไปที่การกู้คืนสิ่งที่เป็นปัญหาให้กลับมาพร้อมใช้งานให้เร็วที่สุด โดยกระบวนการนี้สามารถดาเนินการได้ทั้งเชิงรุกและรับ

4.4.5 การจัดการด้านการเข้าถึง (Access Management) เป็นกระบวนการที่เกี่ยวการกำหนดสิทธิ์หรือจากัดสิทธิ์บังคับใช้ในการเข้าถึงข้อมูลต่างๆ

4.4.6 การรับเรื่องเกี่ยวกับการบริการ (Service Desk) ทำหน้าที่เป็นศูนย์กลางในการติดต่อรับแจ้งปัญหาที่เกิดขึ้นจากผู้ใช้บริการโดยแจ้งผ่านทางโทรศัพท์ เว็บ อีเมล์ และเป็นศูนย์กลางในการติดต่อสื่อสารประสานงานระหว่างผู้ใช้งานกับหน่วยบริการต่างๆ เพื่อทาการแก้ไขปัญหาต่างๆ ที่เกิดขึ้นให้สามารถใช้งานได้เป็นปกติโดยเร็วที่สุดเท่าที่จะเป็นไปได้

4.5 การปรับปรุงงานบริการอย่างต่อเนื่อง (Continual Service Improvement) เน้นไปที่การทาการปรับปรุงการให้บริการที่มีมีคุณภาพและรักษาคุณภาพให้คงอยู่ตลอด และให้มีการบริการที่มีความต่อเนื่องอยู่ตลอดเวลา

5. แนวคิดโคโซ (COSO)

จิณห์ระพีร์ พุ่มสงวน (ม.ป.ป.) โคโซ คือ การควบคุมภายในระบบการควบคุมภายในประกอบด้วยนโยบายและวิธีปฏิบัติงานที่กำหนดขึ้นในองค์กรเพื่อให้ความมั่นใจอย่างสมเหตุสมผลว่ากิจการจะบรรลุวัตถุประสงค์และเป้าหมาย ดังนี้

5.1 ด้านการดำเนินงาน (Operation) โดยมุ่งหมายให้การปฏิบัติงานเกิดประสิทธิภาพ ประสิทธิผล และคุ้มค่า ด้วยการกำกับการใช้ทรัพยากรทุกประเภทให้เป็นไปอย่างมีประสิทธิภาพ บรรลุเป้าหมายที่ผู้บริหารกำหนดไว้ และให้ปลอดจากการกระทำทุจริตของพนักงาน หรือผู้บริหาร และหากมีความเสียหายเกิดขึ้นก็ช่วยให้ทราบถึงความเสียหายนั้นได้โดยเร็วที่สุด

5.2 ด้านการรายงานทางการเงิน (Financial Reporting) รายงานทางการเงินหรืองบการเงินไม่ว่าจะเป็นรายงานที่ใช้ภายในหรือภายนอกองค์กร ต่างต้องมีความเชื่อถือได้และทันเวลา มีคุณภาพเหมาะสมสำหรับการนำไปใช้เป็นข้อมูลประกอบการพิจารณา ตัดสินใจทางธุรกิจของนักบริหาร เจ้าหนี้ ผู้ถือหุ้น และผู้ลงทุนทั่วไป

5.3 ด้านการปฏิบัติให้เป็นไปตาม กฎ ระเบียบ และนโยบาย (Compliance with Application Laws and Regulations) การปฏิบัติงานหรือดำเนินธุรกิจให้สอดคล้อง หรือเป็นไปตามบทบัญญัติ ข้อกำหนดของกฎหมาย นโยบาย ข้อบังคับ ระเบียบที่เกี่ยวข้องกับการปฏิบัติงานหรือการดำเนินธุรกิจนั้น เพื่อป้องกันมิให้เกิดผลเสียหายใดๆ จากการละเว้นการปฏิบัติให้เป็นไปตามกฎ ระเบียบเหล่านั้น

ภาพที่ 2.8 กรอบแนวคิดโคโซ (COSO)

ที่มา: https://www.protiviti.com/en-US/Documents/Resource-Guides/Updated-COSO-Internal-Control-Framework-FAQs-Second-Edition-Protiviti.pdf

จากที่กล่าวมาเป็นหน้าที่ของผู้บริหารที่จะต้องตัดสินใจว่าจะกำหนดมาตรการการควบคุมภายในเพื่อวัตถุประสงค์อะไร ต้องการเน้นชัดว่าเพื่อวัตถุประสงค์ใดวัตถุประสงค์หนึ่งเพียงอย่างเดียว หรือต้องการจัดให้มีระบบการควบคุมภายในเพื่อวัตถุประสงค์หลายประการที่สัมพันธ์กัน โดยมี 5 องค์ประกอบ ดังนี้

1. สภาพแวดล้อมของการควบคุม (Control Environment)

สภาพแวดล้อมของการควบคุมเป็นองค์ประกอบที่เกี่ยวกับการสร้างจิตสำนึกและบรรยากาศของการควบคุมภายใน ซึ่งปัจจัยหลายๆ ปัจจัยที่นำมาพิจารณารวมกันส่งผลให้เกิดความมีประสิทธิผลของมาตรการหรือวิธีการควบคุมในองค์กร หรือทำให้มาตรการและวิธีการควบคุมที่ดีขึ้น โดยส่งเสริมให้ทุกคนในองค์กรตระหนักถึงความจำเป็นของระบบการควบคุมภายในและเน้นการสร้างบรรยากาศโดยผู้บริหารระดับสูง เพื่อให้คนขององค์กรเกิดจิตสำนึกที่ดีในการปฏิบัติตามความรับผิดชอบ ดังนั้น สภาพแวดล้อมของการควบคุมที่ดีจะช่วยให้บุคลากรเข้าใจถึงความจำเป็นและความสำคัญของการควบคุมภายใน ทั้งนี้ ปัจจัยที่แสดงให้เห็นถึงสภาพแวดล้อมของการควบคุมประกอบด้วย

1.1 ความซื่อสัตย์และจริยธรรมผู้บริหารควรจัดทำข้อกำหนดด้านจริยธรรมเป็นแนวทางการปฏิบัติ หรือมีมาตรฐานการปฏิบัติงาน โดยปัจจัยนี้ผู้ศึกษาเห็นว่า ปัจจุบันองค์กรมักจะจัดทำ Code of Conduct หรือหลักในการปฏิบัติงานที่เปรียบเสมือนกฎระเบียบขององค์กร ดังนั้น หากมีการแทรกข้อกำหนดด้านจริยธรรมอันเป็นแนวทางที่ควรปฏิบัติลงไป ก็จะทำให้เกิดความสมบูรณ์ในการนำมาใช้ในทางปฏิบัติมากขึ้นส่วนในด้านของผู้บริหารก็จะต้องปฏิบัติตนให้เป็นแบบอย่างที่ดีอย่างสม่ำเสมอและลดวิธีการหรือแรงจูงใจที่รุนแรง เช่น การไม่กดดันให้พนักงานต้องปฏิบัติงานตามเป้าหมายที่สูงเกินจริง

1.2 ความรู้ทักษะความสามารถเชิงแข่งขันองค์กรควรมีการกำหนดระดับความรู้และความสามารถที่จำเป็นสำหรับการปฏิบัติงานแต่ละอย่างต้องกำหนดออกมาเป็นข้อกำหนดด้านพื้นความรู้ทางการศึกษา และประสบการณ์ในการปฏิบัติงานโดยผลสำเร็จในการประเมินองค์ประกอบด้านนี้สามารถพิจารณาได้จากการจัดทำเอกสารกำหนดลักษณะงาน Job Description) เพื่อให้เป็นเกณฑ์ในการพิจารณาบรรจุพนักงานให้เหมาะสมกับหน้าที่และความรับผิดชอบ

1.3 คณะกรรมการบริษัทหรือคณะกรรมการตรวจสอบฝ่ายบริหารระดับสูงเป็นผู้มีบทบาทสำคัญในการสร้างบรรยากาศการควบคุมของกิจการคณะกรรมการบริษัทเป็นเสมือนตัวแทนผู้ถือหุ้นที่จะแต่งตั้งฝ่ายบริหารระดับสูงและกำกับดูแลการปฏิบัติงานให้บรรลุผลประโยชน์สูงสุดขององค์กร คณะกรรมการตรวจสอบเป็นส่วนหนึ่งของคณะกรรมการบริษัทที่ทำ

หน้าที่ส่งเสริมบรรยากาศของการควบคุม และการตรวจสอบทั้งภายในและการสอบบัญชีให้เป็นไปอย่างอิสระจากฝ่ายบริหาร รวมทั้งความรู้ ประสบการณ์ในการปฏิบัติงาน การตั้งคำถามที่ตรงประเด็นและลึกซึ้งเกี่ยวกับงานของฝ่ายบริหาร และติดตามวิเคราะห์คำตอบที่ได้ความถี่และการมีเวลาในการปฏิบัติหน้าที่และประชุมกับผู้บริหารฝ่ายการเงิน บัญชี ตรวจสอบภายใน และผู้สอบบัญชี ความเพียงพอและทันสมัยของสารสนเทศที่จัดให้คณะกรรมการบริษัทและคณะกรรมการตรวจสอบที่จะติดตามการบรรลุผลของแผนกลยุทธ์ เป้าหมายของฝ่ายบริหารฐานะการเงิน ผลการดำเนินงาน และปฏิบัติตามสัญญาที่สำคัญ ความเพียงพอและทันกาลของสารสนเทศที่คณะกรรมการบริษัทและคณะกรรมการตรวจสอบมีเกี่ยวกับข้อมูลพิเศษ เช่น ค่าใช้จ่ายในการเดินทางของผู้บริหารระดับสูง รายงานการสืบสวนจากสถาบันกำกับดูแล การจ่ายเงินที่ผิดกฎหมาย เป็นต้น

1.4 ปรัชญาและรูปแบบการทำงานของผู้บริหารองค์ประกอบนี้เป็นสิ่งใหม่ของการบริหาร ซึ่งบางครั้งปรัชญาและสไตล์การทำงานผู้บริหารถูกละทิ้งความสนใจไม่เข้าใจอย่างลึกซึ้งการทำความเข้าใจแนวโน้มทางความคิดขององค์ประกอบนี้ เช่น เป็นผู้บริหารที่กล้าเสี่ยง หรือชอบความระมัดระวัง ความถี่ในการติดตามงานระหว่างผู้บริหารระดับสูงกับระดับปฏิบัติการ ทัศนคติของผู้บริหารที่มีต่อการเลือกนโยบายบัญชี ความระมัดระวังในการกำหนดประมาณการทางบัญชี การเปิดเผยข้อมูล และการไม่แสดงข้อมูลที่เป็นเท็จ รวมทั้งการส่งเสริมในงานบัญชี การพัฒนาความรู้ของฝ่ายบัญชี เหล่านี้ล้วนเป็นสิ่งที่ทำให้สามารถทราบทิศทางองค์กรได้ว่าจะถูกวางอยู่ในจุดใดหรือมีความเสี่ยงอย่างไรบ้าง

1.5 โครงสร้างการจัดองค์กรโครงสร้างขององค์กรที่ได้รับการจัดไว้ดีย่อมเป็นพื้นฐานสำคัญที่ทำให้ผู้บริหารสามารถวางแผนงาน สั่งการ และควบคุมการปฏิบัติงานได้อย่างถูกต้อง รวดเร็ว และมีประสิทธิภาพ โดยการจัดโครงสร้างองค์กรให้เหมาะสมกับลักษณะของธุรกิจนั้น

1.6 การมอบอำนาจและความรับผิดชอบ (Assignment of Authority and responsibility) การมอบอำนาจให้กับผู้ปฏิบัติงานในระดับปฏิบัติการ ควรจะต้องมีการกำหนดอย่างชัดเจน โดยในการประเมินองค์ประกอบด้านนี้จะต้องพิจารณาจาก

1.6.1 ความชัดเจนในการระบุความรับผิดชอบและอำนาจในการอนุมัติให้ผู้ปฏิบัติการฝ่ายต่างๆ ในการปฏิบัติงานให้ได้ตามวัตถุประสงค์

1.6.2 ความเหมาะสมของมาตรฐานการควบคุมและวิธีการควบคุมที่เกี่ยวข้อง รวมทั้งเอกสารที่ระบุลักษณะความรับผิดชอบในตำแหน่งงาน

1.6.3 ความเหมาะสมของจำนวนพนักงาน ซึ่งจะต้องมีความรู้และทักษะที่เหมาะสมกับปริมาณงานและความซับซ้อนของกิจกรรม รวมทั้งระบบงานที่เกี่ยวข้อง

1.7 นโยบายและวิธีบริหารงานด้านทรัพยากรมนุษย์ในการบริหารองค์กรมีปัจจัยหลายอย่างที่เป็นสิ่งสำคัญแก่องค์กรไม่ว่าจะเป็นระบบบริหารเทคโนโลยี สิ่งเหล่านี้ล้วนเป็นสิ่งที่องค์กรจะต้องพัฒนาตามยุคสมัยให้ทันแต่อย่างไรก็ตาม สิ่งที่สำคัญที่สุดขององค์กรที่จะขาดไม่ได้ก็คือ ทรัพยากรมนุษย์ เพราะทรัพยากรมนุษย์ที่ดีเป็นปัจจัยที่ทำให้องค์กรบรรลุเป้าหมายอย่างแท้จริง ดังนั้น ฝ่ายบริหารควรกำหนดนโยบายและวิธีบริหารงานด้านทรัพยากรมนุษย์ เช่น การว่าจ้าง การคัดเลือกบุคลากร และเมื่อได้บุคลากรที่เหมาะสมแล้ว ก็ต้องมีนโยบายในการจูงใจและพัฒนาให้มีความรู้ความสามารถที่ทันสมัยตามทันเทคโนโลยีเปลี่ยนแปลงอยู่ตลอดเวลา การประเมินองค์ประกอบนี้ เช่น นโยบายและวิธีปฏิบัติในส่วนที่เกี่ยวกับการคัดเลือก การฝึกอบรม การเลื่อนตำแหน่ง และการจ่ายผลตอบแทน ความเหมาะสมของวิธีการที่ใช้เมื่อพบความประพฤติที่แตกต่างจากนโยบายและวิธีปฏิบัติที่กำหนด เช่น มีบทลงโทษ ความเหมาะสมในการใช้นโยบายการเลื่อนตำแหน่งและความดีความชอบ

1.8 การตรวจสอบภายใน การตรวจสอบภายในถือเป็นส่วนหนึ่งของการควบคุมภายในและเป็นเครื่องมือทางการบริหารที่ทำให้สภาพแวดล้อมของการควบคุมมีคุณภาพ ผู้ตรวจสอบภายในต้องมีความอิสระเพียงพอที่จะรายงานผลการตรวจสอบและประเมินผลให้แก่ผู้บริหาร และผู้รับผิดชอบการปฏิบัติงานที่ได้รับการตรวจสอบและประเมินผลทั้งนี้ผู้ตรวจสอบภายในควรได้รับการสนับสนุนอย่างเหมาะสมจากผู้บริหาร

2. การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงซึ่งจัดได้ว่าเป็นเครื่องมือในการบริหารอย่างหนึ่งที่ผู้บริหารนิยมใช้ในปัจจุบัน เนื่องจากในปัจจุบันเป็นยุคการค้าที่มีการแข่งขันอย่างเสรี ซึ่งมีคู่แข่งมากมายที่กำลังต่อสู้กับองค์กร ดังนั้น ความเสี่ยงจึงเป็นเรื่องที่หลีกเลี่ยงไม่ได้ ซึ่งการประเมินความเสี่ยงนั้น เป็นกระบวนการที่ทำให้กิจการขององค์กรทราบถึงความเสี่ยงที่กำลังจะเผชิญล่วงหน้าได้ เมื่อทราบถึงความเสี่ยงแล้วก็สามารถที่จะบริหารความเสี่ยงเพื่อเปลี่ยนวิกฤติให้เป็นโอกาส และเพื่อลดผลกระทบความเสียหายที่จะเกิดขึ้นได้เนื่องจากเป็นการค้ายุคการแข่งขันเสรีที่มีความเสี่ยงสูงและต้องเตรียมความพร้อมในทุกสภาวการณ์ การประเมินความเสี่ยงจะทำให้ฝ่ายบริหารได้ทราบถึงปัจจัยเสี่ยงทั้งจากปัจจัยภายใน และปัจจัยภายนอกที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์การอย่างเพียงพอและเหมาะสม โดยแบ่งได้เป็น

2.1 ปัจจัยเสี่ยงระดับกิจการอาจเกิดจากปัจจัยเสี่ยงต่างๆ ทั้งภายนอกและภายในกิจการ โดยปัจจัยเสี่ยงภายนอก เป็นปัจจัยที่เกิดจากภายนอกที่กิจการควบคุมไม่ได้ ซึ่งผู้บริหารต้องติดตามศึกษาเพื่อหาวิธีปฏิบัติในการเปลี่ยนวิกฤตให้เป็นโอกาส หรือลดผลเสียหายที่จะเกิดขึ้น ส่วนปัจจัยเสี่ยงภายใน เป็นปัจจัยที่เกิดจากภายในองค์กรที่ผู้บริหารสามารถจัดการได้

ซึ่งสามารถยกตัวอย่างของปัจจัยภายนอก เช่น การเปลี่ยนแปลงทางเทคโนโลยี ความต้องการและความมุ่งหวังของลูกค้าที่มีต่อสินค้าหรือบริการ กฎหมายและข้อกำหนดต่างๆ ของภาครัฐ และตัวอย่างของปัจจัยภายใน เช่น ความซื่อสัตย์และจริยธรรมของผู้บริหาร ความสลับซับซ้อนของการปฏิบัติงาน ขวัญและกำลังใจของพนักงานในการปฏิบัติงาน ขนาดของหน่วยงาน โดยหน่วยงานใหญ่ย่อมมีโอกาสผิดพลาดสูงกว่าหน่วยงานเล็ก

2.2 ปัจจัยเสี่ยงระดับกิจกรรมเป็นปัจจัยเสี่ยงที่อาจเกิดในหน่วยงานสาขา แผนงาน โครงการ และกระบวนการปฏิบัติงานที่สำคัญ เช่น การจัดหา การตลาด เป็นต้นหลังจากระบุปัจจัยเสี่ยงแล้ว ขั้นต่อมาที่สำคัญคือ การวิเคราะห์และจัดระดับความเสี่ยง หากปัจจัยเสี่ยงใดสามารถคำนวณจำนวนที่อาจเกิดขึ้นได้โดยตรงในเชิงปริมาณ เช่น การใช้สูตรคำนวณจำนวนค่าความเสียหาย ก็ให้ประเมินและจัดระดับความเสี่ยงไปตามความสำคัญของจำนวนที่คำนวณได้ หากการวิเคราะห์และจัดระดับความเสี่ยงโดยใช้สูตรคำนวณเป็นไปได้ยาก อาจต้องใช้วิธีการให้คะแนนเชิงเปรียบเทียบแทน เช่น การให้ระดับ 1-3 โดย 1 = ไม่พอใจ 2 = ปานกลาง และ 3 = พอใจ เป็นต้นหลังจากนั้นผู้บริหารควรกำหนดวิธีการบริหารความเสี่ยง และตัดสินใจเกี่ยวกับกิจกรรมควบคุมภายในที่จำเป็นเพื่อลดหรือบรรเทาความเสี่ยงเหล่านั้นและเพื่อให้บรรลุผลสำเร็จตามวัตถุประสงค์ด้านประสิทธิภาพประสิทธิผลของการดำเนินงาน รายงานทางการเงินและการดำเนินงานเป็นที่น่าเชื่อถือ และการปฏิบัติที่เป็นไปตามกฎหมาย และระเบียบข้อบังคับ ผู้บริหารระดับส่วนงาน หรือผู้ประเมินควรจะต้องเน้นการให้ความสำคัญเกี่ยวกับกระบวนการบริหาร

