สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์
Federation of Accounting Professions
Under the Royal Patronage of His Majesty the King

บทที่ 2 เรื่อง การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

(เอกสารประกอบการเตรียมตัวเป็นผู้สอบบัญชีรับอนุญาต)

โดย วันชัย พิทักษ์กรณ์
คณะผู้ทรงคุณวุฒิเกี่ยวกับการทดสอบการปฏิบัติงานสอบบัญชี
ด้านการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์
สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

บทที่ 2
เรื่อง การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

โดย วันชัย พิทักษ์กรณ์
คณะผู้ทรงคุณวุฒิเกี่ยวกับการทดสอบการปฏิบัติงานสอบบัญชี
ด้านการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์
สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

สารบัญ

หน้า

2. วัตถุประสงค์ในการศึกษา

เมื่อได้ศึกษาเนื้อหาของบทนี้แล้ว ผู้ศึกษาควรมีความเข้าใจถึง

1. ความหมายและวัตถุประสงค์ของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ
2. ขั้นตอนและการควบคุมด้านการกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานเทคโนโลยีสารสนเทศ
3. ขั้นตอนและการควบคุมด้านการพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ
4. ขั้นตอนและการควบคุมด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ
5. ขั้นตอนและการควบคุมด้านการปฏิบัติการคอมพิวเตอร์
6. ขั้นตอนและการควบคุมด้านการบริหารข้อมูล
7. ผลกระทบจากการขาดการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ
8. หลักการและขั้นตอนการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

4. คำนำ

ในยุคที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญในการขับเคลื่อนองค์กรและธุรกิจ และการจัดทำรายงานทางการเงิน ดังนั้นการจัดการและควบคุมเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพจึงเป็นสิ่งจำเป็น ซึ่งการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ (Information Technology General Control : ITGC) นั้นถือว่าเป็นพื้นฐานสำคัญของการควบคุมเทคโนโลยีสารสนเทศ ที่มีผลต่อประสิทธิผลของการควบคุมระบบงาน (Application Control) และมีผลต่อความน่าเชื่อถือของข้อมูลและรายงานทางการเงินขององค์กร

บทนี้มีวัตถุประสงค์เพื่อให้ความรู้และแนวทางในการจัดให้มีการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่ดี ของกิจกรรมควบคุมในกระบวนการต่าง ๆ ด้านเทคโนโลยีสารสนเทศที่มีส่วนเกี่ยวข้องกับความน่าเชื่อถือของข้อมูลและรายงานทางการเงิน ซึ่งประกอบด้วย การกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานด้านเทคโนโลยีสารสนเทศ การพัฒนาระบบงานและการเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ การรักษาความปลอดภัยเทคโนโลยีสารสนเทศ การปฏิบัติการคอมพิวเตอร์ และการบริหารจัดการข้อมูล โดยแต่ละกระบวนการ จะเป็นการอธิบายถึง ความรู้ทั่วไป และรายละเอียดของ ความเสี่ยง การควบคุม และการตรวจสอบของกิจกรรมนั้น ๆ

ในบทนี้ยังมีการอธิบายเพิ่มเติมในส่วนของผลกระทบจากการขาดการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่ดี และแนวทางในการประเมินผลกระทบดังกล่าว ตลอดจนการยกตัวอย่างข้อบกพร่องของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่อาจมีผลกระทบต่อรายงานทางการเงิน

ในส่วนสุดท้ายของบทนี้ เป็นการอธิบายหลักการและแนวทางการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ ซึ่งเป็นแนวทางการตรวจสอบที่สอดคล้องกับการตรวจสอบแบบอิงกับความเสี่ยง (Risk-Based Audit Approach)

3. ความหมายและวัตถุประสงค์ของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ (Information Technology General Control) หมายถึง การควบคุมที่เกี่ยวข้องกับกระบวนการด้านเทคโนโลยีสารสนเทศของกิจการที่ช่วยสนับสนุนให้เกิดการทำงานของสภาพแวดล้อมทางเทคโนโลยีสารสนเทศที่เหมาะสมอย่างต่อเนื่อง ซึ่งรวมถึงการทำหน้าที่อย่างมีประสิทธิผลอย่างต่อเนื่องของการควบคุมการประมวลผลเทคโนโลยีสารสนเทศและบูรณภาพของเทคโนโลยีสารสนเทศ (นั่นคือ ความครบถ้วน ความถูกต้องและความสมเหตุสมผลของเทคโนโลยีสารสนเทศ) ในระบบเทคโนโลยีสารสนเทศของกิจการโดยไม่ได้เฉพาะเจาะจงว่าเป็นการควบคุมระบบงานใด (Application Control)

การควบคุมทั่วไปเป็นกิจกรรมการควบคุมที่อยู่ในความรับผิดชอบของผู้บริหารเทคโนโลยีสารสนเทศ และผู้บริหารระดับสูงและส่วนใหญ่เป็นกระบวนการทำงานในฝ่ายเทคโนโลยีสารสนเทศ โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าการดำเนินการด้านเทคโนโลยีสารสนเทศสามารถตอบสนองต่อความต้องการด้านเทคโนโลยีสารสนเทศโดยรวมขององค์กร ซึ่งประกอบด้วยความต้องการด้านประสิทธิภาพและประสิทธิผลของการดำเนินงาน (Efficiency and Effectiveness) ความปลอดภัยของข้อมูลและเทคโนโลยีสารสนเทศ (Security and Confidentiality) ความถูกต้องครบถ้วนของข้อมูล (Integrity) หรือความพร้อมใช้ของข้อมูลและเทคโนโลยีสารสนเทศ (Availability)

อย่างไรก็ตามวัตถุประสงค์ของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับความน่าเชื่อถือของข้อมูลทางการเงินจะประกอบด้วย ความปลอดภัยของข้อมูล (Confidentiality) ความถูกต้องครบถ้วนของข้อมูล (Integrity) และความพร้อมใช้ของข้อมูลและเทคโนโลยีสารสนเทศ (Availability)

ดังนั้นการควบคุมทั่วไปของเทคโนโลยีสารสนเทศเฉพาะส่วนที่เกี่ยวกับความน่าเชื่อถือของข้อมูลทางการเงินประกอบด้วยกิจกรรมการควบคุมในกระบวนการต่าง ๆ ด้านเทคโนโลยีสารสนเทศที่สำคัญ ดังต่อไปนี้

3.1. การกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานเทคโนโลยีสารสนเทศ

