การนำ ISO20000 และ ISO27001 มาวิเคราะห์ความแตกต่าง เพื่อหาแนวทางในการพัฒนาด้านเทคโนโลยีสารสนเทศสำหรับผู้ให้บริการทางด้านไอที

APPLYING ISO20000 AND ISO27001 GAP ANALYSIS TO DEVELOP INFORMATION TECHNOLOGY FOR IT PROVIDER

นางสาวณัฐณิชา พรหมรส

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย – ญี่ปุ่น

พ.ศ. 2561

การนำ ISO20000 และ ISO27001 มาวิเคราะห์ความแตกต่าง เพื่อหาแนวทางในการพัฒนาด้านเทคโนโลยีสารสนเทศสำหรับผู้ให้บริการทางด้านไอที

APPLYING ISO20000 AND ISO27001 GAP ANALYSIS TO DEVELOP INFORMATION TECHNOLOGY FOR IT PROVIDER

นางสาวณัฐณิชา พรหมรส

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย - ญี่ปุ่น
ปีการศึกษา 2561

คณะกรรมการสอบ

..... ประธานกรรมการสอบ
(ผศ. ดร. ประจักษ์ เฉิดโฉม)

..... กรรมการสอบ
(ผศ. ดร. นรังสรรค์ วิไลสกุลยง)

..... อาจารย์ที่ปรึกษา
(อาจารย์อดิศักดิ์ เสือสมิง)

..... ประธานสหกิจศึกษาสาขาวิชา
(อาจารย์สลิลา ชีวกิดาการ)

ชื่อโครงงาน	การนำ ISO20000 และ ISO27001 มาวิเคราะห์ความแตกต่าง เพื่อหาแนวทางในการพัฒนาด้านเทคโนโลยีสารสนเทศสำหรับผู้ให้บริการทางด้านไอที Applying ISO20000 and ISO27001 Gap Analysis To Develop Information Technology For IT Provider
ผู้เขียน	นางสาวณัฐณิชา พรหมรส
คณะวิชา	เทคโนโลยีสารสนเทศ สาขาวิชาเทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษา	อาจารย์อดิศักดิ์ เสือสมิง
พนักงานที่ปรึกษา	นางสาวชลธิชา เรืองทอง
ชื่อบริษัท	บริษัท เอ-โฮสต์ จำกัด
ประเภทธุรกิจ/สินค้า	ให้บริการทางด้าน Oracle Product และ Hosting Service

บทสรุป

ในการสหกิจศึกษาได้รับมอบหมายในตำแหน่ง Internal Audit ช่วยในการตรวจสอบระบบภายในของบริษัทเพื่อลดความเสี่ยงที่จะทำให้เกิดความขัดข้องของระบบ เพื่อแนะนำและปรับปรุงแก้ไข ทำให้ระบบสามารถใช้งานได้อย่างมีประสิทธิ์ภาพ และมีแผนรองรับเมื่อเกิดเหตุฉุกเฉิน

การตรวจสอบระบบภายในองค์กรของบริษัท ได้นำมาตรฐาน ISO20000 ใช้ในการรองรับการตรวจสอบระบบภายในองค์กร โดยอ้างอิงตาม Policy, Process, Procedures และ Plan ในแต่ละกระบวนการของการตรวจสอบ และทำการวิเคราะห์ข้อมูล ISO20000 เพื่อพัฒนาไปให้ถึง ISO27001 โดยวิเคราะห์จากระบบที่มีอยู่เพื่อหาข้อแตกต่างและนำมาพัฒนาเพิ่มขึ้นจากระบบเดิม โดยมีเครื่องมือที่ช่วยในการตรวจสอบคือการทำ Checklist เพื่อช่วยลดเวลาและกำหนดขอบเขตในการสอบถาม จากการทำงานนี้ทำให้ได้เรียนรู้ถึงวิธีการที่ใช้ในการตรวจสอบภายในขององค์กร และทำให้เข้าใจถึงความรับผิดชอบในหน้าที่ของตนเองต่องานที่ได้รับมอบหมาย การบริหารเวลาในสภาวะกดดัน ซึ่งเป็นประสบการณ์ที่ดี และสามารถนำไปใช้ในการปฏิบัติงานได้ในอนาคต

Project's name	Applying ISO20000 and ISO27001 Gap Analysis To Develop Information Technology For IT Provider
Writer	Ms. Natnicha Phromros
Faculty	Faculty of Information of Technology, Information of Technology
Faculty Advisor	Mr. Adisak Suasaming
Job Supervisor	Ms. Chonticha Reangthong
Company's name	A-Host Company Limited
Business Type / Product	Oracle Product and Hosting Service

Summary

I was assigned as a Internal Audit during the cooperative education, which the duty was monitoring of system. It helps an organization achieve its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, governance processes and When have emergency.

The company's internal audit system has adopted ISO20000 standards to support internal auditing. Referenced by Policy, Process, Procedure and Plan in each process of verification. And ISO20000 data analysis to develop to ISO27001. Analyzing the existing system to find the difference and develop it from the original system. The Checklist tool is to help reduce the time and scope of inquiries. By doing this, you learn how to use internal auditing. And to understand their responsibilities in the task assigned. Time management in the pressures. This is a good experience. And can be used in the future.

กิตติกรรมประกาศ

ขอขอบคุณบริษัท เอ-โฮสต์ จำกัด ที่มอบโอกาสให้ข้าพเจ้าได้มาเป็นส่วนหนึ่งของการปฏิบัติงาน ทำให้ข้าพเจ้าได้มีประสบการณ์ในการทำงานจริง อีกทั้งยังได้ความรู้ต่าง ๆ มากมาย ทั้งเรื่องการปฏิบัติตนให้เหมาะสมต่อการทำงาน รู้จักกาลเทศะ การคิดอย่างเป็นระบบระเบียบ การสัมภาษณ์ และการประชุมกับพนักงานภายในบริษัท การดำเนินงานมีการฝึกเรียนรู้ด้วยตนเองและได้รับการชี้แนะจากพนักงานที่ปรึกษา แนะนำแนวทางในการทำงานและแง่คิดต่างๆ ทั้งในทางทฤษฎีและทางปฏิบัติ รวมทั้งขอขอบคุณความอนุเคราะห์ที่ให้นักศึกษาสหกิจศึกษาเข้าร่วมกิจกรรมต่างๆ กับทางทีมงานและทางบริษัทฯ เช่น การประชุมกับพนักงานในบริษัท การแสดงความคิดเห็น และการทำงานอื่นๆ ที่สามารถเป็นประโยชน์กับทางบริษัทฯ ได้ ซึ่งประสบการณ์เหล่านี้ไม่สามารถหาได้จากในห้องเรียนหรือในหนังสือ แต่สามารถหาได้จากการปฏิบัติงานที่บริษัท เอ-โฮสต์ จำกัด

ขอขอบคุณพี่พนักงานทุกท่านที่คอยช่วยเหลือ ให้คำปรึกษาและดูแลข้าพเจ้าอย่างดีมาโดยตลอดระยะเวลา 17 สัปดาห์ในการสหกิจศึกษาที่ผ่านมา ทำให้ข้าพเจ้ารู้สึกผูกพันธ์ และรู้สึกยินดีเป็นอย่างยิ่งที่ได้เป็นส่วนหนึ่งในการปฏิบัติงาน รวมถึงอาจารย์ที่ปรึกษา อาจารย์อดิศักดิ์ เสือสมิง และพนักงานที่ปรึกษา คุณชลธิชา เรืองทอง, คุณพิชานน จะเรียมพันธ์,คุณณัฐพล คำชุ่ม, คุณสุชัย เย็นฤดี และ คุณประสงค์ เอื้อสุริยนันท์ ที่คอยให้คำปรึกษาเกี่ยวกับโครงงานมาโดยตลอด ทำให้การปฏิบัติงานของข้าพเจ้าสำเร็จลุล่วงไปได้ด้วยดี และสุดท้ายนี้ข้าพเจ้าขอขอบคุณคณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีไทย – ญี่ปุ่น ที่ได้ให้โอกาสสำหรับการสหกิจศึกษาในครั้งนี้ จึงขอกราบขอบพระคุณมา ณ ที่นี้ค่ะ

ณัฐณิชา พรหมรส

ผู้จัดทำ

สารบัญ

บทสรุป ..... **ก**

Summary ..... **ข**

กิตติกรรมประกาศ ..... **ค**

สารบัญ ..... **ง**

สารบัญรูป ..... **ฉ**

สารบัญตาราง ..... **ช**

บทที่ 1 บทนำ **1**

1.1 ชื่อและที่ตั้งของสถานประกอบการ 1

1.2 ลักษณะธุรกิจของสถานประกอบการ หรือการให้บริการหลักขององค์กร 2

1.2.1 Hosting & Outsource Service 4

1.2.2 Oracle Core Technology Products and Advanced Services 5

1.2.3 Oracle Enterprise Performance Management (EPM) และ Hyperion Business Intelligence Products and Services 5

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร 6

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย 7

1.5 พนักงานที่ปรึกษา และ ตำแหน่งของพนักงานที่ปรึกษา 7

1.6 ระยะเวลาที่ปฏิบัติงาน 7

1.7 ที่มาและความสำคัญของปัญหา 7

1.8 วัตถุประสงค์หรือจุดมุ่งหมายของโครงงาน 8

1.9 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย 8

1.10 นิยามศัพท์เฉพาะ 9

บทที่ 2 ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน **14**

2.1 ทฤษฎีที่ใช้ในการปฏิบัติงาน 14

2.1.1 ขั้นตอนการตรวจสอบภายในองค์กร 14

2.1.2 ISO 20000 (Service Management System : SMS) 16

2.1.3 ISO27001 (Information Security Management System : ISMS) 25

2.1.4 PDCA / KAIZEN 47

2.1.5 GAP Analysis 48
2.2 มาตรฐานที่เกี่ยวข้อง 49
2.2.1 Information Technology Infrastructure Library (ITIL) 49
2.2.2 Control Objectives for Information and Related Technology (COBIT) 50
2.3 เทคโนโลยีที่ใช้ในการปฏิบัติงาน 53
2.3.1 Microsoft Office 2016 53
2.3.2 Snipping Tool 54
2.3.3 WinZip Background Tools 55
บทที่ 3 แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน 56
3.1 แผนงานการปฏิบัติงาน และแผนการทำโครงงานสหกิจฯ (Gantt Chart) 56
3.2 รายละเอียดงานที่นักศึกษาปฏิบัติในการสหกิจศึกษา 57
3.3 ขั้นตอนการดำเนินงานโครงงานสหกิจศึกษา 58
บทที่ 4 สรุปผลการดำเนินงาน การวิเคราะห์และสรุปผลต่าง ๆ 59
4.1 ขั้นตอนและผลการดำเนินงานโครงงานสหกิจศึกษา 59
4.1.1 รายละเอียดของโครงงานและความรู้ที่ได้รับ 59
4.1.2 ศึกษาและทำความเข้าใจหลักการ และ แนวคิด 60
4.1.3 การวิเคราะห์ความแตกต่างของ ISO 20000 และ ISO 27001 63
4.2 ผลการวิเคราะห์ข้อมูล 69
บทที่ 5 บทสรุปและข้อเสนอแนะ 70
5.1 สรุปผลการดำเนินงานโครงงานสหกิจศึกษา 70
5.2 แนวทางการแก้ไขปัญหา 70
5.3 ข้อเสนอแนะจากการดำเนินงานโครงงานสหกิจศึกษา 71
เอกสารอ้างอิง 72
ภาคผนวก 73
ภาคผนวก ก. รายงานการปฏิบัติงานประจำสัปดาห์ 74
ประวัติผู้จัดทำโครงงาน 92

สารบัญรูป

รูป **หน้า**

รูปที่ 1.1 แผนที่บริษัท เอ-โฮสต์ จำกัด 1
รูปที่ 1.2 รางวัลที่บริษัท A-HOST ได้รับ....3
รูปที่ 1.3 คณะผู้บริหาร A-HOST Company Limited 6
รูปที่ 2.1 วงจร PDCA....48
รูปที่ 2.2 หลักการ Goal Cascade ของ COBIT 51
รูปที่ 2.3 Microsoft Office Icon....53
รูปที่ 2.4 Snipping Tool....54
รูปที่ 2.5 WinZip Background Tools....55
รูปที่ 3.1 ขั้นตอนการดำเนินงานภาพรวม (1) 58
รูปที่ 3.2 ขั้นตอนการดำเนินงาน (2)....58
รูปที่ 4.1 ขั้นตอนการประยุกต์ใช้....64
รูปที่ 4.2 ขั้นตอนการศึกษา ISO 20000 65
รูปที่ 4.3 ขั้นตอนการศึกษา ISO 27001 66
รูปที่ 4.4 ขั้นตอนการหาความแตกต่างระหว่าง ISO 20000 และ ISO 27001....67
รูปที่ 4.5 ตารางการเปรียบเทียบความแตกต่างระหว่าง ISO 20000 และ ISO 27001 68

สารบัญตาราง

ตาราง **หน้า**

ตารางที่ 1.1 นิยามศัพท์เฉพาะ 9
ตารางที่ 2.1 Change Management Process 20
ตารางที่ 2.2 ประเภทของการพิสูจน์ตัวตน (Authentication Types) 23
ตารางที่ 3.1 แผนงานการปฏิบัติงาน 56

บทที่ 1
บทนำ

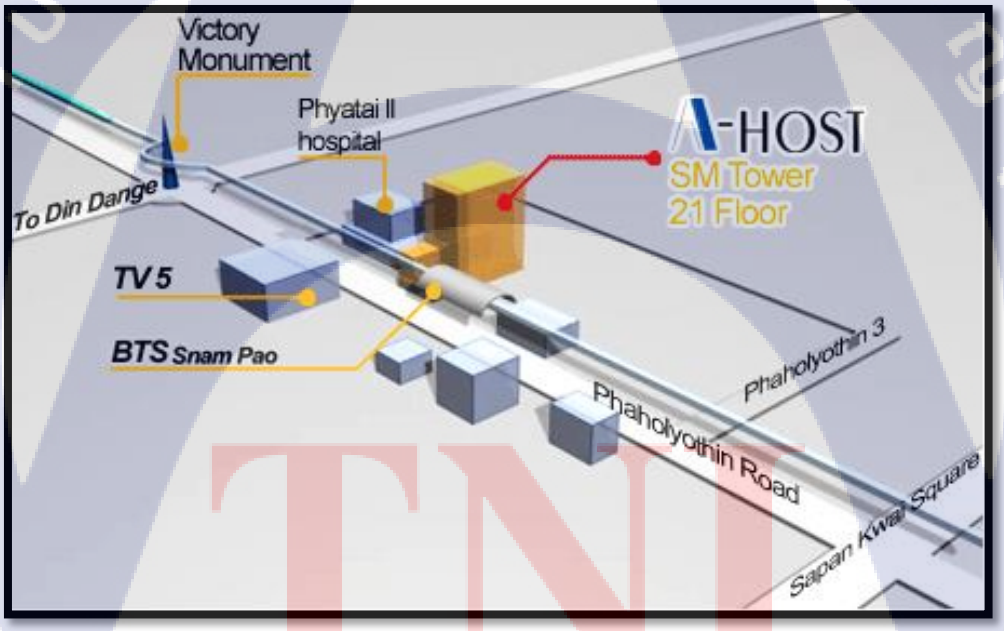
1.1 ชื่อและที่ตั้งของสถานประกอบการ

ชื่อสถานประกอบการ : A-HOST Company Limited.

ที่ตั้งสถานประกอบการ : 979/52-55 SM Tower 21st Fl., Phaholyothin Rd., Samsennai, Phyathai, Bangkok 10400

โทรศัพท์ : 02-298-0625-32

โทรสาร : 02-298-0053



รูปที่ 1.1 แผนที่บริษัท เอ-โฮสต์ จำกัด

1.2 ลักษณะธุรกิจของสถานประกอบการ หรือการให้บริการหลักขององค์กร

บริษัทเอ-โฮสต์จำกัดได้ก่อตั้งขึ้นเมื่อปีพ.ศ.2542 ในฐานะหนึ่งบริษัทในเครือของบริษัทซิสเต็มส์คอร์ปอเรชั่น (มหาชน) จำกัดและเป็นผู้เชี่ยวชาญด้านการบริการจัดวางระบบสารสนเทศ (Information Technology : IT) และบริการเสริมต่างๆสำหรับลูกค้าตั้งแต่ธุรกิจขนาดย่อมไปจนถึงขนาดกลางธุรกิจหลักของบริษัทเอ-โฮสต์คือการให้บริการโฮสติ้ง (Hosting) ซึ่งเป็นการเปิดเครื่องคอมพิวเตอร์แม่ข่ายในการให้เช่าพื้นที่เพื่อวางระบบและบริการระบบสารสนเทศด้วยผลิตภัณฑ์ของออราเคิล (Oracle) เป็นซอฟต์แวร์สำหรับการวางแผนบริหารทรัพยากรของระดับแนวหน้าของโลก

เอ-โฮสต์ถือกำเนิดขึ้นจากกลุ่มผู้เชี่ยวชาญด้านสารสนเทศท่ามกลางภาวะเศรษฐกิจตกต่ำทั่วภูมิภาคเอเชียแต่เอ-โฮสต์ก็สามารถเติบโตอย่างรวดเร็วและมั่นคงตั้งแต่แรกก่อตั้งด้วยจุดแข็งในฐานะผู้บุกเบิกธุรกิจโฮสติงเซอร์วิสพร้อมทั้งนำธุรกิจแนวใหม่อย่างการให้บริการระบบโปรแกรมประยุกต์หรือ ASP (Application Services Provider) เข้ามาให้บริการเป็นรายแรกในเมืองไทยอีกทั้งยังถือเป็นผู้ให้บริการรายแรกนอกประเทศสหรัฐอเมริกาด้วย

ในฐานะผู้นำในอุตสาหกรรมนี้เป็นเวลามากกว่า 10 ปีเอ-โฮสต์ได้เสริมสร้างความแข็งแกร่งทางธุรกิจด้วยบริการที่มีความโดดเด่นและรวบรวมเอาทรัพยากรบุคคลซึ่งได้สั่งสมประสบการณ์และความชำนาญไว้อย่างพร้อมเพรียงส่งผลให้ศูนย์ข้อมูลของเอ-โฮสต์ในปัจจุบันมีความสมบูรณ์ด้วยกลุ่มเซิร์ฟเวอร์ (Server) ที่เชื่อมต่อกันในลักษณะการจัดกลุ่ม (Clustering) ซึ่งเปี่ยมสมรรถนะสามารถให้บริการแก่ผู้ใช้จำนวนมากได้ในเวลาเดียวกัน

นอกจากนี้เอ-โฮสต์ยังติดตั้งระบบรักษาความปลอดภัยระบบสำรองข้อมูลและระบบบริหารจัดการรวมถึงอุปกรณ์ต่างๆอย่างครบครันเพื่อให้เอ-โฮสต์สามารถตอบสนองต่อระดับความต้องการในระดับสูงสุดที่ลูกค้าคาดหวังได้ตลอดจนเป็นการสร้างความมั่นใจให้แก่ลูกค้าที่ใช้บริการโฮสติงและแอพพลิเคชันต่างๆของเอ-โฮสต์ว่าจะได้รับทั้งประสิทธิภาพและความปลอดภัยอย่างครบครันธุรกิจการให้บริการระบบโปรแกรมประยุกต์ในรูปแบบ ASP เอ-โฮสต์ไม่เพียงแต่ให้บริการด้านโปรแกรมประยุกต์ด้านการดำเนินธุรกิจทางอิเล็กทรอนิกส์ระดับโลกของออราเคิลพร้อมโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศเท่านั้นแต่ยังมีบริการที่ครอบคลุมตั้งแต่การให้คำปรึกษาการสนับสนุนและการให้บริการทั่วไปอย่างพรั่งพร้อมครบครัน

นอกจากธุรกิจโฮสติ้งและธุรกิจการให้บริการโปรแกรมประยุกต์ในรูปแบบ ASP ซึ่งถือเป็นธุรกิจหลักเอ-โฮสต์ยังเดินหน้าธุรกิจอย่างต่อเนื่องโดยการขยายหน่วยงานใหม่เพิ่มขึ้นนั่นก็คือ Core Technology Division หน่วยงานเทคโนโลยีหลักที่ให้คำตอบเบ็ดเสร็จแก่ลูกค้าด้วยระบบฐานข้อมูลและเครื่องมือต่างๆ ของออราเคิลซึ่งช่วยเพิ่มความสามารถของลูกค้าในการออกแบบพัฒนาปรับเปลี่ยนระบบแอพพลิเคชันให้เหมาะสมกับธุรกิจนั้นๆภายใต้คำปรึกษาแนะนำและการวางระบบของเอ-โฮสต์ลูกค้าสามารถบริหารระบบฐานข้อมูลของตนเองและดูแลระบบดังกล่าวได้อย่างมีประสิทธิภาพ

ตลอดระยะเวลามากกว่า10ปีในการดำเนินธุรกิจของเอ-โฮสต์ไม่เพียงแต่ในฐานะผู้บุกเบิกธุรกิจโฮสติงและธุรกิจการให้บริการโปรแกรมประยุกต์ในรูปแบบ ASP เท่านั้นแต่เอ-โฮสต์ยังได้ทำการติดตั้งระบบสารสนเทศรวมทั้งผลิตภัณฑ์ของออราเคิลให้กับลูกค้าจนประสบความสำเร็จเป็นจำนวนมากซึ่งหลายรายเป็นหนึ่งในร้อยบริษัทชั้นนำของประเทศไทยแต่สิ่งที่สำคัญกว่านั้นก็คือการที่เอ-โฮสต์ได้สานสัมพันธ์กับลูกค้าและพันธมิตรทางธุรกิจอย่างแนบแน่นจนกลายเป็นหุ้นส่วนทางกลยุทธ์และได้รับตั้งแต่งให้เป็น OCAP (Oracle Certified Advantage Partner) รายแรกในประเทศไทย

รูปที่ 1.2 รางวัลที่บริษัท A-HOST ได้รับ

ปัจจุบันบริษัท เอ-โฮสต์ มีประเภทของสินค้าและการบริการซึ่งสามารถแบ่งออกเป็น 3 กลุ่มใหญ่ได้แก่

1.2.1 Hosting & Outsource Service

เอ-โฮสต์ได้ปรับปรุงและขยายการบริการ Hosting และการให้บริการภายนอก (Outsource) จนสามารถครอบคลุมความต้องการของลูกค้าได้อย่างหลากหลายโดยยึดหลักในการในการให้บริการที่เรียกว่า “Peace of Mind for the customer” ซึ่งหมายถึงการที่จะทำงานให้กับลูกค้าแบบครบวงจรเพื่อที่ลูกค้าจะได้สามารถใช้งานระบบสารสนเทศได้อย่างมีประสิทธิภาพได้อย่างสบายใจไร้ความกังวลต่อความเสี่ยงต่างๆไม่ว่าจะเป็นเรื่องของปัญหาทางเทคนิคการจัดทำระบบและข้อมูลสำรองการปรับแต่งระบบให้ได้ประสิทธิภาพสูงสุด (Performance Tuning) และที่สำคัญที่สุดคือการที่เข้ามารับภาระในด้านการบริหารจัดการบุคลากรทางด้านสารสนเทศทั้งหมดแทนลูกค้า

การใช้บริการ Hosting และ Outsource จะทำให้ลูกค้าสามารถทุ่มเทกำลังสมองเวลาและทรัพยากรขององค์กรให้กับธุรกิจที่เป็นแกนหลัก (Core Business) ซึ่งเป็นสิ่งที่ลูกค้าถนัดกว่าโดยทั่วไปแล้วบริการ Hosting และOutsource จะประกอบด้วยส่วนประกอบและบริการย่อยๆดังต่อไปนี้

1. High Availability and High Performance IT Infrastructure
2. Dedicated or Co-Location Service
3. Disaster Site
4. Oracle E-Business Application (ERP, CRM, SCM)
5. ERP Implementation Service
6. System and Database Administration
7. Help Desk
8. On-Request Service i.e. On-Site Support, Software Customization

ทั้งนี้การบริการ Hosting และ Outsource สามารถครอบคลุมได้ทั้งระบบที่ใช้เทคโนโลยีของออราเคิลและระบบที่ใช้เทคโนโลยีอื่น

1.2.2 Oracle Core Technology Products and Advanced Services

เอ-โฮสต์เป็นผู้นำในการดำเนินธุรกิจในฐานะผู้แทนจำหน่ายเพิ่มมูลค่าให้กับออราเคิลโดยไม่เพียงแต่ทำหน้าที่ในการจัดจำหน่ายสินค้าในกลุ่มแกนหลักของเทคโนโลยี (Core Technology) ของออราเคิลทุกประเภทแต่ยังมีทีมผู้เชี่ยวชาญที่จะให้การสนับสนุนและบริการเสริมอย่างครบวงจรแก่บริษัทคู่ค้าและลูกค้าไม่ว่าจะเป็นการร่วมจัดกิจกรรมทางการตลาดการฝึกอบรมการติดตั้งระบบและการให้คำปรึกษาเพื่อแก้ไขปัญหาต่างๆสินค้าและบริการที่อยู่ในกลุ่ม Oracle Core Technology Products and Advanced Services ได้แก่

1. Oracle Database and database options
2. Oracle Business Intelligence Suite
3. Business Partner Development
4. System Installation, Integration and Optimization
5. Oracle Fusion Middleware (รวมถึง BEA)
6. สินค้าอื่นๆทุกประเภทของออราเคิล
7. Marketing and Lead Generation Activities
8. SOA-Based Development and Implementation

ผลสำเร็จในการดำเนินธุรกิจประเภทนี้ทั้งในด้านการตลาดและบริการทำให้เอ-โฮสต์ได้รับรางวัล ASEAN Partner of the Year ในปี 2005

1.2.3 Oracle Enterprise Performance Management (EPM) และ Hyperion Business Intelligence Products and Services

ความต้องการสูงสุดประการหนึ่งของผู้บริหารในการนำเอาระบบสารสนเทศมาใช้ในองค์กรไม่ว่าจะเป็นภาคราชการหรือเอกชนคือการทำให้ผู้บริหารสามารถได้ข้อมูลที่แสดงให้เห็นถึงสถานะในการดำเนินธุรกิจได้อย่างแม่นยำรวดเร็วและการนำเอาข้อมูลมาวิเคราะห์และวางแผนทั้งในระดับปฏิบัติการและในระดับกลยุทธ์เพื่อให้ธุรกิจสามารถได้เปรียบในการแข่งขันปรับตัวตามเศรษฐกิจได้ในทุกสถานการณ์ Oracle

Enterprise Performance Management (EPM) และ Hyperion Business Intelligence จัดเป็นซอฟต์แวร์ชั้นแนวหน้าของโลกที่สามารถสนองตอบต่อความต้องการในลักษณะดังกล่าวได้เป็นอย่างดี

