การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT

ภาพร ภิยโยดิลกชัย

งานค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2553

Information Technology Auditing by COBIT

Paporn Piyayodilokchai

An Independent Study Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science (Computer and Communication Technology)

Department of Computer and Communication Technology

Graduate School, Dhurakij Pundit University

2010

กิตติกรรมประกาศ

งานค้นคว้าอิสระฉบับนี้สำเร็จลุล่วงได้ด้วยความช่วยเหลือจากบุคคลมากมายที่ขอกล่าวถึงด้วยความขอบพระคุณ

ผู้เขียนขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์ ซึ่งได้ให้คำแนะนำและเสียสละเวลาอันมีค่าของท่านรับเป็นอาจารย์ที่ปรึกษางานค้นคว้าอิสระ และได้กรุณาแนะนำความรู้และสิ่งที่เป็นประโยชน์อย่างอเนกประการ ในการช่วยปรับปรุงงานค้นคว้าอิสระฉบับนี้ ผู้เขียนขอขอบพระคุณ รองศาสตราจารย์ ดร.ณรงค์ มั่งคั่ง ประธานกรรมการสอบงานค้นคว้าอิสระ และ อาจารย์ ดร.ประศาสน์ จันทราทิพย์ กรรมการผู้ทรงคุณวุฒิ ที่ได้สละเวลามาเป็นคณะกรรมการสอบงานค้นคว้าอิสระ ตลอดจนให้ข้อคิดเห็นอันเป็นประโยชน์ ในการทำให้งานค้นคว้าอิสระฉบับนี้ มีคุณค่ามากยิ่งขึ้น

ผู้เขียนขอกราบขอบพระคุณคุณยายและคุณปู่คุณย่าของหลาน ๆ ซึ่งให้การสนับสนุนและให้กำลังใจแก่ผู้เขียนตลอดมา โดยเฉพาะอย่างยิ่งคุณย่าที่ช่วยกรุณาดูแลหลาน ๆ ในช่วงระยะเวลาที่ผู้เขียนทำการศึกษาและจัดทำงานค้นคว้าอิสระฉบับนี้

ผู้เขียนขอขอบพระคุณท่านอาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้แก่ผู้เขียน

ท้ายสุด ผู้เขียนขอขอบคุณนายสุชาติ ภิยโยดิลกชัย สามีผู้เขียน ที่ได้ให้การสนับสนุนและให้กำลังใจผู้เขียนในทุก ๆ ด้านมาโดยตลอด และช่วยดูแลบุตร ซึ่งทำให้ผู้เขียนสามารถทุ่มเทเวลาในการศึกษาและจัดทำงานค้นคว้าอิสระฉบับนี้

ผู้เขียนหวังเป็นอย่างยิ่งว่า งานค้นคว้าอิสระฉบับนี้ จะเป็นประโยชน์กับผู้ที่ต้องการศึกษาด้านการตรวจสอบระบบเทคโนโลยีสารสนเทศ และหากมีข้อผิดพลาดประการใดในงานค้นคว้าอิสระฉบับนี้ ผู้เขียนต้องกราบขออภัยเป็นอย่างสูงมา ณ ที่นี้ด้วย

ภาพร ภิยโยดิลกชัย

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญตาราง(ต่อ)

สารบัญตาราง(ต่อ)

สารบัญภาพ

หัวข้องานค้นคว้าอิสระ การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT

ชื่อผู้เขียน ภาพร ภิยโยดิลกชัย

อาจารย์ที่ปรึกษางานค้นคว้าอิสระ ผู้ช่วยศาสตราจารย์ ดร.ประณต บุญไชยอภิสิทธิ์

สาขาวิชา เทคโนโลยีคอมพิวเตอร์และการสื่อสาร

ปีการศึกษา 2553

บทคัดย่อ

งานค้นคว้าอิสระ การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT เป็นการศึกษารวบรวมข้อมูลเกี่ยวกับเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ความเสียหายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ การตรวจสอบระบบเทคโนโลยีสารสนเทศ และ COBIT FRAMEWORK เพื่อนำกรอบมาตรฐานของ COBIT มาใช้เป็นแนวทางในการจัดทำแนวการตรวจสอบระบบเทคโนโลยีสารสนเทศตามโครงสร้างของมาตรฐาน COBIT บนพื้นฐานของกระบวนการทางธุรกิจ 4 กระบวนการหลัก (Domain) ได้แก่ การวางแผนและการจัดการองค์กร (PO : Planning and Organization) การจัดหาและติดตั้ง (AI : Acquisition and Implementation) การส่งมอบและบำรุงรักษา (DS : Delivery and Support) การติดตามผล (M : Monitoring)

แนวการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT นั้น ผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถนำมาใช้เป็นเครื่องมือในการปฏิบัติงานตรวจสอบ และหัวหน้าหน่วยงานตรวจสอบสามารถใช้เป็นเครื่องมือในการสอบทานและควบคุมงาน ซึ่งทำให้การตรวจสอบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างครอบคลุมตามระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร และบรรลุวัตถุประสงค์ของการตรวจสอบ อย่างไรก็ตาม รายละเอียดของการนำไปปฏิบัติในกระบวนการต่าง ๆ ในมาตรฐาน COBIT ผู้ตรวจสอบจะต้องพิจารณาข้อมูลเพิ่มเติมจาก FRAMEWORK อื่น ๆ เช่น มาตรฐาน ISO/IEC 27001, ISO/IEC 17799, ISO/IEC 13335, ISO/IEC 15408 และ ITIL (IT Infrastructure Library) ตลอดจนเครื่องมือต่าง ๆ ที่ใช้สำหรับบริหารจัดการระบบเทคโนโลยีสารสนเทศ เช่น PRINCE 2, PMBOX, TickIT และ TOGAF 8.1

Independent Study Title Information Technology Auditing by COBIT

Author Paporn Piyayodilokchai

Independent Study Advisor Assistant Professor Dr.Pranot Boonchai-Apisit

Department Computer and Communication Technology

Academic Year 2010

ABSTRACT

Independent study Information Technology Auditing by COBIT , the data is gathered about the information technology, risk of the information technology, damage from use of the information technology, the information technology auditing and COBIT FRAMEWORK to cover the COBIT FRAMEWORK as the guideline to prepare the audit program for information technology auditing based on the structure of the COBIT FRAMEWORK on the 4 main business processes (Domain) i.e. PO : Planning and Organization, AI : Acquisition and Implementation, DS : Delivery and Support, M : Monitoring.

The audit program for the information technology auditing by COBIT, the auditor of the information technology could use it as the tool on the audit, and the chief of the audit unit could use as the tool for review and supervision. The audit of the information technology could be done to cover the risk of the information technology of the organization and to achieve the objectives of audit. However, the details of the application in the procedures of the COBIT FRAMEWORK, the auditor must consider additional data from other framework i.e. ISO/IEC 27001, ISO/IEC 17799, ISO/IEC 13335, ISO/IEC 15408 and ITIL (IT Infrastructure Library) as well as tools used for management of the information technology i.e. PRINCE 2, PMBOX, TickIT and TOGAF 8.1.

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

ในโลกปัจจุบัน เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานขององค์กร ทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผลระบบงานสำคัญต่าง ๆ ซึ่งหากเป็นธุรกิจรับประกันวินาศภัยจะมีการนำเทคโนโลยีสารสนเทศมาใช้สำหรับการประมวลผลระบบงานที่เกี่ยวกับการรับประกันภัย การรับชำระหนี้ การจ่ายค่าสินไหมทดแทน การบริหารจัดการ ตลอดจนระบบงานบัญชี เทคโนโลยีสารสนเทศเป็นโครงสร้างพื้นฐานที่สำคัญในการสนับสนุนการทำธุรกรรม และในการดำเนินงานตั้งแต่การใช้บันทึกรายการธุรกิจที่เกิดขึ้นประจำวัน การให้บริการลูกค้าและให้ข้อมูลสำหรับผู้บริหารในการตัดสินใจ และให้ระบบสารสนเทศที่จะเป็นเครื่องมือที่ช่วยให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพลดต้นทุน เพิ่มขีดความสามารถในการแข่งขัน

ในขณะเดียวกันการนำเทคโนโลยีสารสนเทศมาใช้ก็มีความเสี่ยงหลายประการที่ควรคำนึงถึง ซึ่งหากองค์กรไม่มีการบริหารจัดการและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอ ก็อาจส่งผลกระทบต่อการดำเนินงานหรือสร้างความเสียหายต่อองค์กรและลูกค้าได้ ทั้งนี้ ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการประกอบธุรกิจขององค์กร สามารถแบ่งออกเป็น 4 ประเภทหลัก คือ Access Risk, Integrity Risk, Availabily Risk และ Infrastructure Risk

นอกจากความเสี่ยง 4 ประเภทหลักตามที่กล่าวข้างต้น ยังมีความเสี่ยงเกี่ยวกับการที่ผู้บริหารขององค์กรมิได้รับข้อมูลที่เกี่ยวข้องอย่างถูกต้องและทันเวลาเพื่อใช้ประกอบการตัดสินใจทางธุรกิจ ดังนั้น องค์กรก็ควรพิจารณาว่าข้อมูลใดบ้างที่จำเป็นแก่การตัดสินใจ รวมทั้งจัดให้มีระบบการตรวจสอบความถูกต้องของข้อมูล และจัดเตรียมข้อมูลดังกล่าวให้พร้อม เพื่อประโยชน์การดำเนินธุรกิจขององค์กร

นอกจากความเสี่ยงต่าง ๆ ข้างต้นแล้ว หากจะพิจารณาในด้านการพัฒนาระบบงาน ก็มีผลการวิจัยเกี่ยวกับสาเหตุที่หน่วยงานล้มเหลวในการพัฒนาระบบงานคอมพิวเตอร์ (Charles R. Neco: 1989) ได้แก่ ผู้บริหารระดับสูงไม่สนับสนุนหรือไม่มีส่วนร่วมในการพัฒนา หรือไม่มีคณะกรรมการระดับสูง (Steering Committee) ในการพัฒนาระบบงาน การเปลี่ยนความต้องการ

หรือวัตถุประสงค์ของระบบงานบ่อย การเลือกเทคโนโลยีที่ก้าวหน้า ล้ำสมัยเกินกว่าที่พนักงานจะทำความเข้าใจ การขาดคู่มือหรือวิธีการพัฒนาระบบงานให้เป็นขั้นตอนอย่างเป็นมาตรฐาน และบุคลากรที่เกี่ยวข้องกับการพัฒนาระบบมีไม่เพียงพอและได้รับการฝึกอบรมที่ไม่เพียงพอ

ดังนั้น ทุกวันนี้หลายองค์กรในประเทศไทยและทั่วโลก ได้พิจารณาถึง "Best Practices" หรือมาตรฐานที่ควรนำมาเป็นแนวทางในการเตรียมระบบสารสนเทศขององค์กรให้พร้อมเข้าสู่ยุค IT Governance โดยที่ "Best Practices" ที่นิยมใช้กันได้แก่ มาตรฐาน ISO/IEC17799, COBIT และ ITIL เป็นต้น

มาตรฐาน "COBIT" ย่อมาจาก "Control OBjectives for Information and Related Technology" COBIT นั้นมีจุดประสงค์ในการสร้างความมั่นใจว่าการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศนั้นสอดคล้องกับวัตถุประสงค์เชิงธุรกิจขององค์กร (Business Objectives) เพื่อให้เกิดการใช้ทรัพยากรอย่างมีประสิทธิผลอันจะส่งประโยชน์สูงสุดแก่องค์กร ช่วยให้เกิดความสมดุลย์ระหว่างความเสี่ยงด้านเทคโนโลยีสารสนเทศ และผลตอบแทนของการลงทุนในระบบสารสนเทศ โดย COBIT นั้นมีพื้นฐานมาจาก Framework ชั้นนำต่าง ๆ มากมาย ได้แก่ The Software Engineering Institute's Capability Maturity Model (CMM), ISO 9000 และ The Information Technology Infrastructure Library (ITIL) ของประเทศอังกฤษ อย่างไรก็ตาม COBIT นั้นก็ยังขาดในส่วนของ Guideline เพื่อใช้ในทางปฏิบัติเนื่องจาก COBIT เป็น Framework ที่เน้นในเรื่องของการควบคุม (Control) เป็นหลัก

นอกจากนี้ เพื่อป้องกันความเสี่ยงอันเกิดจากเทคโนโลยีสารสนเทศดังกล่าว มาตรการในการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ซึ่งมีมาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่าง ๆ จะต้องนำมาประยุกต์ใช้ในการบริหารจัดการเทคโนโลยีสารสนเทศ โดยมีการควบคุมและตรวจสอบระบบสารสนเทศเป็นสิ่งที่จะช่วยในการติดตามและควบคุมการปฏิบัติตามมาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่าง ๆ ข้างต้น ดังนั้น การตรวจสอบระบบสารสนเทศจึงมีความสำคัญ และเป็นที่มาของการศึกษาวิจัยนี้

1.2 วัตถุประสงค์ของการวิจัย

วัตถุประสงค์ของการวิจัย มีดังต่อไปนี้

1. เพื่อศึกษาเกี่ยวกับการตรวจสอบระบบสารสนเทศ ซึ่งจะช่วยในการป้องกันความเสี่ยงต่าง ๆ ดังกล่าวข้างต้น

2. การนำมาตรฐานของ COBIT Framework มาประยุกต์ในการจัดทำแนวการตรวจสอบระบบสารสนเทศ (Audit Program)

1.3 ขอบเขตของการวิจัย

ขอบเขตของการวิจัย มีดังต่อไปนี้

1. จัดทำแนวการตรวจสอบระบบเทคโนโลยีสารสนเทศ (Audit Program) ซึ่งประกอบด้วย หัวข้อการตรวจสอบ วัตถุประสงค์การตรวจสอบ ความเสี่ยง การควบคุมที่ควรมี และวิธีการทดสอบ/ตรวจสอบ

2. จัดทำข้อมูลกรณีศึกษาในการนำแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ (Audit Program) มาใช้ในการตรวจสอบ

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับ มีดังต่อไปนี้

1. มีแนวทางการตรวจสอบระบบสารสนเทศ ซึ่งครอบคลุมถึงมาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่าง ๆ

2. องค์กรสามารถสร้างระบบการควบคุมทางด้านระบบสารสนเทศที่ยังขาดอยู่ เพื่อลดความเสี่ยงของระบบสารสนเทศ

3. การบริหารจัดการภายในองค์กร สามารถบรรลุวัตถุประสงค์ในการดำเนินธุรกิจ กล่าวคือ องค์กรมีประสิทธิภาพลดต้นทุน เพิ่มกำไร และเพิ่มขีดความสามารถในการแข่งขัน

บทที่ 2
แนวคิด ทฤษฎี และ ผลงานวิจัยที่เกี่ยวข้อง

2.1 องค์กรหรือหน่วยงานที่ตรวจสอบ

องค์กรที่ตรวจสอบประกอบธุรกิจรับประกันวินาศภัยทุกประเภท ซึ่งแบ่งออกได้เป็นการรับประกันอัคคีภัย การรับประกันภัยทางทะเลและขนส่ง การรับประกันภัยเบ็ดเตล็ด และการรับประกันภัยรถยนต์ ซึ่งการดำเนินธุรกิจรับประกันภัยขององค์กรนอกจากการรับประกันภัยจากผู้เอาประกันภัยโดยตรงแล้ว ยังมีการรับประกันภัยต่อจากบริษัทรับประกันภัยในประเทศและบริษัทรับประกันภัยต่างประเทศด้วย และเพื่อเป็นการกระจายความเสี่ยงภัย จึงมีการนำเอางานที่รับประกันภัยไว้และมีทุนประกันภัยสูง กระจายความเสี่ยงโดยนำไปประกันภัยต่อกับบริษัทประกันภัยทั้งในประเทศและต่างประเทศด้วย นอกจากนี้ ธุรกิจอีกส่วนหนึ่งคือกิจกรรมทางด้านการลงทุน ซึ่งมีการลงทุนเพื่อให้เกิดการเพิ่มรายได้ในหลายรูปแบบ เช่น ซื้อพันธบัตรรัฐบาล ซื้อหุ้น ซื้อเงินลงทุนระยะสั้น ฝากธนาคาร และลงทุนในธุรกิจประเภทอื่น ๆ ทั้งนี้ การดำเนินธุรกิจต่าง ๆ ข้างต้นจะอยู่ในการกำกับดูแลของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.)

การดำเนินการขององค์กรมีสำนักงานใหญ่ตั้งอยู่ที่กรุงเทพมหานคร และมีสาขาต่าง ๆ จำนวน 12 สาขา ซึ่งสาขาต่าง ๆ นี้จะตั้งอยู่ในจังหวัดใหญ่ ๆ ของประเทศไทย เช่น เชียงใหม่ หาดใหญ่ ภูเก็ต ระยอง ขอนแก่น เป็นต้น

องค์กรมีการใช้เทคโนโลยีสารสนเทศรองรับการดำเนินธุรกิจ โดยระบบงานหลัก เช่น ระบบงานรับประกันภัย ระบบงานบัญชี จะใช้บริการบริษัทภายนอกในการพัฒนาระบบงาน โดยมีฝ่ายสารสนเทศขององค์กรทำการทดสอบระบบงาน ตรวจรับระบบงาน ก่อนที่จะนำมาใช้งานจริง ทั้งนี้ หลังจากใช้งานจริง หากมีการปรับปรุงเปลี่ยนแปลงที่ไม่ยุ่งยากซับซ้อน เจ้าหน้าที่ฝ่ายสารสนเทศจะเป็นผู้ดำเนินการแก้ไขปรับปรุงโปรแกรม แต่หากมีความซับซ้อนจะใช้บริษัทภายนอกผู้พัฒนาระบบงานดังกล่าวเป็นผู้ดำเนินการปรับปรุงแก้ไขโปรแกรม มีศูนย์คอมพิวเตอร์ตั้งอยู่ที่สำนักงานใหญ่ และมีการจัดตั้งศูนย์สำรองอยู่ภายนอกบริษัท โดยสาขาต่าง ๆ ดำเนินธุรกรรมเชื่อมต่อมายังสำนักงานใหญ่ในลักษณะออนไลน์ ผ่านระบบสื่อสารเครือข่ายอินเทอร์เน็ต และระบบ Leased Line

ในด้านการกำกับดูแลองค์กร คณะกรรมการบริษัทมีการแต่งตั้งคณะกรรมการตรวจสอบซึ่งประกอบด้วยกรรมการอิสระ จำนวน 3 ท่าน โดยมีคุณสมบัติและหน้าที่ความรับผิดชอบตามที่

ตลาดหลักทรัพย์แห่งประเทศไทย คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ตลอดจนสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) กำหนด นอกจากนี้ยังมีฝ่ายตรวจสอบภายในทำหน้าที่ในการตรวจสอบการปฏิบัติตามระบบการควบคุมภายใน คู่มือการปฏิบัติงาน ระเบียบวิธีปฏิบัติ ตลอดจนกฎหมายที่เกี่ยวข้องกับการประกอบธุรกิจขององค์กร และรายงานผลการตรวจสอบเสนอต่อคณะกรรมการตรวจสอบและผู้บริหารที่เกี่ยวข้อง

สำหรับการตรวจสอบระบบเทคโนโลยีสารสนเทศ ปัจจุบันทำการตรวจสอบโดยผู้สอบบัญชีรับอนุญาต ซึ่งจะทำการตรวจสอบปีละ 1 ครั้ง อย่างไรก็ตาม องค์กรมีนโยบายที่จะให้ฝ่ายตรวจสอบภายในดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศด้วยตนเอง

2.2 ระบบสารสนเทศ

ระบบสารสนเทศ (Information system) หมายถึง ระบบที่ประกอบด้วยส่วนต่างๆ ได้แก่ ระบบคอมพิวเตอร์ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้ระบบ พนักงานที่เกี่ยวข้อง และ ผู้เชี่ยวชาญในสาขา ทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้เพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์และติดตามผลการดำเนินงานขององค์กร (สุชาดา กีระนันทน์, 2541) ดังนั้น ระบบสารสนเทศ หมายถึง ชุดขององค์ประกอบที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บ และแจกจ่ายสารสนเทศ เพื่อช่วยการตัดสินใจ และการควบคุมในองค์กร ในการทำงานของระบบสารสนเทศประกอบไปด้วยกิจกรรม 3 อย่าง คือ การนำข้อมูลเข้าสู่ระบบ (Input) การประมวลผล (Processing) และ การนำเสนอผลลัพธ์ (Output) ระบบสารสนเทศอาจจะมีการสะท้อนกลับ (Feedback) เพื่อการประเมินและปรับปรุงข้อมูลนำเข้า ระบบสารสนเทศอาจจะเป็นระบบที่ประมวลด้วยมือ (Manual) หรือระบบที่ใช้คอมพิวเตอร์ก็ได้ (Computer-based information system – CBIS) (Laudon & Laudon, 2001) แต่อย่างไรก็ตามในปัจจุบันเมื่อกล่าวถึงระบบสารสนเทศ มักจะหมายถึงระบบที่ต้องอาศัยคอมพิวเตอร์และระบบโทรคมนาคม มีผู้ให้ความหมายของระบบสารสนเทศในความหมายต่าง ๆ ดังนี้

ระบบสารสนเทศ หมายถึง ระบบคอมพิวเตอร์ที่จัดเก็บข้อมูล และประมวลผล เป็นสารสนเทศ และระบบสารสนเทศเป็นระบบที่ต้องอาศัยฐานข้อมูล (CIS 105 - Survey of Computer Information Systems, n.d.)

ระบบสารสนเทศ หมายถึง ชุดของกระบวนการ บุคคล และเครื่องมือ ที่จะเปลี่ยนข้อมูลให้เป็นสารสนเทศ (FAO Corporate Document Repository, 1998) ระบบสารสนเทศไม่ว่า

จะเป็นระบบมือหรือระบบอัตโนมัติ หมายถึง ระบบที่ประกอบด้วย คน เครื่องจักรกล (machine) และวิธีการในการเก็บข้อมูล ประมวลผลข้อมูล และเผยแพร่ข้อมูล ให้อยู่ในลักษณะของสารสนเทศของผู้ใช้ (Information system, 2005)

สรุปได้ว่า ระบบสารสนเทศ ก็คือ ระบบของการจัดเก็บ ประมวลผลข้อมูล โดยอาศัยบุคคลและเทคโนโลยีสารสนเทศในการดำเนินการ เพื่อให้ได้สารสนเทศที่เหมาะสมกับงานหรือภารกิจแต่ละอย่าง

Laudon & Laudon (2001) ยังอธิบายว่าในมิติทางธุรกิจ ระบบสารสนเทศเป็นระบบที่ช่วยแก้ปัญหาการจัดการขององค์กร ซึ่งถูกท้าทายจากสิ่งแวดล้อม ดังนั้นการใช้ระบบสารสนเทศอย่างมีประสิทธิภาพ จำเป็นที่จะต้องเข้าใจองค์กร (Organzations) การจัดการ (management) และเทคโนโลยี (Technology)

ปัจจุบันจะเห็นความสัมพันธ์ระหว่างองค์กรกับระบบสารสนเทศและเทคโนโลยีสารสนเทศชัดเจนมากขึ้น และเนื่องจากการบริหารงานในองค์กรมีหลายระดับ กิจกรรมขององค์กรแต่ละประเภทอาจจะแตกต่างกัน ดังนั้นระบบสารสนเทศของแต่ละองค์กรอาจแบ่งประเภทแตกต่างกันออกไป (สุชาดา กีระนันทน์, 2541)

ถ้าพิจารณาจำแนกระบบสารสนเทศตามการสนับสนุนระดับการทำงานในองค์กร จะแบ่งระบบสารสนเทศได้เป็น 4 ประเภท ดังนี้ (Laudon & Laudon, 2001)

1. ระบบสารสนเทศสำหรับระดับผู้ปฏิบัติงาน (Operational – level systems) ช่วยสนับสนุนการทำงานของผู้ปฏิบัติงานในส่วนปฏิบัติงานพื้นฐานและงานทำรายการต่างๆขององค์กร เช่นใบเสร็จรับเงิน รายการขาย การควบคุมวัสดุของหน่วยงาน เป็นต้น วัตถุประสงค์หลักของระบบนี้ก็เพื่อช่วยการดำเนินงานประจำแต่ละวัน และควบคุมรายการข้อมูลที่เกิดขึ้น

2. ระบบสารสนเทศสำหรับผู้ชำนาญการ (Knowledge - level systems) ระบบนี้สนับสนุน
ผู้ทำงานที่มีความรู้เกี่ยวข้องกับข้อมูล วัตถุประสงค์หลักของระบบนี้ก็เพื่อช่วยให้มีการนำความรู้ใหม่มาใช้ และช่วยควบคุมการไหลเวียนของงานเอกสารขององค์กร

3. ระบบสารสนเทศสำหรับผู้บริหาร (Management - level systems) เป็นระบบสารสนเทศที่ช่วยในการตรวจสอบ การควบคุม การตัดสินใจ และการบริหารงานของผู้บริหารระดับกลางขององค์กร

4. ระบบสารสนเทศระดับกลยุทธ์ (Strategic - level system) เป็นระบบสารสนเทศที่ช่วยการบริหารระดับสูง ช่วยในการสนับสนุนการวางแผนระยะยาว หลักการของระบบคือต้องจัด

ความสัมพันธ์ระหว่างสภาพแวดล้อมภายนอกกับความสามารถภายในที่องค์กรมี เช่น ในอีก 5 ปีข้างหน้า องค์กรจะผลิตสินค้าใด

สุชาดา กีระนันทน์ (2541) และ Laudon & Laudon (2001) ได้แบ่งประเภทของระบบสารสนเทศที่สนับสนุนการทำงานของผู้ปฏิบัติงานและผู้บริหารระดับต่าง ๆ ไว้ ดังตารางที่ 2.1 โดยมีรายละเอียดดังต่อไปนี้

ตารางที่ 2.1 ประเภทของระบบสารสนเทศ

ประเภทของระบบสารสนเทศ (สุชาดา กีระนันทน์ , 2541)	ประเภทของระบบสารสนเทศ (Laudon & Laudon, 2001)
1. ระบบประมวลผลรายการ (Transaction Processing Systems)	1. Transaction Processing System – TPS
2. ระบบสำนักงานอัตโนมัติ (Office Automation Systems) 3. ระบบงานสร้างความรู้ (Knowledge Work Systems)	2. Knowledge Work-KWS and office Systems
4. ระบบสารสนเทศเพื่อการจัดการ (Management Information Systems)	3. Management Information Systems - MIS
5. ระบบสนับสนุนการตัดสินใจ (Decision Support Systems)	4. Decision Support Systems - DSS
6. ระบบสารสนเทศสำหรับผู้บริหารระดับสูง (Executive Information Systems)	5. Executive Support System - ESS

1. ระบบประมวลผลรายการ (Transaction Processing Systems - TPS) เป็นระบบที่ทำหน้าที่ในการปฏิบัติงานประจำ ทำการบันทึกจัดเก็บ ประมวลผลรายการที่เกิดขึ้นในแต่ละวัน โดยใช้ระบบคอมพิวเตอร์ทำงานแทนการทำงานด้วยมือ ทั้งนี้เพื่อที่จะทำการสรุปข้อมูลเพื่อสร้างเป็นสารสนเทศ ระบบประมวลผลรายการนี้ ส่วนใหญ่จะเป็นระบบที่เชื่อมโยงกิจการกับลูกค้า ตัวอย่าง เช่น ระบบการจองบัตรโดยสารเครื่องบิน ระบบการฝากถอนเงินอัตโนมัติ เป็นต้น ในระบบต้องสร้างฐานข้อมูลที่จำเป็น ระบบนี้มักจัดทำเพื่อสนองความต้องการของผู้บริหารระดับต้น

เป็นส่วนใหญ่เพื่อให้สามารถปฏิบัติงานประจำได้ ผลลัพธ์ของระบบนี้ มักจะอยู่ในรูปของ รายงานที่มีรายละเอียด รายงานผลเบื้องต้น

2. ระบบสำนักงานอัตโนมัติ (Office Automation Systems - OAS) เป็นระบบที่สนับสนุนงานในสำนักงาน หรืองานธุรการของหน่วยงาน ระบบจะประสานการทำงานของบุคลากรรวมทั้งกับบุคคลภายนอก หรือหน่วยงานอื่น ระบบนี้จะเกี่ยวข้องกับการจัดการเอกสาร โดยการใช้ซอฟท์แวร์ด้านการพิมพ์ การติดต่อผ่านระบบไปรษณีย์อิเล็กทรอนิกส์ เป็นต้น ผลลัพธ์ของระบบนี้ มักอยู่ในรูปของเอกสาร กำหนดการ สิ่งพิมพ์

3. ระบบงานสร้างความรู้ (Knowledge Work Systems - KWS) เป็นระบบที่ช่วยสนับสนุนบุคลากรที่ทำงานด้านการสร้างความรู้เพื่อพัฒนาการคิดค้น สร้างผลิตภัณฑ์ใหม่ๆ บริการใหม่ ความรู้ใหม่เพื่อนำไปใช้ประโยชน์ในหน่วยงาน หน่วยงานต้องนำเทคโนโลยีสารสนเทศเข้ามาสนับสนุนให้การพัฒนาเกิดขึ้นได้โดยสะดวก สามารถแข่งขันได้ทั้งในด้านเวลา คุณภาพ และราคา ระบบต้องอาศัยแบบจำลองที่สร้างขึ้น ตลอดจนการทดลองการผลิตหรือดำเนินการ ก่อนที่จะนำเข้ามาดำเนินการจริงในธุรกิจ ผลลัพธ์ของระบบนี้ มักอยู่ในรูปของสิ่งประดิษฐ์ ตัวแบบ รูปแบบ เป็นต้น

4. ระบบสารสนเทศเพื่อการจัดการ (Management Information Systems - MIS) เป็นระบบสารสนเทศสำหรับผู้ปฏิบัติงานระดับกลางใช้ในการวางแผน การบริหารจัดการ และการควบคุม ระบบจะเชื่อมโยงข้อมูลที่มีอยู่ในระบบประมวลผลรายการเข้าด้วยกัน เพื่อประมวลและสร้างสารสนเทศที่เหมาะสมและจำเป็นต่อการบริหารงาน ตัวอย่างเช่น ระบบบริหารงานบุคลากร ผลลัพธ์ของระบบนี้ มักอยู่ในรูปของรายงานสรุป รายงานของสิ่งผิดปกติ

5. ระบบสนับสนุนการตัดสินใจ (Decision Support Systems – DSS) เป็นระบบที่ช่วยผู้บริหารในการตัดสินใจสำหรับปัญหา หรือที่มีโครงสร้างหรือขั้นตอนในการหาคำตอบที่แน่นอนเพียงบางส่วน ข้อมูลที่ใช้ต้องอาศัยทั้งข้อมูลภายในกิจการและภายนอกกิจการประกอบกัน ระบบยังต้องสามารถเสนอทางเลือกให้ผู้บริหารพิจารณา เพื่อเลือกทางเลือกที่เหมาะสมที่สุดสำหรับสถานการณ์นั้น หลักการของระบบ สร้างขึ้นจากแนวคิดของการใช้คอมพิวเตอร์ช่วยการตัดสินใจ โดยให้ผู้ใช้โต้ตอบโดยตรงกับระบบ ทำให้สามารถวิเคราะห์ ปรับเปลี่ยนเงื่อนไขและกระบวนการพิจารณาได้ โดยอาศัยประสบการณ์ และ ความสามารถของผู้บริหารเอง ผู้บริหารอาจกำหนดเงื่อนไขและทำการเปลี่ยนแปลงเงื่อนไขต่างๆ ไปจนกระทั่งพบสถานการณ์ที่เหมาะสมที่สุด แล้วใช้เป็นสารสนเทศที่ช่วยตัดสินใจ รูปแบบของผลลัพธ์ อาจจะอยู่ในรูปของ รายงานเฉพาะกิจ รายงานการวิเคราะห์เพื่อตัดสินใจ การทำนาย หรือ พยากรณ์เหตุการณ์

6. ระบบสารสนเทศสำหรับผู้บริหารระดับสูง (Executive Information System - EIS) เป็นระบบที่สร้างสารสนเทศเชิงกลยุทธ์สำหรับผู้บริหารระดับสูง ซึ่งทำหน้าที่กำหนดแผนระยะยาวและเป้าหมายของกิจการ สารสนเทศสำหรับผู้บริหารระดับสูงนี้จำเป็นต้องอาศัยข้อมูลภายนอกกิจกรรมเป็นอย่างมาก ยิ่งในยุคปัจจุบันที่เป็นยุค Globalization ข้อมูลระดับโลก แนวโน้มระดับสากลเป็นข้อมูลที่จำเป็นสำหรับการแข่งขันของธุรกิจ ผลลัพธ์ของระบบนี้ มักอยู่ในรูปของการพยากรณ์/การคาดการณ์

ถึงแม้ว่าระบบสารสนเทศจะมีหลายประเภท แต่องค์ประกอบที่จำเป็นของระบบสารสนเทศทุกประเภท ก็คือต้องประกอบด้วยกิจกรรม 3 อย่างตามที่ Laudon & Laudon (2001)ได้กล่าวไว้ คือ ระบบต้องมีการนำเข้าข้อมูล การประมวลผลข้อมูล และการแสดงผลลัพธ์ของข้อมูล

สุชาดา กีระนันทน์ (2541) สรุปไว้ว่า การพัฒนาระบบสารสนเทศในองค์กรนั้นเป็นสิ่งท้าทายผู้บริหารเป็นอย่างมาก การที่จะพัฒนาระบบสารสนเทศขึ้นในหน่วยงานเป็นสิ่งที่ผู้บริหารและผู้รับผิดชอบการพัฒนาระบบ ต้องร่วมกันตัดสินใจอย่างรอบคอบ เพราะการนำระบบสารสนเทศมาใช้อาจจะกระทบต่อกระบวนการดำเนินงานและการบริหารที่เป็นอยู่ หรืออาจจะมีผลก่อให้เกิดการเปลี่ยนแปลงในองค์กร

2.3 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

สหพันธ์นักบัญชีระหว่างประเทศหรือไอแฟค (International Federation of Accountants : IFAC) ได้ให้ความหมายของเทคโนโลยีสารสนเทศ (Information Technology) ไว้ดังนี้ “เทคโนโลยีสารสนเทศ หมายถึง ผลิตภัณฑ์ฮาร์แวร์และซอฟต์แวร์ การปฏิบัติการด้านระบบสารสนเทศ กระบวนการด้านบริหารจัดการ และทรัพยากรมนุษย์ รวมทั้งทักษะที่จำเป็นในการที่จะประยุกต์ผลิตภัณฑ์และกระบวนการที่กล่าวมาให้เข้ากับภาระงานการผลิตสารสนเทศ การพัฒนาระบบสารสนเทศ รวมทั้งการจัดากรและการควบคุมระบบสารสนเทศ”

ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศ พ.ศ. 2535 ได้ให้ความหมายของเทคโนโลยีสารสนเทศ ไว้ดังนี้ “เทคโนโลยีสารสนเทศ หมายถึง ความรู้ในผลิตภัณฑ์หรือในกระบวนการดำเนินการใด ๆ ที่อาศัยเทคโนโลยีซอฟต์แวร์ ฮาร์ดแวร์ การติดต่อสื่อสาร การรวบรวม และการนำข้อมูลมาใช้ทันกาล เพื่อก่อให้เกิดประสิทธิภาพ ทั้งทางด้านการผลิต การบริการ การบริหาร และการดำเนินงาน รวมทั้งเพื่อการศึกษาและการเรียนรู้ ซึ่งจะส่งผลต่อความได้เปรียบทางด้านเศรษฐกิจ การค้า และการพัฒนาด้านคุณภาพของประชาชนในสังคม”

ดังนั้น สรุปได้ว่า เทคโนโลยีสารสนเทศ หมายถึง ฮาร์ดแวร์และซอฟต์แวร์ที่เกี่ยวข้องกับข้อมูลในรูปอิเล็กทรอนิกส์ ไม่ว่าจะเป็นการบันทึก การจัดเก็บ การประมวลผล การผลิตผลลัพธ์ รวมถึงกระบวนการส่งข้อมูลเหล่านั้นผ่านเครือข่ายสื่อสาร

ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการประกอบธุรกิจขององค์กร สามารถแบ่งออกเป็น 4 ประเภทหลัก (สำนักงาน กลต, ที่ ธ.(ว) 32/2545) ดังนี้

1. Access Risk : เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ ซึ่งหมายถึง โปรแกรม ระบบงาน เครือข่าย และอุปกรณ์คอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากบริษัทฯ มิได้มีวิธีการจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การมิได้มีการกำหนดรหัสผ่าน(password)ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การมิได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

2. Integrity Risk : เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่บริษัทฯ มิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูลรวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการมิได้มีระบบการควบคุมและตรวจสอบอย่างเพียงพอเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

3. Availability Risk : เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหรือการดำเนินธุรกิจของบริษัทฯ หยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากการมิได้ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการมิได้มีการสำรองข้อมูล และระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ หากบริษัทหลักทรัพย์มิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์เสียหายได้

4. Infrastructure Risk : เป็นความเสี่ยงเกี่ยวกับการที่บริษัทฯ มิได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี รวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์ และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ โดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการมิได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการมิได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการดำเนินธุรกิจ และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบ

2.4 ความเสียหายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ

จากความเสี่ยงด้านเทคโนโลยีสารสนเทศ อาจมีผลทำให้องค์กรได้รับความเสียหาย ซึ่งสามารถแบ่งเป็น 8 ประเภทใหญ่ ๆ ดังนี้

1. ทรัพย์สินเทคโนโลยีสารสนเทศเสียหาย เนื่องจากสูญหายหรือถูกทำลายโดยตั้งใจ เช่นจากผู้ที่ประสงค์ร้าย หรือมุ่งหวังทรัพย์สิน เป็นต้น หรือโดยไม่ได้ตั้งใจ เช่น เกิดจากภัยธรรมชาติ เป็นต้น ซึ่งทำให้องค์กรต้องเสียค่าใช้จ่ายในการกู้ระบบหรือนำข้อมูลเข้าสู่ระบบใหม่

2. การตัดสินใจผิดพลาด เนื่องจากนำข้อมูลที่ไม่ถูกต้องมาใช้ในการตัดสินใจหรือไม่มีข้อมูลในการตัดสินใจ เช่น ผู้บริหารได้ตัดสินใจในการเปิดโรงงานผลิตใหม่โดยไม่นำข้อมูลงบการเงิน ณ ปัจจุบันมาประกอบการตัดสินใจ เนื่องจากเริ่มนำระบบงานบัญชีและการเงินมาใช้และยังไม่ได้นำข้อมูลทั้งหมดเข้าสู่ระบบ เป็นต้น

3. ข้อมูลไม่มีความน่าเชื่อถือ ซึ่งอาจเกิดจากการบันทึกรายการไม่ตรงตามวันเวลาบันทึกข้อมูลไม่ถูกต้อง และการประมวลผลข้อมูลไม่ถูกต้อง เช่น จำนวนสินค้าคงเหลือที่บันทึกในระบบสินค้าคงคลังกับจำนวนสินค้าจริงไม่ตรงกัน เนื่องจากไม่บันทึกรายการรับ-จ่ายสินค้าทันทีหรือภายในวันเดียวกันกับการรับ-จ่ายสินค้านั้น ทำให้อาจไม่สามารถส่งสินค้าให้กับลูกค้าตามจำนวนที่ลูกค้าสั่งได้ หรือมีการผลิตหรือซื้อสินค้าเพื่อขายมากกว่าจำนวนสินค้าที่คาดว่าลูกค้าต้องการ เป็นต้น

4. ธุรกิจที่ใช้เทคโนโลยีสารสนเทศหยุดชะงัก เนื่องจากสาเหตุหลายประการ เช่น ภัยธรรมชาติ ซึ่งมีผลทำให้ทรัพย์สินเทคโนโลยีสารสนเทศเสียหายไม่สามารถทำงานได้ หรือการหยุดการทำงานหรือการทำงานอย่างผิดปกติของระบบเทคโนโลยีสารสนเทศซึ่งอาจเกิดขึ้นโดยไม่ทราบสาเหตุหรือถูกโจมตีจากแฮกเกอร์

5. การทุจริตและฉ้อฉล เนื่องจากสาเหตุหลายประการ ได้แก่ การนำข้อมูลสำคัญไปใช้ในทางที่มิชอบ เช่น นำสูตรการผลิตหรือรายชื่อของลูกค้าไปขายแก่บริษัทคู่แข่ง เป็นต้น หรือการหาผลประโยชน์เพื่อตนเอง เช่น การนำเงินจากการปัดเศษสตางค์จากบัญชีธนาคารของผู้อื่นเข้าบัญชีธนาคารของตนเอง การบันทึกขายสินค้าแก่ลูกค้าที่ไม่มีตัวตนจริงในระบบรับคำสั่งขายและทำการคืนสินค้าในระบบภายหลังเพื่อสร้างยอดขายให้แก่ตนเอง เป็นต้น

6. รายจ่ายที่เกิดขึ้นโดยไม่จำเป็น หรือรายจ่ายส่วนเกิน เนื่องจากสาเหตุหลายประการ ได้แก่ การปรับรื้อหรือแก้ไขระบบงานให้ใช้งานได้ตามความต้องการ เช่น การแก้ไขระบบงานรับคำสั่งขายให้สามารถนำจำนวนสินค้าคงเหลือจากระบบสินค้าคงคลังมาคำนวณว่ามีสินค้าเพียงพอที่จะขายหรือไม่ โดยผู้ใช้ไม่ต้องไปเปิดดูข้อมูลโดยตรงจากระบบคลังสินค้า การเพิ่มหน้าที่งานการบันทึกรายละเอียดของการเงินจากลูกค้าในระบบเช่าซื้อรถยนต์เพื่อใช้เป็นข้อมูลอ้างอิงกับลูกค้า การซื้อโปรแกรมสำเร็จรูปที่เหมาะกับธุรกิจการเงินการธนาคารมาปรับแก้เพื่อให้ใช้ได้กับธุรกิจการผลิตเพื่อขาย เป็นต้น การซื้อระบบเทคโนโลยีสารสนเทศที่เกินความจำเป็นในการใช้งาน เช่น การซื้อโปรแกรมสำเร็จรูปที่มีหน้าที่งานมากและซับซ้อนมาใช้ในองค์กรที่ต้องการใช้หน้าที่งานหลักเพียงบางส่วนของโปรแกรมสำเร็จรูปนั้นเท่านั้น การซื้อเครื่องเซิร์ฟเวอร์ที่มีเนื้อที่เก็บข้อมูลเกินปริมาณข้อมูลขององค์กรมากเกินไป เป็นต้น การซื้อระบบรักษาความปลอดภัยเพิ่มเติม เนื่องจากระบบที่ใช้ในปัจจุบันไม่มีระบบการรักษาความปลอดภัยที่รัดกุมเพียงพอ เช่น ผู้ใช้เลือกซื้อโปรแกรมสำเร็จรูปที่ไม่สามารถกำหนดหน้าที่งานที่เหมาะสมให้แก่ผู้ใช้แต่ละคนหรือการแบ่งแยกหน้าที่ให้แก่ผู้ใช้ในระบบงานนั้น แต่ได้ไปซื้อโปรแกรมรักษาความปลอดภัยอื่นเพิ่มเติมเพื่อนำมาใช้ทำหน้าที่ดังกล่าว แทนที่จะเลือกซื้อโปรแกรมสำเร็จรูปอื่นที่มีการกำหนดหน้าที่งานให้แก่ผู้ใช้ เป็นต้น