ในการกำหนดวัตถุประสงค์การระบุความเสี่ยง การวิเคราะห์ความเสี่ยงและการบริหารความเสี่ยงในช่วงของการเปลี่ยนแปลง และบางเรื่องมีลักษณะเป็นนามธรรมซึ่งต้องใช้ดุลยพินิจ แต่เรื่องเหล่านี้มีความสำคัญในการใช้ประเมินความเสี่ยงว่าเหมาะสมเพียงพอหรือไม่ ซึ่งการบริหารความเสี่ยงนั้น COSO ได้กำหนดวิธีการตอบสนองความเสี่ยงไว้พอสรุปได้ดังนี้

1. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) หมายถึงการเลิกหรือหลีกเลี่ยงการกระทำเหตุการณ์ที่ก่อให้เกิดความเสี่ยง เช่น การกระทำงานที่องค์กรไม่ถนัดอาจหลีกเลี่ยงโดยการไม่กระทำ หรือจ้างบุคคลภายนอก เป็นต้น

2. การลดความเสี่ยง (Risk Reduction) หมายถึงการลดโอกาสความน่าจะเกิดหรือการลดความเสียหาย หรือการลดทั้งสองด้านพร้อมกัน การลดความเสี่ยงที่สำคัญคือการจัดระบบการควบคุมเพื่อป้องกัน หรือค้นพบความเสี่ยงเฉพาะวัตถุประสงค์นั้นอย่างเหมาะสมทันกาลมากขึ้นรวมถึงการกำหนดแผนสำรองในกรณีมีเหตุการณ์ฉุกเฉิน

3. การแบ่งความเสี่ยง (Risk Sharing) หมายถึงการลดโอกาสความน่าจะเกิดหรือการลดความเสียหาย โดยการแบ่ง การโอน การหาผู้รับผิดชอบร่วมในความเสี่ยง เช่น การจัดประกันภัย

4. การยอมรับความเสี่ยง (Risk Acceptance) หมายถึงการไม่กระทำการใดๆ เพิ่มเติมกรณีนี้ใช้กับความเสี่ยงที่มีสาระสำคัญน้อย ความเสี่ยงน่าจะเกิดน้อย หรือเห็นว่ามีต้นทุนในการบริหารความเสี่ยงสูงกว่าผลที่ได้รับ

3. กิจกรรมการควบคุม (Control Activities)

การกระทำที่สนับสนุนและส่งเสริมการปฏิบัติงานให้เป็นไปตามนโยบายวิธีปฏิบัติงานและคำสั่งต่างๆ ที่ฝ่ายบริหารกำหนด ซึ่งจะต้องเป็นการกระทำที่ถูกต้องและในเวลาที่เหมาะสม จะเพิ่มความมั่นใจในความสำเร็จตามวัตถุประสงค์ที่กำหนดกิจกรรมการควบคุมภายในสามารถแบ่งออกตามประเภทของการควบคุมได้ดังต่อไปนี้

3.1 การควบคุมแบบป้องกันเป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันมิให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก

3.2 การควบคุมแบบค้นพบเป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อทำการค้นพบข้อผิดพลาดที่เกิดขึ้นมาแล้ว

3.3 การควบคุมแบบแก้ไขเป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือเพื่อหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

3.4 การควบคุมแบบส่งเสริมเป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จโดยตรงกับวัตถุประสงค์ที่ต้องการ

4. ข้อมูลสารสนเทศ และการสื่อสารในองค์กร (Information and Communication)

การสื่อสารและสารสนเทศถือเป็นองค์ประกอบสำคัญต่อการควบคุมภายในยุคปัจจุบัน ซึ่งนับได้ว่าเป็นยุคของข้อมูลข่าวสาร และถ้าข้อมูลข่าวสารมีความทันสมัยก็จะทำให้องค์กรรับรู้ข้อมูลได้ทันท่วงที มีความได้เปรียบทางด้านธุรกิจ และสามารถเพิ่มประสิทธิภาพให้กับการบริหารองค์กรได้ดีอีกด้วย แต่อย่างไรก็ตามความถูกต้องของข้อมูลข่าวสารก็ถือว่าเป็นสิ่งสำคัญยิ่งไม่แพ้กัน ดังนั้น ควรให้ผู้ปฏิบัติงานที่เกี่ยวข้องได้เข้าถึงหรือรับทราบข้อมูลที่เกี่ยวข้องผ่านเครื่องมือต่างๆ โดยสามารถแบ่งได้ ดังนี้

4.1 ข้อมูลสารสนเทศ (Information) เป็นข้อมูลที่มีความจำเป็นสำหรับการปฏิบัติงานของบุคลากรทั้งผู้บริหารและผู้ปฏิบัติงานทุกระดับ โดยผู้บริหารต้องใช้ข้อมูลประกอบการพิจารณาสั่งการ ส่วนผู้ปฏิบัติงานมักใช้ข้อมูลสารสนเทศเป็นเครื่องชี้นำทิศทางการปฏิบัติหน้าที่ ข้อมูลสารสนเทศที่ดีที่ควรจัดให้มีในทุกๆ องค์กรควรมีลักษณะดังนี้คือ

4.1.1 ความเหมาะสมกับการใช้ หมายถึง สารสนเทศมีเนื้อหาสาระที่จำเป็นต่อการตัดสินใจของผู้ใช้

4.1.2 ความถูกต้องสมบูรณ์ หมายถึง สารสนเทศที่สามารถสะท้อนผลตามความจำเป็นและให้ข้อมูลที่เป็นจริงและมีรายละเอียดที่จำเป็นครบถ้วน

4.1.3 ความเป็นปัจจุบัน หมายถึง การให้ตัวเลขและข้อเท็จจริงล่าสุดที่เป็นปัจจุบันสามารถใช้เป็นข้อมูลที่เชื่อถือได้สำหรับประกอบการตัดสินใจได้ทันเวลา

4.1.4 สะดวกในการเข้าถึง หมายถึง ความยากง่ายสำหรับผู้ที่มีอำนาจหน้าที่ที่เกี่ยวข้อง และมีระบบรักษาความปลอดภัยป้องกันผู้ที่ไม่มีส่วนเกี่ยวข้องให้ไม่สามารถเข้าถึงข้อมูลสารสนเทศที่มีความสำคัญหรือข้อมูลที่เป็นความลับได้

ในการจัดให้มีสารสนเทศที่ดีเป็นหน้าที่ของผู้บริหารที่จะจัดหาบุคลากรที่มีความรู้ ความสามารถ และประสบการณ์ทางวิชาชีพ รวมทั้งการจัดหาเครื่องมือ เครื่องใช้เทคโนโลยี และระบบงานที่ดี และประสบการณ์ทางวิชาชีพ รวมทั้งการจัดหาเครื่องมือ เครื่องใช้เทคโนโลยี และระบบงานที่ดี เพื่อให้มีการปฏิบัติตามระบบงานที่กำหนดไว้อย่างสม่ำเสมอและควบคุมการปฏิบัติให้เป็นไปตามระเบียบที่กำหนดไว้อย่างเคร่งครัด

การสื่อสาร (Communication) การสื่อสารที่มีประสิทธิภาพนั้น หมายถึง การจัดระบบการสื่อสารให้ข้อมูลส่งไปถึงผู้ที่ควรได้รับ และระบบการสื่อสารที่ดีนั้น จะต้องประกอบด้วยทั้งระบบการสื่อสารกันภายในองค์กรหรือการสื่อสารที่เกิดขึ้นภายในองค์กรเดียวกัน ซึ่งควรจัดให้เป็นรูปแบบการสื่อสารสองทาง และอีกระบบคือการสื่อสารภายนอกซึ่งเป็นการสื่อสารกับลูกค้าหรือบุคคลอื่นๆ นอกองค์กร

5. การติดตามและประเมินผล (Monitoring and Evaluation)

การควบคุมภายในขององค์กรจะสมบูรณ์ไม่ได้หากขาดการติดตามและประเมินผล เพราะเป็นองค์ประกอบสำคัญที่ทำให้ผู้บริหารมั่นใจได้ว่า มาตรการและระบบการควบคุมภายในมีประสิทธิผลและได้รับการปรับปรุงให้ทันสมัยอยู่ตลอดเวลา

5.1 การติดตามผลระหว่างการดำเนินงาน (On Going Monitoring) หมายถึง การสังเกต การติดตาม ระบบรายงานความคืบหน้าของงาน รวมทั้งการสอบทานหรือการยืนยันผลงานระหว่างการปฏิบัติงาน

5.2 การประเมินผลอิสระ (Independent Evaluation) เป็นการประเมินผลที่เกิดขึ้นในช่วงเวลาที่แล้วแต่จะกำหนด หรือการประเมินอิสระอาจหมายถึง การประเมินโดยผู้ที่ไม่มีส่วนเกี่ยวข้องกับการกำหนดระบบควบคุมภายใน เพื่อให้สามารถแสดงความเห็นได้อย่างเป็นอิสระ เช่น การประเมินจากผู้ตรวจสอบภายใน เป็นต้น

5.3 การประเมินการควบคุมด้วยตนเอง (Control Self Assessment : CSA) เป็นการจัดประชุมเชิงปฏิบัติร่วมกัน ระหว่างผู้บริหาร ผู้ปฏิบัติงาน ผู้มีความรู้ด้านการควบคุม และผู้อื่นที่มีส่วนเกี่ยวข้อง เพื่อกำหนดกิจกรรมควบคุมและประเมินผลร่วมกัน ในด้านที่ได้รับมอบหมายให้ดำเนินงานนั้น

6. ไมโครซอฟท์แอคเซส(Microsoft Access)

Microsoft Access เป็นเครื่องมือออกแบบและพัฒนาโปรแกรมประยุกต์ฐานข้อมูลที่คุณสามารถใช้ในการติดตามข้อมูลที่สำคัญได้เป็นโปรแกรมประเภทโปรแกรมจัดการฐานข้อมูลเชิงสัมพันธ์ ที่ทำกันในสำนักงาน หรือองค์กรขนาดเล็ก ซึ่งสามารถเก็บข้อมูล ประมวลผลข้อมูล ออกแบบฟอร์มเก็บข้อมูล ออกแบบแบบสอบถาม (Query) ออกแบบและพิมพ์รายงาน จัดทำเว็บไซต์ในการรับ/ส่ง ข้อมูล และยังสามารถเขียนกลุ่มโปรแกรม (แมโคร และ มอดูล) เพื่อใช้ในการทำงานได้ และสามารถเชื่อมต่อกับฐานข้อมูล Microsoft SQL Server ได้ด้วย (It genius. 2558)

Microsoft Access นั้นสามารถทำงานต่างๆ ได้ดังนี้

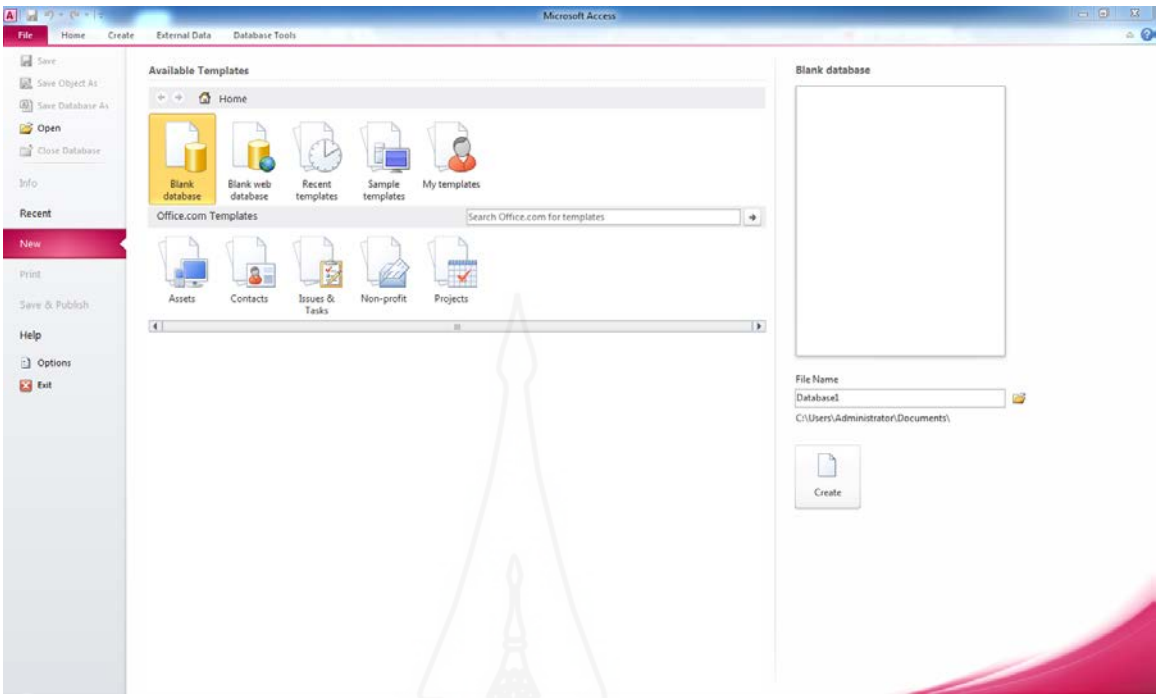
6.1 ใช้สร้างแอปพลิเคชันฐานข้อมูล เช่น โปรแกรมควบคุมสินค้าคงคลัง โปรแกรมบันทึกเวลาเข้าออกของพนักงาน เป็นต้น โดยที่ใน Access นั้น มีเครื่องมือต่างๆ ในการสร้างแอพพลิเคชั่นได้อย่างรวดเร็ว และใช้งานง่าย ซึ่งอาจจะไม่ต้องเขียนโปรแกรมเลยก็ได้

6.2 มีเครื่องมือในการสอบถามข้อมูลต่างๆ จากฐานข้อมูล เพื่อนำผลลัพธ์ไปทำงานบางอย่าง เช่น ต้องการทราบว่ายอดขายสินค้าแต่ละอย่างเป็นเท่าไร เป็นต้น

6.3 สามารถสร้างเครื่องมือในการติดต่อกับผู้ใช้ได้อย่างเหมาะสม เช่น การแสดงข้อมูลลูกค้าให้ผู้ใช้งานแก้ไขข้อมูลได้เป็นต้น

6.4 ช่วยในการสร้างรายงานจากฐานข้อมูลได้ เพื่อใช้ในการทำงานบางอย่าง เช่น พิมพ์ชื่อและที่อยู่ลูกค้าเพื่อทำฉลากติดซองจดหมายส่งข้อมูลไปยังลูกค้า เป็นต้น

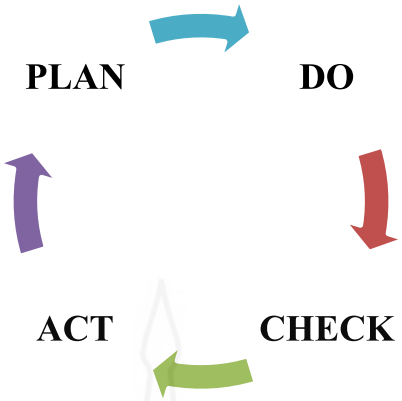
6.5 สามารถเผยแพร่ข้อมูลขององค์กรที่อยู่ในฐานข้อมูลผ่านทางอินเตอร์เน็ต และอินทราเน็ตได้อย่างง่ายดาย เนื่องจากในAccess มีเครื่องมือที่ช่วยในการทำงานต่างๆ เหล่านี้อย่างครบถ้วน



ภาพที่ 2.9 หน้าต่างโปรแกรม Microsoft Access

7. วงจรการบริหารงานคุณภาพ (PDCA)

PDCA หมายถึง วงจรการบริหารงานคุณภาพ หรือวงจรเดมิง (Deming Cycle) โดย W.Edward Deming เป็นเครื่องมือสำหรับการปรับปรุงกระบวนการทำงาน คือ Plan (วางแผน) Do (ปฏิบัติ) Check (ตรวจสอบ) และ Act (การดำเนินการให้เหมาะสม) เพื่อการปรับปรุงงานอย่างต่อเนื่อง ซึ่งการปรับปรุงจะถูกเก็บให้อยู่ในมาตรฐานการทำงานให้มีการพัฒนาอย่างไม่สิ้นสุด (การเขียนผังการปฏิบัติงานด้วยวงจรคุณภาพ PDCA เพื่อการจัดทำคู่มือการปฏิบัติงาน ของบุคลากรสายสนับสนุนในวิทยาเขตจันทบุรี มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก วิทยาเขตจันทบุรี, ม.ป.ป.)



ภาพที่ 2.10 วงจรคุณภาพ PDCA

จากภาพที่ 2.10 สามารถอธิบายการปฏิบัติงานภายใต้วงจรคุณภาพ PDCA ได้ดังนี้

1. Plan หมายถึง การวางแผนการดำเนินงานอย่างรอบคอบในกระบวนการทำงาน เพื่อให้บรรลุเป้าหมายและวัตถุประสงค์อย่างมีประสิทธิภาพ

2. Do หมายถึง การดำเนินงานตามแผนและขั้นตอนการปฏิบัติงานในกระบวนการทำงาน

3. Check หมายถึง การตรวจสอบความถูกต้องของการปฏิบัติงาน

4. Action หมายถึง การตรวจสอบผลการดำเนินงานให้เป็นไปตามแผนและวัตถุประสงค์ของกระบวนการทำงาน หรือมีการรายงานสรุปผลการดำเนินงานต่อผู้บริหาร เพื่อเป็นข้อมูลและแนวทางในการปรับปรุงการปฏิบัติงานให้มีคุณภาพมากยิ่งขึ้น

8. งานวิจัยที่เกี่ยวข้อง

ศศิธร แซ่คู (2552) ได้ทำการวิจัยเรื่อง การนำกรอบแนวคิด ITIL เข้ามาประยุกต์ใช้ในองค์กรให้ประสบความสำเร็จกรณีศึกษา บริษัทแอดอิน คอมพิวเตอร์กร จำกัด โดยมีวัตถุประสงค์เพื่อศึกษาและนำมาตรฐาน ITIL มาใช้เป็นแนวทางในกระบวนการบริหารจัดการระบบสารสนเทศของบริษัทเพื่อให้บริการทางด้านระบบสารสนเทศอย่างมีประสิทธิภาพเป็นระบบ จากการวิธีการดำเนินการโครงการได้นำกระบวนการต่างๆ โดยผลการศึกษา คือ เกิดเอกสารขั้นตอนการปฏิบัติงานที่ชัดเจนข้อตกลงการบริการขึ้นระหว่างฝ่ายสารสนเทศกับผู้ใช้บริการตาม Service Level Agreement ตามกระบวนการ ITIL6 เพื่อให้เกิดความเข้าใจตรงกันได้แก่ 1) คำจำกัดความ 2) ชั่วโมงการทำงานให้บริการ 3) ขอบเขตการให้บริการ 4) เงื่อนไขการให้บริการ 5) บริการที่จัดอยู่ใน

เงื่อนไขการให้บริการ 6) สิ่งที่นอกเหนือจากเงื่อนไขบริการและ 7) การเข้าระบบขอใช้บริการโดยผู้ให้บริการและผลจากการวัดความพึงพอใจของผู้ใช้บริการพบว่าผู้ใช้บริการมีความพึงพอใจมากขึ้นต่อการปรับปรุงบริการของฝ่ายเทคโนโลยีสารสนเทศมีการตอบสนองต่อผู้ใช้บริการได้รวดเร็วยิ่งขึ้นได้