เอ-โฮสต์มีทีมงานที่ปรึกษาที่มีประสบการณ์ทั้งทางด้านธุรกิจและทางด้านเทคนิครวมถึงความเข้าใจในระบบ ERP ของออราเคิลอย่างลึกซึ้งจึงทำให้สามารถให้บริการที่ปรึกษาเพื่อออกแบบติดตั้งเชื่อมโยงและปรับใช้ระบบให้กับลูกค้าจนเกิดประสิทธิภาพสูงสุดอีกทั้งยังมีความยืดหยุ่นและให้การตอบสนองที่เร็วกว่าเมื่อเทียบกับการว่าจ้างที่ปรึกษาจากต่างประเทศ

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร

รูปที่ 1.3 คณะผู้บริหาร A-HOST Company Limited

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย

ตำแหน่งงาน : Internal Audit

หน้าที่ : การปฏิบัติงานจะเป็นการตรวจสอบภายในองค์กร โดยยึดตามมาตรฐาน ISO20000 และ ISO27001 เป็นการตรวจสอบกระบวนการ ขั้นตอนการทำงาน และนโยบาย เพื่อตรวจสอบหาข้อผิดพลาดหรือความเสี่ยงที่จะเกิดขึ้น เมื่อพบเจอปัญหาที่เกิดขึ้น ให้ทำการแจ้งฝ่ายที่มีส่วนในการรับผิดชอบทราบและทำการแก้ไขเพื่อลดความเสี่ยงที่จะทำให้เกิดผลกระทบต่อระบบหรือองค์กร

1.5 พนักงานที่ปรึกษา และ ตำแหน่งของพนักงานที่ปรึกษา

พนักงานที่ปรึกษา : นางสาว ชลธิชา เรืองทอง

ตำแหน่ง : Advisory QA Specialist

E-mail : chonticha@a-host.co.th

1.6 ระยะเวลาที่ปฏิบัติงาน

อบรมเป็นเวลาทั้งสิ้น : 16 เมษายน – 25 พฤษภาคม พ.ศ. 2561

เริ่มต้นการปฏิบัติงาน : 4 มิถุนายน พ.ศ. 2561

สิ้นสุดการปฏิบัติงาน : 28 กันยายน พ.ศ. 2561

เป็นระยะเวลาทั้งสิ้น : 17 สัปดาห์

1.7 ที่มาและความสำคัญของปัญหา

เนื่องจากปัจจุบันเศรษฐกิจ การค้า นวัตกรรม และเทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็ว ส่งผลให้องค์กรต่างๆ ทั้งภาครัฐ และเอกชนต้องเตรียมความพร้อมรับมือสำหรับการเปลี่ยนแปลง และเร่งพัฒนาศักยภาพ ประสิทธิภาพ และคุณภาพขององค์กร ซึ่งความก้าวหน้าทางเทคโนโลยีถือเป็นปัจจัยหนึ่งที่สำคัญทำให้เกิดความต่อเนื่องในการดำเนินธุรกิจ ลดความเสี่ยงที่จะทำให้เกิดผลกระทบต่อองค์กร และการให้บริการขององค์กรต่อผู้ใช้บริการ ทำให้องค์กรได้รับผลกำไร อีกทั้งยังสามารถแข่งขันกับองค์กรอื่นได้ การพัฒนาด้านเทคโนโลยีสารสนเทศให้สามารถตอบสนองต่อการดำเนินธุรกิจขององค์กรและการให้บริการต่อผู้ใช้งาน องค์กรจึงต้องกำหนดนโยบาย และกระบวนการในการบริหารธุรกิจ

เพื่อให้ภายในองค์กรปฏิบัติให้ตรงตามข้อกำหนด ส่งผลให้องค์กรได้นำ ISO20000 และ การพัฒนาไปสู่ ISO27001 มาประยุกต์ใช้ในการให้บริการ หรือควบคุมการให้บริการสำหรับภายในองค์กร เพื่อให้พนักงานในองค์กร สามารถปฏิบัติหรือดำเนินการตามนโยบาย กระบวนการ ข้อกำหนด และขั้นตอนที่กำหนดไว้ เพื่อให้พนักงาน และช่วยเพิ่มความเชื่อมั่นให้กับผู้ใช้บริการ ส่งผลให้ง่ายต่อการวางแผนในการปฏิบัติงาน มีมาตรฐานในการปฏิบัติงาน เข้าใจขั้นตอนในการดำเนินงาน และตรงกับความต้องการของผู้มีส่วนร่วมในการให้บริการ

จากการศึกษาข้อมูลที่เกี่ยวข้อง ทางผู้จัดทำจึงเห็นว่าทฤษฎีของวงจรการบริหารงานคุณภาพ (PDCA : Plan-Do-Check-Act) มีความสอดคล้องกับมาตรฐานงานบริการด้านไอที (ISO20000 : International Standard For IT Service Management) และมาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล (ISO27001 : International Standard For Information Security Management Systems) สามารถนำมาประยุกต์ใช้ในการควบคุมการให้บริการ ให้มีประสิทธิภาพในการให้บริการมากขึ้น และมีการวางแผนขั้นตอนในการดำเนินงานอย่างมีประสิทธิภาพ เพื่อลดความเสี่ยงที่จะเกิดขึ้นกับระบบขององค์กรเพื่อความปลอดภัยของข้อมูล และวางแผนแนวทางในอนาคตขององค์กรได้

1.8 วัตถุประสงค์หรือจุดมุ่งหมายของโครงงาน

1. เพื่อศึกษามาตรฐานงานบริการด้านไอที (ISO20000 : International Standard For IT Service Management)
2. เพื่อศึกษามาตรฐานความปลอดภัยของข้อมูล (ISO27001 : International Standard For Information Security Management Systems)
3. เพื่อศึกษาการตรวจสอบภายใน (Internal Audit)
4. เพื่อวิเคราะห์ความเสี่ยงที่จะเกิดขึ้นกับองค์กร (Risk Management)
5. เพื่อนำความเสี่ยงที่ได้จากการวิเคราะห์ มาวางแผนหาแนวทางป้องกัน
6. เพื่อตรวจความสามารถในการให้บริการ ให้ตรงตามความต้องการ

1.9 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย

1. นักศึกษาได้รับความรู้ในเทคโนโลยีต่างๆ ที่ใช้งานในปัจจุบัน
2. นักศึกษานำความรู้ที่ได้จากการปฏิบัติงานจากการสหกิจไปใช้ประกอบอาชีพในอนาคต
3. นักศึกษาได้รับประสบการณ์ในการตรวจเอกสาร และ ระบบภายในบริษัท

4. นักศึกษาสามารถทำงานร่วมกับผู้อื่นได้เป็นอย่างดี
5. นักศึกษามีความรู้และทักษะเฉพาะทางในสายงานนี้มากยิ่งขึ้น
6. นักศึกษาได้รับประสบการณ์ในการปฏิบัติงานจริง
7. นักศึกษามีความรับผิดชอบในหน้าที่การทำงานงานที่ได้รับมอบหมาย
8. ระบบมีความเสี่ยงลดลง ทำให้มีความความปลอดภัยมากขึ้น
9. ระบบทำงานได้อย่างมีประสิทธิภาพมากขึ้น
10. ระบบสามารถพัฒนาต่อยอดไปในอนาคตได้

1.10 นิยามศัพท์เฉพาะ

ตารางที่ 1.1 นิยามศัพท์เฉพาะ

คำศัพท์	คำนิยาม
Service Management	ชุดของความสามารถและกระบวนการที่จะสั่งการและควบคุมกิจกรรมของผู้ให้บริการและทรัพยากรสำหรับการออกแบบการเปลี่ยนแปลงการส่งมอบและการปรับปรุงการบริการเพื่อตอบสนองความต้องการของบริการ
Service Management System (SMS)	ระบบการจัดการเพื่อควบคุมและบริหารกิจกรรมการจัดการบริการของผู้ให้บริการ
Service Provider	องค์กรหรือส่วนหนึ่งขององค์กรที่จัดการและให้บริการหรือบริการแก่ลูกค้า
Service Level Agreement (SLA)	เอกสารข้อตกลงระหว่างผู้ให้บริการและลูกค้าที่ระบุบริการและเป้าหมายการบริการ
Operational Level Agreement (OLA)	เอกสารข้อตกลงระหว่างผู้ให้บริการกับกลุ่มภายใน

คำศัพท์	คำนิยาม
Underpinning Contract (UC)	เอกสารข้อตกลงระหว่างผู้ให้บริการและผู้จัดจำหน่าย
Incident	การหยุดชะงักของการให้บริการโดยไม่ได้ตั้งใจทำให้การลดคุณภาพของบริการเป็นเหตุการณ์ที่ยังไม่ได้ส่งผลต่อการให้บริการแก่ลูกค้า
Information Security Incident	เหตุการณ์การรักษาความปลอดภัยข้อมูลที่ไม่พึงประสงค์หรือ ที่ไม่คาดคิด ที่มีความเป็นไปได้ เป็นนัยสำคัญที่จะทำให้การดำเนินธุรกิจและการรักษาความปลอดภัยของข้อมูลเป็นไปอย่างน่าเป็นห่วง
Service Request	ข้อมูลคำแนะนำการเข้าถึงบริการหรือการเปลี่ยนแปลงที่ได้รับอนุมัติล่วงหน้า
Problem	สาเหตุของเหตุการณ์อย่างน้อยหนึ่งเหตุการณ์
Known error	ปัญหาที่มีสาเหตุมาจากการระบุสาเหตุหรือวิธีการลดหรือขจัดผลกระทบต่อบริการโดยการแก้ไขปัญหา
Known error database (KEDB)	ฐานข้อมูลที่อธิบายถึงข้อผิดพลาดที่ทราบทั้งหมดภายในระบบโดยรวม
Configuration Database (CMDB)	เก็บข้อมูลที่ใช้ในการบันทึกคุณลักษณะของรายการกำหนดค่าและความสัมพันธ์ระหว่างรายการกำหนดค่าตลอดวงจรการทำงานของพวกเขา
Configuration Item (CI)	องค์ประกอบที่ต้องควบคุมเพื่อส่งมอบบริการ
Configuration baseline	ข้อมูลการกำหนดค่าที่กำหนดอย่างเป็นทางการ ที่กำหนดในช่วงของบริการหรือส่วนประกอบของบริการ
Definitive Media Library (DML)	พื้นที่เก็บข้อมูลเชิงตรรกะเดียวแม้ว่าจะมีหลายตำแหน่งก็ตาม เอาไว้เก็บ Cis ไว้ได้อย่างปลอดภัย
Capacity Database (CDB)	ฐานข้อมูลที่ประกอบด้วยข้อมูล Capacity Management ที่เหมาะสม (ข้อมูลทางด้านเทคนิค ข้อมูลธุรกิจ และข้อมูลอื่น ๆ ทั้งหมดที่เกี่ยวข้องกับ Capacity Management)

คำศัพท์	คำนิยาม
Capacity Management Information System (CMIS)	พื้นเก็บข้อมูลที่มีความเชื่อมโยงกันทั้งหมดของ Capacity Management data มักจะเก็บไว้ใน multiple physical locations
Change	การเพิ่มเติมการปรับเปลี่ยนหรือการกำจัดสิ่งใด ที่อาจส่งผลต่อ IT Services รวมถึงการเปลี่ยนแปลงโครงสร้างสถาปัตยกรรม นโยบาย กระบวนการ ขั้นตอน เครื่องมือ และเอกสารรวมทั้งการเปลี่ยนแปลงไปยัง IT services และ configuration items (CIs) อื่นๆ
Request for Change (RfC)	ข้อเสนออย่างเป็นทางการสำหรับการเปลี่ยนแปลงที่จะทำประกอบด้วยรายละเอียดของการเปลี่ยนแปลงที่เสนอ
Change Advisory Board (CAB)	ผู้มีอำนาจที่พิจารณาและอนุมัติการเปลี่ยนแปลงที่ต้องการ รวมถึงผู้ที่มีความเข้าใจอย่างชัดเจนในทุกช่วงของความต้องการของผู้มีส่วนได้ส่วนเสียและสามารถมองเห็นการเปลี่ยนแปลงได้อย่างเต็มที่ซึ่งอาจส่งผลต่อการให้บริการและการกำหนดค่าต่างๆที่อยู่ในการควบคุม
Emergency Change Advisory Board (ECAB)	ผู้มีอำนาจหรือผู้บริหารที่พิจารณาและอนุมัติการเปลี่ยนแปลงในกรณีฉุกเฉิน
Standard Change	การเปลี่ยนแปลงที่ได้รับการอนุมัติล่วงหน้าซึ่งถือเป็นความเสี่ยงที่ค่อนข้างต่ำ ดำเนินการเป็นประจำและปฏิบัติตามขั้นตอนการจัดทำเป็นเอกสารหรือคำแนะนำในการทำงาน
Emergency Change	การเปลี่ยนแปลงที่ต้องดำเนินการโดยเร็วที่สุดตัวอย่างเช่นเพื่อแก้ไขเหตุการณ์สำคัญหรือใช้โปรแกรมแก้ไขความปลอดภัย การเปลี่ยนแปลงต้องได้รับการประเมินและปฏิเสธหรืออนุมัติในระยะเวลาสั้น ๆ
Normal Change	การเปลี่ยนแปลงใด ๆ ที่ไม่ใช่การเปลี่ยนแปลงตามมาตรฐานหรือการเปลี่ยนแปลงอย่างเร่งด่วนที่ต้องมีการทบทวนการจัดการการเปลี่ยนแปลงทั้งหมด

คำศัพท์	คำนิยาม
Major Change	การเปลี่ยนแปลงการถ่ายโอนหรือการกำจัดบริการที่มีความเสี่ยงปานกลางหรือสูง การละเมิด SLA อย่างร้ายแรงคาดว่าจะเกิดขึ้นและอาจส่งผลต่อการให้บริการที่สำคัญทางธุรกิจ
Release Unit	เป็นส่วนหนึ่งของบริการหรือโครงสร้างพื้นฐาน ที่ออกมาเป็น released เดียว (เช่นระบบ ชุดโปรแกรม โปรแกรม และ โมดูล)
Release Package	ชุดของ Configuration Items (CIs), หนึ่งหรือหลาย release หน่วยที่จะสร้างทดสอบและใช้งานร่วมกันเป็นรุ่นเดียว
Supplier Management (SPM)	ผู้ให้บริการจำเป็นที่จะต้องมีซัพพลายเออร์ เพื่อประโยชน์ในการจัดซื้อสินค้า/บริการ หรือเพื่อให้การสนับสนุนการดำเนินการในด้านต่างๆ ดังนั้น ทั้งสองฝ่ายจึงต้องจัดทำข้อตกลงระหว่างกันเป็นลายลักษณ์อักษร เพื่อระบุขอบเขต บทบาท หน้าที่และความรับผิดชอบของแต่ละฝ่ายอย่างชัดเจน โดยข้อตกลงที่ทำขึ้นระหว่างผู้ให้บริการกับซัพพลายเออร์นี้ จะต้องเป็นไปในทิศทางเดียวกันกับข้อตกลง Service Level Agreement ที่ผู้ให้บริการได้ทำไว้กับลูกค้า/ผู้ใช้บริการ
Information Security Management (ISM)	ผู้รับผิดชอบในการให้คำแนะนำเกี่ยวกับความเป็นไปได้ด้านเทคนิคและความคุ้มค่าในการปฏิบัติตามนโยบายจัดการความมั่นคงปลอดภัยสารสนเทศ
Confidentiality	การเก็บรักษาข้อมูลที่ได้รับการคุ้มครองอย่างถูกต้องโดยมีการจำกัดการเข้าถึงเฉพาะบุคคลที่ได้รับอนุญาตตามความจำเป็นที่จะต้องรู้เท่านั้น และไม่เปิดเผยหรือยอมให้บุคคล หรือองค์กร หรือกระบวนการใดๆ ที่ไม่ได้รับอนุญาตได้รับรู้
Integrity	ข้อมูลที่สมบูรณ์ถูกต้องเชื่อถือได้และสามารถตรวจสอบได้

คำศัพท์	คำนิยาม
Availability	ข้อมูล การประมวลผลข้อมูล และการสื่อสารข้อมูลที่สามารถเข้าถึงได้ และสามารถใช้งานได้ตามความต้องการของบุคคล หรือกิจการ หรือกระบวนการที่ได้รับอนุญาต
Key Performance Indicator (KPI)	ดัชนีชี้วัดผลงานหรือความสำเร็จของงาน โดยจะแสดงให้เห็นรายละเอียดในความสำเร็จหรือล้มเหลวของงานนั้น ๆ
IT General Control (ITGC)	นโยบายและระเบียบปฏิบัติที่ใช้ในการบริหารจัดการกิจกรรมทางด้านเทคโนโลยีสารสนเทศ และ สภาพแวดล้อมของระบบคอมพิวเตอร์ รวมทั้งระบบงานสารสนเทศต่างๆ ที่ช่วยสนับสนุนความมีประสิทธิผลของการควบคุม ภายในของระบบงาน
Business Continuity Planning (BCP)	ชุดของเอกสาร คาแนะนา และวิธีการที่จะช่วยทาให้การดาเนินกิจกรรมทางธุรกิจ สามารถตอบสนองต่อการเกิดเหตุการณ์ที่ไม่ปกติ เช่น อุบัติเหตุ ภัยพิบัติ สภาวะฉุกเฉิน หรือ ภัยคุกคามที่จะเป็นอุปสรรคต่อการดาเนินธุรกิจ ให้สามารถดาเนินต่อไปได้อย่างราบรื่น
Disaster Recovery Planning (DRP)	แผนเตรียมความพร้อมกับเหตุการณ์ที่นาไปสู่การชะงักทางธุรกิจ (Disaster Recovery Planning) คือ แผนการกู้ระบบ IT ขององค์กรเมื่อมีเหตุการณ์ที่ทาให้การทางานขององค์กรหยุดชะงักลง ซึ่งในแผนการนี้ต้องมีขั้นตอนการทางานโดยละเอียดของการกู้ระบบ รวมถึง บุคคลากร และ สิ่งที่ต้องทาก่อนหลัง
Risk	โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ หรือ การกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน ซึ่งอาจจะเกิดขึ้นในอนาคต และมีผลกระทบ หรือ ทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์ การปฏิบัติงาน การเงิน และการบริหาร

บทที่ 2
ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

ในการปฏิบัติงานสหกิจศึกษาครั้งนี้ เป็นการนำความรู้ทางด้านทฤษฎีและเทคโนโลยีมาใช้ในการปฏิบัติงานทุกส่วนตลอดการปฏิบัติงานสหกิจศึกษา ซึ่งเป็นการนำความรู้ทั้งที่เคยเรียนมาประยุกต์ใช้และเป็นการศึกษาเรียนรู้สิ่งใหม่ ๆ ที่ได้จากการปฏิบัติงาน

2.1 ทฤษฎีที่ใช้ในการปฏิบัติงาน

2.1.1 ขั้นตอนการตรวจสอบภายในองค์กร

2.1.1.1 จัดเตรียมทีมงาน Internal Audit

จัดเตรียมทีมงาน Internal Audit ให้เพียงพอ หากจะให้ได้ประสิทธิภาพควรมี Auditor อย่างน้อย 4-8 คนขึ้นอยู่กับขนาดของบริษัทเพราะ Auditor จะต้องทำงานนอกเหนือจากงานประจำและมีภาระงานที่เพิ่มขึ้น เพื่อจะให้ Auditor สามารถเข้าถึงพื้นที่การเข้าถึงยากเพื่อตรวจสอบได้ รวมถึงเป็นการสร้าง Auditor สายเลือดใหม่โดยให้การฝึกอบรมที่สอดคล้องกับทีมเพื่อให้ทุกคนมีแนวความคิดและวิธีการตรวจให้เป็นแนวทางเดียวกัน

2.1.1.2 ตรวจสอบตาม Process ไม่ ตรวจสอบตาม Procedure

ทำให้ได้ผลลัพธ์ที่ดีกว่าเพราะเป็นการตรวจที่คลอบคลุมความต่อเนื่องของขั้นตอน ซึ่งมีความแตกต่างกัน ตัวอย่างเช่น การตรวจสอบกระบวนการจัดส่งสินค้าและรับวัตถุดิบหรือหน่วยงานที่จะครอบคลุมทั้งการจัดส่งสินค้าและกระบวนที่เกี่ยวข้องกับพื้นที่การรับวัตถุดิบรวมถึง procedure ทั้งหมดที่เกี่ยวข้อง เพื่อทำให้คุณมั่นใจได้ว่ากระบวนการทั้งหมดสามารถทำงานได้อย่างมีประสิทธิภาพ

2.1.1.3 ข้อกำหนดที่เป็นกฎหมายภายในประเทศ กฎหมายประเทศคู่ค้า และข้อกำหนดของโรงงาน

เพื่อจัดทำเป็นรายการคำถาม (check list) รวมถึงเพิ่มรายการคำถามได้เล็กน้อยอันได้แก่ คำถามที่ได้จากประสบการณ์ตรวจในครั้งที่ผ่านมา หมายความว่า การตรวจสอบของแต่ละคนจะแตกต่างกันเล็กน้อยและจะตรวจได้ครอบคลุมมากขึ้นเมื่อตรวจไปแล้วหลายๆครั้ง

2.1.1.4 จัดเตรียมพนักงานในพื้นที่ที่ผู้ตรวจสอบจะเข้าตรวจให้พร้อม

เพื่อให้ข้อมูลที่เกี่ยวข้องได้ดีที่สุดและต้องมีการแจ้งให้พนักงานเหล่านั้นทราบว่าพวกเขาต้องเตรียมข้อมูลที่เกี่ยวข้อง เช่น Spec, Record หรือ Procedure ให้พร้อมซึ่งจะเป็นผลดีต่อการตรวจประเมินเป็นอย่างยิ่ง

2.1.1.5 การบันทึกผลใน Check list ไม่เพียงแต่ทำเครื่องหมายถูกในช่องเหมาะสมหรือไม่เหมาะสม

ควรจะต้องจดบันทึกหลักฐานต่างๆที่เราพบเจอด้วย ซึ่งข้อมูลที่ได้นั้นจะเป็นตัวช่วยสะท้อนการทำงานของคุณทั้งสิ่งที่ทำดีแล้วและยังไม่ดีพอ นอกจากนี้ยังแสดงให้เห็นได้ว่า Auditor อย่างคุณเป็นผู้ตรวจประเมินภายในที่มีประสิทธิภาพ

2.1.1.6 จดจำที่สิ่งเคยพบเจอในครั้งที่ผ่านมาเพื่อปรับเปลี่ยนตารางเวลาการตรวจให้เหมาะสม

หากพื้นที่ใดพบความไม่สอดคล้องในปริมาณมาก ก็ให้เพิ่มความถี่ในการตรวจ ซึ่งการตรวจในแต่ละพื้นที่หรือกระบวนการต้องอยู่บนพื้นฐานอย่างน้อยหนึ่งครั้งต่อปี ซึ่งทีมผู้ตรวจถือได้ว่าเป็นกุญแจสำคัญในการวัดประสิทธิภาพและการสร้างการปรับปรุงของระบบเลยทีเดียว

2.1.1.7 เขียนรายงานการตรวจให้สมบูรณ์และชัดเจนตามความไม่สอดคล้องต่างๆที่เราตรวจพบ

ระบุความไม่สอดคล้องให้มากที่สุด ซึ่งถือได้ว่าเป็นข้อมูลที่มีคุณค่าและเป็นประโยชน์อย่างยิ่งต่อการปรับปรุงระบบขององค์กร

2.1.1.8 ให้มีการฝึกอบรมแก่ผู้ตรวจสอบ

จัดสอนโดยใช้ PowerPoint และให้สังเกตการตรวจประเมินร่วมด้วย สำหรับผู้ตรวจมือใหม่อาจเป็นเรื่องยากและรู้สึกอึดอัดที่จะต้องเข้าไปตรวจงานของเพื่อนเราเอง เพราะฉนั้นใน

ส่วนของการฝึกอบรม Auditor นอกจากต้องรู้ขั้นตอนการตรวจและข้อกำหนดแล้ว ยังต้องมีการสอนวิธีการตรวจ การตั้งคำถาม การตรวจสอบบันทึกและการดำเนินงานของแต่ละกระบวนการ เพื่อให้แน่ใจว่า Auditor สามารถดำเนินการตรวจได้อย่างมีประสิทธิผล

2.1.1.9 นำผลการตรวจที่ได้เข้ามาคุยกันในทีมเพื่อสรุปผลเข้าทบทวนฝ่ายบริหาร

เป็นการดีกว่าถ้าข้อมูลที่ได้จากการตรวจได้มีการสรุปก่อนการนำเสนอ ยิ่งมากก็จะแสดงให้เห็นถึงสถานะของระบบได้ดี การมองข้อมูลที่ได้จากการตรวจที่ระบุได้ชัดเจนจะมีประโยชน์มากกว่าการมุ่งเป้าที่จำนวนของความไม่สอดคล้องนั้นๆ ยิ่งการตรวจมีความหลากหลายในพื้นที่การเข้าตรวจมากเท่าใด การปรับปรุงการแก้ไขของระบบก็จะหลากหลายและได้ประโยชน์มากเท่านั้น

2.1.1.10 จัดเตรียมทรัพยากรที่ต้องใช้ให้มีเพียงพอในเวลาที่เหมาะสม

เพื่อให้การตรวจมีประสิทธิภาพเช่นการดำเนินการแก้ไขและการทวนสอบต่างๆ ซึ่งหมายความว่า Auditor ต้องได้รับการฝึกฝนเพื่อเตรียมพร้อมในเวลาที่ต้องดำเนินการตรวจ รวมถึงการแก้ไขและทวนสอบให้ได้ทันเวลา

2.1.2 ISO 20000 (Service Management System : SMS)

ในปัจจุบันองค์กรได้นำ ISO 20000 (Service Management System : SMS) ที่เกี่ยวกับการจัดการบริการด้านเทคโนโลยีสารสนเทศที่ได้รับการยอมรับในระดับสากล ระบบนี้มุ่งเน้นไปที่การให้บริการที่ดีแก่ลูกค้า ไปจนถึงการปรับปรุงบริการเพื่อสร้างความเชื่อมั่นให้กับลูกค้าหรือผู้ที่ใช้บริการกับองค์กร ซึ่งมีกระบวนการการควบคุมระบบการให้บริการดังต่อไปนี้

2.1.2.1 Service Level Management (SLM)

การบริหารระดับการให้บริการ เป็นการทำข้อตกลงระหว่างผู้ให้บริการ และผู้ใช้บริการเป็นลายลักษณ์อักษรอย่างชัดเจน โดยทั้งสองฝ่ายต้องร่วมกันกำหนดขอบเขตของการให้บริการ เช่น ชนิด ประเภทของบริการ รายละเอียดของบริการ บทบาทและหน้าที่ของทั้งสองฝ่าย โดยทั้งนี้ทางผู้ให้บริการสามารถเป็นได้จากทั้งภายในและภายนอกโดยจะแบ่งระดับการให้บริการดังนี้

1. SLA (Service Level Agreement) ข้อตกลงขององค์กรในการให้บริการกับลูกค้า
2. UC (Underpinning Contract) เป็นสัญญาข้อตกลงระหว่างผู้ให้บริการกับองค์กร
3. OLA (Operation Level Agreement) เป็นข้อตกลงภายในขององค์กรเอง เพื่อสนับสนุนการทำงานภายในองค์กร