3.2. การพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ

3.3. การรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

3.4. การปฏิบัติการคอมพิวเตอร์

3.5. การบริหารจัดการข้อมูล

หมายเหตุ : การควบคุมทั่วไปของเทคโนโลยีสารสนเทศข้างต้นไม่ได้รวมการควบคุมด้านการวางแผนเพื่อกู้เทคโนโลยีสารสนเทศ ในกรณีที่เกิดความเสียหายรุนแรงต่อเทคโนโลยีสารสนเทศไว้ด้วย เนื่องจากเป็นการควบคุมที่ไม่เกี่ยวข้องกับความน่าเชื่อถือของข้อมูลทางการเงิน

3.1 การกำหนดนโยบาย การวางแผน และการจัดโครงสร้างงานเทคโนโลยีสารสนเทศ

การกำหนดนโยบายในภาพรวมของการใช้เทคโนโลยีสารสนเทศ และการจัดทำแผนงานด้านเทคโนโลยีสารสนเทศเป็นการดำเนินการเพื่อให้มั่นใจว่า การใช้งานเทคโนโลยีสารสนเทศสอดคล้องกับหลักการควบคุมที่ดี และแผนงานด้านเทคโนโลยีสารสนเทศสอดคล้องกับแผนงานทางธุรกิจ กล่าวคือแผนงานเทคโนโลยีสารสนเทศนั้นมีส่วนสนับสนุนกิจกรรมต่าง ๆ ขององค์กรในการทำให้องค์กรบรรลุถึงวัตถุประสงค์และเป้าหมาย

การจัดโครงสร้างงานเทคโนโลยีสารสนเทศมุ่งเน้นด้านการแบ่งแยกหน้าที่งานเทคโนโลยีสารสนเทศและการกำหนดหน้าที่ความรับผิดชอบของฝ่ายงานเทคโนโลยีสารสนเทศที่ชัดเจน เพื่อเป็นพื้นฐานที่สำคัญในการจัดให้มีการควบคุมที่ดี และเพื่อเอื้อให้เกิดการบริหารงานเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ ในการแบ่งแยกหน้าที่งานเทคโนโลยีสารสนเทศนั้น เป็นทั้งการแบ่งแยกงานระหว่างฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายธุรกิจ รวมทั้งการแบ่งแยกงานเทคโนโลยีสารสนเทศในฝ่ายเทคโนโลยีสารสนเทศเอง

3.2 การพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ

การควบคุมในส่วนนี้เป็นการควบคุมกระบวนการพัฒนาระบบงานเพื่อให้มั่นใจว่าระบบงานที่พัฒนาขึ้นมาเพื่อใช้ในการประมวลผลข้อมูลต่าง ๆ ในองค์กรนั้น มีความสอดคล้องกับวัตถุประสงค์ในการใช้เทคโนโลยีสารสนเทศ และระบบที่นำมาใช้งานนั้นทำงานอย่างถูกต้องครบถ้วนตามเงื่อนไขหรือความต้องการขององค์กร

การควบคุมในส่วนนี้ยังรวมถึงการเปลี่ยนแปลงแก้ไขระบบงานต่าง ๆ หลังจากมีการใช้ระบบงานนั้น ๆ แล้ว เพื่อให้มั่นใจว่าการเปลี่ยนแปลงเทคโนโลยีสารสนเทศ มีการดำเนินการอย่างเหมาะสม และการเปลี่ยนแปลงนั้นมีการอนุมัติให้ดำเนินการจากผู้มีอำนาจตลอดจนมีการทดสอบการเปลี่ยนแปลงก่อนการนำระบบงานหรือโปรแกรมใหม่มาใช้งาน

3.3 การรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

การควบคุมที่มีความสำคัญมากอีกส่วนหนึ่งก็คือการควบคุมด้านความปลอดภัยเทคโนโลยีสารสนเทศ ในส่วนนี้ประกอบด้วยการบริหารจัดการด้านความปลอดภัยที่ดี เช่น การกำหนดนโยบายด้านความปลอดภัย การกำหนดระเบียบปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับความปลอดภัย และกระบวนการการให้ความรู้ในการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัยต่อผู้ใช้งานเทคโนโลยีสารสนเทศ

การควบคุมในส่วนนี้ยังรวมถึงการควบคุมความปลอดภัยทางกายภาพของเทคโนโลยีสารสนเทศ การเข้าถึงห้องหรือศูนย์คอมพิวเตอร์และอุปกรณ์ที่สำคัญ รวมทั้งการจัดให้มีสภาพแวดล้อมในการทำงานที่ดีของเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ตั้งแต่การควบคุมอุณหภูมิความชื้นคลื่นแม่เหล็กและฝุ่นละออง เป็นต้น

การควบคุมในส่วนสุดท้ายด้านการรักษาความปลอดภัยคือการควบคุมเชิงตรรกะ (Logical Security) หรืออีกนัยหนึ่งคือการรักษาความปลอดภัยข้อมูลและโปรแกรมต่าง ๆ ที่จัดเก็บหรือประมวลผลอยู่ในระบบคอมพิวเตอร์ และระบบเครือข่าย ซึ่งการควบคุมส่วนใหญ่เป็นการควบคุมทางเทคนิคของระบบปฏิบัติการคอมพิวเตอร์ ระบบจัดการฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์

3.4 การปฏิบัติการคอมพิวเตอร์

ในส่วนของการควบคุมการปฏิบัติการคอมพิวเตอร์นั้น เป็นการควบคุมเพื่อให้การดำเนินการใด ๆ เกี่ยวกับระบบคอมพิวเตอร์ตั้งแต่การเปิด ปิดเครื่อง บำรุงรักษาและแก้ไขปัญหาต่าง ๆ การประมวลผลสิ้นวัน การสำรองข้อมูล และการจัดพิมพ์รายงานเพื่อให้การดำเนินการต่าง ๆ ดังที่กล่าวมาแล้วดำเนินการอย่างมีประสิทธิภาพและประสิทธิผล โดยมีการกำหนดระเบียบปฏิบัติที่ชัดเจนและมีการสอบทานให้การดำเนินการเป็นไปตามระเบียบดังกล่าว

3.5 การบริหารจัดการข้อมูล

การบริหารจัดการข้อมูลเทคโนโลยีสารสนเทศนั้น ประกอบด้วยการกำหนดโครงสร้างข้อมูลขององค์กรและผู้รับผิดชอบข้อมูลที่ชัดเจน การแบ่งประเภทข้อมูลตามความสำคัญของข้อมูล การบริหารด้านความถูกต้อง ความครบถ้วนของข้อมูล การจัดเก็บข้อมูลและการนำข้อมูลไปใช้งาน โดยมีวัตถุประสงค์เพื่อให้องค์กรมีการใช้ข้อมูลที่ถูกต้องครบถ้วน และตรงกับความต้องการในการใช้ข้อมูลของทุกส่วนในองค์กร

5. การกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานเทคโนโลยีสารสนเทศ

ในส่วนนี้จะอธิบายถึง ความรู้ทั่วไป ความเสี่ยง การควบคุม และการตรวจสอบ ที่เกี่ยวข้องกับการกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานเทคโนโลยีสารสนเทศ รวมถึงผลกระทบที่อาจเกิดขึ้นจากการที่การควบคุมมีข้อบกพร่อง ดังต่อไปนี้

5.1 การกำหนดนโยบายเทคโนโลยีสารสนเทศ

5.1.1 ความรู้ทั่วไป

เนื่องจากเทคโนโลยีสารสนเทศมีส่วนเกี่ยวข้องกับบุคลากรทุกระดับภายในองค์กร ตั้งแต่ผู้บริหารระดับสูง ผู้บริหารและบุคลากรในสายงานต่าง ๆ ผู้บริหารและบุคลากรในฝ่ายเทคโนโลยีสารสนเทศ ในฐานะที่เป็นทั้งผู้ใช้งานโดยตรง และผู้พัฒนาและผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศ การใช้งานเทคโนโลยีสารสนเทศ เป็นไปในแนวทางเดียวกัน องค์กรจึงจำเป็นจะต้องกำหนดให้มีนโยบายที่เกี่ยวกับเทคโนโลยีสารสนเทศ ซึ่งประกอบด้วย

- นโยบายด้านการใช้เทคโนโลยีสารสนเทศโดยรวม
- นโยบายด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ
- นโยบายด้านการพัฒนา เปลี่ยนแปลง และนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้
- นโยบายด้านมาตรฐานของเทคโนโลยีสารสนเทศ ที่จะนำมาใช้กับองค์กร
- นโยบายด้านการกู้คืนเทคโนโลยีสารสนเทศ ในกรณีเกิดความเสียหายรุนแรงต่อเทคโนโลยีสารสนเทศ

นโยบายด้านต่าง ๆ ที่กล่าวมาข้างต้น สามารถจัดทำเป็นนโยบายฉบับรวม หรือแยกเป็นนโยบายแต่ละด้าน ทั้งนี้ขึ้นอยู่กับความเหมาะสมของแต่ละองค์กร

ในการบริหารจัดการที่ดีเกี่ยวกับนโยบายด้านเทคโนโลยีสารสนเทศนั้น องค์กรจะต้องจัดให้มีการบริหารนโยบายที่ดี ซึ่งประกอบด้วย

5.1.1.1 การอนุมัติเพื่อบังคับใช้

ผู้บริหารระดับสูงขององค์กรควรเป็นผู้อนุมัตินโยบายดังกล่าว และควรมีการประกาศใช้อย่างเป็นทางการ

5.1.1.2 การสื่อสารเพื่อให้ความรู้และความเข้าใจ

จัดให้มีการอบรมให้ผู้ที่มีส่วนเกี่ยวข้องรับรู้และเข้าใจในหน้าที่และความรับผิดชอบของแต่ละคนอย่างสม่ำเสมอ ในบางกรณีจำเป็นต้องมีการบันทึกแสดงการรับรู้ของผู้ที่มีส่วนเกี่ยวข้อง เช่น จัดให้มีการลงนามรับทราบ และยินยอมปฏิบัติตามแนวทางที่กำหนดไว้ในนโยบาย เป็นต้น

5.1.1.3 การติดตามการปฏิบัติตามนโยบายฯ

จัดให้มีการติดตามการปฏิบัติงานเพื่อให้มั่นใจว่ามีการปฏิบัติตามนโยบายอย่างเคร่งครัด และมีการลงโทษในกรณีที่มีบุคลากรไม่ปฏิบัติแนวทางที่กำหนดไว้ในนโยบายฯ อย่างเหมาะสม

5.1.1.4 การสอบทานและปรับปรุงนโยบายฯ

เนื่องจากเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงที่ค่อนข้างรวดเร็ว ดังนั้นควรมีการสอบทานความทันสมัยและความเหมาะสมของนโยบายอย่างสม่ำเสมอ เช่น อย่างน้อยปีละครั้ง หรือเมื่อมีการนำเทคโนโลยีสารสนเทศใหม่มาใช้ภายในองค์กร

5.1.2 ความเสี่ยง การควบคุม และการตรวจสอบ

ในส่วนนี้เป็นการอธิบายถึงความเสี่ยง การควบคุมความเสี่ยง และการตรวจสอบเพื่อให้มั่นใจถึงประสิทธิภาพและประสิทธิผลของการควบคุมในการจัดการความเสี่ยง ด้านการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ

ความเสี่ยง	การควบคุม	การตรวจสอบ
การดำเนินงาน และการใช้งานด้านเทคโนโลยีสารสนเทศอาจไม่เป็นไปในแนวทางเดียวกัน	มีการกำหนดและอนุมัตินโยบายที่ชัดเจนในด้านการดำเนินงาน และการใช้งานเทคโนโลยีสารสนเทศ	• สอบถามถึงความมีอยู่จริงของนโยบายฯ • สอบทานนโยบายฯ เพื่อให้มั่นใจว่าครอบคลุมการดำเนินการและการใช้งานเทคโนโลยีสารสนเทศอย่างเหมาะสม และมีการอนุมัติเพื่อบังคับใช้โดยผู้บริหารระดับสูง
บุคลากรอาจขาดการรับรู้ และเข้าใจในแนวทางการปฏิบัติตามที่กำหนดไว้ในนโยบาย	• มีแผนการสื่อสารและอบรมให้บุคลากรที่เกี่ยวข้องทราบและเข้าใจแนวทางการปฏิบัติงานตามนโนบายฯ และมีการติดตามการปฏิบัติตามแผนสื่อสารและแผนอบรม • มีการสำรวจอัตราการรับรู้และเข้าใจในนโยบายฯ อย่างสม่ำเสมอ	• สอบทานแผนการสื่อสารและการอบรมเพื่อให้มั่นใจว่าครอบคลุมบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างครบถ้วนและเหมาะสม • ตรวจสอบการติดตามการปฏิบัติงานตามแผน เพื่อให้มั่นใจว่ามีการติดตามอย่างสม่ำเสมอ
เทคโนโลยีสารสนเทศที่นำมาใช้งานอาจไม่มีความสอดคล้องกัน	• มีการกำหนดมาตรฐานด้านเทคโนโลยีสารสนเทศที่จะนำมาใช้กับองค์กร • มีการทบทวนมาตรฐานอย่างสม่ำเสมอ	• สอบทานความเหมาะสมของมาตรฐานด้านเทคโนโลยีสารสนเทศ • ตรวจสอบเพื่อให้มั่นใจว่ามีการทบทวนมาตรฐานอย่างสม่ำเสมอ