นงลักษณ์ กอศรีลบุตร (2549) ได้ทำการวิจัยเรื่อง การนำมาตรฐาน COBIT มาประยุกต์ใช้ในองค์กร เพื่อปรับปรุงกระบวนการตรวจสอบระบบสารสนเทศ กรณีศึกษา: ผู้ประกอบการธุรกิจทางการเงินที่ไม่ใช่สถาบันการเงิน (Non-bank) แห่งหนึ่งเพื่อให้ทราบถึงปัญหาและอุปสรรคของกระบวนการตรวจสอบระบบสารสนเทศที่ไม่สอดคล้องกับมาตรฐานการควบคุมภายใน และนำแนวทางปรับปรุงการปฏิบัติงานโดยการนำมาตรฐานการควบคุมภายในหรือโคบิตมาประยุกต์ใช้เพื่อช่วยแก้ไขปัญหา เช่น ปัญหาคือ User หรือ IT Auditor รับทราบโครงการล่าช้า ผู้วิจัยได้แนะนำให้ใช้กระบวนการ PO10 ในการจัดการปัญหาดังกล่าว ฯลฯ ซึ่งจากงานวิจัยจะพบว่าการเลือกกระบวนการในกรอบโคบิตเพื่อเข้ามาช่วยในการควบคุมการทำงานไม่จำเป็นต้องเลือกทุกกระบวนการเข้ามาใช้ ควรเลือกเฉพาะบางกระบวนการที่เกี่ยวข้องกับการดำเนินงานเท่านั้น

ประสิทธิ์ ธีรวงศธร (2556) ได้ทำการวิจัยเรื่องการประเมินการบริหารโครงการสารสนเทศ โดยใช้หลักธรรมาภิบาลไอที กรณีของ บริษัท เมืองทองมหาชัย จำกัดโดยมีวัตถุประสงค์เพื่อนำกรอบธรรมาภิบาลด้านไอทีมาใช้ในการบริหารโครงการสารสนเทศและกำหนดตัวชี้วัดและประเมินโครงการสารสนเทศตามหลักธรรมาภิบาลไอที โดยการนำกรอบโคบิตที่ได้รับการยอมรับในการควบคุมกระบวนการด้านไอทีตามหลักธรรมาภิบาลไอที โดยใช้โครงการจัดเก็บข้อมูลและกำหนดสิทธิการใช้งาน ของบริษัท เมืองทองมหาชัย จำกัดพบว่าประสิทธิผลของโครงการในจัดเก็บข้อมูลและกำหนดสิทธิการใช้งาน พบว่า องค์กรสามารถประหยัดค่าใช้จ่ายทางด้านซอฟต์แวร์มาก เนื่องจากเป็นการใช้ซอฟต์แวร์ที่ไม่มีค่าลิขสิทธิ์และคุณสมบัติของซอฟต์แวร์สามารถตอบโจทย์การใช้งานในองค์กรได้ตามที่ต้องการ

จากงานวิจัยดังกล่าวจะเห็นได้ว่าปัจจุบันการใช้กรอบมาตรฐานด้านธรรมาภิบาลในการควบคุมและเป็นแนวทางแก่ระบบสารสนเทศนั้นมีความสำคัญอย่างยิ่ง หลายองค์กรที่ใช้ระบบสารสนเทศในการขับเคลื่อนธุรกิจขององค์กรกำลังพัฒนามาตรฐานทางด้านสารสนเทศของตนเองโดยใช้กรอบมาตรฐานดังกล่าวซึ่งการที่จะได้การยอมรับความเป็นมาตรฐานนั้นจำเป็นต้องผ่านระบบการตรวจสอบ ซึ่งทางผู้วิจัยได้เล็งเห็นความสำคัญของการสร้างพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิตเข้ามาใช้เพื่อบริหารจัดการระบบเทคโนโลยีสารสนเทศของธุรกิจจำหน่ายรถบรรทุกเพื่อช่วยให้เกิดการประสานงานระหว่างการทำงานและแก้ไขปัญหาอย่างเป็นระบบ ตอบสนองความต้องการของ

ผู้ใช้งานภายใต้ข้อตกลงร่วมกันเพื่อทำให้องค์กรปฏิบัติตามได้อย่างถูกต้อง และช่วยให้ธุรกิจสามารถดำเนินงานได้อย่างโปร่งใสในการบริหารในรูปแบบของหลักธรรมาภิบาลอย่างมีประสิทธิภาพและยั่งยืน

บทที่ 3
วิธีดำเนินงานวิจัย

การพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิตมีขั้นตอนและวิธีการวิจัยดังต่อไปนี้

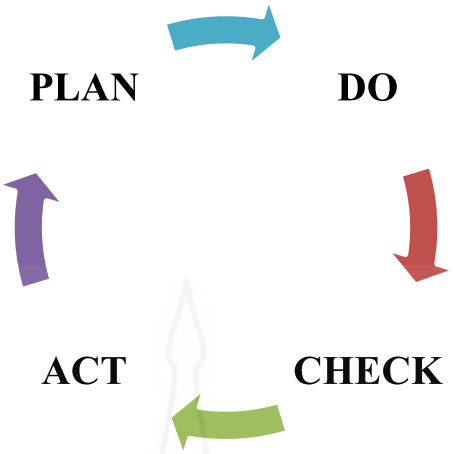
1. ขั้นตอนการดำเนินการวิจัย
2. อุปกรณ์และเครื่องมือที่ใช้ในการวิจัย

1. ขั้นตอนการดำเนินการวิจัย

ในการพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิตผู้วิจัยได้ประยุกต์ใช้แนวคิด PDCA หรือวงจรเดมิง ซึ่งเป็นวงจรการควบคุมคุณภาพมาเป็นแนวทางในการพัฒนาระบบ 4 ขั้นตอนดังตารางที่ 3.1

ตารางที่ 3.1 วงจรเดมิง

วงจรเดมิง	
P=Plan	-กำหนดวัตถุประสงค์และขอบเขตการดำเนินงาน -กำหนดโครงสร้างทีมงานและมอบหมายความรับผิดชอบ -กำหนดตัวชี้วัดและตั้งเป้าหมาย
D=Do	-ดำเนินกิจกรรมตามแผนงาน
C=Check	-ติดตามผลดำเนินงานและเทียบกับเป้าหมาย -สรุปผลการดำเนินงาน
A=Act	-วิเคราะห์ผลสำเร็จของงาน -นำเสนอผลงาน -วิเคราะห์ปัญหาเพื่อการปรับปรุง



ภาพที่ 3.1 วงจรคุณภาพ PDCA

จากภาพที่ 3.1 วงจรคุณภาพ PDCA โดยมีรายละเอียดดังนี้

1.1 การวางแผนการดำเนินงาน (Plan)

การวางแผนงานจากวัตถุประสงค์ และเป้าหมายที่ได้กำหนดขึ้น โดยมีขั้นตอนและรายละเอียดดังนี้

1.1.1 ศึกษาข้อมูลต่างๆ ที่เกี่ยวข้อง ได้แก่ เอกสาร ทฤษฎี โปรแกรม และงานวิจัย

1) มาตรฐานและเครื่องมือที่เกี่ยวข้องกับธรรมาภิบาลด้านไอที

(1) กรอบมาตรฐานโคบิต (Cobit)

(2) กรอบการดำเนินงานมาตรฐาน ISO/IEC 27001

(3) กรอบงานไอทิล (ITIL Framework)

(4) แนวคิดโคโซ (COSO)

2) โปรแกรม

(1) ไมโครซอฟท์แอคเซส

3) งานวิจัยที่เกี่ยวข้อง

1.1.2 ศึกษาและรวบรวมรายการการตรวจคุณภาพด้านสารสนเทศ**จากผู้ตรวจระบบสารสนเทศ ของบริษัท ดีลอยท์ ทู้ช โธมัทสุ** ซึ่งประกอบไปด้วย 8 ด้าน ได้แก่

1) การตั้งค่าระบบปฏิบัติการและระบบฐานข้อมูล เป็นการตรวจสอบการตั้งค่าหรือ configuration ต่างๆ เช่น การตั้งค่าและระยะเวลาการเก็บ Log การกำหนดรูปแบบรหัสผ่านระยะเวลาการเปลี่ยนรหัสผ่าน การกำหนดสิทธิการเข้าถึงการตั้งค่า ความปลอดภัยต่างๆ

ในการใช้งานระบบฐานข้อมูล เพื่อให้แน่ใจว่าระบบปฏิบัติการ และฐานข้อมูลได้รับการควบคุมตามกรอบมาตรฐานความปลอดภัย

2) นโยบายต่างๆ โครงสร้างแผนกและการควบคุมทั่วไปเป็นการตรวจสอบในส่วนของนโยบายต่างๆเช่น กฎระเบียบปฏิบัติในการควบคุมระบบความมั่นคงปลอดภัยทางด้านสารสนเทศและโครงสร้างของแผนกสารสนเทศ

3) หน้าที่ความรับผิดชอบและการปฏิบัติงานของแผนกสารสนเทศเป็นการตรวจสอบหน้าที่ความรับผิดชอบของเจ้าหน้าที่สารสนเทศรวมถึงขั้นตอนหรือกระบวนการทำงาน เช่น ขั้นตอนการร้องขอการสนับสนุนจากแผนกสารสนเทศในการแก้ปัญหาต่างๆ หรือการเพิ่มผู้ใช้งาน และ รหัสผ่าน ว่ามีขั้นตอนการร้องขออย่างไรมีการอนุมัติตามลำดับหรือไม่

4) ความมั่นคงปลอดภัยทางด้านกายภาพ เป็นการตรวจสอบการควบคุมความมั่นคงของระบบสารสนเทศทางกายภาพ เช่น การควบคุมการเข้า-ออก ห้อง Serve ว่ามีระเบียบการปฏิบัติหรือไม่ หรือ มีอุปกรณ์ในการควบคุมหรือไม่

5) ความมั่นคงปลอดภัยของข้อมูล เป็นการตรวจสอบการกำหนดสิทธิต่างๆของการเข้าถึงข้อมูลอย่างเหมาะสมของผู้ใช้งานรวมถึงสิทธิในการแก้ไขเปลี่ยนแปลงหรือลบข้อมูล

6) การควบคุมการปรับเปลี่ยนและแก้ไขระบบเพื่อตรวจสอบการควบคุมการเปลี่ยนแปลงที่เกิดขึ้นในระบบสารสนเทศว่ามีกระบวนการหรือขั้นตอนอย่างไรมีสายงานการอนุมัติหรือไม่

7) การควบคุมระบบโปรแกรมประยุกต์เป็นการตรวจสอบการตั้งค่าต่างๆ ในระบบโปรแกรมประยุกต์ว่าเหมาะสมตามสิทธิต่างๆ ของผู้ใช้งาน เช่นการให้สิทธิในการใช้งานการปฏิบัติงานในระบบโปรแกรมประยุกติ

8) การทดสอบความถูกต้องของข้อมูลในระบบ เป็นการตรวจข้อมูลระดับรายการ (Transaction) ในฐานข้อมูลว่าโปรแกรมประยุกต์มีการทำงานที่ถูกต้องตามมาตรฐานและเงื่อนไขตามที่ออกแบบไว้โดยสอดคล้องกับนโยบายบริษัทหรือไม่

1.1.3 ศึกษาเอกสารหลักฐานที่ใช้ในการควบคุมระบบสารสนเทศของบริษัทและข้อมูลต่างๆ ของแผนกสารสนเทศ

โดยมีเอกสารต่างๆ ดังตารางที่ 3.1

ตารางที่ 3.2 ตารางแสดงรายการการตรวจสอบคุณภาพของระบบสารสนเทศทั้ง 8 ด้าน 74 รายการ จากผู้ตรวจสอบด้านสารสนเทศ

ลำดับ	รายละเอียดการตรวจสอบทางด้านสารสนเทศ
1	Windows Operation system supporting Navision Application : ระบบปฏิบัติการที่สนับสนุนการทำงานของโปรแกรมประยุกต์ Navision
2	Windows Operation system supporting Domain Controller :ระบบปฏิบัติการที่สนับสนุนการทำงานขาดการควบคุมตรวจสอบการเข้าถึงระบบเครือข่าย
3	IT Organization Chart: ผังโครงสร้างแผนกสารสนเทศ
4	Network Diagram: โครงสร้างการเชื่อมโยงระบบเครือข่าย
5	IT Project Plan with status: แผนงานด้านสารสนเทศและสถานะโครงการ
6	IT Project Plan for Year Ending March 2017:แผนงานด้านสารสนเทศพร้อมสถานะปัจจุบัน
7	Information Security Policy Ref No.IT/001/2551: นโยบายความปลอกภัยทางสารสนเทศ
8	IT Backup Policy" as of January 2009 or currently: แผนการสำรองข้อมูล
9	IT Security / ID and Password Control" as of 01/07/2007 or currently: การควบคุมผู้ใช้งานและรหัสผ่าน
10	IT Security / Server Room Access Policy" as of 31/07/2013:นโยบายความปลอดภัยการเข้าถึงศูนย์คอมพิวเตอร์
11	IT Standard Regulation" as of 28/02/2008 or currently: ระเบียบปฏิบัติด้านสารสนเทศ
12	Access Log Review Procedure: กระบวนการตรวจสอบประวัติการเข้า ออกศูนย์คอมพิวเตอร์
13	Change Management Procedure: กระบวนการ การบริหารการเปลี่ยนแปลง
14	Screenshot: IT Policy on Intranet: นโยบายต่างๆ ด้านสารสนเทศใน Intranet ขององค์กร
15	Backup Restoration Procedure: ขั้นตอนการสำรองข้อมูล และการนำข้อมูลกลับมาใช้

ตารางที่ 3.2 (ต่อ)

ลำดับ	รายละเอียดการตรวจสอบทางด้านสารสนเทศ
16	ITR007 MSM IT Standard Regulation: V.3: กฎระเบียบมาตรฐานด้านสารสนเทศ
17	IT Backup Log of NAVISION application system: บันทึกการสำรองข้อมูลของระบบ Navision
18	Screenshot of backup tool showing schedule of backup of ERP: หน้าจอเครื่องมือที่ใช้ในการสำรองข้อมูล
19	Screen shot showing last update of job schedule on ERP: หน้าจอแสดงตารางการ Run Job อัตโนมัติ
20	Business Continuity Plan with sign-off by management: แผนต่อเนื่องทางธุรกิจที่อนุมัติแล้ว
21	Disaster Recovery Plan with sign-off by management: แผนสำรองด้านสารสนเทศที่อนุมัติแล้ว
22	BCP or DRP Testing Result with sign-off by management : ผลทดสอบแผนต่อเนื่องทางธุรกิจและแผนสำรองด้านสารสนเทศ
23	Backup Restoration Testing Result: ผลการทดสอบการสำรองข้อมูลและการเรียกกลับข้อมูล
24	Server Room Visitor Log Book: บันทึกการเข้าออกห้องคอมพิวเตอร์
25	List of authorised persons generated from fingerprint system.: รายชื่อผู้มีสิทธิในการเข้าศูนย์ข้อมูล ที่ออกมาจากระบบการเก็บลายนิ้วมือ
26	Request to add/change/delete access to server room.: ใบขอการเพิ่ม ปรับเปลี่ยน และลบในระบบการควบคุมการเข้าออกศูนย์คอมพิวเตอร์
27	Review of Server Room Visitor Log Book to present: ทบทวนและตรวจสอบการเข้าออกศูนย์คอมพิวเตอร์และนำเสนอต่อผู้ตรวจสอบ
28	Review validation and permission of access to server room to present.ทบทวนและตรวจสอบการเข้าออกศูนย์คอมพิวเตอร์และนำเสนอ

ตารางที่ 3.2 (ต่อ)

ลำดับ	รายละเอียดการตรวจสอบทางด้านสารสนเทศ
29-31	**Maintenance Report or request record of environment control in the server room.**
	a) Air Request record from General Affairs: เอกสารการซ่อมบำรุงเครื่องปรับอากาศในศูนย์คอมพิวเตอร์
	b) UPS Maintenance Report from vendor: เอกสารการซ่อมบำรุงเครื่องสำรองไฟฟ้าอากาศในศูนย์คอมพิวเตอร์
32	Sample of access log from finger scan system: ตัวอย่างข้อมูลการสแกนเข้า-ออกห้องคอมพิวเตอร์ ที่ออกมาจากระบบการเก็บลายนิ้วเมือ
33	List of current employees: รายชื่อพนักงานขององค์กร
34	List of transferred: รายชื่อโอนย้ายพนักงานระหว่างปี
35	List of resigned employees: รายชื่อพนักงานลาออกระหว่างปี
36-38	**List of user accounts with their properties: รายชื่อพนักงานพร้อมสิทธิการใช้งานระบบต่างๆ**
	a) NAVISION Application: สิทธิต่างๆ ในการใช้งานระบบ ERP Navision
	b) SQL Database supporting NAVISION Application: ระบบฐานข้อมูลระบบ Navision
39-41	**Screenshot of password configuration on the following systems: หน้าจอการตั้งค่ารหัสผ่านในระบบต่างๆดังนี้**
	a) NAVISION Application: ระบบ ERP Navison
	b) SQL Database supporting NAVISION Application **:** ระบบฐานข้อมูลของ ERP

ตารางที่ 3.2 (ต่อ)

ลำดับ	รายละเอียดการตรวจสอบทางด้านสารสนเทศ
42-46	**Review access log of the followings,ตรวจสอบประวัติการเข้าใช้งานของระบบต่างๆ ดังนี้**
	a) NAVISION Application:ระบบ ERP Navisioin
	b) SQL Database supporting NAVISION Application :ระบบฐานข้อมูลของ ERP
	c) Windows Operating System supporting NAVISION Application : ระบบปฏิบัติการสนับสนุนการทำงานของ ERP Navison
	d) Windows Operating System supporting Domain Controller : ระบบปฏิบัติการสนับสนุนการควบคุมโดเมน
47-51	**IT Request Form for add/change/delete user accounts from April 2015 to present: การร้องขอในเรื่องของการ เพิ่ม เปลี่ยนแปลง ลบ ข้อมูลผู้ใช้งานในระบบต่างๆ ดังนี้**
	a) NAVISION Application:ระบบ ERP Navisioin
	b) SQL Database supporting NAVISION Application :ระบบฐานข้อมูลของ ERP
	c) Windows Operating System supporting NAVISION Application : ระบบปฏิบัติการสนับสนุนการทำงานของ ERP Navison
	d) Windows Operating System supporting Domain Controller : ระบบปฏิบัติการสนับสนุนการควบคุมโดเมน
52-56	**Review validation and permission of user accounts from April 2015 to present**
	a) NAVISION Application:ระบบ ERP Navisioin
	b) SQL Database supporting NAVISION Application: ระบบฐานข้อมูลของ ERP
	c) Windows Operating System supporting NAVISION Application : ระบบปฏิบัติการสนับสนุนการทำงานของ ERP Navison
	d) Windows Operating System supporting Domain Controller: ระบบปฏิบัติการสนับสนุนการควบคุมโดเมน

ตารางที่ 3.2 (ต่อ)

ลำดับ	รายละเอียดการตรวจสอบทางด้านสารสนเทศ
57-62	**E-mail from HR informing employee movement :หลักฐานจดหมายอิเล็คทรอนิคจาก Sample of Access log or transaction log :ตัวอย่างประวัติการเข้าถึงระบบต่างๆ**
	a) NAVISION Application:ระบบ ERP Navisioin
	b)SQL Database supporting NAVISION Application:ระบบฐานข้อมูลของ ERP
	c) Windows Operating System supporting NAVISION Applicationระบบปฏิบัติการสนับสนุนการทำงานของ ERP Navision
	d) Windows Operating System supporting Domain Controller: ระบบปฏิบัติการสนับสนุนการควบคุมโดเมน
63	NAVISION Application User Matrix (last update with management sign-off): ตารางสิทธิต่างๆ ของผู้ใช้งานบนระบบ Navision พร้อมทั้งการอนุมัติจากผู้บริหาร
64	All document regarding to Navision Application change to present: เอกสารเกี่ยวกับการเปลี่ยนแปลงในโปรแกรมประยุกต์
65	All document regarding to system change (upgrade of operating system or database) to present ,such as the following-Quotation form Vendor- PO and quotation with approval – Network relocation design Moving schedule and announcement : เอกสารที่เกี่ยวข้องกับการเปลี่ยนแปลง อัพเกรดระบบปฏิบัติการหรือฐานข้อมูล เช่นใบเสนอราคาจากผู้ค้า ใบสั่งซื้อที่ได้รับการอนุมัติ
66	List of invoice numbers with following details -invoice number / invoice date / customer-invoice creator-amount-post date:ข้อมูลรายการใบกำกับภาษี ซึ่งประกอบไปด้วย เลขที่ใบกำกับภาษี / วันที่ /ผู้ใช้งานที่สร้างรายการ / วันที่ผ่านรายการ
67	Invoice Number series: ชุดเลขที่เอกสารใบกำกับภาษีในระบบ