ซึ่งตามหลักแล้ว SLA ควรน้อยกว่า UC และ OLA เพื่อให้สามารถมั่นใจว่าองค์กรจะสามารถให้การบริการกับลูกค้าได้อย่างที่ระบุในข้อตกลง

2.1.2.2 Incident Management (ICM)

การบริหารความไม่ต่อเนื่องในการให้บริการ จะเป็นกระบวนการที่มีเป้าหมายในการแก้ไขความไม่ต่อเนื่องที่เกิดขึ้น ให้กลับสู่สภาพเดิมของการให้บริการโดยเร็ว ทั้งนี้ความไม่ต่อเนื่องต่างๆ ที่เกิดขึ้นจะต้องได้รับการบันทึกจัดเก็บเป็นหลักฐานไว้ด้วย รวมถึงจะต้องมีการจัดทำวิธีการปฏิบัติงานในการจัดการกับผลกระทบที่เกิดขึ้นของความไม่ต่อเนื่องในการให้บริการ โดยวิธีการปฏิบัติงานนี้จะต้องมีการระบุถึงการกำหนดความไม่ต่อเนื่องที่เกิดขึ้น การหลีกเลี่ยง หรือการทำให้ผลกระทบที่เกิดขึ้นมีน้อยที่สุดรวมถึงต้องกำหนดให้มีการบันทึก การจัดประเภทการขยายผลการแก้ไขและการปิดความไม่ต่อเนื่องในการบริการทั้งหมด นอกจากนั้น ลูกค้าจะต้องได้รับแจ้งให้ทราบถึงความคืบหน้าของรายงานความไม่ต่อเนื่องในการบริการ หรือการร้องขอในการบริการรวมถึงได้รับการแจ้งเตือน กรณีที่ระดับของการบริการไม่สามารถดำเนินการได้

2.1.2.3 Problem Management (PBM)

การบริหารการแก้ไขปัญหา จะมีเป้าหมายในการระบุสาเหตุของปัญหาที่ซ่อนอยู่ และทำการจัดการแก้ไขปัญหานั้น เพื่อให้เกิดผลกระทบต่อธุรกิจน้อยที่สุด และสามารถให้บริการได้อย่างต่อเนื่องโดยมุ่งเน้นไปที่การดำเนินการเพื่อป้องกันการเกิดขึ้นซ้ำของปัญหา ทั้งนี้ปัญหาทั้งหมดที่เกิดขึ้นจะต้องได้รับการบันทึกไว้ รวมถึงจะต้องมีการกำหนดวิธีปฏิบัติงานซึ่งจะต้องมีการระบุถึง

การกำหนด การจัดประเภทการปรับปรุงให้ทันสมัย การขยายผล การแก้ไขและการปิดปัญหา นอกจากนั้น จะต้องมีการดำเนินการป้องกันเพื่อเป็นการลดปัญหาที่อาจจะเกิดขึ้น เช่น การวิเคราะห์แนวโน้มของความไม่ต่อเนื่อง และเมื่อมีการเปลี่ยนแปลงเกิดขึ้นจากการแก้ไขสาเหตุของของปัญหาโดยจะต้องดำเนินการผ่านกระบวนการบริหารการเปลี่ยนแปลง รวมถึงการปรับปรุงข้อมูลสารสนเทศให้ทันสมัยด้วย เพื่อให้เกิดความผิดพลาดที่รับรู้และปัญหาที่ได้รับการแก้ไข สำหรับกระบวนการบริหารความไม่ต่อเนื่องในการให้บริการต่อไป

บทบาทในการแก้ไขปัญหาของ Problem Management มี 2 แบบ ได้แก่

1. Reactive คือการแก้ไขปัญหาที่เกิดขึ้นแล้ว และป้องกันไม่ให้ปัญหานั้นเกิดขึ้นซ้ำอีก
2. Proactive คือการป้องกันปัญหาก่อนที่ปัญหานั้นจะเกิดขึ้น ซึ่งต้องมีการจัดเก็บและวิเคราะห์ข้อมูลต่างๆ เพื่อหาแนวโน้มของการเกิดปัญหา แล้วหาวิธีป้องกันไม่ให้เกิดปัญหาขึ้นอีก

2.1.2.4 Configuration Management (CFM)

กระบวนการบริหารจัดการกับ Configuration คือ การกำหนดและควบคุมองค์ประกอบต่างๆ ของการบริการและโครงสร้างพื้นฐาน รวมถึงดูแลรักษาความถูกต้องของข้อมูลในการปรับแต่งระบบ ทั้งนี้องค์การจะต้องมีการกำหนดนโยบายในการกำหนดรายการสำหรับการปรับแต่ง (configuration items) รวมถึงองค์ประกอบต่างๆ ที่เกี่ยวข้องกับการให้บริการด้วยการบริหารการปรับแต่งระบบจะเป็นการควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานทางด้าน IT การระบุองค์ประกอบที่สำคัญทั้งหมดภายในโครงสร้าง การรวบรวม บันทึก และดูแลรักษารายละเอียดเกี่ยวกับองค์ประกอบต่างๆ และจัดเตรียมข้อมูลเพื่อให้การสนับสนุนกับกระบวนการอื่นๆ โดยจะต้องส่งข้อมูลให้กับกระบวนการบริหารการเปลี่ยนแปลง เกี่ยวกับผลกระทบของการร้องขอการปรับแต่งระบบ นอกจากนั้น การเปลี่ยนแปลงต่างๆ ในรายการปรับแต่งระบบจะต้องสามารถสอบกลับ และทำการตรวจประเมินได้ด้วย

2.1.2.5 Capacity Management (CPM)

การบริหารขีดความสามารถในการให้บริการ จะช่วยสร้างความมั่นใจได้ว่า องค์การมีความสามารถในการให้บริการอย่างเพียงพอตามความต้องการของลูกค้าที่ได้ตกลงไว้ ทั้งการให้บริการในปัจจุบันและในอนาคต ทั้งนี้จะต้องมีการจัดทำแผนในการบริหารขีดความสามารถ โดยแผนจะประกอบด้วย ความต้องการทางด้านขีดความสามารถ และสมรรถนะทั้งในปัจจุบันและ

ที่คาดการณ์ว่าจะเกิดขึ้น กรอบระยะเวลาและต้นทุนในการดำเนินการให้บริการ การบริหารขีดความสามารถในการให้บริการจะเป็นการสร้างความเหมาะสมของต้นทุน ระยะเวลาในการให้ได้มาและการส่งมอบทรัพยากรทางด้าน IT เพื่อให้การสนับสนุนต่อข้อตกลงที่ได้ทำกับลูกค้า นอกจากนั้น การบริหารขีดความสามารถยังประกอบด้วยการบริหารทรัพยากร การบริหารผลการปฏิบัติงานการบริหารความต้องการ การจำลองแบบ การวางแผนขีดความสามารถ การบริหารภาระงาน และการปรับขนาดโปรแกรม ทั้งนี้ จะมุ่งเน้นให้ความสำคัญกับการวางแผน และการปรับความต้องการ เพื่อให้มั่นใจได้ถึงความสามารถในการตอบสนองต่อระดับการให้บริการที่ได้ตกลงไว้

2.1.2.6 Change Management (CHM)

กระบวนการบริหารการเปลี่ยนแปลง จะเป็นการดำเนินการเพื่อให้มั่นใจว่าการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้น ได้รับการประเมิน อนุมัติ นำไปปฏิบัติ และทบทวน ทั้งนี้การร้องขอการเปลี่ยนแปลงจะต้องมีการบันทึกไว้และทำการแยกประเภทของการเปลี่ยนแปลงด้วย เช่น เร่งด่วน ฉุกเฉิน เรื่องหลัก เรื่องรอง ซึ่งเมื่อมีการร้องขอการเปลี่ยนแปลงเกิดขึ้นแล้ว จะต้องมีการประเมินถึงความเสี่ยง ผลกระทบ และประโยชน์ที่องค์การจะได้รับ นอกจากนั้นในการบริหารการเปลี่ยนแปลง ยังรวมไปถึงการดำเนินการเพื่อเปลี่ยนแปลงกลับสภาพเดิม หรือดำเนินการแก้ไข กรณีที่การเปลี่ยนแปลงที่เกิดขึ้นไม่ประสบความสำเร็จ โดยวัตถุประสงค์ของการตรวจสอบด้าน Change Management มีดังนี้

ตารางที่ 2.1 Change Management Process

กระบวนการ	รายละเอียด
กระบวนการขอ และการอนุมัติ (Request and Approval)	• จะต้องมีการขอและอนุมัติสำหรับการเปลี่ยนแปลง ซึ่งการขอจะต้องมีการระบุถึงรายละเอียดที่จะมีการเปลี่ยนแปลง ผู้ขอเปลี่ยนแปลง • จะต้องได้รับการอนุมัติจากเจ้าของระบบ ซึ่งจะเป็นฝั่ง Business จะต้องมีการวิเคราะห์ผลกระทบที่อาจจะเกิดขึ้นกับตัวระบบโดยฝั่ง IT • จะต้องได้รับการอนุมัติจากผู้มีอำนาจสูงสุดจากฝั่ง IT ให้สามารถดำเนินการได้
การทดสอบ (Testing)	• เป็นการทดสอบระบบหลังการติดตั้ง หรือแก้ไข ซึ่งจะต้องพิจารณาว่าเหมาะสมกับฟังก์ชั่นการทำงานต่าง ๆ หรือไม่ • UAT (User Acceptance Testing) เป็นการทดสอบจากฝั่งผู้ใช้งาน (User) เพื่อให้มั่นใจว่าตรงกับที่ฝั่งผู้ใช้งานร้องขอไป
การขึ้นระบบ (Deployment and After Deployment Review)	• ในการขึ้นระบบงานจริงจะต้องมีการสอบถาม เพื่อสังเกตการณ์ว่าไม่มีปัญหาใด ๆ เกิดขึ้น การสอบถามนี้จะรวมถึงการแบ่งแยกหน้าที่ของผู้พัฒนาระบบ และผู้ย้ายระบบซึ่งไม่ควรเป็นคนๆ เดียวกันตามหลักการ SOD (Segregation of Duty)

2.1.2.7 Release Management (RLM)

กระบวนการบริหารการส่งมอบจัดให้มีการวางแผนในการส่งมอบการบริการระบบซอฟต์แวร์ และฮาร์ดแวร์ ทั้งนี้แผนในการส่งมอบจะต้องได้รับการเห็นชอบจากผู้ที่เกี่ยวข้องต่างๆ ด้วยไม่ว่าจะเป็นลูกค้า ผู้ให้บริการ เจ้าหน้าที่ดำเนินการ หรือเจ้าหน้าที่สนับสนุน รวมถึงจะต้องมีการบันทึกวันที่มีการส่งมอบและผู้ส่งมอบ การอ้างอิงถึงการร้องขอการเปลี่ยนแปลง ความผิดพลาดที่รับรู้แล้ว และปัญหาที่เกิดขึ้นด้วยการส่งมอบการบริการจะเป็นชุดของรายการปรับแต่งระบบ

(configuration items) ที่ได้รับการทดสอบและนำไปใช้ในสภาพแวดล้อมจริง ทั้งนี้เป้าหมายหลักของการบริหารการส่งมอบ คือ การดำเนินการเพื่อ ให้มั่นใจถึงความสำเร็จของการส่งมอบ รวมถึงการเชื่อมโยงสิ่งต่างๆ เข้าด้วยกัน การทดสอบ และการจัดเก็บ โดยจะดูแลให้มั่นใจว่ามีการส่งมอบเฉพาะรุ่นที่ถูกต้องและผ่านการทดสอบแล้วเท่านั้น ซึ่งกระบวนการบริหารการส่งมอบจะทำงานเชื่อมโยงกันอย่างใกล้ชิดกับกระบวนการบริหารการปรับแต่งระบบ และกระบวนการบริหารการเปลี่ยนแปลง

2.1.2.8 Supplier Management (SPM)

การบริหารซัพพลายเออร์ จะเป็นกระบวนการในการสร้างความมั่นใจว่าผู้ส่งมอบสามารถดำเนินการได้อย่างเรียบร้อย รวมถึงการให้บริการที่มีคุณภาพทั้งนี้ผู้ให้บริการจะต้องมีการจัดทำเป็นเอกสารเกี่ยวกับกระบวนการบริหารผู้ส่งมอบและจะต้องมีรายชื่อของผู้จัดการที่รับผิดชอบผู้ส่งมอบแต่ละรายด้วย โดยข้อกำหนด ขอบเขต ระดับของการบริการ และกระบวนการสื่อสารที่มีการจัดเตรียมไว้โดยผู้ส่งมอบ จะต้องมีการจัดทำเป็นเอกสารข้อตกลงของระดับการให้บริการ (SLA) หรือเอกสารอื่นๆซึ่งข้อตกลงระดับการให้บริการที่ทำกับผู้ส่งมอบ จะต้องสอดคล้องกับข้อตกลงระดับการให้บริการของธุรกิจด้วยบทบาทและความสัมพันธ์ระหว่างผู้ส่งมอบหลักและผู้ส่งมอบที่รับช่วงต่อจะต้องมีการจัดทำเป็นเอกสารอย่างชัดเจนด้วยโดยผู้ส่งมอบหลักจะต้องแสดงให้เห็นถึงกระบวนการที่จะมั่นใจได้ว่าผู้ส่งมอบที่รับจ้างช่วงต่อ สามารถตอบสนองต่อข้อกำหนดที่ได้ตกลงไว้นอกจากนั้นผลการดำเนินงานเทียบกับเป้าหมายของระดับการบริการจะต้องได้รับการวัดและทบทวน และนำไปสู่การปรับปรุงการให้บริการ

2.1.2.9 Information Security Management (ISM)

การบริหารความปลอดภัยของระบบสารสนเทศคือ การปกป้องดูแลคุณค่าของข้อมูลสารสนเทศ ในรูปของการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้ ซึ่งจะต้องสอดคล้องกับการบริหารระดับการให้บริการที่เกี่ยวข้องกับข้อกำหนดในข้อตกลง ข้อกฎหมายและนโยบายขององค์กร การบริหารความปลอดภัยจะประกอบด้วย การปฏิบัติตามข้อกำหนดของนโยบายความปลอดภัยของระบบสารสนเทศ และการบริหารความเสี่ยงที่เกี่ยวข้องกับการบริการ หรือระบบ โดยการควบคุมความปลอดภัยจะต้องมีการจัดทำเป็นเอกสารไว้ด้วย ซึ่งเอกสารจะต้องอธิบายถึงความเสี่ยงที่เกี่ยวกับการควบคุม การดำเนินการ และการดูแลรักษา นอกจากนั้นผลกระทบของการ

เปลี่ยนแปลง จะต้องได้รับการประเมินก่อนที่การเปลี่ยนแปลงนั้นจะได้รับการนำไปปฏิบัติ โดยการการเข้าถึงการใช้งานระบบและการสนับสนุนโครงสร้างพื้นฐานระบบก็ควรจะมีการจำกัดสิทธิอย่างถูกต้อง

2.1.2.9.1Authentication

การพิสูจน์ตัวตน (Authentication) คือ ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

1. Actual identity คือ หลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้นคือใคร
2. Electronic Identity คือ หลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้ แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากกว่า 1 หลักฐาน ตัวอย่างเช่น บัญชีชื่อผู้ใช้

กลไกของการพิสูจน์ตัวตน (Authentication mechanisms) สามารถแบ่งออกได้เป็น 3 คุณลักษณะคือ

1. สิ่งที่คุณมี (Possession factor) เช่น กุญแจ, คีย์การ์ด เป็นต้น
2. สิ่งที่คุณรู้ (Knowledge factor) เช่น บัญชีผู้ใช้งาน (username), รหัสผ่าน (passwords) เป็นต้น
3. สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ, ม่านตา เป็นต้น

กระบวนการพิสูจน์ตัวตนนั้นจะนำ 3 ลักษณะข้างต้นมาใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้าง ทั้งนี้ขึ้นอยู่กับระบบ วิธีการที่นำมาใช้เพียงลักษณะอย่างใดอย่างหนึ่ง (Single-factor authentication) นั้นมีข้อจำกัดในการใช้ ตัวอย่างเช่น สิ่งที่คุณมี (Possession factor) นั้นอาจจะสูญหายหรือถูกขโมยได้ สิ่งที่คุณรู้ (Knowledge factor) อาจจะถูกดักฟัง เดา หรือขโมยจากเครื่องคอมพิวเตอร์ สิ่งที่คุณเป็น (Biometric factor) จัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูงอย่างไรก็ตามการที่จะใช้เทคโนโลยีนี้ได้นั้นจาเป็นต้องมีการลงทุนที่สูง เป็นต้น

ตารางที่ 2.2 ประเภทของการพิสูจน์ตัวตน (Authentication Types)

ประเภทของการพิสูจน์ตัวตน	รายละเอียด
การพิสูจน์ตัวตน (Authentication)	ส่วนที่สำคัญที่สุดเพราะเป็นขั้นตอนแรกของการเข้าใช้ระบบ ผู้เข้าใช้ระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าสู่ระบบได้ การพิสูจน์ตัวตนเป็นการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง
การกำหนดสิทธิ์ (Authorization)	ข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง
การบันทึกการใช้งาน (Accountability)	การบันทึกรายละเอียดของการใช้ระบบและรวมถึงข้อมูลต่าง ๆ ที่ผู้ใช้กระทำลงไปในระบบ เพื่อผู้ตรวจสอบจะได้ตรวจสอบได้ว่า ผู้ใช้ที่เข้ามาใช้บริการได้เปลี่ยนแปลงหรือแก้ไขข้อมูลในส่วนใดบ้าง จากที่ได้กล่าวไปข้างต้นว่าการพิสูจน์ตัวตนมีความสำคัญที่สุดกับการเข้าใช้ระบบ

2.1.2.9.2Logical Access Security

เป็นหลักการในการป้องกันการเข้าถึงข้อมูล ซึ่งมักจะเป็นสิ่งที่จับต้องไม่ได้ มีกระบวนการดังนี้

1. Request and Approval
2. User Accountability
3. Segregation of duty (SOD)
4. Access Right
5. Modification and Removal
6. User Activity Logs
7. Security Patches

2.1.2.9.3Physical Access Security

เป็นหลักการในการป้องกันการเข้าถึงข้อมูลในรูปแบบที่จับต้องได้ ซึ่งจะต่างจากขั้นตอนของ Logical Access Security

2.1.2.10 Business Relationship Management (BRM)

การบริหารความสัมพันธ์ทางธุรกิจนี้จะเป็นการสร้างและรักษาความสัมพันธ์ที่ดีระหว่างผู้ให้บริการ และลูกค้าโดยผู้ให้บริการจะต้องกำหนด และจัดทำเป็นเอกสารในส่วนของผู้มีส่วนได้เสียกับองค์การ และลูกค้าของการให้บริการ ทั้งนี้ ผู้ให้บริการและลูกค้าจะต้องมีการทบทวนร่วมกันถึงรายละเอียดของการให้บริการเมื่อมีการเปลี่ยนแปลงข้อตกลงระดับการให้บริการ ข้อสัญญาหรือความต้องการทางธุรกิจอย่างน้อยปีละหนึ่งครั้ง รวมถึงจะต้องมีการประชุมร่วมกันเพื่อทบทวนถึงผลการดำเนินงาน ผลลัพธ์ที่เกิดขึ้น ประเด็นๆ ต่างที่เกี่ยวข้อง และแผนการปฏิบัติงาน ทั้งนี้ผู้ที่มีส่วนเกี่ยวข้องต่างๆ กับการบริการ จะต้องเข้าร่วมในการประชุมนี้ด้วยนอกจากนั้น ผู้ให้บริการจะต้องจัดให้มีกระบวนการจัดการคำร้องเรียนในงานบริการ โดยจะต้องได้รับการบันทึกโดยผู้ให้บริการค้นหาสาเหตุ ตอบสนอง รายงานและการปิดเรื่อง รวมถึงผู้ให้บริการจะต้องกำหนดผู้รับผิดชอบในการจัดการความพึงพอใจของลูกค้าและตอบสนองต่อการวัดความพึงพอใจของลูกค้าด้วย

2.1.2.11 Budgeting and Accounting for Services (BAM)

การจัดทำงบประมาณและบัญชีค่าใช้จ่าย สำหรับองค์ประกอบทั้งหมดของการให้บริการทางด้าน IT ทั้งนี้กระบวนการการจัดการด้านการเงินจะช่วยให้การบริการด้าน IT เป็นไปอย่างรอบคอบ โดยจะเป็นกระบวนการที่ให้ข้อมูลทางด้านต้นทุนที่เกิดขึ้นจากการให้บริการช่วยให้สามารถทำการตัดสินใจเกี่ยวกับต้นทุนและผลตอบแทนที่จะเกิดขึ้นจากการให้บริการหรือเมื่อมีการเปลี่ยนแปลงการให้บริการหรือโครสร้างพื้นฐานทางด้าน IT ทั้งนี้กระบวนการจะสร้างการรับรู้ทางด้านต้นทุนเพื่อนำไปสู่การจัดสรรงบประมาณให้เหมาะสม

2.1.2.12 Service Continuity and Availability Management (SCM&AVM)

กระบวนการบริหารความต่อเนื่องในการให้บริการ จะเป็นการเตรียมการและการวางแผนสำหรับมาตรการแก้ไขภัยพิบัติ หรือเหตุร้ายที่อาจจะเกิดขึ้น ซึ่งมีผลต่อการบริการด้าน IT และมี

ผลกระทบต่อการดำเนินธุรกิจ หรือในบางกรณีจะเรียกกันว่า การวางแผนเพื่อความสม่ำเสมอ (consistency planning) ซึ่งจะเป็นการเชื่อมโยงมาตรการต่างๆ เพื่อดูแลให้เกิดความต่อเนื่องในการให้บริการ เมื่อเกิดเหตุการณ์ภัยพิบัติขึ้นนอกจากนั้น การบริหารความต่อเนื่องในการให้บริการยังเป็นกระบวนการในการวางแผน และประสานงานทางด้านเทคนิค การเงิน และการจัดการทรัพยากรเพื่อให้มั่นใจได้ว่าจะสามารถรักษาความต่อเนื่องในการให้บริการ ภายหลังจากการเกิดภัยพิบัติตามที่ตกลงไว้กับลูกค้าได้ส่วนการบริหารความพร้อมใช้ในการให้บริการจะเป็นกระบวนการสร้างความมั่นใจว่า ได้มีการจัดการทรัพยากร วิธีการและเทคนิคไว้อย่างเหมาะสมเพื่อสนับสนุนให้เกิดความพร้อมในการให้บริการตามที่ได้ตกลงกับลูกค้า นอกจากนั้นการบริหารความพร้อมใช้ยังครอบคลุมถึงจัดให้มีการบำรุงรักษาอย่างเหมาะสมและออกแบบมาตรการเพื่อลดความไม่ต่อเนื่องในการให้บริการให้เกิดขึ้นน้อยที่สุด

2.1.3 ISO27001 (Information Security Management System : ISMS)

ในปัจจุบันองค์กรได้ทำการศึกษา ISO 27001 (Information Security Management System : ISMS) ที่เกี่ยวกับการจัดการความปลอดภัยของข้อมูล ที่ได้รับการยอมรับในระดับสากล ระบบนี้ทำการประเมินความเสี่ยง การออกแบบด้านการรักษาความปลอดภัยและการนำไปปฏิบัติ รวมถึงการบริหารจัดการความปลอดภัย ซึ่งมีกระบวนการการควบคุมระบบการให้บริการดังต่อไปนี้

2.1.3.1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policies)

ชุดของเอกสารที่ระบุถึงวัตถุประสงค์ เป้าหมาย วิธีการปฏิบัติ เพื่อที่จะรักษาความมั่นคงของข้อมูลเอาไว้ โดยเอกสารนี้จะต้องได้รับการอนุมัติให้มีผลบังคับใช้โดยผู้บริหารระดับสูง และจะต้องสอดคล้องกับแนวทางการ ดำเนินธุรกิจขององค์กรด้วย การที่จะจัดทำนโยบายความมั่นคงของข้อมูลขึ้นมาสำหรับองค์กรใดๆ ไม่ใช่แค่การไปนำคำแนะนำต่างๆ จากมาตรฐาน หรือเอกสารที่หาได้ทั่วไปมาใช้แล้วจะประสบผลสำเร็จ เนื่องจากแต่ละองค์กรก็มีรูปแบบการดำเนินงานและวัฒนธรรมองค์กรที่แตกต่างกันไป ดังนั้นจึงต้องมีกระบวนการในการออกแบบ และพัฒนานโยบายความมั่นคงที่สอดคล้องกับรูปแบบการดำเนินธุรกิจ และความต้องการ ขององค์กร

2.1.3.1.1ทิศทางการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Management Directions for Information Security)

วัตถุประสงค์ เพื่อให้มีการกำหนดทิศทางการบริหารจัดการและการสนับสนุนด้านความมั่นคงปลอดภัยสารสนเทศโดยสอดคล้องกับความต้องการทางธุรกิจและกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

2.1.3.1.1.1 นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ (Policies for Information Security)

นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศต้องมีการจัดทำ อนุมัติโดยผู้บริหาร เผยแพร่และสื่อสารให้พนักงานและหน่วยงานภายนอกที่เกี่ยวข้องได้รับทราบ

2.1.3.1.1.2 การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of The Policies for Information Security)

นโยบายความมั่นคงปลอดภัยต้องมีการทบทวนตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร เพื่อให้นโยบายมีความเหมาะสม เพียงพอ และได้ผล

2.1.3.2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)

2.1.3.2.1โครงสร้างภายในองค์กร (Internal Organization)

วัตถุประสงค์ เพื่อให้มีการกำหนดกรอบการบริหารจัดการ โดยต้องมีการเริ่มต้นและควบคุมการปฏิบัติและการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

2.1.3.2.1.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

หน้าที่ความรับผิดชอบทั้งหมดด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนดและมอบหมายความรับผิดชอบ

2.1.3.2.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

หน้าที่และส่วนงานที่รับผิดชอบที่จะทำให้เกิดการขัดต่อการปฏิบัติงานโดยจะทำให้มีการเปลี่ยนแปลงทรัพย์สินขององค์กรหรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์ โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาก็ตาม ต้องมีการแยกหน้าที่ดังกล่าวออกจากกัน เพื่อลดโอกาสการเกิดขึ้นนั้น

2.1.3.2.1.3 การติดต่อกับหน่วยงานผู้มีอำนาจ (Contact with Authorities)

การติดต่อกับหน่วยงานผู้มีอำนาจที่เกี่ยวข้องต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

2.1.3.2.1.4 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with Special Interest Groups)

การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และสมาคมอาชีพ ต้องมีการรักษาไว้ซึ่งการติดต่อนั้นเพื่อให้สามารถติดต่อได้อย่างต่อเนื่อง

2.1.3.2.1.5 ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information Security in Project Management)

การบริหารโครงการไม่ว่าจะเป็นประเภทใดของโครงการก็ตามต้องมีการระบุความมั่นคงปลอดภัยสารสนเทศของโครงการนั้น

2.1.3.2.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile Devices and Teleworking)

วัตถุประสงค์ เพื่อรักษาความมั่นคงปลอดภัยของการปฏิบัติงานจากระยะไกลและของการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา

2.1.3.2.2.1 นโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile Device Policy)

นโยบายและมาตรการสนับสนุนสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพาต้องมีการนำมาใช้งานเพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว

2.1.3.2.2.2 การปฏิบัติงานจากระยะไกล (Teleworking)

นโยบายและมาตรการสนับสนุนสำหรับการปฏิบัติงานจากสถานที่หนึ่งในระยะไกลต้องมีการนำมาใช้งานเพื่อป้องกันข้อมูลที่มีการเข้าถึง การประมวลผล หรือการจัดเก็บ จากสถานที่ดังกล่าว

2.1.3.3 ความมั่นคงปลอดภัยสำหรับบุคลากร (Human Resource Security)

2.1.3.3.1 ก่อนการจ้างงาน (Prior to Employment)

วัตถุประสงค์ เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทของตนเองที่ได้รับการพิจารณา

2.1.3.3.1.1 การคัดเลือก (Screening)

การตรวจสอบภูมิหลังของผู้สมัครงานต้องมีการดำเนินการโดยมีความสอดคล้องกับกฎหมายระเบียบ ข้อบังคับ และจริยธรรมที่เกี่ยวข้อง และต้องดำเนินการในระดับที่เหมาะสมกับความต้องการทางธุรกิจ ชั้นความลับของข้อมูลที่จะถูกเข้าถึง และความเสี่ยงที่เกี่ยวข้อง

2.1.3.3.1.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)

ข้อตกลงและเงื่อนไขในสัญญาจ้างกับพนักงานและผู้ที่ทำสัญญาจ้างต้องกล่าวถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของพนักงาน ของผู้ที่ทำสัญญาจ้าง และขององค์กร

2.1.3.3.2 ระหว่างการจ้างงาน (During Employment)

วัตถุประสงค์ เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของตนเอง

2.1.3.3.2.1 หน้าที่ความรับผิดชอบของผู้บริหาร (Management Responsibilities)

ผู้บริหารต้องกำหนดให้พนักงานและผู้ที่ทำสัญญาจ้างทั้งหมดรักษาความมั่นคงปลอดภัยสารสนเทศโดยปฏิบัติให้สอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กรที่กำหนดไว้

2.1.3.3.2.2 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)

พนักงานขององค์กรทั้งหมดและผู้ที่ทำสัญญาจ้างที่เกี่ยวข้องต้องได้รับการสร้างความตระหนัก ให้ความรู้ และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ และต้องมีการเรียนรู้และทบทวนเพิ่มเติมในนโยบายและขั้นตอนปฏิบัติขององค์กรที่เกี่ยวข้องกับงานที่ตนเองปฏิบัติ

2.1.3.3.2.3 กระบวนการทางวินัย (Disciplinary Process)

กระบวนการทางวินัยต้องมีการกำหนดอย่างเป็นทางการและมีการสื่อสารให้พนักงานได้รับทราบ เพื่อดำเนินการต่อพนักงานที่ละเมิดความมั่นคงปลอดภัยสารสนเทศขององค์กร

2.1.3.3.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

วัตถุประสงค์ เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของกระบวนการเปลี่ยนหรือสิ้นสุดการจ้างงาน

2.1.3.3.3.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or Change of Employment Responsibilities)

หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่ยังต้องคงไว้หลังการสิ้นสุดหรือเปลี่ยนการจ้างงาน ต้องมีการกำหนดและสื่อสารให้ได้รับทราบต่อพนักงานหรือผู้ที่ทำสัญญาจ้างรวมทั้งควบคุมให้ปฏิบัติตามอย่างสอดคล้อง

2.1.3.4 การบริหารจัดการทรัพย์สิน (Asset Management)

2.1.3.4.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)

วัตถุประสงค์ เพื่อให้มีการระบุทรัพย์สินขององค์กรและกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

2.1.3.4.1.1 บัญชีทรัพย์สิน (Inventory of Assets)

ทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องมีการระบุจัดทำเป็นทะเบียนทรัพย์สิน และปรับปรุงให้ทันสมัย

2.1.3.4.1.2 ผู้ถือครองทรัพย์สิน (Ownership of Assets)

ทรัพย์สินในทะเบียนทรัพย์สินต้องมีผู้ถือครองทรัพย์สิน

2.1.3.4.1.3 การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable Use of Assets)

กฎเกณฑ์การใช้อย่างเหมาะสมสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการระบุ จัดทำเป็นลายลักษณ์อักษร และบังคับใช้ให้เป็นไปอย่างสอดคล้อง

2.1.3.4.1.4 การคืนทรัพย์สิน (Return of Assets)

พนักงานและลูกจ้างของหน่วยงานภายนอกทั้งหมดต้องคืนทรัพย์สินขององค์กรทั้งหมดที่ตนเองถือครอง เมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง

2.1.3.4.2 การจัดชั้นความลับของสารสนเทศ (Information Classification)

วัตถุประสงค์ เพื่อให้สารสนเทศได้รับระดับการป้องกันที่เหมาะสมโดยสอดคล้องกับความสำคัญของสารสนเทศนั้นที่มีต่อองค์กร

2.1.3.4.2.1 ชั้นความลับของสารสนเทศ (Classification of Information)

สารสนเทศต้องมีการจัดชั้นความลับโดยพิจารณาจากความต้องการด้านกฎหมาย คุณค่า ระดับความสำคัญ และระดับความอ่อนไหวหากถูกเปิดเผยหรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

2.1.3.4.2.2 การบ่งชี้สารสนเทศ (Labeling of Information)

ขั้นตอนปฏิบัติสำหรับการบ่งชี้สารสนเทศต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้

2.1.3.4.2.3 การจัดการทรัพย์สิน (Handling of Assets)

ขั้นตอนปฏิบัติสำหรับการจัดการทรัพย์สินต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้

2.1.3.4.3 การจัดการสื่อบันทึกข้อมูล (Media Handling)

วัตถุประสงค์ เพื่อป้องกันการเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายสารสนเทศที่จัดเก็บอยู่บนสื่อบันทึกข้อมูล

2.1.3.4.3.1 การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ (Management of Removable Media)

ขั้นตอนปฏิบัติสำหรับการบริหารจัดการกับสื่อบันทึกข้อมูลที่ถอดแยกได้ต้องมีการจัดทำและปฏิบัติตาม โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้

2.1.3.4.3.2 การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

สื่อบันทึกข้อมูลต้องมีการกำจัดหรือทำลายทิ้งอย่างมั่นคงปลอดภัย เมื่อหมดความต้องการในการใช้งาน โดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายซึ่งกำหนดไว้อย่างเป็นทางการ

2.1.3.4.3.3 การขนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น

2.1.3.5 การควบคุมการเข้าถึง (Access Control)

2.1.3.5.1 ความต้องการทางธุรกิจสำหรับการควบคุมการเข้าถึง (Business Requirements of Access Control)

วัตถุประสงค์ เพื่อจำกัดการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

2.1.3.5.1.1 นโยบายควบคุมการเข้าถึง (Access Control Policy)

นโยบายควบคุมการเข้าถึงต้องมีการกำหนด จัดทำเป็นลายลักษณ์อักษร และทบทวนตามความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

2.1.3.5.1.2 การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Networks and Network Services)

ผู้ใช้งานต้องได้รับสิทธิการเข้าถึงเฉพาะเครือข่ายและบริการเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น

2.1.3.5.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

วัตถุประสงค์ เพื่อควบคุมการเข้าถึงของผู้ใช้งานเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงระบบและบริการโดยไม่ได้รับอนุญาต

2.1.3.5.2.1 การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User Registration and Deregistration)

กระบวนการลงทะเบียนและถอดถอนสิทธิผู้ใช้งานอย่างเป็นทางการต้องมีการปฏิบัติตามเพื่อเป็นการให้สิทธิการเข้าถึง

2.1.3.5.2.2 การจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Provisioning)

กระบวนการจัดการสิทธิการเข้าถึงของผู้ใช้งานต้องมีการปฏิบัติตาม ทั้งให้และถอดถอนสิทธิการเข้าถึงสำหรับผู้ใช้งานทุกประเภทและทุกระบบและบริการทั้งหมดขององค์กร

2.1.3.5.2.3 การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ (Management of Privileged Access Right)

การให้และใช้สิทธิการเข้าถึงตามระดับสิทธิต้องมีการจำกัดและควบคุม

2.1.3.5.2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of Users)

การมอบข้อมูลการพิสูจน์ ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับต้องมีการควบคุมโดยผ่านกระบวนการบริหารจัดการที่เป็นทางการ

2.1.3.5.2.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

เจ้าของทรัพย์สินต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานตามรอบระยะเวลาที่กำหนดไว้

2.1.3.5.2.6 การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง (Removal or Adjustment of Access Rights)

สิทธิการเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง หรือต้องได้รับการปรับปรุงให้ถูกต้องเมื่อมีการเปลี่ยนการจ้างงาน

2.1.3.5.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลการพิสูจน์ตัวตน

2.1.3.5.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)

ผู้ใช้งานต้องดำเนินตามวิธีปฏิบัติขององค์กรสำหรับการใช้งานข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ

2.1.3.5.4 การควบคุมการเข้าถึงระบบ (System and Application Access Control)

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

2.1.3.5.4.1 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมี การจำกัดให้ สอดคล้องกับนโยบายควบคุมการเข้าถึง

2.1.3.5.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedures)

กรณีมีการกำหนดโดยนโยบายควบคุมการเข้าถึง การเข้าถึงระบบต้องมีการควบคุมโดยผ่านทางขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย

2.1.3.5.4.3 ระบบบริหารจัดการรหัสผ่าน (Password Management System)

ระบบบริหารจัดการรหัสผ่านต้องมีปฏิสัมพันธ์กับผู้ใช้งานและบังคับการตั้งรหัสผ่านที่มีคุณภาพ

2.1.3.5.4.4 การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

2.1.3.5.4.5 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access Control to Program Source Code)

การเข้าถึงซอร์สโค้ดของโปรแกรมต้องมีการจำกัดและควบคุม

2.1.3.6 การเข้ารหัสข้อมูล (Cryptography)

2.1.3.6.1 มาตรการเข้ารหัสข้อมูล (Cryptographic Controls)

วัตถุประสงค์ เพื่อให้มีการใช้การเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผลและป้องกันความลับการปลอมแปลง หรือความถูกต้องของสารสนเทศ

2.1.3.6.1.1 นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

นโยบายการใช้มาตรการเข้ารหัสข้อมูลเพื่อป้องกันสารสนเทศต้องมีการจัดทำและปฏิบัติตาม

2.1.3.6.1.2 การบริหารจัดการกุญแจ (Key management)

นโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจ ต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ

2.1.3.7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

2.1.3.7.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure Areas)

วัตถุประสงค์ เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต ความเสียหาย และการแทรกแซงการทำงาน ที่มีต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

2.1.3.7.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter)

ขอบเขตหรือบริเวณโดยรอบพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการกำหนดขึ้นมาเพื่อใช้ในการป้องกันพื้นที่สำคัญดังกล่าวอันประกอบไปด้วยสารสนเทศหรืออุปกรณ์

2.1.3.7.1.2 การควบคุมการเข้าออกทางกายภาพ (Physical Entry Controls)

พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการป้องกันโดยมีการควบคุมการเข้าออกอย่างเหมาะสม โดยกำหนดให้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้นที่สามารถเข้าถึงพื้นที่สำคัญได้

2.1.3.7.1.3 การรักษาความมั่นคงปลอดภัยสำหรับ สำนักงาน ห้องทำงาน และอุปกรณ์ (Securing Office, Room and Facilities)

ความมั่นคงปลอดภัยทางกายภาพของสำนักงาน ห้องทำงาน และอุปกรณ์ต่างๆ ต้องมีการออกแบบและดำเนินการ

2.1.3.7.1.4 การป้องกันต่อภัยคุกคามจากภายนอกและสภาพแวดล้อม (Protecting Against External End Environmental Threats)

การป้องกันทางกายภาพต่อภัยพิบัติทางธรรมชาติ การโจมตีหรือการบุกรุก หรืออุบัติเหตุ ต้องมีการออกแบบและดำเนินการ

2.1.3.7.1.5 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in Secure Areas)

ขั้นตอนปฏิบัติสำหรับการปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย ต้องมีการจัดทำและปฏิบัติตาม

2.1.3.7.1.6 พื้นที่สำหรับรับส่งสิ่งของ (Delivery and Loading Areas)

จุดหรือบริเวณที่สามารถเข้าถึงองค์กร เช่น พื้นที่สำหรับรับส่งสิ่งของ บริเวณอื่นๆ ที่ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่ขององค์กรได้ ต้องมีการควบคุม และหากเป็นไปได้ จุดหรือบริเวณดังกล่าวควรแยกออกมาจากบริเวณที่มีอุปกรณ์ประมวลผลสารสนเทศ เพื่อหลีกเลี่ยงการเข้าถึงโดยไม่ได้รับอนุญาต

2.1.3.7.2 อุปกรณ์ (Equipment)

วัตถุประสงค์ เพื่อป้องกัน การสูญหาย การเสียหาย การขโมย หรือ การเป็นอันตรายต่อทรัพย์สินและป้องกันการหยุดชะงักต่อการดำเนินงานขององค์กร

2.1.3.7.2.1 การจัดตั้งและป้องกันอุปกรณ์ (Equipment Sitting and Protection)

อุปกรณ์ต้องมีการจัดตั้งและป้องกันเพื่อลดความเสี่ยงจากภัย คุกคามและอันตรายด้านสภาพแวดล้อม และจากโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต

2.1.3.7.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

อุปกรณ์ต้องได้รับการป้องกันจากการล้มเหลวของกระแสไฟฟ้าและการหยุดชะงักอื่นๆ ที่มีสาเหตุมาจากการล้มเหลวของระบบและอุปกรณ์สนับสนุนการทำงานต่างๆ

2.1.3.7.2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling Security)

การเดินสายไฟฟ้าและสายสื่อสารโทรคมนาคม ซึ่งส่งข้อมูลหรือสนับสนุนบริการสารสนเทศต้องมีการป้องกันจากการขัดขวางการทำงาน การแทรกแซงสัญญาณ หรือการทำให้เสียหาย

2.1.3.7.2.4 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

อุปกรณ์ต้องได้รับการบำรุงรักษาอย่างถูกต้องเพื่อให้มีสภาพความพร้อมใช้งานและการทำงานที่ถูกต้องอย่างต่อเนื่อง

2.1.3.7.2.5 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of Assets)

อุปกรณ์ สารสนเทศ หรือซอฟต์แวร์ ต้องไม่มีการนำออกนอกสำนักงาน โดยปราศจากการขออนุญาตก่อน

2.1.3.7.2.6 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Security of Equipment and Assets Off- Premises)

ทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงานต้องมีการรักษาความมั่นคงปลอดภัยโดยพิจารณาจากความเสี่ยงของการปฏิบัติงานอยู่ภายนอกสำนักงาน

2.1.3.7.2.7 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure Disposal or Re-Use of Equipment)

อุปกรณ์ที่มีสื่อบันทึกข้อมูลต้องมีการตรวจสอบเพื่อให้มั่นใจว่าข้อมูลสำคัญและซอฟต์แวร์ที่มีใบอนุญาตมีการลบทิ้งหรือเขียนทับอย่างมั่นคงปลอดภัย ก่อนการกำจัดอุปกรณ์ หรือก่อนการนำอุปกรณ์ไปใช้งานอย่างอื่น

2.1.3.7.2.8 อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended User Equipment)

ผู้ใช้งานต้องมีการป้องกันอุปกรณ์อย่างเหมาะสม ซึ่งเป็นอุปกรณ์ที่ทิ้งไว้ในสถานที่หนึ่ง ณ ช่วงเวลาหนึ่งโดยไม่มีผู้ดูแล

2.1.3.7.2.9 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

นโยบาย “โต๊ะทำงานปลอดเอกสารสำคัญ” เพื่อป้องกันเอกสารกระดาษและสื่อบันทึกข้อมูลที่ถอดแยกได้ และนโยบาย “การป้องกันหน้าจอคอมพิวเตอร์” เพื่อป้องกันสารสนเทศในอุปกรณ์ประมวลผลสารสนเทศ ต้องมีการนำมาใช้งาน (เพื่อป้องกันการเข้าถึงทางกายภาพต่อเอกสารและข้อมูลสำคัญขององค์กร

2.1.3.8 ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)

2.1.3.8.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities)

วัตถุประสงค์ เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

2.1.3.8.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented Operating Procedures)

ขั้นตอนการปฏิบัติงานต้องมีการจัดทำเป็นลายลักษณ์อักษรและต้องสามารถเข้าถึงได้โดยผู้ที่จำเป็นต้องใช้งาน

2.1.3.8.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change Management)

การเปลี่ยนแปลงต่อองค์กร กระบวนการทางธุรกิจ อุปกรณ์ประมวลผลสารสนเทศ และระบบที่มีผลต่อความมั่นคงปลอดภัยสารสนเทศ ต้องมีการควบคุมการดำเนินการ

2.1.3.8.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

การใช้ทรัพยากรของระบบต้องมีการติดตาม ปรับปรุง และคาดการณ์ความต้องการเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพตามที่ต้องการ

2.1.3.8.1.4 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of Development, Testing and Operational Environments)

สภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการ ต้องมีการจัดทำแยกกันเพื่อลดความเสี่ยงของการเข้าถึงหรือการเปลี่ยนแปลงสภาพแวดล้อมสำหรับการให้บริการโดยไม่ได้รับอนุญาต

2.1.3.8.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์ เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศได้รับการป้องกันจากโปรแกรมไม่ประสงค์ดี

2.1.3.8.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls Against Malware)

มาตรการตรวจหา การป้องกัน และการกู้คืนจากโปรแกรมไม่ประสงค์ดีต้องมีการดำเนินการร่วมกับการสร้างความตระหนักผู้ใช้งานที่เหมาะสม

2.1.3.8.3 การสำรองข้อมูล (Backup)

วัตถุประสงค์ เพื่อป้องกันการสูญหายของข้อมูล

2.1.3.8.3.1 การสำรองข้อมูล (Information Backup)

ข้อมูลสำรองสำหรับสารสนเทศ ซอฟต์แวร์ และอิมเมจของระบบ ต้องมีการดำเนินการสำรองไว้และมีการทดสอบความพร้อมใช้ของข้อมูลอย่างสม่ำเสมอตามนโยบายการสำรองข้อมูลที่ได้ตกลงไว้

2.1.3.8.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

วัตถุประสงค์ เพื่อให้มีการบันทึกเหตุการณ์และจัดทำหลักฐาน

2.1.3.8.4.1 การบันทึกข้อมูลล็อกแสดงเหตุการณ์ (Event Logging)

ข้อมูลล็อกแสดงเหตุการณ์ซึ่งบันทึกกิจกรรมของผู้ใช้งาน การทำงานของระบบที่ไม่เป็นไปตามขั้นตอนปกติ ความผิดพลาดในการทำงานของระบบ และเหตุการณ์ความมั่นคงปลอดภัยต้องมีการบันทึกไว้ จัดเก็บ และทบทวนอย่างสม่ำเสมอ

2.1.3.8.4.2 การป้องกันข้อมูลล็อก (Protection of Log Information)

อุปกรณ์บันทึกข้อมูลล็อกและข้อมูลล็อกต้องได้รับการป้องกันจากการเปลี่ยนแปลงแก้ไขและการเข้าถึงโดยไม่ได้รับอนุญาต

2.1.3.8.4.3 ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and Operator Logs)

กิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการต้องมีการบันทึกไว้เป็นข้อมูลล็อก ข้อมูลดังกล่าวต้องมีการป้องกันและทบทวนอย่างสม่ำเสมอ

2.1.3.8.4.4 การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)

นาฬิกาของระบบที่เกี่ยวข้องทั้งหมดภายในองค์กรหรือในขอบเขตหนึ่ง ต้องมีการตั้งให้ตรงและถูกต้องเทียบกับแหล่งอ้างอิงเวลาแห่งหนึ่ง

2.1.3.8.5 การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ (Control of Operational Software)

วัตถุประสงค์ เพื่อให้ระบบให้บริการมีการทำงานที่ถูกต้อง

2.1.3.8.5.1 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of Software on Operational Systems)

ขั้นตอนปฏิบัติสำหรับการควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการต้องมีการปฏิบัติตามให้สอดคล้อง

2.1.3.8.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์ เพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ทางเทคนิค

2.1.3.8.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ข้อมูลเกี่ยวกับช่องโหว่ทางเทคนิคของระบบที่ใช้งานต้องมีการติดตามอย่างทันกาล จุดอ่อนต่อช่องโหว่ดังกล่าวขององค์กรต้องมีการประเมิน และมาตรการที่เหมาะสมต้องถูกนำมาใช้เพื่อจัดการกับความเสี่ยงที่เกี่ยวข้อง

2.1.3.8.6.2 การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

กฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งานต้องมีการกำหนดและปฏิบัติตาม

2.1.3.8.7สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit Considerations)

วัตถุประสงค์ เพื่อลดผลกระทบของกิจกรรมการตรวจประเมินบนระบบให้บริการ

2.1.3.8.7.1 มาตรการการตรวจประเมินระบบ (Information Systems Audit Controls)

ความต้องการในการตรวจประเมินและกิจกรรมการตรวจประเมินระบบให้บริการต้องมีการวางแผนและตกลงร่วมกันอย่างระมัดระวังเพื่อลดโอกาสการหยุดชะงักที่มีต่อกระบวนการทางธุรกิจ

2.1.3.9 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

2.1.3.9.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Network Security Management)

วัตถุประสงค์ เพื่อให้มีการป้องกันสารสนเทศในเครือข่ายและอุปกรณ์ประมวลผลสารสนเทศ

2.1.3.9.1.1 มาตรการเครือข่าย (Network Controls)

เครือข่ายต้องมีการบริหารจัดการและควบคุมเพื่อป้องกันสารสนเทศในระบบต่างๆ

2.1.3.9.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of Network Services)

กลไกด้านความมั่นคงปลอดภัย ระดับการให้บริการ และความต้องการในส่วนของผู้บริหารสำหรับบริการเครือข่ายทั้งหมด ต้องมีการระบุและรวมไว้ในข้อตกลงการให้บริการเครือข่าย ไม่ว่าบริการเหล่านี้จะมีการให้บริการโดยองค์กรเองหรือจ้างการให้บริการก็ตาม

2.1.3.9.1.3 การแบ่งแยกเครือข่าย (Segregation in Networks)

กลุ่มของบริการสารสนเทศ ผู้ใช้งาน และระบบ ต้องมีการจัดแบ่งเครือข่ายตามกลุ่มที่กำหนด

2.1.3.9.2 การถ่ายโอนสารสนเทศ (Information Transfer)

วัตถุประสงค์ เพื่อให้มีการรักษาความมั่นคงปลอดภัยของสารสนเทศที่มีการถ่ายโอนภายในองค์กรและถ่ายโอนกับหน่วยงานภายนอก

2.1.3.9.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information Transfer Policies and Procedures)

นโยบาย ขั้นตอนปฏิบัติ และมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการต้องมีการปฏิบัติเพื่อป้องกันสารสนเทศที่มีการถ่ายโอน โดยผ่านทางการใช้อุปกรณ์การสื่อสารทุกประเภท

2.1.3.9.2.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on Information Transfer)

ข้อตกลงสำหรับการถ่ายโอนสารสนเทศทางธุรกิจให้มีความมั่นคงปลอดภัยต้องมีการระบุระหว่างองค์กรกับหน่วยงานภายนอก

2.1.3.9.2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic Messaging)

สารสนเทศที่เกี่ยวข้องกับการส่งข้อความทางอิเล็กทรอนิกส์ต้องได้รับการป้องกันอย่างเหมาะสม

2.1.3.9.2.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or Non-Disclosure Agreements)

ความต้องการในการรักษาความลับหรือการไม่เปิดเผยความลับซึ่งสะท้อนถึงความจำเป็นขององค์กรในการป้องกันสารสนเทศ ต้องมีการระบุ ทบทวนอย่างสม่ำเสมอ และบันทึกไว้อย่างเป็นลายลักษณ์อักษร

2.1.3.10 การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System Acquisition, Development and Maintenance)

2.1.3.10.1 ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security Requirements of Information Systems)

วัตถุประสงค์ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศเป็นองค์ประกอบสำคัญหนึ่งของระบบตลอดวงจรชีวิตของการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านระบบที่มีการให้บริการผ่านเครือข่ายสาธารณะด้วย

2.1.3.10.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Requirements Analysis and Specification)

ความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศต้องมีการรวมเข้ากับความต้องการสำหรับระบบใหม่หรือการปรับปรุงระบบที่มีอยู่แล้ว

2.1.3.10.1.2 ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing Application Services on Public Networks)

สารสนเทศที่เกี่ยวข้องกับบริการสารสนเทศซึ่งมีการส่งผ่านเครือข่ายสาธารณะต้องได้รับการป้องกันจากการฉ้อโกง การโต้เถียง และการเปิดเผยและการเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต

2.1.3.10.1.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting Application Services Transactions)

สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่ง ข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รบอนุญาต การส่งข้อความซ้ำโดยไม่ได้รับอนุญาต

2.1.3.10.2 ความมันคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in Development and Support Processes)

วัตถุประสงค์ เพื่อให้ความมั่นคงปลอดภัยสารสนเทศมีการออกแบบและดำเนินการตลอดวงจรชีวิตของการพัฒนาระบบ

2.1.3.10.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure Development Policy)

กฎเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบต้องมีการกำหนดและปฏิบัติตามสำหรับการพัฒนาระบบขององค์กร

2.1.3.10.2.2 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change Control Procedures)

การเปลี่ยนแปลงระบบในวงจรชีวิตของการพัฒนาระบบต้องมีการควบคุมโดยปฏิบัติตามขั้นตอนปฏิบัติสำหรับการเปลี่ยนแปลงระบบที่กำหนดไว้อย่างเป็นทางการ

2.1.3.10.2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical Review of Applications After Operating Platform Changes)

เมื่อมีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบระบบสำคัญต้องมีการทบทวนและทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบในทางลบต่อการปฏิบัติงานหรือด้านความมั่นคงปลอดภัยขององค์กร

2.1.3.10.2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)

การเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูปต้องไม่อนุญาตการดำเนินการ จำกัดการเปลี่ยนแปลงเท่าที่จำเป็น และต้องมีการควบคุมอย่างรัดกุม

2.1.3.10.2.5 หลักการวิศวะกรรมระบบด้านความมั่นคงปลอดภัย (Secure System Engineering Principles)

หลักการวิศวกรรมระบบให้มีความมั่นคงปลอดภัยต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร ปรับปรุงอย่างต่อเนื่อง และประยุกต์กับงานการพัฒนาระบบ

2.1.3.10.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure Development Environment)

องค์กรต้องจัดทำและป้องกันอย่างเหมาะสมต่อสภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย ทั้งการพัฒนาและปรับปรุงระบบเพิ่มเติมตลอดวงจรชีวิตของการพัฒนาระบบ

2.1.3.10.2.7 การจ้างหน่วยงานภายนอกพัฒนาระบบ (Outsourced Development)