7. การเสื่อมเสียชื่อเสียงหรือการขาดความเชื่อมั่นของลูกค้า เนื่องจากสาเหตุหลายประการ ได้แก่ ระบบเทคโนโลยีสารสนเทศที่ใช้สนับสนุนการให้บริการแก่ลูกค้าไม่สามารถให้บริการลูกค้าได้ หรือประมวลผลข้อมูลที่เกี่ยวข้องกับลูกค้าผิดพลาด เช่น ธนาคารไม่สามารถรับฝาก-ถอนเงินกับลูกค้าได้เนื่องจากระบบรับฝากเงินขัดข้องหรือเซิร์ฟเวอร์ล่ม ใบแจ้งหนี้ค่าโทรศัพท์มือถือแสดงยอดสูงกว่าการใช้จริงของลูกค้าเนื่องจากคำนวณระยะเวลาการใช้ผิด เป็นต้น หรือข้อมูลลูกค้าถูกขโมยจากผู้บุกรุกระบบ

8. การไม่ปฏิบัติตามกฎหมายหรือกฎระเบียบจากหน่วยราชการที่เกี่ยวข้อง เนื่องจากระบบงานที่พัฒนานั้นไม่ได้พัฒนาตามวิธีการที่ได้กำหนดไว้ หรือไม่คำนึงถึงกฎระเบียบที่เกี่ยวข้อง เช่น ระบบงานเงินเดือนและค่าจ้าง ไม่ได้คำนวณภาษีเงินได้หัก ณ ที่จ่ายตามอัตราและกฎที่กรมสรรพากรกำหนด ซึ่งมีผลให้นำส่งภาษีหัก ณ ที่จ่ายในแต่ละเดือนสูงหรือต่ำไป เป็นต้น

2.5 การตรวจสอบระบบเทคโนโลยีสารสนเทศ (อภิณห์พร เมธาวัชนานนท์ , 2551)

การตรวจสอบระบบเทคโนโลยีสารสนเทศมีความสำคัญ โดยเป็นกระบวนการที่ใช้ในการเก็บรวบรวมและประเมินหลักฐาน ในอันที่จะพิจารณาว่าระบบสารสนเทศนั้นสามารถที่จะบรรลุวัตถุประสงค์หลัก ในการป้องกันสินทรัพย์จากการทุจริตหรือผิดพลาด การรักษาความถูกต้องของข้อมูล ความมีประสิทธิผลของระบบงาน และความมีประสิทธิภาพในการใช้ทรัพยากรของระบบหรือไม่เพียงใด

การตรวจสอบระบบสารสนเทศ หมายถึง การตรวจสอบการควบคุมระบบสารสนเทศที่มีอยู่ของหน่วยงาน เพื่อให้ทราบว่าการควบคุมนั้น ๆ มีเพียงพอหรือไม่ การตรวจสอบระบบสารสนเทศ แบ่งออกเป็น 3 ประเภท ได้แก่ การตรวจสอบทั่วไป การตรวจสอบระบบงานประยุกต์ และการตรวจสอบฐานข้อมูล

หน่วยงานที่ทำหน้าที่ตรวจสอบระบบเทคโนโลยีสารสนเทศจะต้องมีความเป็นอิสระจากการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ (แนวทางการจัดระบบการควบคุมภายใน, 2540) ผู้ตรวจสอบจะต้องมีความรู้ทางเทคนิคคอมพิวเตอร์อย่างเพียงพอ โดยผู้ที่จะทำหน้าที่ตรวจสอบการควบคุมทั่วไป จะต้องมีความรู้เกี่ยวกับการทำงานของระบบจัดการของเครื่องคอมพิวเตอร์ที่จะทำการตรวจสอบ และผู้ที่ตรวจสอบการควบคุมภายในระบบงาน จะต้องมีความรู้พื้นฐานในการออกแบบระบบและการควบคุมภายในของแต่ละระบบงาน

2.5.1 ความสำคัญของการตรวจสอบ

การควบคุมและตรวจสอบระบบเทคโนโลยีสารสนเทศมีความสำคัญและจำเป็นดังนี้

1. เพื่อป้องกันข้อมูลสูญหาย ข้อมูลในระบบสารสนเทศมีความสำคัญต่อการดำเนินงานของหน่วยงานหรือองค์กร ถ้าเกิดการสูญหายและต้องการให้กลับคืนมา หน่วยงานจะต้องใช้ทรัพยากรเพิ่มขึ้น ทำให้เกิดต้นทุนเพิ่มขึ้นด้วย

2. เพื่อลดการตัดสินใจผิดพลาด การเชื่อมโยงข้อมูลจากหลายระบบ อันจะนำไปสู่ข้อมูล สำหรับใช้ในการบริหารและการตัดสินใจ กรณีที่ข้อมูลหรือสารสนเทศที่ได้จากระบบสารสนเทศขาดความถูกต้องน่าเชื่อถือ ผู้บริหารหรือผู้ที่ใช้ข้อมูลสารสนเทศในการตัดสินใจ ย่อมได้รับผลกระทบที่ก่อให้เกิดความผิดพลาดในการตัดสินใจได้

3. เพื่อป้องกันการใช้คอมพิวเตอร์ในทางมิชอบ การทุจริตโดยใช้คอมพิวเตอร์เป็นเครื่องมือ ทำให้การสืบค้นหาจุดที่มีการทุจริตทำได้ยาก และความเสียหายที่เกิดขึ้นนั้นจะมีมูลค่าสูงกว่าระบบที่ไม่ใช้คอมพิวเตอร์ อันจะนำไปถึงความน่าเชื่อถือของหน่วยงานด้วย

4. เพื่อรักษาทรัพย์สิน ได้แก่ อุปกรณ์ โปรแกรมระบบงานประยุกต์ รวมทั้งบุคคลที่เกี่ยวข้องกับระบบสารสนเทศ ซึ่งมีการลงทุนที่สูงกว่าด้านอื่น ๆ มาก ถ้าทรัพยากรดังกล่าวได้รับความเสียหาย ย่อมมีผลกระทบต่อการดำเนินงานของหน่วยงาน

5. เพื่อป้องกันความผิดพลาด จากการเชื่อมโยงเครื่องคอมพิวเตอร์เข้าด้วยกันเป็นระบบเครือข่าย และมีการโปรแกรมมากขึ้น โดยเฉพาะในลักษณะของการป้อนข้อมูลและทราบผลทันที (On-line Real Time) ถ้าบางเครื่องทำงานผิดพลาด ก็อาจก่อให้เกิดความเสียหายต่อระบบงานและส่งผลทั้งระบบ ซึ่งย่อมมีผลต่อการดำเนินงานของหน่วยงาน

6. เพื่อรักษาความเป็นส่วนตัว ข้อมูลบางอย่างของหน่วยงานจำเป็นต้องมีการรักษาความลับ เปิดเผยได้เฉพาะเจ้าของข้อมูลเท่านั้น เช่น ข้อมูลลูกค้า เป็นต้น ข้อมูลเหล่านี้ควรมีการรักษาความปลอดภัยและมีการควบคุมการนำไปใช้งานอย่างดี

2.5.2 ความเสี่ยงด้านการตรวจสอบระบบเทคโนโลยีสารสนเทศ (ประทักษ์ วงศ์สินคงมั่น, 2545)

การที่จะประเมินว่าองค์กรบรรลุวัตถุประสงค์ของการตรวจสอบเกี่ยวกับการดูแลรักษาทรัพย์สิน ความถูกต้องสมบูรณ์ของข้อมูล การรักษาความลับ และการปกิบัติตามกฎระเบียบนั้น ผู้ตรวจสอบจะต้องมีการรวบรวมหลักฐานโดยการทดสอบ เมื่อผู้ตรวจสอบได้ทดสอบการควบคุมที่มีอยู่ในระบบแล้ว จะประเมินถึงระดับของความเสี่ยง โดยที่ความเสี่ยงจะขึ้นอยู่กับข้อตกลงที่ผู้ตรวจสอบมีต่อผู้บริหารระดับสูงในเรื่องที่เกี่ยวกับประเภทและขอบเขตของการตรวจสอบ อย่างไรก็

ตาม ในการทดสอบนั้น ผู้ตรวจสอบอาจไม่สามารถค้นพบข้อเท็จจริงหรือความสูญเสียที่อาจเกิดขึ้น ความเสี่ยงที่ผู้ตรวจสอบไม่สามารถค้นพบนี้เรียกว่า ความเสี่ยงด้านการตรวจสอบ (audit risks)

ความเสี่ยงด้านการตรวจสอบระบบเทคโนโลยีสารสนเทศ เป็นความเสี่ยงที่ผู้ตรวจสอบแสดงความเห็น หรือรายงานผลการตรวจสอบผิดพลาด ไม่ตรงกับข้อเท็จจริงอย่างมีนัยสำคัญ เช่น สรุปผลการตรวจสอบและให้ความเห็นว่า ระบบเทคโนโลยีสารสนเทศนั้นทำงานถูกต้อง ควรนำออกใช้งานได้ ทั้ง ๆ ที่มีข้อผิดพลาดสำคัญ คือ ระบบทำงานได้ไม่ครบถ้วนตามหนี่ที่ต้องการเมื่อนำออกใช้งาน เนื่องจากผู้ตรวจสอบไม่ทราบว่ามีการแก้ไขโปรแกรมให้ลดหน้าที่การทำงาน เป็นต้น

ความเสี่ยงด้านการตรวจสอบ (audit risks) ที่กำหนดโดยสมาคมผู้ตรวจสอบบัญชีรับอนุญาตแห่งสหรัฐอเมริกา (The American Institute of Certified Public Accountants, AICPA) ประกอบด้วย ความเสี่ยงจากลักษณะธุรกิจ ความเสี่ยงจากการควบคุม และความเสี่ยงจากการสืบค้น

ความเสี่ยงจากลักษณะธุรกิจ (financial risk) หมายถึง ความเสี่ยงที่เกิดขึ้นสืบเนื่องจากคุณลักษณะของธุรกิจหรือเรื่องที่ตรวจสอบ ซึ่งอาจเกิดความผิดพลาดโดยยังไม่คำนึงถึงการควบคุมภายในที่กิจการจัดให้มีขึ้น ความเสี่ยงจากลักษณะธุรกิจจึงเป็นความเสี่ยงที่มีอยู่โดยธรรมชาติในธุรกิจหรืองานแต่ละประเภท เมื่อใดก็ตามที่จะทำธุรกิจหรืองานนั้น ก็ย่อมจะมีความเสี่ยงเกิดขึ้น เช่น ระบบที่เกี่ยวข้องกับทางด้านการเงิน ซึ่งครอบคลุมทรัพย์สินหลักขององค์กร เช่น ระบบบัญชีเงินสดรับ-จ่าย ระบบเงินเดือน ระบบบัญชีลูกหนี้ ระบบบัญชีเจ้าหนี้ เป็นต้น เนื่องจากทรัพย์สินเหล่านี้มีความเสี่ยงจากลักษณะธุรกิจสูงกว่าทรัพย์สินอื่น ๆ เพราะเป็นเป้าหมายของการทุจริตและฉ้อฉล โดยเฉพาะธุรกิจธนาคารหรือ บริษัทเงินทุน บริษัทหลักทรัพย์ ซึ่งเป็นธุรกิจที่ค้าเงิน หลักทรัพย์หรือตราสารการเงิน ขั้นตอนของงานเกือบทุกขั้นตอนเกี่ยวกับการซื้อ ขาย แลกเปลี่ยน โอน รับ จ่าย เงินหรือหลักทรัพย์ ซึ่งทรัพย์สินเหล่านี้เป็นทรัพย์สินซึ่งมีสภาพคล่องสูง ระบบสารสนเทศที่เกี่ยวข้องกับทรัพย์สินดังกล่าวจึงมีความล่อแหลมต่อการสูญหายหรือทุจริต เป็นต้น

ความเสี่ยงจากการควบคุม (control risk) หมายถึง ความเสี่ยงที่ระบบการควบคุมภายในขององค์กรไม่อาจป้องกันข้อผิดพลาดในส่วนที่เกิดจากความเสี่ยงจากลักษณะธุรกิจได้ทั้งหมด ความเสี่ยงในส่วนนี้เกิดขึ้นเนื่องจากแม้ว่าองค์กรจะกำหนดให้มีการควบคุมภายในเพื่อลดความเสี่ยงจากลักษณะธุรกิจลงแล้วก็ตาม แต่ก็อาจมีโอกาสที่การควบคุมภายในดังกล่าวมีข้อบกพร่องอยู่ ก็ทำให้เกิดความเสียหายขึ้นได้เช่นกัน

ความเสี่ยงจากการสืบค้น (detection risk) หมายถึง ความเสี่ยงที่เกิดขึ้นในเรื่องที่ตรวจสอบนั้น ไม่สามารถค้นหาหรือค้นพบความไม่ถูกต้องของรายการหรือข้อผิดพลาดที่มีอยู่ ทั้งนี้เพราะในการปฏิบัติงานตรวจสอบของผู้ตรวจสอบจำเป็นต้องใช้วิธีการตรวจสอบโดยเลือกสุ่ม

ตัวอย่าง ไม่สามารถตรวจสอบทุกเรื่องได้ทั้งหมด เนื่องจากข้อจำกัดเกี่ยวกับอัตรากำลัง เวลา และความจำเป็นอื่น ๆ

2.5.3 ลักษณะของการตรวจสอบระบบเทคโนโลยีสารสนเทศ

ลักษณะของการตรวจสอบระบบเทคโนโลยีสารสนเทศมี 2 ลักษณะ คือ การตรวจสอบที่ไม่พิจารณาถึงการทำงานของคอมพิวเตอร์ และการตรวจสอบที่พิจารณาถึงการทำงานของคอมพิวเตอร์

การตรวจสอบที่ไม่พิจารณาถึงการทำงานของคอมพิวเตอร์ (audit around the computer) เป็นการตรวจสอบที่ไม่เน้นส่วนของการประมวลผล แต่จะพิจารณาส่วนที่เป็นการนำเข้าข้อมูลและการผลิดผลลัพธ์เป็นหลัก ระบบงานที่ใช้การตรวจสอบลักษณะนี้ควรมีคุณสมบัติ คือ เป็นระบบงานที่ใช้ตรรกะ (logic) แบบตรงไปตรงมา ข้อมูลนำเข้าเรียงตามลำดับ การประมวลผลใช้วิธีการเรียงข้อมูลนำเข้าให้ทำการปรับปรุงข้อมูลในแฟ้มข้อมูลหลักในลักษณะทำงานตามลำดับ มีข้อมูลที่ใช้สำหรับเป็นร่องรอยในการตรวจสอบ (audit trails) หรือมีรายงานเตรียมไว้ให้สำหรับจุดสำคัญต่าง ๆ ในระบบ สภาพแวดล้อมการทำงานของระบบคงที่หรือระบบมีการเปลี่ยนแปลงน้อย ซึ่งการตรวจสอบลักษณะนี้มีข้อจำกัดสำคัญคือ การตรวจสอบลักษณะนี้จะไม่ใช้กับระบบงานที่มีความซับซ้อน เนื่องจากผู้ตรวจสอบอาจขาดความเข้าใจในระบบงานและก่อให้เกิดผลกระทบที่สำคัญกับการตรวจสอบ และการตรวจสอบในลักษณะนี้ ไม่มีข้อมูลให้ผู้ตรวจสอบใช้ในการตรวจสอบอย่างเพียงพอเมื่อระบบมีการเปลี่ยนแปลงเกิดขึ้น

การตรวจสอบที่พิจารณาถึงการทำงานของคอมพิวเตอร์ (audit through the computer) เป็นการตรวจสอบที่เน้นการประมวลผลเป็นหลัก เพื่อทดสอบตรรกะการประมวลผลและการควบคุมที่วางไว้อยู่ในระบบงาน การตรวจสอบข้อมูลที่ถูกสร้างขึ้นจากระบบงานที่ใช้คอมพิวเตอร์จะง่ายหรือยากนั้นขึ้นอยู่กับความซับซ้อนของระบบ ซึ่งบางครั้งจำเป็นต้องมีความรู้ความสามารถทางด้านเทคนิคประกอบด้วย ระบบงานที่ใช้การตรวจสอบในลักษณะนี้ ควรมีคุณสมบัติ ดังนี้คือ มีการประมวลผลด้วยข้อมูลนำเข้าและมีข้อมูลผลลัพธ์เป็นจำนวนมาก ส่วนที่สำคัญที่เกี่ยวกับการควบคุมถูกนำมารวมไว้เป็นส่วนหนึ่งในระบบ ตรรกะที่ใช้ประมวลผลซึ่งสร้างไว้ในระบบสารสนเทศมีความซับซ้อน อย่างไรก็ตาม การตรวจสอบในลักษณะนี้ ผู้ตรวจสอบไม่สามารถตรวจข้อมูลทั้งหมดที่เกิดขึ้นจากการประมวลผลภายในองค์กร ดังนั้น งานสำคัญของผู้ตรวจสอบคือการประเมินว่าการควบคุมที่วางไว้ทำงานอย่างมีประสิทธิภาพหรือไม่ ซึ่งการควบคุมนั้นจะเป็นกลไกที่ใช้สำหรับการป้องกัน ค้นหา และแก้ไข เหตุการณ์ที่เกิดขึ้นจากข้อผิดพลาดหรือเหตุผิดปกติที่เกิดขึ้นจากส่วนประกอบต่าง ๆ ของระบบสารสนเทศ

2.5.4 โครงสร้างการตรวจสอบ

โครงสร้างการตรวจสอบ ประกอบด้วยคณะกรรมการตรวจสอบ (IT Audit Committee) และ คณะทำงานตรวจสอบ (IT Audit Workgroup) โดยคณะกรรมการตรวจสอบ (IT Audit Committee) มีหน้าที่และความรับผิดชอบที่สำคัญ ได้แก่ กำหนด/ปรับปรุงนโยบาย ข้อบังคับ ตลอดจนกรอบแนวทางการตรวจสอบระบบสารสนเทศ ส่งเสริมการพัฒนาประสิทธิภาพของระบบสารสนเทศ ตัดสินใจเพื่อแก้ปัญหาสำคัญที่เกี่ยวข้อง เผยแพร่/ให้ความรู้เกี่ยวกับนโยบาย ข้อบังคับ ตลอดจนกรอบแนวทางการตรวจสอบระบบสารสนเทศ ติดตามหรือมอบหมายงานการติดตามในการผลักดันข้อเสนอแนะจากการตรวจสอบระบบสารสนเทศให้มีผลในเชิงรูปธรรม ตลอดจนดูแลปัญหาในระดับนโยบายเพื่อให้เกิดธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT Governance) และคณะทำงานตรวจสอบ (IT Audit Workgroup) มีหน้าที่และความรับผิดชอบที่สำคัญ ได้แก่ ประสานงานกับผู้ที่เกี่ยวข้องกับระบบสารสนเทศหรือเทคโนโลยีสารสนเทศที่จะตรวจสอบ ทั้งในส่วนของผู้ดูแลระบบและผู้ใช้ระบบ ดำเนินงานตรวจสอบ ตามกรอบแนวทางการตรวจสอบระบบสารสนเทศที่คณะกรรมการตรวจสอบได้กำหนดไว้ จัดทำรายงานผลการดำเนินงานเสนอต่อคณะกรรมการตรวจสอบ เพื่อพิจารณาปรับแนวทางต่อไป ตลอดจนติดตามและรายงานผลแก่ผู้บริหารถึงผลความคืบหน้าในการแก้ไข ปรับปรุงระบบสารสนเทศให้เป็นไปตามที่คณะทำงานตรวจสอบเสนอแนะอย่างเหมาะสมและต่อเนื่อง

2.5.5 ขั้นตอนการตรวจสอบ

การตรวจสอบระบบเทคโนโลยีสารสนเทศ มีขั้นตอนที่สำคัญดังนี้

1. ทำการรวบรวมและจัดเก็บข้อมูล
2. ระบุ Key Controls
3. วางแผนและออกแบบโปรแกรมการตรวจสอบ
4. จัดเก็บข้อมูลภาคสนาม
5. วิเคราะห์ข้อมูลที่ได้มาจากภาคสนาม
6. ร่างสรุปผลการตรวจสอบ
7. นัดประชุมผู้ที่มีส่วนเกี่ยวข้อง
8. สรุปรายงาน
9. ส่งรายงานให้ผู้บริหารรับทราบ
10. ติดตามผลความคืบหน้า
11. รายงานถึงผู้บริหาร

2.6 COBIT FRAMEWORK

มาตรฐาน COBIT เป็นทั้งแนวคิดและแนวทางการปฏิบัติ (Framework) เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่างๆ ที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดี (Best Practice) ซึ่งสามารถนำไปปรับใช้ได้ในทุกองค์กรสำหรับกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ แนวคิดที่ใช้สร้าง COBIT (สถาบันเทคโนโลยีสารสนเทศาภิบาล, 2547) เริ่มต้นจากการควบคุมด้านเทคโนโลยีสารสนเทศโดยใช้วิธีการพิจารณาจากสารสนเทศที่จำเป็นในการสนับสนุนวัตถุประสงค์ทางธุรกิจหรือความต้องการทางธุรกิจ และพิจารณาจากสารสนเทศที่เป็นผลลัพธ์จากการประยุกต์ใช้ทรัพยากรต่าง ๆ ด้านเทคโนโลยีสารสนเทศ ซึ่งจำเป็นต้องจัดการด้วยกระบวนการด้านเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อให้บรรลุถึงวัตถุประสงค์ทางธุรกิจ สารสนเทศจำเป็นต้องมีคุณสมบัติบางประการ ซึ่ง COBIT อ้างถึงความต้องการทางธุรกิจด้านสารสนเทศ ในการกำหนดความต้องการดังกล่าว COBIT จึงได้ผนวกหลักการของต้นแบบที่มีอยู่และเป็นที่รู้จักดังตารางที่ 2.2 โดยมีรายละเอียดดังต่อไปนี้

ตารางที่ 2.2 ความต้องการทางธุรกิจด้านสารสนเทศ

ความต้องการด้านคุณภาพ	คุณภาพ ต้นทุน การส่งมอบ
ความต้องการด้านความไว้วางใจ (Fiduciary Requirement) (รายงานของ COSO)	การมีประสิทธิภาพและประสิทธิผลในการดำเนินงาน ความเชื่อถือได้ของข้อมูล การปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ
ความต้องการด้านการรักษาความปลอดภัย	การรักษาความลับของข้อมูล ความครบถ้วนของข้อมูล สภาพพร้อมใช้งาน

สำหรับความต้องการด้านคุณภาพนั้น การรักษาคุณภาพจะมีมุมมองจากคุณลักษณะในด้านลบ เช่น ความไม่ผิดพลาด ความน่าเชื่อถือ เป็นต้น ซึ่งส่วนใหญ่มักจัดอยู่ในคุณลักษณะเรื่องความครบถ้วนถูกต้อง แต่ในมุมมองด้านบวกอื่น ๆ ของคุณภาพ เช่น สไตล์ ความดึงดูดใจ การให้ความรู้สึกที่ดีเกินกว่าความคาดหมาย เป็นต้น ยังไม่ได้นำมาพิจารณาในมุมมองของวัตถุประสงค์การควบคุมด้านเทคโนโลยีสารสนเทศ ทั้งนี้ โดยใช้หลักการที่ว่า การจัดการความเสี่ยงอย่าง

เหมาะสมสมควรมาก่อนการใช้โอกาสทางธุรกิจ คุณภาพในด้านประโยชน์การใช้งานจะรวมอยู่ในคุณลักษณะด้านประสิทธิผล สำหรับคุณภาพในด้านการส่งมอบนั้น อาจพิจารณาได้ว่าซ้ำซ้อนกับคุณลักษณะในเรื่องสภาพพร้อมใช้งานภายใต้ความต้องการด้านการรักษาความปลอดภัย และกับคุณลักษณะด้านประสิทธิภาพและประสิทธิ ผลในการดำเนินงาน ท้ายสุด ต้นทุนได้รับการพิจารณาให้รวมอยู่กับคุณลักษณะด้านประสิทธิภาพ

สำหรับความต้องการด้านความไว้วางใจนั้น COBIT ไม่ได้พัฒนาขึ้นใหม่ แต่ได้นำข้อกำหนดของ COSO ในเรื่องของการมีประสิทธิภาพและประสิทธิผลในการดำเนินงาน ความเชื่อถือได้ของข้อมูล และการปฏิบัตามกฎหมายและข้อบังคับต่าง ๆ มาใช้ อย่างไรก็ดีได้ขยายคำจำกัดความของคุณลักษณะด้านความเชื่อถือได้ของข้อมูลให้ครอบคลุมสารสนเทศทั้งหมดขององค์กรไม่ใช่เพียงข้อมูลด้านการเงินเท่านั้น

สำหรับเรื่องของความต้องการด้านการรักษาความปลอดภัย COBIT ได้กำหนดปัจจัยสำคัญ ได้แก่ การรักษาความลับ ความครบถ้วนถูกต้อง และสภาพพร้อมใช้งาน ซึ่งปัจจัยทั้งสามดังกล่าวได้นำไปใช้ในการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศทั่วโลก

จากการวิเคราะห์ในภาพกว้างของความต้องการด้านคุณภาพ ด้านความไว้วางใจ และด้านการรักษาความปลอดภัยนั้น ได้แยกแยะคุณลักษณะที่เด่นชัดและไม่ซ้ำซ้อนของสารสนเทศที่ดีออกมาเป็น 7 ประการ ซึ่งคำนิยามของคุณลักษณะแต่ละประการ มีดังนี้

ประสิทธิผล หมายถึง สารสนเทศที่ตรงประเด็นและสัมพันธ์กับกระบวนการทางธุรกิจ อีกทั้งเป็นสารสนเทศที่ทันต่อเวลา ถูกต้อง สม่ำเสมอ และนำไปใช้ประโยชน์ได้

ประสิทธิภาพ หมายถึง การได้มาซึ่งสารสนเทศโดยการใช้ประโยชน์จากทรัพยากรต่าง ๆ อย่างเต็มที่ ได้ผลผลิตสูงสุดและประหยัดที่สุด

การรักษาความลับ หมายถึง การป้องกันการเปิดเผยข้อมูลที่สำคัญโดยไม่ได้รับอนุญาต

ความครบถ้วนถูกต้อง หมายถึง ความครบถ้วนและถูกต้องของสารสนเทศ รวมทั้งเป็นสารสนเทศที่ใช้ได้อย่างสอดคล้องกับค่านิยมและความคาดหวังของธุรกิจ

สภาพพร้อมใช้งาน หมายถึง การมีใช้ของสารสนเทศเมื่อมีความต้องการใช้งานในกระบวนการทางธุรกิจทั้งในปัจจุบันและอนาคต รวมถึงการรักษาความปลอดภัยและความสามารถในการใช้งานของทรัพยากรต่าง ๆ ที่เกี่ยวข้อง

การปฏิบัติตามกฎ หมายถึง การปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และข้อสัญญาที่เกี่ยวข้องกับกระบวนการทางธุรกิจ อาทิเช่น กฎเกณฑ์ข้อบังคับที่กำหนดขึ้นจากภายนอก

ความเชื่อถือได้ หมายถึง การให้สารสนเทศที่เหมาะสมแก่ผู้บริหารเพื่อใช้ในการดำเนินกิจการ และเพื่อให้ผู้บริหารสามารถปฏิบัติความรับผิดชอบในเรื่องการรายงานข้อมูลทางการเงินและรายงานการปฏิบัติตามกฎได้

ส่วนคำนิยามของทรัพยากรด้านเทคโนโลยีสารสนเทศที่กล่าวถึงใน COBIT มีดังนี้

ข้อมูล หมายถึง วัตถุต่าง ๆ ในความหมายที่กว้างที่สุด นั่นคือ ทั้งภายในและภายนอก ทั้งที่มีโครงสร้างและไม่มีโครงสร้าง ตลอดจนข้อมูลที่เป็นกราฟิก หรือเป็นเสียง เป็นต้น

ระบบงานประยุกต์ หมายถึง การทำงานร่วมกันของโปรแกรมคอมพิวเตอร์และการปฏิบัติงานโดยคน

เทคโนโลยี หมายถึง ฮาร์ดแวร์ ระบบปฏิบัติการ ระบบจัดการฐานข้อมูล ระบบเครือข่ายมัลติมีเดีย เป็นต้น

สิ่งอำนวยความสะดวก หมายถึง ทรัพยากรต่าง ๆ ที่ใช้เพื่อเป็นที่ตั้งและสนับสนุนการทำงานของระบบสารสนเทศ

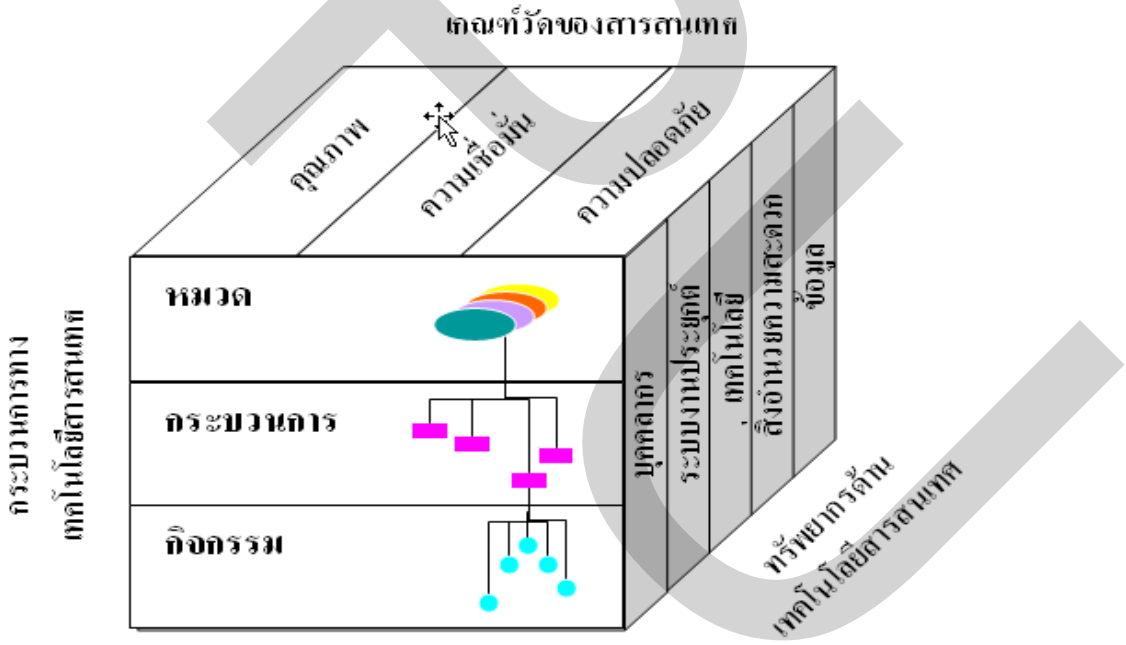
บุคลากร หมายถึง ทักษะของพนักงาน ความตื่นตัว และความมีประสิทธิภาพในการวางแผน การจัดองค์การ การจัดหา การส่งมอบ การสนับสนุน การเฝ้าติดตามระบบสารสนเทศ และการให้บริการสารสนเทศ

เงินทุนไม่ได้นับเป็นทรัพยากรด้านเทคโนโลยีสารสนเทศในการจัดประเภทของวัตถุประสงค์ของการควบคุมข้างต้น เนื่องจากสามารถมองได้ว่าเงินทุนใช้ลงทุนในทรัพยากรด้านเทคโนโลยีสารสนเทศต่าง ๆ ดังกล่าวข้างต้นแล้ว อีกทั้งแม้ว่ากรอบงานนั้นไม่ได้ระบุไว้อย่างชัดเจนว่าต้องมีการจัดทำเอกสารสำหรับเรื่องที่สำคัญทุกเรื่องในกระบวนการทำงานต่าง ๆ ด้านเทคโนโลยีสารสนเทศก็ตาม แต่วิธีปฏิบัติที่ดีนั้น การจัดทำเอกสารเป็นสิ่งที่จำเป็นสำหรับการควบคุมที่ดี และการขาดเอกสารอ้างอิงย่อมทำให้เกิดความจำเป็นที่จะต้องมีการสอบทานและวิเคราะห์เพิ่มเติม เพื่อหาแนวทางการควบคุมอื่นที่จะใช้ทดแทนในขอบเขตที่กำลังสอบทานนั้น และเพื่อให้แน่ใจได้ว่าความต้องการสารสนเทศของธุรกิจได้รับการตอบสนอง จำเป็นต้องกำหนดมาตรการควบคุมที่เหมาะสม รวมถึงการนำไปใช้ และเฝ้าติดตามทรัพยากรเหล่านั้น อย่างไรก็ดี องค์กรจะรู้ได้อย่างไรว่าสารสนเทศที่ได้รับมีคุณลักษณะที่ต้องการ จึงเป็นที่มาของความต้องการกรอบงานที่ดีของวัตถุประสงค์การควบคุมด้านเทคโนโลยีสารสนเทศ

กรอบงาน COBIT ประกอบด้วยวัตถุประสงค์การควบคุมในระดับสูง และโครงสร้างสำหรับการจัดกลุ่มวัตถุประสงค์เหล่านั้น ซึ่งการจัดกลุ่มจะดำเนินการภายใต้ทฤษฎีที่ว่าการทำงานด้านเทคโนโลยีสารสนเทศสามารถแบ่งออกเป็น 3 ระดับด้วยกัน โดยพิจารณาถึงการจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ เริ่มจากระดับล่างสุด มีกิจกรรมและภารกิจที่จะต้องทำให้

สำเร็จและสามารถวัดผลได้ โดยที่กิจกรรมมีลักษณะที่ทำเป็นวงจร ในขณะที่ภารกิจมีลักษณะที่ทำเป็นครั้ง ๆ แยกจากกัน ในส่วนของกิจกรรมที่มีลักษณะของวงจรจะต้องการมาตรการควบคุมที่แตกต่างไปจากลักษณะของภารกิจที่แยกจากกัน ขึ้นมาในระดับที่สอง ได้แก่ กระบวนการ ซึ่งก็คือกิจกรรมและภารกิจต่าง ๆ ที่นำมาทำต่อเนื่องกันไป โดยมีการควบคุมในแต่ละจุด ในระดับที่สามที่เป็นระดับสูงสุด คือ การที่กระบวนการต่าง ๆ ได้รับการจัดกลุ่มโดยแยกเป็นโดเมน ซึ่งการจัดกลุ่มเป็นโดเมนมักจะสอดคล้องกับหน้าที่ความรับผิดชอบในโครงสร้างขององค์กรนั้น ๆ และสอดคล้องกับวงจรของการบริหารหรือวงจรการทำงานของกระบวนการทำงานด้านเทคโนโลยีสารสนเทศ

ดังนั้น สามารถมองกรอบงานในเชิงแนวคิดได้เป็น 3 มิติด้วยกัน คือ (1) คุณลักษณะของสารสนเทศที่ดี (Information Criteria) (2) ทรัพยากรด้านเทคโนโลยีสารสนเทศ (3) กระบวนการด้านเทคโนโลยีสารสนเทศ มิติทั้งสามนี้สามารถแสดงเป็นภาพของลูกบาศก์โคบิต (COBIT Cube) ได้ดังแสดงในภาพที่ 2.1 ดังนี้



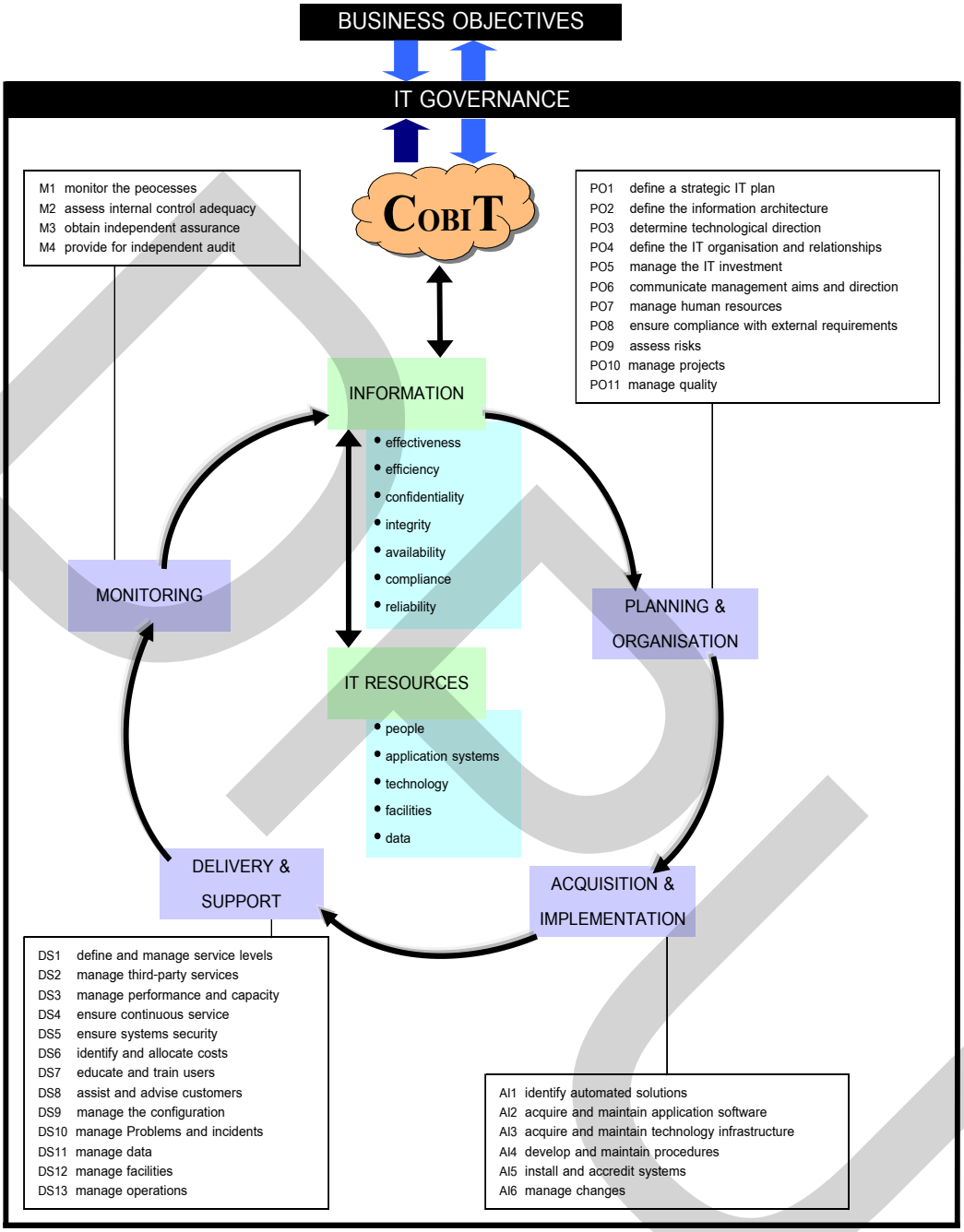
ภาพที่ 2.1 COBIT Cube

ที่มา : IT Governance Institute, 2000

โครงสร้างของมาตรฐาน COBIT ได้ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ Business Process สามารถแบ่งได้เป็น 4 กระบวนการหลัก (Domain) ดังภาพที่ 2.2 ได้แก่

1. การวางแผนและการจัดการองค์กร (PO : Planning and Organization)
2. การจัดหาและการนำระบบออกใช้งานจริง (AI : Acquisition and Implementation)
3. การส่งมอบและการสนับสนุน (DS : Delivery and Support)
4. การติดตามผล (M : Monitoring)

ในแต่ละกระบวนการหลักข้างต้น มาตรฐาน COBIT แสดงวัตถุประสงค์ของการควบคุมหลัก (High-level Control Objectives) รวมถึง 34 หัวข้อ และในแต่ละหัวข้อจะประกอบด้วยวัตถุประสงค์ของการควบคุมย่อยลงไปอีกขั้นหนึ่ง (Detailed Control Objectives) รวมถึง 318 หัวข้อย่อย โดยมีรายละเอียดดังต่อไปนี้



ภาพที่ 2.2 กรอบมาตรฐาน COBIT

ที่มา : http://www.isaca.org, www.itgi.org

2.6.1 การวางแผนและการจัดองค์กร

การวางแผนและการจัดองค์กร (PO : Planning and Organization) โดเมนนี้รวมถึงการวางกลยุทธ์และยุทธวิธี ตลอดจนการหาหนทางที่จะทำให้เทคโนโลยีสารสนเทศมีบทบาทสำคัญที่จะทำให้ธุรกิจบรรลุวัตถุประสงค์ ยิ่งไปกว่านั้น การดำเนินงานให้เป็นไปตามวิสัยทัศน์เชิงกลยุทธ์จำเป็นต้องมีการวางแผนงาน สื่อสาร และจัดการในหลาย ๆ ด้าน และท้ายสุด องค์การจำเป็นต้องมีการจัดองค์การและโครงสร้างพื้นฐานด้านเทคโนโลยีที่เหมาะสม ทั้งนี้ การวางแผนและการจัดองค์กร (PO : Planning and Organization) ประกอบด้วย

PO1 การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (Define a Strategic IT Plan) เพื่อให้องค์กรได้รับประโยชน์สูงสุดจากการใช้ IT

1.1 เทคโนโลยีสารสนเทศเป็นส่วนหนึ่งของแผนงานระยะสั้นและระยะยาวขององค์กร

1.2 แผนงานระยะยาวด้านเทคโนโลยีสารสนเทศ

1.3 วิธีการและโครงสร้างของการจัดทำแผนงานระยะยาวด้านเทคโนโลยีสารสนเทศ

1.4 การปรับเปลี่ยนแผนงานระยะยาวด้านเทคโนโลยีสารสนเทศ

1.5 แผนงานระยะสั้นสำหรับหน่วยงานด้านเทคโนโลยีสารสนเทศ

1.6 การสื่อสารแผนงานด้านเทคโนโลยีสารสนเทศ

1.7 การเฝ้าติดตามและประเมินผลการดำเนินงานตามแผนงานด้านเทคโนโลยีสารสนเทศ

1.8 การประเมินผลระบบงานที่มีอยู่

PO2 การกำหนดโครงสร้างด้านสารสนเทศ (Define the Information Architecture) เพื่อให้ได้รับประโยชน์สูงสุดจากการจัดรูปแบบระบบสารสนเทศ

2.1 ต้นแบบโครงสร้างด้านสารสนเทศ

2.2 พจนานุกรมและไวยากรณ์ข้อมูล

2.3 การจัดประเภทของข้อมูล

2.4 ระดับการรักษาความปลอดภัยของข้อมูล

PO3 การกำหนดทิศทางด้านเทคโนโลยี (Determine Technological Direction) เพื่อให้สามารถใช้เทคโนโลยีสมัยใหม่เป็นกลยุทธ์ในการบริหารธุรกิจ

3.1 การวางแผนโครงสร้างพื้นฐานด้านเทคโนโลยี

3.2 การติดตามทิศทางและกฎข้อบังคับทางด้านเทคโนโลยีในอนาคต

3.3 การจัดหา Contingency Plan ของโครงสร้างพื้นฐานด้านเทคโนโลยี

3.4 แผนการจัดซื้อฮาร์ดแวร์และซอฟต์แวร์

3.5 มาตรฐานด้านเทคโนโลยี

PO4 การจัดโครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศและความสัมพันธ์กับหน่วยงานอื่น (Define the IT Organisation and Relationships) เพื่อให้สามารถให้บริการด้าน IT ได้อย่างเหมาะสมถูกต้อง

4.1 คณะกรรมการกำกับดูแลหรือวางแผนด้านเทคโนโลยีสารสนเทศ

4.2 การจัดองค์กรของหน่วยงานด้านเทคโนโลยีสารสนเทศ

4.3 การทบทวนความสำเร็จขององค์กร

4.4 หน้าที่และความรับผิดชอบ

4.5 ความรับผิดชอบด้านคุณภาพงาน

4.6 ความรับผิดชอบด้านการรักษาความปลอดภัยทั้งด้านระบบงานและข้อมูล

4.7 การกำหนดเจ้าของและผู้จัดเก็บข้อมูล

4.8 การกำหนดเจ้าของระบบงานและข้อมูล

4.9 การควบคุมดูแลงาน

4.10 การแบ่งแยกหน้าที่ความรับผิดชอบของแต่ละตำแหน่งงาน

4.11 การประเมินอัตราบุคลากรด้านเทคโนโลยีสารสนเทศ

4.12 การกำหนดหน้าที่ความรับผิดชอบของบุคลากรด้านเทคโนโลยีสารสนเทศ

4.13 บุคลากรหลักในหน่วยงานด้านเทคโนโลยีสารสนเทศ

4.14 นโยบายและขั้นตอนการว่าจ้างบุคลากรภายนอก

4.15 ความสัมพันธ์

PO5 การจัดการด้านการลงทุนในเทคโนโลยีสารสนเทศ (Manage the IT Investment) เพื่อให้มั่นใจในเงินลงทุนที่ต้องใช้ และมีการดูแลการใช้จ่ายเงินอย่างเหมาะสม