5.2 การวางแผนงานเทคโนโลยีสารสนเทศ

5.2.1 ความรู้ทั่วไป

การจัดทำแผนงานด้านเทคโนโลยีสารสนเทศเป็นการดำเนินการเพื่อกำหนดแนวทางการลงทุน และกิจกรรมต่าง ๆ ที่องค์กรจำเป็นต้องดำเนินการ เพื่อสนับสนุนการดำเนินธุรกิจ และช่วยให้องค์กรบรรลุถึงวัตถุประสงค์และเป้าหมายขององค์กร การวางแผนงานด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์ของการควบคุมเพื่อ

- ให้มั่นใจว่ากลยุทธ์และแผนการดำเนินงานด้านเทคโนโลยีสารสนเทศ สอดคล้องและสนับสนุนวัตถุประสงค์ เป้าหมายและกลยุทธ์ทางธุรกิจขององค์กร
- เพื่อให้การทำงานโดยรวมของเทคโนโลยีสารสนเทศ ทำงานสอดประสานกันอย่างเป็นบูรณาการ และมีประสิทธิภาพสูงสุด
- เพื่อให้มีการสื่อสารและทำความเข้าใจต่อแผนงานเทคโนโลยีสารสนเทศให้กับบุคคลหรือหน่วยงานที่เกี่ยวข้องอย่างชัดเจน
- เพื่อให้มีการติดตามการปฏิบัติตามแผนงานอย่างสม่ำเสมอ

ดังมีแนวทางการควบคุมดังต่อไปนี้

5.2.1.1 การกำหนดผู้รับผิดชอบในการวางแผนงานด้านเทคโนโลยีสารสนเทศ

5.2.1.2 จัดให้มีกระบวนการการวางแผนงานเทคโนโลยีสารสนเทศ

5.2.1.3 การอนุมัติ การสื่อสารและควบคุมแผนงานเทคโนโลยีสารสนเทศ

5.2.1.4 การติดตามการดำเนินงานตามแผนฯ

5.2.1.1 การกำหนดผู้รับผิดชอบในการวางแผนงานด้านเทคโนโลยีสารสนเทศ

ในการวางแผนงานด้านเทคโนโลยีสารสนเทศนั้นมิใช่เป็นความรับผิดชอบเฉพาะผู้บริหารงานเทคโนโลยีสารสนเทศเท่านั้น ทั้งนี้เพราะการใช้เทคโนโลยีสารสนเทศเป็นการใช้งานโดยรวมเพื่อก่อให้เกิดประโยชน์สูงสุดต่อองค์กร โดยเฉพาะอย่างยิ่งเพื่อทำให้บทบาทที่สำคัญของเทคโนโลยีสารสนเทศ ในการสนับสนุนให้กิจกรรมทางธุรกิจดำเนินการอย่างมีประสิทธิภาพและประสิทธิผล และก่อให้เกิดสินค้าและการบริการที่ทันสมัย เพื่อทำให้องค์กรมีความได้เปรียบในการแข่งขัน ดังนั้นผู้ที่รับผิดชอบในการวางแผนงานเทคโนโลยีสารสนเทศควรเริ่มตั้งแต่ผู้บริหารระดับสูง ผู้บริหารสายงานธุรกิจต่าง ๆ และผู้บริหารงานเทคโนโลยีสารสนเทศ ซึ่งสามารถสรุปบทบาทหน้าที่ได้ดังนี้

- ผู้บริหารระดับสูง เป็นผู้รับผิดชอบหลักในการกำหนดแนวทางและกลยุทธ์ในการใช้เทคโนโลยีสารสนเทศสนับสนุนวัตถุประสงค์ เป้าหมายและกลยุทธ์โดยรวมขององค์กร
- ผู้บริหารสายงานต่าง ๆ รับผิดชอบในการศึกษาและให้ข้อมูลเกี่ยวกับการนำเทคโนโลยีสารสนเทศมาใช้ให้เกิดประโยชน์ในสายงานธุรกิจที่ตัวเองเป็นผู้รับผิดชอบ รวมทั้งให้ข้อมูลเกี่ยวกับการดำเนินธุรกิจต่อผู้บริหารเทคโนโลยีสารสนเทศเพื่อนำไปใช้ประกอบการจัดทำแผนงานเทคโนโลยีสารสนเทศในรายละเอียด
- ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ รับผิดชอบในการจัดทำแผนงานในรายละเอียด สำหรับการดำเนินงานด้านต่าง ๆ เกี่ยวกับเทคโนโลยีสารสนเทศ นอกจากนี้ยังมีหน้าที่ในการให้ความรู้ต่อผู้บริหารสายงานต่าง ๆ เกี่ยวกับเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการดำเนินกิจการของธุรกิจขององค์กร

5.2.1.2 จัดให้มีกระบวนการวางแผนงานเทคโนโลยีสารสนเทศ

การวางแผนงานเทคโนโลยีสารสนเทศนั้นมีวัตถุประสงค์เพื่อจัดให้มีแผนการดำเนินการด้านเทคโนโลยีสารสนเทศที่ตอบสนองต่อความต้องการทางธุรกิจ ขั้นตอนสำคัญในการวางแผนงานด้านเทคโนโลยีสารสนเทศแสดงไว้ในภาพข้างล่างนี้

ภาพที่ 2.1 กระบวนการวางแผนงานเทคโนโลยีสารสนเทศ

การวางแผนควรเริ่มจากการทำความเข้าใจต่อกลยุทธ์วัตถุประสงค์และเป้าหมายทางธุรกิจ และทำการกำหนดลักษณะของระบบข้อมูล ระบบงานเทคโนโลยี โครงสร้างงานและบุคลากรที่จำเป็นต่อการดำเนินการเพื่อให้บรรลุถึงวัตถุประสงค์ดังกล่าว ซึ่งต้องคำนึงถึงเทคโนโลยีใหม่ ๆ ที่สามารถนำเข้ามาใช้ในอนาคตด้วย หรือการประมวลผลข้อมูลใดบ้าง โดยกำหนดให้เป็นเทคโนโลยีสารสนเทศเป้าหมาย

จากนั้นเป็นการทำความเข้าใจต่อระบบสารสนเทศที่มีอยู่ในปัจจุบันว่า ระบบข้อมูล ระบบงาน เทคโนโลยี โครงสร้างงานและบุคลากร มีลักษณะและรายละเอียดอย่างไร

