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 คณะกรรมการบริษัทมีการแต่งตั้งคณะกรรมการตรวจสอบ ซึ่งประกอบด้วยกรรมการอิสระ 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

ผู้บริหารระดับต้นเป็นส่วนใหญ่เพื่อให้สามารถปฏิบัติงานประจำได้ 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

ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการประกอบธุรกิจขององค์กรสามารถแบ่งออกเป็น 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 ระบบบัญชีเงินสด รับ-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

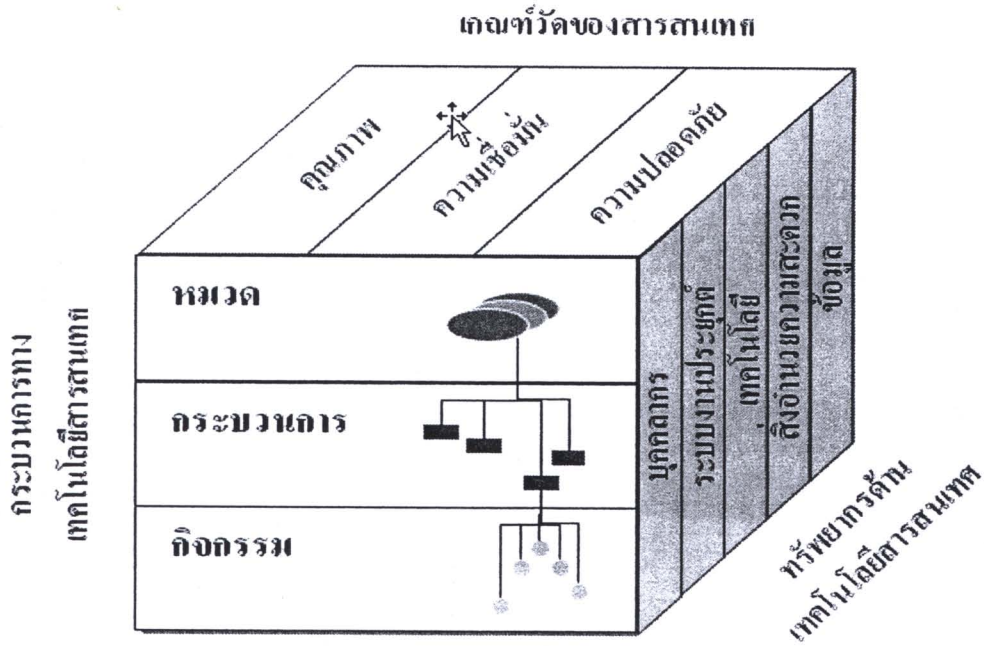
บุคลากร หมายถึง ทักษะของพนักงาน ความตื่นตัว และความมีประสิทธิภาพในการวางแผน การจัดองค์การ การจัดหา การส่งมอบ การสนับสนุน การเฝ้าติดตามระบบสารสนเทศ และการให้บริการสารสนเทศ