องค์กรต้องกำกับดูแลเฝ้าระวังและติดตามกิจกรรมการพัฒนาระบบที่จ้างหน่วยงานภายนอกเป็นผู้ดำเนินการ

2.1.3.10.2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System Security Testing)

การทดสอบคุณสมบัติด้านความมั่นคงปลอดภัยของระบบต้องมีการดำเนินการในระหว่างที่ระบบอยู่ในช่วงการพัฒนา

2.1.3.10.2.9 การทดสอบเพื่อรับรองระบบ (System Acceptance Testing)

แผนการทดสอบและเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ ต้องมีการจัดทำสำหรับระบบใหม่ ระบบที่ปรับปรุง และระบบเวอร์ชั่นใหม่

2.1.3.10.3 ข้อมูลสำหรับการทดทดสอบ (Test Data)

วัตถุประสงค์ เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

2.1.3.10.3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

ข้อมูลสำหรับการทดสอบระบบต้องมีการคัดเลือกอย่างระมัดระวัง มีการป้องกัน และควบคุมการนำมาใช้งาน

2.1.3.11 ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier Relationships)

2.1.3.11.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security in Supplier Relationship)

วัตถุประสงค์ เพื่อให้มีการป้องกันทรัพย์สินขององค์กรที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

2.1.3.11.1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information Security Policy for Supplier Relationships)

ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศเพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงทรัพย์สินขององค์กรโดยผู้ให้บริการภายนอก ต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอก และจัดทำเป็นลายลักษณ์อักษร

2.1.3.11.1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing Security within Supplier Agreements)

ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศต้องมีการกำหนดและตกลงกับผู้ให้บริการภายนอกในเรื่องที่เกี่ยวข้องกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการโครงสร้างพื้นฐานของระบบสำหรับ สารสนเทศขององค์กรโดยผู้ให้บริการภายนอก

2.1.3.11.1.3 ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and Communication Technology Supply Chain)

ข้อตกลงกับผู้ให้บริการภายนอกต้องรวมความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก

2.1.3.11.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier Service Delivery Management)

วัตถุประสงค์ เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัยและระดับการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการของผู้ให้บริการภายนอก

2.1.3.11.2.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and Review of Supplier Services)

องค์กรต้องมีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

2.1.3.11.2.2 การบริหารจัดการการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอก รวมทั้งการปรับปรุงนโยบาย ขั้นตอนปฏิบัติ และมาตรการที่ใช้อยู่ในปัจจุบัน ต้องมีการบริหารจัดการ โดยต้องนำระดับความสำคัญของสารสนเทศ ระบบ และกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วย และต้องทบทวนการประเมินความเสี่ยงใหม่

2.1.3.12 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

2.1.3.12.1 การบริหารจัดการเหตุการณ์ ความมั่น คงปลอดภัย สารสนเทศและการปรับปรุง (Management of Information Security Incidents and Improvements)

วัตถุประสงค์ เพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการแจ้งสถานการณ์ความมั่นคงปลอดภัยสารสนเทศและจุดอ่อนความมั่นคงปลอดภัยสารสนเทศให้ได้รับทราบ

2.1.3.12.1.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการบริหารจัดการต้องมีการกำหนดเพื่อให้มีการตอบสนองอย่างรวดเร็ว ได้ผล และตามลำดับต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

2.1.3.12.1.2 การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Events)

สถานการณ์ความมั่นคงปลอดภัยสารสนเทศต้องมีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้

2.1.3.12.1.3 การรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศ (Reporting Information Security Weaknesses)

พนักงานและผู้ที่ทำสัญญาจ้างซึ่งใช้ระบบและบริการสารสนเทศขององค์กรต้องสังเกตและรายงานจุดอ่อนความมั่นคงปลอดภัยสารสนเทศในระบบหรือบริการที่สังเกตพบหรือที่สงสัย

2.1.3.12.1.4 การประเมิน และตัด สินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and Decision on Information Security Events)

สถานการณ์ ความมั่น คงปลอดภัย สารสนเทศต้องมีการประเมิน และต้องมีการตัดสินว่าสถานการณ์นั้นเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่

2.1.3.12.1.5 การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to Information Security Incidents)

เหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

2.1.3.12.1.6 การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning from Information Security Incidents)

ความรู้ที่ได้รับจากการวิเคราะห์และแก้ไขเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องถูกนำมาใช้เพื่อลดโอกาสหรือผลกระทบของเหตุการณ์ความมั่นคงปลอดภัยที่จะเกิดขึ้นในอนาคต

2.1.3.12.1.7 การเก็บรวบรวมหลักฐาน (Collection of Evidence)

องค์กรต้องกำหนดและประยุกต์ใช้ขั้นตอนปฏิบัติสำหรับการระบุ การรวบรวม การจัดหาและการจัดเก็บสารสนเทศซึ่งสามารถใช้เป็นหลักฐาน

2.1.3.13 ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

2.1.3.13.1 ความต่อเนื่องด้านความมันคงปลอดภัยสารสนเทศ (Information Security Continuity)

2.1.3.13.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศและด้านความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติหนึ่ง

2.1.3.13.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing Information Security Continuity)

องค์กรต้องกำหนด จัดทำเป็นลายลักษณ์อักษร ปฏิบัติ และปรับปรุง กระบวนการ ขั้นตอนปฏิบัติ และมาตรการ เพื่อให้ได้ระดับความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เมื่อมีสถานการณ์ความเสียหายหนึ่งเกิดขึ้น

2.1.3.13.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, Review and Evaluate Information Security Continuity)

องค์กรต้องมีการตรวจสอบมาตรการสร้างความต่อเนื่องที่ได้เตรียมการไว้ตามรอบระยะเวลาที่กำหนดไว้ เพื่อให้มั่นใจว่ามาตรการเหล่านั้นยังถูกต้องและได้ผลเมื่อมีสถานการณ์ความเสียหายเกิดขึ้น

2.1.3.13.2 การเตรียมการอุปกรณ์ประมวลผลสำรอง (Redundancies)

วัตถุประสงค์ เพื่อจัดเตรียมสภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ

2.1.3.13.2.1 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of Information Processing Facilities)

อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้อย่างเพียงพอเพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนดไว้

2.1.3.14 ความสอดคล้อง (Compliance)

2.1.3.14.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

วัตถุประสงค์ เพื่อหลีกเลี่ยงการละเมิดข้อผูกพันในกฎหมาย ระเบียบข้อบังคับ หรือสัญญาจ้าง ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และที่เป็นความต้องการด้านความมั่นคงปลอดภัย

2.1.3.14.1.1 การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of Applicable Legislation and Contractual Requirements)

ความต้องการทั้งหมดที่เกี่ยวข้องกับกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้างรวมทั้งวิธีการขององค์กรเพื่อให้สอดคล้องกับความต้องการดังกล่าว ต้องมีการระบุอย่างชัดเจน จัดทำเป็นลายลักษณ์อักษร และปรับปรุงให้ทันสมัย สำหรับแต่ละระบบและสำหรับองค์กร

2.1.3.14.1.2 สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)

ขั้นตอนปฏิบัติที่เหมาะสมต้องได้รับการปฏิบัติอย่างสอดคล้องเพื่อให้มั่นใจว่ามีความสอดคล้องกับความต้องการของกฎหมาย ระเบียบข้อบังคับ และสัญญาจ้าง ที่ว่าด้วยเรื่องสิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์

2.1.3.14.1.3 การป้องกันข้อมูล (Protection of Records)

ข้อมูลขององค์กรต้องได้รับการป้องกันจากการสูญหาย การถูกทำลาย การปลอมแปลง การเข้าถึงโดยไม่ได้รับอนุญาต และการเผยแพร่โดยไม่ได้รับอนุญาต โดยต้องสอดคล้องกับความต้องการของกฎหมาย ระเบียบข้อบังคับ สัญญาจ้าง และความต้องการทางธุรกิจ

2.1.3.14.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and Protection of Personal Identifiable Information)

ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคลต้องมีการดำเนินการให้ สอดคล้องกับกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

2.1.3.14.1.5 ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Regulation of Cryptographic Controls)

มาตรการเข้ารหัสข้อมูลต้องมีการใช้ให้สอดคล้องกับข้อตกลงกฎหมายและระเบียบข้อบังคับทั้งหมดที่เกี่ยวข้อง

2.1.3.14.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

วัตถุประสงค์ เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศอย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

2.1.3.14.2.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent Review of Information Security)

วิธีการในการบริหารจัดการความมั่น คงปลอดภัย สารสนเทศและการปฏิบัติขององค์กร (กล่าวคือ วัตถุประสงค์ มาตรการ นโยบาย กระบวนการ และขั้นตอนปฏิบัติเพื่อความมั่นคงปลอดภัยสารสนเทศ) ต้องมีการทบทวนอย่างอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงองค์กรที่มากเกิดขึ้น

2.1.3.14.2.2 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with Security Policies and Standards)

ผู้จัดการต้องดำเนินการทบทวนความสอดคล้องอย่างสม่ำเสมอของการประมวลผลสารสนเทศและขั้นตอนปฏิบัติที่อยู่ภายใต้ความรับผิดชอบของตนเอง โดยเทียบกับนโยบายมาตรฐานและความต้องการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

2.1.3.14.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

ระบบต้องได้รับการทบทวนอย่างสม่ำเสมอเพื่อพิจารณาความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

2.1.4 PDCA / KAIZEN

PDCA เป็นแนวคิดหนึ่ง ที่ไม่ได้ให้ความสำคัญเพียงแค่การวางแผน แต่แนวคิดนี้เน้นให้การดาเนินงานเป็นไปอย่างมีระบบ โดยมีเป้าหมายให้เกิดการพัฒนาอย่างต่อเนื่อง วงจรนี้มีอีกชื่อหนึ่งว่า “Deming Cycle”

2.1.4.1 โครงสร้างของ PDCA ประกอบด้วย

1) Plan คือ การวางแผน
2) Do คือ การปฏิบัติตามแผน
3) Check คือ การตรวจสอบ
4) Act หรือ Action คือ การปรับปรุงการดำเนินการอย่างเหมาะสม หรือ การจัดทำมาตรฐานใหม่ ซึ่งถือเป็นพื้นฐานของการยกระดับคุณภาพ

ขั้นตอนการบริหารกิจกรรมการเพิ่มประสิทธิภาพการดำเนินการสอดคล้องกับแนวทางของ PDCA นั้น จะเป็นไปอย่างมีระบบ และครบถ้วน ซึ่งก็จะทำให้กิจกรรมการเพิ่มประสิทธิภาพมีความเหมาะสมกับองค์กร จากการที่มีการสำรวจสถานการณ์ขององค์กรในประเด็นต่าง ๆ ไม่ว่าจะเป็นด้านการผลิต หรือ ด้านบุคลากร เพื่อมาใช้เป็นข้อมูลป้อนเข้าสำหรับการวางแผน และกำหนดแนวทางการดำเนินงาน มีการตรวจสอบประเมินผลเป็นระยะทำให้สามารถปรับแผนให้สอดคล้องกับสถานการณ์ได้ อีกทั้งยังมีการวิเคราะห์ผลสำเร็จของโครงการทำให้รู้ถึงจุดอ่อน จุดแข็งของการดำเนินงาน และถือเป็นบทเรียนสำหรับการดำเนินงานต่อไป และตรงจุดนี้เองที่จะทำให้สามารถ

ยกระดับการปรับปรุง และพัฒนาได้จริง จึงมีโอกาสที่การพัฒนาต่อยอดจะเป็นไปอย่างเหมาะสม และถูกทิศทาง

การดำเนินงาน ไม่ว่าจะเป็นการปรับปรุงผ่านเครื่องมือการเพิ่มประสิทธิภาพ หรือ การปรับปรุงคุณภาพ หรือ แม้แต่การบริหารกิจกรรมภายในองค์กร การวางแผนงานอย่างเหมาะสมจากการศึกษาข้อมูลที่เกี่ยวข้องรอบด้าน ถือเป็นจุดเริ่มต้นที่ดี และการดำเนินการที่สอดคล้องกับแผนจะเป็นเส้นทางที่นำไปสู่ความสำเร็จ และบรรลุเป้าหมายที่วางไว้ แต่ก็จะต้องมีการตรวจสอบความคืบหน้า หรือปัญหาต่างๆ ที่เกิดขึ้นเป็นระยะ เพื่อให้ได้ข้อมูลที่สามารถนำมาใช้ในการปรับแผนให้สอดคล้องกับสถานการณ์ได้ และที่สำคัญ เมื่อการดำเนินงานเสร็จสิ้นแต่ละครั้ง บทเรียนต่างๆ ที่ได้รับ ก็ถือเป็นสิ่งสำคัญ หากได้มีการนำมาทบทวน และสรุปข้อดี ข้อด้อย หรือ หาจุดปรับปรุงเพื่อให้การดำเนินงานในรอบต่อไปทำได้ง่ายขึ้น ได้ผลลัพธ์ที่ดีขึ้น และที่กล่าวมาทั้งหมดนี้ ก็คือการดำเนินงานอย่างครบถ้วนตามแนวคิดของวงจร PDCA ซึ่งถือเป็นหัวใจสำคัญของการปรับปรุงอย่างต่อเนื่อง

รูปที่ 2.1 วงจร PDCA

2.1.5 GAP Analysis

การตรวจประเมินเบื้องต้นเพื่อหาความแตกต่างของระบบที่เป็นอยู่ปัจจุบันขององค์กรกับข้อกำหนดของมาตรฐานที่ต้องการจัดทำ ซึ่งจะทำให้ทราบว่าต้องทำอะไรเพิ่มเติมอีกเพื่อสอดคล้องตามข้อกำหนดของมาตรฐาน

2.2 มาตรฐานที่เกี่ยวข้อง

2.2.1 Information Technology Infrastructure Library (ITIL)

ITIL หรือ Information Technology Infrastructure Library เป็นทฤษฎีแนวทางปฏิบัติที่ถูกยอมรับกันอย่างแพร่หลายในการจัดการเกี่ยวกับการให้บริการงาน IT ในหลักการของ ITIL นี้จะนำเสนอหลักการในการทำงานที่เป็นแบบอย่างที่ดีที่สุดในการที่องค์กรจะจัดการและควบคุมการให้บริการของ IT โดยจะประกอบ ด้วยแบบแผนการทำงานที่มีประสิทธิภาพ การนำไปปฏิบัติในองค์กร และการประเมิน หรือกำหนดเครื่องมือที่จะนำไปใช้ในองค์กร ซึ่งในแต่ละองค์กรจะมีสิ่งแวดล้อมที่ต่างกัน จึงเป็นข้อจำกัดที่ไม่สามารถนำวิธีการจัดการจากองค์กรหนึ่งไปยังอีกองค์กรหนึ่งได้

2.2.1.1 โครงสร้าง Information Technology Infrastructure Library (ITIL)

2.2.1.1.1 กลยุทธ์ด้านการบริการ SS : Service Strategy

เป็นกลยุทธ์ในด้านบริการเป็นการกำหนดแนวทางโดยให้หลักไว้ว่า Service Management จะเป็นพื้นฐานในการกำหนด และบริหารนโยบายแนวทางปฏิบัติ และกระบวนการในการบริหารการบริการอย่างครบวงจร

2.2.1.1.2 การออกแบบงานบริการ SD : Service Design

เน้นการออกแบบกิจกรรมที่จะเกิดขึ้น ในการะบวนการให้บริการรวมทั้ง การพัฒนากลยุทธ์ และวิธีการบริหารจัดการระบบบริการ โดยมีกุญแจหลักอยู่ที่

1) Availability Management คือความพร้อมที่จะให้บริการ
2) Capacity Management คือขีดความสามารถในการให้บริการอย่างรวดเร็วและมีประสิทธิภาพ
3) Continuity Management คือความสามารถในการให้บริการที่ต่อเนื่อง
4) Security Management คือการบริหารระบบรักษาความปลอดภัย

2.2.1.1.3 การส่งมอบงานบริการ ST : Service Transition

เน้นที่การดำเนินการเพื่อให้ได้ผลลัพธ์ของการบริการที่ดีที่สุดเป็นบริการที่ส่งมอบเพื่อนำไปใช้ในระบบปฏิบัติงาน การรับข้อมูลจาก Service Design การส่งมอบสถานการณ์ดำเนินงาน

ในทุกรายการเพื่อให้ระบบปฏิบัติการทำงานได้อย่างต่อเนื่อง โดยมีกุญแจหลักอยู่ที่ของ Service Transition คือ

1) Change Management Configuration Management Release Management
2) Service Knowledge Management คือการจัดการความรู้บริการ

2.2.1.1.4 การปฏิบัติงานบริการ SO : Service Operation

เน้นไปทางด้านกิจกรรมที่จำเป็นต่อการปฏิบัติงานเพื่อให้บรรลุผลสำเร็จในการดูแลรักษาหน้าที่การทำงานหรือบริการ ที่เป็นไปตามข้อตกลงว่าด้วย พันธะ สัญญาบริการ Service Level Agreement ที่มีต่อลูกค้า

2.2.1.1.5 การพัฒนางานด้านบริการ CSI : Continual Service Improvement

เน้นที่ขีดความสามารถที่ทำให้เกิดขีดความสามารถในการปรับปรุงการให้บริการที่มีคุณภาพอยู่แล้ว ให้มีความต่อเนื่องกัน

2.2.2 Control Objectives for Information and Related Technology (COBIT)

Control Objectives for Information and Related Technology (COBIT) มีจุดประสงค์ในการสร้างความมั่นใจว่าการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศนั้นสอดคล้องกับวัตถุประสงค์เชิงธุรกิจขององค์กร Business Objectives เพื่อให้เกิดการใช้ทรัพยากรอย่างมีประสิทธิผลอันจะส่งประโยชน์สูงสุดแก่องค์กร ช่วยให้เกิดความสมดุลระหว่างความเสี่ยงด้านเทคโนโลยีสารสนเทศ IT Risk และผลตอบแทนของการลงทุนในระบบสารสนเทศ IT ROI ซึ่งจะทำให้การควบคุมการใช้งานเทคโนโลยีสารสนเทศ ในองค์กรเป็นไปอย่างถูกต้อง และมีประสิทธิผล ส่งผลให้ตรงกับความต้องการทางธุรกิจ และบรรลุเป้าหมายทางธุรกิจที่ตั้งเป้าไว้

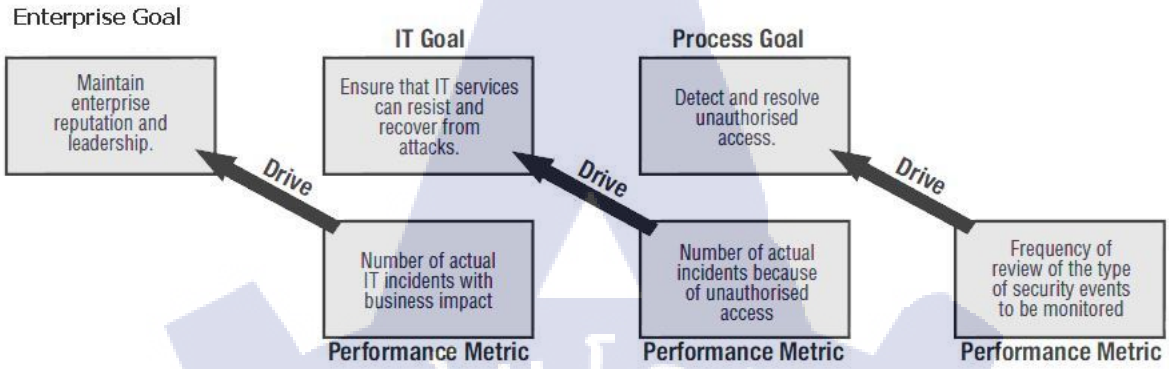
2.2.2.1 ปัจจัยก่อเกิด COBIT

2.2.2.1.1 กระบวนการ (Processes)

องค์กรต้องมีกระบวนการเพื่อให้งานได้ผลลัพธ์หรือบรรลุเป้าหมายของกระบวนการ ซึ่งจะนำไปสู่การบรรลุซึ่งเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและเป้าหมายระดับองค์กรได้

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

- การบรรลุเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ต้องได้รับการสนับสนุนจากการบรรลุเป้าหมายของกระบวนการ (Process Goals)



รูปที่ 2.2 หลักการ Goal Cascade ของ COBIT

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

2.2.2.1.2 วัฒนธรรม จริยธรรม และความประพฤติ (Culture, ethics, behaviour)

หากวัฒนธรรม จริยธรรม และความประพฤติของบุคลากรขององค์กร ไม่ได้รับการปลูกฝังอบรม บ่มเพาะ หรือบ่มนิสัย ในทิศทางที่เหมาะสมที่องค์กรต้องการแล้ว อาจส่งผลต่อการบรรลุเป้าหมายระดับองค์กรได้ เช่น หากองค์กรขาดการปลูกฝังเรื่องการมีวินัยที่ดีหรือการรู้จักหน้าที่ความรับผิดชอบของตนเองแล้ว ก็ยากที่จะทำให้การ ปฏิบัติตามกระบวนการที่สร้างขึ้นมาสำเร็จได้ ซึ่งอาจเป็นเพราะคนขาดวินัย ก็เลยปฏิบัติตามบ้าง ไม่ปฏิบัติตามบ้าง เป้าหมายของกระบวนการเป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และตามด้วยเป้าหมายระดับองค์กร จึงไม่สามารถบรรลุได้

2.2.2.1.3 โครงสร้างบุคลากร (Organizational structures)

องค์กรต้องกำหนดโครงสร้างด้านบุคลากรขึ้นมาเพื่อให้มีหน้าที่ความรับผิดชอบที่ชัดเจนว่าต้องทำอะไรบ้าง หน้าที่ความรับผิดชอบส่วนหนึ่งคือการปฏิบัติตามบทบาทในกระบวนการที่กำหนดไว้ หากขาดโครงสร้างนี้ การปฏิบัติหน้าที่ของตนเองตามบทบาทในกระบวนการ จะไม่สามารถเกิดขึ้นได้ ซึ่งอาจส่งผลต่อการบรรลุเป้าหมายในระดับองค์กรได้

2.2.2.1.4 ข้อมูล (Information)

ข้อมูลเป็นหัวใจสำคัญขององค์กร หลายๆ กระบวนการมีข้อมูลเป็น Input หรือ Output เข้าสู่หรือออกจากกระบวนการก็ตาม ข้อมูลถูกนำไปใช้ในหลายๆ เรื่อง เช่น เพื่อเป็นข้อมูลพื้นฐาน เพื่อใช้ในการตัดสินใจ เพื่อการวางแผน เพื่อการพยากรณ์ หรืออื่นๆ ดังนั้นหากปราศจากข้อมูลที่ต้องการแล้ว อาจทำให้งานหรือกระบวนการขององค์กรไม่สามารถทำได้เลย หรือทำได้อย่างไม่ได้ผลหรือสัมฤทธิ์ผลเท่าที่ควร

2.2.2.1.5 หลักการและนโยบายองค์กร (Principles and policies)

หลักการและนโยบายองค์กรที่กำหนดไว้โดยทั่วไปจะสะท้อนให้เห็นถึงภาพรวม ทิศทาง กรอบแนวคิด หรือกรอบการปฏิบัติที่องค์กรต้องการให้บรรลุเพื่อบังเกิดความสำเร็จตามที่ต้องการ บุคลากรขององค์กรควรยึดตามหลักการและนโยบายที่กำหนดไว้และปฏิบัติตามอย่างสอดคล้องเพื่อให้เกิดผลตามที่องค์กรต้องการ อาจมีผลต่อการทำงานตามหน้าที่และกระบวนการที่ตนเองต้องรับผิดชอบ ซึ่งสามารถส่งผลต่อการบรรลุเป้าหมายในระดับองค์กรได้

2.2.2.1.6 ทักษะ ความรู้ และความสามารถของบุคลากร (Skills and competences)

องค์กรต้องอาศัยบุคลากรเป็นกุญแจสำคัญไปสู่ความสำเร็จของงานและกระบวนการ ซึ่งโดยทั่วไปจำเป็นอย่างยิ่งที่จะต้องให้หรือต้องสร้างให้บุคลากรมีทักษะ ความรู้ และความสามารถที่จำเป็นสำหรับงานหรือกระบวนการที่ปฏิบัติ ถ้าไม่เช่นนั้นแล้ว อาจจะเป็นอุปสรรคสำคัญต่องานหรือกระบวนการที่ทำและต่อความสำเร็จของงานที่จะเกิดขึ้น

2.2.2.1.7 โครงสร้างพื้นฐานของการให้บริการสารสนเทศ (Service capabilities)

โครงสร้างพื้นฐานของการให้บริการสารสนเทศ หมายรวมถึงฮาร์ดแวร์ ซอฟต์แวร์ แอพพลิเคชัน และเทคโนโลยีอื่นๆ ที่ทำหน้าที่เป็นพื้นฐานในการให้บริการด้านระบบงานและข้อมูลแก่ผู้ใช้งานขององค์กร หากปราศจากโครงสร้างพื้นฐานนี้ จะเป็นอุปสรรคต่อการทำงานซึ่งอาจทำให้งาน กระบวนการ หรือข้อมูลที่จำเป็นต้องใช้ เกิดความล่าช้าจนธุรกิจไม่สามารถยอมรับได้

2.3 เทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.3.1 Microsoft Office 2016

ชุดโปรแกรมสำนักงาน พัฒนาโดยบริษัท Microsoft ซึ่งสามารถใช้งานได้ในระบบปฏิบัติการ Microsoft Windows และ Mac ทั้งนี้ยังมีการส่งเสริมให้ใช้บริการผ่านระบบเครื่องแม่ข่าย (Server) และบริการผ่านหน้าเว็บ (Web Based) ในรุ่นใหม่ๆ ของ Microsoft Office จะถูกเรียกว่า ระบบสำนักงาน (Office System) แทนแบบเก่าคือ ชุดโปรแกรมสำนักงาน (Office Suite) ซึ่งการเรียกว่า ระบบสำนักงานจะรวมการทำงานกับเครื่องแม่ข่ายเอาไว้ด้วย

1) Microsoft Word 2016 : โปรแกรมที่นิยมในการประมวลผลคา มีความสามารถในการจัดรูปแบบตัวอักษร ย่อหน้า ใส่รูปภาพ จดหมายเวียน และอื่น ๆ อีกมากมาย
2) Microsoft Excel 2016 : โปรแกรมที่ใช้ในการจัดทำตารางงาน มีความสามารถในการคำนวณสูตรต่าง ๆ พร้อมทั้งฟังก์ชั่นที่ช่วยในการคำนวณทางคณิตศาสตร์อีกด้วย
3) Microsoft Power Point 2016 : โปรแกรมนาเสนอผลงาน สามารถนาเสนอผลงานในแบบต่าง ๆ รวมถึงมีแม่แบบที่ช่วยผู้ใช้ใช้งานอย่างง่ายดาย และมีแอฟเฟคแบบต่าง ๆ ช่วยตกแต่งให้งานนาเสนอมีความสวยงาม
4) Microsoft Visio 2016 : โปรแกรมที่ใช้ออกแบบแผนผัง แผนที่ต่าง ๆ
5) Microsoft Outlook 2016 : โปรแกรมรับ/ส่งอีเมลล์ มีความสามารถในการเชื่อมต่อเครื่องแม่ข่ายอีเมลล์ แบบ IMAP, POP3 และ Microsoft Exchange Server
6) Microsoft OneNote 2016 : สมุดบันทึกแบบ Digital