ตารางที่ 3.2 (ต่อ)

ลำดับ	รายละเอียดการตรวจสอบทางด้านสารสนเทศ
68-74	a) GL Transaction Field required-Document Number – Documents type-GL Account Number –Account Name / Description-Transaction Detail /Description Amount Debit/ Amount Credit-Enter date –Posting date-Enterer. :ข้อมูลบัญชีแยกประเภท
	b) April – December :ข้อมูลบัญชีแยกประเภทของเดือน เมษายน ถึง ธันวาคม
	c) January - March: ข้อมูลบัญชีแยกประเภทของเดือนมกราคม ถึง มีนาคม
	d) Trial Balance(TB) generated from Navision: ข้อมูลงบทดลอง ที่ออกมาจากโปรแกรมประยุกต์
	e) End of March previous year :ข้อมูลงบทดลองเดือนมีนาคมปีที่แล้ว
	f) End of December previous year :ข้อมูลงบทดลองเดือนธันวาคมปีที่แล้ว
	g) End of March current year ข้อมูลงบทดลองเดือนมีนาคมปีปัจจุบัน

1.2 การปฏิบัติตามแผน (DO)

การปฏิบัติตามขั้นตอนในแผนงานที่ได้เขียนไว้อย่างเป็นระบบและมีความต่อเนื่อง โดยการพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุก โดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิต แบ่งกระบวนการทำงานหลักๆ ได้ดังนี้ 1. ออกแบบระบบตรวจสอบมาตรฐานระบบสารสนเทศ 2. พัฒนาระบบตรวจสอบมาตรฐานระบบสารสนเทศ

1.2.1 ออกแบบระบบตรวจสอบมาตรฐานระบบสารสนเทศ

1) การจัดแบ่งหัวข้อการตรวจสอบของผู้ตรวจสอบด้านระบบเทคโนโลยีสารสนเทศโดยทางผู้วิจัยได้ออกแบบระบบตรวจสอบสารสนเทศโดยอ้างอิงจากหัวข้อการตรวจสอบของผู้ตรวจสอบด้านระบบเทคโนโลยีสารสนเทศ ดังภาพที่ 3.2

	Request Document	Request Date	Responsibility
1. OS & DB Configuration Request			
1.01	Windows operating system supporting NAVISION Application	9-Feb-2016	Dumrong
1.02	Windows operating system supporting Domain Controller	9-Feb-2016	Dumrong
2. IT Policy, Organization and general control			
2.01	IT Organisation Chart	9-Feb-2016	Kawin
2.02	Network Diagram	9-Feb-2016	Dumrong
2.03	IT Project Plan for Year Ending March 2016 with status	9-Feb-2016	Kawin
2.04	IT Project Plan for Year Ending March 2017	9-Feb-2016	Kawin
2.05	"Information Security Policy Ref No.IT/001/2551"	9-Feb-2016	Kawin
2.06	"IT Backup Policy" as of January 2009 or currently	9-Feb-2016	Paisan
2.07	"IT Security / ID and Password Control" as of 01/07/2007 or currently	9-Feb-2016	Kawin
2.08	"IT Security / Server Room Access Policy" as of 31/07/2013	9-Feb-2016	Kawin
2.09	"IT Standard Regulation" as of 28/02/2008 or currently	9-Feb-2016	Kawin
2.10	Access Log Review Procedure	9-Feb-2016	Winit
2.11	Change Management Procedure	9-Feb-2016	Kawin
2.12	Screenshot: IT Policy on Intranet	9-Feb-2016	Dumrong
2.13	Bakcup Restoration Procedure	9-Feb-2016	Paisan
2.14	ITR007 MSM IT Standard Regulation V.3	9-Feb-2016	Kawin
3. IT Operation			
3.01	"IT Backup Log" of NAVISION application system * Selected Sample: 20 - 24 April 2015, 13 - 17 July 2015 and 18 - 22 January 2016	9-Feb-2016	Kawin
3.02	Screenshot of backup tool showing schedule of backup of NAVISION Application System	9-Feb-2016	Kawin
3.03	Screenshot showing last update of job schedule on NAVISION Application	9-Feb-2016	Kawin
3.04	Business Continuity Plan with sign-off by management	9-Feb-2016	Kawin
3.05	Disaster Recovery Plan with sign-off by management	9-Feb-2016	Kawin
3.06	BCP or DRP Testing Result with sign-ff by management	9-Feb-2016	Kawin
3.07	Backup Restoration Testing Result	9-Feb-2016	Kawin
4. Physical Security			
4.01	"Server Room Visitor Log Book" from April 2015 to present	9-Feb-2016	Paisan
4.02	List of authorised persons generated from fingerprint system	9-Feb-2016	Winit
4.03	Request to add/change/delete access to server room from April 2015 to present	9-Feb-2016	Winit
4.04	Review of Server Room Visitor Log Book from April 2014 to present	-	Winit
4.05	Review validation and permission of access to server room from April 2014 to present	9-Feb-2016	Winit
4.06	Maintenance Report or request record of environment control in the server room, from April 2015 to present	-	-
	a) Air, Request record from General Affirs	9-Feb-2016	GA/ Kawin

ภาพที่ 3.2 ตารางหัวข้อการตรวจสอบใน 8 ด้าน จากทางผู้ตรวจสอบระบบสารสนเทศในรูปแบบไฟล์เอ็กเซล

	Request Document	Request Date	Responsibility
5. Information Security			
5.01	List of **current employees**	9-Feb-2016	Kawin/HR
5.02	List of **transferred employees** from April 2014 to January 2015	9-Feb-2016	Kawin/HR
5.03	List of **resigned employees** from April 2014 to January 2015	9-Feb-2016	Kawin/HR
5.04	List of user accounts with their properties ** including description (owner's name), status, last login, role, password parameters, last password change (if any)*	-	Dumrong
	a) NAVISION Application	9-Feb-2016	Winit
	b) SQL Database supporting NAVISION Application	9-Feb-2016	Winit
5.05	Screenshot of password configuration on the following systems,	-	
	a) NAVISION Application	9-Feb-2016	Winit
	b) SQL Database supporting NAVISION Application	9-Feb-2016	Winit
5.06	Review access log of the followings, * Selected Sample: August 2015 and December 2015	-	Winit
	a) NAVISION Application	9-Feb-2016	Winit
	b) SQL Database supporting NAVISION Application	9-Feb-2016	Winit
	c) Windows Operating System supporting NAVISION Application	9-Feb-2016	Dumrong
	d) Windows Operating System supporting Domain Controller	9-Feb-2016	Dumrong
5.07	IT Request Form for add/change/delete user accounts from April 2015 to present	-	-
	a) NAVISION Application	9-Feb-2016	Paisan
	b) SQL Database supporting NAVISION Application	9-Feb-2016	Paisan
	c) Windows Operating System supporting NAVISION Application	9-Feb-2016	Paisan
	d) Windows Operating System supporting Domain Controller	9-Feb-2016	Paisan
5.08	Review validation and permission of user accounts from April 2015 to present	-	-
	a) NAVISION Application	9-Feb-2016	Winit
	b) SQL Database supporting NAVISION Application	9-Feb-2016	Winit
	c) Windows Operating System supporting NAVISION Application	9-Feb-2016	Dumrong
	d) Windows Operating System supporting Domain Controller	9-Feb-2016	Dumrong
5.09	E-mail from HR informing employee movement (new/transferr/resign) of August 2015 and December 2015	9-Feb-2016	Kawin/HR
5.10	Sample of Access log or transaction log on 1 April 2015	-	-
	a) NAVISION Application	9-Feb-2016	Winit
	b) SQL Database supporting NAVISION Application	9-Feb-2016	Winit
	c) Windows Operating System supporting NAVISION Application	9-Feb-2016	Dumrong
	d) Windows Operating System supporting Domain Controller	9-Feb-2016	Dumrong
5.11	NAVISION Application User Matrix (last update with management sign-off)	9-Feb-2016	Kawin

ภาพที่ 3.2 ตารางหัวข้อการตรวจสอบใน 8 ด้าน จากทางผู้ตรวจสอบระบบสารสนเทศในรูปแบบไฟล์เอ็กเซล (ต่อ)

	Request Document	Request Date	Responsibility
6. System Change Control			
6.01	All document regardings to **Navision Application Change** from April 2015 to present, such as the followings, - IT Request Form - Memo and Quotation approval - Service Log Sheet - ใบแจ้งหนี้ / ใบวางหนี้	9-Feb-2016	Kawin
6.02	All documenst regarding to **System Change (upgrade of Operating System or Database)** from April 2015 to present, such as the following - Quotation from vendor - PO and Quotation with approval - Network relocation design - Moving Schedule and annoucement - UAT with vendor	9-Feb-2016	Kawin
7. Application Control - NAVISION			
7.01	List of invoice numbers from 1 April 2015 to 31 January 2016 with the following details, - invoice number - invoice date - customer - invoice creator - amount - post date	9-Feb-2016	Kawin
7.02	Invoice No. Series	9-Feb-2016	
8. Journal Entry Testing			
8.01	GL transactions ***Field Required:*** - Document Number - Document Type - GL Account Number - Account Name / Description - Transaction Detail / Description - Amount Debit - Amount Credit - Entered Date - Posting Date - Enterer	-	Kawin

ภาพที่ 3.2 ตารางหัวข้อการตรวจสอบใน 8 ด้าน จากทางผู้ตรวจสอบระบบสารสนเทศ ในรูปแบบไฟล์เอ็กเซล (ต่อ)

จากภาพที่ 3.2 จะมีการจัดและแบ่งกลุ่มการตรวจสอบออกเป็น 2 ส่วน คือ

(1) แบ่งหัวข้อใหญ่เพื่อการตรวจสอบระบบสารสนเทศ 8 ด้าน โดยการนำหัวข้อมาจาก check List Requisition จากผู้ตรวจสอบระบบสารสนเทศดังนี้

ก) Operation system & Database Configuration Request (การขอตรวจสอบระบบปฏิบัติการ และระบบฐานข้อมูล)

ข) IT Policy Organization and general control (การควบคุมทั่วไปในด้านนโยบายด้านสารสนเทศ)

ค) IT Operation (การดำเนินงานต่างๆ ทางด้านสารสนเทศ)

ง) Physical Security (ความปลอดภัยทางกายภาพ)

จ) Information Security (ความปลอดภัยในด้านข้อมูล)

ฉ) System Change Control (การควบคุมการปรับเปลี่ยนระบบ)

ช) Application Control (การควบคุมการใช้งานโปรแกรมประยุกต์)

ซ) Journal Entry Testing (การทดสอบระบบการลงบันทึกบัญชี)

(2) แบ่งหัวข้อย่อยใน 8 หัวข้อใหญ่ในการตรวจสอบระบบสารสนเทศ โดยการนำหัวข้อมาจาก check List Requisition 74 หัวข้อย่อยจากตารางแสดงรายการการตรวจสอบคุณภาพของระบบสารสนเทศทั้ง 8 ด้าน 74 รายการ จากผู้ตรวจสอบด้านสารสนเทศ

2) ส่วนประกอบของระบบตรวจสอบมาตรฐานระบบสารสนเทศ

(1) ระบบความปลอดภัยในการเข้าใช้งาน

(2) ระบบการสร้างผู้ใช้งาน (User) และกลุ่ม (GROUP) การใช้งาน

(3) ระบบการกำหนดสิทธิการใช้งาน

(4) ระบบการบันทึกข้อมูล

(5) ระบบแสดงผลการวิเคราะห์สถานะมาตรฐานของระบบสารสนเทศ

(6) ระบบรายงานสถานะมาตรฐานของระบบสารสนเทศ

1.2.2 พัฒนาระบบตรวจสอบมาตรฐานระบบสารสนเทศ

มีรายละเอียดดังนี้

1) นำหัวข้อการตรวจสอบ 8 ด้านและหัวข้อย่อย 74 หัวข้อจากทางผู้ตรวจสอบระบบสารสนเทศในตารางไฟล์เอ็กเซลมาทำการบันทึกลงในระบบตรวจสอบมาตรฐานระบบสารสนเทศจากโปรแกรม Microsoft Accessดังตัวอย่างภาพที่ 3.3

ID	Group	Item	Description	objective	Linkdoc
1	1	1.01	Windows operating system supporting NAVISION Applica		
2	1	1.02	Windows operating system supporting Domain Controller		
3	2	2.01	IT Organisation Chart	To check the structure of IT Manpow	document\2.01 IT Organ
4	2	2.02	Network Diagram	To check the nework design	document\2.02 Network
5	2	2.03	IT Project Plan for Year Ending March 2016 with status	Auditor would like to check for the qu	document\2.03 IT Projec
6	2	2.04	IT Project Plan for Year Ending March 2017		document\2.04 IT Projec
7	2	2.05	"Information Security Policy Ref No.IT/001/2551"		document\2.05 Informati
8	2	2.06	"IT Backup Policy" as of January 2009 or currently		document\2.06 IT Backu
9	2	2.07	"IT Security / ID and Password Control" as of 01/07/2007 (		
10	2	2.08	"IT Security / Server Room Access Policy" as of 31/07/20		
11	2	2.09	"IT Standard Regulation" as of 28/02/2008 or currently		
12	2	2.1	Access Log Review Procedure		
13	2	2.11	Change Management Procedure		
14	2	2.12	Screenshot: IT Policy on Intranet		
15	2	2.13	Bakcup Restoration Procedure		
16	2	2.14	ITR007 MSM IT Standard Regulation V.3		
17	3	3.01	"IT Backup Log" of NAVISION application system		
18	3	3.02	Screenshot of backup tool showing schedule of backup of		
19	3	3.03	Screenshot showing last update of job schedule on NAVIS		
20	3	3.04	Business Continuity Plan with sign-off by management		
21	3	3.05	Disaster Recovery Plan with sign-off by management		
22	3	3.06	BCP or DRP Testing Result with sign-ff by management		
23	3	3.07	Backup Restoration Testing Result		
24	4	4.01	"Server Room Visitor Log Book" from April 2015 to presen		

STD	Evidence	checklist	indicator	auditorcommen	Period
	☐	☐	1		2016
	☐	☐	1		2016
	☑	☐	1		2016
	☑	☐	1		2016
	☑	☐	1		2016
	☑	☐	1		2016
	☑	☐	1		2016
	☑	☐	1		2016
	☐	☐	1		2016
	☐	☐	1		2016
	☐	☑	1		2016
	☐	☐	0		2016
	☐	☐	0		2016
	☐	☐	0		2016
	☐	☐	0		2016
	☐	☐	0		2016
	☐	☐			2016
	☐	☐			2016
	☐	☐			2016

ภาพที่ 3.3 หัวข้อการตรวจสอบ 8 ด้านและหัวข้อย่อย 74 หัวข้อ
ในระบบตรวจสอบมาตรฐานระบบสารสนเทศโดยโปรแกรม
Microsoft Access

2) ตั้งค่าสถานะต่างๆ ที่กำหนดไว้ในระบบ โดยมีรายละเอียดต่างๆ ได้แก่

(1) มาตรฐานทางด้านกรอบสารสนเทศ

(2) เอกสารหรือข้อมูลสนับสนุนการตรวจสอบตามภาพที่ 3.3 หัวข้อการตรวจสอบ 8 ด้านและหัวข้อย่อย 74 หัวข้อ ในระบบตรวจสอบมาตรฐานระบบสารสนเทศโดยโปรแกรม Microsoft Access

(3) สถานะต่างๆ ที่กำหนดไว้ในระบบตรวจสอบมาตรฐานระบบสารสนเทศประกอบไปด้วยดังภาพที่ 3.4

ก. Standard –ใช้อ้างอิงกรอบมาตรฐานทางด้านสารสนเทศว่าตรงกับหัวข้อใด

ข. Evidence check list –เป็นการเช็คว่าในแต่ละรายการการตรวจระบบสารสนเทศนั้นมีเอกสารหรือข้อมูลสนับสนุนหรือไม่

ค. Comment from Audit –สำหรับบันทึกความคิดเห็นจากผู้ตรวจสอบทางสารสนเทศของแต่ละรายการของการตรวจ เช่น ในเรื่องของการสำรองข้อมูล จะแน่ใจได้อย่างไรว่าคุณภาพการสำรองข้อมูลนั้นสามารถเรียกกลับมาใช้งานได้ 100% ทางผู้ตรวจสอบจึงแนะนำให้มีการ Verify ความถูกต้อง

(4) Document support - ในกรณีที่มีเอกสารหลักฐานหรือเอกสารสนับสนุนในแต่ละรายการการตรวจสอบแนบ สามารถเชื่อมโยงไปยังแหล่งเอกสารในรูปแบบของดิจิทัลไฟล์

(5) Status - เป็นการ update สถานะของรายการตรวจสอบว่าในแต่ละหัวข้อการตรวจสอบอยู่ในสถานะใด เช่น

ก. สถานะ A มีข้อมูล / เอกสาร /ระเบียบปฏิบัติ และปฏิบัติตาม อย่างเคร่งครัด

ข. สถานะ B มีระเบียบปฏิบัติ และปฏิบัติตาม อย่างเคร่งครัด แต่ไม่มีเอกสารหรือข้อมูลที่สนับสนุน

ค. สถานะ C ไม่มีข้อมูล / ไม่มีเอกสาร / ไม่มีระเบียบปฏิบัติ

ง. สถานะ D มีระเบียบปฏิบัติ แต่ไม่ปฏิบัติตาม

Group:	Item:	Description:	Evidence	checklist	Commer	Period:	indicatorx:	Linkdoc:
1	1.01	Windows operating system supporting NAVISION Application	☐	☐		2016	75	document
1	1.02	Windows operating system supporting Domain Controller	☐	☐		2016	50	document
2	2.01	IT Organisation Chart	☑	☐		2016	100	document
2	2.02	Network Diagram	☑	☐		2016	100	document
2	2.03	IT Project Plan for Year Ending March 2016 with status	☑	☐		2016	100	document
2	2.04	IT Project Plan for Year Ending March 2017	☑	☐		2016	100	document
2	2.05	"Information Security Policy Ref No.IT/001/2551"	☑	☐		2016	100	document
2	2.06	"IT Backup Policy" as of January 2009 or currently	☑	☐		2016	100	document
2	2.07	"IT Security / ID and Password Control" as of 01/07/2007 or currently	☐	☐		2016	75	document
2	2.08	"IT Security / Server Room Access Policy" as of 31/07/2013	☐	☐		2016	75	document
2	2.09	"IT Standard Regulation" as of 28/02/2008 or currently	☐	☑		2016	75	document
2	2.1	Access Log Review Procedure	☐	☑		2016	100	document
2	2.11	Change Management Procedure	☐	☐		2016	75	document
2	2.12	Screenshot: IT Policy on Intranet	☐	☐		2016	75	document
2	2.13	Bakcup Restoration Procedure	☐	☐		2016	50	document
2	2.14	ITR007 MSM IT Standard Regulation V.3	☐	☐		2016	75	document
3	3.01	"IT Backup Log" of NAVISION application system	☐	☐		2016	75	document
3	3.02	Screenshot of backup tool showing schedule of backup of NAVISION Ap	☐	☐		2016	75	document
3	3.03	Screenshot showing last update of job schedule on NAVISION Applicati	☐	☐		2016	75	document
3	3.04	Business Continuity Plan with sign-off by management	☐	☐		2016	75	document
3	3.05	Disaster Recovery Plan with sign-off by management	☐	☐		2016	75	document
3	3.06	BCP or DRP Testing Result with sign-ff by management	☐	☐		2016	75	document
3	3.07	Backup Restoration Testing Result	☐	☐		2016	75	document
4	4.01	"Server Room Visitor Log Book" from April 2015 to present	☐	☐		2016	75	document
4	4.02	List of authorised persons generated from fingerprint system	☐	☐		2016	75	document
4	4.03	Request to add/change/delete access to server room from April 2015 to	☐	☐		2016	75	document
4	4.04	Review of Server Room Visitor Log Book from April 2014 to present	☐	☐		2016	75	document
4	4.05	Review validation and permission of access to server room from April 20	☐	☐		2016	50	document
4	4.06	Maintenance Report or request record of environment control in the serv	☐	☐		2016	50	document
4		a) Air, Request record from General Affirs	☐	☐		2016	50	document
4		b) UPS, Maintenance Report from vendor	☐	☐		2016	50	document
4	4.07	Sample of Access log from finger scan system* Selected sample: 1 Apr	☐	☐		2016	75	document
5	5.01	List of current employees	☐	☐		2016	50	document
5	5.02	List of transferred employees from April 2014 to January 2015	☐	☐		2016	50	document
5	5.03	List of resigned employees from April 2014 to January 2015	☐	☐		2016	75	document
5	5.04	List of user accounts with their properties* including description (owner's	☐	☐		2016	50	document
5		a) NAVISION Application	☐	☐		2016	50	document
5		b) SQL Database supporting NAVISION Application	☐	☐		2016	75	document
5	5.05	Screenshot of password configuration on the following systems.	☐	☐		2016	75	document