จากนั้นก็เริ่มดำเนินการวิเคราะห์ความแตกต่าง ระหว่างระบบเป้าหมายกับระบบปัจจุบัน ว่ามีความแตกต่างกันอย่างไร เพื่อนำมากำหนดเป็นกิจกรรมเพื่อแปลงจากระบบปัจจุบันเป็นระบบที่ควรเป็นในอนาคต ซึ่งอาจเป็นกิจกรรมในการพัฒนาระบบงานใหม่ การติดตั้งเทคโนโลยีใหม่ หรือการพัฒนาศักยภาพของบุคลากร เป็นต้น

สุดท้ายเป็นการรวบรวมกิจกรรมต่าง ๆ มาจัดทำเป็นแผนการดำเนินงานด้านเทคโนโลยีสารสนเทศ ซึ่งควรครอบคลุมแผนการดำเนินการด้านระบบข้อมูล ระบบงาน เทคโนโลยี และโครงสร้างงานและบุคลากรอย่างครบถ้วน

5.2.1.3 การอนุมัติ การสื่อสารและควบคุมแผนงานเทคโนโลยีสารสนเทศ

เมื่อจัดทำแผนงานเสร็จเรียบร้อยแล้ว ควรจัดให้มีการอนุมัติแผนงานอย่างเป็นทางการ ซึ่งในขั้นตอนการอนุมัตินั้นควรประกอบด้วยความเห็นชอบของทั้งผู้บริหารระดับสูง และผู้บริหารเทคโนโลยีสารสนเทศ ซึ่งในกรณีที่องค์กรมีคณะกรรมการเทคโนโลยีสารสนเทศก็ควรให้คณะกรรมการชุดดังกล่าวเป็นผู้อนุมัติแผน แต่ถ้าไม่มีคณะกรรมการฯ ก็ควรให้ผู้บริหารระดับสูงเป็นผู้อนุมัติ

ลำดับถัดมาคือการสื่อสารเพื่อทำความเข้าใจกับผู้ที่เกี่ยวข้องกับการดำเนินการตามแผนฯ ซึ่งรวมทั้งผู้บริหารฝ่ายเทคโนโลยีสารสนเทศต่าง ๆ และผู้บริหารสายงานธุรกิจที่เกี่ยวข้อง

ในระหว่างการดำเนินการตามแผนงานนั้นก็จะต้องจัดให้มีการติดตามความคืบหน้าและจัดทำสรุปการดำเนินการเพื่อรายงานให้ผู้บริหารในแต่ละระดับ เช่นผู้บริหารเทคโนโลยีสารสนเทศและผู้บริหารระดับสูงเพื่อติดตามให้การดำเนินการเป็นไปตามแผนงานที่กำหนด

5.2.1.4 การติดตามการดำเนินงานตามแผนงานเทคโนโลยีสารสนเทศ

ควรมีการติดตามการดำเนินงานตามแผนงานอย่างสม่ำเสมอและประเมินเปรียบเทียบผลสำเร็จของแผนงานตามเป้าหมายที่กำหนดไว้ สำหรับในส่วนที่การดำเนินงานไม่เป็นไปตามแผนงาน ก็ควรมีการดำเนินการแก้ไขหรือปรับปรุง หรือระบุสาเหตุที่ชัดเจน

5.2.2 ความเสี่ยง การควบคุม และการตรวจสอบ

ในส่วนนี้เป็นการอธิบายถึงความเสี่ยง การควบคุมความเสี่ยง และการตรวจสอบเพื่อให้มั่นใจถึงประสิทธิภาพและประสิทธิผลของการควบคุมในการจัดการความเสี่ยง ด้านการวางแผนงานด้านเทคโนโลยีสารสนเทศ

ความเสี่ยง	การควบคุม	การตรวจสอบ
เทคโนโลยีสารสนเทศ ที่นำมาใช้งานนั้นอาจไม่สามารถทำงานแบบบูรณการ (Integrated) ที่สมบูรณ์ เพราะขาดการกำหนดกรอบหรือแนวทางในการนำเทคโนโลยีสารสนเทศ มาใช้งานที่ชัดเจน กล่าวคือ มีการนำระบบมาใช้งานตามความต้องการในแต่ละครั้งคราว ซึ่งมีแนวโน้มว่าการนำระบบดังกล่าวมาใช้งานนั้น อาจไม่ได้คำนึงถึงการทำงานที่ต้องเชื่อมโยงกันกับระบบงานอื่น ๆ ที่มีอยู่ และอาจทำให้เกิดผลกระทบกับการบริหารจัดการข้อมูลโดยรวมของเทคโนโลยีสารสนเทศ	• มีการสอบทานแผนงานเพื่อให้มั่นใจว่าแผนงานด้านเทคโนโลยีสารสนเทศนั้นสอดคล้องกับสถาปัตยกรรมด้านเทคโนโลยีสารสนเทศที่คำนึงถึงการบูรณาการกันระหว่างระบบงานต่าง ๆ และเทคโนโลยีที่จะนำมาใช้ในองค์กร • มีการอนุมัติแผนงานด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม เช่น มีผู้บริหารระดับสูงเป็นผู้อนุมัติแผนงานเทคโนโลยีสารสนเทศ	• ตรวจสอบเพื่อให้มั่นใจว่ามีการสอบทานแผนและเปรียบเทียบ ความสอดคล้องกันของแผนงาน กับสถาปัตยกรรมเทคโนโลยีสารสนเทศขององค์กร • ตรวจสอบเพื่อให้มั่นใจว่าแผนงานด้านเทคโนโลยีสารสนเทศ ได้รับการอนุมัติอย่างเหมาะสม
บุคลากรที่เกี่ยวข้องกับแผนงานด้านเทคโนโลยีสารสนเทศ อาจขาดการรับรู้และเข้าใจในแผนงาน	• มีการสื่อสารให้ผู้ที่เกี่ยวข้องในการดำเนินการตามแผนงานให้รับรู้ในแผนงานที่เกี่ยวข้อง เพื่อเตรียมการดำเนินการตามแผนงานด้านเทคโนโลยีสารสนเทศ	• สอบทานแผนการสื่อสารแผนงานด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าครอบคลุมบุคลากรที่เกี่ยวข้องกับการดำเนินงานตามแผนงานเทคโนโลยีสารสนเทศอย่างครบถ้วนและเหมาะสม
การดำเนินงานไม่เป็นไปตามแผนงานด้านเทคโนโลยีสารสนเทศ	• มีกระบวนการติดตามการดำเนินการตามแผนงานด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ • มีการแก้ไขปรับปรุงอย่างทันท่วงทีในกรณีที่การดำเนินงานจริงไม่เป็นไปตามแผนฯ	• ตรวจสอบเพื่อให้มั่นใจว่ามีการติดตามการดำเนินการตามแผนฯ และมีการปรับปรุงการดำเนินการในกรณีที่การปฏิบัติงานจริงไม่เป็นไปตามแผนงานด้านเทคโนโลยีสารสนเทศ