5.1 งบประมาณประจำปีของการดำเนินงานด้านเทคโนโลยีสารสนเทศ

5.2 การติดตามดูแลค่าใช้จ่ายและประโยชน์ที่ได้รับ

5.3 ความเหมาะสมของค่าใช้จ่ายและประโยชน์ที่ได้รับ

PO6 การสื่อสารเป้าหมายและทิศทางภายในองค์กร (Communicate Management Aims and Direction) เพื่อให้แน่ใจว่าคนในองค์กรรับรู้และเข้าใจในเป้าหมายและทิศทาง

6.1 สภาพแวดล้อมที่ดีด้านการควบคุมสารสนเทศ

6.2 ความรับผิดชอบด้านนโยบายของผู้บริหาร

6.3 การสื่อสารนโยบายขององค์กร

6.4 ทรัพยากรที่ใช้เพื่อให้บรรลุตามนโยบาย

6.5 การดูแลรักษานโยบาย

6.6 การปฏิบัติตามนโยบาย, ระเบียบขั้นตอนการปฏิบัติงาน และมาตรฐานต่างๆ

6.7 การยึดมั่นในคุณภาพ

6.8 แนวทางนโยบายในการรักษาความปลอดภัยและการควบคุมภายใน

6.9 สิทธิที่เกี่ยวกับทรัพย์สินทางปัญญา

6.10 การกำหนดนโยบายเฉพาะกิจ

6.11 การสื่อสารให้ตระหนักถึงการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

PO7 การจัดการทรัพยากรบุคคล (Manage Human Resources) เพื่อให้มีบุคลากรที่มีความสามารถ และทุ่มเทในการทำงาน

7.1 การจ้างงานและการเลื่อนตำแหน่งบุคลากร

7.2 คุณวุฒิหรือคุณสมบัติของบุคลากร

7.3 บทบาทหน้าที่และความรับผิดชอบ

7.4 การฝึกอบรมบุคลากร

7.5 การฝึกอบรมข้ามส่วนงาน หรือการมีพนักงานทดแทน

7.6 ระเบียบปฏิบัติการตรวจสอบบุคลากร

7.7 การประเมินผลงานพนักงาน

7.8 การเปลี่ยนแปลงตำแหน่งงานและการเลิกจ้างงาน

PO8 การปฏิบัติตามข้อกำหนดขององค์กรภายนอก (Ensure Compliance with External Requirements) เพื่อให้สอดคล้องถูกต้องตามกฎหมาย ระเบียบ และสัญญา

8.1 การสอบทานข้อกำหนดขององค์กรภายนอก

8.2 วิธีการและระเบียบปฏิบัติเพื่อให้เป็นไปตามข้อกำหนดขององค์กร ภายนอก

8.3 การปฏิบัติตามมาตรฐานด้านความปลอดภัยและสุขลักษณะในการทำงานงาน

8.4 ความเป็นส่วนตัว ทรัพย์สินทางปัญญา และข้อมูล

8.5 พาณิชย์อิเล็กทรอนิกส์

8.6 การปฏิบัติตามสัญญาประกันภัย

PO9 การประเมินความเสี่ยง (Assess Risks) เพื่อให้ IT สามารถตอบสนองความต้องการของผู้บริหารในการตัดสินใจเพื่อลดความเสี่ยง โดยให้ข้อมูลที่เป็นรูปธรรม และชี้ให้เห็นประเด็นที่สำคัญ

9.1 การประเมินความเสี่ยงของธุรกิจ

9.2 วิธีการประเมินความเสี่ยง

9.3 การระบุความเสี่ยง

9.4 การประเมินความเสี่ยง

9.5 แผนปฏิบัติงานเพื่อจัดการความเสี่ยง

9.6 การยอมรับความเสี่ยง

9.7 การเลือกมาตรการควบคุม

9.8 การสนับสนุนของผู้บริหารในการประเมินความเสี่ยง

PO10 การจัดการโครงการ (Manage Projects) เพื่อกำหนดระดับความสำคัญและดำเนินการให้แล้วเสร็จภายในเวลาและงบประมาณที่กำหนด

10.1 กรอบงานการจัดการโครงการ

10.2 การมีส่วนร่วมในการริเริ่มโครงการของหน่วยงานผู้ใช้/ปฏิบัติงาน

10.3 ทีมงานโครงการและหน้าที่ความรับผิดชอบ

10.4 ข้อกำหนดของโครงการ

10.5 การอนุมัติโครงการ

10.6 การอนุมัติโครงการในแต่ละระยะ

10.7 แผนงานหลักของโครงการ

10.8 แผนงานรับรองคุณภาพระบบ

10.9 การกำหนดวิธีการรับรองคุณภาพ

10.10 การบริหารความเสี่ยงของโครงการอย่างเป็นทางการ

10.11 แผนการทดสอบ

10.12 แผนการฝึกอบรม

10.13 แผนการสอบทานระบบภายหลังการใช้งานจริง

PO11 การจัดการคุณภาพ (Manage Quality) เพื่อให้สามารถตอบสนองความต้องการของผู้ใช้ (ข้อมูล)

11.1 แผนคุณภาพทั่วไป

11.2 วิธีการรับรองคุณภาพ

11.3 แผนการรับรองคุณภาพ

11.4 การสอบทานการรับรองคุณภาพ โดยคำนึงถึงมาตรฐานระบบสารสนเทศและวิธีการทำงาน

11.5 กรรมวิธีวงจรการพัฒนาระบบงาน

11.6 กรรมวิธีวงจรการพัฒนาระบบงานสำหรับการเปลี่ยนแปลงที่สำคัญต่อเทคโนโลยีที่มีอยู่

11.7 การปรับปรุงกรรมวิธีวงจรการพัฒนาระบบงาน

11.8 การประสานงานและการสื่อสาร

11.9 กรอบงานการจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี

11.10 สัมพันธภาพกับผู้ติดตั้งระบบงานจากภายนอก

11.11 มาตรฐานของเอกสารโปรแกรม

11.12 มาตรฐานการทดสอบโปรแกรม

11.13 มาตรฐานการทดสอบระบบงาน

11.14 การทดสอบคู่ขนานหรือการทดสอบนำร่อง

11.15 เอกสารการทดสอบระบบงาน

11.16 การประเมินเพื่อรับรองคุณภาพ โดยเทียบกับมาตรฐานการพัฒนา

11.17 การสอบทานเพื่อรับรองคุณภาพเกี่ยวกับการบรรลุวัตถุประสงค์ด้านเทคโนโลยีสารสนเทศ

11.18 ตารางเทียบวัดคุณภาพ

11.19 รายงานการสอบทานการรับรองคุณภาพ

2.6.2 การจัดหาและการนำระบบออกใช้งานจริง

ในการดำเนินงานตามกลยุทธ์ที่วางไว้ จะต้องมีการระบุถึงเทคโนโลยีสารสนเทศต่าง ๆ ที่ต้องใช้ในการดำเนินงาน และจะต้องมีการพัฒนาหรือจัดซื้อจัดหา การนำระบบออกใช้งานจริง ตลอดจนการผนวกรวมเทคโนโลยีสารสนเทศเข้าเป็นส่วนหนึ่งของกระบวนการทางธุรกิจ ในโดเมนนี้ยังรวมถึงการเปลี่ยนแปลงและปรับปรุงระบบงานที่มีอยู่แล้วเพื่อให้วงจรของระบบเหล่านี้ดำเนินต่อไปดังนั้น การจัดหาและการนำระบบออกใช้งานจริง (AI : Acquisition and Implementation) ประกอบด้วย

AI1 การเลือกเทคโนโลยีมาใช้ในการปฏิบัติงาน (Identify Automated Solutions) เพื่อให้มั่นใจว่าจะตอบสนองความต้องการข้อมูลของผู้ใช้ได้อย่างมีประสิทธิผลและประสิทธิภาพ

1.1 การกำหนดความต้องการสารสนเทศ

1.2 การกำหนดทางเลือกในการดำเนินการ

1.3 รูปแบบกลยุทธ์การจัดหา

1.4 การกำหนดระดับการบริการจากบุคคลภายนอก

1.5 การศึกษาความเป็นไปได้ของเทคโนโลยี

1.6 การศึกษาความคุ้มค่าในการลงทุน

1.7 โครงสร้างพื้นฐานสารสนเทศ

1.8 รายงานการวิเคราะห์ความเสี่ยง

1.9 การคุ้มทุนของการรักษาความปลอดภัย

1.10 การออกแบบหลักฐานเพื่อการตรวจสอบ

1.11 สุขลักษณะในการทำงาน

1.12 การคัดเลือกซอฟต์แวร์ระบบ

1.13 การควบคุมการจัดซื้อ

1.14 การจัดซื้อซอฟต์แวร์

1.15 การบำรุงรักษาซอฟต์แวร์ที่จัดซื้อจากบุคคลภายนอก

1.16 สัญญาการใช้โปรแกรมระบบงานประยุกต์

1.17 การตรวจรับสิ่งอำนวยความสะดวกต่างๆ

1.18 การตรวจรับด้านเทคโนโลยี

AI2 การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์ (Acquire and Maintain Application Software) เพื่อให้บริการประมวลผลที่สนับสนุนการดำเนินงาน และการปฏิบัติงานขององค์กรได้อย่างมีประสิทธิผล

2.1 วิธีการออกแบบระบบ

2.2 การเปลี่ยนแปลงที่สำคัญกับระบบงานปัจจุบัน

2.3 การอนุมัติการออกแบบ

2.4 การกำหนดความต้องการเกี่ยวกับแฟ้มข้อมูล และการจัดทำเอกสาร

2.5 ข้อกำหนดของโปรแกรม

2.6 การออกแบบวิธีการเก็บรวบรวมข้อมูลต้นทาง

2.7 การกำหนดความต้องการเกี่ยวกับข้อมูลนำเข้า และการจัดทำเอกสาร

2.8 การกำหนดเกี่ยวกับการเชื่อมต่อประสาน

2.9 การเชื่อมโยงระหว่างเครื่องกับผู้ใช้งาน

2.10 การกำหนดความต้องการเกี่ยวกับการประมวลผล และการจัดทำเอกสาร

2.11 การกำหนดความต้องการเกี่ยวกับผลลัพธ์ และการจัดทำเอกสาร

2.12 ความสามารถในการควบคุม

2.13 ความพร้อมใช้งานที่เป็นปัจจัยหลักในการออกแบบระบบ

2.14 ข้อกำหนดเกี่ยวกับความครบถ้วนถูกต้องของเทคโนโลยีสารสนเทศในโปรแกรมระบบงานประยุกต์

2.15 การทดสอบโปรแกรมระบบงานประยุกต์

2.16 คู่มือผู้ใช้ระบบและคู่มือสนับสนุนการปฏิบัติงาน

2.17 การประเมินผลซ้ำสำหรับด้านการออกแบบระบบ

AI3 การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี (Acquire Maintain Technology Infrastructure) เพื่อให้องค์กรมี IT platform ที่เหมาะสมกับระบบงาน

3.1 การประเมินความต้องการฮาร์ดแวร์และซอฟต์แวร์ใหม่

3.2 การบำรุงรักษาฮาร์ดแวร์แบบมีแผนกำหนดเวลาล่วงหน้า

3.3 การรักษาความปลอดภัยของโปรแกรมระบบ

3.4 การติดตั้งโปรแกรมระบบ

3.5 การดูแลและบำรุงรักษาโปรแกรมระบบ

3.6 การควบคุมการเปลี่ยนแปลงแก้ไขโปรแกรมระบบ

3.7 การใช้และการติดตามโปรแกรมอรรถประโยชน์

AI4 ระเบียบปฏิบัติในการพัฒนาและบำรุงรักษา (Develop and Maintain Procedures) เพื่อให้มีการใช้ระบบงานได้อย่างถูกต้องและเป็นระเบียบ

4.1 ความต้องการในการปฏิบัติงานและระดับการให้บริการ

4.2 คู่มือปฏิบัติงานของผู้ใช้

4.3 คู่มือปฏิบัติงานด้านปฏิบัติการคอมพิวเตอร์

4.4 เอกสารประกอบการฝึกอบรม

AI5 การติดตั้งและรับรองระบบ (Install and Accredit Systems) เพื่อสอบทานให้แน่ใจว่าระบบงานนั้นถูกต้องตรงตามวัตถุประสงค์ที่ต้องการ

5.1 การฝึกอบรม

5.2 ขีดความสามารถของโปรแกรมระบบ

5.3 แผนการนำระบบออกใช้งานจริง

5.4 การโอนย้ายระบบเดิมไปยังระบบงานใหม่

5.5 การโอนย้ายข้อมูลไปยังระบบงานใหม่

5.6 การกำหนดแผนและกลยุทธ์ในการทดสอบ

5.7 การทดสอบโปรแกรมที่เปลี่ยนแปลงหรือแก้ไข

5.8 ขั้นตอนและเกณฑ์การทดสอบแบบคู่ขนานหรือแบบนำร่อง

5.9 การทดสอบครั้งสุดท้ายเพื่อตรวจรับระบบ

5.10 การทดสอบด้านการรักษาความปลอดภัย และระดับความน่าเชื่อถือ

5.11 การทดสอบด้านการปฏิบัติงาน

5.12 การเริ่มใช้งานจริง

5.13 การประเมินความสอดคล้องกับความต้องการของผู้ใช้งาน

5.14 การประเมินผลหลังจากนำระบบออกใช้งานจริง

AI6 การจัดการการเปลี่ยนแปลง (Manage Changes) เพื่อลดโอกาสการหยุดการแก้ไขโดยพลการ และความผิดพลาด

6.1 การควบคุมคำขอปรับปรุงแก้ไขระบบงาน

6.2 การประเมินผลกระทบ

6.3 การควบคุมการเปลี่ยนแปลงแก้ไข

6.4 การเปลี่ยนแปลงแก้ไขกรณีเร่งด่วน

6.5 การจัดทำเอกสารและระเบียบปฏิบัติ

6.6 การอนุมัติการบำรุงรักษา

6.7 นโยบายการอนุมัตินำโปรแกรมระบบงานออกใช้งาน

6.8 การกระจายติดตั้งโปรแกรม

2.6.3 การส่งมอบและการสนับสนุน (DS : Delivery and Support)

โดเมนนี้เกี่ยวข้องกับการส่งมอบบริการด้านข้อมูลตามความต้องการ ซึ่งรวมตั้งแต่การดำเนินงานด้านการรักษาความปลอดภัย ความต่อเนื่องของการให้บริการ ไปจนถึงการฝึกอบรม การจัดให้มีกระบวนการสนับสนุนสำหรับการส่งมอบบริการ การประมวลผลข้อมูลจริงในระบบงานประยุกต์ ซึ่งมักจัดอยู่ในส่วนของการควบคุมเฉพาะระบบ (Application Control) ดังนั้น การส่งมอบและการสนับสนุน (DS : Delivery and Support) จะประกอบด้วย

DS1 การกำหนดและการจัดการระดับการให้บริการ (Define and Manage Service Levels) เพื่อให้เกิดความเข้าใจที่ถูกต้องของระดับบริการที่เป็นที่ต้องการ

1.1 กรอบข้อตกลงเกี่ยวกับระดับการให้บริการ

1.2 หลักเกณฑ์ข้อตกลงของระดับการให้บริการ

1.3 วิธีปฏิบัติเพื่อให้เกิดประสิทธิภาพ

1.4 การติดตามและการรายงาน

1.5 การทบทวนข้อตกลงและสัญญาระดับการให้บริการ

1.6 รายการที่คิดค่าบริการ

1.7 แผนการปรับปรุงการให้บริการ

DS2 การจัดการการใช้บริการจากบุคคลภายนอก (Manage Third-Party Services) เพื่อให้มั่นใจว่าหน้าที่และความรับผิดชอบของ Third-Party มีกำหนดไว้ชัดเจน และมีการดำเนินการที่ถูกต้อง ต่อเนื่อง

2.1 การประสานงานกับผู้ให้บริการ

2.2 ความสัมพันธ์กับเจ้าของระบบ

2.3 สัญญากับผู้ให้บริการภายนอก

2.4 คุณสมบัติของผู้ให้บริการ

2.5 สัญญาการใช้บริการจากบุคคลภายนอก

2.6 ความต่อเนื่องของการให้บริการ

2.7 การตกลงร่วมมือด้านการรักษาความปลอดภัย

2.8 การติดตาม

DS3 การจัดการด้านประสิทธิภาพและความสามารถ (Manage Performance and Capacity) เพื่อให้มั่นใจว่ามี Capacity อย่างเหมาะสม ใช้ประโยชน์ได้สูงสุด ให้บริการได้ตามที่กำหนด

3.1 ความต้องการเกี่ยวกับความพร้อม และประสิทธิภาพในการใช้งาน

3.2 แผนงานความพร้อมสำหรับการใช้งาน

3.3 การติดตามผล และการรายงาน

3.4 เครื่องมือเสริมการทำงาน

3.5 การบริหารประสิทธิภาพแบบมีการคาดการณ์ล่วงหน้า

3.6 การคาดการณ์ปริมาณงาน

3.7 ความสามารถในการบริหารทรัพยากร

3.8 ความพร้อมใช้งานด้านทรัพยากร

3.9 แผนการจัดหาทรัพยากร

DS4 ความต่อเนื่องในการให้บริการ (Ensure Continuous Service) เพื่อให้มั่นใจว่าบริการด้านIT มีให้ใช้ได้ตามที่ต้องการและเกิดปัญหาต่อการดำเนินธุรกิจน้อยที่สุด หากมีเหตุการณ์สำคัญทำให้ต้องหยุดชะงัก

4.1 กรอบงานการดำเนินการอย่างต่อเนื่องด้านเทคโนโลยีสารสนเทศ

4.2 กลยุทธ์และปรัชญาในการจัดทำแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ

4.3 เนื้อหาของแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ

4.4 ความต้องการขั้นต่ำสำหรับดำเนินการอย่างต่อเนื่องด้านเทคโนโลยีสารสนเทศ

4.5 การบำรุงรักษาแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ

4.6 การทดสอบแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ

4.7 การฝึกอบรมเกี่ยวกับแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ

4.8 การเผยแพร่แผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศ

4.9 ระเบียบการปฏิบัติงานสำรองของผู้ใช้

4.10 ทรัพยากรที่มีความสำคัญด้านเทคโนโลยีสารสนเทศ

4.11 ศูนย์สำรอง และฮาร์ดแวร์

4.12 การจัดเก็บสื่อข้อมูลสำรองไว้นอกสถานที่

4.13 ระเบียบปฏิบัติในการสรุปผล

DS5 การรักษาความปลอดภัยระบบ (Ensure Systems Security) เพื่อปกป้องข้อมูลจากการถูกใช้ เปิดเผย แก้ไข ทำลาย โดยไม่ได้รับอนุมัติหรือการสูญหาย

5.1 การประเมินระบบรักษาความปลอดภัย

5.2 การให้อำนาจ/สิทธิ์และการควบคุมการเข้าสู่ระบบ

5.3 ความปลอดภัยในการเข้าถึงข้อมูลแบบออนไลน์

5.4 การจัดการบัญชีผู้ใช้งาน (user account)

5.5 การสอบทานบัญชีผู้ใช้งาน

5.6 การควบคุมบัญชีผู้ใช้งานด้วยตนเอง

5.7 มาตรการติดตามรักษาความปลอดภัย

5.8 การจำแนกประเภทข้อมูล

5.9 การจัดการเกี่ยวกับการแสดงตน และสิทธิในการเข้าถึงข้อมูลแบบรวมศูนย์

5.10 รายงานการละเมิดและกิจกรรมที่เกี่ยวข้องกับความปลอดภัย

5.11 การจัดการกับเหตุการณ์ที่เกิดขึ้น

5.12 การทบทวนความน่าเชื่อถือของระบบรักษาความปลอดภัย

5.13 ความน่าเชื่อถือของคู่ค้า

5.14 การอนุมัติรายการ

5.15 การปฏิเสธรายการที่ผิดเงื่อนไข

5.16 ช่องทางการรับส่งข้อมูลที่เชื่อถือได้

5.17 การป้องกันการแก้ไขระบบควบคุมที่กำหนดไว้

5.18 การจัดการเกี่ยวกับรหัสลับ

5.19 การป้องกัน การตรวจหา และการแก้ไขเกี่ยวกับโปรแกรมที่เป็นอันตรายต่อองค์กร

5.20 โครงสร้างไฟร์วอลล์และการเชื่อมโยงกับเครือข่ายสาธารณะ

5.21 การป้องกันความเสียหายของข้อมูลอิเล็กทรอนิกส์

DS6 การกำหนดและจัดสรรต้นทุน (Identify and Allocate Costs) เพื่อให้เกิดการรับรู้อย่างถูกต้องในต้นทุนของบริการด้าน IT

6.1 รายการที่สามารถบันทึกค่าใช้จ่ายเป็นต้นทุนด้านเทคโนโลยีได้

6.2 ระเบียบปฏิบัติเรื่องต้นทุน

6.3 ระเบียบปฏิบัติในการเรียกเก็บค่าใช้จ่ายและการคืนค่าใช้จ่าย

DS7 การให้ความรู้และฝึกอบรมผู้ใช้งาน (Educate and Train Users) เพื่อให้มั่นใจว่าผู้ใช้สามารถใช้บริการได้อย่างมีประสิทธิภาพ และเข้าใจถึงความเสี่ยง ความรับผิดชอบที่เกี่ยวเนื่องในการใช้นั้นๆ

7.1 กำหนดแผนการฝึกอบรมที่จำเป็นให้แก่พนักงานในแต่ละระดับ

7.2 การกำหนดเป้าหมายของการอบรมในแต่ละระดับพนักงาน

7.3 การอบรมให้มีความตระหนักในเรื่องการรักษาความปลอดภัย

DS8 การให้ความช่วยเหลือและคำแนะนำแก่ผู้ใช้ระบบงานในองค์กร (Assist and Advise Customers) เพื่อให้มั่นใจว่าปัญหาที่ผู้ใช้ประสบได้รับการแก้ไขอย่างเหมาะสม

8.1 หน่วยงานช่วยเหลือผู้ใช้งาน

8.2 การบันทึกปัญหาต่างๆ ที่ถูกสอบถาม

8.3 ขั้นตอนการแก้ไขปัญหา

8.4 การติดตามการแก้ไขปัญหาที่เกิดขึ้น

8.5 การวิเคราะห์แนวโน้มและรายงาน

DS9 การจัดการรายละเอียดทรัพย์สิน (Manage the Configuration) เพื่อให้มีการดูแลรักษา จดบันทึกอย่างเหมาะสมในอุปกรณ์ IT ป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุมัติ มีการตรวจนับ และมีระบบการควบคุมการเปลี่ยนแปลง

9.1 การบันทึกรายการรายละเอียดทรัพย์สิน

9.2 ข้อมูลพื้นฐานของรายละเอียดทรัพย์สิน

9.3 การบันทึกสถานภาพของทรัพย์สิน

9.4 การควบคุมรายละเอียดทรัพย์สิน

9.5 โปรแกรมที่ไม่ได้รับอนุญาตให้นำมาใช้งาน

9.6 การจัดเก็บซอฟต์แวร์

9.7 ระเบียบปฏิบัติการจัดการเกี่ยวกับรายละเอียดทรัพย์สิน

9.8 การกำหนดความรับผิดชอบด้านซอฟต์แวร์

DS10 การจัดการปัญหาและเหตุการณ์ที่เกิดขึ้น (Manage Problems and Incidents) เพื่อให้มั่นใจว่าปัญหาและอุบัติเหตุที่เกิดขึ้นได้รับการแก้ไข มีการหาสาเหตุ และ ป้องกันไม่ให้เกิดขึ้นซ้ำอีก

10.1 ระบบการจัดการปัญหา

10.2 ขั้นตอนในการแก้ไขปัญหา

10.3 หลักฐานการตรวจสอบและการติดตามปัญหา

10.4 การอนุญาตให้เข้าถึงระบบในกรณีฉุกเฉินและชั่วคราว

10.5 การกำหนดลำดับการประมวลผลกรณีฉุกเฉิน

DS11 การจัดการข้อมูล (Manage Data) เพื่อให้มั่นใจว่าข้อมูลมีความสมบูรณ์ ถูกต้องและน่าเชื่อถือ ทั้งในช่วง input, update & storage

11.1 ระเบียบปฏิบัติในการจัดเตรียมข้อมูล

11.2 ระเบียบปฏิบัติในการอนุมัติให้นำข้อมูลเอกสารเข้าสู่ระบบ

11.3 การรวบรวมข้อมูลเข้าสู่ระบบ

11.4 การแก้ไขข้อผิดพลาดของข้อมูลเข้าสู่ระบบ

11.5 ระยะเวลาการจัดเก็บข้อมูลเอกสารประกอบรายการ

11.6 ระเบียบปฏิบัติว่าด้วยสิทธิในการนำข้อมูลเข้าประมวลผล

11.7 การตรวจสอบความสมบูรณ์ ถูกต้อง และการอนุมัติรายการ

11.8 การแก้ไขข้อมูลที่บันทึกผิดพลาด

11.9 ความครบถ้วนถูกต้องของการประมวลผลข้อมูล

11.10 การตรวจสอบความสมเหตุสมผลในการแก้ไขข้อผิดพลาดของการประมวลผลข้อมูล

11.11 การแก้ไขข้อผิดพลาดในการประมวลผลข้อมูล

11.12 การจัดการผลลัพธ์และการจัดเก็บ

11.13 การแจกจ่ายรายงาน

11.14 การสอบยันและกระทบยอดรวมของรายงาน

11.15 การสอบทานและการแก้ไขข้อผิดพลาดของรายงาน

11.16 ข้อกำหนดในการรักษาความปลอดภัยของรายงาน

11.17 การป้องกันข้อมูลที่มีความสำคัญในระหว่างการเคลื่อนย้ายหรือส่งผ่าน

11.18 การป้องกันข้อมูลสำคัญที่บันทึกอยู่บนสื่อบันทึกข้อมูลที่องค์กรได้จำหน่ายทิ้ง

11.19 การจัดการด้านการจัดเก็บข้อมูล

11.20 ระยะเวลาและเงื่อนไขการจัดเก็บข้อมูล

11.21 ระบบการจัดการคลังสื่อบันทึกข้อมูล

11.22 ความรับผิดชอบในการจัดการคลังสื่อบันทึกข้อมูล

11.23 การสำรองข้อมูล

11.24 งานด้านการสำรองข้อมูล

11.25 การจัดเก็บข้อมูลชุดสำรอง

11.26 การจัดเก็บข้อมูลถาวร

11.27 การป้องกันข้อความที่สำคัญ

11.28 การพิสูจน์ตนและความครบถ้วนถูกต้อง

11.29 ความครบถ้วนถูกต้องของรายการธุรกรรมอิเล็กทรอนิกส์

11.30 การคงความถูกต้องของข้อมูลที่จัดเก็บ

DS12 การจัดการด้านสิ่งอำนวยความสะดวก (Manage Facilities) เพื่อให้มีบรรยากาศแวดล้อมทางกายภาพที่เหมาะสมในการปกป้องอุปกรณ์ IT และบุคลากรจากภัยธรรมชาติและบุคคล

12.1 ความปลอดภัยทางกายภาพ

12.2 ความปลอดภัยของสถานที่ที่ตั้งศูนย์คอมพิวเตอร์

12.3 การควบคุมการเข้า – ออกศูนย์คอมพิวเตอร์

12.4 ความปลอดภัยและสุขอนามัยของบุคลากร

12.5 การป้องกันภัยจากปัจจัยรอบข้าง

12.6 เครื่องจ่ายกระแสไฟฟ้าสำรอง

DS13 การจัดการด้านการปฏิบัติการ (Manage Operations) เพื่อให้มั่นใจว่าการปฏิบัติการด้าน IT ที่สำคัญมีการดำเนินงานอย่างสม่ำเสมอและเป็นลำดับอย่างถูกต้อง

13.1 ระเบียบปฏิบัติและคู่มือคำสั่งการประมวลผล

13.2 เอกสารขั้นตอนการเริ่มทำงานของระบบ และคู่มือการปฏิบัติงานอื่นๆ

13.3 ตารางการปฏิบัติงาน

13.4 การประมวลผลนอกเหนือจากตารางการปฏิบัติงาน

13.5 ความต่อเนื่องของการประมวลผล

13.6 การบันทึกเหตุการณ์การปฏิบัติงาน

13.7 การป้องกันเอกสารและอุปกรณ์ที่สำคัญ

13.8 การปฏิบัติงานระยะไกล

2.6.4 การติดตามผล (M : Monitoring)

กระบวนการด้านเทคโนโลยีสารสนเทศทั้งหมดจะต้องได้รับการประเมินเป็นประจำเมื่อเวลาผ่านไป เพื่อรบประกันได้ถึงคุณภาพและการปฏิบัติตามข้อบังคับด้านการควบคุม โดเมนนี้จึงเป็นการระบุถึงการกำกับดูแลการดำเนินงานโดยผู้บริหารในด้านกระบวนการควบคุมขององค์กรและประเมินโดยหน่วยงานอิสระทั้งจากผู้ตรวจสอบภายในและภายนอก หรือจากแหล่งทางเลือกอื่น ดังนั้น การติดตามผล (M : Monitoring) จะประกอบด้วย

M1 การติดตามกระบวนการทำงาน (Monitor the Processes) เพื่อให้มั่นใจว่ากิจกรรมด้าน IT สามารถบรรลุเป้าหมายการปฏิบัติงานตามที่กำหนด

1.1 การรวบรวมข้อมูล

1.2 การประเมินประสิทธิภาพการปฏิบัติงาน

1.3 การประเมินความพึงพอใจของผู้รับบริการ

1.4 การรายงานสำหรับผู้บริหาร

M2 การประเมินความเพียงพอของการควบคุมภายใน (Assess Internal Control Adequacy) เพื่อให้มั่นใจว่าเป้าหมายของการควบคุมภายในของกิจกรรมด้าน IT สามารถบรรลุได้ตามที่กำหนด

2.1 การติดตามการควบคุมภายใน

2.2 ระยะเวลาการปฏิบัติงานของการควบคุมภายใน

2.3 การจัดลำดับการรายงานการควบคุมภายใน

2.4 ความน่าเชื่อถือในความปลอดภัยของการทำงาน และการควบคุมภายใน

M3 การรับรองความเป็นอิสระ (Obtain Independent Assurance) เพื่อเพิ่มความมั่นใจและการไว้วางใจระหว่างองค์กร ผู้ใช้ และ Third-Party

3.1 การเป็นอิสระในการรับรองความปลอดภัยและการควบคุมภายในของการให้บริการด้านเทคโนโลยีสารสนเทศ

3.2 การรับรองความปลอดภัย และการควบคุมภายในของการให้บริการที่รับรองจากบุคคลภายนอก

3.3 ความเป็นอิสระในการประเมินประสิทธิภาพ/ประสิทธิผลของการบริการด้านเทคโนโลยีสารสนเทศ

3.4 ความเป็นอิสระในการประเมินประสิทธิภาพ/ประสิทธิผลของการให้บริการจากบุคคลภายนอก

3.5 ความเป็นอิสระในการรับรองการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับและข้อตกลงที่กำหนดไว้

3.6 ความเป็นอิสระในการรับรองการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับและข้อตกลงที่กำหนดไว้กับผู้ให้บริการภายนอก

3.7 ความรู้ความสามารถในการทำหน้าที่รับรองอย่างเป็นอิสระ

3.8 การมีส่วนร่วมของการตรวจสอบ

M4 ความเป็นอิสระในการตรวจสอบ (Provide for Independent Audit) เพื่อเพิ่มระดับความมั่นใจและประโยชน์จากผู้เชี่ยวชาญในวิธีการปฏิบัติที่ดี

4.1 กฎบัตรการตรวจสอบ

4.2 ความเป็นอิสระ

4.3 จรรยาบรรณและมาตรฐานวิชาชีพ

4.4 ความรู้ความสามารถของผู้ตรวจสอบ

4.5 การวางแผน

4.6 การปฏิบัติงานตรวจสอบ

4.7 การรายงาน

4.8 การติดตามผล

ทั้งนี้ ในแต่ละหัวข้อของวัตถุประสงค์การควบคุม มาตรฐาน COBIT แสดงถึงความสัมพันธ์ต่อปัจจัย 2 ประการ ได้แก่ คุณภาพของระบบข้อมูล (Information Criteria) และทรัพยากรด้านเทคโนโลยี (IT Resources)

2.6.5 ประเด็นการตรวจสอบ

การกำหนดประเด็นการตรวจสอบ จะต้องผ่านการประเมินความเสี่ยงตามกรอบของ COBIT เพื่อพิจารณาถึงจุดที่มีความเสี่ยงสูง และควรจะได้รับการตรวจสอบ

สมมติจากการประเมินความเสี่ยงตามกรอบของ COBIT และสามารถกำหนดประเด็นการตรวจสอบแล้ว จะสามารถแบ่งประเภทการตรวจสอบเป็น 3 ประเภทใหญ่ ๆ ได้แก่

1. การตรวจสอบทั่วไป อาทิเช่น
   - PO4 การจัดโครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศและความสัมพันธ์ กับหน่วยงานอื่น
   - PO6 การสื่อสารเป้าหมายและทิศทางภายในองค์กร
   - P07 การจัดการทรัพยากรมนุษย์
   - P09 การประเมินความเสี่ยง
   - P011 การจัดการคุณภาพ
   - AI3 การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี
   - AI4 ระเบียบปฏิบัติในการพัฒนาและบำรุงรักษา
   - DS5 การรักษาความปลอดภัยระบบ
   - DS6 การกำหนดและจัดสรรต้นทุน
   - DS8 การให้ความช่วยเหลือและคำแนะนำแก่ผู้ใช้ระบบงานในองค์กร
   - DS10 การจัดการปัญหาและเหตุการณ์ที่เกิดขึ้น
   - M1 การติดตามกระบวนการทำงาน
   - M4 ความเป็นอิสระในการตรวจสอบ
2. การตรวจสอบระบบงานประยุกต์ อาทิเช่น
   - AI2 การจัดหาและบำรุงรักษาซอฟท์แวร์ประยุกต์
3. การตรวจสอบฐานข้อมูล อาทิเช่น
   - DS11 การจัดการข้อมูล

2.7 การควบคุมระบบสารสนเทศ (สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย, 2548)

การควบคุมระบบสารสนเทศ ประกอบด้วย กรอบการควบคุม การวางแผน การปฏิบัติงานตรวจสอบ และการรายงาน โดยมีรายละเอียดดังต่อไปนี้

2.7.1 กรอบการควบคุม (Controls Framework)

ตามคำนิยามของ COBIT การควบคุม หมายถึง นโยบาย ขั้นตอนการปฏิบัติงาน วิธีการปฏิบัติและโครงสร้างองค์กร ที่ออกแบบมาเพื่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลว่า การดำเนินธุรกิจจะบรรลุเป้าหมายที่วางไว้ และเหตุการณ์ที่ไม่พึงประสงค์จะได้รับการป้องกันหรือตรวจพบและแก้ไข ในแต่ละการตรวจสอบระบบสารสนเทศ ผู้ตรวจสอบต้องจำแนกความแตกต่างระหว่างการควบคุมทั่วไปซึ่งมีผลกระทบต่อระบบสารสนเทศและการปฏิบัติงานโดยรวม (สภาพแวดล้อมของการควบคุมระบบสารสนเทศ) (Pervasive IS Controls) กับ การควบคุมในระดับที่เฉพาะเจาะจง (การควบคุมระบบสารสนเทศในรายละเอียด (Detailed IS Controls)) ซึ่งมุ่งเน้นการตรวจสอบพื้นที่เสี่ยงที่มีความเกี่ยวข้องกับวัตถุประสงค์ของการตรวจสอบ กรอบการควบคุมที่จะกล่าวถึงดังต่อไปนี้ จะช่วยผู้ตรวจสอบในการบรรลุการดำเนินการดังกล่าว

สภาพแวดล้อมของการควบคุมระบบสารสนเทศ (Pervasive IS Controls) ได้แก่ การควบคุมสำหรับกระบวนการทางด้านระบบสารสนเทศ ตามที่นิยามไว้ใน ข้อกำหนดการวางแผน การจัดการ และการติดตามของ COBIT ตัวอย่างเช่น PO1 การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ และ M1 การติดตามประเมินกระบวนการทำงาน สภาพแวดล้อมของการควบคุมระบบสารสนเทศ เป็นกระบวนการย่อยของการควบคุมทั่วไป ซึ่งเน้นเรื่องการบริหารจัดการและการเฝ้าติดตามประเมินระบบสารสนเทศ

ผลกระทบของสภาพแวดล้อมของการควบคุมระบบสารสนเทศ ไม่ได้จำกัดผลอยู่เพียงการก่อให้เกิดความน่าเชื่อถือการควบคุมเฉพาะระบบงานในระบบการเงินเท่านั้น แต่ยังส่งผลให้เกิดความเชื่อมั่นของการควบคุมระบบสารสนเทศในรายละเอียดในเรื่องต่างๆ เช่น การพัฒนาโปรแกรม การนำระบบงานมาใช้ การจัดการด้านความปลอดภัย ตลอดจนกระบวนการสำรองข้อมูล

ระบบสารสนเทศที่มีการบริหารและเฝ้าติดตามที่อ่อนแอ (สภาพแวดล้อมของการควบคุมระบบสารสนเทศที่อ่อนแอ) เป็นสัญญาณเตือนผู้ตรวจสอบถึงความเสี่ยงสูงที่การควบคุมซึ่งได้ออกแบบให้ทำงานในระดับรายละเอียดอาจจะไม่มีประสิทธิผล

การควบคุมระบบสารสนเทศในรายละเอียด (Detailed IS Controls) ประกอบด้วยการควบคุมระบบงาน รวมถึงการควบคุมทั่วไปที่ไม่รวมอยู่ใน สภาพแวดล้อมของการควบคุมระบบสารสนเทศ ซึ่งตามกรอบงาน COBIT แล้ว การควบคุมระบบสารสนเทศในรายละเอียด คือ การ

ควบคุมที่ครอบคลุมถึงการจัดหา การนำมาใช้ การส่งมอบและการสนับสนุนระบบสารสนเทศและการบริการ ตัวอย่างได้แก่การควบคุมในเรื่อง การนำโปรแกรมสำเร็จรูปมาใช้ การตั้งค่าพารามิเตอร์ที่เกี่ยวกับระบบความปลอดภัยของระบบ การวางแผนกู้พิบัติภัย การตรวจสอบความถูกต้องของข้อมูลเข้า การออกรายงานแสดงรายการที่ผิดปกติ การล็อกบัญชีผู้ใช้งานเมื่อมีการใช้ความพยายามอย่างไม่ถูกต้องที่จะเข้าสู่ระบบ

การควบคุมระบบงาน (Application Control) เป็นส่วนหนึ่งของการควบคุมระบบสารสนเทศในรายละเอียด เช่น การตรวจสอบความถูกต้องของข้อมูลเข้า เป็นทั้งการควบคุมระบบสารสนเทศในรายละเอียด และการควบคุมระบบงาน ส่วนการติดตั้งและการตรวจรับการทำงานของระบบ (AI5) เป็นการควบคุมระบบสารสนเทศในรายละเอียด แต่ไม่ใช่การควบคุมระบบงาน

ความสัมพันธ์ระหว่างการควบคุมระบบสารสนเทศประเภทต่าง ๆ แสดงให้เห็นได้ดังต่อไปนี้

- การควบคุมระบบสารสนเทศ (IS Controls)
- การควบคุมทั่วไป (General Controls)
- สภาพแวดล้อมของการควบคุมระบบสารสนเทศ (Pervasive IS controls)
- การควบคุมระบบสารสนเทศในรายละเอียด (Detailed IS controls)
- การควบคุมระบบงาน (Application controls)

ดังนั้น ผู้ตรวจสอบควรพิจารณาถึงผลกระทบต่อขอบเขตและกระบวนการตรวจสอบหากไม่มีการควบคุมระบบสารสนเทศ

ผลกระทบระหว่างกันของสภาพแวดล้อมและการควบคุมระบบสารสนเทศในรายละเอียด (Interaction of Pervasive and Detailed IS Controls) กรอบงาน COBIT จัดแบ่งกระบวนการควบคุมระบบสารสนเทศ 4 กลุ่ม (โดเมน : Domains) คือ การวางแผนและจัดองค์กร (Planning and Organization) การจัดหาและการนำระบบออกใช้งาน (Acquisition and Implementation) การส่งมอบและการสนับสนุน (Delivery and Support) และ การติดตามประเมินผล (Monitoring)

ความมีประสิทธิผลของการควบคุมกระบวนการวางแผนและจัดองค์กร (PO) และการติดตามประเมินผล (M) มีผลต่อความมีประสิทธิผลของการควบคุมในกระบวนการจัดหาและการนำระบบออกใช้งาน (AI) และ การจัดส่งและการสนับสนุน(DS) การที่ฝ่ายจัดการมีกระบวนการวางแผน จัดองค์กร และติดตามประเมินผลไม่เพียงพอจะเป็นผลให้การควบคุมเกี่ยวกับการจัดหาการนำระบบออกใช้งานและ การให้บริการและการสนับสนุนไม่มีประสิทธิผลไปด้วย ในทาง

ตรงกันข้ามการวางแผน การจัดองค์กร และการเฝ้าระวังที่เข้มแข็งสามารถแสดงและแก้ไขจุดอ่อนของการควบคุมเกี่ยวกับการจัดหา การนำระบบออกใช้งาน การส่งมอบและการสนับสนุน

ตัวอย่างเช่น ประสิทธิผลของการควบคุมระบบสารสนเทศในรายละเอียดเกี่ยวกับกระบวนการที่ได้มาและบำรุงรักษาซอฟท์แวร์ระบบงานประยุกต์ (อ้างอิงถึงกระบวนการ AI2 ของ COBIT) จะได้รับผลกระทบจากความเพียงพอของสภาพแวดล้อมของการควบคุมระบบสารสนเทศต่อกระบวนการ ดังต่อไปนี้

- การกำหนดแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (อ้างอิงถึงกระบวนการ PO ของ COBIT)
- การจัดการโครงการ (อ้างอิงถึงกระบวนการ PO10 ของ COBIT)
- การจัดการคุณภาพ (อ้างอิงถึงกระบวนการ PO11 ของ COBIT)
- การติดตามประเมินผลกระบวนการ (อ้างอิงถึงกระบวนการ M1 ของ COBIT)

การตรวจสอบการจัดหาระบบงานประยุกต์ ควรรวมถึงการระบุผลกระทบต่อกลยุทธ์ระบบสารสนเทศ วิธีการบริหารจัดการโครงการ การบริหารจัดการคุณภาพ และวิธีการในการติดตามประเมินผล ในกรณีตัวอย่างเช่น การบริหารจัดการโครงการไม่เพียงพอ ผู้ตรวจสอบควรพิจารณาดังนี้

- ทำการตรวจสอบเพิ่มเติมเพื่อให้เชื่อมั่นได้ว่า โครงการนั้นๆ มีการบริหารจัดการได้อย่างมีประสิทธิผล
- รายงานจุดอ่อนของสภาพแวดล้อมของการควบคุมระบบสารสนเทศต่อฝ่ายบริหาร