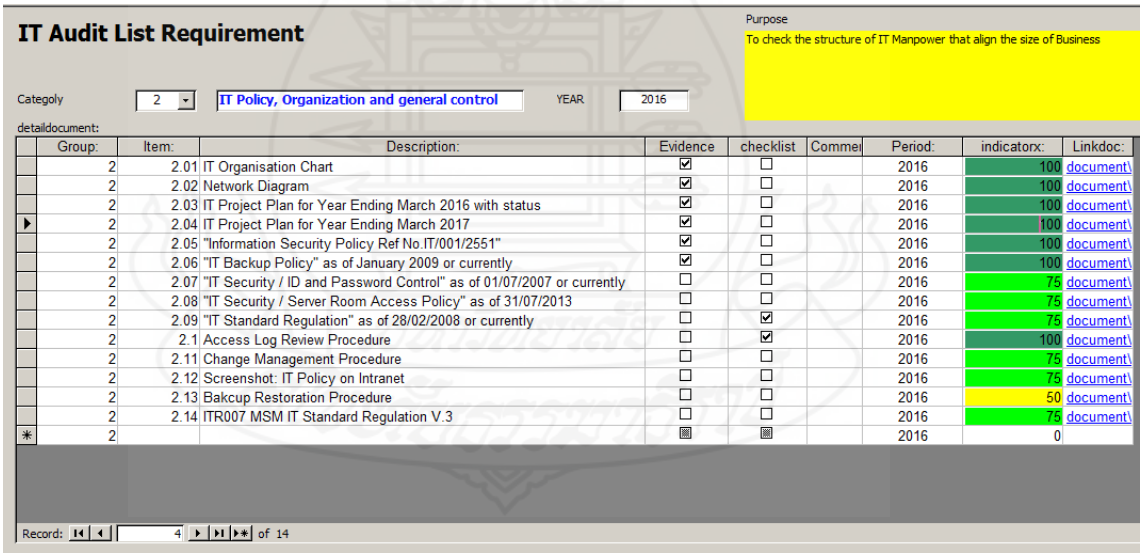
ภาพที่ 3.4 สถานะต่างๆ ที่กำหนดไว้ในระบบตรวจสอบมาตรฐานระบบสารสนเทศ โดยโปรแกรม Microsoft Access

3) ประเมินสถานะความพร้อมของระบบตรวจสอบมาตรฐานระบบสารสนเทศ หลังจากเสร็จสิ้นการตั้งค่าสถานะต่างๆ ที่กำหนดไว้ในระบบดังตารางที่ 3.3

ตางรางที่ 3.3 แสดงประเมินสถานะความพร้อมระบบตรวจสอบมาตรฐานระบบสารสนเทศ โดยโปรแกรม Microsoft Access

สถานะ	คำอธิบาย	คะแนน
A	มีข้อมูล / เอกสาร / ระเบียบปฏิบัติ และปฏิบัติตาม อย่างเคร่งครัด	100
B	มีระเบียบปฏิบัติ และปฏิบัติตาม อย่างเคร่งครัด แต่ไม่มีเอกสารหรือข้อมูลที่สนับสนุน	75
C	กำลังจัดเตรียมเอกสาร / กำลังจัดทำระเบียบปฏิบัติ	50
D	ไม่มีข้อมูล / ไม่มีเอกสาร / ไม่มีระเบียบปฏิบัติ	25
F	มีระเบียบปฏิบัติ แต่ไม่ปฏิบัติตาม	0

4) ทำการออกแบบหน้าจอสำหรับการบันทึกข้อมูลเข้าสู่ระบบตรวจสอบตรวจสอบมาตรฐานระบบสารสนเทศ โดยมีการออกแบบเพื่อให้สะดวกต่อการใช้งานและเข้าใจได้ง่าย เพื่อให้ตรงตามความต้องการของผู้ตรวจสอบด้านระบบดังภาพที่ 3.5



ภาพที่ 3.5 หน้าจอสำหรับการบันทึกข้อมูลเข้าสู่ระบบตรวจสอบมาตรฐานระบบสารสนเทศ โดยโปรแกรม Microsoft Access

5) ทำการออกแบบฐานข้อมูล ผู้วิจัยได้ออกแบบตาราง (Table) ต่างๆ ที่มีความสัมพันธ์ในลักษณะ RDBMS (Relational Database Management System) ในโปรแกรม Microsoft Access โดยมีรายละเอียดดังตารางที่ 3.4– 3.7

ตารางที่ 3.4 ตารางหัวข้อหลักในการตรวจสอบด้านต่างๆ ของระบบสารสนเทศ

Table: Maintopic		
Attribute Name	Type	Description
MainNo	INT	ลำดับหัวข้อการตรวจด้านต่างๆ ของการตรวจสอบระบบสารสนเทศ
MainTopic	TEXT	รายการการตรวจด้านต่างๆ ของการตรวจสอบระบบสารสนเทศ

ตารางที่ 3.5 ตารางเอกสารและข้อมูลที่ทางผู้ตรวจสอบต้องการ

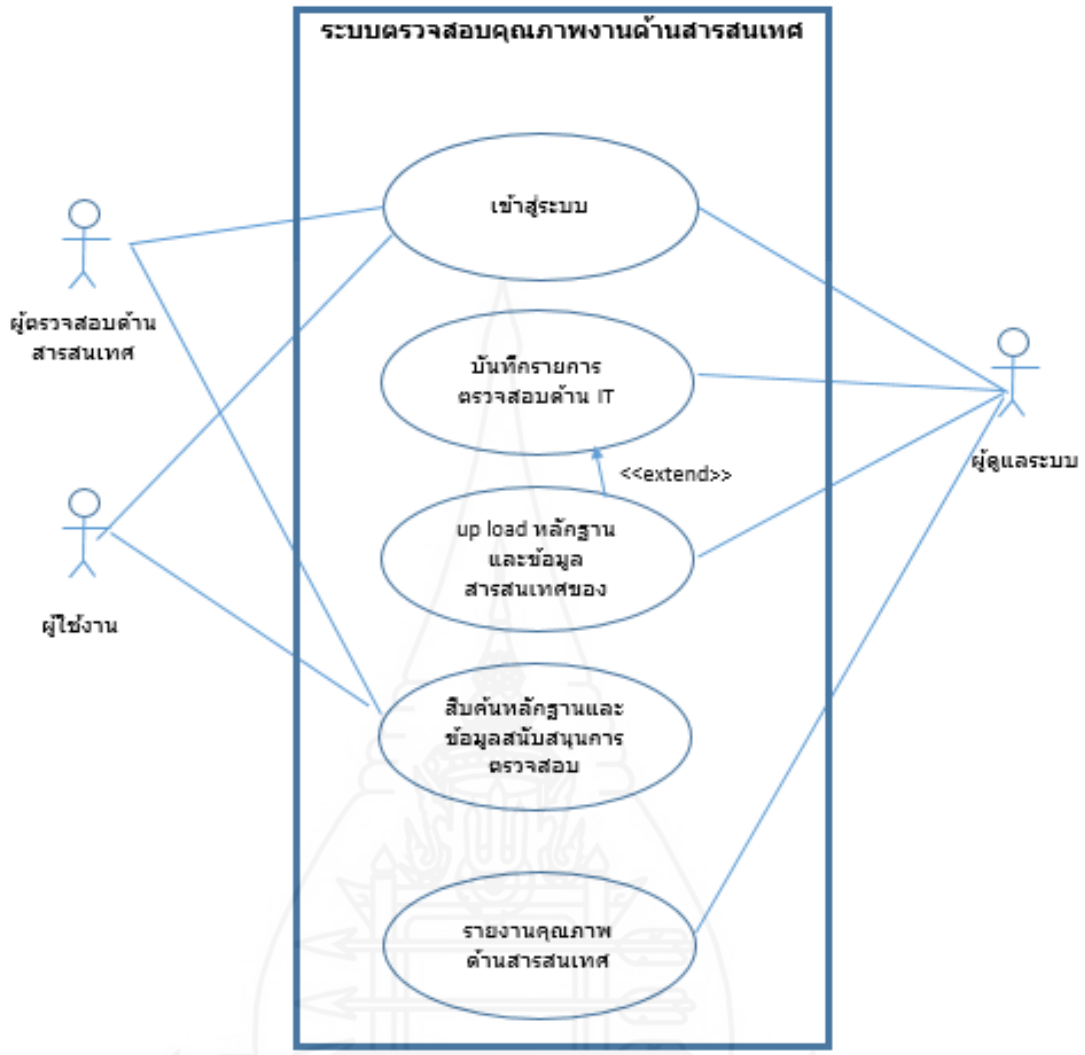
Table: Document List		
Attribute Name	Type	Description
Group	INT	มาตรฐานด้านต่างๆ ของระบบสารสนเทศ
Item	INT	รายการลำดับที่
Description	TEXT	คำอธิบายรายการ
Objective	TEXT	วัตถุประสงค์ของการตรวจรายการ
STD	TEXT	เข้ากับมาตรฐานใดในกรอบมาตรฐาน
Evidence	Boolean	หลักฐานหรือข้อมูลที่สนับสนุน
Checklist	Boolean	เป็นเช็คสถานะว่ามีหรือไม่มีหลักฐานหรือข้อมูลที่สนับสนุน
Indicator	INT	คะแนนประเมิน
Auditorcomment	TEXT	ข้อเสนอแนะของผู้ตรวจสอบ
Linkdoc	Object	เชื่อมโยงไปหลักฐานหรือข้อมูลที่สนับสนุน
Period	INT	ปีที่ตรวจสอบระบบสารสนเทศ

ตารางที่ 3.6 ตารางสถานะคุณภาพ

Table: Score		
Attribute Name	Type	Description
StatusID	INT	ลำดับหัวข้อสถานะ
Score	INT	คะแนนที่ได้รับจากความมีคุณภาพ
Description	TEXT	รายละเอียดคำอธิบายคะแนนคุณภาพ

ตารางที่ 3.7 ตารางผู้ใช้งาน

Table: User		
Attribute Name	Type	Description
ID	INT	รหัสสมาชิก
Username	Varcha	ชื่อผู้ใช้
Password	Varcha	รหัสผ่าน
USERTYPE	INT	รหัสประเภทผู้ใช้งาน
Userstatus	INT	สถานะของผู้ใช้งาน (Active,Non Active)



ภาพที่ 3.6 Use Case ระบบตรวจสอบและควบคุมคุณภาพงานไอที

6) ทำการพัฒนาระบบตรวจสอบมาตรฐานระบบสารสนเทศ เพื่อรองรับการใช้งานต่างๆ ดังนี้

(1) ระบบความปลอดภัยในการเข้าใช้งานเพื่อควบคุมการเข้าถึงระบบตรวจสอบและควบคุมคุณภาพงานไอทีป้องกันมิให้ผู้ที่ไม่มีสิทธิสามารถเข้าไปใช้งานในระบบ

(2) ระบบการสร้างผู้ใช้งาน (User) และกลุ่ม (GROUP) การใช้งานเพื่อการกำหนดผู้ใช้งาน (User) ที่สามารถเข้าใช้ระบบและกลุ่มผู้ใช้งาน (Groups)

(3) ระบบการกำหนดสิทธิการใช้งานเพื่อเป็นการกำหนดระดับสิทธิของการใช้งานระบบ

(4) ระบบการจัดการและบันทึกข้อมูลเพื่อการจัดการและบันทึกข้อมูล โดยสามารถแก้ไขเปลี่ยนแปลง ตามสิทธิการใช้งาน

(5) ระบบแสดงผลการวิเคราะห์สถานะมาตรฐานของระบบสารสนเทศ โดยแสดงคุณภาพในด้านต่างๆ 8 ด้านแสดงออกมาในรูปของกราฟแท่ง

(6) ระบบรายงานสถานะมาตรฐานของระบบสารสนเทศ เป็นการรายงานคุณภาพด้านสารสนเทศขององค์กรเพื่อให้ผู้บริหารรับทราบ

1.3 การตรวจสอบ (CHECK)

การตรวจสอบผลการดำเนินงานในแต่ละขั้นตอนของแผนงานว่าเกิดปัญหาหรืออุปสรรคใดเกิดขึ้น จำเป็นต้องเปลี่ยนแปลงแก้ไขหรือไม่ ซึ่งเมื่อมีการกำหนดขั้นตอนการทำงานบนระบบตรวจสอบมาตรฐานระบบสารสนเทศแล้วเสร็จ จึงควรมีการทดสอบการทำงานของระบบตรวจสอบมาตรฐานระบบสารสนเทศ โดยมีรายละเอียดต่างๆ ดังนี้

1.3.1 ทดสอบระบบความปลอดภัย

เป็นการทดสอบเมื่อเริ่มต้นการเข้าสู่โปรแกรมระบบมีการแสดงหน้าจอให้มีการใส่ชื่อผู้ใช้งานและรหัสผ่านหรือไม่

1) ทดสอบเรียกการใช้งาน โดยไม่ต้องใส่ User และ Passwordแล้วระบบยอมให้ผ่านสามารถเข้าไปใช้งานได้แสดงว่าไม่ผ่านการทดสอบ

2) ทดสอบโดยการใส่ User และไม่ใส่ Password ถ้าระบบยอมให้ผ่านสามารถเข้าไปใช้งานได้แสดงว่าไม่ผ่านการทดสอบ

3) ทดสอบโดยการใส่ User และใส่ Password ที่ไม่ถูกต้องถ้าระบบยอมให้ผ่านสามารถเข้าไปใช้งานได้แสดงว่าไม่ผ่านการทดสอบ

4) ทดสอบโดยการใส่ User และใส่ Password ที่ถูกต้องถ้าระบบยอมให้ผ่านสามารถเข้าไปใช้งานได้แสดงว่าผ่านการทดสอบ

1.3.2 ทดสอบสิทธิการใช้งาน เป็นการทดสอบการกำหนดสิทธิต่างๆ

ในการใช้งานให้เป็นไปตามกำหนด โดยมีการกำหนดกลุ่มการใช้งานขึ้นมา 2 กลุ่ม คือ 1. กลุ่ม “Admin” 2. กลุ่ม “General user” โดยมีรายละเอียดดังตารางที่ 3.8 – 3.9

ตารางที่ 3.8 กลุ่ม “Admin” สามารถกำหนดสิทธิการทดสอบ

Admin \ สิทธิ	ดู	เปลี่ยนแปลง	เพิ่ม	ลบ
การใช้งาน	x	x	x	x
หน้าจอการตั้งค่าผู้ใช้งาน	x	x	x	x
หน้าจอการตั้งกลุ่มผู้ใช้งาน	x	x	x	x
หน้าจอการใช้งานระบบ	x	x	x	x
หน้าจอการประเมินผล	x	x	x	x

ตารางที่ 3.9 กลุ่ม “General user” สามารถกำหนดสิทธิการทดสอบ

General User \ สิทธิ	ดู	เปลี่ยนแปลง	เพิ่ม	ลบ
การใช้งาน	x	x	x	x
หน้าจอการตั้งค่าผู้ใช้งาน				
หน้าจอการตั้งกลุ่มผู้ใช้งาน				
หน้าจอการใช้งานระบบ	x			
หน้าจอการประเมินผล	x			

จากตารางที่ 3.8-3.9 สามารถอธิบายรายละเอียดเพิ่มเติมได้ดังนี้

1) กำหนดกลุ่มการใช้งานขึ้นมา 2 กลุ่ม

(1) กลุ่ม “Admin”

ก. สามารถทำการเข้าถึงข้อมูล

ข. สามารถทำการ บันทึก แก้ไข ลบ ข้อมูลในระบบได้

ค. สามารถกำหนดสิทธิการใช้งานในระบบ

(2) กลุ่ม “General user”

ก. สามารถเข้าถึงข้อมูลแต่ใช้งานได้แค่ดูอย่างเดียว

ข. ไม่สามารถทำการ บันทึก แก้ไข ลบ ข้อมูลในระบบได้

2) ทดลองสร้างผู้ใช้งานโดยแบ่งตามกลุ่มการใช้งาน

(1) กลุ่ม “Admin”

ก. ตั้งชื่อ User1 และกำหนด รหัสผ่าน

(2) กลุ่ม “General user”

ก. ตั้งชื่อ User2 และกำหนด รหัสผ่าน

3) ทดสอบการใช้งานของผู้ใช้งานโดยแบ่งตามกลุ่มการใช้งาน

(1) กลุ่ม “Admin”

ก. User1 ทำการ Login เข้าสู่ระบบ

ข. ถ้าสามารถเพิ่มเติม แก้ไข ลบ ข้อมูลได้แสดงว่าผ่านการทดสอบ

ค. ถ้าไม่สามารถเพิ่มเติม แก้ไข ลบ ข้อมูลได้แสดงว่าไม่ผ่านการทดสอบ

(2) กลุ่ม “General user”

ก. User2 ทำการ Login เข้าสู่ระบบ

ข. สามารถดูข้อมูลได้อย่างเดียวไม่สามารถเพิ่มเติม แก้ไข ลบข้อมูลได้แสดงว่าผ่านการทดสอบ

ค. ถ้าสามารถไม่ดูข้อมูลได้อย่างเดียว สามารถเพิ่มเติม แก้ไข ลบข้อมูลได้แสดงว่าไม่ผ่านการทดสอบ

4) ทดสอบการใช้งานของระบบตรวจสอบมาตรฐานสารสนเทศของผู้ใช้งาน โดยแบ่งตามกลุ่มการใช้งาน

1.4 การปรับปรุงการดำเนินการอย่างเหมาะสม (ACT)

การปรับปรุงแก้ไขส่วนที่มีปัญหา หรือถ้าไม่มีปัญหาใดๆ ก็ยอมรับแนวทางการปฏิบัติตามแผนงานที่ได้ผลสำเร็จ เพื่อนำไปใช้ในการทำงานครั้งต่อไปเช่นความเหมาะสมในการให้คะแนนการประเมินมาตรฐาน หรือ ปรับปรุงหน้าจอ การบันทึกข้อมูลลงระบบ

2. อุปกรณ์และเครื่องมือที่ใช้ในการวิจัย

2.1 อุปกรณ์ฮาร์ดแวร์ที่จะนำมาใช้

2.1.1 เครื่องคอมพิวเตอร์โน้ตบุ๊ค

1) หน่วยประมวลผล intel core2 Duo

2) หน่วยความจำ 2 GB

3) จอภาพ 15 นิ้ว

4) พื้นที่ในการจัดเก็บข้อมูล 500 GB

2.2ซอฟต์แวร์ที่จะนำมาใช้

2.2.1 ระบบปฏิบัติการ Windows 7 Professional 32bit

2.2.2 โปรแกรม Microsoft Access

บทที่ 4
ผลการวิเคราะห์ข้อมูล

จากการศึกษาการพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิตผู้วิจัยได้ดำเนินการวิจัยประยุกต์ใช้แนวคิด PDCA หรือวงจรเดมิงซึ่งเป็นวงจรการควบคุมคุณภาพมาเป็นแนวทางในการพัฒนาระบบจนสามารถพัฒนาระบบที่สร้างขึ้นให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้คือ 1. พัฒนาระบบธรรมาภิบาลด้านสารสนเทศ 2. สร้างต้นแบบระบบและควบคุมภาพงานสารสนเทศ 3. ปรับปรุงการเตรียมความพร้อมในการตรวจสอบระบบสารสนเทศจากผู้ตรวจสอบทางด้านเทคโนโลยีสารสนเทศ ได้ผลดังนี้