5.3 การจัดโครงสร้างงานเทคโนโลยีสารสนเทศ

5.3.1 ความรู้ทั่วไป

การจัดโครงสร้างงานเทคโนโลยีสารสนเทศมีวัตถุประสงค์ของการควบคุมเพื่อให้มั่นใจว่าฝ่ายเทคโนโลยีสารสนเทศอยู่ในตำแหน่งที่เหมาะสมและเอื้อให้เกิดการดำเนินการด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและประสิทธิผลในการสนับสนุนการดำเนินการทางธุรกิจ และมีการแบ่งแยกงานเทคโนโลยีสารสนเทศที่เหมาะสมและเอื้อให้เกิดการควบคุมภายในที่ดี

เพื่อบรรลุถึงวัตถุประสงค์ด้านการควบคุมดังกล่าวข้างต้น ควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

5.3.1.1 การจัดวางตำแหน่งของฝ่ายเทคโนโลยีสารสนเทศ

5.3.1.2 การแบ่งแยกงานเทคโนโลยีสารสนเทศ

5.3.1.3 งานที่ควรพิจารณาให้อยู่นอกฝ่ายเทคโนโลยีสารสนเทศ

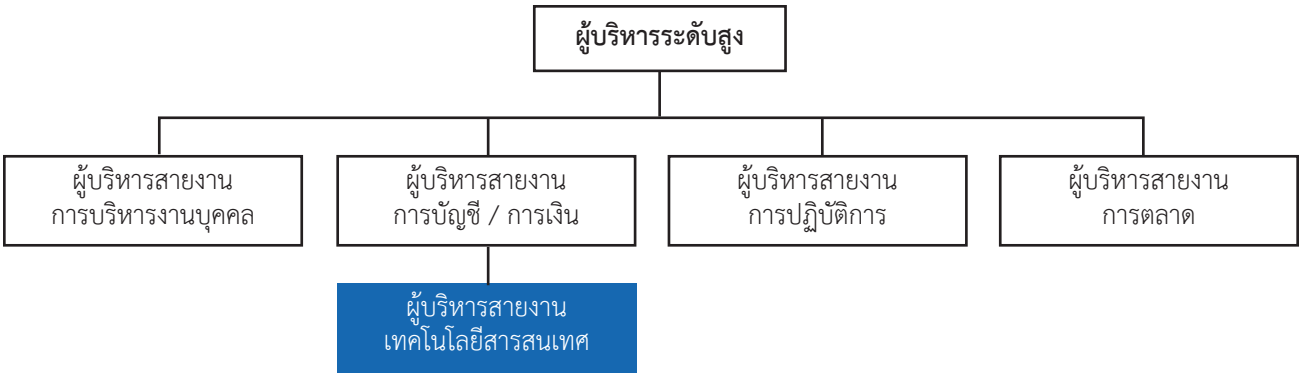
ดังมีรายละเอียด ดังต่อไปนี้

5.3.1.1 การจัดวางตำแหน่งของฝ่ายเทคโนโลยีสารสนเทศ

ในการจัดวางตำแหน่งงานด้านเทคโนโลยีสารสนเทศนั้น สิ่งที่ควรคำนึงถึงเป็นลำดับแรกก็คือลักษณะการใช้งานเทคโนโลยีสารสนเทศขององค์กร กล่าวคือถ้าองค์กรใช้เทคโนโลยีสารสนเทศในกระบวนการทำงานแทบทุกกระบวนการทำงานและทุกสายงาน ก็ควรจัดวางตำแหน่งงานเทคโนโลยีสารสนเทศให้อยู่ในระดับที่ค่อนข้างสูงในองค์กร เช่น จัดให้อยู่ในระดับเดียวกันกับผู้บริหารสายงานอื่น ๆ และขึ้นตรงกับผู้บริหารระดับสูง ดังแสดงไว้ในภาพที่ 2.2

ภาพที่ 2.2 ตัวอย่างของผังโครงสร้างองค์กรแสดงตำแหน่งของสายงานเทคโนโลยีสารสนเทศกรณีขึ้นตรงกับผู้บริหารระดับสูง

ทั้งนี้เพื่อเอื้อให้มีการบริการด้านเทคโนโลยีสารสนเทศที่เท่าเทียมกัน และทำให้การประสานงานระหว่างผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ และผู้บริหารสายงานอื่น ๆ เป็นไปอย่างมีประสิทธิภาพแต่ถ้าลักษณะการใช้เทคโนโลยีสารสนเทศขององค์กรเป็นการใช้งานเฉพาะด้าน เช่น ใช้เทคโนโลยีสารสนเทศเฉพาะงานด้านการบัญชีการเงิน ถ้าจัดให้งานเทคโนโลยีสารสนเทศอยู่ภายใต้การกำกับดูแลของผู้บริหารงานด้านการบัญชีการเงิน ตามภาพที่ 2.3 ก็อาจยังคงการบริหารงานด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพตรงกับความต้องการใช้เทคโนโลยีสารสนเทศขององค์กร



ภาพที่ 2.3 ตัวอย่างของผังโครงสร้างองค์กรแสดงตำแหน่งของสายงานเทคโนโลยีสารสนเทศ กรณีขึ้นตรงกับผู้บริหารสายงานการบัญชีการเงิน