ตัวอย่างเพิ่มเติม ได้แก่ ประสิทธิผลของการควบคุมระบบสารสนเทศโดยละเอียดต่อกระบวนการความมั่นใจในความมั่นคงของระบบ(Ensure Systems Security)(COBIT อ้างอิงในกระบวนการ DS5)ให้ได้ผลนั้น ขึ้นอยู่กับความเพียงพอของสภาพแวดล้อมของการควบคุมระบบสารสนเทศต่อกระบวนการดังต่อไปนี้

- การกำหนดเทคโนโลยีสารสนเทศขององค์กรและความสัมพันธ์ (อ้างอิงถึงกระบวนการ PO4 ของ COBIT)
- การสื่อสารเป้าหมายและทิศทางการจัดการ (COBIT อ้างอิงในกระบวนการPO6)
- การประเมินความเสี่ยง (อ้างอิงถึงกระบวนการ PO9 ของ COBIT)
- การติดตามประเมินผลกระบวนการ (อ้างอิงถึงกระบวนการ M1 ของ COBIT)

การตรวจสอบความเพียงพอของค่าพารามิเตอร์ความปลอดภัยที่กำหนดในระบบหนึ่ง ๆ เช่น UNIX, Windows NT, RACF ควรรวมถึงการพิจารณานโยบายการการรักษาความปลอดภัยของผู้บริหาร (PO6) การแบ่งความรับผิดชอบด้านการรักษาความปลอดภัย (PO4) ขั้นตอนการ

ประเมินความเสี่ยง (PO9) และขั้นตอนติดตามประเมินผลการปฏิบัติตามนโยบายการรักษาความปลอดภัย (M1) แม้ในกรณีที่ค่าพารามิเตอร์ที่กำหนดไว้ไม่เป็นไปตามที่ผู้ตรวจสอบเห็นว่าเป็นการปฏิบัติที่ดีที่สุด (best practice) ก็ตาม ผลการประเมินอาจถือว่าเพียงพอ เมื่อเห็นว่าฝ่ายบริหารได้ทราบความเสี่ยงนั้น และฝ่ายบริหารมีนโยบายที่จะจัดการกับความเสี่ยงดังกล่าวแล้ว ข้อเสนอแนะของการตรวจสอบควรมุ่งเน้นไปที่การจัดการความเสี่ยงหรือนโยบาย เช่นเดียวกันกับค่าพารามิเตอร์ในรายละเอียดเหล่านั้น

2.7.2 การวางแผน (Planning)

การตรวจสอบเกี่ยวกับสภาพแวดล้อมของการควบคุมระบบสารสนเทศ (Approach to Pervasive IS Controls) แนวทางการตรวจสอบเกี่ยวกับการวางแผนการตรวจสอบระบบสารสนเทศกำหนดให้ผู้ตรวจสอบควรทำการประเมินเบื้องต้นเกี่ยวกับการควบคุมของงานที่จะตรวจสอบ การประเมินเบื้องต้นนี้ควรรวมการระบุและประเมินที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุมระบบสารสนเทศการทดสอบสภาพแวดล้อมของการควบคุมระบบสารสนเทศอาจดำเนินการในรอบการตรวจสอบที่แยกต่างหากจากการตรวจสอบที่ปฏิบัติงานอยู่ เนื่องจากสภาพของการควบคุมนี้จะเกี่ยวข้องกับการใช้ระบบสารสนเทศในหลายด้าน ผู้ตรวจสอบควรพิจารณาว่าการตรวจสอบในด้านนี้ที่ผ่านมา สามารถให้ความเชื่อมั่นในการระบุและประเมินการควบคุมเหล่านี้ได้หรือไม่

ในกรณีที่การตรวจสอบแสดงว่าสภาพแวดล้อมของการควบคุมระบบสารสนเทศไม่เป็นที่น่าพอใจ ผู้ตรวจสอบควรพิจารณาว่าผลการตรวจพบนี้กระทบกับวิธีการที่ได้วางแผนไว้เพื่อให้บรรลุถึงวัตถุประสงค์ของการตรวจสอบ

- สภาพแวดล้อมของการควบคุมระบบสารสนเทศที่เข้มแข็ง สามารถก่อให้เกิดความเชื่อมั่นที่ซึ่งจะได้จากผู้ตรวจสอบในการตรวจสอบการควบคุมระบบสารสนเทศในรายละเอียด
- สภาพแวดล้อมของการควบคุมระบบสารสนเทศที่อ่อนแอ อาจมีผลในทางลบต่อการควบคุมระบบสารสนเทศในรายละเอียดหรือเป็นการก่อให้เกิดจุดอ่อนในระดับรายละเอียด

ขั้นตอนการปฏิบัติงานตรวจสอบที่เพียงพอ ในกรณีที่สภาพแวดล้อมของการควบคุมระบบสารสนเทศมีแนวโน้มที่จะส่งผลกระทบที่สำคัญต่อวัตถุประสงค์ของการตรวจสอบ การวางแผนตรวจสอบเพียงการควบคุมในรายละเอียดไม่เป็นการเพียงพอ ในกรณีที่ไม่อาจเป็นไปได้หรือไม่สามารถทำการตรวจสอบสภาพแวดล้อมของการควบคุมระบบสารสนเทศได้ ผู้ตรวจสอบจะต้องรายงานข้อจำกัดในขอบเขตการทำงานดังกล่าว และต้องวางแผนเพื่อทดสอบสภาพแวดล้อมของการควบคุมระบบสารสนเทศที่เกี่ยวข้องเมื่อการควบคุมเหล่านี้มีส่วนช่วยให้บรรลุวัตถุประสงค์การตรวจสอบ

การควบคุมที่เกี่ยวข้อง สภาพแวดล้อมของการควบคุมระบบสารสนเทศที่เกี่ยวข้อง หมายถึง การควบคุมที่ส่งผลต่อวัตถุประสงค์การตรวจสอบเฉพาะที่กำหนดขึ้นสำหรับภารกิจนั้น เช่น กรณีที่วัตถุประสงค์การตรวจสอบต้องการรายงานการควบคุมที่เกี่ยวข้องกับการเปลี่ยนแปลงเฉพาะคลังโปรแกรม (program library) สภาพแวดล้อมของการควบคุมระบบสารสนเทศที่เกี่ยวกับนโยบายรักษาความปลอดภัย (PO6) จะถือว่าเกี่ยวข้องกัน แต่สภาพแวดล้อมของการควบคุมระบบสารสนเทศเกี่ยวกับการกำหนดทิศทางเทคโนโลยี (PO3) อาจไม่เกี่ยวข้องกัน ในการวางแผนการตรวจสอบ ผู้ตรวจสอบต้องระบุว่าประชากรกลุ่มใดของสภาพแวดล้อมของการควบคุมระบบสารสนเทศ มีผลกระทบต่อวัตถุประสงค์การตรวจสอบที่วางไว้เป็นการเฉพาะ และต้องวางแผนที่จะนำเข้ามารวมในขอบเขตการตรวจสอบ วัตถุประสงค์ในการควบคุมของ COBIT สำหรับการวางแผน การจัดการ และการติดตาม อาจช่วยผู้ตรวจสอบระบบสารสนเทศในการระบุสภาพแวดล้อมของการควบคุมระบบสารสนเทศที่เกี่ยวข้อง

หลักฐานการตรวจสอบ สภาพแวดล้อมของการควบคุมระบบสารสนเทศอาจไม่จำเป็นที่จะต้องจัดทำเป็นเอกสาร แต่ผู้ตรวจสอบต้องวางแผนหาหลักฐานการตรวจสอบว่าการควบคุมที่เกี่ยวข้องได้ดำเนินการไปอย่างมีประสิทธิผล แนวทางการทดสอบมีระบุไว้ในส่วนของการปฏิบัติงานตรวจสอบ(Performance of Audit Work)

การตรวจสอบเกี่ยวกับการควบคุมระบบสารสนเทศในรายละเอียด (Approach to Relevant Detailed IS Controls) กรณีที่ผลการตรวจสอบแสดงว่าสภาพแวดล้อมการควบคุมระบบสารสนเทศเป็นที่น่าพอใจ ผู้ตรวจสอบควรพิจารณาลดระดับการทดสอบการควบคุมระบบสารสนเทศในรายละเอียด ที่วางแผนไว้ เนื่องจากหลักฐานการตรวจสอบของสภาพแวดล้อมการควบคุมระบบสารสนเทศที่เข้มแข็ง ส่งผลต่อความเชื่อมั่นที่ ผู้ตรวจสอบอาจได้รับจากการตรวจสอบการควบคุมระบบสารสนเทศในรายละเอียด แต่ในกรณีที่ผลการตรวจสอบระบบสารสนเทศแสดงว่าสภาพแวดล้อมการควบคุมระบบสารสนเทศไม่เป็นที่น่าพอใจ ผู้ตรวจสอบควรดำเนินการทดสอบการควบคุมระบบสารสนเทศในรายละเอียด อย่างเพียงพอ เพื่อให้มีหลักฐานการตรวจสอบที่เชื่อว่าการควบคุมระบบสารสนเทศในรายละเอียด ยังมีประสิทธิผลอยู่ ถึงแม้สภาพแวดล้อมการควบคุมระบบสารสนเทศที่เกี่ยวข้องยังมีจุดอ่อนอยู่

2.7.3 การปฏิบัติงานตรวจสอบ (Performance of Audit Work)

การทดสอบสภาพแวดล้อมการควบคุมระบบสารสนเทศ ผู้ตรวจสอบควรดำเนินการทดสอบเพียงพอเพื่อให้เกิดความเชื่อมั่นว่าสภาพแวดล้อมการควบคุมระบบสารสนเทศที่เกี่ยวข้องเป็นไปอย่างมีประสิทธิผล ในช่วงที่ตรวจสอบหรือในช่วงเวลาใดเวลาหนึ่ง ขั้นตอนการทดสอบอาจรวมถึง การสังเกต การสอบถามหาหลักฐานสนับสนุน การสอบทานเอกสารที่เกี่ยวข้อง

(นโยบาย มาตรฐาน รายงานการประชุม ฯลฯ) การปฏิบัติซ้ำ (Re-performance) (เช่น เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วย (CAAT))

หากการทดสอบ สภาพแวดล้อมการควบคุมระบบสารสนเทศที่เกี่ยวข้อง มีผลเป็นที่น่าพอใจ ผู้ตรวจสอบควรปฏิบัติตามแผนการตรวจสอบการควบคุมระบบสารสนเทศในรายละเอียดที่เกี่ยวข้องกับวัตถุประสงค์การตรวจสอบต่อไป โดยการทดสอบอาจจะลดระดับลงกว่าการทดสอบในกรณีที่สภาพแวดล้อมการควบคุมระบบสารสนเทศมีผลไม่เป็นที่น่าพอใจ

2.7.4 การรายงาน (Reporting)

จุดอ่อนของสภาพแวดล้อมการควบคุมระบบสารสนเทศ ในกรณีที่ผู้ตรวจสอบระบุถึงจุดอ่อนที่พบในสภาพแวดล้อมการควบคุมระบบสารสนเทศ ผู้ตรวจสอบควรรายงานต่อฝ่ายบริหารเพื่อให้ความสนใจ แม้ว่างานในส่วนนี้จะไม่ได้กำหนดไว้ในขอบเขตการตรวจสอบก็ตาม

ในกรณีที่สภาพแวดล้อมการควบคุมระบบสารสนเทศ อาจส่งผลกระทบอย่างมีนัยสำคัญต่อประสิทธิผลของการควบคุมระบบสารสนเทศในรายละเอียด และยังไม่มีการตรวจสอบสภาพแวดล้อมการควบคุมระบบสารสนเทศ ผู้ตรวจสอบควรรายงานเรื่องดังกล่าวต่อฝ่ายบริหารโดยระบุไว้ในรายงานการตรวจสอบขั้นสุดท้าย พร้อมระบุผลที่อาจกระทบจากข้อตรวจพบดังกล่าว ข้อสรุป และข้อเสนอแนะ เช่น เมื่อผู้ตรวจสอบออกรายงานการตรวจสอบการจัดซื้อโปรแกรมสำเร็จรูป แต่ไม่พบว่าองค์กรมีแผนกลยุทธ์ทางด้านระบบสารสนเทศ ดังนั้น รายงานการตรวจสอบควรระบุด้วยว่า องค์กรไม่ได้จัดทำแผนกลยุทธ์ด้านระบบสารสนเทศไว้ให้พร้อมใช้งานหรือองค์กรไม่มีแผนกลยุทธ์ดังกล่าว และผู้ตรวจสอบควรรายงานผลที่อาจเกิดจากข้อตรวจพบ ข้อสรุป และข้อเสนอแนะ เช่น ข้อความที่ว่า ดังนั้นไม่อาจจะกล่าวได้ว่าการจัดซื้อโปรแกรมสำเร็จรูปเป็นไปตามแผนกลยุทธ์ด้านระบบสารสนเทศและจะเป็นการสนับสนุนแผนการดำเนินธุรกิจในอนาคตหรือไม่

2.8 งานวิจัยที่เกี่ยวข้อง

กฤษฎา แก้วผุดผ่อง (2551) ศึกษาเรื่อง ระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กร ตามมาตรฐานสากล BS 7799 กรณีศึกษา : สำนักหอสมุด มหาวิทยาลัยมหิดล ซึ่งมาตรฐาน BS7799 (Britist Standard) หรือมาตรฐานสากล ISO/IEC 17799:2005 และ ISO/IEC27001 มุ่งเน้นด้านการศึกษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร โดยแบ่งเนื้อหาออกเป็น 11 หัวข้อหลัก (Domain) ซึ่งแต่ละหัวข้อประกอบด้วยวัตถุประสงค์ที่แตกต่างกัน รวมทั้งสิ้น 39 วัตถุประสงค์ (Control objectives) และภายใต้วัตถุประสงค์แต่ละข้อประกอบด้วยมาตรการในการรักษาความปลอดภัยที่แตกต่างกัน รวมจำนวน 133 ข้อ (Controls)

มาตรฐาน ISO/IEC27001 เป็นเรื่องของข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยให้กับองค์กร และใช้เป็นแนวทางการประเมินความเสี่ยงมาประกอบการพิจารณาหาวิธีการหรือมาตรการเพื่อป้องกัน ลดความเสี่ยง และรักษาทรัพย์สินสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยในระดับที่เหมาะสม รวมไปถึงการรักษาความปลอดภัยของข้อมูลซึ่งเป็นส่วนสำคัญส่วนหนึ่งในการบริหารหน่วยงานให้เป็นไปอย่างมีประสิทธิภาพ อันจะนำไปสู่ความปลอดภัยในหน่วยงาน ทั้งนี้ มีการจัดทำกระบวนการจัดการประเมินความเสี่ยง เพื่อศึกษาถึงปัญหาหรือภัยคุกคามในรูปแบบต่าง ๆ ที่ก่อให้เกิดความเสียหายต่อทรัพย์สินด้านสารสนเทศขององค์กร ซึ่งมีการจัดหมวดหมู่ของทรัพย์สินออกเป็น 5 หมวดคือ อุปกรณ์คอมพิวเตอร์ (Hardware) โปรแกรม (Software) บุคลากร (People) ข้อมูล (Information) และงานบริการ (Service) เพื่อทำการคำนวณหาค่าความเสี่ยงที่เกิดขึ้นในทรัพย์สินนั้น ๆ แล้วจัดระดับของความเสี่ยง รวมไปถึงการศึกษาเพื่อค้นหาถึงจุดอ่อนของตัวข้อมูลและทรัพย์สินนั้น ๆ ซึ่งเป็นสาเหตุที่ก่อให้เกิดปัญหาและภัยคุกคาม เพื่อนำความเสี่ยงที่เกินระดับที่องค์กรสามารถยอมรับได้ไปดำเนินการควบคุมและแก้ไขความเสี่ยงโดยการออกเป็นมาตรการป้องกันเพื่อให้บุคลากรในหน่วยงานปฏิบัติตาม รวมทั้งยังเป็นการกำหนดรูปแบบการรับมือในเรื่องความปลอดภัยได้อย่างมีระบบและมีประสิทธิภาพ นอกจากนี้ การพัฒนาระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กร สามารถช่วยในการเผยแพร่ข้อมูลให้ผู้ใช้งานทราบถึงแนวทางในการจัดทำการบริหารความเสี่ยงสำหรับทรัพย์สินสารสนเทศภายในองค์กร กระบวนการจัดการประเมินความเสี่ยง ผู้ใช้งานยังทราบถึงช่องโหว่ ภัยคุกคาม ระดับของความเสี่ยงที่เกิดขึ้นต่อทรัพย์สินในประเภทต่าง ๆ รวมไปถึงแนวทางการป้องกัน และสามารถค้นหาทรัพย์สินที่ผู้ใช้ต้องการทราบถึงรายละเอียดในการจัดทำการบริหารความเสี่ยงสำหรับทรัพย์สินนั้นแล้วเชื่อมโยงไปยังข้อมูลเหล่านั้นได้ และแสดงรายงาการจัดระดับความเสี่ยงของทรัพย์สินให้ผู้ใช้ได้ทราบ อีกทั้งยังเป็นการสร้างความมั่นใจในการติดต่อสื่อสารระหว่างหน่วยงานให้มีความมั่นคงปลอดภัยในระดับที่สูงขึ้นด้วย

เบ็ญจมาศ ฮะยิ้ม (2549) ศึกษาเรื่อง การศึกษาการควบคุมภายในโดยการประเมินตนเอง (Control Self – Assessment : CSA) โดยการวิจัยครั้งนี้เพื่อศึกษาข้อมูลพื้นฐานในเรื่องการจัดวางระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศ ระดับอุดมศึกษาทั้งภาครัฐบาลและเอกชนว่ามีวิธีการ รูปแบบปฏิบัติอย่างไร ทั้งนี้ต้องสอดคล้องกับนโยบาย ระเบียบวิธีปฏิบัติของการควบคุมภายในโดยต้องมีการบริหารความเสี่ยงที่เหมาะสม โดยมีวัตถุประสงค์เพื่อศึกษานโยบายที่เกี่ยวข้องกับการบริหารเทคโนโลยีสารสนเทศของสถาบันอุดมศึกษา การจัดวางระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศโดยการประเมินตนเอง (Control Self-Assessment : CSA) ของสถาบันอุดมศึกษา รูปแบบการบริหารความเสี่ยงและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ของสถาบันอุดมศึกษาในปัจจุบัน และเสนอแนะการจัดวางระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศโดยการประเมินตนเอง (Control Self-Assessment : CSA) ของสถาบันอุดมศึกษาในอนาคต การศึกษาครั้งนี้ได้รวบรวมทฤษฎีและหลักการเกี่ยวกับการตรวจสอบภายในเทคโนโลยีสารสนเทศ การควบคุมภายในโดยการประเมินตนเอง (Control Self – Assessment : CSA) ด้านเทคโนโลยีสารสนเทศ, Balanced Scorecard (BSC), Key Performance Indicators (KPIs), การประเมิน Measurement, Knowledge Management และ Infromation Technology Program โดยงานวิจัยนี้ได้กล่าวถึงแนวทางการตรวจสอบเทคโนโลยีสารสนเทศไว้ว่า จากกระบวนการ COBIT เป็นรายละเอียดสำคัญที่จะต้องปฏิบัติตามและเป็นส่วนหนึ่งของระบบควบคุมภายใน โดยส่วนที่สำคัญคือกระบวนการประเมินความเสี่ยงจากการควบคุมในระบบควบคุมภายในทางด้านคอมพิวเตอร์ เช่นเดียวกับระบบควบคุมภายในด้วยมือ ดังนั้น กระบวนการประเมินความเสี่ยงจากการควบคุมด้านคอมพิวเตอร์ประกอบด้วย

1. พิจารณาความรู้ที่ได้รับจากการศึกษาทำความเข้าใจเกี่ยวกับเทคโนโลยีสารสนเทศและการควบคุมภายใน

2. ระบุข้อผิดพลาดที่อาจเกิดขึ้นในระบบสารสนเทศ และระบบควบคุมภายใน

3. ระบุวิธีการควบคุมภายในที่จำเป็นเพื่อป้องกัน ค้นหา หรือแก้ไขข้อผิดพลาดเหล่านั้น

4. ปฏิบัติการทดสอบการควบคุม

5. ประเมินหลักฐานการตรวจสอบเทคโนโลยีสารสนเทศและประเมินผล

พิมพ์กมล ศรีสวัสดิ์ (2551) ศึกษาเรื่อง การประเมินความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศด้วย Cobit เป็นการศึกษาค้นคว้าอิสระด้วยตนเองโดยเป็นการศึกษากระบวนการประเมินความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศ เป็นการทำความเข้าใจและวิเคราะห์เป้าหมาย ความเสี่ยงและการควบคุมภายในขององค์กร แล้วนำผลที่ได้มาพิจารณาประเมินระดับความเสี่ยงและการควบคุมทั่วไปทางด้านเทคโนโลยีสารสนเทศ สำหรับใช้เป็นข้อมูลในการจัดทำรายงานและสรุปผลเพื่อวางแผนโครงการบริหารจัดการเทคโนโลยีสารสนเทศในองค์กรต่อไป โดยในการศึกษาค้นคว้าอิสระนี้ได้ใช้กระบวนการประเมินความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศ ซึ่งอ้างอิงตามมาตรฐาน Cobit (Control Objective for Information and Related Technology) ของสมาคมผู้ตรวจสอบและควบคุมสารสนเทศ (Information System Audit and Control Association (ISACA)) งานวิจัยครั้งนี้ได้รวบรวมทฤษฎีและหลักการเกี่ยวกับการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ , กรอบงานโคบิต (Cobit Framework) โดยมีขั้นตอนสำคัญดังนี้

1. การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Analysis) จะมีการกำหนดหรือบ่งชี้ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การกำหนดปัจจัยที่ใช้ในการประเมินระดับความเสี่ยง

ด้านเทคโนโลยีสารสนเทศ ผลการประเมินปัจจัยที่มีผลต่อความเสี่ยงด้านเทคโนโลยีสารสนเทศ ผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ และสรุปผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

2. การประเมินการควบคุมภายใน จะมีการกำหนดเกณฑ์ที่ใช้ประเมินระดับการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ขั้นตอนการประเมินการควบคุมภายในเทคโนยีสารสนเทศ สรุปผลการประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ และการสรุปภาพรวมของระดับการควบคุมภายในเทคโนโลยีสารสนเทศ

3. การรายงานผลต่างของระดับความเสี่ยงกับการควบคุมภายใน (Gap Analysis Report) ซึ่งเป็นการพิจารณาเปรียบเทียบถึงผลต่างระหว่างระดับความเสี่ยงกับการควบคุมภายในเทคโนโลยีสารสนเทศ ซึ่งถือเป็นขั้นตอนสำคัญที่ใช้ในการบ่งชี้ถึงระดับความเสี่ยงที่ยังคงเหลืออยู่ เนื่องจากมีระดับการควบคุมภายในที่ยังไม่ครอบคลุมความเสี่ยงที่มีอยู่ในปัจจุบัน เพื่อให้ผู้บริหารรับทราบและพิจารณาปรับปรุงการควบคุมภายในด้านต่างๆ ให้เหมาะสมกับระดับความเสี่ยง ที่อาจส่งผลกระทบรุนแรงต่อความสามารถในการบรรลุเป้าหมายขององค์กร โดยการอ้างอิงข้อมูลจากรายงานผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ และรายงานผลการประเมินการควบคุมภายในเทคโนโลยีสารสนเทศ เพื่อนำข้อมูลมาเปรียบเทียบวิเคราะห์

4. รายงานสรุปผล (Summary Report) เป็นขั้นตอนของการนำผลลัพธ์ที่ได้จากการวิเคราะห์ผลต่างของระดับความเสี่ยง กับการควบคุมภายในเทคโนโลยีสารสนเทศ มาจัดประชุมเพื่อสรุปผลและนำเสนอกิจกรรมการควบคุมภายในสารสนเทศที่ควรปรับปรุงและพัฒนา ให้ถือปฏิบัติเป็นมาตรฐานการควบคุมภายในขององค์กรประกอบด้วยการดำเนินการตามขั้นตอนดังต่อไปนี้

4.1 นำเสนอกระบวนการควบคุมภายในที่ยังไม่ได้รับการจัดการควบคุมอย่างเพียงพอ

4.2 จัดลำดับความสำคัญของการควบคุมภายในที่ไม่เพียงพอต่อการจัดการความเสี่ยง

4.3 จัดทำตารางเวลาในการดำเนินโครงการบริหารจัดการเทคโนโลยีสารสนเทศตามลำดับความสำคัญ

จตุพล จิตรพงษ์ (2548) ศึกษาเรื่อง การตรวจสอบระบบสารสนเทศเพื่อประสิทธิผลโดยรวมขององค์กร ด้านซอฟต์แวร์และฮาร์ดแวร์ เป็นการศึกษาค้นคว้าอิสระด้วยตนเองโดยมีวัตถุประสงค์ในการศึกษาและหาแนวทางในการตรวจสอบระบบสารสนเทศในองค์กรทางด้านฮาร์ดแวร์และซอฟต์แวร์ ตลอดจนการนำฮาร์ดแวร์และซอฟต์แวร์ไปใช้ให้เกิดประโยชน์สูงสุดด้านประสิทธิภาพ (efficiency) และประสิทธิผล (Effectiveness) เพื่อให้องค์กร สามารถนำแนวทางการปฏิบัติงานและแบบแผนการกำกับดูแลที่ดีของกระบวนการปฏิบัติงานด้านสารสนเทศที่เกิดจากการค้นคว้านี้ไปประยุกต์ใช้ในองค์กรได้โดยง่ายและรวดเร็ว ทำให้ระบบสารสนเทศภายในองค์กรมี

ประสิทธิภาพและประสิทธิผลมากขึ้น และองค์กรต่างๆในประเทศมีแนวทางในการตรวจสอบไปในทิศทางเดียวกัน สามารถนำผลลัพธ์ที่ได้จากการประเมินการใช้งานระบบสารสนเทศภายในองค์กรมาเปรียบเทียบและประเมินศักยภาพ โดยรวมของการใช้งานระบบสารสนเทศภายในองค์กรและสามารถสร้างบรรทัดฐานสำหรับอ้างอิงให้องค์กรต่างๆใช้เปรียบเทียบและอ้างอิง เพื่อการปรับปรุงและพัฒนาระบบสารสนเทศภายในองค์กรอย่างมีประสิทธิภาพและประสิทธิพลต่อไปได้ ทั้งนี้ การศึกษานี้ได้รวบรวมทฤษฎีและหลักการสำหรับการตรวจสอบทางด้านฮาร์ดแวร์และซอฟต์แวร์ การประเมินความเสี่ยง และ กรอบงานสำหรับการตรวจสอบคุณภาพของระบบสารสนเทศ ซึ่งประกอบด้วย TCO (Total Cost of Ownership) ซึ่งได้รับการพิจารณาและได้รับการยอมรับให้เป็นมาตรฐานเพื่อที่จะประเมินต้นทุนรวม, ITIL (Information Technology Infrastructure Library) เป็นโมเดลที่เหมาะสำหรับนำไปใช้งานกับองค์กรที่เป็นผู้ให้บริการทางด้านสารสนเทศ (Service Information Technology), CMM (Capability Maturity Model) ซึ่งเป็นต้นแบบของการวัดวุฒิภาวะความสามารถในการทำงาน ที่ทางสถาบัน Software Engineering Institute (SEI) แห่งมหาวิทยาลัย คาร์เนกี เมลลอน ได้พัฒนาขึ้น, COBIT (Control Objectives for Information and related Technology) ซึ่งกำหนดโดย Information Systems Audit and Control Foundation (ISACF) ซึ่งเป็นองค์กรภายใต้สมาคมการตรวจสอบและการควบคุมระบบสารสนเทศ (ISACA) ซึ่ง COBIT Framework เป็นกรอบที่สามารถใช้ในการบริหารและจัดการเทคโนโลยีสารสนเทศ, Six Sigma ซึ่งมีแนวคิดหลักคือการลดความแปรปรวนของกระบวนการที่อาจเป็นสาเหตุของปญหาคุณภาพ, ISO 9000 มาตรฐานระบบการบริหารงานซึ่งเป็นมาตรฐานระบบการบริหารงานขององค์กร โดยมุ่งเน้นด้านคุณภาพที่ประเทศต่าง ๆ ทั่วโลกให้การยอมรับและนำไปใช้อย่างแพร่หลาย กำหนดขึ้นโดยองค์การระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization - ISO), Malcolm Baldrige (สำนักมาตรฐานและประเมินผลอุดมศึกษา, 2547) เป็นกรอบของเกณฑ์ในการดำเนินการเพื่อสร้างความตระหนักเรื่องความสำคัญของคุณภาพและการทำให้มีผลการดำเนินงานที่เป็นเลิศเพื่อเพิ่มศักยภาพในการแข่งขัน ตลอดจนวิธีการในการประเมินผลการปฏิบัติงานในรูปแบบ Balance Scorecard (BSC)

อรพรรณ เชาว์สุวรรณกิจ (2549) ศึกษาเรื่อง การพัฒนาโมเดลและเครื่องมือสำหรับการตรวจประเมินทรัพยากรสารสนเทศ สำหรับการบริหารจัดการข้อมูลที่ดี ซึ่งมีวัตถุประสงค์เพื่อศึกษากระบวนการตรวจประเมินทรัพยากรสารสนเทศ และออกแบบระบบสำหรับการตรวจประเมินระบบสารสนเทศในรูปแบบโปรแกรมประยุกต์เชิงเว็บ โดยอาศัยมาตรฐานการควบคุมเทคโนโลยีสารสนเทศและการบริหารจัดการคุณภาพแบบเบ็ดเสร็จ ในการพัฒนาโมเดลและเครื่องมือให้มีประสิทธิภาพ ซึ่งผลที่ได้จากการศึกษาคือกระบวนการและเครื่องมือสำหรับการ

ตรวจประเมินที่มีคุณภาพ (Quality Checklist) การศึกษาครั้งนี้ได้รวบรวมทฤษฎีและหลักการเกี่ยวกับมาตรฐานการควบคุมเทคโนโลยีสารสนเทศ ได้แก่ COSO Framework และ COBIT Framework หลักการของ Total Quality Management (TQM) หลักการของ Total Data Quality Management (TDQM) ซึ่งเมื่อนำทฤษฎีของ TDQM และทฤษฎีการตรวจสอบและการควบคุมสารสนเทศมาประยุกต์ร่วมกัน จะทำให้เกิดแนวทางการตรวจสอบและการควบคุมสารสนเทศเพื่อให้ได้ข้อมูลที่ดีและมีคุณภาพมากที่สุด โดยสามารถปฏิบัติเป็นวัฏจักร เพื่อให้เกิดการมีคุณภาพของข้อมูลตลอดเวลา นอกจากนี้ ผู้ศึกษายังได้รวบรวมทฤษฎีสำหรับการสร้างเครื่องมือในการตรวจสอบระบบสารสนเทศ (Checklist) ได้แก่ หลักการตั้งคำถาม หลักการสัมภาษณ์ การสังเกต การเลือกผู้ถูกสัมภาษณ์ เครื่องมือการจัดการความรู้ ตลอดจนเทคโนโลยีสำหรับการพัฒนาโปรแกรมประยุกต์เชิงเว็บ (Web based Application) รวมถึงการออกแบบการจัดเก็บฐานข้อมูล

บทที่ 3
ระเบียบวิธีวิจัย

3.1 ขั้นตอนการดำเนินการวิจัย

ขั้นตอนการดำเนินการวิจัย มีดังต่อไปนี้

1. ศึกษาทฤษฎีที่เกี่ยวข้องและงานวิจัย
2. ศึกษาเทคโนโลยีสารสนเทศขององค์กร
3. จัดทำประเด็นการตรวจสอบ
4. จัดทำแนวการตรวจสอบสำหรับการตรวจสอบเทคโนโลยีสารสนเทศ
5. นำแนวการตรวจสอบมาทดลองตรวจสอบเทคโนโลยีสารสนเทศขององค์กรในบางประเด็น

3.2 อุปกรณ์และเครื่องมือที่ใช้ในการวิจัย

3.2.1 อุปกรณ์ฮาร์ดแวร์ที่จะนำมาใช้

1. เครื่องไมโครคอมพิวเตอร์ (Desktop) หรือ Labtop
   - หน่วยความจำหลักไม่น้อยกว่า 512 MB
   - หน่วยความจำสำรองไม่น้อยกว่า 40 GB
2. เครื่องคอมพิวเตอร์โน้ตบุ๊ค
   - ระดับ Pentium M 1.73 Ghz
   - หน่วยความจำ (RAM) 2 GB
   - ความจุของฮาร์ดดิสก์ 60 GB
   - จอภาพขนาด 15 นิ้ว
   - เม้าส์ และ แป้นพิมพ์

3.2.2 ซอฟต์แวร์ที่จะนำมาใช้

- MS-Windows XP
- MS Office 2006
- Internet Explorer Version 6.0 or Higher

3.3 ระยะเวลาในการดำเนินการวิจัย

ระยะเวลาในการดำเนินการวิจัย สรุปได้ดังตารางที่ 3.1

ตารางที่ 3.1 ระยะเวลาในการดำเนินการวิจัย

ขั้นตอน/ระยะเวลา (เดือน)	1	2	3	4	5	6	7	8	9	10	11	12
1. ศึกษาทฤษฎีที่เกี่ยวข้องและงานวิจัย												
2. ศึกษาเทคโนโลยีสารสนเทศขององค์กร												
3. จัดทำประเด็นการตรวจสอบ												
4. จัดทำแนวการตรวจสอบสำหรับการตรวจสอบเทคโนโลยีสารสนเทศ												
5. นำแนวการตรวจสอบมาทดลองตรวจสอบเทคโนโลยีสารสนเทศขององค์กรในบางประเด็น												

บทที่ 4
ผลการศึกษา

เนื้อหาของบทนี้กล่าวถึง การศึกษาเกี่ยวกับการตรวจสอบระบบสารสนเทศ และการนำมาตรฐานของ COBIT Framework มาประยุกต์ในการจัดทำแนวการตรวจสอบระบบเทคโนโลยีสารสนเทศ โดยมีรายละเอียดดังต่อไปนี้

4.1 การศึกษาเกี่ยวกับการตรวจสอบสารสนเทศ

เนื่องจากการตรวจสอบระบบเทคโนโลยีสารสนเทศ เป็นกระบวนการในการรวบรวมหลักฐานและประเมินหลักฐาน เพื่อแสดงความเห็นเกี่ยวกับความถูกต้อง เชื่อถือได้ การรักษาความปลอดภัย การปฏิบัติงานได้อย่างมีประสิทธิภาพและประสิทธิผลตามวัตถุประสงค์ที่กำหนด

กระบวนการตรวจสอบระบบเทคโนโลยีสารสนเทศ (อุษณา ภัทรมนตรี, 2551)

การตรวจสอบระบบเทคโนโลยีสารสนเทศ จะประกอบด้วยขั้นตอนต่างๆ โดยมีรายละเอียดดังต่อไปนี้

1. การวางแผนการตรวจ ซึ่งจะแบ่งเป็นการวางแผนการตรวจโดยรวม เช่น การทำความเข้าใจในเรื่องที่ตรวจ การประเมินความเสี่ยง และการวางแผนงานตรวจสอบในรายละเอียด เช่น การกำหนดโปรแกรมการตรวจสอบและเทคนิควิธีการตรวจสอบ
2. การปฏิบัติงานรวบรวมหลักฐานตามแผนและโปรแกรมการตรวจสอบที่กำหนด
3. การสรุปผลและรายงานผลการตรวจ
4. การติดตามผลการตรวจ

ทั้งนี้ จากลักษณะการปฏิบัติงานขององค์กรในปัจจุบันที่เปลี่ยนแปลงไปเมื่อองค์กรมีการใช้คอมพิวเตอร์ในการประมวลผลสารสนเทศ ทำให้เกิดความเสี่ยงและโอกาสในการตรวจสอบระบบเทคโนโลยีสารสนเทศที่ใช้คอมพิวเตอร์ในภาพรวม ดังนี้

1. ความเสี่ยงจากการขาดการแบ่งแยกหน้าที่ในการปฏิบัติงาน มีการรวมโปรแกรมและแฟ้มข้อมูลในที่เดียวกัน ทำให้ผู้ปฏิบัติงานคนเดียวอาจเข้าถึงโปรแกรม และทำการอนุมัติและบันทึกข้อมูลในแฟ้มข้อมูลได้โดยคนเดียวกัน
2. ความเสี่ยงจากการขาดเอกสารนำเข้าและไม่มีร่อยรอยติดตามการบันทึกที่มองเห็นได้ด้วยตา ทำให้ยากต่อการตรวจพบความผิดพลาด

3. ความเสี่ยงจากความผิดพลาดของโปรแกรม

4. โอกาสในการเกิดข้อผิดพลาดและรายการผิดปกติมีสูง และค้นพบยากกว่าระบบมือ เนื่องจากมีรายละเอียดและปริมาณมาก

5. โอกาสการเข้าถึงโปรแกรมและแฟ้มข้อมูลโดยไม่ได้รับอนุญาตมีมากจากเทอร์มินัลห่างไกล

6. การเกิดรายการหรือการประมวลผลโดยอัตโนมัติด้วยโปรแกรมที่กำหนด จึงต้องมีการควบคุมในระหว่างการพัฒนาและเปลี่ยนแปลงโปรแกรมอย่างเพียงพอและมีประสิทธิผลสูง

7. การควบคุมกำกับดูแลโดยผู้บริหารและการควบคุมสภาพแวดล้อมของการควบคุมมีความสำคัญกว่าในระบบมือมาก เพราะมีผลกระทบกว้างต่อทุกระบบงาน

การประเมินความเสี่ยง

การตรวจสอบระบบเทคโนโลยีสารสนเทศ ควรจะต้องตระหนักถึงการเปลี่ยนแปลงของความเสี่ยง และการยืดหยุ่นในการปรับวิธีการตรวจสอบตามการเปลี่ยนแปลงของความเสี่ยง

การประเมินความเสี่ยง ประกอบด้วยขั้นตอนที่สำคัญ ได้แก่การพิจารณาวัตถุประสงค์ที่ต้องการ การระบุเหตุการณ์และปัจจัยความเสี่ยง การประเมินจัดระดับความเสี่ยง การจัดการตอบสนองความเสี่ยง และ กิจกรรมควบคุม

1. การพิจารณาวัตถุประสงค์ที่ต้องการ (Objective Setting)

เป็นการพิจารณาว่าอะไรเป็นวัตถุประสงค์สำคัญที่ต้องการของระบบเทคโนโลยีสารสนเทศนั้น เช่น การรักษาความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งาน การปฏิบัติตามกฎระเบียบ ซึ่งแต่ละกิจการหรือแต่ละระบบอาจมีวัตถุประสงค์ไม่เหมือนกัน

2. การระบุเหตุการณ์หรือปัจจัยความเสี่ยงที่เกี่ยวข้อง

เป็นการพิจารณาว่าอะไรเป็นเหตุการณ์ที่อาจเกิดขึ้นมีผลกระทบต่อวัตถุประสงค์ที่กำหนดไว้ในข้อ 1 ซึ่งอาจเกิดจากปัจจัยเสี่ยงที่มีอิทธิพลทั้งภายนอกและภายใน การระบุเหตุการณ์มีขั้นตอนย่อยที่สำคัญ ได้แก่

2.1 การระบุเหตุกาณ์หรือปัจจัยเสี่ยง ซึ่งเหตุการณ์หรือปัจจัยเสี่ยง หมายถึงเหตุการณ์ความไม่แน่นอนที่อาจเกิดขึ้นทั้งจากปัจจัยภายในและภายนอก ทั้งเหตุการณ์ที่เคยและไม่เคยเกิด แต่หากเกิดแล้วจะมีผลกระทบสำคัญต่อวัตถุประสงค์ที่ต้องการ เช่น การเปลี่ยนแปลงกฎระเบียบและสภาพแวดล้อมในการปฏิบัติงาน บุคลากรใหม่หรือการเปลี่ยนแปลง ระบบสารสนเทศใหม่หรือการเปลี่ยนแปลงระบบ เทคโนโลยีใหม่ รูปแบบธุรกิจใหม่ การปรับปรุงโครงสร้างขององค์กร เป็นต้น

2.2 การพิจารณาความสัมพันธ์ของเหตุการณ์หรือปัจจัยความเสี่ยงด้านไอที เป็นการพิจารณาถึงความสัมพันธ์ของปัจจัยเสี่ยงที่เกิดขึ้น เป็นการพิจารณาเป็นองค์รวม (Holistically) นอกจากนี้ต้องพิจารณาว่าเป็นความเสี่ยงที่มีผลกระทบกว้าง (Pervasive Risk) ในระดับทั้งองค์การ หรือเป็นความเสี่ยงที่มีผลกระทบเฉพาะ (Specific Risk) ในระดับระบบงาน

3. การประเมินจัดระดับความเสี่ยง (Risk Assessment)

เป็นการพิจารณาจากสองด้าน คือ จากระดับความน่าจะเกิด (Likelihood) และระดับนัยสำคัญของผลกระทบหรือความเสียหายที่อาจเกิดขึ้น (Impact, Significance, Materiality, Consequences) เพื่อหาวิธีการจัดการตอบสนองและควบคุมความเสี่ยงนั้นให้เหมาะสม มีขั้นตอนย่อยดังนี้

3.1 การกำหนดระดับความน่าจะเกิด อาจกำหนดเป็นค่า 1-5 จากน้อยไปถึงมากที่สุด ซึ่งอาจพิจารณาจากความถี่ที่เคยเกิดในอดีต หรือจากระยะเวลาที่คาดว่าจะเกิดในอนาคต หรือจากระยะเวลาที่คาดว่าจะเกิดในอนาคต หรือพิจารณาจากความซับซ้อน ปริมาณงาน และจุดอ่อนในการควบคุมของเหตุการณ์นั้น และพิจารณาตามข้อมูลในเชิงปริมาณที่นับได้ คำนวณได้ และข้อมูลเชิงคุณภาพที่มาจากความคิดเห็นและดุลยพินิจ

3.2 การกำหนดนัยสำคัญของผลกระทบที่เกิด อาจกำหนดเป็นค่า 1-5 จากน้อยไปถึงมากที่สุด ซึ่งอาจพิจารณาจากจำนวนเงิน หรือจากระดับที่เกิด เช่น เกิดผลกระทบระดับรายการค้า ระดับแฟ้ม หรือระดับระบบงาน เป็นต้น

3.3 การวิเคราะห์ทบทวนค่าและตำแหน่งความเสี่ยง เป็นการทบทวนโดยการขอความเห็นชอบร่วมกันระหว่างผู้บริหาร ผู้ปฏิบัติงาน และผู้เกี่ยวข้องอื่นว่า ระดับความน่าจะเกิดและระดับนัยสำคัญที่กำหนดเป็นค่าที่เหมาะสมเชื่อถือได้แล้วหรือไม่ เช่น การพิจารณาความเสี่ยงที่ซ่อนเร้นยังไม่แสดงให้เห็นในปัจจุบัน เป็นต้น

4. การจัดการตอบสนองความเสี่ยง

เป็นการพิจารณาว่ากิจการมีวิธีการตอบสนองความเสี่ยงที่เหมาะสมแล้วหรือไม่ ซึ่งวิธีการตอบสนองความเสี่ยงที่เป็นพื้นฐานมี 4 วิธี ได้แก่ การยอมรับ การขจัด การถ่ายโอนหรือกระจายความเสี่ยง และการควบคุมความเสี่ยง

ทั้งนี้ จะต้องพิจารณาว่า วิธีการที่เลือกจะเป็นวิธีการที่จะลดระดับความน่าจะเกิด และหรือระดับนัยสำคัญของผลกระทบที่เกิด ให้อยู่ในระดับความเสี่ยงที่กิจการยอมรับได้หรือไม่ ก่อให้เกิดภาระและค่าใช้จ่ายเท่าไร และคุ้มค่าหรือไม่เมื่อเทียบกับความเสียหายที่อาจจะเกิดจากความเสี่ยงนั้น