รูปที่ 2.3 Microsoft Office Icon

2.3.2 Snipping Tool

เครื่องมือสำหรับ Screenshot หน้าจอคอมพิวเตอร์ เริ่มใช้งานมาตั้งแต่ Windows Vista มาจนถึงปัจจุบัน โดยสามารถเลือกรูปแบบในการ Screenshot ได้ 4 รูปแบบ ประกอบด้วย

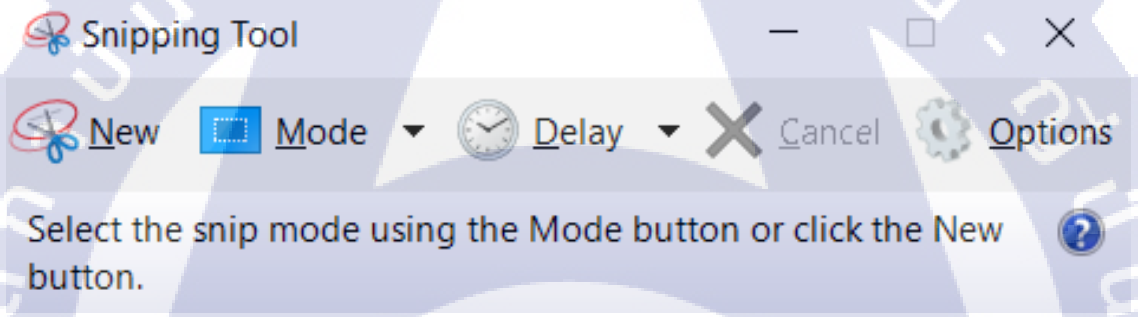
1) Free-form

2) Rectangular

3) Window

4) Full screen

เครื่องมือ Snipping Tool Editor สาหรับคอมเม้น หรือ ไฮน์ไลน์ข้อความก่อนบันทึกข้อมูล สาหรับชนิดของไฟล์ที่โปรแกรมรองรับได้แก่ PNG, GIF, JPEG และ HTML

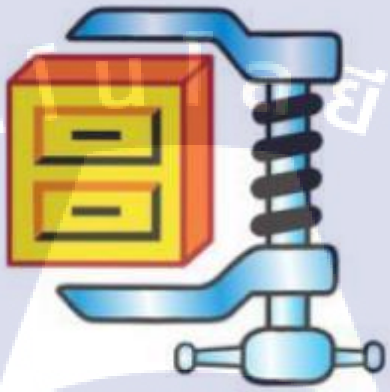


รูปที่ 2.4 Snipping Tool

2.3.3 WinZip Background Tools

โปรแกรมที่เอาไว้ย่อไฟล์จากที่มีขนาดใหญ่ทำให้มีขนาดเล็กลง ด้วยการจัดเรียง algorithm ใหม่เพื่อให้ไฟล์ที่มีขนาดใหญ่นั้นเล็กลง ผลคือทำให้อุปกรณ์สำรองข้อมูลนั้นสามารถเก็บข้อมูลได้มากขึ้น และสามารถขยายข้อมูลที่บีบไว้แล้วนำข้อมูลกลับมาใช้ต่อได้

โปรแกรมนี้จะสนับสนุนไฟล์ ที่มีนามสกุล TAR, ZIP, UUencode, XXencode, BinHex, MIME Unix-Compressed Files, ARJ, LZH, และ ARC Files



รูปที่ 2.5 WinZip Background Tools

บทที่ 3
แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน

3.1 แผนงานการปฏิบัติงาน และแผนการทำโครงงานสหกิจฯ (Gantt Chart)

ตารางที่ 3.1 แผนงานการปฏิบัติงาน

หัวข้องาน	ปี 2561															
	มิถุนายน				กรกฎาคม				สิงหาคม				กันยายน			
ศึกษากระบวนการทำงาน ISO 20000																
ศึกษา Process ที่เกี่ยวข้องในกระบวนการทำงาน ISO 20000																
ศึกษาหลักการ Audit และเอกสารที่เกี่ยวข้องในกระบวนการ Audit																
สนับสนุนการทำ Service Quality Profile เพื่อเป็นข้อมูลในการทำ Internal Audit																
ศึกษากระบวนการทำงาน ISO 27001																
เปรียบเทียบ ISO 20000 และ ISO 27001 หา GAP Analysis																
จัดทำรูปเล่มรายงานและ ตรวจสอบแก้ไขข้อผิดพลาด																
สนับสนุนการทำ Internal Audit และ งานด้านอื่นๆ ของ ISO 20000																

3.2 รายละเอียดงานที่นักศึกษาปฏิบัติในการสหกิจศึกษา

3.2.1 เครื่องมือที่ใช้

1) เครื่องคอมพิวเตอร์ เพื่อทำการเก็บและเรียบเรียงข้อมูล
2) อินเตอร์เน็ต เพื่อค้นคว้าหาข้อมูล

3.2.2 การค้นคว้าหาข้อมูล และการศึกษาเพิ่มเติม

ทางผู้จัดทำได้ทำการศึกษา ISO 20000 และ ISO 27001 ทำให้ทราบถึงทฤษฎีที่ใช้ในการดำเนินงาน วิเคราะห์ข้อมูล ความเสี่ยง และวิธีจัดการความเสี่ยง เพื่อที่จะได้นำความรู้ที่ได้มาใช้ในการปฏิบัติงานเพื่อให้เกิดผลสำเร็จตรงตามขั้นตอน

3.2.3 การเก็บรวบรวมข้อมูล

ทางผู้จัดทำได้ทำการเก็บรวบรวมข้อมูลและเอกสาร จากการศึกษารวมถึงการประยุกต์ใช้ทฤษฎีในการวิเคราะห์ความแตกต่าง และการประเมินความเสี่ยง เพื่อใช้ในการการจำแนกและพิจารณาจัดลำดับความสำคัญของความเสี่ยง เพื่อประกอบการวิเคราะห์ วางแผนขั้นตอนในการดำเนินงาน ลงมือปฏิบัติ ตรวจสอบการทำงาน และแก้ไขข้อบกพร่อง เพื่อใช้ในการสรุปข้อมูลที่ได้จากการทำงาน

3.2.4 วัตถุประสงค์ของโครงงาน

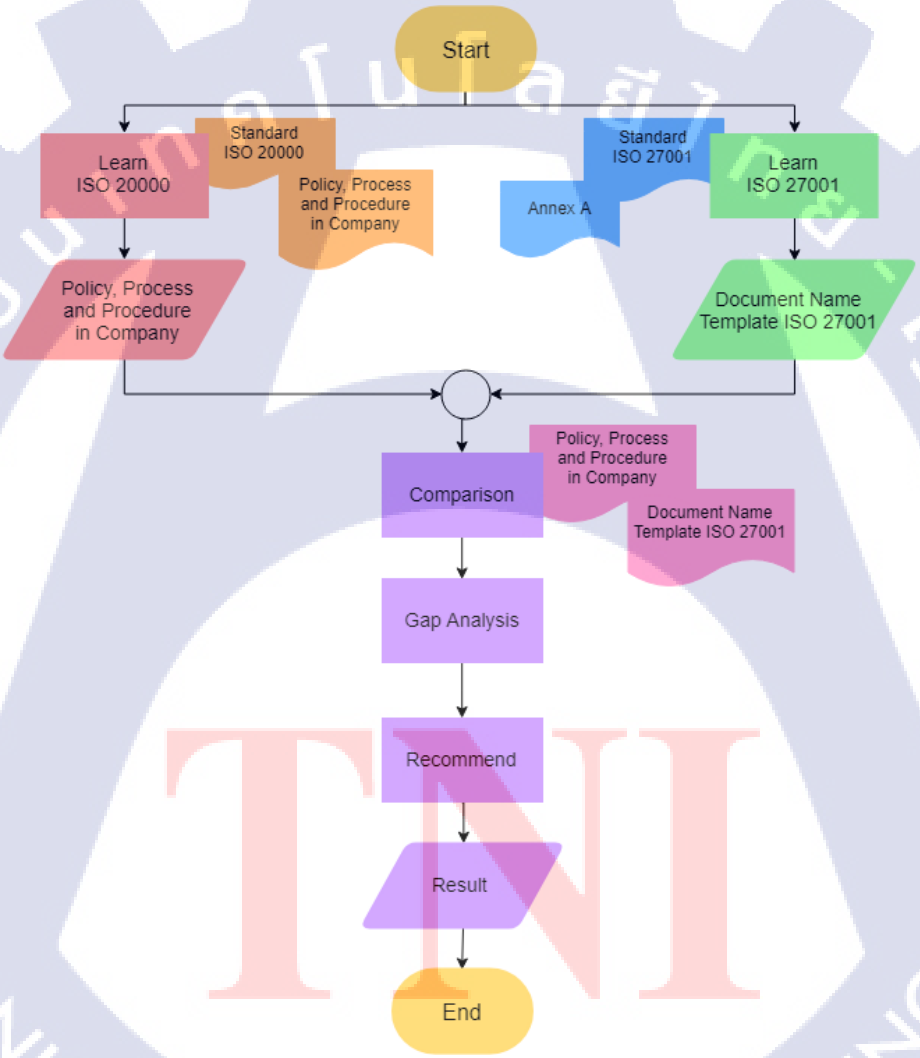
1) ศึกษาหลักการดำเนินงานเพื่อหาความแตกต่างระหว่าง ISO 20000 และ ISO 27001
2) เข้าใจหลักการในการวิเคราะห์ความแตกต่าง (GAP Analysis)
3) สามารถนำโครงงานนี้ไปพัฒนาต่อยอดได้อีกในอนาคต

3.2.5 งานอื่นๆ ที่ได้รับมอบหมาย

1) ศึกษา Policy, Process และ Procedure ขององค์กร
2) สนับสนุนการทำ Internal Audit
3) สนับสนุนการทำ Service Quality Profile

3.3 ขั้นตอนการดำเนินงานโครงงานสหกิจศึกษา

รูปที่ 3.1 ขั้นตอนการดำเนินงานภาพรวม (1)



รูปที่ 3.2 ขั้นตอนการดำเนินงาน (2)

บทที่ 4
สรุปผลการดำเนินงาน การวิเคราะห์และสรุปผลต่าง ๆ

4.1 ขั้นตอนและผลการดำเนินงานโครงงานสหกิจศึกษา

ขั้นตอนต่างๆ ในการศึกษารายละเอียดเกี่ยวกับการวิเคราะห์ความแตกต่าง (GAP Analysis) และการประเมินความเสี่ยง (Risk Assessment) เพื่อใช้ในการวิเคราะห์ จัดลำดับความเสี่ยง และวางแผนการพัฒนาจากความแตกต่างของเอกสารที่มีอยู่ขององค์กร ให้สอดคล้องกับมาตรฐาน และสถานการณ์ในปัจจุบัน สามารถแจกแจงขั้นตอนในการดำเนินงาน และผลการดำเนินงานได้ดังนี้

4.1.1 รายละเอียดของโครงงานและความรู้ที่ได้รับ

4.1.1.2 ที่มาของปัญหาและความรู้ที่ได้รับ

เนื่องจากในปัจจุบันเทคโนโลยีสารสนเทศภายในองค์กรทางธุรกิจเริ่มมีบทบาท และความสำคัญมากยิ่งขึ้นเพื่อตอบสนองความต้องการทางธุรกิจที่มีมากขึ้นเรื่อย ๆ ส่งผลให้แผนการพัฒนาด้านเทคโนโลยีสารสนเทศต้องมีความสอดคล้องกับแผนในการพัฒนาทางธุรกิจ ซึ่งขั้นตอนการวิเคราะห์ และวางแผนการทำงานจึงมีความจำเป็นอย่างมากในการดำเนินการพัฒนา ดังนั้นการวิเคราะห์ความแตกต่าง (GAP Analysis) ระหว่างสิ่งที่มีอยู่ในองค์กร กับสิ่งที่จะพัฒนาต่อในอนาคต ซึ่งมีความจำเป็นอย่างมากในการวางแผน หากแต่การวิเคราะห์ความแตกต่าง (GAP Analysis) ยังไม่สามารถวิเคราะห์ความแตกต่างและเลือกการควบคุมได้ ด้วยเหตุนี้ข้าพเจ้าจึงนำเอาการประเมินความเสี่ยง (Risk Assessment) มาประยุกต์ใช้ควบคู่กับการวิเคราะห์ เพื่ออธิบายการรักษาความปลอดภัยของข้อมูล และวางแผนในการหาความแตกต่างในสิ่งที่มีอยู่กับสิ่งที่จะพัฒนาในอนาคต โดยคำนึงถึงความปลอดภัยของข้อมูล รวมทั้งเพื่อเป็นประโยชน์กับผู้อื่นได้

4.1.2 ศึกษาและทำความเข้าใจหลักการ และ แนวคิด

4.1.2.1 GAP Analysis

GAP Analysis หรือ การวิเคราะห์ความแตกต่าง เป็นวิธีการประเมินสถานะในปัจจุบัน กับทิศทางในอนาคต รวมทั้งแนวทางปฏิบัติที่ดีที่สุด (Best Practice) เพื่อให้ทราบถึงสถานะทางธุรกิจขององค์กรว่าเป็นไปตามมาตรฐานหรือไม่ โดยการทำการวิเคราะห์จะต้องแสดงให้เห็นถึงความแตกต่างระหว่างสถานะในปัจจุบัน กับแนวทางในการพัฒนา ซึ่งจะทำให้องค์กรสามารดำเนินการตามขั้นตอนต่อไป อย่างไรก็ตามการวิเคราะห์ความแตกต่าง (GAP Analysis) เป็นแค่เพียงกระบวนการในการทำความเข้าใจสถานะขององค์กรเท่านั้น

การวิเคราะห์ความแตกต่าง (GAP Analysis) มักถูกใช้โดยผู้จัดการโครงการ หรือ ผู้จัดการผลิตภัณฑ์เพื่อระบุความแตกต่าง ที่ทำให้เกิดปัญหาในการเติบโตขององค์กร และอาจเป็นประโยชน์มากขึ้นสำหรับองค์กรขนาดเล็ก หากสามารถปรับปรุงประสิทธิภาพได้โดยระบุความแตกต่าง (GAP) ทำการวิเคราะห์กระบวนการที่ต้องได้รับการปรับปรุงความแตกต่าง (GAP) ที่มีอยู่ และนำผลที่ได้จากการดำเนินการที่เหมาะสมเพื่อให้บรรลุเป้าหมายขององค์กร

4.1.2.1.1 วิธีการวิเคราะห์ความแตกต่าง (GAP)

การวิเคราะห์ความแตกต่าง (GAP) จะพิจารณาถึงสถานะปัจจุบัน กับทิศทางในอนาคต คำแนะนำ และแนวทางการดำเนินงาน ก่อนจะทำการวิเคราะห์ จาเป็นต้องสร้างเป้าหมายขององค์กรที่มีประสิทธิภาพ และมีความเฉพาะเจาะจง ประเมินได้ สามารถทำให้บรรลุผลได้จริง และมีระยะเวลา

4.1.2.1.2 องค์ประกอบของการวิเคราะห์ความแตกต่าง (GAP Analysis)

การวิเคราะห์ความแตกต่าง (GAP Analysis) ต้องมีคำนึงถึงองค์ประกอบดังต่อไปนี้

4.1.2.1.2.1 สถานะในปัจจุบัน (Present State)

ต้องมีความเข้าใจในกระบวนการต่าง ๆ ขององค์กรอย่างสมบูรณ์ ที่ต้องการปรับปรุงเพื่อให้เข้าใจถึงสถานะในปัจจุบัน โดยผลการวิเคราะห์ต้องเป็นปริมาณ หรือ สิ่งที่เน้นแนวโน้มและสามารถเปรียบเทียบได้

4.1.2.1.2.2 ทิศทางในอนาคต (Future State)

ระบุเป้าหมายโดยการสำรวจตำแหน่ง หรือสถานะในปัจจุบัน และทิศทางในอนาคต รวมทั้งต้องเป็นปริมาณ หรือ สิ่งที่เน้นแนวโน้ม และสามารถเปรียบเทียบได้

4.1.2.1.2.3 ระบุความแตกต่าง (Identify GAP)

ระบุว่าความแตกต่าง (GAP) ที่อยู่ระหว่างสถานะปัจจุบัน กับทิศทางในอนาคตขององค์กร และคำอธิบายความแตกต่าง (GAP) ซึ่งเป็นสิ่งที่ก่อให้เกิดความแตกต่าง (GAP) และปัจจัยที่มีส่วนร่วม

4.1.2.1.2.4 ข้อเสนอ / แนวทางการปฏิบัติ (Proposal/Solution)

ระบุแนวทางปฏิบัติที่เป็นไปได้ทั้งหมดที่สามารถนำมาใช้เพื่อเติมเต็มความแตกต่าง (GAP) โดยวัตถุประสงค์เหล่านี้ต้องเฉพาะเจาะจง และแสดงถึงปัจจัยต่าง ๆ ที่ถูกระบุไว้ในคาอธิบายความแตกต่าง (GAP) และควรอยู่ในรูปแบบที่สามารถใช้งานได้ น่าสนใจ เช่น บทสรุปของผู้บริหารที่อธิบายถึงผลที่ได้จากการสังเกต ผลลัพธ์ที่ต้องการ และเป้าหมาย เพื่อให้สามารถทำความเข้าใจได้อย่างรวดเร็ว นอกจากนี้ควรระบุถึงเหตุผลที่เชื่อว่าเป็นเหตุให้เกิดความแตกต่าง (GAP)

4.1.2.2 การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยง (Risk Assessment) หมายถึง การจำแนกและ พิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจาก โอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact)

1) โอกาสที่จะเกิด (Likelihood) เป็นการพิจารณาความเป็นไปได้ที่จะ เกิดเหตุการณ์ความเสี่ยงในช่วงเวลาหนึ่ง หรือจะเรียกว่า ความถี่หรือ โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงก็ได้
2) ผลกระทบ (Impact) ระดับความรุนแรงของผลเสียหายที่เกิดขึ้น จาก ความเสี่ยงและ มีผลกระทบต่อองค์กรซึ่งอาจเป็นได้ทั้งในด้านบวก และด้านลบ โดยสามารถแบ่งเป็นผลกระทบทางด้านการเงินและ ผลกระทบที่ไม่ใช่ทางการเงิน

4.1.2.2.1 การจัดระดับความเสี่ยง (Risk Rating)

การจัดระดับความเสี่ยง (Risk Rating) คือการนำความเสี่ยงที่ประเมิน ได้มาจัดซึ่งมีอยู่ 4 ระดับคือ ต่ำ ปานกลาง สูง และสูงมาก เพื่อช่วยในการ ตัดสินใจของผู้บริหารสำหรับการเลือกจัดการกับความเสี่ยงที่มีระดับความสำคัญก่อน

4.1.2.2.2 เจ้าของความเสี่ยง (Risk Owner)

เจ้าของความเสี่ยง (Risk Owner) คือ หน่วยงานที่ทำให้เกิดความเสี่ยง หรือหน่วยงานที่ได้รับผลกระทบโดยตรงจากความเสี่ยงที่ถูกระบุขึ้น และเป็น ผู้ประเมินความเสี่ยง/จัดทำแผนบริหารความเสี่ยง/ให้ข้อเสนอแนะ รวมทั้ง ติดตามประเมินผลการบริหารความเสี่ยงอย่างสม่ำเสมอ เพื่อให้ผลการ บริหารความเสี่ยงบรรลุเป้าหมายที่ตั้งไว้

4.1.2.2.3 แผนผังความเสี่ยง (Risk Map)

แผนผังความเสี่ยง (Risk Map) คือ แผนผังที่แสดงความสัมพันธ์ของ ความเสี่ยงกับวัตถุประสงค์ขององค์กร ความเสี่ยงกับความเสี่ยง สาเหตุกับ ความเสี่ยง สาเหตุกับสาเหตุและระดับความรุนแรง/ผลกระทบ เพื่อนำมา ประกอบการพิจารณาจัดทำแผนบริหารความเสี่ยง

4.1.2.2.4 ดัชนีชี้วัดความเสี่ยงหลัก (KRI : Key Risk Indicator)

ดัชนีชี้วัดความเสี่ยงหลัก (KRI : Key Risk Indicator) คือ มาตรวัดหรือ จุดเตือนภัย (Trigger Point) ของระดับหรือสถานะความเสี่ยง เพื่อใช้ ประเมินสถานะของความเสี่ยง และประสิทธิผลของแผนบริหารความเสี่ยง และต้องสอดคล้องกับ Risk Appetite และ Risk Tolerance

4.1.2.2.5 ค่าระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite)

ค่าระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite) คือ การกำหนด ระดับความเสี่ยงในเชิงปริมาณหรือคุณภาพที่องค์กรจะสามารถยอมรับ ความเสียหาย/สูญเสียจากความเสี่ยงโดยกำหนดให้สอดคล้องกับเป้าหมาย ในแผนปฏิบัติการประจำปีหรือตามตัวชี้วัดขององค์กร ซึ่งไม่ควรต่ำกว่าค่า “ระดับ 3”

4.1.2.2.6 ช่วงเบี่ยงเบนของค่าระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Tolerance)

ช่วงเบี่ยงเบนของค่าระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Tolerance) คือการกำหนดค่าช่วงเบี่ยงเบนของระดับความเสี่ยงที่ยังคงอยู่ ในระดับที่องค์กรยังสามารถยอมรับได้เช่น + 5% หรือ +1 เดือน เป็นต้น โดยกำหนดให้สอดคล้องกับเป้าหมายในแผนปฏิบัติการประจำปีหรือตามตัวชี้วัดขององค์กร ซึ่งอาจจะเท่ากับหรือต่ำกว่าค่า “ระดับ 3” ได้

4.1.2.2.7 ความเสี่ยงขั้นต้น (Gross Risk)

ความเสี่ยงขั้นต้น (Gross Risk) คือ ระดับความเสี่ยงที่เกิดขึ้น (ก่อนที่จะมี การควบคุม) ซึ่งจะทำให้การดำเนินงานไม่บรรลุวัตถุประสงค์

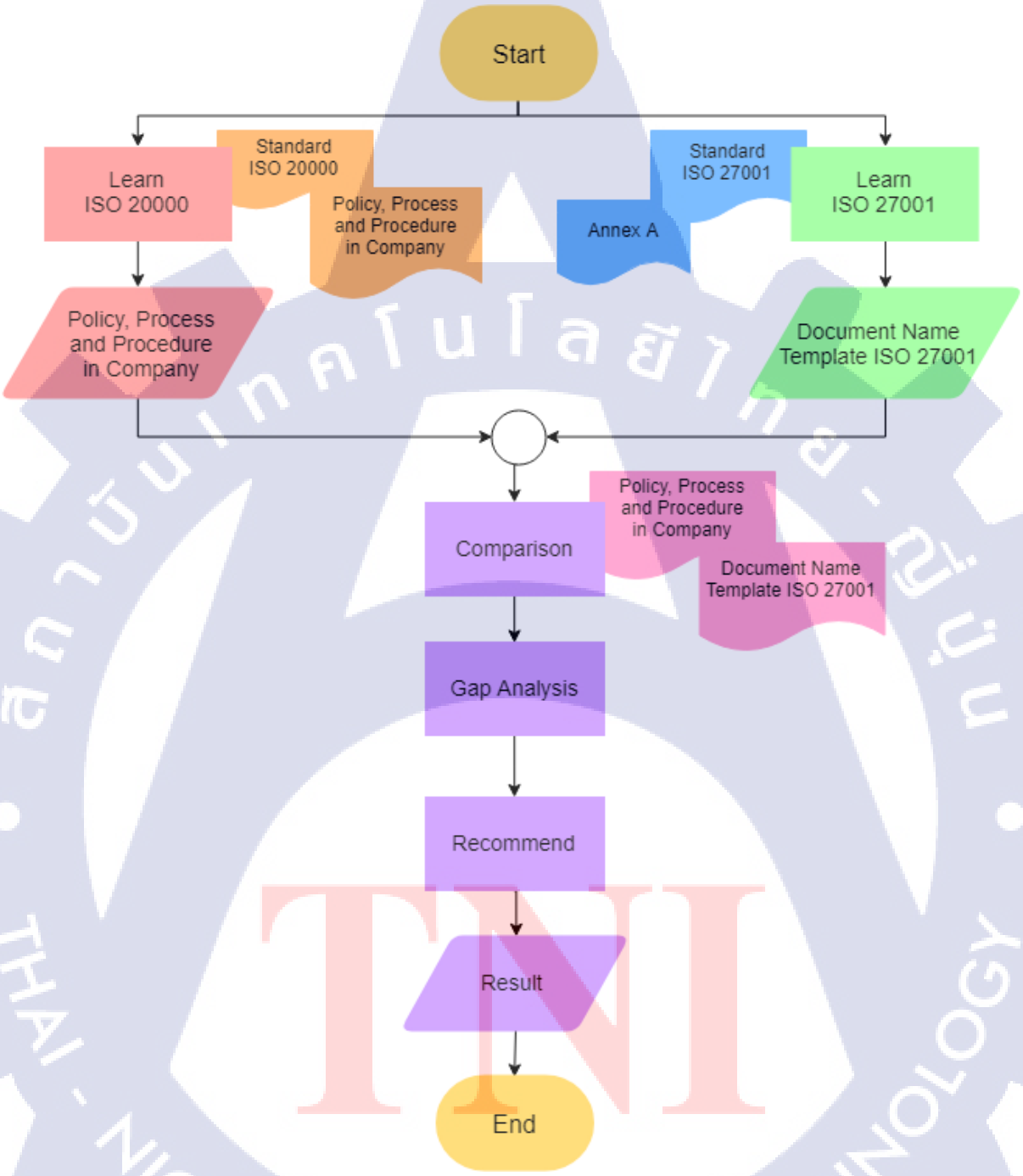
4.1.2.2.8 ความเสี่ยงคงเหลือ (Residual Risk)

ความเสี่ยงคงเหลือ (Residual Risk) คือ ระดับความเสี่ยงที่เหลืออยู่ หลังจากใส่การควบคุมที่มีอยู่เข้าไปในการบริหารงานแล้ว ซึ่งหากยังคงเหลืออยู่ในระดับสูง-สูงมาก หน่วยงานก็ควรให้ความสนใจเป็นพิเศษและ จัดทำแผนเพื่อลดความเสี่ยงให้อยู่ในระดับที่เหมาะสมต่อไป