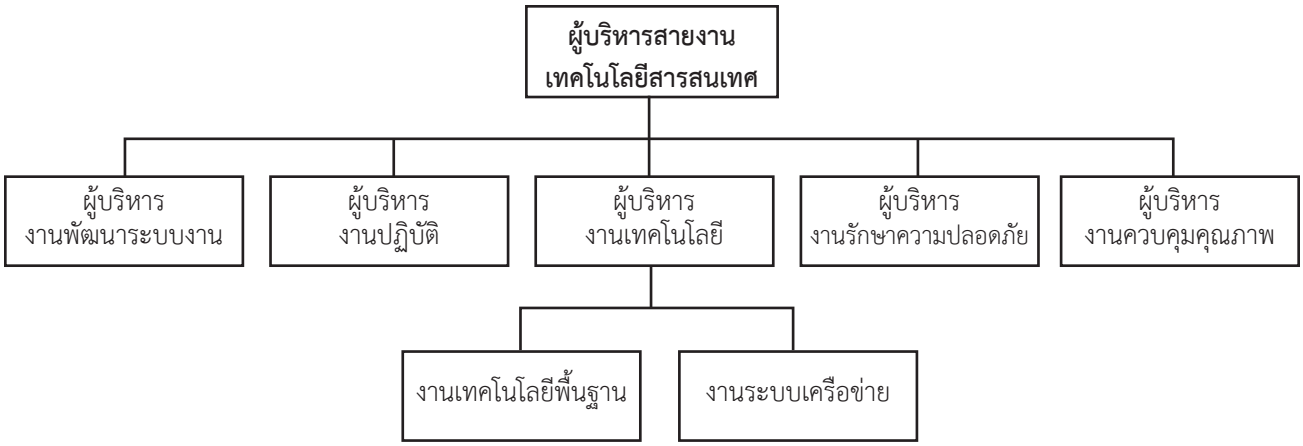
สำหรับองค์กรที่ใช้เทคโนโลยีสารสนเทศเป็นกลยุทธ์สำคัญในการดำเนินธุรกิจ โดยเฉพาะอย่างยิ่งเป็นกลไกสำคัญในการแข่งขัน อาจจำเป็นต้องมีการจัดตั้งคณะกรรมการด้านเทคโนโลยีสารสนเทศ (IT Steering Committee) ซึ่งประกอบด้วยผู้บริหารระดับสูงและผู้บริหารสายงานต่าง ๆ เพื่อทำหน้าที่กำหนดแนวทางในการจัดการด้านเทคโนโลยีสารสนเทศ และกำกับดูแลให้การใช้เทคโนโลยีสารสนเทศสอดคล้องกับกลยุทธ์ทางธุรกิจมากขึ้น อีกทั้งเอื้อให้เกิดการประสานงานระหว่างผู้บริหารเทคโนโลยีสารสนเทศและผู้บริหารสายงานต่าง ๆ มีประสิทธิภาพยิ่งขึ้น

5.3.1.2 การแบ่งแยกงานเทคโนโลยีสารสนเทศ

หลักการการควบคุมที่ดีด้านการจัดโครงสร้างองค์กร คือ การแบ่งแยกหน้าที่งานเทคโนโลยีสารสนเทศ ซึ่งงานเทคโนโลยีสารสนเทศในองค์กรส่วนใหญ่ ประกอบด้วย

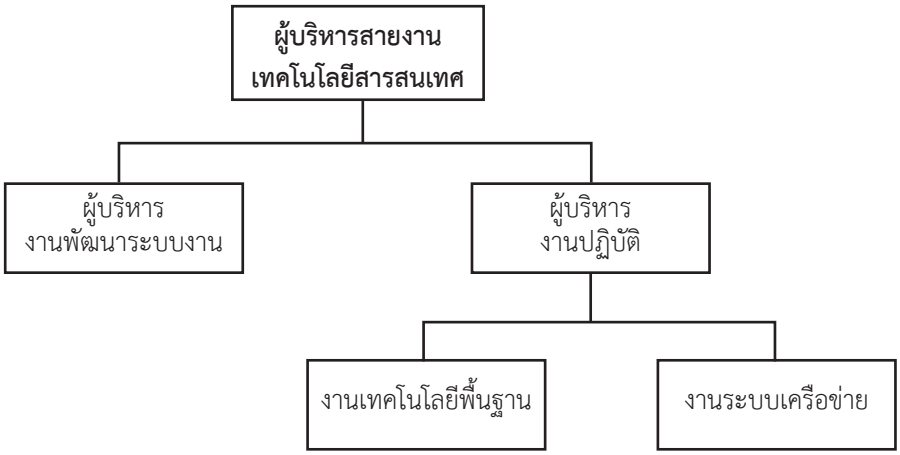
- งานพัฒนาระบบงาน
- งานปฏิบัติการคอมพิวเตอร์
- งานบริหารเทคโนโลยีพื้นฐาน
- งานบริหารระบบเครือข่าย
- งานรักษาความปลอดภัย
- งานควบคุมคุณภาพ

งานดังกล่าวข้างต้น ถ้าสามารถแยกออกจากกันได้ ก็จะทำให้การควบคุมสามารถทำได้อย่างมีประสิทธิภาพและประสิทธิผลมากขึ้น แต่ในความเป็นจริงคงจะแบ่งแยกได้เฉพาะองค์กรที่มีขนาดใหญ่ หรือมีการลงทุนด้านเทคโนโลยีสารสนเทศที่สูงเท่านั้น ซึ่งสามารถแสดงเป็นผังโครงสร้างงานดังแสดงในภาพที่ 2.4



ภาพที่ 2.4 ตัวอย่างผังโครงสร้างองค์กรแสดงการแบ่งแยกหน้าที่สายงานเทคโนโลยีสารสนเทศสำหรับองค์กรขนาดใหญ่

สำหรับองค์กรที่มีขนาดเล็กและมีการใช้เทคโนโลยีสารสนเทศในปริมาณที่น้อยจะไม่สามารถแบ่งแยกงานต่าง ๆ เหล่านี้ได้ทุกงาน แต่ก็ยังมีความจำเป็นที่จะต้องแบ่งแยกหน้าที่สำหรับงานที่สำคัญบางงาน เช่น งานพัฒนาระบบงาน และงานด้านการปฏิบัติการคอมพิวเตอร์ ส่วนงานด้านอื่น ๆ นั้นอาจจะพิจารณาให้อยู่ในส่วนใดส่วนหนึ่งภายในสองงานดังแสดงในภาพที่ 2.5



ภาพที่ 2.5 ตัวอย่างผังโครงสร้างองค์กรแสดงการแบ่งแยกหน้าที่สายงานเทคโนโลยีสารสนเทศสำหรับองค์กรขนาดเล็ก

ความจำเป็นที่จะต้องแยกงานพัฒนาระบบงานและงานปฏิบัติการคอมพิวเตอร์ออกจากกันก็เพราะว่าความต้องการในการใช้ระบบคอมพิวเตอร์ของ 2 กลุ่มงานนี้แตกต่างกัน โดยที่งานพัฒนาระบบงานนั้นต้องการใช้ระบบคอมพิวเตอร์ที่เตรียมไว้สำหรับการพัฒนาระบบงานเท่านั้น ในขณะที่งานปฏิบัติการคอมพิวเตอร์จำเป็นจะต้องใช้ระบบงานที่เก็บข้อมูลจริงและประมวลผลข้อมูลจริง ซึ่งถ้าให้ผู้พัฒนาระบบงานทำหน้าที่ปฏิบัติการคอมพิวเตอร์ด้วย ก็จะต้องให้สิทธิในการเข้าถึงระบบงานจริงด้วย ซึ่งอาจเป็นสาเหตุที่เอื้อต่อการเปลี่ยนแปลงแก้ไขโปรแกรมหรือข้อมูลที่ส่อไปในทางทุจริตได้