5 การจัดการควบคุมด้านเทคโนโลยีสารสนเทศ

การควบคุมด้านเทคโนโลยีสารสนเทศ (IT Controls) หมายถึง กระบวนการที่สร้างความมั่นใจในความถูกต้องเชื่อถือได้ของสารสนเทศและการให้บริการด้านสารสนเทศ รวมทั้งการช่วยลดความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยี ทั้งนี้ การควบคุมด้านเทคโนโลยีสารสนเทศมี 3 ประเภทใหญ่ ๆ ได้แก่

5.1 การควบคุมทั่วไปกับการควบคุมระบบงาน

- การควบคุมทั่วไป (General Control) หมายถึง การควบคุมทั่วไปที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุม การควบคุมทางนโยบาย การบริหาร และการควบคุมด้านโครงสร้างทางเทคนิค ซึ่งการควบคุมทั่วไปนี้จะเป็นพื้นฐานสำคัญต่อประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศทั้งหมด รวมทั้งประสิทธิผลของการควบคุมระบบงาน

- การควบคุมระบบงาน (Application Controls) หมายถึง การควบคุมที่มีเฉพาะกระบวนการหรือระบบงาน เพื่อควบคุมความถูกต้องครบถ้วนของข้อมูลในระหว่างการนำเข้า การประมวลผล และผลลัพธ์ที่ได้จากระบบงานนั้น

5.2 การควบคุมตามวัตถุประสงค์หรือหน้าที่ ได้แก่ การควบคุมแบบป้องกันแบบค้นพบ และแบบแก้ไข

- การควบคุมแบบป้องกัน (Preventive Controls) หมายถึง การควบคุมที่สร้างขึ้นเพื่อป้องกันความผิดพลาด การละเว้น ความไม่ปลอดภัย และอุบัติภัยที่อาจเกิดขึ้น

- การควบคุมแบบค้นพบ (Detective Controls) หมายถึง การควบคุมที่สร้างขึ้นเพื่อค้นพบ ความผิดพลาด การละเลย ความไม่ปลอดภัย และอุบัติภัยที่เกิดขึ้น ซึ่งหลุดรอดมาจากการควบคุมแบบป้องกัน

- การควบคุมแบบแก้ไข (Corrective Controls) หมายถึง การควบคุมที่สร้างขึ้นเพื่อแก้ไขความผิดพลาด การละเลย ความไม่ปลอดภัย หรืออุบัติภัยที่ค้นพบ ซึ่งอาจมีการแก้ไขทั้งแบบง่ายหรือที่ซับซ้อนตามความเหมาะสม

5.3 การควบคุมตามระดับการบริหาร ได้แก่ การควบคุมระดับการกำกับดูแล ระดับการบริหาร และระดับเทคนิคการปฏิบัติงาน

- การควบคุมระดับการกำกับดูแล (Governance Controls) หมายถึง การควบคุมที่คณะกรรมการองค์การ มีบทบาทหน้าที่ความรับผิดชอบ ส่วนใหญ่จะเกี่ยวข้องกับการควบคุมระดับนโยบาย กลยุทธ์ แผนงานสำคัญ หรือที่มีผลกระทบต่อสถาบันกำกับดูแลและบุคคลภายนอก

- การควบคุมระดับการบริหาร (Management Controls) หมายถึง การควบคุมที่ฝ่ายบริหารมีบทบาทหน้าที่ความรับผิดชอบ โดยต้องประสานงานกับคณะกรรมการองค์การ เช่น การควบคุมสินทรัพย์สำคัญ ข้อมูลที่สำคัญ กระบวนการปฏิบัติงานที่สำคัญ รวมทั้งการควบคุมที่สร้างความเชื่อถือและการปฏิบัติงานที่ต่อเนื่อง

- การควบคุมระดับเทคนิคการปฏิบัติงาน (Technical Controls) หมายถึง การควบคุมในระดับรายละเอียด เพื่อสร้างความเชื่อถือได้ของการควบคุมที่ไม่ได้อยู่ในความรับผิดชอบของระดับสูง การควบคุมในระดับนี้จะเชื่อถือได้มากขึ้น หากเป็นการควบคุมด้วยเทคโนโลยี การควบคุมแบบอัตโนมัติ รวมทั้งการมีร่องรอยการตรวจสอบและหลักฐานที่พิสูจน์ได้

ทั้งนี้ องค์การควรมีการกำหนดระบบการควบคุมขั้นพื้นฐาน (Baseline Controls) สำคัญ ซึ่งต้องได้รับการจัดการให้มั่นใจในประสิทธิภาพและประสิทธิผลของการควบคุมดังกล่าวตลอดเวลา และกำหนดการควบคุมตามระดับความเสี่ยงที่เปลี่ยนแปลงไป เมื่อองค์การประเมินความเสี่ยง ซึ่งต้องปฏิบัติอย่างสม่ำเสมอ หากผลการประเมินพบความเสี่ยงเรื่องใดที่สูงผิดปกติ ผู้บริหารต้องใช้วิธีการตอบสนองความเสี่ยงตามวิธีการหรือแผนที่กำหนด เพื่อที่จะลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้อย่างทันกาล และเพียงพอที่ให้การปฏิบัติงานโดยรวมเป็นไปตามวัตถุประสงค์ที่กำหนด

6. การติดตามและประเมินผลการควบคุม

การติดตามประเมินผล เพื่อให้มั่นใจในการนำการควบคุมไปใช้ให้เกิดประสิทธิภาพ ประสิทธิผล และมีการปรับปรุงให้ทันสมัยอยู่เสมอ ซึ่งผู้บริหารมีหน้าที่รับผิดชอบในการติดตามผลระหว่างการปฏิบัติงาน ในขณะที่ผู้ตรวจสอบอิสระมีหน้าที่ในการประเมินผลอย่างเป็นอิสระและเป็นครั้งคราว ซึ่งการติดตามประเมินผลการควบคุมด้านเทคโนโลยีสารสนเทศเป็นกระบวนการที่ต้องจัดทำอย่างต่อเนื่อง เพื่อให้ทันต่อการเปลี่ยนแปลงของสภาพแวดล้อมและปัจจัยภายนอกที่เกิดขึ้นตลอดเวลา

การพิจารณาเพื่อให้เกิดความมั่นใจในการนำการควบคุมไปใช้ให้เกิดประสิทธิภาพและประสิทธิผลนั้น Cobit Framework ได้กำหนดระดับความสามารถของการควบคุมหรือระดับพัฒนาการของการควบคุม (Internal Control Capability Continuum) ได้เป็น 5 ระดับโดยควรใกล้เคียงกับระดับความเสี่ยงในเรื่องนั้น เช่น เรื่องใดมีความเสี่ยงระดับ 5 ก็ควรมีการควบคุมระดับ 5 ไม่ควรมีช่องว่างของการควบคุม (Control Gap) มาก เป็นต้น สรุปได้ดังตารางที่ 4.1

ตารางที่ 4.1 ระดับความสามารถของการควบคุมหรือระดับพัฒนาการของการควบคุม (Internal Control Capability Continuum)

ระดับความสามารถ	คำอธิบาย (Description)	ลักษณะ (Attributes)
1. เริ่มต้น (Initial State)	- กิจการยังไม่ให้ความสำคัญกับการควบคุม ทำบ้างไม่ทำบ้าง - จะทำเมื่อเกิดปัญหาแบบเชิงรับ - ทำเป็นบางส่วน - เป็นครั้งคราวเฉพาะกิจ	- ขึ้นอยู่กับความริเริ่มของบุคคลใดบุคคลหนึ่ง - ทำเฉพาะกิจ - ไม่มีการกำหนดนโยบายเป็นลายลักษณ์อักษร - มีการระบุกระบวนการและวิธีการเล็กน้อย
2. ทำซ้ำ ทำเป็นประจำ (Repeatable)	- การควบคุมขึ้นอยู่กับคุณภาพของผู้รับผิดชอบ - ทำซ้ำ ทำเป็นประจำ เคยทำอย่างไรก็ทำอย่างนั้น - ใช้ดุลยพินิจ ลางสังหรณ์	- มีนโยบาย กรอบงาน วิธีการควบคุมขั้นพื้นฐาน - มีความตระหนักและเข้าใจมากขึ้น - ใช้กระบวนการและวิธีการควบคุมตามเดิม ซ้ำ ๆ - บางวิธีการไม่มีเป็นลายลักษณ์อักษร - ขาดการสื่อสาร - ระดับการติดตามประเมินผลและการปรับปรุงน้อย
3. มีหลักฐานเอกสารเป็นมาตรฐานและสื่อสารให้ทุกคนทราบแล้ว	- การจัดทำนโยบาย วิธีการควบคุมเป็นลายลักษณ์อักษรและได้มาตรฐานทั้งองค์การ - มีผู้รับผิดชอบประจำตามหน้าที่ - มีวิธีจัดการเชิงปริมาณและเชิงคุณภาพหรือการใช้ดุลยพินิจ	- มีรูปแบบการควบคุมที่เป็นมาตรฐาน (Uniform) ทั้งองค์การ - มีผังภาพการควบคุมภายในกระบวนการและรายการค้าสำคัญ - สามารถระบุแหล่งที่เกิดความเสี่ยงและจุดที่มีการละเลยการควบคุมที่สำคัญ

ตารางที่ 4.1 (ต่อ)

ระดับความสามารถ	คำอธิบาย (Description)	ลักษณะ (Attributes)
(Defined)		- มีการจัดการและการควบคุมกับความเสี่ยงที่เกิดขึ้นจริง แต่ยังไม่ครอบคลุมทุกความเสี่ยง - ความเสี่ยงบางอย่างต้องให้ฝ่ายบริหารตัดสินใจ หรือขึ้นอยู่กับดุลยพินิจของฝ่ายบริหาร - เจ้าของระบบงานยังไม่มีการประเมินผลตนเอง - แผนการตรวจสอบภายในยังไม่เชื่อมโยง หรือไม่มีการประเมินผลโดยผู้ตรวจสอบภายในอิสระ
4. มีการบริหาร (Managed)	- การจัดการบริหารความเสี่ยงเชิงปริมาณและทั่วทั้งองค์การ และมีการติดตามประเมินผลและปรับปรุงอย่างเป็นระบบ - การบริหารความเสี่ยงมีแนวคิดและการวิเคราะห์โดยวิธีการเชิงปริมาณที่ลึกซึ้งในระดับองค์การ	- มีกระบวนการบริหารจัดการความเสี่ยงและการควบคุมอย่างจริงจังและเป็นมาตรฐานทั่วทั้งองค์การ - ใช้การควบคุมแบบอัตโนมัติมากกว่าการพึ่งพิงการควบคุมด้วยคน - มีระบบการติดตามผล การกำหนดตัววัดเป้าหมายความสำเร็จที่ชัดเจน และมีรายงานการติดตามผลความคลาดเคลื่อนเป็นประจำอย่างน้อยทุกไตรมาส - แผนงานการตรวจสอบภายในเชื่อมโยงสอดคล้องกับผลการประเมินความเสี่ยง และมีการรายงานการประเมินผลโดยผู้ตรวจสอบภายในอิสระตามแผนงาน

ตารางที่ 4.1 (ต่อ)

ระดับความสามารถ	คำอธิบาย (Description)	ลักษณะ (Attributes)
		เป็นประจำ - การประเมินผลตนเองได้ส่งผลการประเมินให้ฝ่ายบริหารหรือคณะ - กรรมการองค์การ - มีการติดตามประเมินผลและการปรับปรุง ในระดับระบบงานที่สำคัญ
5. การเกิดผลประโยชน์สูงสุด (Optimizing)	-ใช้วิธีการที่ดีที่สุด (Best Practices) และมีการแชร์ความรู้ระหว่างกันทั้งองค์การ - ใช้กระบวนการจัดทำงบการเงินและกรอบงานการควบคุมระดับสากล - มีความพยายามที่จะลดการขาดประสิทธิภาพในระดับกิจการ - มีการติดตามผลของปัจจัยภายนอกและภายในในกรอบงานการควบคุม - เห็นความสำเร็จในด้านความมีประสิทธิภาพและได้รับประโยชน์อย่างคุ้มค่ามากที่สุด	- มีกระบวนการปรับปรุงตลอดเวลาอย่างต่อเนื่องทันต่อการเปลี่ยนแปลงทั้งจากปัจจัยภายนอกและภายใน และเกิดประสิทธิภาพประสิทธิผลทั่วทั้งองค์การ - มีระบบการติดตามผลระดับองค์การที่ใช้ในการปฏิบัติจริง สามารถให้รายงานหรือสัญญาณเตือนภัยในเวลาเกิดจริง (Real Time Reporting) - มีการประเมินผลตนเองอย่างต่อเนื่องและมีการปรับปรุงกระบวนการทำงานทุกหน่วยงาน - เจ้าของระบบงานใช้เทคโนโลยีในการจัดเก็บเอกสารหลักฐาน รายงาน วิธีการวิเคราะห์ ที่สามารถเข้าถึงและพร้อมใช้งาน - กิจการสามารถบรรลุผลเป้าหมายด้านความโปร่งใสในการรายงานทั้งภายนอกและภายใน

4.2 แนวการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT

ผู้ตรวจสอบมีหน้าที่ในการติดตามประเมินผลการควบคุมทางด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจในการนำการควบคุมไปใช้ให้เกิดประสิทธิภาพประสิทธิผล ผู้ตรวจสอบจึงต้องการวางแผนงานตรวจสอบในรายละเอียด เช่น การกำหนดโปรแกรมการตรวจสอบและเทคนิควิธีการตรวจสอบ โดยการกำหนดประเด็นการตรวจสอบ และจัดทำแนวการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งจะได้พิจารณาจัดทำแนวการตรวจสอบการแนวทางของ COBIT โดยจะแบ่งการตรวจสอบตามโครงสร้างของมาตรฐาน COBIT บนพื้นฐานของกระบวนการทางธุรกิจ Business Process สามารถแบ่งได้เป็น 4 กระบวนการหลัก (Domain) ได้แก่ การวางแผนและการจัดการองค์กร (PO : Planning and Organization) การจัดหาและการนำระบบออกใช้งานจริง (AI : Acquisition and Implementation) การส่งมอบและการสนับสนุน (DS : Delivery and Support) การติดตามผล (M : Monitoring)

4.2.1 การวางแผนและการจัดองค์กร (PO : Planning and Organization)

วัตถุประสงค์ของการตรวจสอบ : เพื่อให้มั่นใจว่า

1. องค์กรได้รับประโยชน์สูงสุดจากการใช้เทคโนโลยีสารสนเทศ การจัดรูปแบบระบบสารสนเทศ สามารถใช้เทคโนโลยีสมัยใหม่เป็นกลยุทธ์ในการบริหารธุรกิจ
2. การให้บริการด้านเทคโนโลยีสารสนเทศเป็นไปอย่างถูกต้องและเหมาะสม
3. เงินลงทุนในเทคโนโลยีสารสนเทศมีการประมาณการอย่างเหมาะสม และมีการควบคุมดูแลการใช้จ่ายเงินลงทุนนั้น
4. มีการสื่อสารให้คนในองค์กรรับรู้และเข้าใจในเป้าหมายและทิศทางขององค์กร บุคลากรมีความสามารถ และทุ่มเทในการทำงาน
5. มีการปฏิบัติงานที่สอดคล้องถูกต้องตามกฎหมาย ระเบียบ และสัญญา
6. มีการบริหารความเสี่ยงอย่างเหมาะสม
7. การจัดการโครงการสามารถดำเนินการให้แล้วเสร็จภายในระยะเวลาและงบประมาณที่กำหนดไว้

ตารางที่ 4.2 ถึง ตารางที่ 4.12 แสดงแนวการตรวจสอบการวางแผนและการจัดองค์กร (PO : Planning and Organization)

ตารางที่ 4.2 PO1 : การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (Define a Strategic IT Plan)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. การใช้เทคโนโลยีขององค์กร ไม่สามารถตอบสนองวัตถุประสงค์และกลยุทธ์ทางธุรกิจขององค์กร 2. แผนงานระยะสั้นและระยะยาว ไม่สามารถสนับสนุนให้บรรลุวัตถุประสงค์และเป้าหมายขององค์กร 3. ผู้เกี่ยวข้องไม่เข้าใจ ทำให้ไม่ได้รับความร่วมมือจากผู้เกี่ยวข้อง 4. การปรับเปลี่ยนแผนระยะสั้นและระยะยาวด้านเทคโนโลยีสารสนเทศไม่ทันกับการเปลี่ยนแปลงที่เกิดขึ้น	1. เทคโนโลยีสารสนเทศ เป็นส่วนหนึ่งของแผนงานระยะสั้นและระยะยาวขององค์กร 2. มีการใช้โครงสร้างของกระบวนการวางแผนที่ทำให้แผนที่จัดทำขึ้นมีคุณภาพ คำนึงถึงผลการประเมินความเสี่ยง และมีการประเมินเป็นระยะ ๆ ตามที่กำหนด 3. มีกระบวนการจัดการในสื่อสื่อสารแผนระยะสั้นและแผนระยะยาวให้แก่พนักงานหรือผู้ที่มีความเกี่ยวข้องในองค์กร 4. กำหนดให้มีกระบวนการจัดการสำหรับการตรวจสอบและรายงานผลสะท้อนกลับจากพนักงานหรือผู้ใช้งานในด้านของคุณภาพและประโยชน์ของแผนระยะสั้นและแผนระยะยาว 5. กำหนดให้ผู้บริหารเทคโน - โลยีสารสนเทศ มีการประเมินระบบสารสนเทศที่ใช้อยู่ในปัจจุบันก่อนที่จะมีการพัฒนาหรือเปลี่ยนกลยุทธ์สำหรับแผนระยะสั้น	1. สอบทานว่าองค์กรมีการจัดทำแผนระยะสั้นหรือระยะยาวหรือไม่ 2. สอบทานกระบวนการวางแผนระยะยาวและระยะสั้นขององค์การ และพิจารณาว่าผู้บริหารระดับสูงได้เข้ามามีส่วนเกี่ยวข้องในการวางแผนหรือไม่ 3. สอบทานว่ามีการกำหนดเทคโนโลยีสารสนเทศเป็นส่วนหนึ่งของแผนระยะสั้นและระยะยาวหรือไม่ 4. สอบทานว่าองค์กรมีการจัดทำแผนระยะสั้นและระยะยาวด้านเทคโนโลยีสารสนเทศหรือไม่ 5. สอบทานว่ามีการสื่อสารแผนงานด้านเทคโนโลยีให้พนักงานในองค์กรได้รับทราบหรือไม่ 6. สอบทานว่ามีการติดตามและรายงานผลการปฏิบัติตามแผนระยะสั้นและแผนระยะยาวหรือไม่

ตารางที่ 4.2 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
		7. สอบทานว่าแผนระยะสั้นของส่วนงานเทคโนโลยีสารสนเทศสอดคล้องกับแผนงานระยะยาวหรือไม่ 8. สอบถามหน่วยงานสำคัญอื่นๆ ที่เกี่ยวข้อง เพื่อให้มั่นใจว่ากลยุทธ์ของหน่วยงานอื่นและหน่วยงานเทคโนโลยีสารสนเทศมีความสอดคล้องในแนวทางเดียวกันหรือไม่ 9. สอบทานการจัดสรรทรัพยากรที่จำเป็นต้องใช้ตามแผนระยะสั้นและระยะยาวมีความเหมาะสมหรือไม่

ตารางที่ 4.3 PO2 : การกำหนดโครงสร้างด้านสารสนเทศ (Define the Information Architecture)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. โครงสร้างของระบบเทคโนโลยีสารสนเทศไม่เหมาะสมกับโครงสร้างของธุรกิจ 2. ผู้ไม่มีสิทธิเข้าถึงสารสนเทศโดยไม่ได้รับ	1. มีการกำหนดสถาปัตยกรรมของระบบด้านการออกแบบและพัฒนาระบบงาน 2. มีการกำหนดรูปแบบและกฎเกณฑ์ของการพัฒนาพจนานุกรมข้อมูล	1. สอบทานว่ามีการกำหนดสถาปัตยกรรมของการออกแบบและพัฒนาระบบงานหรือไม่ อย่างไร 2. สอบทานว่ามีการรักษาความปลอดภัยของข้อมูลหรือไม่

ตารางที่ 4.3 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
อนุญาต	3. มีการจัดทำรูปแบบการจัดกลุ่มข้อมูล 4. มีการจัดระดับความปลอดภัยของข้อมูล	อย่างไร 3. สอบทานว่ามีการกำหนดรูปแบบและกฎเกณฑ์ในการพัฒนาพจนานุกรมข้อมูลและการจัดกลุ่มข้อมูลหรือไม่อย่างไร 4. สอบทานว่าองค์กรมีการกำหนดกรอบงานการจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยีสนเทศ

ตารางที่ 4.4 PO3 : การกำหนดทิศทางด้านเทคโนโลยี (Determine Technological Direction)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- ไม่สามารถใช้เทคโนโลยีสมัยใหม่เป็นเครื่องมือในการบริหารธุรกิจ ซึ่งอาจทำให้ไม่สามารถแข่งขันทางธุรกิจกับคู่แข่งในตลาด	1. มีการวางแผนโครงสร้างทางด้านเทคโนโลยีที่ทันสมัยอย่างสม่ำเสมอทั้งในแผนระยะสั้นและแผนระยะยาว 2. มีการวางแผนพัฒนาและบำรุงรักษาโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ 3. มีการวางแผนการจัดหาฮาร์ดแวร์และซอฟต์แวร์ 4. มีการกำหนดเทคโนโลยีที่เป็นบรรทัดฐานเพื่อที่จะ	1. สอบทานว่าองค์กรมีการวางแผนโครงสร้างทางเทคโนโลยีสารสนเทศ มีการกำหนดทิศทางของเทคโนโลยีสารสนเทศหรือไม่ และมีการวางแผนในการจัดหาฮาร์ดแวร์และซอฟต์แวร์หรือไม่ อย่างไร สอดคล้องกับแผนระยะสั้นและระยะยาวด้านเทคโนโลยีสารสนเทศหรือไม่ อย่างไร 2. สอบทานว่าองค์กรมีการ

ตารางที่ 4.4 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	สนับสนุนความมีมาตรฐานเดียวกัน	วางแผนพัฒนาและบำรุงรักษาโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศหรือไม่

ตารางที่ 4.5 PO4 : การจัดโครงสร้างองค์กรด้านเทคโนโลยีสารสนเทศและความสัมพันธ์กับหน่วยงานอื่น (Define the IT Organization and Relationships)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. ไม่สามารถให้บริการทางด้านเทคโนโลยีสาร – สนเทศได้อย่างถูกต้องเหมาะสม 2. หากพนักงานไม่ทราบถึงหน้าที่ความรับผิดชอบของตนเอง ทำให้การทำงานเกิดความซ้ำซ้อนและขาดการควบคุมได้	1. มีการจัดโครงสร้างองค์กรของหน่วยงานเทคโนโลยีสาร - สนเทศ โดยมีการกำหนดสิทธิ บทบาท หน้าที่และความรับผิดชอบ และการแบ่งแยกหน้าที่ความรับผิดชอบที่เหมาะสม 2. มีการจัดทำคู่มือวิธีปฏิบัติงานสำหรับหน้าที่งานต่าง ๆ อย่างชัดเจนและเหมาะสม	1. ตรวจสอบจากโครงสร้างการจัดองค์กรโดยรวมและพิจารณาการจัดแบ่งส่วนงานภายใต้ส่วนงานเทคโนโลยีสารสนเทศ 2. สอบทานคู่มือการปฏิบัติงาน คำบรรยายลักษณะงานของส่วนงานเทคโนโลยีสารสนเทศ 3. สังเกตการณ์การปฏิบัติงานจริงของพนักงานในส่วนงานเทคโนโลยีสารสนเทศ 4. สัมภาษณ์บุคลากรในส่วนงานเทคโนโลยีสารสนเทศในเรื่องต่าง ๆ ที่เกี่ยวข้อง

ตารางที่ 4.6 PO5 : การจัดการด้านการลงทุนในเทคโนโลยีสารสนเทศ (Manage the IT Investment)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. การลงทุนในเทคโนโลยีสารสนเทศได้ผลตอบแทนไม่คุ้มค่า 2. กระบวนการใช้จ่ายเงินที่ไม่เหมาะสม ขาดการควบคุม อาจเกิดทุจริตในการใช้จ่ายเงินขึ้นได้	1. มีการกำหนดงบประมาณด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องกับแผนระยะสั้นและระยะยาวขององค์กรและสอดคล้องกับแผนระยะสั้นและระยะยาวด้านเทคโนโลยีสารสนเทศ 2. มีกระบวนการในการติดตามดูแลค่าใช้จ่ายและผลประโยชน์ที่ได้รับ โดยเปรียบเทียบกับงบประมาณ 3. มีกระบวนการในการวิเคราะห์ความถูกต้องและผลกำไรของการดำเนินงานด้านเทคโนโลยีสารสนเทศ	1. สอบทานว่าองค์กรมีการจัดงบประมาณด้านเทคโนโลยีสารสนเทศหรือไม่ อย่างไร 2. สอบทานว่ามีการติดตามดูแลค่าใช้จ่ายด้านเทคโนโลยีสารสนเทศอย่างไร การอนุมัติค่าใช้จ่ายเป็นไปตามอำนาจดำเนินการหรือไม่ อย่างไร 3. สอบทานว่าการบันทึกการใช้จ่ายว่ามีการบันทึกครบถ้วนถูกต้องหรือไม่ 4. สอบทานกระบวนการวิเคราะห์ผลดำเนินงานด้านเทคโนโลยีสารสนเทศ

ตารางที่ 4.7 PO6 : การสื่อสารเป้าหมายและทิศทางภายในองค์กร (Communicate Management Aims and Direction)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- พนักงานไม่ทราบเป้า-หมายและทิศทางขององค์กร อาจทำให้ขาดความตระหนักในเรื่องความเสี่ยงทั้งด้านธุรกิจและดเทคโนโลยีสารสนเทศ	- มีกระบวนการในการสื่อสารให้ทุกคนในองค์กรทราบถึงภารกิจ วัตถุประสงค์ในการให้บริการ นโยบาย และขั้นตอนต่าง ๆ	- สอบทานว่าองค์กรมีกระบวนการหรือวิธีการในการสื่อสารเกี่ยวกับเป้าหายและทิศทางขององค์กรให้พนักงานทราบถึงไม่อย่างไร

ตารางที่ 4.8 PO7 : การจัดการทรัพยากรบุคคล (Manage Human Resources)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. บุคลากรไม่มีคุณสมบัติเหมาะสมกับหน้าที่ความรับผิดชอบ 2. จำนวนบุคลากรไม่เหมาะสมกับแผนระยะสั้นและระยะยาวด้านเทคโนโลยีสารสนเทศ	- มีการกำหนดแนวทางการปฏิบัติในเรื่องของการสรรหาบุคลากรใหม่ คุณสมบัติของบุคลากร การฝึกอบรม การประเมินผลงาน การโยกย้ายเลื่อนตำแหน่ง และการเลิกจ้างเป็นต้น	1. สอบทานว่ามีการจัดทำคำบรรยายลักษณะงาน หน้าที่ความรับผิดชอบ ตลอดจนคุณสมบัติของบุคลากรตำแหน่งต่าง ๆ ในส่วนงานเทคโนโลยีสารสนเทศหรือไม่ 2. สอบทานว่ามีกระบวนการหรือวิธีการจัดหาคนเข้าทำงาน การกำหนดวิธีการเพื่อความปลอดภัยด้านการพนักงานของส่วนงานเทคโนโลยีสารสนเทศหรือไม่

ตารางที่ 4.8 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
		3. สอบทานว่ามีการฝึกอบรมพนักงานของส่วนของเทคโนโลยีสารสนเทศหรือไม่ 4. สอบทานว่ามีการประเมินผลการปฏิบัติงานตามหน้าที่งานของพนักงาน โดยเปรียบเทียบกับมาตรฐานหรือแนวทางปฏิบัติที่ได้กำหนดไว้หรือไม่ 5. สัมภาษณ์บุคลากรในส่วนงานเทคโนโลยีสารสนเทศ

ตารางที่ 4.9 PO8 : การปฏิบัติตามข้อกำหนดขององค์กรภายนอก (Ensure Compliance with External Requirements)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- องค์กรมีการปฏิบัติงานที่ไม่สอดคล้องถูกต้องตามกฎหมาย ระเบียบ และสัญญา ซึ่งอาจมีผลทำให้ถูกปรับ ถูกฟ้องร้อง หรือเสื่อมเสียชื่อเสียงได้	1. มีการกำหนดวิธีการและระเบียบปฏิบัติ เพื่อให้เป็นไปตามข้อกำหนดขององค์กรภายนอก 2. มีการกำหนดผู้รับผิดชอบในการสอบทานข้อกำหนดขององค์กรภายนอก และสอบทานการปฏิบัติตามข้อกำหนดนั้น ๆ	1. สอบทานคู่มือปฏิบัติงานของหน่วยงานด้านเทคโนโลยีสารสนเทศว่ามีการกำหนดขั้นตอนการปฏิบัติงานที่ไม่เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ หรือสัญญา กับบุคคลภายนอกหรือองค์กรภายนอกหรือไม่ อย่างไร 2. สอบทานการปฏิบัติงานของ

ตารางที่ 4.9 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
		ผู้รับผิดชอบในการสอบทานข้อกำหนดหรือการปฏิบัติตามข้อกำหนดต่าง ๆ

ตารางที่ 4.10 PO9 : การประเมินความเสี่ยง (Assess Risks)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- การดำเนินธุรกิจไม่สามารถบรรลุวัตถุประ - สงค์และเป้าหมายขององค์กร	1. มีการกำหนดคู่มือการบริหารความเสี่ยง โดยมีการกำหนดขั้นตอนการประเมินความเสี่ยงตั้งแต่การระบุปัจจัยเสี่ยง การวิเคราะห์ความเสี่ยง และการบริหารความเสี่ยง 2. มีการดำเนินการตามขั้นตอนที่กำหนดคู่มือการบริหารความเสี่ยง	1. สอบทานคู่มือการบริหารความเสี่ยงว่ามีการกำหนดขั้นตอนอย่างเหมาะสมหรือ ไม่อย่างไร 2. สอบทานการปฏิบัติตามขั้นตอนการบริหารความเสี่ยงที่กำหนดไว้ในการประเมินความเสี่ยงเกี่ยวกับเทคโนโลยีสารสนเทศ เช่น การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง แผนปฏิบัติงานเพื่อจัดการความเสี่ยง ตลอดจนการสนับสนุนของผู้บริหารในการประเมินความเสี่ยง

ตารางที่ 4.11 PO10 : การจัดการโครงการ (Manage Projects)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- ไม่สามารถดำเนินการโครงการให้แล้วเสร็จภายในเวลาและงบประมาณที่กหนดไว้	- มีการกำหนดระเบียบวิธีการบริหารจัดการโครงการซึ่งครอบคลุมถึงการกำหนดทีมงานการจัดสรรความรับผิดชอบ งบประมาณและเวลาของโครงการ ทรัพยากรที่ใช้ แผนงานหลักของโครงการ แผนงานรับรองคุณภาพ การบริหารความเสี่ยงของโครงการ แผนการทดสอบ แผนการฝึกอบรม แผนการสอบทานระบบภายหลังการใช้งานจริง และขั้นตอนการอนุมัติโครงการ เป็นต้น	1. สอบทานว่าองค์กรมีการกำหนดระเบียบวิธีการบริหารจัดการโครงการหรือไม่อย่างไร เช่น มีการกำหนดแผนงานหลักของโครงการ มีการกำหนดงบประ-มาณ ระยะเวลา และทรัพยากรที่ใช้ในโครงการ เป็นต้น 2. สอบทานว่าองค์กรมีการกำหนดทีมงานของโครงการและหน้าที่ความรับผิดชอบของทีมงานหรือไม่อย่างไร หน่วยงานผู้ใช้ระบบงานมีส่วนร่วมในโครงการหรือไม่ 3. สอบทานว่ามีการอนุมัติโครงการโดยผู้บริหารหรือไม่ และผู้บริหารมีการพิจารณารายงานการศึกษาความเป็นไปได้ของโครงการ ประกอบการพิจารณาอนุมัติโครงการหรือไม่ 4. สอบทานความสมเหตุสมผลของการศึกษาความเป็นไปได้ของโครงการ 5. สอบทานว่าองค์กรมีการกำหนดแผนงานรับรองคุณภาพของโครงการหรือไม่

ตารางที่ 4.11 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
		6. สอบทานว่าองค์กรมีการกำหนดกระบวนการบริหารความเสี่ยงของโครงการหรือไม่ 7. สอบทานว่าองค์กรมีการกำหนดแผนการทดสอบแผนการฝึกอบรม และแผนการสอบทานระบบภายหลังการใช้งานจริงหรือไม่ อย่างไร

ตารางที่ 4.12 PO11 : การจัดการคุณภาพ (Manage Quality)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- เทคโนโลยีสารสนเทศไม่สามารถตอบสนองความต้องการของผู้ใช้งาน	1. มีการจัดการคุณภาพ พัฒนา ติดตั้ง และดูแลรักษา มีการกำหนดนโยบายและขั้นตอนการปฏิบัติงาน การกำหนดความต้องการด้านคุณภาพ การตรวจสอบติดตาม และการรายงานผลไปยังผู้ที่มีส่วนเกี่ยวข้อง 2. มีการกำหนดขั้นตอนการปฏิบัติงานเกี่ยวกับการพัฒนาระบบงาน เอกสารประกอบการพัฒนาระบบงาน	1. สอบทานว่าองค์กรมีการจัดทำแผนคุณภาพทางด้านเทคโนโลยีสารสนเทศหรือไม่ 2. สอบทานว่าองค์กรมีการจัดทำแผนการรับรองคุณภาพของระบบเทคโนโลยีสารสนเทศหรือไม่ 3. สอบทานว่าองค์กรมีการกำหนดนโยบายและขั้นตอนการปฏิบัติงานในการจัดการคุณภาพหรือไม่ 4. สอบทานว่ามีการปฏิบัติตาม

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
		นโยบายหรือขั้นตอนการปฏิบัติงานที่กำหนดไว้หรือไม่ 5. สอบทานว่าการพัฒนาระบบเทคโนโลยีสารสนเทศในแต่ละขั้นตอนว่าเป็นไปตามกรรมวิธีวงจรการพัฒนาระบบงานหรือไม่ รวมทั้งมีการปรับปรุงกรรมวิธีวงจรการพัฒนาระบบงานหรือไม่ 6. สอบทานว่ามีการจัดทำแผนการทดสอบระบบงานหรือไม่ และพิจารณาความครบถ้วนของแผนการทดสอบระบบงานและการปฏิบัติการ 7. สอบทานว่ามีการทดสอบการทดสอบระบบงานตามแผนการทดสอบระบบงานหรือไม่ 8. สอบทานว่ามีกระบวนการในการประสานงานและติดต่อสื่อสารระหว่างบุคลากรที่เกี่ยวข้องหรือไม่ 9. สอบทานว่าองค์กรมีการกำหนดกรอบงานการจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ

ตารางที่ 4.12 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
		หรือไม่ 10. สอบทานว่าองค์กรมีการกำหนดมาตรฐานของเอกสารโปรแกรม มาตรฐานการทดสอบโปรแกรมและระบบงานหรือไม่อย่างไร 11. สอบทานว่าองค์กรมีการประเมินเพื่อรับรองคุณภาพโดยเทียบกับมาตรฐานการพัฒนาหรือไม่ 12. สอบทานว่ามีการรายงานการสอบทานการรับรองคุณภาพและรายงานดังกล่าวมีเนื้อหาที่เหมาะสมเพียงพอหรือไม่

4.2.2 การจัดหาและการนำระบบออกใช้งานจริง (AI : Acquisition and Implementation)

วัตถุประสงค์ของการตรวจสอบ : เพื่อให้มั่นใจว่า

1. การตอบสนองของความต้องการข้อมูลของผู้ใช้เป็นไปอย่างมีประสิทธิผลและประสิทธิภาพ

2.การประมวลผลสามารถสนับสนุนการดำเนินและการปฏิบัติงานขององค์กรได้

3.องค์กรมีโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศที่เหมาะสมกับระบบงาน

4.ระบบงานถูกต้องตรงตามวัตถุประสงค์ที่ต้อง การใช้ระบบงานเป็นไปอย่างถูกต้องและเป็นระเบียบ

ตารางที่ 4.13 ถึง ตารางที่ 4.18 แสดงแนวการตรวจสอบการจัดหาและการนำระบบออกใช้งานจริง (AI : Acquisition and Implementation)

ตารางที่ 4.13 AI1 : การเลือกเทคโนโลยีมาใช้ในการปฏิบัติงาน (Identify Automated Solutions)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. เทคโนโลยีสารสนเทศไม่สามารถตอบสนองความต้องการของผู้ใช้งาน 2. ต้นทุนการจัดหาเทคโนโลยีสารสนเทศสูงเกินกว่าความจำเป็น	1. มีการกำหนดระเบียบวิธีปฏิบัติเกี่ยวกับการจัดหาเทคโนโลยีสานสนเทศ ตั้งแต่ขั้นตอนการกำหนดความต้องการ การพิจารณาทางเลือกของแหล่งที่มาหรือผู้จัดจำหน่าย การพิจารณาความเป็นไปได้ในด้าน เทคโนโลยีและด้านธุรกิจ การวิเคราะห์ความเสี่ยง การวิเคราะห์ต้นทุนและผลประโยชน์ที่จะได้รับ เป็นต้น 2. มีระเบียบปฏิบัติเกี่ยวกับขั้นตอนการจัดซื้อ 3. กรณีการว่าจ้างบุคคลภายนอกมีการจัดทำสัญญาเป็นลายลักษณ์อักษร และมีการกำหนดเงื่อนไขในสัญญาอย่างครบถ้วนถูกต้อง มีผลบังคับทางกฎหมาย	1. สอบทานว่าองค์กรมีการกำหนดระเบียบวิธีปฏิบัติเกี่ยวกับการจัดหาเทคโนโลยีสารสนเทศ เช่น มีการกำหนดความต้องการด้านเทคโนโลยีสารสนเทศ การพิจารณาทางเลือกของแหล่งที่มีหรือผู้จัดจำหน่าย รูปแบบกลยุทธ์การจัดหา การกำหนดระดับการบริการจากบุคคลภายนอก การศึกษาความเป็นไปได้ของเทคโนโลยี การศึกษาความคุ้มค่าในการลงทุน เป็นต้น 2. สอบทานว่าองค์กรมีการกำหนดระเบียบปฏิบัติเกี่ยวกับการจัดซื้อ หรือการคัดเลือกซอฟต์แวร์มาใช้งานหรือไม่ และมีการปฏิบัติตามหลักเกณฑ์ที่

ตารางที่ 4.13 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
		ระเบียบได้กำหนดไว้หรือไม่ อย่างไร 3. สอบทานว่าการว่าจ้างบุคคลภายนอกมีการจัดทำสัญญาเป็นลายลักษณ์อักษณ์ ข้อกำหนดเงื่อนไขครบถ้วนสมบูรณ์หรือไม่ อย่างไร 4. สอบทานว่าองค์กรมีการกำหนดข้อตกลงกับบริษัทคู่ค้าเกี่ยวกับกระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศหรือไม่ อย่างไร

ตารางที่ 4.14 AI2 : การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์ (Acquire and Maintain Application Software)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. ระบบงานไม่ถูกต้องเหมาะสม ทำให้การดำเนินงานขององค์กรไม่มีประสิทธิภาพและประสิทธิผล 2. เสียค่าใช้จ่ายและเวลาในการแก้ไขโปรแกรม	1. มีขั้นตอนวิธีปฏิบัติเกี่ยวกับการจัดหาและดูแลระบบงานประยุกต์ที่องค์กรนำมาใช้ ตั้งแต่การออกแบบระบบงาน การอนุมัติการออกแบบ การกำหนดความต้องการเกี่ยวกับแฟ้มข้อมูล ข้อกำหนดของโปรแกรม	1. สอบทานว่าองค์กรมีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการจัดหาและดูแลระบบงานประยุกต์ที่องค์กรนำมาใช้ตั้งแต่การออกแบบระบบงาน การอนุมัติการออกแบบ การกำหนดความ

ตารางที่ 4.14 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
ภายหลัง 3. ระบบงานอาจเข้าถึงโดยผู้ที่ไม่มีสิทธิและไม่ได้รับอนุญาต	การกำหนดความต้องการเกี่ยวกับข้อมูลนำเข้า การประมวลผลและผลลัพธ์ การควบคุม การรักษาความปลอดภัยเข้าไปในระบบงานที่ จะพัฒนา การลงมือสร้างระบบ และการตั้งค่า configuration ให้เป็นไปตามมาตรฐานความปลอดภัย 2. มีข้อกำหนดเกี่ยวกับความครบถ้วนถูกต้องของเทคโนโลยีสารสนเทศในโปรแกรมระบบงานประยุกต์ 3. มีการทดสอบโปรแกรมระบบงานประยุกต์และมีการกำหนดมาตรฐานในการทดสอบ มีวิธีการทดสอบที่เหมาะสม ผู้ใช้ระบบงานมีส่วนร่วมในการทดสอบระบบงานหรือโปรแกรม 4. มีคู่มือผู้ใช้ระบบและคู่มือสนับสนุนการปฏิบัติงานที่มีความละเอียด ครบถ้วน สามารถนำมาใช้เป็นคู่มือในการปฏิบัติงานได้จริง	ต้องการเกี่ยวกับแฟ้มข้อมูล ข้อกำหนดของโปรแกรม การกำหนดความต้องการเกี่ยวกับข้อมูลนำเข้า การประมวลผลและผลลัพธ์ การควบคุม การรักษาความปลอดภัยเข้าไปในระบบงานที่จะพัฒนา ตลอดจนการตั้งค่า configuration ต่าง ๆ หรือไม่ และสอบทานว่ามีการปฏิบัติตามขั้นตอนวิธีปฏิบัติที่กำหนดไว้หรือไม่ 2. สอบทานว่าองค์กรมีข้อกำหนดเกี่ยวกับความครบถ้วนถูกต้องของโปรแกรมระบบงานประยุกต์หรือไม่ 3. สอบทานว่ามีการทดสอบโปรแกรมระบบงานประยุกต์ตามมาตรฐานการทดสอบ หรือมีวิธีการทดสอบที่เหมาะสมหรือไม่ ผู้ใช้ระบบงานมีส่วนร่วมในการทดสอบหรือไม่ 4. สอบทานคู่มือผู้ใช้ระบบและคู่มือสนับสนุนการปฏิบัติงานว่ามีความละเอียด ครบถ้วน เพียงพอหรือไม่

ตารางที่ 4.14 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
		5. สอบทานว่าเมื่อมีข้อขัดแย้งทางด้านเทคนิคหรือลอจิกเกิดขึ้นระหว่างการบำรุงรักษาหรือการพัฒนา การออกแบบจะถูกประเมินซ้ำอีกครั้งหนึ่ง

ตารางที่ 4.15 AI3 : การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี (Acquire and Maintain Technology Infrastructure)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- องค์กรมีโครงสร้างพื้นฐานทางด้านเทคโน - โลยีสารสนเทศที่ไม่เหมาะสมกับระบบงาน	- มีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการวางแผนในการจัดหา การติดตั้ง การดูแลรักษาและการป้องกันในส่วนของโครงของโครงสร้างพื้นฐานเพื่อให้เป็นไปตามกลยุทธ์ด้านเทคโนโลยีที่องค์กรได้กำหนดไว้	1. สอบทานว่ามีการกำหนดขั้นตอน วิธีปฏิบัติเกี่ยวกับโครงสร้างพื้นฐานทางด้านเทคโนโลยีหรือไม่ ดังนี้ 1.1 การวางแผนในการจัดหา 1.2 การดูแลรักษาและการป้องกันในส่วนของโครงของโครงสร้างพื้นฐาน 1.3 สอบทานว่ามีการปฏิบัติตามขั้นตอนที่กำหนดไว้หรือไม่ 2. สอบทานในเรื่องต่าง ๆ ดังนี้ 2.1 มีการประเมินความต้องด้านฮาร์ดแวร์และซอฟต์แวร์ 2.2 การบำรุงรักษาฮาร์ดแวร์มี