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

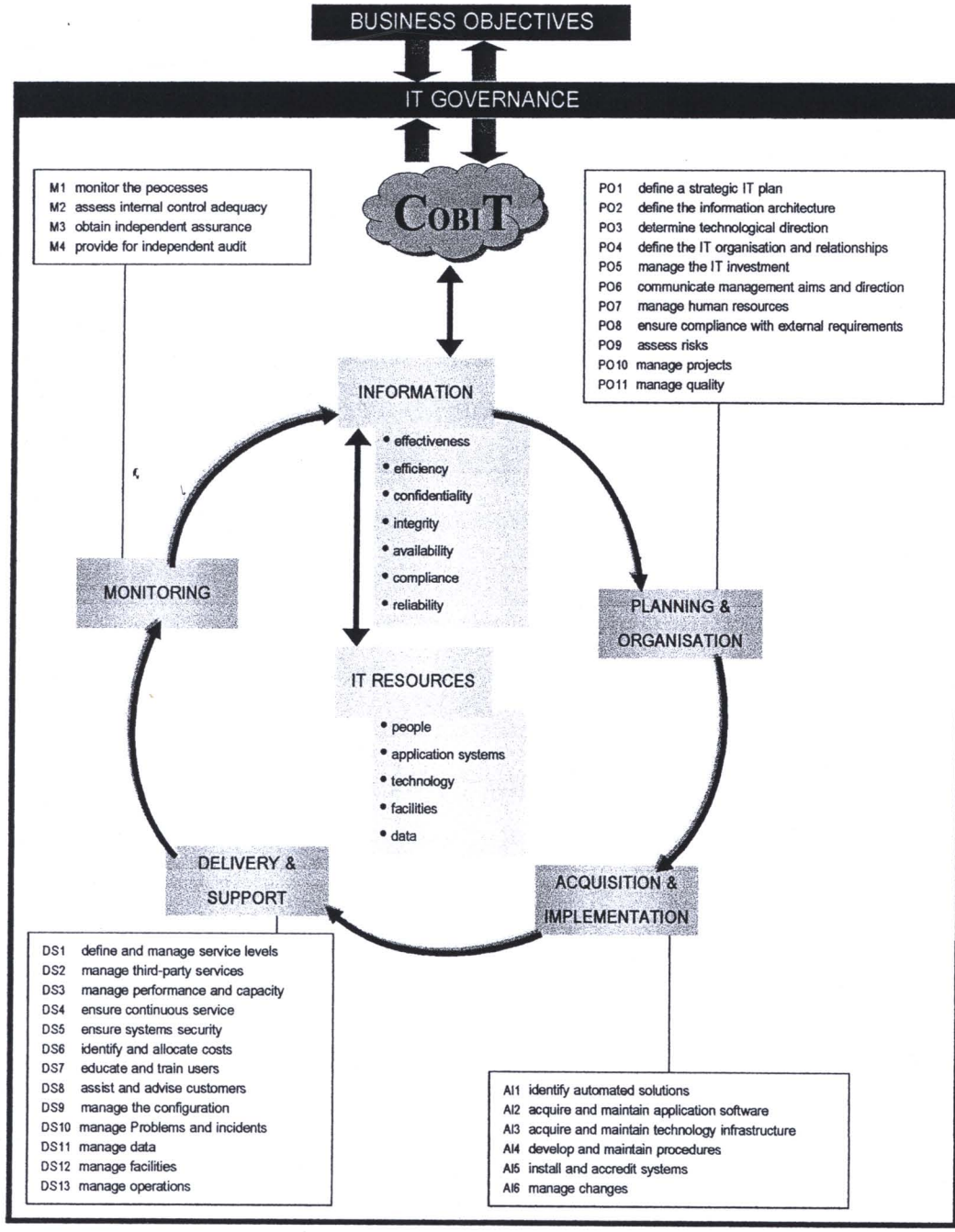
ที่มา : IT Governance Institute, 2000

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

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 องค์การจำเป็นต้องมีการจัดองค์การและ โครงสร้างพื้นฐานด้านเทคโนโลยีที่เหมาะสม 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 การปฏิบัติตามมาตรฐานด้านความปลอดภัยและสุขลักษณะในการทำงาน งาน

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 ระเบียบข้อบังคับ และข้อตกลงที่กำหนดไว้

3.6 ความเป็นอิสระในการรับรองการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ และข้อตกลงที่กำหนดไว้กับผู้ให้บริการภายนอก

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 ผู้ตรวจสอบควรรายงานเรื่องดังกล่าวต่อฝ่ายบริหาร โดยระบุไว้ในรายงานการตรวจสอบขั้นสุดท้าย 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 : สำนักหอสมุดมหาวิทยาลัยมหิดล 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 เป็นการศึกษาค้นคว้าอิสระด้วยตนเอง โดยเป็นการศึกษากระบวนการประเมินความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศ 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 ซึ่งมีแนวคิดหลักคือการลดความแปรปรวนของกระบวนการที่อาจเป็นสาเหตุของปัญหาคุณภาพ, 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