1. ผลลัพธ์ของการออกแบบและพัฒนาระบบ
2. ผลลัพธ์ของการประเมินประสิทธิภาพของระบบ

1. ผลลัพธ์ของการออกแบบและพัฒนาระบบ

จากการออกแบบและพัฒนาระบบ มีส่วนประกอบของโปรแกรมเพื่อรองรับการใช้งานต่างๆ ของระบบดังนี้

1.1 ระบบความปลอดภัยในการเข้าใช้งาน

1.2 ระบบการสร้างผู้ใช้งาน (User) และกลุ่ม (GROUP) การใช้งาน

1.3 ระบบการกำหนดสิทธิการใช้งาน

1.4 ระบบการจัดการและบันทึกข้อมูล

1.5 ระบบแสดงผลการวิเคราะห์สถานะมาตรฐานของระบบสารสนเทศ

1.6 ระบบรายงานสถานะมาตรฐานของระบบสารสนเทศ

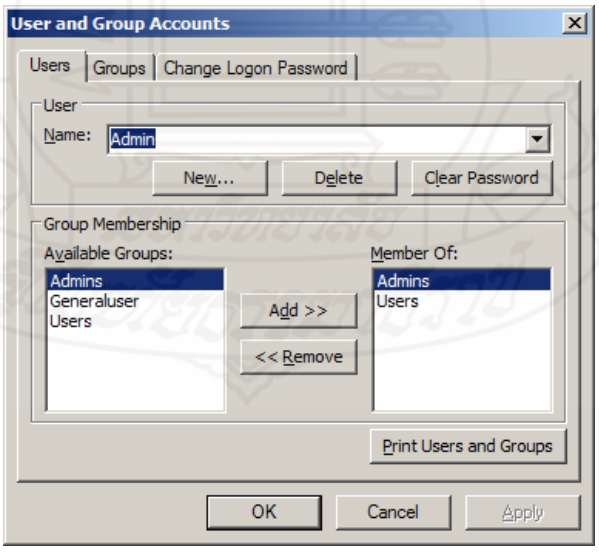
1.1 ระบบความปลอดภัยในการเข้าใช้งาน

เพื่อเป็นการควบคุมการเข้าถึงระบบตรวจสอบและควบคุมคุณภาพงานไอที ป้องกันมิให้ผู้ที่ไม่มีสิทธิสามารถเข้าไปใช้งานในระบบทำการเปลี่ยนแปลงหรือลบข้อมูล เพิ่มความปลอดภัยในการใช้งานของระบบและป้องกันความเสียหายของข้อมูลโดยเมื่อทำการเรียกใช้งานระบบจะแสดงหน้าจอที่ต้องใส่ ชื่อผู้ใช้งานและรหัสผ่านตามสิทธิที่ได้ถูกกำหนดไว้ (ซึ่งมีอยู่ในฐานข้อมูลตาราง USERLOGIN) ดังภาพที่ 4.1

ภาพที่ 4.1 แสดงหน้าจอ login ชื่อผู้ใช้และรหัสผ่าน

1.2 ระบบการสร้างผู้ใช้งาน (User) และกลุ่ม (GROUP) การใช้งาน

เพื่อเป็นการกำหนดผู้ใช้งาน (User) ที่สามารถเข้าใช้ระบบและกลุ่มผู้ใช้งาน (Groups) โดยมีฟังชั่นงานต่างๆ ดังตัวอย่างภาพที่ 4.2 - 4.5



ภาพที่ 4.2 แสดงหน้าจอการสร้างผู้ใช้งาน (User) และกลุ่ม (GROUP) การใช้งาน

จากภาพที่ 4.2 แสดงหน้าจอการสร้างผู้ใช้งาน (User) และกลุ่ม (GROUP) การใช้งาน ซึ่งมี 3 แถบการทำงาน โดยมีรายละเอียดดังนี้

1.2.1 แถบการทำงาน Users

1) User เป็นส่วนที่แสดงชื่อผู้ใช้งาน

(1) Name :รายชื่อผู้ใช้งานทั้งหมดในระบบที่มีสิทธิเข้าใช้งาน

(2) New :เพื่อต้องการสร้างหรือเพิ่ม ผู้ใช้งานที่ต้องการจะใช้งานในระบบ

(3) Delete :เป็นการลบผู้ใช้งานในกรณีที่ๆ ไม่ต้องการให้เข้าระบบ

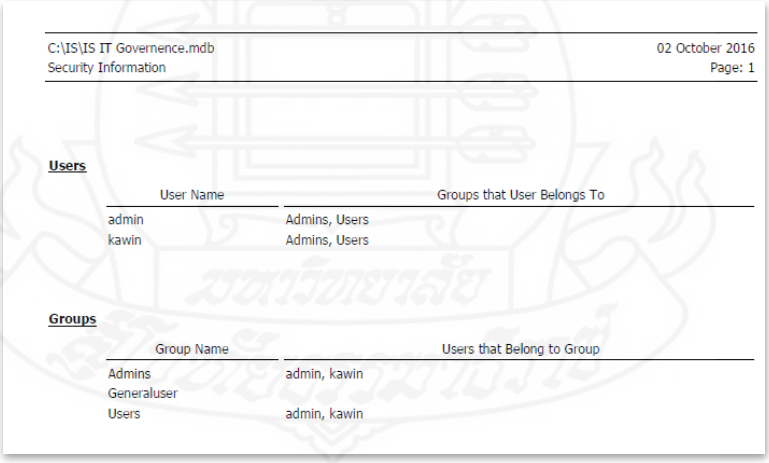
(4) Clear Password : ใช้เพื่อล้างรหัสผ่านในกรณีต้องการเปลี่ยนรหัสผ่าน

2) Group Membership ส่วนแสดงกลุ่มการใช้งานต่างๆ ที่อยู่ในระบบ ซึ่งสามารถเพิ่ม (Add) ลด (Remove) เพื่อเพิ่มหรือลดผู้ใช้งานในแต่ละกลุ่มมีรายละเอียดดังนี้

(1) Available Groupsคือกลุ่มต่างๆ ที่มีอยู่ในระบบซึ่งในแต่ละกลุ่มจะถูกกำหนดสิทธิการใช้งานที่ต่างกันออกไป

(2) Member ofคือผู้ใช้งานที่อยู่ในแต่ละกลุ่มต่างๆ

3) Print Users and Groups เพื่อพิมพ์เพื่อแสดงรายละเอียด รายชื่อผู้ใช้งาน (User) และกลุ่มการใช้งาน (Group) ทั้งหมดที่มีอยู่ในระบบแสดงดังตัวอย่างภาพที่ 4.3



C:\IS\IS IT Governence.mdb — 02 October 2016
Security Information — Page: 1

Users

User Name	Groups that User Belongs To
admin	Admins, Users
kawin	Admins, Users

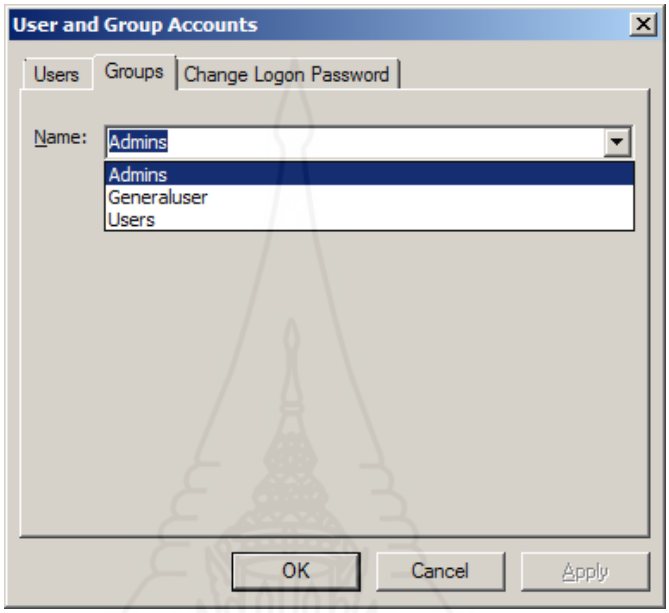
Groups

Group Name	Users that Belong to Group
Admins	admin, kawin
Generaluser	
Users	admin, kawin

ภาพที่ 4.3 แสดงตัวอย่างการสั่งพิมพ์รายชื่อผู้ใช้งาน (User) และกลุ่มการใช้งาน (Group)

1.2.2 แถบการทำงาน Groups

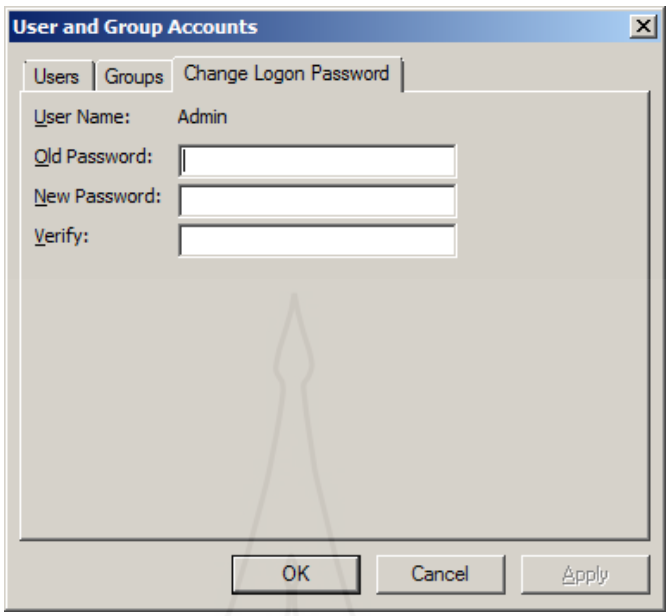
แสดงกลุ่มการใช้งานที่มีอยู่ในระบบคือ 1. Admins 2. Generaluser 3. Users ดังตัวอย่างภาพที่ 4.4



ภาพที่ 4.4 แสดงแถบการทำงาน Groups

1.2.3 แถบการทำงาน Change Logon Password

เพื่อการเปลี่ยนรหัสผ่านของการเข้าสู่ระบบ โดยเมื่อผู้ใช้งานต้องการเปลี่ยนแปลงรหัสผ่าน ระบบจะให้ผู้ใช้งานใส่รหัสผ่านเดิมก่อนถ้ารหัสผ่านเดิมถูกต้องระบบจะให้ใส่รหัสผ่านใหม่ที่ช่อง New Password และต้องพิมพ์รหัสผ่านใหม่อีกครั้งที่ช่อง Verify: เพื่อเป็นการเปรียบเทียบรหัสผ่านใหม่ อีกครั้งว่ารหัสผ่านใหม่ตรงกัน ดังตัวอย่างภาพที่ 4.5



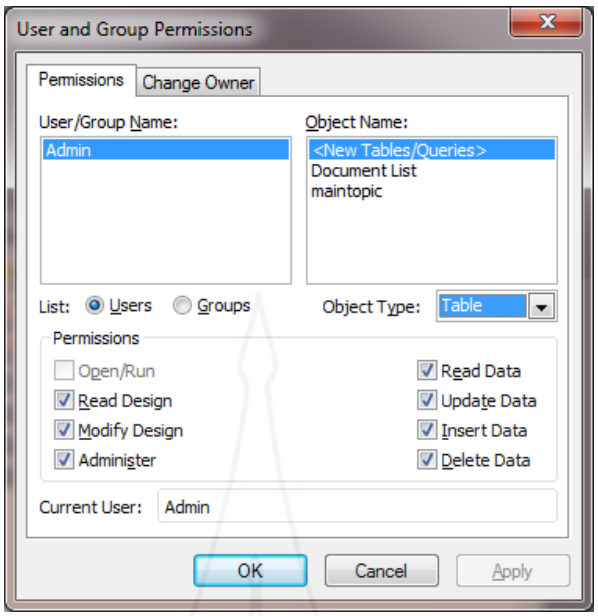
ภาพที่ 4.5 แถบการทำงาน Change Logon Password

1.3 ระบบการกำหนดกลุ่มสิทธิการใช้งาน (User and Group Permissions)

เพื่อการกำหนดระดับสิทธิของการใช้งานระบบว่าในแต่ละส่วนของระบบนั้นผู้ใช้งานสามารถเข้าถึงข้อมูล บันทึก แก้ไข เปลี่ยนแปลง ลบ เป็นการป้องกันความปลอดภัยของข้อมูลโดยมีคำสั่งในการกำหนดสิทธิของการใช้งาน โดยมีรายละเอียดดังภาพที่ 4.6 - 4.7 ดังนี้

1.3.1 แถบการทำงาน Permissions

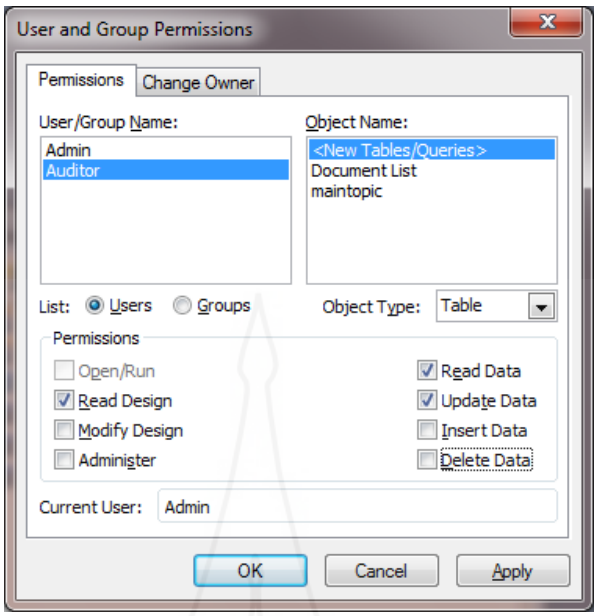
เป็นการกำหนดกลุ่มที่มีความสัมพันธ์กันกับ Object ทั้งในส่วนตารางการเก็บข้อมูล (Table) รายงาน (Report) หน้าจอใช้งาน (FORM) และแบบสอบถาม (Query) เพื่อเป็นการกำหนดสิทธิในการใช้งาน ในรูปด้านล่างเป็นการแสดงสิทธิการใช้งานของตารางข้อมูลตามนี้ดังตัวอย่างภาพที่ 4.6



ภาพที่ 4.6 รูปแสดงหน้าจอการกำหนดสิทธิในการใช้งานระบบของ Admin

จากภาพที่ 4.6 แสดงหน้าจอการกำหนดสิทธิในการใช้งานระบบของ Admin ซึ่งมีสิทธิดังนี้

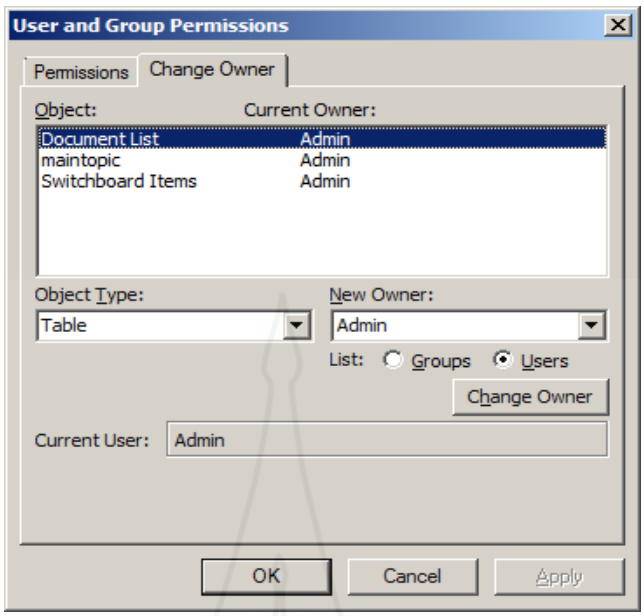
1) สิทธิในการเห็นข้อมูล (Read Data)
2) มีสิทธิในการแก้ไขเปลี่ยนแปลงข้อมูล (Update Data)
3) มีสิทธิในการบันทึกเพิ่มข้อมูล (Insert Data)
4) มีสิทธิในการลบข้อมูล (Insert Data)



ภาพที่ 4.7 รูปแสดงหน้าจอการกำหนดสิทธิในการใช้งานระบบของ Auditor

จากภาพที่ 4.7 แสดงหน้าจอการกำหนดสิทธิในการใช้งานระบบของ Auditor ซึ่งมีสิทธิดังนี้

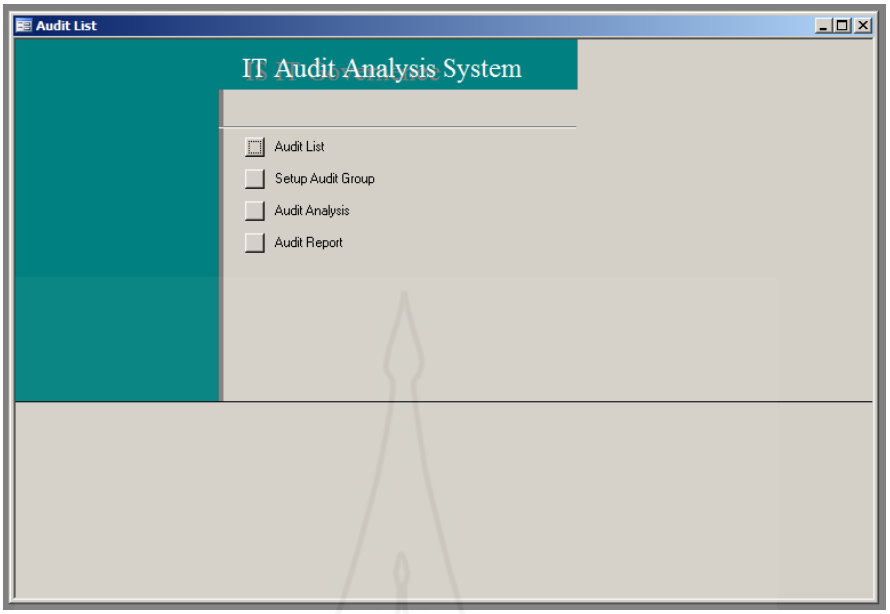
1) สิทธิในการเห็นข้อมูล (Read Data)
2) มีสิทธิในการแก้ไขเปลี่ยนแปลงข้อมูล (Update Data)
3) ไม่มีสิทธิในการบันทึกเพิ่มข้อมูล (Insert Data)
4) ไม่มีสิทธิในการลบข้อมูล (Insert Data)



ภาพที่ 4.8 รูปแสดงหน้าจอการเปลี่ยนแปลงสิทธิการใช้งาน

1.4 ระบบการจัดการและบันทึกข้อมูล

เพื่อการจัดการและบันทึกข้อมูล โดยสามารถแก้ไขเปลี่ยนแปลง ตามสิทธิการใช้งาน เป็นการนำข้อมูลการตรวจระบบสารสนเทศเข้าสู่ระบบฐานข้อมูล และทำการ update สถานะของหัวข้อการตรวจสอบตามรายการที่ผู้ตรวจสอบด้านสารสนเทศร้องขอมา เพื่อนำข้อมูลที่ทำการ update สถานะต่างๆ นั้นมาทำการวิเคราะห์ถึง คุณภาพงานไอทีตามหลักธรรมาภิบาล โดยมีรายละเอียดดังนี้