ตารางที่ 4.15 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
		แผนกำหนดไว้ล่วงหน้า 2.3 มีการรักษาความปลอดภัยของโปรแกรมระบบ 2.4 มีการกำหนดขั้นตอนในการติดตั้ง ดูแลบำรุงรักษา การควบคุมการเปลี่ยนแปลงแก้ไขโปรแกรมระบบ 2.5 มีการใช้และติดตามประเมินการใช้งานโปรแกรมอรรถประโยชน์หรือไม่ อย่างไร

ตารางที่ 4.16 AI4 : ระเบียบปฏิบัติในการพัฒนาและบำรุงรักษา (Develop and Maintain Procedures)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- ผู้ใช้งานไม่สามารถใช้งานระบบสารสนเทศและโครงสร้างพื้นฐานต่าง ๆ ได้อย่างถูกต้องเหมาะสม	1. มีการปฏิบัติตรงตามความต้องการและระดับการให้บริการในเวลาที่เหมะสม 2. มีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการเผยแพร่ความรู้ของระบบงานใหม่ให้กับพนักงานในองค์กรรับทราบ 3. มีการสร้างคู่มือในการปฏิบัติงานของผู้ใช้งาน คู่มือ	1. ทำการสอบทานว่ามีการปฏิบัติงานตรงตามความต้องการและระดับการให้ บริการในเวลาที่เหมาะสมหรือไม่ อย่างไร 2. สอบทานคู่มือการปฏิบัติงานของผู้ใช้งานและคู่มือการปฏิบัติการคอมพิวเตอร์ของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศว่ามีความละเอียด ครบถ้วน สมบูรณ์

ตารางที่ 4.16 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	ปฏิบัติงานด้านปฏิบัติการคอมพิวเตอร์ของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ 4. มีการฝึกอบรม เพื่อให้ผู้ใช้งานสามารถใช้งานระบบสารสนเทศและโครงสร้างพื้นฐานต่างๆ ได้อย่างถูกต้องและเหมาะสม	สามารถใช้เป็นคู่มือปฏิบัติงานได้อย่างแท้จริง 3. สอบทานว่ามีการฝึกอบรมผู้ใช้ระบบงานและมีเอกสารการฝึกอบรม สำหรับระบบงานที่พัฒนาหรือไม่ อย่างไร

ตารางที่ 4.17 AI5 : การติดตั้งและรับรองระบบ (Install and Accredit Systems)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- ระบบงานไม่ถูกต้องตรงตามวัตถุประสงค์ที่ต้องการ	1. มีการจัดทำคู่มือสำหรับการติดตั้งระบบ 2. มีการเตรียมแผนการติดตั้งระบบใหม่ 3. มีการเตรียมแผนในการผลักดันระบบที่พัฒนาออกใช้งานจริง 4. มีการฝึกอบรมการใช้งานระบบงานใหม่ 5. มีการกำหนดขั้นตอนการโอนย้ายระบบงานเดิมและข้อมูลไปยังระบบงานใหม่	1. สอบทานว่ามีการจัดทำคู่มือสำหรับการติดตั้งระบบหรือไม่ 2. สอบทานแผนการติดตั้งระบบงานใหม่ 3. สอบทานวิธีการวัดขีดความสามารถของโปรแกรม 4. สอบทานว่ามีแผนในการนำระบบออกใช้งานจริงหรือไม่ 5. สอบทานว่ามีการโอนย้ายระบบงานเดิมและข้อมูลไปยัง 6. สอบทานว่ามีการกำหนดแผนและกลยุทธ์ในการทดสอบ

ตารางที่ 4.17 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	6. มีการกำหนดแผนและกลยุทธ์ในการทดสอบ 7. มีการทดสอบด้านการรักษาความปลอดภัยและระดับความน่าเชื่อถือ 8. มีการทดสอบด้านการปฏิบัติงาน 9. มีการเตรียมความพร้อมก่อนใช้งานจริง 10. มีการประเมินความสอดคล้องกับความต้องการผู้ใช้งาน 11. มีการประเมินผลหลังจากนำระบบออกใช้งานจริง	หรือไม่ 7. สอบทานว่ามีการทดสอบโปรแกรมที่มีการเปลี่ยนแปลงหรือแก้ไขหรือไม่ 8. สอบทานว่าการทดสอบระบบว่ามีใช้การทดสอบแบบคู่ขนานหรือแบบนำร่องหรือไม่และมีการทดสอบครั้งสุดท้ายเพื่อตรวจรับระบบหรือไม่ 9. สอบทานว่ามีการทดสอบและรับรองความปลอดภัยของระบบหรือไม่ 10. สอบทานว่ามีการทดสอบการปฏิบัติงานของระบบหรือไม่ 11. สอบทานว่ามีการเตรียมความพร้อมก่อนใช้งานจริงหรือไม่ 12. สอบทานว่ามีการประเมินความสอดคล้องกับความต้องการของผู้ใช้งานหรือไม่ 13. สอบทานว่ามีการประเมินผลหลังจากนำระบบออกใช้งานจริงหรือไม่

ตารางที่ 4.18 AI6 : การจัดการการเปลี่ยนแปลง (Manage Changes)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. มีการแก้ไขเปลี่ยนแปลงโปรแกรม ระบบงาน ข้อมูลโดยผู้ไม่มีสิทธิ และไม่ได้รับอนุญาต 2. ข้อมูล ระบบงานเกิดความเสียหาย 3. การดำเนินธุรกิจเกิดความเสียหาย จากการทุจริตของผู้เกี่ยวข้อง	1. มีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับคำขอปรับปรุงแก้ไขระบบงาน และมีกระบวนการควบคุมการเปลี่ยนแปลงแก้ไข 2. มีการประเมินผลกระทบจากการเปลี่ยนแปลงความต้องการของผู้ใช้ระบบงาน 3. การแก้ไขเปลี่ยนแปลงระบบงาน ข้อมูล ต้องได้รับการอนุมัติ และมีการควบคุมการเปลี่ยนแปลงเวอร์ชันของซอฟต์แวร์ 4. การนำโปรแกรมระบบงานออกใช้งาน ต้องได้รับการอนุมัติ 5. มีการควบคุมการติดตั้งโปรแกรมให้มีความเหมาะสม	1. สอบทานว่ามีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการขอปรับปรุงแก้ไขระบบงานหรือไม่ และมีกระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขหรือไม่ 2. สอบทานว่ามีเอกสารบันทึกการเปลี่ยนแปลงความต้องการระบบของผู้ใช้งานหรือไม่ 3. สอบทานว่าการเปลี่ยนแปลงระบบงานหรือข้อมูลมีการขออนุมัติจากผู้มีอำนาจหรือไม่ 4. สอบทานว่าการนำโปรแกรมระบบงานออกใช้งาน ได้รับการอนุมัติจากผู้มีอำนาจหรือไม่ 5. สอบทานว่ามีการควบคุมการติดตั้งโปรแกรมให้มีความเหมาะสมหรือไม่ เช่น มีกระบวนการติดตั้งที่ถูกต้องทั้งเวลา และสถานที่

4.2.3 การส่งมอบและการสนับสนุน (DS : Delivery and Support)

วัตถุประสงค์ของการตรวจสอบ : เพื่อให้มั่นใจว่า

1. มีความเข้าใจที่ถูกต้องในระดับบริการที่ต้องการ

2. มีการกำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการอย่างชัดเจน และมีการดำเนินการที่ถูกต้อง ต่อเนื่อง

3. เทคโนโลยีสารสนเทศมีประสิทธิภาพและความสามารถในการให้บริการได้ตามที่กำหนด สามารถให้บริการได้อย่างต่อเนื่อง และกระทบต่อธุรกิจน้อยที่สุดหากมีเหตุการณ์ที่ทำให้หยุดชะงัก

4. มีการปกป้องข้อมูลจากการถูกใช้ เปิดเผย แก้ไข ทำลาย โดยไม่ได้รับอนุมัติ หรือป้องกันข้อมูลสูญหาย ข้อมูลมีความสมบูรณ์ ถูกต้อง และน่าเชื่อถือ

5. การกำหนดและจัดสรรต้นทุนเป็นไปอย่างถูกต้องและเหมาะสม

6. ผู้ใช้ระบบงานสามารถใช้ได้อย่างมีประสิทธิภาพ มีการให้ความช่วยเหลือและแก้ไขปัญหาแก่ผู้ใช้ระบบงานอย่างเหมาะสม มีการหาสาเหตุของปัญหาและป้องกันไม่ให้เกิดขึ้นซ้ำอีก

7. มีการควบคุมดูแลทรัพย์สินทางด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม และมีการควบคุมการเปลี่ยนแปลง

8. ทรัพยากรทางด้านเทคโนโลยีสารสนเทศ และบุคลากร มีความปลอดภัย

9. การปฏิบัติการด้านเทคโนโลยีสารสนเทศมีการดำเนินงานอย่างสม่ำเสมอและเป็นลำดับอย่างถูกต้อง

ตารางที่ 4.19 ถึง ตารางที่ 4.31 แสดงแนวการตรวจสอบการส่งมอบและการสนับสนุน (DS : Delivery and Support)

ตารางที่ 4.19 DS1 : การกำหนดและการจัดการระดับการให้บริการ (Define and Manage Service Levels)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- เกิดการเข้าใจที่คลาดเคลื่อนของระดับบริการที่เป็นที่ต้องการ	1. มีการกำหนดกรอบข้อตกลงและหลักเกณฑ์ข้อตกลงของระดับการให้บริการ โดยจัดทำเป็นเอกสารลายลักษณ์อักษรและชัดเจน 2. มีการกำหนดวิธีปฏิบัติเกี่ยวกับการให้บริการ เพื่อให้เกิดประสิทธิภาพ 3. มีกระบวนการในการติดตามและการรายงานความก้าวหน้าของการให้บริการ 4. มีการทบทวนข้อตกลงและสัญญาเกี่ยวกับระดับการให้บริการ 5. มีการกำหนดแผนการปรับปรุงการให้บริการ 6. มีการกำหนดรายการที่คิดค่าบริการอย่างชัดเจน	1. สอบทานว่ามีการกำหนดกรอบและหลักเกณฑ์ข้อตกลงของระดับการให้บริการ โดยจัดทำเป็นเอกสารลายลักษณ์อักษรซึ่งมีความสมบูรณ์และชัดเจนหรือไม่ และข้อตกลงดังกล่าวครอบคลุมถึงความน่าเชื่อถือและความมีประสิทธิภาพหรือไม่ 2. สอบทานว่ามีการกำหนดวิธีปฏิบัติเกี่ยวกับการให้บริการหรือไม่ 3. สอบทานว่ามีกระบวนการในการติดตามและการรายงานความก้าวหน้าของการให้บริการหรือไม่ 4. สอบทานว่ามีการตรวจสอบหรือมีการทบทวนข้อตกลงและสัญญาเกี่ยวกับระดับการให้บริการหรือไม่ 5. สอบทานว่ามีการกำหนดแผนการปรับปรุงการให้บริการหรือไม่ 6. สอบทานว่ามีการกำหนด

ตารางที่ 4.19 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
		รายการที่คิดค่าบริการอย่างชัดเจนหรือไม่

ตารางที่ 4.20 DS2 : การจัดการการใช้บริการจากบุคคลภายนอก (Manage Third-Party Services)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- ได้รับบริการที่ไม่มีประสิทธิภาพ และไม่เป็นไปตามข้อตกลงที่ได้กำหนดไว้	1. มีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการใช้บริการจากบุคคลภายนอกและมีการกำหนดคุณสมบัติของผู้ให้บริการ 2. สัญญาการใช้บริการจากบุคคลภายนอกจะต้องมีความละเอียดชัดเจน ทั้งขอบเขตของการบริการ การกำหนดบทบาทหน้าที่ความรับผิดชอบของคู่สัญญา ความต่อเนื่องของการบริการ และมีการระบุข้อตกลงในด้านการรักษาความปลอดภัย 3. มีกระบวนการในการติดตามและการรายงานความก้าวหน้าของการให้บริการ	1. สอบทานการประสานงานกับผู้ให้บริการว่าเป็นอย่างไร มีความสัมพันธ์ที่ดีกับเจ้าของระบบหรือไม่ 2. สอบทานว่ามีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการใช้บริการจากบุคคลภายนอกและมีการกำหนดคุณสมบัติของผู้ให้บริการหรือไม่ และมีการมีปฏิบัติตามขั้นตอนวิธีปฏิบัติที่กำหนดไว้หรือไม่ 3. สอบทานว่าสัญญาการใช้บริการจากบุคคลภายนอก มีความละเอียดชัดเจน ทั้งขอบเขตของการบริการ การกำหนดบทบาทหน้าที่ความรับผิดชอบของคู่สัญญา ความต่อเนื่องของการบริการ และมีการระบุ

ตารางที่ 4.20 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
		ข้อตกลงในด้านการรักษาความปลอดภัยหรือไม่ 4. สอบทานกระบวนการในการติดตามและการรายงานความก้าวหน้าของการให้บริการ

ตารางที่ 4.21 DS3 : การจัดการด้านประสิทธิภาพและความสามารถ (Manage Performance and Capacity)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- ทรัพยากรด้านเทคโน-โลยีสารสนเทศไม่มีประสิทธิภาพ ส่งผลให้ไม่สามารถสนับสนุนความต้องการทางด้านธุรกิจได้อย่างต่อเนื่องตลอดเวลา ทำให้ขาดโอกาสในดำเนินธุรกิจ	1. มีการกำหนดความต้องการด้านความพร้อมสำหรับการใช้งานและประสิทธิภาพของการให้บริการสารสนเทศโดยพิจารณาจากความต้องการของธุรกิจ 2. มีการกำหนดแผนงานเกี่ยวกับสภาพความพร้อมใช้งานของเทคโนโลยีสารสนเทศ 3. มีการกำหนดกระบวนการในการติดตามและรายงานถึงประสิทธิภาพของทรัพยากรทางด้านเทคโนโลยีสารสนเทศ	1. สอบทานว่ามีการกำหนดความต้องการด้านความพร้อมสำหรับการใช้งานและประสิทธิภาพของการให้บริการสารสนเทศโดยพิจารณาจากความต้องการของธุรกิจหรือไม่ 2. สอบทานว่ามีการกำหนดแผนงานเกี่ยวกับสภาพความพร้อมใช้งานของเทคโนโลยีสารสนเทศหรือไม่ 3. สอบทานว่ามีการกำหนดกระบวนการในการติดตามและรายงานถึงประสิทธิภาพของ

ตารางที่ 4.21 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	4. มีการใช้เครื่องมือในการจำลองระบบ เพื่อช่วยในการคาดคะเนความสามารถ ความไว้วางใจ ประสิทธิภาพความต้องการความพร้อมใช้งานตลอดจนมีการพยากรณ์ทางด้านเทคโนโลยีในอนาคต 5. มีกระบวนการในการวางแผนสำหรับการทบทวนประสิทธิภาพของฮาร์แวร์และความสามารถของทรัพยากรด้านเทคโนโลยีสารสนเทศ และมีการป้องกันทรัพยากรจากการไม่สามารถพร้อมใช้งาน 6. มีแผนการจัดหาทรัพยากรด้านเทคโนโลยีสารสนเทศ	ทรัพยากรทางด้านเทคโนโลยีสารสนเทศหรือไม่ 4. สอบทานว่ามีการใช้เครื่องมือในการจำลองระบบ เพื่อช่วยในการคาดคะเนความสามารถ ความไว้วางใจ ประสิทธิภาพความต้องการความพร้อมใช้งานตลอดจนมีการพยากรณ์ทางด้านเทคโนโลยีในอนาคตหรือไม่ หรือมีการตรวจสอบปัญหาทางด้านฮาร์ดแวร์และซอฟต์แวร์ก่อนที่จะเกิดความเสียหายหรือไม่ 5. สอบทานว่ามีการกำหนดกระบวนการในการวางแผนสำหรับการทบทวนประสิทธิภาพของฮาร์แวร์และความสามารถของทรัพยากรด้านเทคโนโลยีสารสนเทศ และมีการป้องกันทรัพยากรจากการไม่สามารถพร้อมใช้งานหรือไม่ 6. สอบทานว่ามีการกำหนดแผนการจัดหาทรัพยากรด้านเทคโนโลยีสารสนเทศหรือไม่

ตารางที่ 4.22 DS4 : ความต่อเนื่องในการให้บริการ (Ensure Continuous Service)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- ธุรกิจเกิดการหยุดชะงัก ซึ่งทำให้สูญเสียลูกค้า รายได้ หากเกิดการหยุดชะงักเป็นเวลานานเกินไป อาจเกิดผลกระทบจนถึงขั้นต้องปิดกิจการ	1. มีการกำหนดกรอบงานความต่อเนื่องทางธุรกิจ ซึ่งมีการกำหนดบทบาท หน้าที่ ความรับผิดชอบ ระบียบวิธีพื้นฐานความเสี่ยง กฎและโครงสร้างการวางแผนต่อเนื่อง และกระบวนการในการอนุมัติ 2. มีการจัดแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และมีเนื้อหาเกี่ยวกับแนวทางฉุกเฉินเพื่อทำให้แน่ใจถึงความปลอดภัยของผู้ร่วมงาน มีกระบวนการกู้คืนระบบที่จะนำกลับสู่สภาวะเดิมก่อนที่จะเกิดเหตุการณ์หรือความเสียหายต่าง ๆ กระบวนการประสานงานกับผู้ที่มีอำนาจ กระบวนการสื่อสารกับผู้มีส่วนได้เสีย ลูกค้า ลูกจ้างและคู่ค้า 3. การจัดทำแผนการดำรงอยู่หรือแผนต่อเนื่องด้านเทคโนโลยีสารสนเทศ มีความครอบคลุมแผนต่อเนื่องทางด้านธุรกิจทั้งหมด เพื่อให้มีความสอดคล้อง และคำนึงถึงการวางแผน	1. สอบทานว่าองค์กรมีการกำหนดกรอบงานความต่อเนื่องทางธุรกิจ ซึ่งมีการกำหนดบทบาท หน้าที่ ความรับผิดชอบ ระบียบวิธีพื้นฐานความเสี่ยง กฎและโครงสร้างการวางแผนต่อเนื่อง และกระบวนการในการอนุมัติหรือไม่ 2. สอบทานว่าองค์กรมีการจัดแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และมีเนื้อหาเกี่ยวกับแนวทางฉุกเฉิน เพื่อทำให้แน่ใจถึงความปลอดภัยของผู้ร่วมงาน มีกระบวนการกู้คืนระบบที่จะนำกลับสู่สภาวะเดิมก่อนที่จะเกิดเหตุการณ์หรือความเสียหายต่างๆ กระบวน การประสานงานกับผู้ที่มีอำนาจ กระบวนการสื่อสารกับผู้มีส่วนได้เสีย ลูกค้า ลูกจ้างและคู่ค้า หรือไม่ 3. สอบทานว่าการจัดทำแผนการดำรงอยู่หรือแผนต่อเนื่องด้านเทคโนโลยีสารสนเทศ มีความครอบคลุมแผนต่อเนื่องทางด้าน

ตารางที่ 4.22 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	เทคโนโลยีสารสนเทศระยะสั้นและระยะยาว 4. มีการกำหนดความต้องการขั้นต่ำในเรื่องของบุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์แบบฟอร์ม ความสะดวกสบายคู่ค้าต่าง ๆ 5. มีการบำรุงรักษาแผนการดำรงอยู่ด้านเทคโนโลยีสาร-สนเทศให้มีความทันสมัยและสะท้อนความต้องการทางธุรกิจอย่างแท้จริง 6. มีการทดสอบแผนการดำรงอยู่ทางด้านเทคโนโลยีสารสน-เทศ ซึ่งผลการทดสอบสามารถนำมาใช้และปรับปรุงแผนให้มีความเหมาะสม 7. มีการฝึกอบรมเกี่ยวกับแผนการดำรงอยู่ทางด้านเทคโนโลยีสารสนเทศ 8. มีการเผยแพร่แผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศให้แก่บุคคลที่เกี่ยวข้อง 9. มีระเบียบการปฏิบัติงานสำรองที่เป็นทางเลือกในการ	ธุรกิจทั้งหมด เพื่อให้มีความสอดคล้อง และคำนึงถึงการวางแผนเทคโนโลยีสารสนเทศระยะสั้นและระยะยาวหรือไม่ 4. สอบทานว่าองค์กรมีการกำหนดความต้องการขั้นต่ำในเรื่องของบุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์ แบบฟอร์ม ความสะดวกสบาย คู่ค้าต่าง ๆ หรือไม่ 5. สอบทานว่ามีการบำรุงรักษาแผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศให้มีความทันสมัยและสะท้อนความต้องการทางธุรกิจอย่างแท้จริง หรือไม่ 6. สอบทานว่ามีการทดสอบแผนการดำรงอยู่ทางด้านเทคโนโลยีสารสนเทศ ซึ่งผลการทดสอบสามารถนำมาใช้และปรับปรุงแผนให้มีความเหมาะสมหรือไม่ 7. สอบทานว่ามีการฝึกอบรมเกี่ยวกับแผนการดำรงอยู่ทางด้านเทคโนโลยีสารสนเทศหรือไม่

ตารางที่ 4.22 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	ปฏิบัติของผู้ใช้ โดยมีกระบวนการในการให้ผู้ใช้แต่ละแผนกมีส่วนร่วมในการสำรองข้อมูลเพื่อให้กู้คืนระบบได้หลังจากเกิดความเสียหาย 10. ในการวางแผนต่อเนื่องควรมีการระบุถึงทรัพยากรทางด้านเทคโนโลยีสารสนเทศ เช่น รายการของแอพลิเคชั่น การบริการของบุคคลภยนอก ระบบปฏิบัติการ บุคลากร คู่ค้า ข้อมูล และช่วงเวลาที่จำเป็นสำหรับการกู้คืนระบบหลังจากมีความเสียหายเกิดขึ้น ข้อมูลที่สำคัญและการปฏิบัติงานควรจะถูกระบุเป็นลายลักษณ์อักษร จัดลำดับความสำคัญ และมีการอนุมัติโดยเจ้าของธุรกิจ 11. มีการกำหนดศูนย์สำรองและฮาร์ดแวร์ที่ใช้ในการสำรองระบบ 12. มีการจัดเก็บสื่อข้อมูลสำรองไว้นอกสถานที่ ซึ่งมีสภาพแวด - ล้อมที่เหมาะสมกับสื่อบันทึก มีมาตรการในการป้องกันความ	8. สอบทานว่ามีการเผยแพร่แผนการดำรงอยู่ด้านเทคโนโลยีสารสนเทศให้แก่บุคคลที่เกี่ยวข้องหรือไม่ 9. สอบทานว่าองค์กรมีการกำหนดให้มีระเบียบการปฏิบัติงานสำรองที่เป็นทางเลือกในการปฏิบัติของผู้ใช้ โดยมีกระบวนการในการให้ผู้ใช้แต่ละแผนกมีส่วนร่วมในการสำรองข้อมูลเพื่อให้กู้คืนระบบได้หลังจากเกิดความเสียหายหรือไม่ 10. สอบทานว่าในการวางแผนต่อเนื่องมีการระบุถึงทรัพยากรทางด้านเทคโนโลยีสารสนเทศสำหรับการกู้คืนระบบ โดยมีการระบุเป็นลายลักษณ์อักษร จัดลำดับความสำคัญ และมีการอนุมัติโดยผู้มีอำนาจหรือไม่ 11. สอบทานว่าองค์กรมีการกำหนดศูนย์สำรองและฮาร์ดแวร์ที่ใช้ในการสำรองระบบหรือไม่ 12. สอบทานว่ามีการจัดเก็บสื่อข้อมูลสำรองไว้นอกสถานที่ซึ่งมีสภาพแวดล้อม ที่เหมาะสม

ตารางที่ 4.22 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	ปลอดภัยของการสำรองทรัพยากร การจัดเก็บภายนอกมีการประเมินและตรวจสอบเป็นระยะๆ ในเรื่องการป้องกันจากสิ่งแวดล้อมและความปลอดภัย 13. มีการกำหนดระเบียบปฏิบัติในการสรุปผล โดยมีกระบวนการในการประเมินการวางแผนและมีการปรับปรุงแผนให้ทันสมัยอยู่เสมอ	กับสื่อบันทึก มีมาตรการในการป้องกันความปลอดภัยของการสำรองทรัพยากร มีการประเมินและตรวจสอบเป็นระยะ ๆ ในเรื่องการป้องกันจากสิ่งแวดล้อมและความปลอดภัยหรือไม่ 13. สอบทานว่ามีการกำหนดระเบียบปฏิบัติในการสรุปผล โดยมีกระบวนการในการประเมินการวางแผน และมีการปรับปรุงแผนให้ทันสมัยอยู่เสมอหรือไม่

ตารางที่ 4.23 DS5 : การรักษาความปลอดภัยระบบ (Ensure Systems Security)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. ข้อมูลถูกใช้ เปิดเผย แก้ไข ทำลาย โดยไม่ได้รับอนุญาต 2. ข้อมูลสูญหาย 3. ระบบงานไม่สามารถทำงานได้	1. มีกระบวนการบริหารจัดการด้านความปลอดภัยที่ดี โดยการกำหนดนโยบาย มาตรฐาน ขั้นตอนการปฏิบัติงานด้านการรักษาความปลอดภัย มีการตรวจสอบติดตามด้านความปลอดภัย มีการทดสอบความถูกต้องเป็นประจำ มีการแก้ไข	1. สอบทานว่ามีกระบวนการบริหารจัดการด้านความปลอดภัยหรือไม่ 2. สอบทานว่ามีการกำหนดอำนาจหรือสิทธิและมีการควบคุมการเข้าสู่ระบบหรือไม่ 3. สอบทานว่ามีการป้องกันการแก้ไขระบบควบคุมที่กำหนดไว้

ตารางที่ 4.23 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	จุดอ่อนด้านความปลอดภัยที่ตรวจพบด้วยกระบวนการที่มีความถูกต้อง และมีการทบทวนความน่าเชื่อถือของระบบรักษาความปลอดภัย 2. มีการกำหนดอำนาจหรือสิทธิและมีการควบคุมการเข้าสู่ระบบ 3. มีการป้องกันการแก้ไขระบบควบคุมที่กำหนดไว้ 4. มีการจัดการเกี่ยวกับรหัสลับ 5. มีมาตรการรักษาความปลอดภัยในการเข้าถึงข้อมูลแบบออนไลน์ 6. มีการจำแนกประเภทข้อมูล 7. มีการสอบทานและควบคุมบัญชีผู้ใช้งาน 8. มีการรายงานการละเมิดและกิจกรรมที่เกี่ยวข้องกับความปลอดภัย และมีการจัดการกับเหตุการณ์ที่เกิดขึ้น 9. มีการกำหนดการอนุมัติรายการ 10. กำหนดให้มีการปฏิเสธรายการที่ผิดเงื่อนไข 11. มีการกำหนดช่องทางการ	หรือไม่ 4. สอบทานว่ามีการจัดการเกี่ยวกับรหัสลับหรือไม่ 5. สอบทานว่ามีมาตรการรักษาความปลอดภัยในการเข้าถึงข้อมูลแบบออนไลน์หรือไม่ 6. สอบทานว่ามีการจำแนกประเภทข้อมูลหรือไม่ 7. สอบทานว่ามีการควบคุมบัญชีผู้ใช้งานหรือไม่ 8. สอบทานว่ามีการรายงานการละเมิดและกิจกรรมที่เกี่ยวข้องกับความปลอดภัย การจัดการกับเหตุการณ์ที่เกิดขึ้นหรือไม่ 9. สอบทานความเหมาะสมของการกำหนดอำนาจการอนุมัติรายการ 10. สอบทานว่ามีการกำหนดให้มีการปฏิเสธรายการที่ผิดเงื่อนไขหรือไม่ 11. สอบทานว่ามีการกำหนดช่องทางการรับส่งข้อมูล และพิจารณาว่ามีความน่าเชื่อถือหรือไม่

ตารางที่ 4.23 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	รับส่งข้อมูลที่เชื่อถือได้ 12. มีการป้องกัน การตรวจหาและการแก้ไขเกี่ยวกับโปรแกรมที่เป็นอันตรายต่อองค์กร 13. กำหนดโครงสร้างไฟร์วอลล์และการเชื่อมโยงกับเครือข่ายสาธารณะ 14. มีการป้องกันความเสียหายของข้อมูลอิเล็กทรอนิกส์	12. สอบทานว่ามีการป้องกันการตรวจหา และการแก้ไขเกี่ยวกับโปรแกรมที่เป็นอันตรายต่อองค์กรหรือไม่ 13. สอบทานว่ามีการกำหนดโครงสร้างไฟร์วอลล์และการเชื่อมโยงกับเครือข่ายสาธารณะหรือไม่ 14. สอบทานว่ามีการป้องกันความเสียหายของข้อมูลอิเล็กทรอนิกส์หรือไม่

ตารางที่ 4.24 DS6 : การกำหนดและจัดสรรต้นทุน (Identify and Allocate Costs)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. เกิดความเสียหายจากการกำหนดนโยบายในการจัดสรรงบประมาณในการดำเนินงานที่ไม่เหมาะสม 2. เกิดความเสียหายจากการใช้ทรัพยากรที่ไม่เหมาะสม 3. การเรียกเก็บค่าบริการ	1. รายการที่สามารถบันทึกค่าใช้จ่ายเป็นต้นทุนด้านเทคโนโลยีสารสนเทศได้มีการระบุไว้ สามารถวัดได้ และสามารถคำนวณได้โดยผู้ใช้งานเพื่อผู้ใช้งานจะสามารถควบคุมการใช้บริการทางเทคโนโลยีสารสนเทศ 2. การจัดสรรต้นทุนด้าน	1. สอบทานว่ามีการระบุรายการที่สามารถคิดค่าบริการได้หรือไม่ 2. สอบทานว่ามีการกำหนดระเบียบปฏิบัติในเรื่องการจัดการต้นทุน 3. สอบทานความเหมาะสมของการจัดสรรต้นทุนด้านเทคโน - โลยีสารสนเทศ 4. สอบทานว่ามีการกำหนด

ตารางที่ 4.24 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
กับผู้ใช้งานไม่ถูกต้องเหมาะสม	เทคโนโลยีสารสนเทศมีความยุติธรรม ตัววัดมีความถูกต้องแม่นยำและได้รับความเห็นชอบจากผู้ใช้งาน 3. มีการกำหนดระเบียบปฏิบัติในเรื่องการจัดการต้นทุน ความแตกต่างระหว่างต้นทุนที่ประมาณการและต้นทุนที่เกิดขึ้นจริงได้มีการวิเคราะห์อย่างเหมาะสม 4. ผู้บริหารมีการประเมินผลของต้นทุนทางเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ 5. มีการกำหนดระเบียบปฏิบัติการเรียกเก็บค่าใช้จ่ายและการคืนค่าใช้จ่าย โดยมีการคิดค่าบริการที่เหมาะสมกับทรัพยากรทางเทคโนโลยีสารสนเทศและเกิดความยุติธรรมกับหน่วยงานผู้ใช้งานและความต้องการ อัตราการเก็บค่าบริการสะท้อนถึงต้นทุนการจัดการบริการ	ระเบียบปฏิบัติการเรียกเก็บค่าใช้จ่ายและการคืนค่าใช้จ่ายหรือไม่ 5. สอบทานความเหมาะสมของการเรียกเก็บค่าใช้จ่าย และการคืนค่าใช้จ่าย

ตารางที่ 4.25 DS7 : การให้ความรู้และฝึกอบรมผู้ใช้งาน (Educate and Train Users)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. ผู้ใช้ขาดความรู้ความเข้าใจในระบบงาน ทำให้ไม่สามารถใช้ระบบงานได้อย่างมีประสิทธิภาพ 2. ผู้ใช้ขาดความเข้าใจถึงความเสี่ยง และความรับผิดชอบที่เกี่ยวเนื่องในการใช้นั้น ๆ	1. มีการกำหนดแผนฝึกอบรมที่จำเป็นให้แก่พนักงานในแต่ละระดับ โดยมีการให้ความรู้และฝึกอบรมในเรื่องเกี่ยวกับระบบสารสนเทศ และมีการวัดผลของการฝึกอบรมนั้น ๆ 2. มีการกำหนดเป้าหมายของการอบรมในแต่ละระดับพนักงาน 3. มีการอบรมให้มีความตระหนักในเรื่องการรักษาความปลอดภัย	1. สอบทานว่ามีการกำหนดแผนฝึกอบรมที่จำเป็นให้แก่พนักงานในแต่ละระดับ และมีการกำหนดเป้าหมายของการอบรมในแต่ละระดับของพนักงานหรือไม่ 2. สอบทานว่ามีการอบรมพนักงานให้มีความตระหนักในเรื่องการรักษาความปลอดภัยหรือไม่

ตารางที่ 4.26 DS8 : การให้ความช่วยเหลือและคำแนะนำแก่ผู้ใช้ระบบงานในองค์กร (Assist and Advise Customers)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- ไม่สามารถแก้ไขปัญหาของผู้ใช้งาน หรือแก้ไขปัญหาไม่ตรงจุด	1. มีการจัดตั้งหน่วยงานที่ทำหน้าที่ในการให้บริการช่วยเหลือผู้ใช้งาน ติดต่อแก้ไขปัญหาให้กับผู้ใช้งานอย่างใกล้ชิด 2. มีการกำหนดระดับขั้นในการจัดการเหตุการณ์ วิเคราะห์แนวโน้มและสาเหตุของปัญหา	1. สอบทานว่ามีการจัดตั้งหน่วยงานที่ทำหน้าที่ใน การให้บริการช่วยเหลือ ผู้ใช้งานหรือไม่ 2. สอบทานว่ามีการกำหนดระเบียบหรือขั้นตอนปฏิบัติงานในการแก้ไขปัญหาข้อซักถาม

ตารางที่ 4.26 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	และกำหนดแนวทางที่ใช้ในการแก้ไขปัญหาที่ชัดเจน 3. มีการบันทึกปัญหาต่าง ๆ ที่ถูกสอบถาม 4. มีการกำหนดระเบียบหรือขั้นตอนวิธีปฏิบัติงานในการแก้ไขปัญหาข้อซักถามของผู้ใช้งานที่ไม่สามารถแก้ไขได้ทันที 5. มีการกำหนดระเบียบหรือขั้นตอนวิธีปฏิบัติงานสำหรับการติดตามการแก้ไขปัญหาที่เกิดขึ้น 6. มีการรายงานอย่างเพียงพอเกี่ยวกับการถามคำถามจากผู้ใช้งานและแนวทางการแก้ไข เวลาที่ตอบกลับ มีการวิเคราะห์แนวโน้มและรายงานการวิเคราะห์	ของผู้ใช้งานหรือไม่ 3. สอบทานว่ามีการกำหนดระเบียบหรือขั้นตอนการปฏิบัติในการติดตามการแก้ไขปัญหาหรือไม่ 4. สอบทานว่ามีการรายงานอย่างเพียงพอเกี่ยวกับการถามคำถามจากผู้ใช้งานและแนวทางการแก้ไข เวลาที่ตอบกลับ มีการวิเคราะห์แนวโน้มและรายงานการวิเคราะห์ หรือไม่

ตารางที่ 4.27 DS9 : การจัดการรายละเอียดทรัพย์สิน (Manage the Configuration)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. มีการแก้ไขเปลี่ยนแปลงรายละเอียดทรัพย์สินโดยไม่ได้รับอนุญาต 2. มีการนำโปรแกรมที่ไม่ได้รับอนุญาตให้นำมาใช้งานเข้ามา ซึ่งอาจทำให้เกิดการละเมิดลิขสิทธิ์ได้ 3. ทรัพย์สินมีการสูญหาย	1. มีการสร้างและดูแลรักษาแหล่งที่ใช้ในการเก็บค่ารายละเอียด ต่าง ๆ ให้มีความถูกต้องและสมบูรณ์อยู่เสมอ 2. ข้อมูลพื้นฐานของรายละเอียดทรัพย์สิน สถานภาพของทรัพย์สิน ซึ่งสามารถตรวจสอบได้ถ้ามีการเปลี่ยนแปลง 3. มีการควบคุมรายละเอียดทรัพย์สิน เพื่อให้มั่นใจในความคงอยู่และความถูกต้องของการบันทึกลักษณะต่าง ๆ ทางด้านเทคโนโลยีสารสนเทศได้ถูกตรวจสอบเป็นระยะ ๆ 4. มีการกำหนดนโยบายที่ชัดเจนในการใช้ซอฟต์แวร์ เพื่อป้องกันการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์หรือไม่ได้รับอนุญาตให้นำมาใช้งาน มีการตรวจสอบคอมพิว - เตอร์ของบุคลากรเป็นระยะ ๆ มีการทบทวนความต้องการของฮาร์ดแวร์และซอฟต์แวร์ที่มีลิขสิทธิ์อย่างสม่ำเสมอ 5. การจัดเก็บซอฟต์แวร์และข้อมูลที่ใช้งานจริง แยกออกจาก	1. สอบทานว่ามีบันทึกรายการและรายละเอียดของทรัพย์สินอย่างครบถ้วนถูกต้องหรือไม่ 2. สอบทานว่ามีการบันทึกสถานภาพปัจจุบันของทรัพย์สินต่าง ๆ และมีการสอบทานอย่างสม่ำเสมอหรือไม่ 3. สอบทานว่ามีการกำหนดนโยบายที่ชัดเจนในการใช้ซอฟต์แวร์ และมีการตรวจสอบคอมพิวเตอร์ของบุคลากรเป็นระยะ ๆ หรือไม่ 4. สอบทานว่ามีการทบทวนความต้องการของฮาร์ดแวร์และซอฟต์แวร์ที่มีลิขสิทธิ์อย่างสม่ำเสมอหรือไม่ 5. สอบทานว่ามีการจัดเก็บซอฟต์แวร์และข้อมูลที่ใช้งานจริง แยกออกจากส่วนอื่น ๆ เช่น การพัฒนาระบบการทดสอบหรือไม่ 6. สอบทานว่ามีการกำหนดระเบียบหรือขั้นตอนปฏิบัติการจัดการเกี่ยวกับรายละเอียดทรัพย์สินหรือไม่

ตารางที่ 4.27 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	ส่วนอื่น ๆ เช่น การพัฒนาระบบ การทดสอบ 6. มีการกำหนดระเบียบหรือขั้นตอนปฏิบัติ การจัดการเกี่ยวกับรายละเอียดทรัพย์สิน เพื่อให้มั่นใจว่าองค์ประกอบสำคัญของการใช้ทรัพยากรในองค์กรมีการระบุและการบำรุงรักษาที่เหมาะสม 7. มีการกำหนดความรับผิดชอบด้านซอฟต์แวร์ โดยซอฟต์แวร์ควรมีการทำฉลาก (Label), มีการเก็บรายละเอียด มีการจัดการเรื่องไลบรารี่ของซอฟต์แวร์ เพื่อตรวจสอบการเปลี่ยนแปลงของโปรแกรมและการบำรุงรักษาเวอร์ชันของโปรแกรม เป็นต้น 8. มีการเก็บรวบรวมค่า configuration เริ่มต้น มีการสร้าง baseline ต่าง ๆ มีการตรวจสอบความถูกต้องของค่า configuration และมีการปรับปรุงแหล่งที่เก็บค่า configuration ให้ทันสมัยอยู่เสมอ	7. สอบทานว่ามีการกำหนดความรับผิดชอบด้านซอฟต์แวร์ โดยซอฟต์แวร์ควรมีการทำฉลาก (Label) หรือไม่

ตารางที่ 4.28 DS10 : การจัดการปัญหาและเหตุการณ์ที่เกิดขึ้น (Manage Problems and Incidents)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- ปัญหาเดิมอาจเกิดขึ้นอีก เพราะไม่สามารถป้องกันการเกิดขึ้นของปัญหาได้	1. มีระบบการจัดการปัญหา มีการจัดระบุและจัดกลุ่มของปัญหา การวิเคราะห์สาเหตุของปัญหา เพื่อให้มั่นใจว่า เหตุการณ์ทั้งหมดที่เกิดขึ้น ปัญหา และข้อบกพร่องได้ถูกบันทึก วิเคราะห์ และได้การแก้ไขปัญหาได้ทันเวลา 2. มีการกำหนดขั้นตอนการแก้ไขปัญหา เพื่อให้การดำเนินการแก้ไขปัญหาที่ตรวจสอบในแนวทางที่ได้ผลและทันเวลา การจัดลำดับความสำคัญมีความเหมาะสม มีการจัดทำเป็นเอกสารเป็นต้น 3. มีการจัดเก็บหลักฐานการตรวจสอบและการติดตามปัญหาการตรวจสอบอย่างพอเพียงจากเหตุการณ์เพื่อหาสาเหตุของปัญหา 4. มีการกำหนดลำดับการประมวลผลกรณีฉุกเฉิน และและขั้นตอนการอนุญาตให้เข้าถึงระบบในกรณีฉุกเฉินและชั่วคราว มีการกำหนดผู้อนุมัติในกรณีดังกล่าว	1. สอบทานว่ามีระบบการจัดการปัญหา เช่น มีการจัดระบุและจัดกลุ่มของปัญหาและการวิเคราะห์สาเหตุของปัญหา หรือไม่ 2. สอบทานว่ามีการกำหนดขั้นตอนการแก้ไขปัญหา หรือไม่ 3. สอบทานว่ามีการจัดเก็บหลักฐานการตรวจสอบและการติดตามเพื่อหาสาเหตุของปัญหาหรือไม่ 4. สอบทานว่ามีการกำหนดลำดับการประมวลผลกรณีฉุกเฉิน และขั้นตอนการอนุญาตให้เข้าถึงระบบในกรณีฉุกเฉินและชั่วคราว มีการกำหนดผู้อนุมัติหรือไม่

ตารางที่ 4.29 DS11 : การจัดการข้อมูล (Manage Data)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
- ข้อมูลสูญหาย ไม่ถูกต้องครบถ้วน ขาดความน่าเชื่อถือ ทำให้การตัดสินใจของผู้บริหารผิดพลาดได้	1. มีการกำหนดขั้นตอนปฏิบัติในการจัดเตรียมข้อมูล 2. มีการกำหนดขั้นตอนปฏิบัติในการอนุมัติให้นำข้อมูลเอกสารเข้าสู่ระบบ 3. การกำหนดขั้นตอนการรวบรวมข้อมูลเข้าสู่ระบบ การแก้ไขข้อผิดพลาดของข้อมูลเข้าสู่ระบบ ระยะเวลาการจัดเก็บข้อมูลเอกสารประกอบรายการ 4. มีการกำหนดระเบียบปฏิบัติว่าด้วยสิทธิในการนำข้อมูลเข้าประมวลผล 5. มีการตรวจสอบความสมบูรณ์ถูกต้องของการอนุมัติรายการการประมวลผลข้อมูล 6. มีการแก้ไขข้อมูลที่บันทึกผิดพลาด และมีการแก้ไขข้อผิดพลาดในการประมวลผลข้อมูล 7. มีการตรวจสอบความสมเหตุสมผลในการแก้ไขข้อผิดพลาดของการประมวลผลข้อมูล 8. มีขั้นตอนปฏิบัติในการจัดการผลลัพธ์และการจัดเก็บ การแจกจ่ายรายงาน การสอบยันและ	1. สอบทานว่าองค์กรมีการมีการกำหนดระเบียบหรือขั้นตอนปฏิบัติในเรื่องต่างๆ ดังนี้ หรือไม่ - การจัดเตรียมข้อมูล - การอนุมัติให้นำข้อมูลเอกสารเข้าสู่ระบบ - การรวบรวมข้อมูลเข้าสู่ระบบ การแก้ไข้อผิดพลาดของข้อมูลเข้าสู่ระบบ - ระยะเวลาการจัดเก็บข้อมูลและเอกสารประกอบรายการ - สิทธิในการนำข้อมูลเข้าประมวลผล 5. สอบทานว่ามีการตรวจสอบความสมบูรณ์ ถูกต้องของการอนุมัติรายการ การประมวลผลข้อมูล หรือไม่ 6. สอบทานว่ามีการแก้ไขข้อมูลที่บันทึกผิดพลาด และมีการแก้ไขข้อผิดพลาด ในการประมวลผลข้อมูลหรือไม่ 7. สอบทานความสมเหตุสมผลในการแก้ไขข้อผิดพลาดของการประมวลผลข้อมูล

