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 ระดับ โดยควรใกล้เคียงกับระดับความเสี่ยงในเรื่องนั้น 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
- พนักงานไม่ทราบเป้าหมายและทิศทางขององค์กร อาจทำให้ขาดความตระหนักในเรื่องความเสี่ยงทั้งด้านธุรกิจและด้านเทคโนโลยีสารสนเทศ	- 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 และการเลิกจ้าง เป็นต้น	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
- การดำเนินธุรกิจไม่สามารถบรรลุวัตถุประสงค์และเป้าหมายขององค์กร	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 มีการกำหนดงบประมาณ 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. สอบทานว่าองค์กรมีการกำหนดมาตรฐานของเอกสาร โปรแกรม 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
- ทรัพยากรด้านเทคโนโลยีสารสนเทศไม่มีประสิทธิภาพ 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 ความสะดวกสบาย คู่ค้าต่าง 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. สอบทานว่ามีการกำหนดระเบียบปฏิบัติในการสรุปผลโดยมีกระบวนการในการประเมินการวางแผน 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 การตรวจหา และการแก้ไขเกี่ยวกับโปรแกรมที่เป็นอันตรายต่อองค์กร 13. กำหนดโครงสร้างไฟร์วอลล์และการเชื่อมโยงกับเครือข่ายสาธารณะ 14. มีการป้องกันความเสียหายของข้อมูลอิเล็กทรอนิกส์	12. สอบทานว่ามีการป้องกัน การตรวจหา 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 การพัฒนาระบบการทดสอบ 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. มีการจัดเก็บหลักฐานการตรวจสอบและการติดตามปัญหา การตรวจสอบอย่างพอเพียงจากเหตุการณ์เพื่อหาสาเหตุของปัญหา 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 การแก้ไขข้อผิดพลาดของข้อมูลเข้าสู่ระบบ - 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. สอบทานว่าองค์กรมีการกำหนดขั้นตอนปฏิบัติในการจัดการผลลัพธ์และการจัดเก็บ การแจกจ่ายรายงาน การสอบยันและกระทบยอดรวมของรายงาน การสอบทานและการแก้ไขข้อผิดพลาดของรายงาน และมีข้อกำหนดในการรักษาความปลอดภัยของรายงานหรือไม่ 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
- การปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ไม่สามารถบรรลุเป้าหมายการปฏิบัติงานตามที่กำหนด	1. มีกระบวนการในการกำหนดตัวชี้วัดประสิทธิภาพที่เกี่ยวข้อง 2. มีกระบวนการในการรวบรวมข้อมูล การประเมินประสิทธิภาพการปฏิบัติงานอย่างต่อเนื่อง 3. มีการประเมินความพึงพอใจของผู้รับบริการ เพื่อระบุระดับการให้บริการและตั้งวัตถุประสงค์ในการพัฒนา 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

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	ผลการ ตรวจสอบ		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	ผลการ ตรวจสอบ		บันทึกผลการ ตรวจสอบ	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	ผลการ ตรวจสอบ		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		บันทึกผลการ ตรวจสอบ	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	ผลการตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
2.5 มีการใช้และติดตามประเมินการใช้งานโปรแกรมอรรถประโยชน์หรือไม่ 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	ผลการ ตรวจสอบ		บันทึกผลการ ตรวจสอบ	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 ตลอดจนระบบงานไม่สามารถทำงานได้	องค์กรควรจัดทำนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เพื่อก่อให้เกิดความปลอดภัยกับข้อมูลและระบบเทคโนโลยีสารสนเทศของบริษัท โดยพิจารณาถึงความซับซ้อนของการประมวลผล ต้นทุนและประโยชน์ที่จะได้รับ ทั้งนี้ขอบเขตและเนื้อหาของนโยบายเมื่อจัดทำแล้วควรจะสื่อสารกับหน่วยงานที่เกี่ยวข้องอย่างชัดเจน รายละเอียดสำคัญในนโยบายการรักษา

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการ ตรวจสอบ		บันทึกของผู้ตรวจสอบ	ผลกระทบ	ข้อเสนอแนะ
	มี	ไม่มี			
					ความปลอดภัยระบบเทคโนโลยีสารสนเทส ควรประกอบด้วย ข้อตกลงหรือการสนับสนุนของผู้บริหาร, หลักการเข้าถึงข้อมูล เช่น การเข้าถึงข้อมูลในระบบควรใช้เกณฑ์จำเป็นต้องทำหรือจำเป็นต้องรู้, การสอบทานการให้สิทธิการเข้าถึง โดยการควบคุมการเข้าถึงควรถูกประเมินอย่างสม่ำเสมอ, ความตระหนักเรื่องการรักษาความปลอดภัย, บทบาทของเจ้าหน้าที่บริหารความปลอดภัย คณะกรรมการด้าน

ตารางที่ 4.36 (ต่อ)

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

ตารางที่ 4.36 (ต่อ)

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

ตารางที่ 4.36 (ต่อ)

ทดสอบ/ตรวจสอบ	ผลการตรวจสอบ		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	/				

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