4.1.3 การวิเคราะห์ความแตกต่างของ ISO 20000 และ ISO 27001

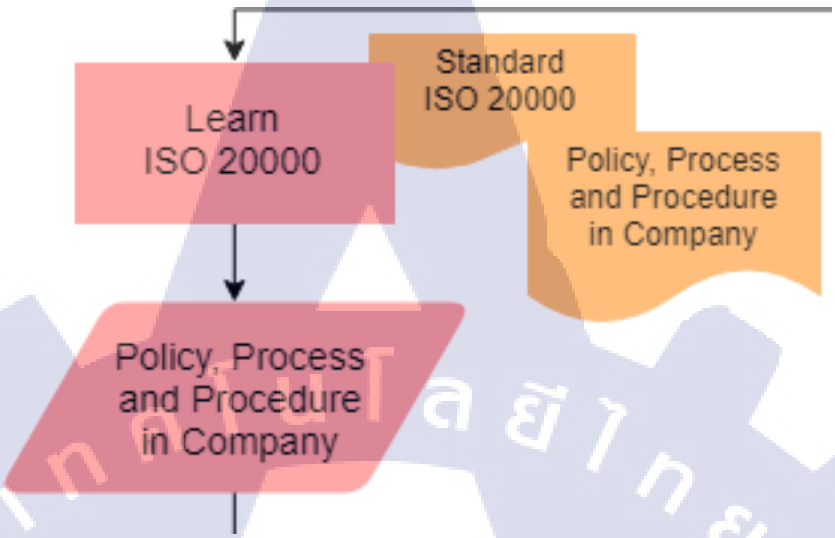
การวิเคราะห์มาตรฐานการจัดการบริการด้านเทคโนโลยีสารสนเทศ (ISO 20000) ที่องค์กรดำเนินการอยู่ในปัจจุบัน และ มาตรฐานการจัดการความปลอดภัยของข้อมูล (ISO 27001) ที่เริ่มศึกษาและหาความแตกต่าง (GAP Analysis) เพื่อจะนำมาพัฒนาและเพิ่มเติมในส่วนของเอกสารที่ทางองค์กรมีอยู่ ให้ครอบคลุมในขอบเขตของ ISO 27001 จำเป็นต้องอาศัยความรู้ความเข้าใจในระบบเทคโนโลยีสารสนเทศ กระบวนการบริหารจัดการเทคโนโลยีสารสนเทศในองค์กร และในมาตรฐาน จึงต้องมีการดำเนินการวิเคราะห์เพื่อหาแนวทางในการพัฒนาด้านเทคโนโลยีสารสนเทศและแนวทางในการจัดทำเอกสารเพื่อกำหนดเงื่อนไขในการปฏิบัติ ให้มีความสอดคล้องกับแนวทางด้านธุรกิจ จึงจำเป็นต้องดำเนินการวิเคราะห์ความแตกต่าง และหาแนวทางเพื่อลดความเสี่ยงที่จะเกิดขึ้นกับข้อมูลภายในองค์กร โดยอิงแนวทางการทำงานที่ดีจากการปฏิบัติงานในองค์กร รวมถึงการตรวจทานเอกสารขององค์กร การสัมภาษณ์ผู้บริหาร และคณะผู้ปฏิบัติงาน

แผนภาพแสดงขั้นตอนการดำเนินงาน การวิเคราะห์ และวางแผนในการหาความแตกต่าง



รูปที่ 4.1 ขั้นตอนการประยุกต์ใช้

4.1.3.1 ขั้นตอนการศึกษา ISO 20000

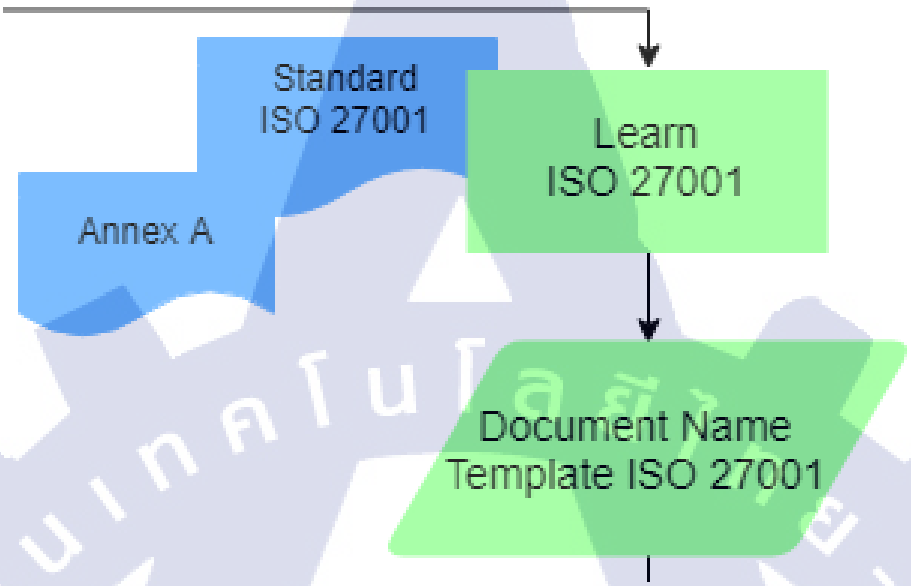


รูปที่ 4.2 ขั้นตอนการศึกษา ISO 20000

ในการศึกษามาตรฐานการจัดการบริการด้านเทคโนโลยีสารสนเทศ (ISO 20000) เพื่อนำมาใช้เป็นแนวทางในการหาความแตกต่าง มีขั้นตอนในการศึกษาดังนี้

1) ศึกษามาตรฐานการจัดการบริการด้านเทคโนโลยีสารสนเทศ ISO 20000 (Service Management System : SMS)
2) เอกสารที่ใช้ในศึกษาได้แก่ เอกสารมาตรฐาน ISO 20000 และ Policy, Process และ Procedure ขององค์กร
3) นำผลที่ได้จากการศึกษามาเตรียมเอกสาร Policy, Process และ Procedure ขององค์กรนำมาใช้ในการเปรียบเทียบหาความแตกต่าง

4.1.3.2 ขั้นตอนการศึกษา ISO 27001

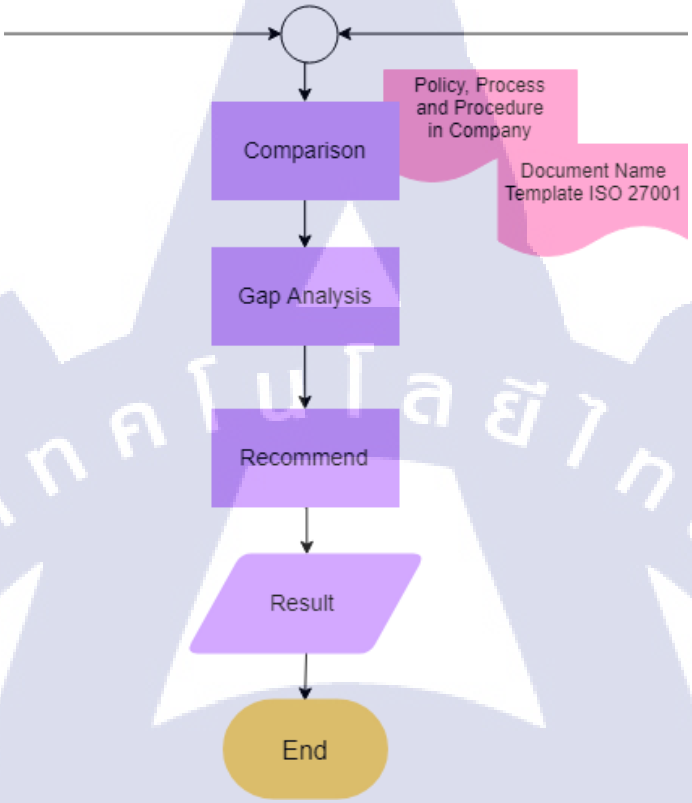


รูปที่ 4.3 ขั้นตอนการศึกษา ISO 27001

ในการศึกษามาตรฐานการจัดการความมั่นคงปลอดภัยของข้อมูล (ISO 27001) เพื่อนำมาใช้เป็นแนวทางในการหาความแตกต่าง มีขั้นตอนในการศึกษาดังนี้

1) ศึกษามาตรฐานการจัดการความมั่นคงปลอดภัยของข้อมูล ISO 27001 (Information Security Management System : ISMS)
2) เอกสารที่ใช้ในศึกษาได้แก่ เอกสารมาตรฐาน ISO 27001 และ Annex A
3) ค้นหาเอกสาร Policy, Process และ Procedure ที่ใช้ในมาตรฐาน ISO 27001 เพื่อนำมาเทียบกับเอกสารที่มีอยู่ภายในองค์กร

4.1.3.3 ขั้นตอนการหาความแตกต่างระหว่าง ISO 20000 และ ISO 27001



รูปที่ 4.4 ขั้นตอนการหาความแตกต่างระหว่าง ISO 20000 และ ISO 27001

จากการศึกษามาตรฐาน ISO 20000 และ ISO 27001 ได้ทำการเตรียมเอกสารของมาตรฐานทั้ง 2 มาตรฐานมาเทียบกัน มีขั้นตอนในการหาความแตกต่างดังต่อไปนี้

1) เปรียบเทียบเอกสารของมาตรฐาน ISO 20000 และ ISO 27001 โดยเทียบจากเอกสารขององค์กรและ เอกสารที่ใช้ในมาตรฐาน ISO 27001
2) หาความแตกต่างจากเอกสาร โดยการเปรียบเทียบรายละเอียด หัวข้อที่อยู่ในเอกสารของมาตรฐาน ISO 27001 เทียบกับ เอกสารขององค์กร
3) เมื่อพบว่าเอกสารขององค์กรไม่ตรงกับ เอกสารของ ISO 27001 ให้ทำการแนะนำ สิ่งที่ควรเพิ่มเติมลงในเอกสารขององค์กร
4) นำผลที่ได้จากการวิเคราะห์ความแตกต่างให้องค์กรเพื่อให้องค์กรนำไปดำเนินการ

4.1.3.4 ตารางการเปรียบเทียบความแตกต่างระหว่าง ISO 20000 และ ISO 27001

Number in the package	Document Name	Document Detail	Description	Purpose	Relevant Clauses in the Standard ISO/IEC 27001	Controls	DOC	Company	COMPANY DOC NAME	Comment
0	Procedure for Document and Record Control	1. Purpose, Scope and users	The purpose of this procedure is to ensure control over creation, approval, distribution, usage and updates of documents and records (also called: documented information) used in the Information Security Management System (ISMS) and for compliance with the EU GDPR. This procedure is applied to all documents and records related to the ISMS, regardless of whether the documents and records were created inside [organization name] or whether they are of external origin. This procedure encompasses all documents and records, stored in any possible form-paper, audio, video, etc.	Users of this document are all employees of [organization name] inside the scope of the ISMS.	7.5	Documented information	✓	✓	PRD-SMS-02 1-2	มีแต่จะยังไม่ครบ documents records control ขาดดังต่อไปนี้ : - used in the Information Security Management System (ISMS) - applied to the entire ISMS
		2. Reference documents	ISO/IEC 27001 standard, clause 7.5				✓	×		ยังไม่มีการ Ref.ISO27001
		3. Control of internal document	Internal documents are all documents created inside the organization.				✓	✓	PRD-SMS-02 5	- 5. DOCUMENTED INFORMATION IDENTIFICATION AND CONTROL - มี Process ในการ Control แต่ยังไม่ได้ Control ลงไปใน ISO27001 ถูก control ด้วย Process เดิมหรือเปล่า วิธีการในการควบคุมเอกสารมี

รูปที่ 4.5 ตารางการเปรียบเทียบความแตกต่างระหว่าง ISO 20000 และ ISO 27001

ในการเปรียบเทียบความแตกต่างของเอกสารภายในองค์กรและเอกสารของ ISO 27001 ได้จัดทำในรูปแบบไฟล์ Excel ประกอบด้วยหัวข้อดังต่อไปนี้

1) Document Name คือ ชื่อเอกสารที่มีอยู่ในมาตรฐาน ISO 27001
2) Document Detail คือ รายละเอียดในเอกสารของมาตรฐาน ISO 27001
3) Description คือ คำอธิบายรายละเอียดในหัวข้อย่อยของเอกสาร ISO 27001
4) Purpose คือ ระบุถึงจุดประสงค์ในการใช้เอกสาร
5) Relevant Clauses in the Standard ISO/IEC 27001 คือ การอ้างอิงถึงมาตรฐาน
6) Controls คือชื่อของ Clauses หรือ Annex A ในมาตรฐาน ISO 27001 ซึ่งเป็นการให้รายละเอียดในหัวข้อของ Relevant Clauses in the Standard ISO/IEC 27001
7) DOC คือ ค้นหาเอกสาร ISO 27001 หากพบเอกสารให้ทำเครื่องหมายถูก หากไม่พบเอกสารให้ทำเครื่องหมายกากบาท
8) Company คือ องค์กรมีเอกสารรอบรับตรงตามหัวข้อ Document Detail หากพบเอกสารให้ทำเครื่องหมายถูก หากไม่พบเอกสารให้ทำเครื่องหมายกากบาท
9) COMPANY DOC NAME คือ หากพบเอกสารให้ทำการใส่ชื่อเอกสารที่พบ
10) Comment คือ คำแนะนำ และสิ่งที่ควรเพิ่มเติมในเอกสาร

4.2 ผลการวิเคราะห์ข้อมูล

1) ทำให้ทราบถึงข้อมูลในปัจจุบันขององค์กร
2) ทำให้ทราบถึงทิศทางในการพัฒนาในอนาคต
3) ทำให้ทราบถึงความครบถ้วนของข้อมูล และสามารถเพิ่มเติมข้อมูลให้ตรงตามมาตรฐาน
4) ช่วยลดความเสี่ยงที่จะเกิดขึ้นกับองค์กร
5) สามารถนำผลที่ได้ไปวางแผนเพื่อพัฒนาองค์กรได้อย่างมีประสิทธิภาพ

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงานโครงงานสหกิจศึกษา

ผลลัพธ์ของการศึกษาในครั้งนี้ คือทราบกระบวนการในการพัฒนาด้านเทคโนโลยีสารสนเทศ เพื่อจัดการกับการให้บริการ การบริหารความเสี่ยงภายในองค์กรและ แนวทางในการรับมือกับความเสี่ยงที่จะเกิดขึ้นในอนาคตของผู้ให้บริการทางด้านไอที ขั้นตอนในการพัฒนามีกระบวนการใดบ้าง รวมทั้งการนำทฤษฎีในการวิเคราะห์ความแตกต่าง และการประเมินความเสี่ยงมาประยุกต์ใช้ในการจำแนกและ พิจารณาจัดลำดับความสำคัญของความเสี่ยง เพื่อประกอบการวิเคราะห์ วางแผนขั้นตอนในการดำเนินงาน ลงมือปฏิบัติ ตรวจสอบการทำงาน และแก้ไขข้อบกพร่อง เพื่อหาความแตกต่างระหว่างมาตรฐาน ISO 20000 และ ISO 27001 นำมาทำการวิเคราะห์ความแตกต่างและ แนะนำแนวทางในการพัฒนาให้ตรงตามมาตรฐาน ISO 27001 ซึ่งการพัฒนายังสามารถใช้ทฤษฎีอื่นได้อีกหลายทฤษฎี เช่น ITIL, COBIT5 และ IEEE เป็นต้น ขึ้นอยู่กับความถนัด และ ความเชี่ยวชาญของแต่ละบุคคล

5.2 แนวทางการแก้ไขปัญหา

เนื่องจากทางผู้จัดทำ ยังไม่มีประสบการณ์ในการนำทฤษฎีของการวิเคราะห์ความแตกต่าง (GAP Analysis) และการประเมินความเสี่ยง (Risk Assessment) ไปประยุกต์ใช้ในการวางแผนเพื่อพัฒนาการบริหารจัดการด้านเทคโนโลยีสารสนเทศ เพื่อลดความเสี่ยงที่จะเกิดขึ้นภายในองค์กรและการให้คำแนะนำที่เหมาะสม จึงมีความเห็นว่าการนำทฤษฎีดังกล่าวมาประยุกต์ใช้นั้นเพียงพอแล้วในการวางแผนเพื่อพัฒนาองค์กรสำหรับผู้ให้บริการทางด้านไอที ในด้านการบริหารจัดการ และ การควบคุมเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ หากแต่ Policy, Process และ Procedure ขององค์กรที่ใช้ในการควบคุมการดำเนินงานด้านเทคโนโลยีสารสนเทศมีเงื่อนไขไม่ตรงตามมาตรฐาน ISO 27001 ส่งผลให้ต้องทำการเปรียบเทียบหาความแตกต่างและ ให้คำแนะนำแนวทางในการดำเนินงานให้ครบถ้วนตรงตามมาตรฐาน ISO 27001 เพื่อที่จะได้ดำเนินการพัฒนาระบบให้เหมาะสมกับองค์กร

5.3 ข้อเสนอแนะจากการดำเนินงานโครงงานสหกิจศึกษา

จากประสบการณ์ในการสหกิจศึกษาพบว่า ในการทำงานในสายงานการตรวจสอบด้านเทคโนโลยีสารสนเทศนั้น ต้องมีความรู้ในการตรวจสอบ และ ต้องเพิ่มความรู้อย่างสม่ำเสมอเพื่อให้ทันกับการเปลี่ยนแปลงของเทคโนโลยีใหม่ๆ ที่มีการเปลี่ยนแปลงอย่างรวดเร็ว ซึ่งผู้ตรวจสอบต้องเรียนรู้ทักษะในด้านการตรวจสอบให้ครอบคลุม ทั้งด้านเทคโนโลยีและ ภัยคุกคามใหม่ๆ เพื่อที่จะได้แนะนำแนวทางในการป้องกันระบบ และเป็นที่ปรึกษาทางด้านความเสี่ยงได้อย่างมีประสิทธิภาพ และ ดำเนินงานได้อย่างน่าเชื่อถือ

เอกสารอ้างอิง

ISO 20000 [Online], Available: https://bit.ly/2yDyIYy [4 มิถุนายน 2561]

PDCA [Online], Available: https://goo.gl/sEvJWt [6 มิถุนายน 2561]

ITIL/ISO 20000 Knowledge [Online], Available: https://bit.ly/2z9ucAi [18 มิถุนายน 2561]

การตรวจ Internal Audit [Online], Available: https://bit.ly/2yCyPng [12 กรกฎาคม 2561]

ระบบสารสนเทศ [Online], Available : https://goo.gl/5DEvby [24 กรกฎาคม 2561]

การบริหารจัดการความเสี่ยง[Online], Available : https://goo.gl/u26EeI [1 สิงหาคม 2561]

การบริหารความเสี่ยง [Online], Available : https://goo.gl/gRkjXA [16 สิงหาคม 2561]

ISO 27001 [Online], Available: https://bit.ly/2nA5EN0 [3 กันยายน 2561]

Annex A ISO 27001 [Online], Available: https://bit.ly/2xVl0xh [7 กันยายน 2561]

ISO 27002 [Online], Available: https://bit.ly/1IiAiLD [10 กันยายน 2561]

What is GAP analysis [Online], Available: https://goo.gl/MrXELh [18 กันยายน 2561]

Document Name ISO 27001 [Online], Available: https://advisera.com/27001academy/ [26 กันยายน 2561]

Information security for cloud services [Online], Available: https://bit.ly/2EJxL6i [10 ตุลาคม 2561]

ภาคผนวก

ภาคผนวก ก.

รายงานการปฏิบัติงานประจำสัปดาห์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่.....1.....

ชื่อ-สกุลนักศึกษา นางสาว ณัฐณิชา พรหมรส รหัสนักศึกษา 58121086-1
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 4/6/61	8	ศึกษาเรื่อง Internal Audit เกี่ยวกับ SMS, SLM เข้าประชุม Internal Audit ของฝ่าย Sales	เข้าใจลักษณะการตรวจสอบของ Audit	ความรู้ทางด้าน Process ยังไม่เพียงพอทำให้ไม่เข้าใจ
อังคาร 5/6/61	8	ศึกษา Process ใน Internal Audit เกี่ยวกับ ICM, PBM	เข้าใจลึง Process ของ ICM และ PBM	-
พุธ 6/6/61	9	ศึกษา Process ใน Internal Audit ที่ใช้ในส่วนของ Service level Management Policy	เข้าใจ Process ของ Service level Management Policy	-
พฤหัสบดี 7/6/61	9	Update ข้อมูลที่ทำการ Audit มาลงใน Checklist และศึกษา Process CFM จาก VDO	เข้าใจ Process CFM มากขึ้น	-
ศุกร์ 8/6/61	8	ส่ง File Checklist ที่ทำการ Audit ให้พี่เลี้ยง และศึกษา Incident, Problem, Configuration	เริ่มปรับตัวเข้ากับการทำงานได้ดีขึ้น เข้าใจ Process มากขึ้น	-
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	42	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	-	ลงชื่อ.....ณัฐณิชา พรหมรส..... (ณัฐณิชา พรหมรส)	ลงชื่อ.....ชลธิชา เรืองกอง..... (ชลธิชา เรืองกอง)	
จำนวนชั่วโมงรวมทั้งหมด	42	วัน/เดือน/ปี 8/6/18 นักศึกษา	ตำแหน่ง Advisory QA Specialist วัน/เดือน/ปี 8/6/18 ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762. 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่.....2.....

ชื่อ-สกุลนักศึกษา นางสาว ณัฐณิชา พรหมรส์ รหัสนักศึกษา 5812108L-1
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 11/6/61	8	ศึกษา Incident, Problem, Configuration ใน Internal Audit	เข้าใจกระบวนการของ Process มากขึ้น	-
อังคาร 12/6/61	8	ศึกษา ISO 20000-1 ในส่วนของ Scope, General และ Application	เข้าใจว่า ISO 20000 คือ มาตรฐานในการบริหาร งานด้าน IT	-
พุธ 13/6/61	8	ศึกษา ISO20000-1 ในส่วนของ Terms and definitions และ Normative references	เข้าใจข้อกลลุของ ISO20000 ที่ต้องปฏิบัติ	-
พฤหัสบดี 14/6/61	8	ศึกษา Process ใน Internal Audit เรื่อง RLM และ SLM	เข้าใจกระบวนการของ RLM และ SLM	-
ศุกร์ 15/6/61	8	ทราบเอกสารที่ใช้ในการ Audit ไปในส่วนของ Process SLM	เข้าใจกระบวนการตรวจ ต่อมากขึ้น	-
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	40	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	42	ลงชื่อ.....ณัฐณิชา พรหมรส์..... (.....ณัฐณิชา พรหมรส์.....) วัน/เดือน/ปี 15/6/61 นักศึกษา	ลงชื่อ.....รสธิชา เชื้อทอง..... (.....รสธิชา เชื้อทอง.....) ตำแหน่ง Advisory QA Specialist วัน/เดือน/ปี 15/6/61 ผู้ควบคุมการปฏิบัติงาน	
จำนวนชั่วโมงรวมทั้งหมด	82			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 3

ชื่อ-สกุลนักศึกษา ณัฐณิชา พรหมรส์ รหัสนักศึกษา 5812408-1
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 18/6/61	8	ศึกษาเอกสาร Internal Audit และ ทำเอกสารสัมภาษณ์ พิมเอกสาร Implementation Service	เข้าใจการพิมเอกสารของ Service Quality Profile	ยังทำครั้งแรกเลยพิมเยอะ และสอบถามเพิ่มเติม
อังคาร 19/6/61	8	ทำเอกสาร Service quality Profile ทำในส่วน Service name : upgrade / Migrate Service	สรุปใจความสำคัญ และเพิ่มเติมจากเอกสารที่มีอยู่	-
พุธ 20/6/61	8	ทำเอกสาร Service Quality Profile แผนก AMS Service name : Customization / Job Estimation		-
พฤหัสบดี 21/6/61	8	ทำเอกสาร Service Quality Profile แผนก BS Service name : Digital Tranformation Service และ ส่วนเตรียม Audit Process CFM	เข้าใจ Process CFM มากขึ้น เตรียมความพร้อมเพื่อรอตรวจ	-
ศุกร์ 22/6/61	8	เข้าประชุม Internal Audit Process CFM และ สรุป checklist Process CFM	เข้าใจการทำงาน Audit ในส่วนของ Process CFM	ยังไม่เข้าใจระบวนการภายในของ CI ที่มีการเปลี่ยน Change
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	40	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	40	ลงชื่อ ณัฐณิชา พรหมรส์	ลงชื่อ ชลธิชา เรืองทอง	
จำนวนชั่วโมงรวมทั้งหมด	122	(ณัฐณิชา พรหมรส์)	(ชลธิชา เรืองทอง)	
		วัน/เดือน/ปี 22/06/61	ตำแหน่ง Advisory QA Specialist	
		นักศึกษา	วัน/เดือน/ปี 22/06/61	
			ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์
สัปดาห์ที่ 4

ชื่อ-สกุลนักศึกษา หม่าง ณัฐณิชา พรหมมาส รหัสนักศึกษา 5816108G-1
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 25/6/61	8	สรุป checklist CFM ที่ Audit มา และสนับสนุนการทำ Service quality Profile	มีความรู้ความเข้าใจเรื่อง CFM มากขึ้น	-
อังคาร 26/6/61	8	สนับสนุนการทำ Service quality Profile Check Customer ว่าอยู่ใน Service Type ไหน	เข้าใจลักษณะงานมากขึ้น มีทักษะเพิ่มขึ้น	-
พุธ 27/6/61	8	ศึกษา Process Incident และ Problem เพื่อไปในการไป Internal Audit	มีความรู้ความเข้าใจเรื่อง Incident และ Problem	-
พฤหัสบดี 28/6/61	8	Internal Audit ใน Process ของ Incident และ Problem สัมภาษณ์พร้อมหลักฐานและสอบทาน	ได้ทำงานร่วมกับผู้มีความเข้าใจมากขึ้นใน Process	ในทฤษฎีมีความเข้าใจพอแต่ case งานจริงมีความไม่เข้าใจบาง case ว่าเป็น Incident ไหน
ศุกร์ 29/6/61	8	สนับสนุนในการสรุปหลักฐานใน Process Incident และ Problem และ สรุปงานลงใน checklist	มีความชำนาญมากขึ้นในการทำ checklist	-
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	40	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ
จำนวนชั่วโมงในรายงานฉบับก่อน	40	ลงชื่อ ณัฐณิชา พรหมมาส (ณัฐณิชา พรหมมาส) วัน/เดือน/ปี 29/6/61 นักศึกษา	ลงชื่อ ชลธิชา เรืองทอง (ชลธิชา เรืองทอง) ตำแหน่ง Advisory QA specialist วัน/เดือน/ปี 29/6/61 ผู้ควบคุมการปฏิบัติงาน
จำนวนชั่วโมงรวมทั้งหมด	162		