ตารางที่ 4.29 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	กระทบยอดรวมของรายงาน การสอบทานและการแก้ไขข้อผิดพลาดของรายงาน มีข้อกำหนดในการรักษาความปลอดภัยของรายงาน 9. มีการป้องกันข้อมูลที่มีความสำคัญในระหว่างการเคลื่อนย้ายหรือส่งผ่าน 10. มีการป้องกันข้อมูลสำคัญที่บันทึกอยู่บนสื่อบันทึกข้อมูลที่องค์กรได้จำหน่ายทิ้ง 11. มีขั้นตอนปฏิบัติในการจัดการด้านการจัดเก็บข้อมูล กำหนดระยะเวลาและเงื่อนไขการจัดเก็บข้อมูล มีระบบการจัดการคลังสื่อบันทึกข้อมูล มีการกำหนดความรับผิดชอบในการจัดการคลังสื่อบันทึกข้อมูล การคงความถูกต้องของข้อมูลที่จัดเก็บ 12. มีการกำหนดขั้นตอนปฏิบัติงานด้านการสำรองข้อมูล การจัดเก็บข้อมูลชุดสำรอง การจัดเก็บข้อมูลถาวร 13. การป้องกันข้อความที่สำคัญ 14. การกำหนดวิธีการพิสูจน์ตน	8. สอบทานว่าองค์กรมีการกำหนดขั้นตอนปฏิบัติในการจัดการผลลัพธ์และการจัดเก็บการแจกจ่ายรายงาน การสอบยันและกระทบยอดรวมของรายงาน การสอบทานและการแก้ไขข้อผิดพลาดของรายงานและมีข้อกำหนดในการรักษาความปลอดภัยของรายงานหรือไม่ 9. สอบทานว่ามีการป้องกันข้อมูลที่มีความสำคัญในระหว่างการเคลื่อนย้าย 10. สอบทานว่ามีการป้องกันข้อมูลสำคัญที่บันทึกอยู่บนสื่อบันทึกข้อมูลที่องค์กรได้จำหน่ายทิ้ง 11. สอบทานว่ามีการกำหนดขั้นตอนปฏิบัติในการจัดการด้านการจัดเก็บข้อมูล กำหนดระยะเวลา และเงื่อนไขการจัดเก็บข้อมูล มีระบบการจัดการคลังสื่อบันทึกข้อมูล มีการกำหนดความรับผิดชอบในการจัดการคลังสื่อบันทึกข้อมูล การ

ตารางที่ 4.29 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	และความครบถ้วนถูกต้อง 15. การกำหนดวิธีการดำเนินการและการตรวจสอบความครบถ้วนถูกต้องของรายการธุรกรรมอิเล็กทรอนิกส์	คงความถูกต้องของข้อมูลที่จัดเก็บ 12. สอบทานว่ามีการกำหนดขั้นตอนปฏิบัติงานด้านการสำรองข้อมูล การจัด เก็บข้อมูลชุดสำรอง การจัดเก็บข้อมูลถาวร 13. สอบทานวิธีการป้องกันข้อความที่สำคัญ 14. สอบทานการกำหนดวิธีการพิสูจน์ตนและความครบถ้วนถูกต้อง

ตารางที่ 4.30 DS12 : การจัดการด้านสิ่งอำนวยความสะดวก (Manage Facilities)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. บุคลากรได้รับอันตรายจากการทำงาน 2. อุปกรณ์ทางด้านเทคโนโลยีสารสนเทศได้รับความเสียหาย 3. เกิดการหยุดชะงักของการดำเนินธุรกิจ หากเกิดความเสียหายกับอุปกรณ์	1. มีกระบวนการของการบริหารจัดการในด้านสิ่งอำนวยความสะดวก ตั้งแต่ขั้นตอนของการระบุความต้องการของสถานที่ตั้ง การคัดเลือกอุปกรณ์ที่เหมาะสม การออกแบบกระบวนการที่มีประสิทธิภาพเพื่อใช้การตรวจสอบติดตามปัจจัยของ	1. สอบทานว่ามีกระบวนการของการบริหารจัดการในด้านสิ่งอำนวยความสะดวก หรือไม่ 2. สอบทานว่ามีการกำหนดมาตรการความปลอดภัยทางกายภาพ ความปลอดภัยของสถานที่ที่ตั้งศูนย์คอมพิวเตอร์

ตารางที่ 4.30 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
ทางด้านเทคโนโลยีที่มีความสำคัญ	สภาพแวดล้อมต่าง ๆ 2. มีมาตรการความปลอดภัยทางกายภาพ ความปลอดภัยของสถานที่ที่ตั้งศูนย์คอมพิวเตอร์ 3. มีการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ 4. มีมาตรการความปลอดภัยและสุขอนามัยของบุคลากร 5. มีมาตรการป้องกันภัยจากปัจจัยรอบข้าง 6. มีเครื่องจ่ายกระแสไฟฟ้าสำรอง	หรือไม่ 3. สอบทานว่ามีการควบคุมการเข้าออกศูนย์คอมพิวเตอร์หรือไม่ 4. สอบทานว่ามีมาตรการความปลอดภัยและสุขอนามัยของบุคลากรหรือไม่ 5. สอบทานว่ามีมาตรการป้องกันภัยจากปัจจัยรอบข้างหรือไม่ 6. สอบทานว่ามีเครื่องจ่ายกระแสไฟฟ้าสำรองหรือไม่

ตารางที่ 4.31 DS13 : การจัดการด้านการปฏิบัติการ (Manage Operations)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
1. เกิดปฏิบัติการด้านเทคโนโลยีสารสนเทศเกิดการหยุดชะงัก 2. ผลลัพธ์จากปฏิบัติการด้านเทคโนโลยีสารสน-เทศ ไม่ครบถ้วนสมบูรณ์	1. มีระเบียบปฏิบัติและคู่มือคำสั่งการประมวลผล 2. มีเอกสารขั้นตอนการเริ่มทำงานของระบบ และคู่มือการปฏิบัติ งานอื่น ๆ 3. มีการจัดตารางการปฏิบัติงาน 4. มีการกำหนดขั้นตอนการปฏิบัติงานกรณีมีการประมวลผล	1. สอบทานว่ามีระเบียบปฏิบัติและคู่มือคำสั่งการประมวลผลหรือไม่ 2. สอบทานว่ามีเอกสารแสดงขั้นตอนการเริ่มทำงานของระบบและคู่มือการปฏิบัติงานอื่นๆ หรือไม่ 3. สอบทานว่ามีการจัดตาราง

ตารางที่ 4.31 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	นอกเหนือจากตารางการปฏิบัติงาน 5. มีการควบคุมความต่อเนื่องของการประมวลผล 6. มีการบันทึกเหตุการณ์การปฏิบัติงาน 7. มีมาตรการในการป้องกันเอกสารหรืออุปกรณ์ที่สำคัญ 8. มีขั้นตอนปฏิบัติงานและการควบคุมการปฏิบัติงานระยะไกล	การปฏิบัติงาน และมีการกำหนดขั้นตอนการปฏิบัติงานกรณีมีการประมวลผลนอกเหนือจากตารางการปฏิบัติงานหรือไม่ 5. สอบทานว่ามีการควบคุมความต่อเนื่องของการประมวลผลหรือไม่ 6. สอบทานว่ามีการบันทึกเหตุการณ์การปฏิบัติงานหรือไม่ 7. สอบทานว่ามีมาตรการในการป้องกันเอกสารหรืออุปกรณ์ที่สำคัญหรือไม่ 8. สอบทานว่ามีขั้นตอนปฏิบัติงานและการควบคุมการปฏิบัติงานระยะไกลหรือไม่

4.2.4 การติดตามผล (M : Monitoring)

วัตถุประสงค์ของการตรวจสอบ : เพื่อให้มั่นใจว่า

1. กิจกรรมด้านเทคโนโลยีสารสนเทศสามารถบรรลุเป้าหมายการปฏิบัติงานตามที่กำหนด

2. เป้าหมายของการควบคุมภายในของกิจกรรมด้านเทคโนโลยีสารสนเทศสามารถบรรลุได้ตามที่กำหนด

3. เพื่อเพิ่มความมั่นใจและการไว้วางใจระหว่างองค์กร ผู้ใช้ระบบ และบุคคลภายนอก

4. เพื่อเพิ่มระดับความมั่นใจและประโยชน์จากผู้เชี่ยวชาญในวิธีการปฏิบัติที่ดี

ตารางที่ 4.32 ถึง ตารางที่ 4.35 แสดงแนวการตรวจสอบการติดตามผล (M : Monitoring)

ตารางที่ 4.32 M1 : การติดตามกระบวนการทำงาน (Monitor the Processes)

ความเสี่ยง	**การควบคุมที่ควรมี (Suggested Control)**	**ทดสอบ/ตรวจสอบ**
- การปฏิบัติงานด้านเทค-โนโลยีสารสนเทศ ไม่สามารถบรรลุเป้าหมายการปฏิบัติงานตามที่กำหนด	1. มีกระบวนการในการกำหนดตัวชี้วัดประสิทธิภาพที่เกี่ยวข้อง 2. มีกระบวนการในการรวบรวมข้อมูล การประเมินประสิทธิภาพการปฏิบัติงานอย่างต่อเนื่อง 3. มีการประเมินความพึงพอใจของผู้รับบริการ เพื่อระบุระดับการให้บริการและตั้งวัตถุประ – สงค์ในการพัฒนา 4. มีการรายงานผลการติดตามต่อผู้บริหาร	1. สอบทานว่ามีกระบวนการในการกำหนดตัวชี้วัดประสิทธิภาพหรือไม่ 2. สอบทานว่ามีกระบวนการในการรวบรวมข้อมูล การประเมินประสิทธิภาพการปฏิบัติงานอย่างต่อเนื่องหรือไม่ 3. สอบทานว่ามีการประเมินความพึงพอใจของผู้รับบริการหรือไม่ 4. สอบทานมีการรายงานผลการติดตามต่อผู้บริหารหรือไม่

ตารางที่ 4.33 M2 : การประเมินความเพียงพอของการควบคุมภายใน (Assess Internal Control Adequacy)

ความเสี่ยง	**การควบคุมที่ควรมี (Suggested Control)**	**ทดสอบ/ตรวจสอบ**
1. การดำเนินงานขององค์กรไม่สามารถบรรลุเป้าหมายที่กำหนดไว้ 2. อาจเกิดการทุจริตในองค์กร 3. การดำเนินงานขาดประสิทธิภาพและประสิทธิผล	1. มีกระบวนการในการติดตามการควบคุมภายใน เพื่อพิจารณาประสิทธิภาพการควบคุมภายในขององค์กร 2. ระยะเวลาการปฏิบัติงานของการควบคุมภายใน มีการปรับปรุงการควบคุมภายในให้เหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลงไป และมีการบันทึกสิ่งที่ถูกควบคุมและรายงานกับผู้บริหารอย่างเป็นระบบ 3. การจัดลำดับการรายงานการควบคุมภายใน มีการระบุว่าเทคโนโลยีสารสนเทศใดต้องการการควบคุมในระดับใด สำหรับผู้บริหารใช้ในการตัดสินใจ	1. สอบทานว่ามีกระบวนการในการติดตามการควบคุมภายใน เพื่อพิจารณาประสิทธิภาพการควบคุมภายในขององค์กรหรือไม่ 2. สอบทานว่าระยะเวลาการปฏิบัติงานของการควบคุมภายในมีความเหมาะสม 3. สอบทานว่ามีการจัดทำรายงานลำดับการควบคุมภายในหรือไม่

ตารางที่ 4.34 M3 : การรับรองความเป็นอิสระ (Obtain Independent Assurance)

ความเสี่ยง	**การควบคุมที่ควรมี (Suggested Control)**	**ทดสอบ/ตร วจสอบ**
- ผลการประเมินจากผู้ประเมินที่ไม่มีความเป็นอิสระ อาจไม่น่าเชื่อถือการนำผลการประเมินมาใช้ในการดำเนินการปรับปรุงแก้ไขต่าง ๆ อาจไม่ตรงกับข้อเท็จจริงที่เกิดขึ้น	1. ผู้ประเมินทั้งจากภายในหรือบุคคลภายในมีความเป็นอิสระในการรับรองในเรื่องต่าง ๆ ได้แก่ การรับรองความปลอดภัยและการควบคุมภายในของการให้บริการด้านเทคโนโลยีสารสนเทศ การประเมินประสิทธิภาพและประสิทธิผลของการบริการด้านเทคโนโลยีสารสนเทศ การรับรองการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับและข้อตกลงที่กำหนดไว้ 2. ผู้ประเมินมีความรู้ความสามารถในการทำหน้าที่รับรองอย่างเป็นอิสระ	1. สอบทานว่าผู้ประเมินทั้งจากภายในหรือบุคคลภายในมีความเป็นอิสระหรือไม่ 2. สอบทานว่าผู้ประเมินเป็นผู้ที่มีความรู้ความสามารถในการทำหน้าที่รับรองอย่างเป็นอิสระหรือไม่

ตารางที่ 4.35 M4 : ความเป็นอิสระในการตรวจสอบ (Provide for Independent Audit)

ความเสี่ยง	**การควบคุมที่ควรมี (Suggested Control)**	**ทดสอบ/ตรวจสอบ**
- ผลการตรวจสอบจากผู้ตรวจสอบที่ไม่มีความเป็นอิสระ อาจไม่น่าเชื่อถือ การนำผลการตรวจสอบมาใช้ในการดำเนินการ ปรับปรุงแก้ไขต่าง ๆ อาจไม่ตรงกับข้อเท็จจริงที่เกิดขึ้น	1. มีกฎบัตรของการตรวจสอบซึ่งระบุหน้าที่และความรับผิดชอบของหน่วยงานที่ทำหน้าที่ตรวจสอบระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรที่ชัดเจนและเหมาะสม 2. หน่วยงานที่ทำหน้าที่ตรวจสอบระบบเทคโนโลยีสารสนเทศจะต้องมีอิสระจากผู้รับการตรวจสอบ ปราศจากความขัดแย้งในผลประโยชน์ 3. มีการกำหนดให้ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศต้องประพฤติปฏิบัติตนให้สอดคล้องตามมรรยาทของผู้ประกอบวิชาชีพตรวจสอบที่กำหนดโดยหน่วยงานกำกับดูแล เช่น สมาคมวิชาชีพที่เกี่ยวข้อง และปฏิบัติงานตรวจสอบตามมาตรฐานการปฏิบัติงานที่เกี่ยวข้อง 4. ผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศต้องมีความรู้ความสามารถทางวิชาการ มีทักษะที่จำเป็นในการปฏิบัติงาน มีการศึกษาหาความรู้หรือเข้าอบรม	1. สอบทานว่าหน่วยงานตรวจสอบเทคโนโลยีสารสนเทศมีกฎบัตรของการตรวจสอบหรือไม่ 2. สอบทานความเหมาะสมของหน้าที่ความรับผิดชอบของหน่วยงานตรวจสอบเทคโนโลยีสารสนเทศ 3. สอบทานว่าหน่วยงานที่ทำหน้าที่ตรวจสอบระบบเทคโนโลยีสารสนเทศจะต้องมีอิสระจากผู้รับการตรวจสอบหรือไม่ 4. สอบทานว่าผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศมีการประพฤติปฏิบัติตนให้สอดคล้องตามมรรยาทของผู้ประกอบวิชาชีพตรวจสอบหรือไม่ 5. สอบทานว่าผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศมีความรู้ความสามารถทางวิชาการ มีทักษะที่จำเป็นในการปฏิบัติงานหรือไม่ 6. สอบทานว่าผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศ มี

ตารางที่ 4.35 (ต่อ)

ความเสี่ยง	การควบคุมที่ควรมี (Suggested Control)	ทดสอบ/ตรวจสอบ
	อย่างต่อเนื่อง เพื่อให้มีความรู้ความสามารถในการปฏิบัติงานอย่างเพียงพอ 5. การปฏิบัติงานของผู้ตรวจสอบระบบสารสนเทศมีกระบวนการเป็นไปตามที่มาตรฐานการปฏิบัติงานตรวจสอบ เช่น มีการวางแผนการตรวจสอบ การปฏิบัติงานตรวจสอบ การรายงานผลการตรวจสอบ และการติดตามผลการตรวจสอบ	การศึกษาหาความรู้หรือเข้าอบรมอย่างต่อเนื่องหรือไม่ 7. สอบทานว่าการปฏิบัติงานของผู้ตรวจสอบระบบสารสนเทศเป็นไปตามกระบวนการที่มาตรฐานการปฏิบัติงานตรวจสอบกำหนดไว้หรือไม่

4.3 กรณีตัวอย่างการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT

จากแนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT จะได้นำใช้เป็นแนวทางในการตรวจสอบระบบเทคโนโลยีสารสนเทศขององค์กรในบางประเด็น โดยจะได้ดำเนินการตรวจสอบในประเด็นดังต่อไปนี้

- PO1 การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ
- P07 การจัดการทรัพยากรมนุษย์
- AI3 การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี
- AI4 ระเบียบปฏิบัติในการพัฒนาและบำรุงรักษา
- DS5 การรักษาความปลอดภัยระบบ
- M1 การติดตามกระบวนการทำงาน

- AI2 การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์

ข้อมูลด้านเทคโนโลยีสารสนเทศเบื้องต้นขององค์กร

องค์กรที่จะทำการตรวจสอบระบบเทคโนโลยีสารสนเทศ ตามแนวทางของ COBIT ประกอบธุรกิจรับประกันวินาศภัย มีพนักงานประมาณ 250 คน ระบบเทคโนโลยีสารสนเทศหลักขององค์กรมีอยู่สองระบบงานคือ ระบบงานประกันภัย และระบบงานบัญชีและเงินเดือน ซึ่งประมวลผลบนเครื่อง RISC/6000 และเครื่อง Windows NT Server สำหรับฐานข้อมูลที่ใช้คือ Informix การปฏิบัติงานมีทั้งที่สำนักงานใหญ่ และสาขาต่างจังหวัดจำนวน 12 สาขา

หน่วยงานทางด้านเทคโนโลยีสารสนเทศมีบุคลากรจำนวน 12 คน แบ่งเป็น 3 แผนก คือ แผนกพัฒนาระบบงาน แผนกเทคนิค และแผนกระบบปฏิบัติการ

การดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศ

วิธีการตรวจสอบการควบคุมทั่วไปของระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

1. การทำความเข้าใจในธุรกิจและสภาพแวดล้อมทางเทคโนโลยีสารสนเทศ โดยการศึกษาทำความเข้าใจโครงสร้างขององค์กร สภาพแวดล้อมทางธุรกิจ ระเบียบวิธีขั้นตอนการปฏิบัติงาน นโยบายต่างๆ ทำการสัมภาษณ์ผู้บริหารที่เกี่ยวกับการกำหนดนโยบายและการควบคุมติดตามผลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และทำการสัมภาษณ์เจ้าหน้าที่ที่เกี่ยวข้องกับการปฏิบัติงาน การควบคุมต่างๆ และระเบียบวิธีขั้นตอนปฏิบัติงานในระบบเทคโนโลยีสารสนเทศ

2. ทำการทดสอบจุดควบคุม โดยใช้วิธีการตรวจสอบต่างๆ เช่น การสัมภาษณ์เจ้าหน้าที่ที่เกี่ยวข้อง การสอบถามเพื่อยืนยัน การสอบทานเอกสารที่เกี่ยวข้อง และการสังเกตการณ์การปฏิบัติงาน โดยตัวอย่างการบันทึกข้อมูลจากการตรวจสอบตามที่แสดงในหน้า 110 – 130

3. ทำการรายงานผลการตรวจสอบ ซึ่งประกอบด้วยประเด็นความเสี่ยงที่ตรวจพบ ผลกระทบ และข้อเสนอแนะเพื่อการปรับปรุงแก้ไข ดังตัวอย่างรายงานผลการตรวจสอบที่แสดงในหน้า 133-135

ตัวอย่างรายงานผลการตรวจสอบระบบเทคโนโลยีสารสนเทศ

ฝ่ายตรวจสอบภายใน ได้ดำเนินการตรวจสอบการควบคุมของระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีวัตถุประสงค์ในการประเมินการควบคุมภายในขั้นต้นของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งฝ่ายตรวจสอบภายในได้ดำเนินการตรวจสอบแล้วเสร็จ สามารถสรุปขอบเขตและผลการตรวจสอบได้ดังนี้

ขอบเขตการตรวจสอบการควบคุมของระบบเทคโนโลยีสารสนเทศ

ทำการสอบทานข้อมูลและทดสอบการควบคุมด้านเทคโนโลยีสารสนเทศ ในประเด็นดังต่อไปนี้

1. การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ
2. การจัดการทรัพยากรมนุษย์
3. การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี
4. ระเบียบปฏิบัติในการพัฒนาและบำรุงรักษา
5. การรักษาความปลอดภัยระบบ
6. การติดตามกระบวนการทำงาน
7. การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์

วิธีการตรวจสอบ

วิธีการตรวจสอบการควบคุมของระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

1. การทำความเข้าใจในธุรกิจและสภาพแวดล้อมทางเทคโนโลยีสารสนเทศ โดยการศึกษาทำความเข้าใจโครงสร้างขององค์กร สภาพแวดล้อมทางธุรกิจ ระเบียบวิธีขั้นตอนการปฏิบัติงาน นโยบายต่างๆ ทำการสัมภาษณ์ผู้บริหารที่เกี่ยวกับการกำหนดนโยบายและการควบคุมติดตามผลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และทำการสัมภาษณ์เจ้าหน้าที่ที่เกี่ยวข้องกับการปฏิบัติงาน การควบคุมต่างๆ และระเบียบวิธีขั้นตอนปฏิบัติงานในระบบเทคโนโลยีสารสนเทศ
2. ทำการทดสอบจุดควบคุม โดยใช้วิธีการตรวจสอบต่างๆ เช่น การสัมภาษณ์เจ้าหน้าที่ที่เกี่ยวข้อง การสอบถามเพื่อยืนยัน การสอบทานเอกสารที่เกี่ยวข้อง และการสังเกตการณ์การปฏิบัติงาน
3. ทำการรายงานผลการตรวจสอบ ซึ่งประกอบด้วยประเด็นความเสี่ยงที่ตรวจพบ ผลกระทบ และข้อเสนอแนะเพื่อการปรับปรุงแก้ไข

ผลการตรวจสอบ

ผลการตรวจสอบ มีดังต่อไปนี้

1. ไม่มีการกำหนดแผนล่วงหน้าสำหรับการบำรุงรักษาฮาร์ดแวร์ขององค์กร ประเด็นที่พบ

องค์กรไม่มีการกำหนดตารางเวลาประจำและช่วงเวลาในการบำรุงรักษาและดูแลฮาร์ดแวร์ ซึ่งอาจทำให้อายุการใช้งานของฮาร์ดแวร์สั้นกว่าที่คาดการณ์ไว้ หรือเกิดการหยุดชะงักการทำงานโดยไม่ได้คาดคิด มีผลกระทบต่อการดำเนินธุรกิจขององค์กร

ผลกระทบ

ฮาร์ดแวร์เกิดความล้มเหลวหรือไม่สามารถทำงานได้ มีผลกระทบต่อการดำเนินธุรกิจเนื่องจากการออกกรมธรรม์ หรือการดำเนินการด้านการจ่ายค่าสินไหมทดแทน จะดำเนินการโดยใช้ข้อมูลจากระบบงานคอมพิวเตอร์ อาจทำให้ลูกค้าไม่พึงพอใจในการบริการขององค์กรได้

ข้อเสนอแนะเพื่อการปรับปรุง

องค์กรควรมีการกำหนดแผนล่วงหน้าสำหรับการบำรุงรักษาฮาร์ดแวร์ โดยการกำหนดตารางเวลาประจำและช่วงเวลาในการบำรุงรักษาและดูแลฮาร์ดแวร์ เพื่อลดความถี่ของผลกระทบที่ทำให้ฮาร์ดแวร์เกิดความล้มเหลวหรือไม่สามารถทำงานได้

2. ไม่มีนโยบายการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศเป็นลายลักษรอักษร ประเด็นที่พบ

ทรัพยากรเทคโนโลยีสารสนเทศขององค์กรเป็นทรัพย์สินที่มีมูลค่าซึ่งต้องได้รับการป้องกันการสูญหาย ถูกทำลาย และการใช้ที่ผิดวัตถุประสงค์ นโยบายการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศจะช่วยเป็นแนวทางในการรักษาความปลอดภัยของทรัพยากรเทคโนโลยีและความถูกต้องของข้อมูลองค์กร สิทธิในการเข้าถึงข้อมูล การเก็บรักษาข้อมูล และอำนาจหน้าที่ของผู้ดูแลรักษาระบบ เมื่อมีการนำนโยบายและระเบียบวิธีปฏิบัติเพื่อการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศมาใช้ องค์กรจะได้มีการดำเนินการด้านการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศให้เป็นไปตามแนวนโยบายและระเบียบวิธีปฏิบัติดังกล่าว ซึ่งในช่วงระยะเวลาการตรวจสอบการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ พบว่า องค์กรยังไม่ได้มีการจัดทำนโยบายการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร เพื่อใช้ควบคุมความปลอดภัยในระบบเทคโนโลยีสารสนเทศขององค์กร และเพื่อประกาศใช้อย่างเป็นทางการกับระบบเทคโนโลยีสารสนเทศขององค์กร

ผลกระทบ

การปราศจากนโยบายการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร อาจส่งผลให้ทรัพยากรเทคโนโลยีสูญหาย ถูกทำลาย มีการใช้ที่ผิดวัตถุประสงค์ ซึ่งอาจส่งผลให้การใช้เกิดการใช้งานในระบบเป็นไปอย่างไม่ถูกต้องและไม่เป็นไปตามวัตถุประสงค์ที่ตั้งไว้ ข้อมูลถูกใช้ เปิดเผย แก้ไข ทำลายโดยไม่ได้รับอนุญาต ข้อมูลสูญหาย ตลอดจนระบบงานไม่สามารถทำงานได้

ข้อเสนอแนะเพื่อการปรับปรุง

องค์กรควรมีการจัดทำนโยบายการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร เพื่อก่อให้เกิดความปลอดภัยแก่ทรัพยากรเทคโนโลยีสารสนเทศและข้อมูลขององค์กร โดยพิจารณาจากความซับซ้อนของการประมวลผลของระบบเทคโนโลยีสารสนเทศที่มีอยู่ ต้นทุน และผลประโยชน์ที่จะได้รับ ทั้งนี้ เนื้อหาและขอบเขตของนโยบายเมื่อจัดทำแล้วควรมีการสื่อสารกับหน่วยงานที่เกี่ยวข้องอย่างชัดเจน นโยบายการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศควรมีรายละเอียดสำคัญในเรื่องต่าง ๆ ดังนี้

- ข้อตกลงหรือการสนับสนุนของผู้บริหาร
- ความตระหนักเรื่องการรักษาความปลอดภัย โดยผู้บริหารและพนักงานทุกคนควรได้รับการแจ้งเรื่องนโยบายและระเบียบวิธีปฏิบัติเพื่อตระหนักถึงความสำคัญของการรักษาความปลอดภัย เช่น การออกจากระบบทุกครั้งหลังการใช้งาน การป้องกันการติดต่อของไวรัสคอมพิวเตอร์ เป็นต้น
- หลักการเข้าถึง ซึ่งควรใช้เกณฑ์ความจำเป็นที่ต้องทำและความจำเป็นที่ต้องรู้
- การสอบทานการให้สิทธิการเข้าถึง โดยการควบคุมการเข้าถึงควรถูกประเมินอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าเป็นไปตามสิทธิการเข้าถึงที่ได้กำหนดไว้
- บทบาทของเจ้าหน้าที่บริหารความปลอดภัย ซึ่งมีหน้าที่รับผิดชอบในการติดตั้งระบบ การติดตามควบคุม และการบังคับใช้กฎการรักษาความปลอดภัยที่ผู้บริหารได้กำหนดขึ้น
- คณะกรรมการด้านความปลอดภัย ซึ่งประกอบด้วยตัวแทนจากหน่วยงานต่าง ๆ ภายในองค์กร เพื่อทำหน้าที่พิจารณาการปฏิบัติงานต่าง ๆ ด้านความปลอดภัย
- การควบคุมฮาร์ดแวร์และซอฟต์แวร์ โดยควรมีการจัดทำบัญชีรายชื่อและทำสารบัญ เพื่อทำให้มั่นใจว่าองค์กรสามารถทราบถึงทรัพยากรทางด้านเทคโนโลยีสารสนเทศที่มีอยู่ การใช้งาน และความต้องการในทรัพยากรเหล่านั้น

ตารางที่ 4.36 ตัวอย่าง การบันทึกข้อมูลจากการตรวจสอบ

PO1 : การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (Define a Strategic IT Plan)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่าองค์กรมีการจัดทำแผนระยะสั้นหรือระยะยาวหรือไม่	/		มีการจัดทำแผนประจำปีและแผนระยะยาว 3 ปี		
2. สอบทานกระบวนการวางแผนระยะยาวและระยะสั้นขององค์การและพิจารณาว่าผู้บริหารระดับสูงได้เข้ามามีส่วนเกี่ยวข้องในการวางแผนหรือไม่	/		คณะกรรมการบริหารรับผิดชอบในการจัดทำแผนระยะสั้นและระยะยาว และอนุมัติโดยคณะกรรมการบริษัท		
3. สอบทานว่ามีการกำหนดเทค – โนโลยีสารสนเทศเป็นส่วนหนึ่งแผนระยะสั้นและระยะยาวหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
4. สอบทานว่าองค์กรมีการจัดทำแผนระยะสั้นและระยะยาวด้านเทคโนโลยีสารสนเทศหรือไม่	/		มีการจัดทำแผนประจำปีและแผนระยะยาว 3 ปี		
5. สอบทานว่ามีการสื่อสารแผนงานด้านเทคโนโลยีให้พนักงานในองค์กรได้รับทราบหรือไม่	/		มีการประชุมเพื่อสื่อสารเกี่ยวกับแผนและการดำเนินงานด้านเทคโนโลยีสารสนเทศทุกเดือนในการประชุมหัวหน้างาน		
6. สอบทานว่ามีการติดตามและรายงานผลการปฏิบัติตามแผนระยะสั้นและแผนระยะยาวหรือไม่	/		ผู้บริหารจะมีการรายการผลการติดตามและรายงานผลการปฏิบัติตามแผนระยะสั้นและระยะยาวในที่ประชุมคณะกรรมการบริษัท		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
7. สอบทานว่าแผนระยะสั้นของส่วนงานเทคโนโลยีสารสนเทศมีความสอดคล้องกับแผนงานระยะยาวหรือไม่	/				
8. สอบถามหน่วยงานสำคัญอื่น ๆ ที่เกี่ยวข้อง เพื่อให้มั่นใจว่ากลยุทธ์ของหน่วยงานต่างๆ มีความสอดคล้องในแนวทางเดียวกันหรือไม่	/		จะมีการสอบถามยังหน่วย-งานอื่น ๆ ว่ามีแผนงานอย่างไร เพื่อให้การวางกลยุทธ์ของหน่วยงานสารสนเทศสอดคล้องกัน		
9.สอบทานการจัดสรรทรัพยากรที่จำเป็นต้องใช้ตามแผนระยะสั้นและระยะยาวมีความเหมาะสมหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

PO7 : การจัดการทรัพยากรบุคคล

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่ามีการจัดทำคำบรรยายลักษณะงาน หน้าที่ ความรับผิดชอบ ตลอดจนคุณสมบัติของบุคลากรตำแหน่งต่าง ๆ ในส่วนงานเทคโนโลยีสารสนเทศหรือไม่	/				
2. สอบทานว่ามีกระบวนการหรือวิธีการจัดหาคนเข้าทำงาน การกำหนดวิธีการเพื่อความปลอดภัยด้านการพนักงานของส่วนงาน	/		จะมีการสอบทานประวัติบุคลากรใหม่ ก่อนรับเข้าทำงาน		
3. สอบทานว่ามีการฝึกอบรมพนักงานของส่วนของเทคโนโลยีสารสนเทศหรือไม่	/		มีแผนการฝึกอบรมประจำปี		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
4. สอบทานว่ามีการประเมินผลการปฏิบัติงานตามหน้าที่งานของพนักงาน โดยเปรียบเทียบกับมาตรฐานหรือแนวทางปฏิบัติที่ได้กำหนดไว้หรือไม่	/		มีการกำหนดมาตรฐานการปฏิบัติงานของตำแหน่งงานต่าง ๆ ไว้ล่วงหน้า		

ตารางที่ 4.36 (ต่อ)

AI3 การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1.สอบทานว่ามีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับโครงสร้างพื้นฐานทางด้านเทคโนโลยี ดังนี้					
1.1 การวางแผนในการจัดหา	/				
1.2 การดูแลรักษาและการป้องกันในส่วนของโครงของโครงสร้างพื้นฐาน	/				
1.3 สอบทานว่ามีการปฏิบัติตามขั้นตอนที่กำหนดไว้หรือไม่	/		มีการปฏิบัติตามขั้นตอนที่กำหนดไว้อย่างครบถ้วน		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2. สอบทานในเรื่องต่าง ๆ ดังนี้					
2.1 มีการประเมินความต้องการด้านฮาร์ดแวร์และซอฟต์แวร์ใหม่	/		จะมีการส่งแบบสอบถามความต้องการไปยังหน่วยงานต่าง ๆ		
2.2 การบำรุงรักษาฮาร์ดแวร์มีแผนกำหนดไว้ล่วงหน้า		/	เมื่อฮาร์ดแวร์มีปัญหาในการทำงาน จะติดตามช่างมาดำเนินการแก้ไข	ฮาร์ดแวร์ไม่สามารถทำงานได้ ทำให้การปฏิบัติงานเกิดการหยุดชะงัก	ควรมีการกำหนดแผนการบำรุงรักษาฮาร์ดแวร์ไว้ล่วงหน้า
2.3 มีการรักษาความปลอดภัยของโปรแกรมระบบ	/				
2.4 มีการกำหนดขั้นตอนในการติดตั้ง ดูแลบำรุงรักษา การควบคุมการเปลี่ยนแปลงแก้ไขโปรแกรมระบบ	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2.5 มีการใช้และติดตามประเมินการใช้งานโปรแกรมอรรถประ-โยชน์หรือไม่ อย่างไร	/				

ตารางที่ 4.36 (ต่อ)

AI4 : ระเบียบปฏิบัติในการพัฒนาและบำรุงรักษา

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. ทำการสอบทานว่ามีการปฏิบัติงานตรงตามความต้องการและระดับการให้บริการในเวลาที่เหมาะสมหรือไม่ อย่างไร	/				
2. สอบทานความละเอียด ครบถ้วนสมบูรณ์ของคู่มือดังนี้					
2.1 คู่มือการปฏิบัติงานของผู้ใช้งาน	/				
2.2 คู่มือการปฏิบัติการคอมพิว-เตอร์ของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
3. สอบทานว่ามีการฝึกอบรมผู้ใช้ระบบงานและมีเอกสารการฝึกอบรม สำหรับระบบงานที่พัฒนาหรือไม่ อย่างไร	/		ก่อนเริ่มใช้ระบบงาน จะมีการฝึกอบรมผู้ใช้งานก่อนและมีเอกสารการฝึกอบรมครบถ้วน		

ตารางที่ 4.36 (ต่อ)

DS5 : การรักษาความปลอดภัยระบบ

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1.สอบทานว่ามีการกำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรหรือไม่		/	มีกระบวนการในการบริหารจัดการด้านความปลอดภัย แต่ไม่ได้จัดทำเป็นนโยบายที่เป็นลายลักษณ์อักษรอย่างชัดเจน	ข้อมูลในระบบคอมพิวเตอร์ขององค์กรเป็นทรัพย์สินที่มีมูลค่า การปราศจากนโยบายความปลอดภัยของระบบเทคโนโลยีสารสนเทศอาจส่งผลให้เกิดการใช้งานในระบบเป็นไปอย่างไม่ถูกต้องและไม่เป็นไปตามวัตถุประสงค์ที่ตั้งไว้ ข้อมูลถูกใช้ เปิดเผย แก้ไข ทำลายโดยไม่ได้รับอนุญาต ข้อมูลสูญหาย ตลอดจนระบบ-งานไม่สามารถทำงานได้	องค์กรควรจัดทำนโยบายการรักษยความปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อก่อให้เกิดความปลอดภัยกับข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัท โดยพิจารณาถึงความซับซ้อนของการประมวลผล ต้นทุนและประโยชน์ที่จะได้รับ ทั้งนี้ขอบเขตและเนื้อหาของนโยบายเมื่อจัดทำแล้วควรจะสื่อสารกับหน่วยงานที่เกี่ยว-ข้องอย่างชัดเจน รายละเอียดสำคัญในนโยบายการรรักษา

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
					ความปลอดภัยระบบเทคโน-โลยีสารสนเทส ควรประ-กอบด้วย ข้อตกลงหรือการสนับสนุนของผู้บริหาร, หลักการเข้าถึงข้อมูล เช่น การเข้าถึงข้อมูลในระบบควรใช้เกณฑ์จำเป็นต้องทำหรือจำเป็นต้องรู้, การสอบทานการให้สิทธิการเข้าถึง โดยการควบคุมการเข้าถึงควรถูกประเมินอย่างสม่ำเสมอ, ความตระหนักเรื่องการรักษาความปลอดภัย, บทบาทของเจ้าหน้าที่บริหารความปลอดภัย คณะกรรมการด้าน

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2. สอบทานว่ามีการกำหนดอำนาจหรือสิทธิและมีการควบคุมการเข้าสู่ระบบหรือไม่	/		มีการกำหนดสิทธิในการเข้าสู่ระบบตามตำแหน่งหน้าที่งานของผู้ใช้ระบบงานแต่ละคน		ความปลอดภัย, การควบคุมซอฟต์แวร์และฮาร์ดแวร์
3. สอบทานว่ามีการป้องกันการแก้ไขระบบควบคุมที่กำหนดไว้หรือไม่	/		มีการบันทึกรายละเอียดการเข้าสู่ระบบงานของผู้ใช้ระบบงานทุกคนและสอบทานโดยผู้ที่ได้รับมอบหมาย		
4. สอบทานว่ามีการจัดการเกี่ยวกับรหัสลับหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
5.สอบทานว่ามีมาตรการรักษาความปลอดภัยในการเข้าถึงข้อมูลแบบออนไลน์หรือไม่	/				
6. สอบทานว่ามีการจำแนกประเภทข้อมูลหรือไม่	/				
7. สอบทานว่ามีการควบคุมบัญชีผู้ใช้งานหรือไม่	/				
8. สอบทานว่ามีการรายงานการละเมิดและกิจกรรมที่เกี่ยวข้องกับความปลอดภัย การจัดการกับเหตุการณ์ที่เกิดขึ้นหรือไม่	/		จะมีการล็อครหัสผู้ใช้งานกรณีพนักงานผู้นั้นลาออก		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
9. สอบทานความเหมาะสมของการกำหนดอำนาจการอนุมัติรายการ	/		เป็นไปตามระเบียบเกี่ยวกับอำนาจดำเนินการที่บริษัทกำหนดวงเงินการอนุมัติสำหรับแต่ละตำแหน่งงาน		
10. สอบทานว่ามีการกำหนดให้มีการปฏิเสธรายการที่ผิดเงื่อนไขหรือไม่	/				
11. สอบทานว่ามีการกำหนดช่องทางการรับส่งข้อมูล และพิจารณาว่ามีความน่าเชื่อถือหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
12. สอบทานว่ามีการป้องกัน การตรวจหา และการแก้ไขเกี่ยวกับโปรแกรมที่เป็นอันตรายหรือไม่	/		จะมีการส่งข่าวสารให้พนักงานทราบเกี่ยวกับข้อควรระวังในการใช้โปแกรมที่อาจเป็นอันตราย ไวรัสคอมพิวเตอร์ และโปรแกรมที่ไม่มีลิขสิทธิ์		
13. สอบทานว่ามีการกำหนดโครงสร้างไฟร์วอลล์และการเชื่อมโยงกับเครือข่ายสาธารณะหรือไม่	/				
14. สอบทานว่ามีการป้องกันความเสียหายของข้อมูลอิเล็กทรอนิกส์หรือไม่	/				

ตารางที่ 4.36 (ต่อ)

M1 : การติดตามกระบวนการทำงาน

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่ามีกระบวนการในการกำหนดตัวชี้วัดประสิทธิภาพหรือไม่	/		มีการรวบรวมข้อมูลเพื่อกำหนดตัวชี้วัดประสิทธิ-ภาพ โดยมีการกำหนด KPI ของงาน		
2. สอบทานว่ามีกระบวนการในการรวบรวมข้อมูล การประเมินประสิทธิภาพการปฏิบัติงานอย่างต่อเนื่องหรือไม่	/				
3.สอบทานว่ามีการประเมินความพึงพอใจของผู้รับบริการหรือไม่	/				
4.สอบทานมีการรายงานผลการติดตามต่อผู้บริหารหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

AI2 : การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่าองค์กรมีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการจัดหาระบบงานประยุกต์ที่องค์กรนำมาใช้หรือไม่	/		กรณีเป็นระบบงานที่มีความซับซ้อน จะใช้วิธีการว่าจ้างบุคคลภายนอกในการพัฒนาระบบงาน ซึ่งจะมีการระบุในสัญญาว่าจ้างถึงขั้น-ตอนต่าง ๆ ในการพัฒนาระบบงานตั้งแต่การออก - แบบระบบงาน การอนุมัติการออกแบบ การกำหนดความต้องการเกี่ยวกับแฟ้มข้อมูล ข้อกำหนดของโปรแกรม ความต้องการเกี่ยวกับข้อมูลนำเข้า การประมวลผล และ ผลลัพธ์		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2. สอบทานว่าองค์กรมีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการดูแลรักษาระบบงานประยุกต์ที่องค์กรนำมาใช้หรือไม่	/		มีการกำหนดขั้นตอนการเข้าถึงโปรแกรมระบบงานประยุกต์ การดูแล version ของโปรแกรมที่ใช้งานจริง		
3. สอบทานว่าองค์กรมีข้อกำหนดเกี่ยวกับความครบถ้วนถูกต้องของโปรแกรมระบบงานประยุกต์หรือไม่	/		มีการกำหนดอย่างละเอียดชัดเจนในสัญญาการจ้างบริษัทบุคคลภายนอกในการพัฒนาระบบงาน		
3. สอบทานว่ามีการทดสอบโปรแกรมระบบงานประยุกต์ด้วยวิธีการทดสอบที่เหมาะสมหรือไม่	/		มีการทดสอบโปรแกรมระบบงานประยุกต์ โดยจะมีการทดสอบโปรแกรมและระบบงานโดยเจ้าหน้าที่หน่วยงานเทคโนโลยีสาร –		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
4. สอบทานว่าผู้ใช้ระบบงานมีส่วนร่วมในการทดสอบหรือไม่	/		สนเทศก่อน หลังจากนั้นจะมีการให้ผู้ใช้ระบบงานเข้าทดสอบระบบงานอีกครั้งหนึ่ง และก่อนจะยกเลิกระบบงานเดิมจะมีการทำงานคู่ขนานก่อนจนกว่าจะมั่นใจในความถูกต้องของโปรแกรมระบบงานใหม่		
5. สอบทานคู่มือผู้ใช้ระบบและคู่มือสนับสนุนการปฏิบัติงานว่ามีความละเอียด ชัดเจน เพียงพอหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
6. สอบทานว่าเมื่อมีข้อขัดแย้งทางด้านเทคนิคหรือลอจิกเกิดขึ้นระหว่างการบำรุงรักษาหรือการพัฒนา การออกแบบจะถูกประเมินซ้ำอีกครั้งหนึ่ง	/				