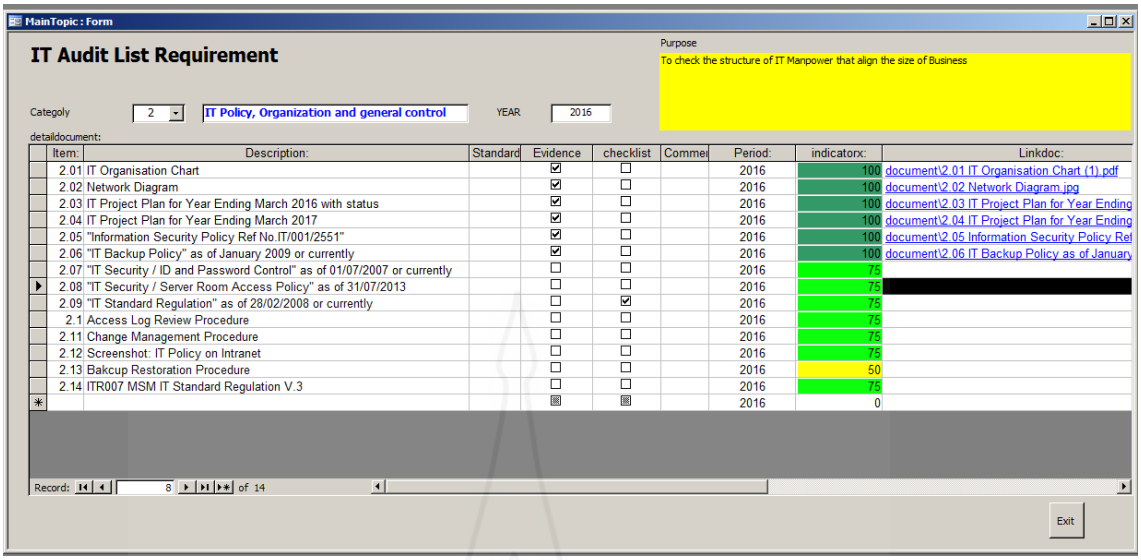
ภาพที่ 4.9 แสดงหน้าจอการใช้งานระบบตรวจสอบและควบคุมคุณภาพงานไอที

1.4.1 Audit List

เพื่อใช้ในการจัดการและบันทึกรายการ การตรวจสอบทางด้านสารสนเทศจากผู้ตรวจสอบ (IT Auditor) โดยข้อมูลจะได้มาในรูปแบบ File Excel ซึ่งประกอบไปด้วยหัวข้อหลักในการตรวจ และรายละเอียดที่จะทำการตรวจดังแสดงในตัวอย่างภาพที่ 4.9 – 4.11

	Request Document	Frequency	No. of sample	Request Date	Responsibility	Received Date	Status	Remarks
1. OS & DB Configuration Request								
1.01	Windows operating system supporting NAVISION Application	-	-	9-Feb-2016	Dumrong			Refer to "MAT_2_YE2016_Windows Configuration.doc"
1.02	Windows operating system supporting Domain Controller	-	-	9-Feb-2016	Dumrong			Refer to "MAT_2_YE2016_Windows Configuration.doc"
2. IT Policy, Organization and gene								
2.01	IT Organisation Chart	-	-	9-Feb-2016	Kawin			
2.02	Network Diagram	-	-	9-Feb-2016	Dumrong			
2.03	IT Project Plan for Year	-	-	9-Feb-2016	Kawin			
2.04	IT Project Plan for Year	-	-	9-Feb-2016	Kawin			
2.05	"Information Security Policy	-	-	9-Feb-2016	Kawin			
2.06	"IT Backup Policy" as of	-	-	9-Feb-2016	Paisan			
2.07	"IT Security / ID and Password Control" as of 01/07/2007 or	-	-	9-Feb-2016	Kawin			
2.08	"IT Security / Server Room	-	-	9-Feb-2016	Kawin			
2.09	"IT Standard Regulation" as of	-	-	9-Feb-2016	Kawin			
2.10	Access Log Review Procedure	-	-	9-Feb-2016	Winit			
2.11	Change Management	-	-	9-Feb-2016	Kawin			
2.12	Screenshot: IT Policy on	-	-	9-Feb-2016	Dumrong			
2.13	Bakcup Restoration Procedure	-	-	9-Feb-2016	Paisan			
2.14	ITR007 MSM IT Standard	-	-	9-Feb-2016	Kawin			
3. IT Operation								
3.01	"IT Backup Log" of NAVISION application system * Selected Sample: 20 - 24	daily	15 samples	9-Feb-2016	Kawin			
3.02	Screenshot of backup tool showing schedule of backup of	-	-	9-Feb-2016	Kawin			
3.03	Screenshot showing last update of job schedule on	-	-	9-Feb-2016	Kawin			
3.04	Business Continuity Plan with	-	-	9-Feb-2016	Kawin			
3.05	Disaster Recovery Plan with	-	-	9-Feb-2016	Kawin			
3.06	BCP or DRP Testing Result with sign-ff by management	-	All transactions	9-Feb-2016	Kawin			
3.07	Backup Restoration Testing Result	-	All transactions	9-Feb-2016	Kawin			
4. Physical Security								
4.01	"Server Room Visitor Log Book" from April 2015 to	-	All transactions	9-Feb-2016	Paisan			
4.02	List of authorised persons	-	-	9-Feb-2016	Winit			- Current list
4.03	Request to add/change/delete access to server room from April 2015 to present	-	All transactions	9-Feb-2016	Winit			- Sample would be selected from Request #4.02

ภาพที่ 4.10 รายละเอียดหัวข้อต่างๆ ในการตรวจสอบระบบสารสนเทศของ File Excel



ภาพที่ 4.11 แสดงหน้าจอรายละเอียดระบบตรวจสอบและควบคุมคุณภาพงานไอที เพื่อใช้สำหรับการนำข้อมูลจากผู้ตรวจสอบทางสารสนเทศที่อยู่ในรูปแบบของ File Excel

จากภาพที่ 4.10 – 4.11 แสดงถึงซึ่งเป็นหัวข้อต่างๆ ในการตรวจสอบระบบสารสนเทศบันทึกลงฐานข้อมูลในระบบ ตรวจสอบและควบคุมคุณภาพงานด้านไอทีซึ่งประกอบด้วยส่วนต่างๆ ดังนี้

1) Category เป็นกลุ่มหัวข้อในด้านต่างๆ ของการตรวจซึ่งประกอบไปด้วย 8 ด้าน ดังนี้

(1) OS & DB Configuration Request

(2) IT Policy, Organization and general control

(3) IT Operation

(4) Physical Security

(5) Information Security

(6) System Change Control

(7) Application Control – NAVISION

(8) Journal Entry Testing

2) Year เป็นรอบปีที่ถูกตรวจสอบงานระบบตรวจสอบและควบคุมคุณภาพงานไอที โดยหัวข้อต่างๆ ในการตรวจสอบระบบสารสนเทศจะถูกแยกเป็นปีของการตรวจ

3) Purpose แสดงวัตถุประสงค์ของการตรวจสอบเพื่ออธิบายรายละเอียดของรายการการตรวจว่าอยู่ในมาตรฐานใดของกรอบมาตรฐานทางสารสนเทศ

4) Item เป็นลำดับรายระเอียดการตรวจระบบสารสนเทศภายใต้กลุ่มหัวข้อการตรวจสอบระบบสารสนเทศ

5) Standard ใช้สำหรับการเทียบรายละเอียดการตรวจว่าอยู่ในด้านใดในกรอบมาตรฐานสารสนเทศ

6) Evidence check list เป็นการเช็คว่าในแต่ละรายการการตรวจระบบสารสนเทศนั้นมีเอกสารหรือข้อมูลสนับสนุนหรือไม่

7) Comment from Audit สำหรับบันทึกความคิดเห็นจากผู้ตรวจสอบทางสารสนเทศของแต่ละรายการของการตรวจ

8) Document support ในกรณีที่มีเอกสารหลักฐานหรือเอกสารสนับสนุนในแต่ละรายการการตรวจสอบแนบ สามารถเชื่อมโยงไปยังแหล่งเอกสารในรูปแบบของดิจิทัลไฟล์

9) Status เป็นการ update สถานะของรายการตรวจสอบและเกณฑ์การให้คะแนนซึ่งเพื่อนำไปใช้ในการวิเคราะห์คุณภาพงานด้านไอที โดยแบ่งดังตารางที่ 4.1

ตารางที่ 4.1 แสดงสถานะของรายการตรวจสอบและเกณฑ์การให้คะแนนเพื่อนำไปใช้ในการวิเคราะห์คุณภาพงานด้านไอที

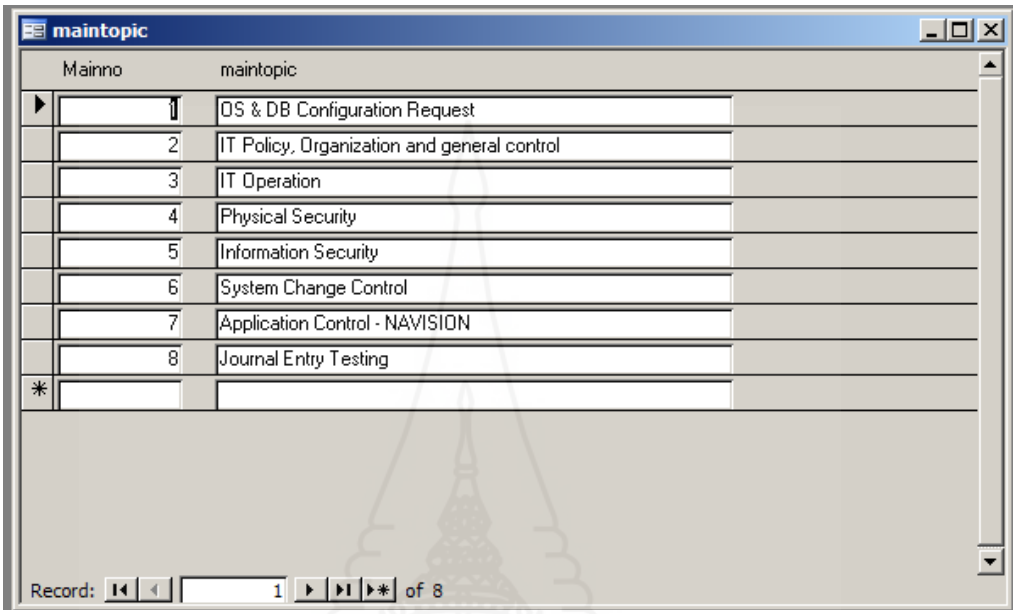
สถานะ	คำอธิบาย	คะแนน
A	มีข้อมูล / เอกสาร / ระเบียบปฏิบัติ และปฏิบัติตาม อย่างเคร่งครัด	100
B	มีระเบียบปฏิบัติ และปฏิบัติตาม อย่างเคร่งครัด แต่ไม่มีเอกสารหรือข้อมูลที่สนับสนุน	75
C	กำลังจัดเตรียมเอกสาร / กำลังจัดทำระเบียบปฏิบัติ	50
D	ไม่มีข้อมูล / ไม่มีเอกสาร / ไม่มีระเบียบปฏิบัติ	25
F	มีระเบียบปฏิบัติ แต่ไม่ปฏิบัติตาม	0

1.4.2 Setup Audit Group

เป็นหน้าจอใช้สำหรับการจัดกลุ่มในแต่ละด้านของการตรวจสอบระบบสารสนเทศประกอบไปด้วยรายละเอียดดังต่อไปนี้

1) Mainno หมายเลขกลุ่มการตรวจสอบระบบสารสนเทศในแต่ละด้าน

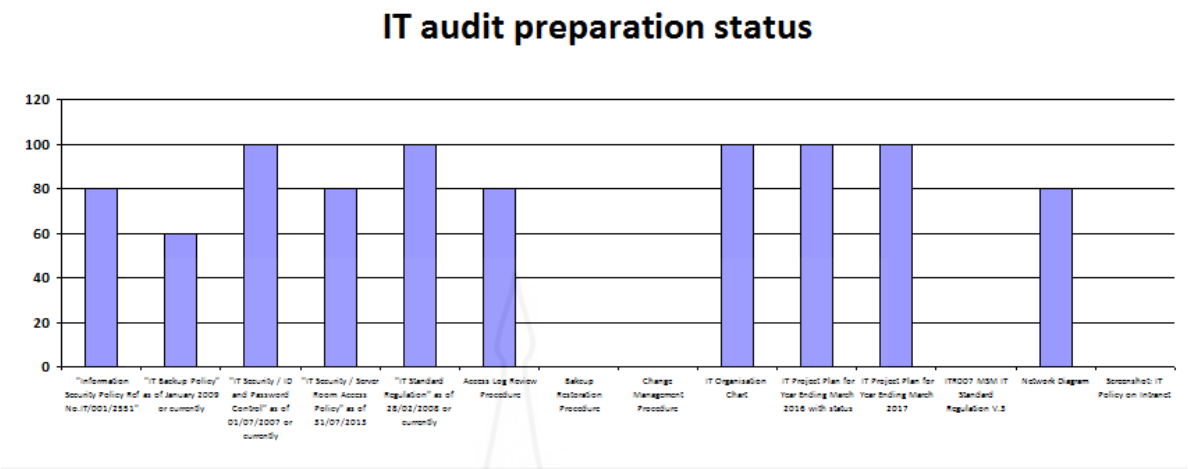
2) Maintopic เพื่ออธิบายรายละเอียดการตรวจสอบระบบสารสนเทศในแต่ละด้าน



ภาพที่ 4.12 ภาพหน้าต่างการทำงานของ Setup Audit Group

1.4.3 Audit Analysis

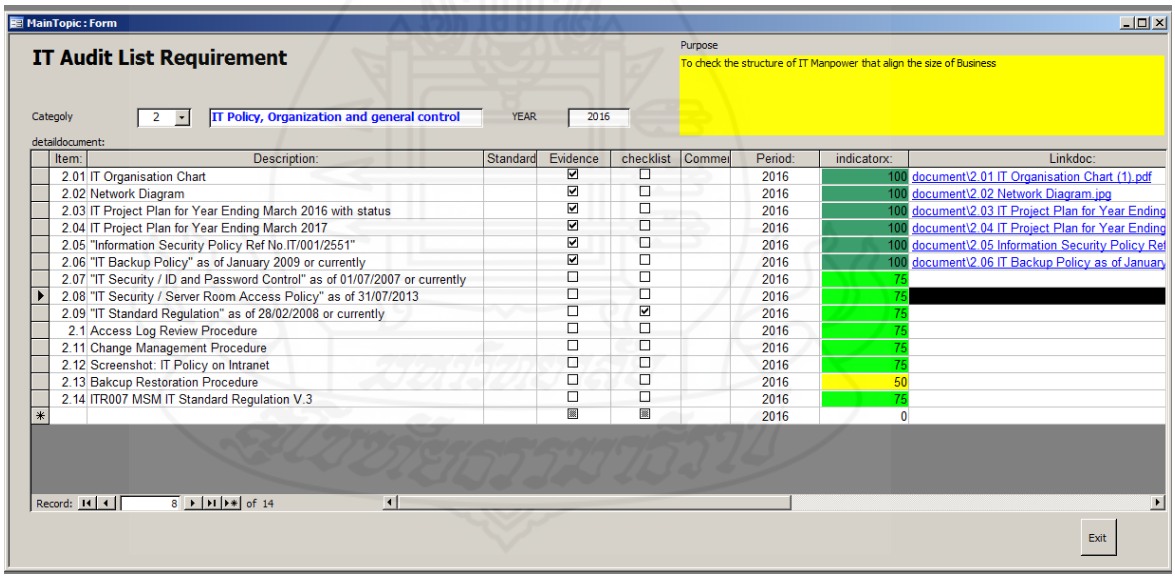
เป็นการนำเสนอการควบคุมคุณภาพในแต่ละด้านในรูปแบบของกราฟแท่ง เป็นผลมาจากการนำข้อมูลที่บันทึกลงไปในระบบควบคุมคุณภาพของระบบสารสนเทศมาทำการวิเคราะห์และสรุปผลออกมา



ภาพที่ 4.13 แสดงตัวอย่างภาพกราฟแสดงสถานะคุณภาพด้านเทคโนโลยีจากการประเมิน

1.5 ระบบแสดงผลการวิเคราะห์สถานะมาตรฐานของระบบสารสนเทศ

โดยแสดงสถานะด้วยการใช้สีในช่อง indicator ในการสื่อความหมายของคุณภาพด้านต่างๆ ของระบบสารสนเทศ ดังภาพที่ 4.14



ภาพที่ 4.14 แสดงสถานะด้วยการใช้สีในช่อง indicator ในการสื่อความหมายของคุณภาพด้านต่างๆ ของระบบสารสนเทศ

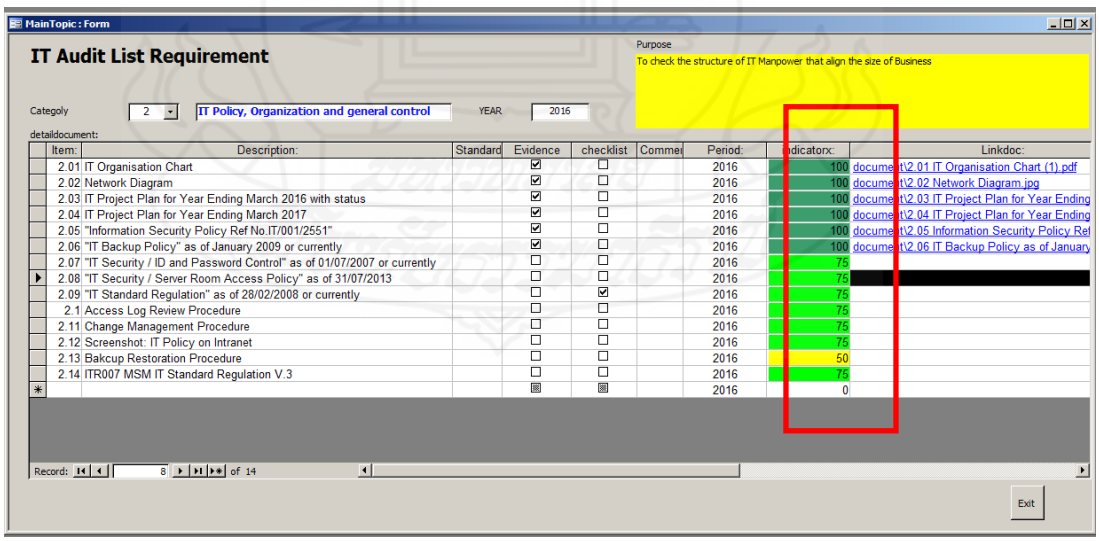
2. ผลลัพธ์ของการประเมินประสิทธิภาพของระบบ

จากการทดสอบการวิเคราะห์คุณภาพงานไอที โดยใช้ระบบที่ได้พัฒนาขึ้นนั้นทางผู้วิจัยได้ทำการบันทึกข้อมูลลงในระบบโดยการให้คะแนนในแต่ละด้านตามเกณฑ์ที่กำหนดไว้ดังนี้

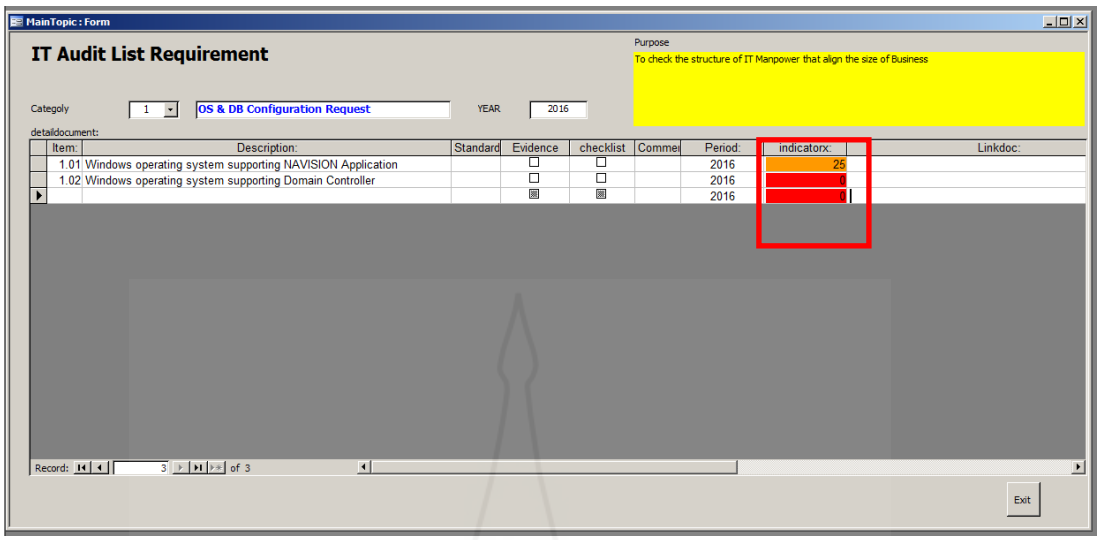
ตารางที่ 4.2 แสดงสถานะทำการบันทึกข้อมูลลงในระบบโดยการให้คะแนนในแต่ละด้านตามเกณฑ์