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 5

ชื่อ-สกุลนักศึกษา นางสาว ณัฐณิชา พรหมมาส รหัสนักศึกษา 58121086-1
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 2/7/61	8	สนับสนุนในการสรุป Process Problem และ ให้ checklist และ ศึกษา Process CFM	มีความสำคัญในการทำ checklist	-
อังคาร 3/7/61	8	ศึกษา Process CPM และ แปลเอกสาร Process, Policy ของ Process CPM	มีความเข้าใจใน Process CPM มากขึ้น	ยังไม่เห็นสถานการณ์จริง จึงยังไม่เข้าใจมากนัก
พุธ 4/7/61	8	สนับสนุนการทำ Service Quality Profile เรื่อง IT Safe และ Data safe	มีความสำคัญในการทำ Service Quality Profile	ข้อมูลยังมาไม่ครบถ้วน งานจึงยังไม่สมบูรณ์
พฤหัสบดี 5/7/61	8	สนับสนุนการทำ Service Quality Profile เรื่อง Supplementary Service	เข้าใจระบบการทำงานมากขึ้น	-
ศุกร์ 6/7/61	8	สนับสนุนการทำ Service Quality Profile เรื่อง Upgrade Migrade Service	มีความรู้เพิ่มเติมเรื่อง Upgrade , Migrade	-
เสาร์ ../../..				
อาทิตย์ ../../..				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	40	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	40	ลงชื่อ ณัฐณิชา พรหมมาส (ณัฐณิชา พรหมมาส) วัน/เดือน/ปี 6/7/61 นักศึกษา	ลงชื่อ ชลธิชา เรืองกฤว (ชลธิชา เรืองกฤว) ตำแหน่ง Advisory QA Specialist วัน/เดือน/ปี 6/7/61 ผู้ควบคุมการปฏิบัติงาน
จำนวนชั่วโมงรวมทั้งหมด	202			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 6

ชื่อ-สกุลนักศึกษา นางสาว ณัฐณิชา พรหมมล์ **รหัสนักศึกษา** 58121036-1

คณะวิชา เทคโนโลยีสารสนเทศ **สาขาวิชา** เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 9/7/61	8	ศึกษาเรื่อง CPM (Capacity Management) และ สรุป, เช็ค Service Quality Profile	-	-
อังคาร 10/7/61	8	ประชุม Internal Audit เรื่อง CPM และ แก้ไข เพิ่มเติมข้อมูล Service Quality Profile	พยายามเก็บข้อมูลระบบการในบริษัทให้เข้าใจ	ไม่เข้าใจระบบการในของบริษัท
พุธ 11/7/61	8	สรุปผลการ Audit และ สรุปผล Checklist และ ทำการศึกษา Internal Audit เรื่อง CHM	เข้าใจระบบการของบริษัทมากขึ้น	มีบางระบบที่ยังไม่เข้าใจ ต้องสอบถามจะเริ่มดำเนินการไหน
พฤหัสบดี 12/7/61	8	ศึกษาเรื่อง CHM (Change Management Process) และ RLM Process	เข้าใจเรื่องของ CHM มากขึ้น	-
ศุกร์ 13/7/61	8	ประชุม Internal Audit เรื่อง CHM และ สรุปงานในการทำ checklist CHM และ RLM	มีความเข้าใจมากขึ้นเพราะได้ลงมือทำจริง เห็นจริง	ยังมีประเด็นที่ยังไม่ลงตัว ทำให้ยังไม่ได้สรุป
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	40	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ ณัฐณิชา พรหมมล์ (ณัฐณิชา พรหมมล์) วัน/เดือน/ปี 13/7/61 นักศึกษา	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ ชลธิชา เรืองกอง (ชลธิชา เรืองกอง) ตำแหน่ง Advisory QA Specialist วัน/เดือน/ปี 13/7/61 ผู้ควบคุมการปฏิบัติงาน
จำนวนชั่วโมงในรายงานฉบับก่อน	40			
จำนวนชั่วโมงรวมทั้งหมด	242			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 7

ชื่อ-สกุลนักศึกษา นางสาวณัฐณิชา พรหมมล รหัสนักศึกษา 5812108-1
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 16/7/61	8	สนับสนุนการทำ Checklist CHM และ RLM สรุปผลการตรวจลงใน Checklist CPM	เข้าใจกระบวนการของ CHM และ RLM ทั้ง Policy และ Process	–
อังคาร 17/7/61	8	สนับสนุน และ ปรับปรุงการทำ Checklist CPM และดู Checklist SLM สรุปเพื่อเก็บหลักฐาน	รู้ Process ของ CPM และดูหลักฐานเป็น	–
พุธ 18/7/61	8	สนับสนุนในการตรวจหลักฐาน SLA, OLA และ UC ใน Process ของ SLM	สามารถตรวจหลักฐาน SLA, OLA และ UC เป็น	เอกสารมีจำนวนเยอะมาก ทำให้เกิดความสับสนได้
พฤหัสบดี 19/7/61	8	อ่าน และแปล Policy ของ ITSMR ในเรื่องของ CSI และ SMS	ทำความเข้าใจ Policy ของ ITSMS	แปลเอกสารเลือกใช้คำไม่ถูก
ศุกร์ 20/7/61	8	แปลเอกสาร Design and Transition of New or Changed Services Process	เข้าใจ Process DTN มากขึ้น	–
เสาร์ ...../...../.....				
อาทิตย์ ...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	40	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	40	ลงชื่อ ณัฐณิชา พรหมมล (ณัฐณิชา พรหมมล)	ลงชื่อ รสริชา เสื่องทอง (รสริชา เสื่องทอง)	
จำนวนชั่วโมงรวมทั้งหมด	282	วัน/เดือน/ปี 20/7/61 นักศึกษา	ตำแหน่ง Advisory QA Specialist วัน/เดือน/ปี 20/7/61 ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่.....8.....

ชื่อ-สกุลนักศึกษา ...ปาณสาวณัฐณิชา พรหมมล์... รหัสนักศึกษา ...5812103241...
คณะวิชา ...เทคโนโลยีสารสนเทศ... สาขาวิชา ...เทคโนโลยีสารสนเทศ...

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 23/7/61	8	อ่านและแปลเอกสาร Service Improvement Procedure และ SMS Procedure	เข้าใจ Procedure ของ SMS และ Service Improv	–
อังคาร 24/7/61	8	อ่านและแปลเอกสาร Supplier Management Policy และดู Checklist ปี 2017	เข้าใจ Policy ของ SPM มากขึ้น	–
พุธ 25/7/61	8	ศึกษาอ่านทบทวนเพิ่มเติม Audit ITSMR เพิ่มเติม สนับสนุนการทำ Checklist ITSMR	มีความชำนาญในการทำ Checklist มากขึ้น	–
พฤหัสบดี 26/7/61	8	ประชุม Internal Audit เรื่อง ITSMR และ สนับสนุนการทำ Checklist ITSMR	เข้าใจและขยายการมากขึ้น ได้แนวทางในการทำงาน	–
ศุกร์ 27/7/61	–	หยุดวันอาสาฬหบูชา	–	–
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	32	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	40	ลงชื่อ.....ณัฐณิชา พรหมมล์..... (.....ณัฐณิชา พรหมมล์.....)	ลงชื่อ.....รสชิตา เชื้อทอง..... (.....รสชิตา เชื้อทอง.....)	
จำนวนชั่วโมงรวมทั้งหมด	314	วัน/เดือน/ปี.....26/7/61..... นักศึกษา	ตำแหน่ง.....Advisory QA Specialist..... วัน/เดือน/ปี.....26/7/61..... ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 9

ชื่อ-สกุลนักศึกษา ทางสาวณัฐณิชา พรหมมาส์ รหัสนักศึกษา 58121086-1
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 30/7/61	–	หยุดชดเชย วันเฉลิมพระชนมพรรษา พระบาทสมเด็จพระเจ้าอยู่หัว	–	–
อังคาร 31/7/61	8	ศึกษา Process, Policy ของ SPM และ ดูเพื่อหา Checklist SPM	เข้าใจ Process, Policy SPM มากขึ้น	–
พุธ 1/8/61	9	ประชุม Internal Audit ของ Process SPM และ สนับสนุนการทำ Checklist SPM	เข้าใจกระบวนการทำงาน ของ Process SPM	ยังไม่คล่องเข้าใจกระบวนการดำเนินงาน
พฤหัสบดี 2/8/61	8	สนับสนุนการทำ Checklist SPM และ สรุปหลักฐาน, ใบ CAR	เข้าใจการดำเนินงาน มากขึ้น	–
ศุกร์ 3/8/61	8	สนับสนุนการทำ Checklist ITSMR ลงแบบ Form และ สรุปหลักฐาน	มีความชำนาญในการทำ Checklist มากขึ้น	–
เสาร์ ../../..				
อาทิตย์ ../../..				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	33	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ ณัฐณิชา พรหมมาส์ (ณัฐณิชา พรหมมาส์) วัน/เดือน/ปี 3/8/61 นักศึกษา	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ รสริชา เรืองทอง (รสริชา เรืองทอง) ตำแหน่ง Advisory QA Specialist วัน/เดือน/ปี 3/8/61 ผู้ควบคุมการปฏิบัติงาน
จำนวนชั่วโมงในรายงานฉบับก่อน	32			
จำนวนชั่วโมงรวมทั้งหมด	347			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 10

ชื่อ-สกุลนักศึกษา ณัฐณิชา พรหมมาส์ รหัสนักศึกษา 58121086-1
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 6/8/61	8	ศึกษาเอกสาร Information Security Management และ Password Creation Policy	มีความรู้ในการตั้งรหัสผ่านที่มีความปลอดภัย	-
อังคาร 7/8/61	8	ศึกษาเอกสาร Information Security Management และ Disposal of Media	มีความเข้าใจเกี่ยวกับ CIA มากขึ้น	-
พุธ 8/8/61	8	ศึกษา ISO 27001 เพิ่มเติมเกี่ยวกับ CIA และความปลอดภัยของระบบและการเข้าถึงระบบ	วิเคราะห์เป็นว่าเป็น C, I หรือ A	-
พฤหัสบดี 9/8/61	8	ศึกษาเอกสาร International Standard ISO 27001 เกี่ยวกับ IT General Control	เข้าใจ IT General Control	-
ศุกร์ 10/8/61	8	Audit Information Security Management และทำสรุปข้อมูลที่ Audit ลง Checklist	มีความชำนาญในการทำ Checklist และเข้าใจ ISM	มีเนื้อหา Detail เยอะมาก ทำให้เข้าใจยากเล็กน้อย
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	40	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	33	ลงชื่อ ณัฐณิชา พรหมมาส์	ลงชื่อ รสริชา เชื้อทอง	
จำนวนชั่วโมงรวมทั้งหมด	387	(ณัฐณิชา พรหมมาส์)	(รสริชา เชื้อทอง)	
		วัน/เดือน/ปี 10/8/61	ตำแหน่ง Advisory QA Specialist	
		นักศึกษา	วัน/เดือน/ปี 10/8/61	
			ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา/ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762. 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 11

ชื่อ-สกุลนักศึกษา ณัฐณิชา พรหมมาส รหัสนักศึกษา 58121086-1
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 13/8/61	-	หยุดชดเชยวันแม่	-	-
อังคาร 14/8/61	8	ศึกษา Iso 27001 Control objective and Controls และทำ Powerpoint นำเสนอ	เข้าใจ Control objective และ Controls A5-A15	ต้องทำการศึกษาด้วยตนเอง หาข้อมูลด้วยตนเอง
พุธ 15/8/61	8	ทำ powerpoint นำเสนอ ISO27001 เกี่ยวกับเรื่อง Annex A ใน Standard ทั้งแท่ A5-A10	เข้าใจ Annex มากขึ้น ในหัวข้อที่ศึกษา	-
พฤหัสบดี 16/8/61	8	ศึกษา Standard ISO 27001 และ Checklist ของ ISo27001 และทำ powerpoint เพิ่มเติม	เข้าใจการทำ Checklist ของ ISO27001	
ศุกร์ 17/8/61	8	present powerpoint ISO 27001 ให้พี่ฟังเพื่อเปรียบเทียบ ISo27000 กับ Iso27001 ที่เพิ่มเติม	ฝึกการพูดในการ present งานให้พี่ฟัง	-
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	32	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ ณัฐณิชา พรหมมาส (ณัฐณิชา พรหมมาส) วัน/เดือน/ปี 17/08/18 นักศึกษา	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ รลธิชา เรืองทอง (รลธิชา เรืองทอง) ตำแหน่ง Advisory QA Specialist วัน/เดือน/ปี 17/08/18 ผู้ควบคุมการปฏิบัติงาน	
จำนวนชั่วโมงในรายงานฉบับก่อน	40			
จำนวนชั่วโมงรวมทั้งหมด	419			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่....12.....

ชื่อ-สกุลนักศึกษา ณัฐณิชา พรหมมล รหัสนักศึกษา 5812106-1
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 20/8/61	9	ประชุม Internal Audit เรื่อง BRM และ scan ใบ CAR เอา Update ขึ้น Alfresco	scan ใบ CAR เป็น check ใบ CAR เป็น	-
อังคาร 21/8/61	8	สรุปประชุม Internal Audit ลงใน Checklist และ scan ใบ CAR เอา Update ขึ้น Alfresco	เข้าใจ Process BRM มากขึ้น	ไม่รู้เรื่องศัพท์มากนัก ทำให้เข้าใจพื้นๆ
พุธ 22/8/61	8	ศึกษาเก็บรายละเอียด ISO27001 เกี่ยวกับ เรื่อง Annex A เพื่อหา GAP มาตั้งประเด็น	รู้เกี่ยวกับ Annex A ใน หัวข้อย่อยมากขึ้น	-
พฤหัสบดี 23/8/61	8	list ประเด็น GAP ออกมา และตั้งคำถามเพื่อ ถามหาข้อมูลเพิ่มเติม	ได้หัวข้อย่อยในการทำงาน และรายละเอียดเพิ่ม	-
ศุกร์ 24/8/61	8	นำคำถามไปถามเพื่อหาความแตกต่างในการทำงาน ISO20000 และ ISO27001 แล้วเพิ่มข้อมูลที่ได้ลง	ได้ GAP มาใช้ในการทำงาน	-
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	41	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	32	ลงชื่อ.....ณัฐณิชา พรหมมล..... (.....ณัฐณิชา พรหมมล.....)	ลงชื่อ.....รสธิชา เสือทอง..... (.....รสธิชา เสือทอง.....)	
จำนวนชั่วโมงรวมทั้งหมด	460	วัน/เดือน/ปี.....24/8/61..... นักศึกษา	ตำแหน่ง Advisory QA Specialist วัน/เดือน/ปี.....24/8/61..... ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 13

ชื่อ-สกุลนักศึกษา ณัฐณิชา พรหมมาส รหัสนักศึกษา 58121086-1
คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 27/8/61	8	หา Document ที่ใช้ใน ISO27001 และ ศึกษา ISO27001 Version 2013 และทำสไลด์นำเสนอ	รู้ ISO27001 Version ล่าสุด และ GAP ที่ต่างกันของ Ver.	หาข้อมูลค่อนข้างยาก และ เยอะ
อังคาร 28/8/61	8	ศึกษา ISO27001 Version 2013 และ A5-A18 ใน Annex A ที่เพิ่มขึ้นมา และทำสไลด์นำเสนอ	ทราบ A5-A18 ที่เพิ่มขึ้นมาจากเดิม	-
พุธ 29/8/61	9	ศึกษา Cloud Security Alliance - Security, Trust & Assurance Registry และ ISO27001 เพื่อนำมาเขียนในสไลด์ที่จะนำไปนำเสนอ	ทราบวิธีการยกระดับความปลอดภัยให้กับ Cloud	หาข้อมูลน้อยเพราะข้อมูลส่วนใหญ่เป็นภาษาอังกฤษ
พฤหัสบดี 30/8/61	8	ศึกษา CSA-STAR ต่อ และ present กับพี่เลี้ยง ห้า DOC ที่ควรมีใน ISO27001 มาเทียบกับที่ใช้กันมี เพื่อหาความแตกต่าง และ สิ่งที่ควรเพิ่มเติม	วิเคราะห์ความต่างของ DOC และเพิ่มเติมได้	หาข้อมูลมา support ยาก DOC มันเป็นความลับ เพื่อนๆไม่สามารถหาได้
ศุกร์ 31/8/61	8	เปรียบเทียบ DOC ของ ISO27001 ทั้งแต่ A5-A18 กับ DOC ที่มีอยู่ของบริษัทหาความแตกต่างกันอะไร	กระบวนการวิเคราะออกแบบ form	หาข้อมูล Support แต่ละเอกสารค่อนข้างยาก
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	41	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	41	ลงชื่อ ณัฐณิชา พรหมมาส (ณัฐณิชา พรหมมาส) วัน/เดือน/ปี 31/8/61 นักศึกษา	ลงชื่อ ชลธิชา เชื้อทอง (ชลธิชา เชื้อทอง) ตำแหน่ง Advisory QA Specialist วัน/เดือน/ปี 31/8/61 ผู้ควบคุมการปฏิบัติงาน	
จำนวนชั่วโมงรวมทั้งหมด	501			

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 14

ชื่อ-สกุลนักศึกษา กัญญ์ณิชา พรหมมาส รหัสนักศึกษา 58121066-1

คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 3/9/61	8	list Document name ใน ISO 27001 ลงใน excel และ Map กับ Standard	ทราบถึง Document name ใน ISO27001	หาไฟล์สนับสนุนค่อนข้างยาก
อังคาร 4/9/61	8	list Document name เพิ่มเติม และ Map Standard เทียบกับ ISO20000 ที่มีอยู่	เปรียบเทียบความแตกต่างและความคล้าย	Document name ต่างต่างกัน ทำให้ต้องหา
พุธ 5/9/61	9	Check Document name ของ ISO27001 และ ISO20000 ที่มีอยู่ และใส่อ้างอิงเอกสาร	เข้าใจเนื้อหามากขึ้น และใช้ Alfresco เป็น	-
พฤหัสบดี 6/9/61	8	Check Document ของ A-host และของ ISO 27001 เทียบกัน และหาความต่าง	ทราบถึง ความต่างของ A-host และ ISO27001	-
ศุกร์ 7/9/61	8	Document name ที่เหลืออยู่นำมาตั้งต่างตาม และ presentation ในครั้งต่อไป	มีทักษะการตั้งต่างตาม	-
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	41	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	41	ลงชื่อ กัญญ์ณิชา พรหมมาส (กัญญ์ณิชา พรหมมาส)	ลงชื่อ ชลธิชา เรืองทอง (ชลธิชา เรืองทอง)	
จำนวนชั่วโมงรวมทั้งหมด	542	วัน/เดือน/ปี 7/9/61 นักศึกษา	ตำแหน่ง Advisory QA Specialist วัน/เดือน/ปี 7/9/61 ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 15

ชื่อ-สกุลนักศึกษา ณัฐณิชา พรหมมล์ รหัสนักศึกษา 5812T086-1

คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 10/9/61	8	แปลเอกสาร Budgeting and Accounting for Service Policy และ Present GAP ISO27001	เข้า Policy ของ BAM และทักษะ Present	ทำงานไม่ทันตรงตามเวลาที่กำหนด
อังคาร 11/9/61	9	ทำ Document ISO27001 รายละเอียดแต่ละเอกสาร และเปรียบเทียบ GAP กับ เอกสารของบริษัท จำนวนหน้าตามเข้าไป	เข้าใจ Document ใน ISO 27001 ว่าต้องมีอะไรบ้าง	ทำงานแข่งกับ เวลา และนำมาแก้ปัญหาก่อนเวลาส่ง
พุธ 12/9/61	8	ทำ GAP ลงใน excel เพื่อให้พี่เลี้ยงวิเคราะห์และพิจารณา และ ทำไป Present ให้ผู้เชี่ยวชาญฟังช่วงใหม่ Confirm การวิเคราะห์	เรียนรู้การคัดวิเคราะห์จากผู้เชี่ยวชาญและพี่เลี้ยง	ยังเป็นห่วงสิ่งที่ทำและทำความเข้าใจเพิ่ม
พฤหัสบดี 13/9/61	8	แปลเอกสาร Budgeting and Accounting for Service Process และ ทำ GAP Excel เพิ่มเติม	เข้าใจ Process ของ BAM และมีทักษะ GAP เพิ่ม	-
ศุกร์ 14/9/61	8	ทำ Slide Presentation ของ A-Host และทำ Document ISO27001 ที่สามารถเพิ่มเติมและเตรียมใส่ข้อมูล comment ถึงความแตกต่าง	ทักษะการทำ Slide Present และการใส่ข้อมูล	-
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	41	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	41	ลงชื่อ ณัฐณิชา พรหมมล์	ลงชื่อ รสริชา เชื้อกอง	
จำนวนชั่วโมงรวมทั้งหมด	583	(ณัฐณิชา พรหมมล์) วัน/เดือน/ปี 14/9/61 นักศึกษา	(รสริชา เชื้อกอง) ตำแหน่ง Advisory QA Specialist วัน/เดือน/ปี 13/9/61 ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้ เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762, 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 16

ชื่อ-สกุลนักศึกษา ณัฐณิชา พรหมเส รหัสนักศึกษา 58121086-1

คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 17/9/61	8	ทำสไลด์ Present นโยบายเกี่ยวกับ ISO20000 และ ISO27001 และ เข้าประชุม Internal Audit ใน Process BAM	ความรู้เรื่อง BAM มากขึ้น มีทักษะการจดที่ดี	-
อังคาร 18/9/61	9	Review Slide และ แก้ไข Slide Presentation และทำ GAP ISO27001 และ ISO20000 ต่อ	เข้าใจหน้าที่ และ เรื่องที่ทำมากขึ้น	หาข้อมูลยาก และ เนื้อหาเยอะ
พุธ 19/9/61	8	แก้ไข Slide Presentation เพิ่มเติม และ ศึกษาความแตกต่างของเอกสาร A-host และ ISe	เข้าใจ GAP ของเอกสาร นโยบาย และ ISO27001 เพิ่ม	การจัดการเวลา ในการทำงาน ให้ทัน
พฤหัสบดี 20/9/61	11	Presentation อัด VDO ของนโยบาย และ Review GAP ISO27001 และ ISO20000	มีความกล้าแสดงออก และ เข้าใจงาน	ทำงานเร่งกับเวลา
ศุกร์ 21/9/61	10	Presentation GAP กับ ผู้เชี่ยวชาญ และ พี่เลี้ยง และ ใส่ Comment อธิบายความต่าง	มีทักษะการสื่อ และ ทักษะภาษาเพิ่มขึ้น	ศัพท์เฉพาะทาง ที่ค่อนข้าง ยากต้องจำเพิ่ม
เสาร์ ../../..				
อาทิตย์ ../../..				
จำนวนชั่วโมงรวม ในรายงานฉบับนี้	46	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมง ในรายงานฉบับก่อน	41	ลงชื่อ ณัฐณิชา พรหมเส	ลงชื่อ ชลธิชา เชื้อทอง	
จำนวนชั่วโมง รวมทั้งหมด	629	(ณัฐณิชา พรหมเส)	(ชลธิชา เชื้อทอง)	
		วัน/เดือน/ปี 21/9/61	ตำแหน่ง Advisory QA Specialist	
		นักศึกษา	วัน/เดือน/ปี 21/9/61	
			ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้ เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์สหกิจศึกษาและจัดหางาน สถาบันเทคโนโลยีไทย - ญี่ปุ่น
Co-operative Education and Career Center
1771/1 ถนนพัฒนาการ แขวงสวนหลวง เขตสวนหลวง กรุงเทพฯ 10250 โทรศัพท์: 0-2763-2762. 02-763-2750 Fax: 0-2763-2600 ต่อ 2788 www.tni.ac.th

แบบฟอร์มรายงานการปฏิบัติงานประจำสัปดาห์

สัปดาห์ที่ 17

ชื่อ-สกุลนักศึกษา ณัฐณิชา พรหมรส รหัสนักศึกษา 5812105 6-1

คณะวิชา เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ความรู้/ทักษะที่ได้รับ	ปัญหา/อุปสรรค
จันทร์ 24/9/61	9	แปล Process, Policy ของ SCM & AVM ประชุม Internal Audit SCM & AVM	เข้าใจการทำงานให้เกิด downtime น้อยที่สุด	มีบางเรื่องที่ไม่เข้าใจ ก็ทำให้ไม่เข้าใจ และ ศัพท์เทคนิคเยอะมาก
อังคาร 25/9/61	8	Up file งานที่ทำขึ้น Alfresco และ สรุปผล mr Audit SCM & AVM ลงใน Checklist และ ทำรูปเล่มในแต่ละบทเพิ่ม	รู้จักการสรุปผลที่ดี และ แบ่งการทำงานดี	แบ่งกับเวลาที่มีอยู่มากเกินไป
พุธ 26/9/61	8	ใส่ Annex A ISO27001 ให้การกับ Document ในแต่ละหัวข้อ และอ่านทำความเข้าใจเอกสาร หาข้อมูลเอกสารเพิ่มเติม และ Checklist	เข้าใจ Annex A ใน ISO27001 มากขึ้น	ต้องดี scope GAP ให้ลงลึก หาข้อมูลเพิ่มเติม
พฤหัสบดี 27/9/61	8	หาข้อมูลว่า Certificate ISO27001 มีกี่ระดับ มีอะไรบ้าง ดำเนินการอย่างไร และดี Scope GAP	การวิเคราะห์ scope GAP	—
ศุกร์ 28/9/61	8	หาข้อมูล Cloud เกี่ยวกับ Certificate ISO27001 มีสิ่งใดบ้าง ดำเนินการอย่างไร และหาแนวทางในการดำเนินงาน ทำบท 3 ต่อ	จัดหน้าการดำเนินงานให้มีความยุ่งยากขึ้น	หาข้อมูลที่แน่ชัดของ Certificate ยากมาก ต้องถามผู้เชี่ยวชาญ
เสาร์...../...../.....				
อาทิตย์...../...../.....				
จำนวนชั่วโมงรวมในรายงานฉบับนี้	41	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ	
จำนวนชั่วโมงในรายงานฉบับก่อน	46	ลงชื่อ ณัฐณิชา พรหมรส	ลงชื่อ รลธิชา เสืองทอง	
จำนวนชั่วโมงรวมทั้งหมด	670	(ณัฐณิชา พรหมรส)	(รลธิชา เสืองทอง)	
		วัน/เดือน/ปี 28/9/61	ตำแหน่ง Advisory QA Specialist	
		นักศึกษา	วัน/เดือน/ปี 28/9/61	
			ผู้ควบคุมการปฏิบัติงาน	

หมายเหตุ นักศึกษาต้องส่งรายงานฉบับนี้ถึงอาจารย์ที่ปรึกษาสหกิจศึกษา / ฝึกงานทุกคณะวิชา ทุกสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้เพื่อทำรายงานฉบับสมบูรณ์

ประวัติผู้จัดทำโครงงาน

ชื่อ – สกุล นางสาวณัฐณิชา พรหมรส

วัน เดือน ปีเกิด วันอาทิตย์ที่ 25 กุมภาพันธ์ พ.ศ. 2539

ประวัติการศึกษา

ระดับประถมศึกษา ประถมศึกษาตอนปลาย พ.ศ. 2551
โรงเรียนเซนต์โยเซฟ บางนา

ระดับมัธยมศึกษา มัธยมศึกษาตอนปลาย พ.ศ. 2557
โรงเรียนเซนต์โยเซฟ บางนา

ระดับอุดมศึกษา คณะเทคโนโลยีสารสนเทศ สาขาเทคโนโลยีสารสนเทศ พ.ศ. 2558
สถาบันเทคโนโลยีไทย – ญี่ปุ่น

ทุนการศึกษา - ไม่มี -

ประวัติการฝึกอบรม 1. มาตรฐาน ISO 20000 Internal Audit
2. กระบวนการทำงานของ ISO 20000

ผลงานที่ได้รับการตีพิมพ์ - ไม่มี -

สถาบันเทคโนโลยีไทย-ญี่ปุ่น
THAI - NICHI INSTITUTE OF TECHNOLOGY
TNI