ตารางที่ 4.36 ตัวอย่าง การบันทึกข้อมูลจากการตรวจสอบ

PO1 : การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (Define a Strategic IT Plan)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่าองค์กรมีการจัดทำแผนระยะสั้นหรือระยะยาวหรือไม่	/		มีการจัดทำแผนประจำปีและแผนระยะยาว 3 ปี		
2. สอบทานกระบวนการวางแผนระยะยาวและระยะสั้นขององค์การและพิจารณาว่าผู้บริหารระดับสูงได้เข้ามามีส่วนเกี่ยวข้องในการวางแผนหรือไม่	/		คณะกรรมการบริหารรับผิดชอบในการจัดทำแผนระยะสั้นและระยะยาว และอนุมัติโดยคณะกรรมการบริษัท		
3. สอบทานว่ามีการกำหนดเทค – โนโลยีสารสนเทศเป็นส่วนหนึ่งแผนระยะสั้นและระยะยาวหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
4. สอบทานว่าองค์กรมีการจัดทำแผนระยะสั้นและระยะยาวด้านเทคโนโลยีสารสนเทศหรือไม่	/		มีการจัดทำแผนประจำปีและแผนระยะยาว 3 ปี		
5. สอบทานว่ามีการสื่อสารแผนงานด้านเทคโนโลยีให้พนักงานในองค์กรได้รับทราบหรือไม่	/		มีการประชุมเพื่อสื่อสารเกี่ยวกับแผนและการดำเนินงานด้านเทคโนโลยีสารสนเทศทุกเดือนในการประชุมหัวหน้างาน		
6. สอบทานว่ามีการติดตามและรายงานผลการปฏิบัติตามแผนระยะสั้นและแผนระยะยาวหรือไม่	/		ผู้บริหารจะมีการรายการผลการติดตามและรายงานผลการปฏิบัติตามแผนระยะสั้นและระยะยาวในที่ประชุมคณะกรรมการบริษัท		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
7. สอบทานว่าแผนระยะสั้นของส่วนงานเทคโนโลยีสารสนเทศมีความสอดคล้องกับแผนงานระยะยาวหรือไม่	/				
8. สอบถามหน่วยงานสำคัญอื่น ๆ ที่เกี่ยวข้อง เพื่อให้มั่นใจว่ากลยุทธ์ของหน่วยงานต่างๆ มีความสอดคล้องในแนวทางเดียวกันหรือไม่	/		จะมีการสอบถามยังหน่วย-งานอื่น ๆ ว่ามีแผนงานอย่างไร เพื่อให้การวางกลยุทธ์ของหน่วยงานสารสนเทศสอดคล้องกัน		
9.สอบทานการจัดสรรทรัพยากรที่จำเป็นต้องใช้ตามแผนระยะสั้นและระยะยาวมีความเหมาะสมหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

PO7 : การจัดการทรัพยากรบุคคล

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่ามีการจัดทำคำบรรยายลักษณะงาน หน้าที่ ความรับผิดชอบ ตลอดจนคุณสมบัติของบุคลากรตำแหน่งต่าง ๆ ในส่วนงานเทคโนโลยีสารสนเทศหรือไม่	/				
2. สอบทานว่ามีกระบวนการหรือวิธีการจัดหาคนเข้าทำงาน การกำหนดวิธีการเพื่อความปลอดภัยด้านการพนักงานของส่วนงาน	/		จะมีการสอบทานประวัติบุคลากรใหม่ ก่อนรับเข้าทำงาน		
3. สอบทานว่ามีการฝึกอบรมพนักงานของส่วนของเทคโนโลยีสารสนเทศหรือไม่	/		มีแผนการฝึกอบรมประจำปี		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
4. สอบทานว่ามีการประเมินผลการปฏิบัติงานตามหน้าที่งานของพนักงาน โดยเปรียบเทียบกับมาตรฐานหรือแนวทางปฏิบัติที่ได้กำหนดไว้หรือไม่	/		มีการกำหนดมาตรฐานการปฏิบัติงานของตำแหน่งงานต่าง ๆ ไว้ล่วงหน้า		

ตารางที่ 4.36 (ต่อ)

AI3 การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1.สอบทานว่ามีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับโครงสร้างพื้นฐานทางด้านเทคโนโลยี ดังนี้					
1.1 การวางแผนในการจัดหา	/				
1.2 การดูแลรักษาและการป้องกันในส่วนของโครงของโครงสร้างพื้นฐาน	/				
1.3 สอบทานว่ามีการปฏิบัติตามขั้นตอนที่กำหนดไว้หรือไม่	/		มีการปฏิบัติตามขั้นตอนที่กำหนดไว้อย่างครบถ้วน		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2. สอบทานในเรื่องต่าง ๆ ดังนี้					
2.1 มีการประเมินความต้องการด้านฮาร์ดแวร์และซอฟต์แวร์ใหม่	/		จะมีการส่งแบบสอบถามความต้องการไปยังหน่วยงานต่าง ๆ		
2.2 การบำรุงรักษาฮาร์ดแวร์มีแผนกำหนดไว้ล่วงหน้า		/	เมื่อฮาร์ดแวร์มีปัญหาในการทำงาน จะติดตามช่างมาดำเนินการแก้ไข	ฮาร์ดแวร์ไม่สามารถทำงานได้ ทำให้การปฏิบัติงานเกิดการหยุดชะงัก	ควรมีการกำหนดแผนการบำรุงรักษาฮาร์ดแวร์ไว้ล่วงหน้า
2.3 มีการรักษาความปลอดภัยของโปรแกรมระบบ	/				
2.4 มีการกำหนดขั้นตอนในการติดตั้ง ดูแลบำรุงรักษา การควบคุมการเปลี่ยนแปลงแก้ไขโปรแกรมระบบ	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2.5 มีการใช้และติดตามประเมินการใช้งานโปรแกรมอรรถประ-โยชน์หรือไม่ อย่างไร	/				

ตารางที่ 4.36 (ต่อ)

AI4 : ระเบียบปฏิบัติในการพัฒนาและบำรุงรักษา

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. ทำการสอบทานว่ามีการปฏิบัติงานตรงตามความต้องการและระดับการให้บริการในเวลาที่เหมาะสมหรือไม่ อย่างไร	/				
2. สอบทานความละเอียด ครบถ้วนสมบูรณ์ของคู่มือดังนี้					
2.1 คู่มือการปฏิบัติงานของผู้ใช้งาน	/				
2.2 คู่มือการปฏิบัติการคอมพิว-เตอร์ของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
3. สอบทานว่ามีการฝึกอบรมผู้ใช้ระบบงานและมีเอกสารการฝึกอบรม สำหรับระบบงานที่พัฒนาหรือไม่ อย่างไร	/		ก่อนเริ่มใช้ระบบงาน จะมีการฝึกอบรมผู้ใช้งานก่อนและมีเอกสารการฝึกอบรมครบถ้วน		

ตารางที่ 4.36 (ต่อ)

DS5 : การรักษาความปลอดภัยระบบ

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1.สอบทานว่ามีการกำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรหรือไม่		/	มีกระบวนการในการบริหารจัดการด้านความปลอดภัย แต่ไม่ได้จัดทำเป็นนโยบายที่เป็นลายลักษณ์อักษรอย่างชัดเจน	ข้อมูลในระบบคอมพิวเตอร์ขององค์กรเป็นทรัพย์สินที่มีมูลค่า การปราศจากนโยบายความปลอดภัยของระบบเทคโนโลยีสารสนเทศอาจส่งผลให้เกิดการใช้งานในระบบเป็นไปอย่างไม่ถูกต้องและไม่เป็นไปตามวัตถุประสงค์ที่ตั้งไว้ ข้อมูลถูกใช้ เปิดเผย แก้ไข ทำลายโดยไม่ได้รับอนุญาต ข้อมูลสูญหาย ตลอดจนระบบ-งานไม่สามารถทำงานได้	องค์กรควรจัดทำนโยบายการรักษยความปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อก่อให้เกิดความปลอดภัยกับข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัท โดยพิจารณาถึงความซับซ้อนของการประมวลผล ต้นทุนและประโยชน์ที่จะได้รับ ทั้งนี้ขอบเขตและเนื้อหาของนโยบายเมื่อจัดทำแล้วควรจะสื่อสารกับหน่วยงานที่เกี่ยว-ข้องอย่างชัดเจน รายละเอียดสำคัญในนโยบายการรรักษา

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
					ความปลอดภัยระบบเทคโน-โลยีสารสนเทส ควรประ-กอบด้วย ข้อตกลงหรือการสนับสนุนของผู้บริหาร, หลักการเข้าถึงข้อมูล เช่น การเข้าถึงข้อมูลในระบบควรใช้เกณฑ์จำเป็นต้องทำหรือจำเป็นต้องรู้, การสอบทานการให้สิทธิการเข้าถึง โดยการควบคุมการเข้าถึงควรถูกประเมินอย่างสม่ำเสมอ, ความตระหนักเรื่องการรักษาความปลอดภัย, บทบาทของเจ้าหน้าที่บริหารความปลอดภัย คณะกรรมการด้าน

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2. สอบทานว่ามีการกำหนดอำนาจหรือสิทธิและมีการควบคุมการเข้าสู่ระบบหรือไม่	/		มีการกำหนดสิทธิในการเข้าสู่ระบบตามตำแหน่งหน้าที่งานของผู้ใช้ระบบงานแต่ละคน		ความปลอดภัย, การควบคุมซอฟต์แวร์และฮาร์ดแวร์
3. สอบทานว่ามีการป้องกันการแก้ไขระบบควบคุมที่กำหนดไว้หรือไม่	/		มีการบันทึกรายละเอียดการเข้าสู่ระบบงานของผู้ใช้ระบบงานทุกคนและสอบทานโดยผู้ที่ได้รับมอบหมาย		
4. สอบทานว่ามีการจัดการเกี่ยวกับรหัสลับหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
5.สอบทานว่ามีมาตรการรักษาความปลอดภัยในการเข้าถึงข้อมูลแบบออนไลน์หรือไม่	/				
6. สอบทานว่ามีการจำแนกประเภทข้อมูลหรือไม่	/				
7. สอบทานว่ามีการควบคุมบัญชีผู้ใช้งานหรือไม่	/				
8. สอบทานว่ามีการรายงานการละเมิดและกิจกรรมที่เกี่ยวข้องกับความปลอดภัย การจัดการกับเหตุการณ์ที่เกิดขึ้นหรือไม่	/		จะมีการล็อครหัสผู้ใช้งานกรณีพนักงานผู้นั้นลาออก		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
9. สอบทานความเหมาะสมของการกำหนดอำนาจการอนุมัติรายการ	/		เป็นไปตามระเบียบเกี่ยวกับอำนาจดำเนินการที่บริษัทกำหนดวงเงินการอนุมัติสำหรับแต่ละตำแหน่งงาน		
10. สอบทานว่ามีการกำหนดให้มีการปฏิเสธรายการที่ผิดเงื่อนไขหรือไม่	/				
11. สอบทานว่ามีการกำหนดช่องทางการรับส่งข้อมูล และพิจารณาว่ามีความน่าเชื่อถือหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
12. สอบทานว่ามีการป้องกัน การตรวจหา และการแก้ไขเกี่ยวกับโปรแกรมที่เป็นอันตรายหรือไม่	/		จะมีการส่งข่าวสารให้พนักงานทราบเกี่ยวกับข้อควรระวังในการใช้โปแกรมที่อาจเป็นอันตราย ไวรัสคอมพิวเตอร์ และโปรแกรมที่ไม่มีลิขสิทธิ์		
13. สอบทานว่ามีการกำหนดโครงสร้างไฟร์วอลล์และการเชื่อมโยงกับเครือข่ายสาธารณะหรือไม่	/				
14. สอบทานว่ามีการป้องกันความเสียหายของข้อมูลอิเล็กทรอนิกส์หรือไม่	/				

ตารางที่ 4.36 (ต่อ)

M1 : การติดตามกระบวนการทำงาน

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่ามีกระบวนการในการกำหนดตัวชี้วัดประสิทธิภาพหรือไม่	/		มีการรวบรวมข้อมูลเพื่อกำหนดตัวชี้วัดประสิทธิ-ภาพ โดยมีการกำหนด KPI ของงาน		
2. สอบทานว่ามีกระบวนการในการรวบรวมข้อมูล การประเมินประสิทธิภาพการปฏิบัติงานอย่างต่อเนื่องหรือไม่	/				
3.สอบทานว่ามีการประเมินความพึงพอใจของผู้รับบริการหรือไม่	/				
4.สอบทานมีการรายงานผลการติดตามต่อผู้บริหารหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

AI2 : การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่าองค์กรมีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการจัดหาระบบงานประยุกต์ที่องค์กรนำมาใช้หรือไม่	/		กรณีเป็นระบบงานที่มีความซับซ้อน จะใช้วิธีการว่าจ้างบุคคลภายนอกในการพัฒนาระบบงาน ซึ่งจะมีการระบุในสัญญาว่าจ้างถึงขั้น-ตอนต่าง ๆ ในการพัฒนาระบบงานตั้งแต่การออก - แบบระบบงาน การอนุมัติการออกแบบ การกำหนดความต้องการเกี่ยวกับแฟ้มข้อมูล ข้อกำหนดของโปรแกรม ความต้องการเกี่ยวกับข้อมูลนำเข้า การประมวลผล และ ผลลัพธ์		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2. สอบทานว่าองค์กรมีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการดูแลรักษาระบบงานประยุกต์ที่องค์กรนำมาใช้หรือไม่	/		มีการกำหนดขั้นตอนการเข้าถึงโปรแกรมระบบงานประยุกต์ การดูแล version ของโปรแกรมที่ใช้งานจริง		
3. สอบทานว่าองค์กรมีข้อกำหนดเกี่ยวกับความครบถ้วนถูกต้องของโปรแกรมระบบงานประยุกต์หรือไม่	/		มีการกำหนดอย่างละเอียดชัดเจนในสัญญาการจ้างบริษัทบุคคลภายนอกในการพัฒนาระบบงาน		
3. สอบทานว่ามีการทดสอบโปรแกรมระบบงานประยุกต์ด้วยวิธีการทดสอบที่เหมาะสมหรือไม่	/		มีการทดสอบโปรแกรมระบบงานประยุกต์ โดยจะมีการทดสอบโปรแกรมและระบบงานโดยเจ้าหน้าที่หน่วยงานเทคโนโลยีสาร –		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
4. สอบทานว่าผู้ใช้ระบบงานมีส่วนร่วมในการทดสอบหรือไม่	/		สนเทศก่อน หลังจากนั้นจะมีการให้ผู้ใช้ระบบงานเข้าทดสอบระบบงานอีกครั้งหนึ่ง และก่อนจะยกเลิกระบบงานเดิมจะมีการทำงานคู่ขนานก่อนจนกว่าจะมั่นใจในความถูกต้องของโปรแกรมระบบงานใหม่		
5. สอบทานคู่มือผู้ใช้ระบบและคู่มือสนับสนุนการปฏิบัติงานว่ามีความละเอียด ชัดเจน เพียงพอหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
6. สอบทานว่าเมื่อมีข้อขัดแย้งทางด้านเทคนิคหรือลอจิกเกิดขึ้นระหว่างการบำรุงรักษาหรือการพัฒนา การออกแบบจะถูกประเมินซ้ำอีกครั้งหนึ่ง	/				

ตารางที่ 4.36 ตัวอย่าง การบันทึกข้อมูลจากการตรวจสอบ

PO1 : การจัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศ (Define a Strategic IT Plan)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่าองค์กรมีการจัดทำแผนระยะสั้นหรือระยะยาวหรือไม่	/		มีการจัดทำแผนประจำปีและแผนระยะยาว 3 ปี		
2. สอบทานกระบวนการวางแผนระยะยาวและระยะสั้นขององค์การและพิจารณาว่าผู้บริหารระดับสูงได้เข้ามามีส่วนเกี่ยวข้องในการวางแผนหรือไม่	/		คณะกรรมการบริหารรับผิดชอบในการจัดทำแผนระยะสั้นและระยะยาว และอนุมัติโดยคณะกรรมการบริษัท		
3. สอบทานว่ามีการกำหนดเทค – โนโลยีสารสนเทศเป็นส่วนหนึ่งแผนระยะสั้นและระยะยาวหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
4. สอบทานว่าองค์กรมีการจัดทำแผนระยะสั้นและระยะยาวด้านเทคโนโลยีสารสนเทศหรือไม่	/		มีการจัดทำแผนประจำปีและแผนระยะยาว 3 ปี		
5. สอบทานว่ามีการสื่อสารแผนงานด้านเทคโนโลยีให้พนักงานในองค์กรได้รับทราบหรือไม่	/		มีการประชุมเพื่อสื่อสารเกี่ยวกับแผนและการดำเนินงานด้านเทคโนโลยีสารสนเทศทุกเดือนในการประชุมหัวหน้างาน		
6. สอบทานว่ามีการติดตามและรายงานผลการปฏิบัติตามแผนระยะสั้นและแผนระยะยาวหรือไม่	/		ผู้บริหารจะมีการรายการผลการติดตามและรายงานผลการปฏิบัติตามแผนระยะสั้นและระยะยาวในที่ประชุมคณะกรรมการบริษัท		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
7. สอบทานว่าแผนระยะสั้นของส่วนงานเทคโนโลยีสารสนเทศมีความสอดคล้องกับแผนงานระยะยาวหรือไม่	/				
8. สอบถามหน่วยงานสำคัญอื่น ๆ ที่เกี่ยวข้อง เพื่อให้มั่นใจว่ากลยุทธ์ของหน่วยงานต่างๆ มีความสอดคล้องในแนวทางเดียวกันหรือไม่	/		จะมีการสอบถามยังหน่วย-งานอื่น ๆ ว่ามีแผนงานอย่างไร เพื่อให้การวางกลยุทธ์ของหน่วยงานสารสนเทศสอดคล้องกัน		
9.สอบทานการจัดสรรทรัพยากรที่จำเป็นต้องใช้ตามแผนระยะสั้นและระยะยาวมีความเหมาะสมหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

PO7 : การจัดการทรัพยากรบุคคล

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่ามีการจัดทำคำบรรยายลักษณะงาน หน้าที่ ความรับผิดชอบ ตลอดจนคุณสมบัติของบุคลากรตำแหน่งต่าง ๆ ในส่วนงานเทคโนโลยีสารสนเทศหรือไม่	/				
2. สอบทานว่ามีกระบวนการหรือวิธีการจัดหาคนเข้าทำงาน การกำหนดวิธีการเพื่อความปลอดภัยด้านการพนักงานของส่วนงาน	/		จะมีการสอบทานประวัติบุคลากรใหม่ ก่อนรับเข้าทำงาน		
3. สอบทานว่ามีการฝึกอบรมพนักงานของส่วนของเทคโนโลยีสารสนเทศหรือไม่	/		มีแผนการฝึกอบรมประจำปี		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
4. สอบทานว่ามีการประเมินผลการปฏิบัติงานตามหน้าที่งานของพนักงาน โดยเปรียบเทียบกับมาตรฐานหรือแนวทางปฏิบัติที่ได้กำหนดไว้หรือไม่	/		มีการกำหนดมาตรฐานการปฏิบัติงานของตำแหน่งงานต่าง ๆ ไว้ล่วงหน้า		

ตารางที่ 4.36 (ต่อ)

AI3 การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานด้านเทคโนโลยี

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1.สอบทานว่ามีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับโครงสร้างพื้นฐานทางด้านเทคโนโลยี ดังนี้					
1.1 การวางแผนในการจัดหา	/				
1.2 การดูแลรักษาและการป้องกันในส่วนของโครงของโครงสร้างพื้นฐาน	/				
1.3 สอบทานว่ามีการปฏิบัติตามขั้นตอนที่กำหนดไว้หรือไม่	/		มีการปฏิบัติตามขั้นตอนที่กำหนดไว้อย่างครบถ้วน		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2. สอบทานในเรื่องต่าง ๆ ดังนี้					
2.1 มีการประเมินความต้องการด้านฮาร์ดแวร์และซอฟต์แวร์ใหม่	/		จะมีการส่งแบบสอบถามความต้องการไปยังหน่วยงานต่าง ๆ		
2.2 การบำรุงรักษาฮาร์ดแวร์มีแผนกำหนดไว้ล่วงหน้า		/	เมื่อฮาร์ดแวร์มีปัญหาในการทำงาน จะติดตามช่างมาดำเนินการแก้ไข	ฮาร์ดแวร์ไม่สามารถทำงานได้ ทำให้การปฏิบัติงานเกิดการหยุดชะงัก	ควรมีการกำหนดแผนการบำรุงรักษาฮาร์ดแวร์ไว้ล่วงหน้า
2.3 มีการรักษาความปลอดภัยของโปรแกรมระบบ	/				
2.4 มีการกำหนดขั้นตอนในการติดตั้ง ดูแลบำรุงรักษา การควบคุมการเปลี่ยนแปลงแก้ไขโปรแกรมระบบ	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2.5 มีการใช้และติดตามประเมินการใช้งานโปรแกรมอรรถประ-โยชน์หรือไม่ อย่างไร	/				

ตารางที่ 4.36 (ต่อ)

AI4 : ระเบียบปฏิบัติในการพัฒนาและบำรุงรักษา

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. ทำการสอบทานว่ามีการปฏิบัติงานตรงตามความต้องการและระดับการให้บริการในเวลาที่เหมาะสมหรือไม่ อย่างไร	/				
2. สอบทานความละเอียด ครบถ้วนสมบูรณ์ของคู่มือดังนี้					
2.1 คู่มือการปฏิบัติงานของผู้ใช้งาน	/				
2.2 คู่มือการปฏิบัติการคอมพิว-เตอร์ของเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
3. สอบทานว่ามีการฝึกอบรมผู้ใช้ระบบงานและมีเอกสารการฝึกอบรม สำหรับระบบงานที่พัฒนาหรือไม่ อย่างไร	/		ก่อนเริ่มใช้ระบบงาน จะมีการฝึกอบรมผู้ใช้งานก่อนและมีเอกสารการฝึกอบรมครบถ้วน		

ตารางที่ 4.36 (ต่อ)

DS5 : การรักษาความปลอดภัยระบบ

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1.สอบทานว่ามีการกำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรหรือไม่		/	มีกระบวนการในการบริหารจัดการด้านความปลอดภัย แต่ไม่ได้จัดทำเป็นนโยบายที่เป็นลายลักษณ์อักษรอย่างชัดเจน	ข้อมูลในระบบคอมพิวเตอร์ขององค์กรเป็นทรัพย์สินที่มีมูลค่า การปราศจากนโยบายความปลอดภัยของระบบเทคโนโลยีสารสนเทศอาจส่งผลให้เกิดการใช้งานในระบบเป็นไปอย่างไม่ถูกต้องและไม่เป็นไปตามวัตถุประสงค์ที่ตั้งไว้ ข้อมูลถูกใช้ เปิดเผย แก้ไข ทำลายโดยไม่ได้รับอนุญาต ข้อมูลสูญหาย ตลอดจนระบบ-งานไม่สามารถทำงานได้	องค์กรควรจัดทำนโยบายการรักษยความปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อก่อให้เกิดความปลอดภัยกับข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัท โดยพิจารณาถึงความซับซ้อนของการประมวลผล ต้นทุนและประโยชน์ที่จะได้รับ ทั้งนี้ขอบเขตและเนื้อหาของนโยบายเมื่อจัดทำแล้วควรจะสื่อสารกับหน่วยงานที่เกี่ยว-ข้องอย่างชัดเจน รายละเอียดสำคัญในนโยบายการรรักษา

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
					ความปลอดภัยระบบเทคโน-โลยีสารสนเทส ควรประ-กอบด้วย ข้อตกลงหรือการสนับสนุนของผู้บริหาร, หลักการเข้าถึงข้อมูล เช่น การเข้าถึงข้อมูลในระบบควรใช้เกณฑ์จำเป็นต้องทำหรือจำเป็นต้องรู้, การสอบทานการให้สิทธิการเข้าถึง โดยการควบคุมการเข้าถึงควรถูกประเมินอย่างสม่ำเสมอ, ความตระหนักเรื่องการรักษาความปลอดภัย, บทบาทของเจ้าหน้าที่บริหารความปลอดภัย คณะกรรมการด้าน

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2. สอบทานว่ามีการกำหนดอำนาจหรือสิทธิและมีการควบคุมการเข้าสู่ระบบหรือไม่	/		มีการกำหนดสิทธิในการเข้าสู่ระบบตามตำแหน่งหน้าที่งานของผู้ใช้ระบบงานแต่ละคน		ความปลอดภัย, การควบคุมซอฟต์แวร์และฮาร์ดแวร์
3. สอบทานว่ามีการป้องกันการแก้ไขระบบควบคุมที่กำหนดไว้หรือไม่	/		มีการบันทึกรายละเอียดการเข้าสู่ระบบงานของผู้ใช้ระบบงานทุกคนและสอบทานโดยผู้ที่ได้รับมอบหมาย		
4. สอบทานว่ามีการจัดการเกี่ยวกับรหัสลับหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		บันทึกผลการตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
5.สอบทานว่ามีมาตรการรักษาความปลอดภัยในการเข้าถึงข้อมูลแบบออนไลน์หรือไม่	/				
6. สอบทานว่ามีการจำแนกประเภทข้อมูลหรือไม่	/				
7. สอบทานว่ามีการควบคุมบัญชีผู้ใช้งานหรือไม่	/				
8. สอบทานว่ามีการรายงานการละเมิดและกิจกรรมที่เกี่ยวข้องกับความปลอดภัย การจัดการกับเหตุการณ์ที่เกิดขึ้นหรือไม่	/		จะมีการล็อครหัสผู้ใช้งานกรณีพนักงานผู้นั้นลาออก		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
9. สอบทานความเหมาะสมของการกำหนดอำนาจการอนุมัติรายการ	/		เป็นไปตามระเบียบเกี่ยวกับอำนาจดำเนินการที่บริษัทกำหนดวงเงินการอนุมัติสำหรับแต่ละตำแหน่งงาน		
10. สอบทานว่ามีการกำหนดให้มีการปฏิเสธรายการที่ผิดเงื่อนไขหรือไม่	/				
11. สอบทานว่ามีการกำหนดช่องทางการรับส่งข้อมูล และพิจารณาว่ามีความน่าเชื่อถือหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
12. สอบทานว่ามีการป้องกัน การตรวจหา และการแก้ไขเกี่ยวกับโปรแกรมที่เป็นอันตรายหรือไม่	/		จะมีการส่งข่าวสารให้พนักงานทราบเกี่ยวกับข้อควรระวังในการใช้โปแกรมที่อาจเป็นอันตราย ไวรัสคอมพิวเตอร์ และโปรแกรมที่ไม่มีลิขสิทธิ์		
13. สอบทานว่ามีการกำหนดโครงสร้างไฟร์วอลล์และการเชื่อมโยงกับเครือข่ายสาธารณะหรือไม่	/				
14. สอบทานว่ามีการป้องกันความเสียหายของข้อมูลอิเล็กทรอนิกส์หรือไม่	/				

ตารางที่ 4.36 (ต่อ)

M1 : การติดตามกระบวนการทำงาน

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่ามีกระบวนการในการกำหนดตัวชี้วัดประสิทธิภาพหรือไม่	/		มีการรวบรวมข้อมูลเพื่อกำหนดตัวชี้วัดประสิทธิ-ภาพ โดยมีการกำหนด KPI ของงาน		
2. สอบทานว่ามีกระบวนการในการรวบรวมข้อมูล การประเมินประสิทธิภาพการปฏิบัติงานอย่างต่อเนื่องหรือไม่	/				
3.สอบทานว่ามีการประเมินความพึงพอใจของผู้รับบริการหรือไม่	/				
4.สอบทานมีการรายงานผลการติดตามต่อผู้บริหารหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

AI2 : การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
1. สอบทานว่าองค์กรมีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการจัดหาระบบงานประยุกต์ที่องค์กรนำมาใช้หรือไม่	/		กรณีเป็นระบบงานที่มีความซับซ้อน จะใช้วิธีการว่าจ้างบุคคลภายนอกในการพัฒนาระบบงาน ซึ่งจะมีการระบุในสัญญาว่าจ้างถึงขั้น-ตอนต่าง ๆ ในการพัฒนาระบบงานตั้งแต่การออก - แบบระบบงาน การอนุมัติการออกแบบ การกำหนดความต้องการเกี่ยวกับแฟ้มข้อมูล ข้อกำหนดของโปรแกรม ความต้องการเกี่ยวกับข้อมูลนำเข้า การประมวลผล และ ผลลัพธ์		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2. สอบทานว่าองค์กรมีการกำหนดขั้นตอนวิธีปฏิบัติเกี่ยวกับการดูแลรักษาระบบงานประยุกต์ที่องค์กรนำมาใช้หรือไม่	/		มีการกำหนดขั้นตอนการเข้าถึงโปรแกรมระบบงานประยุกต์ การดูแล version ของโปรแกรมที่ใช้งานจริง		
3. สอบทานว่าองค์กรมีข้อกำหนดเกี่ยวกับความครบถ้วนถูกต้องของโปรแกรมระบบงานประยุกต์หรือไม่	/		มีการกำหนดอย่างละเอียดชัดเจนในสัญญาการจ้างบริษัทบุคคลภายนอกในการพัฒนาระบบงาน		
3. สอบทานว่ามีการทดสอบโปรแกรมระบบงานประยุกต์ด้วยวิธีการทดสอบที่เหมาะสมหรือไม่	/		มีการทดสอบโปรแกรมระบบงานประยุกต์ โดยจะมีการทดสอบโปรแกรมและระบบงานโดยเจ้าหน้าที่หน่วยงานเทคโนโลยีสาร –		

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
4. สอบทานว่าผู้ใช้ระบบงานมีส่วนร่วมในการทดสอบหรือไม่	/		สนเทศก่อน หลังจากนั้นจะมีการให้ผู้ใช้ระบบงานเข้าทดสอบระบบงานอีกครั้งหนึ่ง และก่อนจะยกเลิกระบบงานเดิมจะมีการทำงานคู่ขนานก่อนจนกว่าจะมั่นใจในความถูกต้องของโปรแกรมระบบงานใหม่		
5. สอบทานคู่มือผู้ใช้ระบบและคู่มือสนับสนุนการปฏิบัติงานว่ามีความละเอียด ชัดเจน เพียงพอหรือไม่	/				

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
6. สอบทานว่าเมื่อมีข้อขัดแย้งทางด้านเทคนิคหรือลอจิกเกิดขึ้นระหว่างการบำรุงรักษาหรือการพัฒนา การออกแบบจะถูกประเมินซ้ำอีกครั้งหนึ่ง	/				

บทที่ 5
สรุปผลการวิจัย

5.1 สรุปผลการวิจัย

การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT เกี่ยวข้องกับการศึกษารวบรวมข้อมูลเกี่ยวกับเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ความเสียหายที่อาจเกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศ และการตรวจสอบระบบเทคโนโลยีสารสนเทศ และ COBIT FRAMEWORK เพื่อนำกรอบมาตรฐานของ COBIT มาใช้เป็นแนวทางในการจัดทำแนวการตรวจสอบระบบเทคโนโลยีสารสนเทศ โดยได้พิจารณาจัดทำแนวการตรวจสอบโดยแบ่งการตรวจสอบตามโครงสร้างของมาตรฐาน COBIT บนพื้นฐานของกระบวนการทางธุรกิจ 4 กระบวนการหลัก (Domain) ได้แก่ การวางแผนและการจัดการองค์กร (PO : Planning and Organization) การจัดหาและติดตั้ง (AI : Acquisition and Implementation) การส่งมอบและบำรุงรักษา (DS : Delivery and Support) การติดตามผล (M : Monitoring) ทั้งนี้แนวการตรวจสอบระบบเทคโนโลยีสารสนเทศ (Audit Program) จะประกอบด้วย หัวข้อการตรวจสอบ วัตถุประสงค์การตรวจสอบ ความเสี่ยง การควบคุมที่ควรมี และวิธีการทดสอบ/ตรวจสอบ ซึ่งสามารถใช้เป็นเครื่องมือช่วยผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศในการปฏิบัติงานตรวจสอบ และทำให้หัวหน้าหน่วยงานตรวจสอบระบบเทคโนโลยีสารสนเทศสามารถใช้เป็นเครื่องมือในการสอบทานและควบคุมงานตรวจสอบให้สามารถดำเนินการได้บรรลุวัตถุประสงค์ของการตรวจสอบ

มาตรฐาน COBIT นั้นมีจุดประสงค์ในการสร้างความมั่นใจว่าการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศสอดคล้องกับวัตถุประสงค์เชิงธุรกิจขององค์กร (Business Objectives) เพื่อให้เกิดการใช้ทรัพยากรอย่างมีประสิทธิผลอันจะส่งประโยชน์สูงสุดแก่องค์กร ช่วยให้เกิดความสมดุลระหว่างความเสี่ยงด้านเทคโนโลยีสารสนเทศและผลตอบแทนของการลงทุนในระบบสารสนเทศ โดยมาตรฐาน COBIT มีพื้นฐานมาจาก FRAMEWORK ชั้นนำต่าง ๆ มากมาย ได้แก่ The Software Engineering Institute's Capability Maturity Model (CMM), ISO 9000, The Information Technology Infrastructure Library (ITIL) ของประเทศอังกฤษ อย่างไรก็ตาม COBIT ยังขาดในส่วนของ Guideline เพื่อใช้ในทางปฏิบัติ เนื่องจาก COBIT เป็น FRAMEWORK ที่เน้นในเรื่องของการควบคุม (Control) เป็นหลัก COBIT จะมุ่งประเด็นในการบอกว่าองค์กรต้องการอะไรบ้าง (What) แต่ไม่มีรายละเอียดในแง่ของวิธีการที่จะนำไปสู่จุดนั้น (How) ซึ่งเหมาะกับผู้

ตรวจสอบระบบเทคโนโลยีสารสนเทศที่จะนำมาตรฐาน COBIT มาใช้เพื่อทำเป็น Audit Program แต่ในกรณีผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศมีประเด็นที่พบจากการตรวจสอบ และพิจารณาข้อเสนอแนะเพื่อการปรับปรุง จะต้องนำ FRAMEWORK อื่น ๆ เข้าร่วมเพื่อเพิ่มเติมรายละเอียดของการนำไปปฏิบัติ เช่น รายละเอียดในกระบวนการของ ITIL สามารถนำไปใช้เป็นรายละเอียดในข้อเสนอแนะเพื่อการปรับปรุงหากมีประเด็นที่พบจากการตรวจสอบในกระบวนการการส่งมอบและบำรุงรักษา (DS : Delivery and Support)

5.2 อภิปรายผลการศึกษา

ผลการศึกษาพบว่า แนวการตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT ผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถนำมาใช้เป็นเครื่องมือในการปฏิบัติงานตรวจสอบ และหัวหน้าหน่วยงานตรวจสอบสามารถใช้เป็นเครื่องมือในการสอบทานและควบคุมงาน ซึ่งทำให้การตรวจสอบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างครอบคลุมตามระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร และบรรลุวัตถุประสงค์ของการตรวจสอบ อย่างไรก็ตาม รายละเอียดของการนำไปปฏิบัติในกระบวนการต่าง ๆ ในมาตรฐาน COBIT ผู้ตรวจสอบจะต้องพิจารณาข้อมูลเพิ่มเติมจาก FRAMEWORK อื่น ๆ เช่น มาตรฐาน ISO/IEC27001 ,ISO/IEC17799 ที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร, ISO/IEC 13335 ซึ่งเป็นมาตรฐานว่าด้วยแนวทางปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัย, ISO/IEC 15408 ซึ่งเป็นมาตรฐานว่าด้วยเรื่องเทคนิควิธีด้านความมั่นคงปลอดภัยซึ่งจะถูกใช้เป็นเงื่อนไขกลางหรือเกณฑ์กลาง (Common Criteria) ในการประเมินระบบในเรื่องของความมั่นคงปลอดภัย , ITIL (IT Infrastructure Library) ซึ่งเป็นแนวทางปฏิบัติว่าด้วยเรื่องเกี่ยวกับโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ซึ่ง ITIL นี้เป็นแนวทางปฏิบัติที่ดีเยี่ยม (best practice) ในการบริหารจัดการด้าน IT Service ตลอดจนเครื่องมือต่าง ๆ ที่ใช้สำหรับบริหารจัดการระบบเทคโนโลยีสารสนเทศ เช่น PRINCE2, PMBOX, TickIT, TOGAF8.1

5.3 ข้อเสนอแนะ

ผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถใช้แนวการตรวจสอบระบบเทคโนโลยีสารสนเทศเป็นเครื่องมือในการปฏิบัติงานตรวจสอบ อย่างไรก็ตาม หากสามารถรวบรวมข้อมูลเกี่ยวกับรายละเอียดการนำไปปฏิบัติสำหรับกระบวนการทางธุรกิจทั้ง 4 กระบวนการหลัก (Domain) ไม่ว่าจะเป็นกระบวนการ การวางแผนและการจัดการองค์กร (PO : Planning and Organization) การจัดหาและติดตั้ง (AI : Acquisition and Implementation) การส่งมอบและบำรุงรักษา (DS : Delivery and Support) การติดตามผล (M : Monitoring) จะช่วยให้การปฏิบัติงานตรวจสอบระบบเทคโนโลยีสารสนเทศใช้ระยะเวลาน้อยลง

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

หนังสือ

จันทนา สาขากร นิพันธ์ เห็นโชคชัยชนะ และ ศิลปะพร ศรีจั่นเพชร. (2548). **การควบคุมภายในและการตรวจสอบภายใน**. กรุงเทพฯ : ที พี เอ็น เพรส.

ตลาดหลักทรัพย์แห่งประเทศไทย. (2540). **แนวทางการจัดระบบการควบคุมภายใน**. กรุงเทพฯ : บุญศิริการพิมพ์.

ตลาดหลักทรัพย์แห่งประเทศไทยและสมาคมผู้ตรวจสอบภายในแห่งประเทศไทย. (2548) .**แนวทางการตรวจสอบภายใน** .กรุงเทพฯ : ผู้แต่ง.

ประทักษ์ วงศ์สินคงมั่น และ คณะ. (2545). **การตรวจสอบระบบงานคอมพิวเตอร์และการควบคุมภายใน**. นนทบุรี : โรงพิมพ์มหาวิทยาลัยสุโขทัยธรรมาธิราช.

เมธา สุวรรณสาร. (2545). **IT Governance**. กรุงเทพฯ : ชมรม IT ประกันภัย สมาคมประกันวินาศภัย.

วศิน เพิ่มทรัพย์ และ วิโรจน์ ชัยมูล. (2548). **ความรู้เบื้องต้นเกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศ**. กรุงเทพฯ : โปรวิชั่น.

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. (2550). **มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550.** กรุงเทพฯ : หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

ศริญญา เปี่ยมศิลป์ และ คณะ. (2547). **COBIT บทสรุปสำหรับผู้บริหาร**. กรุงเทพฯ : สถาบันเทคโนโลยีสารสนเทศาภิบาล.

สมาคมนักบัญชีและผู้สอบบัญชีรับอนุญาตแห่งประเทศไทย. **การใช้คอมพิวเตอร์ในการจัดทำและตรวจสอบบัญชี** (เอกสารประกอบการเตรียมตัวเป็นผู้สอบบัญชีรับอนุญาต). กรุงเทพฯ : พี.เอ. ลีฟวิ่ง

อภิณห์พร เมธาวัชนานนท์. (2551). **การตรวจสอบเทคโนโลยีสารสนเทศ** (เอกสารการสอน). กรุงเทพฯ : คณะวิศวกรรมศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์.

อุษณา ภัทรมนตรี. (2551). **การตรวจสอบและการควบคุมด้านคอมพิวเตอร์ทางบัญชี** . กรุงเทพฯ : จามจุรีโปรดักท์.

อุษณา ภัทรมนตรี. (2552). **การตรวจสอบภายในสมัยใหม่** . กรุงเทพฯ : จามจุรีโปรดักท์.

งานค้นคว้าอิสระ

กฤษฎา แก้วผุดผ่อง.(2551). **ระบบต้นแบบการจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศในองค์กรตามมาตรฐานสากล BS 7799 กรณีศึกษา : สำนักหอสมุด มหาวิทยาลัยมหิดล.** งานค้นคว้าอิสระปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีคอมพิวเตอร์และการสื่อสาร. กรุงเทพฯ : มหาวิทยาลัยธุรกิจบัณฑิตย์.

จตุพล จิตรพงษ์.(2548). **การตรวจสอบระบบสารสนเทศเพื่อประสิทธิผลโดยรวมขององค์กรด้านซอฟต์แวร์และฮาร์ดแวร์.** งานค้นคว้าอิสระปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ. กรุงเทพฯ : มหาวิทยาลัยเกษตรศาสตร์.

เบ็ญจมาศ ฮะยิ้ม.(2548). **การศึกษาการควบคุมภายในโดยการประเมินตนเอง (Control Self Assessment : CSA).** งานค้นคว้าอิสระปริญญามหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศและการสื่อสาร. กรุงเทพฯ : มหาวิทยาลัยหอการค้าไทย.

พิมพ์กมล ศรีสวัสดิ์. (2551). **การประเมินความเสี่ยงจากการใช้เทคโนโลยีด้วย Cobit.** งานค้นคว้าอิสระปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ. กรุงเทพฯ : มหาวิทยาลัยเกษตรศาสตร์.

อรพรรณ เชาว์สุวรรณกิจ. (2549). **การพัฒนาโมเดลและเครื่องมือสำหรับการตรวจประเมินทรัพยากรสารสนเทศ สำหรับการบริหารจัดการข้อมูลที่ดี.** งานค้นคว้าอิสระปริญญามหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ. กรุงเทพ: มหาวิทยาลัยเกษตรศาสตร์.

สารสนเทศจากสื่ออิเล็กทรอนิกส์

ดวงกมล ทรัพย์พิทยากร. (2550, กุมภาพันธ์). มาตรฐาน แนวทางปฏิบัติ และกรอบวิธีปฏิบัติต่างๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ. สืบค้นเมื่อ 31 กรกฎาคม 2552, จาก **http:/www.thaicert.org**

ปริญญา หอมเอนก. (2548). การเตรียมองค์กรให้พร้อมเข้าสู่ยุค IT Governance ด้วยมาตรฐาน Cobit และ ITIL. สืบค้นเมื่อ 23 กรกฎาคม 2552, จาก **http://www.acisonline.net**

ภาษาต่างประเทศ

BOOKS

Chambers,D.A., and Court, M.J. (1991). **Computer Auditing** (3ed). London:Pitman Publishing.

Donald A. Watne and Peter B.B. Turney. (1990). **Auditing EDP Systems**. 2nd ed. New York : Prentice Hall Internatioanl, Inc.

ประวัติผู้เขียน

ชื่อ-นามสกุล	นางภาพร ภิยโยดิลกชัย
ประวัติการศึกษา	บัญชีบัณฑิต คณะบัญชี มหาวิทยาลัยกรุงเทพ, 2532 บริหารธุรกิจบัณฑิต สาขาวิชาคอมพิวเตอร์ธุรกิจ คณะบริหารธุรกิจ มหาวิทยาลัยสยาม, 2534 นิติศาสตรบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2543 บัญชีมหาบัณฑิต คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย, 2539 นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์, 2548
สถานที่ทำงานปัจจุบัน	ผู้สอบบัญชีรับอนุญาต สำนักงานกฎหมายและการบัญชี พีพีแอนด์แอสโซซิเอทส์