สถานะ	คำอธิบาย	คะแนน	สี
A	มีข้อมูล / เอกสาร / ระเบียบปฏิบัติ และปฏิบัติตาม อย่างเคร่งครัด	100	เขียวเข้ม
B	มีระเบียบปฏิบัติ และปฏิบัติตาม อย่างเคร่งครัด แต่ไม่มีเอกสารหรือข้อมูลที่สนับสนุน	75	เขียวอ่อน
C	กำลังจัดเตรียมเอกสาร / กำลังจัดทำระเบียบปฏิบัติ	50	สีเหลือง
D	ไม่มีข้อมูล / ไม่มีเอกสาร / ไม่มีระเบียบปฏิบัติ	25	สีส้ม
F	มีระเบียบปฏิบัติ แต่ไม่ปฏิบัติตาม	0	สีแดง

จากนั้นจึงนำไปใช้ในการวิเคราะห์คุณภาพงานด้านไอทีในแต่ละด้าน โดยช่อง indicator จะเป็นคะแนนคุณภาพและแสดงผลเป็นสีต่างๆ ดังภาพที่ 4.15 – 4.16



ภาพที่ 4.15 แสดงของทำงานของ IT Audit List Requirement โดยใช้สีเป็นตัววัดคุณภาพ สีเขียวเข้ม 100 / สีเขียวอ่อน / สีเหลือง



ภาพที่ 4.16 แสดงของทำงานของ IT Audit List Requirement โดยใช้สีเป็นตัววัดคุณภาพสีส้ม / สีแดง

ผลจากการประเมินประสิทธิภาพของระบบนั้น ทางผู้วิจัยได้ทำการทดสอบระบบโดยเริ่มตั้งแต่การบันทึกข้อมูลลงฐานข้อมูลของระบบโดยใช้รายการคุณภาพจากผู้ตรวจสอบระบบสารสนเทศ จากนั้นประเมินคุณภาพทางด้านต่างๆ ของระบบสารสนเทศตามหลักเกณฑ์ที่กำหนดไว้ซึ่งระบบสามารถวิเคราะห์คุณภาพงานด้านสารสนเทศได้อย่างถูกต้องตามที่ได้ออกแบบและพัฒนาขึ้น

บทที่ 5
สรุปการวิจัย อภิปรายผล และข้อเสนอแนะ

จากการศึกษาค้นคว้าและพัฒนาเรื่อง “การพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิต” สามารถสรุปสิ่งที่ได้รับจากการศึกษาค้นคว้าได้ดังนี้

1. สรุปการวิจัย

1.1 วัตถุประสงค์ของการวิจัย

1.1.1 ออกแบบและพัฒนาระบบควบคุมภาพงานสารสนเทศสำหรับธุรกิจจำหน่ายรถบรรทุก

1.1.2 ประเมินต้นแบบในการรับการตรวจสอบระบบสารสนเทศจากผู้ตรวจสอบทางด้านเทคโนโลยีสารสนเทศภายนอก

1.2 วิธีดำเนินการวิจัย

1.2.1 ขอบเขตด้านพื้นที่

บริษัท มิตซุย บุซซัน ออโตโมทีฟ (ประเทศไทย) จำกัด ได้รับการแต่งตั้งเป็นตัวแทนจำหน่ายอย่างเป็นทางการจาก บริษัท ฮีโน่ มอเตอร์สเซลส์ (ประเทศไทย) จำกัด ในปี พ.ศ. 2524 ปัจจุบัน มีโชว์รูม 3 แห่ง คือ 1. สำนักงานใหญ่บนถนนกิ่งแก้ว จังหวัดสมุทรปราการ 2.ชลบุรี (ใกล้นิคมอมตะนคร) 3. แหลมฉบัง

1.2.2 ขอบเขตด้านข้อมูล

โดยครอบคลุมข้อมูลงานของระบบเทคโนโลยีสารสนเทศสารสนเทศทั้ง 8 ด้านของบริษัท มิตซุย บุซซัน ออโตโมทีฟ(ประเทศไทย) จำกัดดังนี้

1) ระบบปฏิบัติการ (Operation System) ระบบฐานข้อมูล ในเรื่องของการ Setup ค่าต่างๆ

2) ระเบียบปฏิบัติ และนโยบายต่างๆ ด้านสารสนเทศโครงสร้างแผนกสารสนเทศและการควบคุมทั่วไปด้านสารสนเทศ

3) การปฏิบัติงานด้านต่างๆ ของแผนกสารสนเทศ

4) ความมั่นคงปลอดภัยทางกายภาพของระบบสารสนเทศ

5) ความมั่นคงปลอดภัยด้านสารสนเทศ

6) การควบคุมในด้านการเปลี่ยนแปลงระบบสารสนเทศ(System Change Control)

7) การควบคุมระบบการทำงานของโปรแกรมประยุกต์

8) การทดสอบรายความถูกต้องของรายการการบันทึกข้อมูลทางบัญชี

1.2.3 ขอบเขตของระบบ

โปรแกรมประยุกต์ที่ใช้ในการประเมินคุณภาพทางด้านสารสนเทศนั้นมีขอบเขตการใช้งานเพื่อการประเมินความพร้อมจากการตรวจสอบคุณภาพ ด้านสารสนเทศจาก IT Auditor เท่านั้น ฟังชั้นหลักๆ ของระบบนี้มีดังต่อไปนี้

1) ระบบความปลอดภัยในการใช้โปรแกรม และ สิทธิการใช้งานและการเข้าถึงข้อมูล

2) ระบบการบันทึกข้อมูลลงในฐานข้อมูล

3) รายงานและการแสดงผลด้วยกราฟจากการวิเคราะห์ข้อมูลในระบบฐานข้อมูล

4) ฟังก์ชั่นการนำข้อมูลออกมาในรูปแบบ File Excel

1.2.4 เครื่องมือที่ใช้ในการวิจัย

1) รายการการตรวจคุณภาพด้านสารสนเทศจากผู้ตรวจระบบสารสนเทศ (IT Auditor)

2) โปรแกรมประยุกต์ระบบฐานข้อมูลเพื่อใช้เตรียมความพร้อมและประเมินระบบสารสนเทศรองรับการตรวจระบบจากผู้ตรวจสอบทางด้านเทคโนโลยีสารสนเทศ

3) เอกสารหลักฐานที่ใช้ในการควบคุมระบบสารสนเทศของบริษัทและข้อมูลต่างๆ ของแผนกสารสนเทศ

1.3 ผลการวิจัย

1.3.1 ผลลัพธ์ของการออกแบบและพัฒนาระบบ

จากการออกแบบและพัฒนาระบบ มีส่วนประกอบของโปรแกรมเพื่อรองรับการใช้งานต่างๆ ของระบบดังนี้

1) ระบบความปลอดภัยในการเข้าใช้งานสามารถป้องกันและสร้างความปลอดภัยจากการใช้งานของระบบตรวจสอบและควบคุมคุณภาพงานไอทีโดยผ่านการระบุตัวตนผู้ใช้งาน (User) และใช้รหัสผ่าน (password)

2) ระบบการสร้าง ผู้ใช้งาน (User) และกลุ่ม (GROUP) การใช้งานระบบสามารถสร้างผู้ใช้งานและกลุ่มการใช้งานเพื่อเป็นการจัดประเภทและหน้าที่การใช้งานได้อย่างเหมาะสม

3) ระบบการกำหนดสิทธิการใช้งาน ระบบตรวจสอบและควบคุมคุณภาพงานไอทีสามารถที่จะจัดการสิทธิการใช้งานในแต่ละส่วนของการใช้งานเพื่อความปลอดภัยในการเข้าถึง เปลี่ยนแปลง แก้ไข ข้อมูล ได้อย่างถูกต้องตามสิทธิที่ให้ไว้ในแต่ละผู้ใช้งาน

4) ระบบการจัดการและบันทึกข้อมูล ระบบตรวจสอบและควบคุมคุณภาพงานไอทีสามารถใช้งานในฟังชั่นต่างๆ ได้ตามที่พัฒนาและออกแบบไว้ ในการบันทึกข้อมูล การเปลี่ยนแปลง แก้ไขข้อมูล แสดงผลต่างๆ

5) ระบบแสดงผลการวิเคราะห์สถานะมาตรฐานของระบบสารสนเทศ ระบบตรวจสอบและควบคุมคุณภาพงานไอที สามารถแสดงผลการวิเคราะห์ข้อมูลออกมาในรูปแบบของกราฟตามที่ออกแบบและพัฒนาไว้

6) ระบบรายงานสถานะมาตรฐานของระบบสารสนเทศ ระบบตรวจสอบและควบคุมคุณภาพงานไอทีสามารถแสดงผลและพิมพ์รายงานนำเสนอต่อผู้บริหารเพื่อเป็นข้อมูลในการตัดสินใจคุณภาพงานสารสนเทศได้ตามที่ออกแบบและพัฒนาไว้

1.3.2 ผลลัพธ์ของการประเมินประสิทธิภาพของระบบ

จากการทดสอบการวิเคราะห์คุณภาพงานไอที โดยใช้ระบบที่ได้พัฒนาขึ้น นั้นทางผู้วิจัยได้ทำการบันทึกข้อมูลลงในระบบโดยการให้คะแนนในแต่ละด้านตามเกณฑ์ที่กำหนดไว้ดังนี้

1) สถานะ A มีข้อมูล / เอกสาร / ระเบียบปฏิบัติ และปฏิบัติตาม อย่างเคร่งครัดมีคะแนนเท่ากับ 100 สีเขียวเข้ม

2) สถานะ B มีระเบียบปฏิบัติ และปฏิบัติตาม อย่างเคร่งครัด แต่ไม่มีเอกสารหรือข้อมูลที่สนับสนุน มีคะแนนเท่ากับ 75 สีเขียวอ่อน

3) สถานะ C กำลังจัดเตรียมเอกสาร / กำลังจัดทำระเบียบปฏิบัติ มีคะแนนเท่ากับ 50 สีเหลือง

4) สถานะ D ไม่มีข้อมูล / ไม่มีเอกสาร / ไม่มีระเบียบปฏิบัติ มีคะแนนเท่ากับ 25 สีส้ม

5) สถานะ F มีระเบียบปฏิบัติ แต่ไม่ปฏิบัติตาม มีคะแนนเท่ากับ 0 สีแดง

2. อภิปรายผล

ในการพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิต สามารถดำเนินการได้บรรลุวัตถุประสงค์ที่ตั้งไว้ เพราะสามารถดำเนินการได้สำเร็จตามระยะเวลาและเป้าหมายที่กำหนด ทำให้เกิดประสิทธิภาพและประสิทธิผล ซึ่งผู้วิจัยได้ประยุกต์ใช้แนวคิด PDCA หรือวงจรเดมิง ซึ่งเป็นวงจรการควบคุมคุณภาพมาเป็นแนวทางในการพัฒนาระบบ 4 ขั้นตอน คือ 1. การวางแผนการดำเนินงาน 2. การปฏิบัติตามแผน 3. การตรวจสอบ 4. การปรับปรุงการดำเนินการอย่างเหมาะสม ตั้งแต่เริ่มต้นการพัฒนาระบบจนกระทั่งสิ้นสุดกระบวนการจึงทำให้เกิดมาตรฐานในการพัฒนาอย่างสมบูรณ์

จากผลการศึกษาและวิเคราะห์การพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิตทำให้องค์กรที่ได้ทำการวิจัยพัฒนาคุณภาพด้านสารสนเทศดังนี้

2.1 ด้านของกรอบแนวคิดธรรมาภิบาลด้านไอที

2.1.1 การกำหนดกลยุทธ์ (Strategic Alignment) แผนกสารสนเทศได้จัดทำแผนและงบประมาณประจำปีในการพัฒนาระบบเทคโนโลยีสารสนเทศไปในทิศทางเดียวกันกับนโยบายและทิศทางขององค์กรโดยอ้างอิงการตรวจสอบเช่นรายละเอียดการตรวจสอบข้อที่ 5 IT Project Plan with status: ของผู้ตรวจสอบระบบสารสนเทศแผนงานด้านสารสนเทศและสถานะโครงการ ซึ่งเป็นการกำหนดกลยุทธ์ด้านสารสนเทศให้สอดคล้องกับธุรกิจ

2.1.2 การบริหารจัดการทรัพยากร (Resource Management) การลงทุนและจัดสรรทรัพยากรเทคโนโลยีสารสนเทศให้กับองค์กรตามความต้องการและความเหมาะสมเช่นการตรวจสอบในหัวข้อที่ 3 รายละเอียดการตรวจสอบจากผู้ตรวจสอบระบบสารสนเทศ IT Organization Chart: ผังโครงสร้างแผนกสารสนเทศซึ่งเป็นการจัดการบริหารบุคคลากรในหน่วยงานสารสนเทศใน Function งานต่างๆเพื่อให้เหมาะสมกับการลงทุนขององค์กร

2.1.3 การสร้างระบบเทคโนโลยีสารสนเทศให้กิจกรรม (Value delivery) เช่นในหัวข้อการตรวจสอบที่ 20 และ 21 ในการจัดทำแผนการบริหารธุรกิจต่อเนื่อง (Business Continuity Plan)หรือการจัดทำแผนสำรองด้านสารสนเทศ เป็นการสร้างคุณค่าแก่องค์กรในด้านสารสนเทศ

2.1.4 การบริหารความเสี่ยง (Risk management) การประมาณความเสี่ยงที่จะเกิดขึ้นและแนวทางลดความเสียหายที่อาจจะเกิดขึ้นเช่นการตรวจสอบในหัวข้อที่ Backup Restoration

Testing Result: ผลการทดสอบการสำรองข้อมูลและการเรียกกลับข้อมูล เป็นการลดความเสี่ยงที่อาจจะก่อให้เกิดความเสียหายแก่ข้อมูลขององค์กร

2.2 ด้านของกรอบมาตรฐานโคบิต

จากการพัฒนาต้นแบบระบบตรวจสอบและควบคุมคุณภาพงานไอทีเพื่อรองรับการตรวจสอบจากผู้ตรวจสอบทางด้านสารสนเทศนั้นผู้วิจัยสามารถสร้างมาตรฐานให้แก่ระบบสารสนเทศขององค์กรอันเป็นผลที่ได้จากการเตรียมความพร้อมในการตรวจสอบนั้นหนึ่งในมาตรฐานที่ระบบสารสนเทศองค์กรได้รับคือ มาตรฐานโคบิตซึ่งเป็นไปดังนี้

2.2.1 กระบวนการ (Processes) สร้างกระบวนการเพื่อให้งานได้ผลลัพธ์หรือบรรลุเป้าหมายของกระบวนการ ซึ่งจะนำไปสู่การบรรลุซึ่งเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและเป้าหมายระดับองค์กรได้

2.2.2 วัฒนธรรม จริยธรรม และความประพฤติ (Culture, ethics, behavior) ปฏิบัติตามกระบวนการที่สร้างขึ้นมาสำเร็จได้ จนบรรลุเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและตามเป้าหมายระดับองค์กร

2.2.3 โครงสร้างบุคลากร (Organizational structures) มีความชัดเจนในด้านโครงสร้างทางด้านบุคลากรขึ้นมาเพื่อให้มีหน้าที่ความรับผิดชอบที่ชัดเจนว่าต้องทำอะไรบ้าง

2.2.4 ข้อมูล (Information) กระบวนการดูแลรักษาและเรื่องความปลอดภัยในการเข้าถึงข้อมูลและการตรวจสอบความน่าเชื่อถือของข้อมูล

2.2.5 เข้าใจหลักการและนโยบายองค์กร (Principles and policies) ที่กำหนดไว้เห็นถึงภาพรวม ทิศทาง กรอบแนวคิด หรือกรอบการปฏิบัติที่องค์กรต้องการให้บรรลุเพื่อบังเกิดความสำเร็จตามที่ต้องการ ปฏิบัติตามอย่างสอดคล้อง เพื่อให้เกิดผลตามที่องค์กรต้องการ

2.2.6 เสริมสร้างทักษะ ความรู้ และความสามารถของบุคลากร (Skills and competences) เป็นกุญแจสำคัญไปสู่ความสำเร็จของงานและกระบวนการ

2.2.7 ปรับปรุงโครงสร้างพื้นฐานของการให้บริการสารสนเทศ (Service capabilities) โครงสร้างพื้นฐานของการให้บริการสารสนเทศ หมายรวมถึงฮาร์ดแวร์ ซอฟต์แวร์ แอพพลิเคชันและเทคโนโลยีอื่นๆที่ทำหน้าที่เป็นพื้นฐานในการให้บริการด้านระบบงานและข้อมูลแก่ผู้ใช้งานขององค์กร

3. ข้อเสนอแนะ

3.1 ข้อเสนอแนะในการนำการวิจัยไปใช้งานจริง

ระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุก ทางผู้วิจัยขอแนะนำข้อต่างๆ ดังนี้

3.1.1 คอมพิวเตอร์ที่ติดตั้งระบบปฏิบัติการ OS (Operation System) ตั้งแต่ Windows XP ขึ้นไป

3.1.2 ติดตั้งโปรแกรมประยุกต์ Microsoft Access ตั้งแต่ เวอร์ชั่น 2003 ขึ้นไป และติดตั้งโปรแกรมระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุก

3.1.3 ติดตั้งอุปกรณ์สิ่งพิมพ์ (Printer) เชื่อมต่อกับ computer เพื่อใช้ในการพิมพ์รายงานสรุปผลของการควบคุมคุณภาพนำเสนอต่อผู้บริหาร

3.2 ข้อเสนอแนะในการวิจัยครั้งต่อไป

ควรมีการศึกษาและพัฒนาต่อยอดระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุกโดยใช้หลักธรรมาภิบาลไอทีและกรอบมาตรฐานโคบิตเพื่อนำไปสู่การกำหนดนโยบายองค์กรโดยการพัฒนาระบบตรวจสอบและควบคุมคุณภาพงานไอทีของธุรกิจจำหน่ายรถบรรทุก ไม่ว่าจะเป็นในส่วนของมาตรฐานการชี้วัด การแสดงผล การใช้งานของตัวโปรแกรม โดยแลกเปลี่ยนความรู้และความคิดเห็นด้านคุณภาพระบบสารสนเทศในด้านอื่นๆ กับตัวแทนธุรกิจจำหน่ายรถบรรทุกเพื่อสร้างเกณฑ์มาตรฐานและพัฒนาคุณภาพด้านสารสนเทศต่อไป

ประวัติผู้ศึกษา

ชื่อ สกุล	นายกวิน บุญทวี
วัน เดือน ปีเกิด	2 มิถุนายน 2513
สถานที่เกิด	กรุงเทพมหานคร
ประวัติการศึกษา	ปริญญาตรีคณะรัฐศาสตร์ สาขาความสัมพันธ์ระหว่างประเทศ มหาวิทยาลัยรามคำแหง
สถานที่ทำงาน	บริษัท มิตซุย บุซซัน ออโตโมทีฟ (ประเทศไทย) จำกัด
ตำแหน่งงาน	ผู้จัดการแผนกสารสนเทศ