5.3.1.3 งานที่ควรพิจารณาให้อยู่นอกฝ่ายเทคโนโลยีสารสนเทศ

เทคโนโลยีสารสนเทศอาจทำให้การควบคุมคุณภาพขาดความเป็นอิสระ ซึ่งมีผลต่อประสิทธิภาพในการควบคุมคุณภาพของงานเทคโนโลยีสารสนเทศดังกล่าว

5.3.2 ความเสี่ยง การควบคุม และการตรวจสอบ

ในส่วนนี้เป็นการอธิบายถึงความเสี่ยง การควบคุมความเสี่ยง และการตรวจสอบเพื่อให้มั่นใจถึงประสิทธิภาพและประสิทธิผลของการควบคุมในการจัดการความเสี่ยง ด้านการจัดโครงสร้างงานเทคโนโลยีสารสนเทศ

ความเสี่ยง	การควบคุม	การตรวจสอบ
การแบ่งแยกงานเทคโนโลยีสารสนเทศอย่างเหมาะสม เช่น การรวมงานด้านการพัฒนาระบบงาน กับงานปฏิบัติการคอมพิวเตอร์ไว้ด้วยกัน อาจทำให้การควบคุมภายในเทคโนโลยีสารสนเทศด้านต่าง ๆ ไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพ เช่น อาจไม่สามารถจัดให้มีการควบคุมการเปลี่ยนแปลงแก้ไขระบบงานที่ดีได้	• มีการจัดโครงสร้างงานเทคโนโลยีสารสนเทศให้มีการแบ่งแยกงานเทคโนโลยีสารสนเทศที่ดี โดยอย่างน้อยมีการแบ่งแยกระหว่างการปฏิบัติการคอมพิวเตอร์ และการพัฒนาระบบงานเทคโนโลยีสารสนเทศ • ในกรณีที่ไม่สามารถแบ่งแยกหน้าที่งานได้อย่างเหมาะสม มีการกำหนดการควบคุมทดแทน เช่น การสอบทานการดำเนินงานที่มีความขัดแย้งกับหน้าที่งานหลัก	• สอบทานโครงสร้างงานเทคโนโลยีสารสนเทศเพื่อให้มั่นใจว่ามีการแบ่งแยกงานเทคโนโลยีสารสนเทศที่เหมาะสม • สอบทานคำอธิบายหน้าที่งานเพื่อให้มั่นใจว่ามีการกำหนดหน้าที่งานอย่างเหมาะสมตามโครงสร้างงานเทคโนโลยีสารสนเทศและการแบ่งแยกหน้าที่งานที่เหมาะสม • ในกรณีที่มีความขัดแย้งในการแบ่งแยกหน้าที่งาน ตรวจสอบเพื่อให้มั่นใจว่ามีการสอบทานการทำงานที่ไม่ใช่หน้าที่หลักอย่างสม่ำเสมอ
ผู้ปฏิบัติงานได้สิทธิในการเข้าถึงฟังก์ชันหรือคำสั่งงานคอมพิวเตอร์ (Computer Command) ที่อยู่นอกเหนือจากหน้าที่ความรับผิดชอบ	• มีการกำหนดสิทธิและสอบทานสิทธิการเข้าถึงฟังก์ชัน หรือ คำสั่งงานคอมพิวเตอร์ (Computer Command) ตามความจำเป็นในการปฏิบัติตามหน้าที่งาน	• สอบทานสิทธิการเข้าถึงฟังก์ชันหรือคำสั่งงานคอมพิวเตอร์ เพื่อให้มั่นใจว่าผู้ปฏิบัติหน้าที่ด้านเทคโนโลยีสารสนเทศได้สิทธิตามความจำเป็นในการปฏิบัติหน้าที่เท่านั้น
ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศจำเป็นต้องดำเนินงานในส่วนที่เป็นความรับผิดชอบของผู้ใช้งาน (End Users) เช่น การปรับปรุงข้อมูลในแฟ้มข้อมูลหลัก (Master Data)	• มีการกำหนดขั้นตอนการทำงาน สำหรับงานที่เจ้าหน้าที่คอมพิวเตอร์จำเป็นต้องปฏิบัติหน้าที่ในงานที่ควรรับผิดชอบโดยผู้ใช้งานอย่างชัดเจน • มีการสอบทานผลของการดำเนินงานโดยผู้ใช้งาน	• สอบทานความเหมาะสมของขั้นตอนการปฏิบัติ และตรวจสอบเพื่อให้มั่นใจว่ามีการสอบทานผลงานที่ดำเนินงานโดยเจ้าหน้าที่คอมพิวเตอร์ ในกรณีที่ทำหน้าที่แทนผู้ใช้งานอย่างสม่ำเสมอ

6.การพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ

ในส่วนนี้จะอธิบายถึง ความรู้ทั่วไป ความเสี่ยง การควบคุม และการตรวจสอบ ที่เกี่ยวข้องกับการพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ

6.1 การพัฒนาระบบงานเทคโนโลยีสารสนเทศ

6.1.1 ความรู้ทั่วไป

ในส่วนนี้เป็นการอธิบายองค์ประกอบต่าง ๆ ของการพัฒนาระบบงานสารสนเทศ เพื่อประกอบการทำความเข้าใจในการพัฒนาเทคโนโลยีสารสนเทศ และสามารถนำไปใช้ในการตรวจสอบการพัฒนาเทคโนโลยีสารสนเทศ

ในการพัฒนาระบบงานเทคโนโลยีสารสนเทศนั้น องค์กรสามารถเลือกการพัฒนาระบบงานได้ 2 ลักษณะ คือ

ก. การพัฒนาระบบงานขึ้นมาใหม่ทั้งหมด (Custom Development) หรือ

ข. การพัฒนาระบบงานจากซอฟต์แวร์สำเร็จรูป (Software Package Customization)

การพัฒนาระบบงานแบบ Custom Development นั้น เป็นการพัฒนาระบบงานขึ้นมาใหม่ทั้งหมด โดยเริ่มจากการรวบรวมและวิเคราะห์ความต้องการในการใช้ระบบงานแล้วทำการออกแบบระบบ จัดทำโปรแกรม ทดสอบ โอนย้ายข้อมูล และนำระบบมาใช้งาน

สำหรับการพัฒนาระบบโดยใช้ซอฟต์แวร์สำเร็จรูปนั้น เริ่มจากการรวบรวมและวิเคราะห์ความต้องการในการใช้ระบบงานเช่นกัน แต่จะไม่เขียนโปรแกรมขึ้นมาใหม่ แต่จะทำการปรับการทำงานของซอฟต์แวร์สำเร็จรูป (Configuration) ให้สอดคล้องกับความต้องการของผู้ใช้งาน ก่อนที่จะทำการทดสอบและนำระบบมาใช้งาน

ในปัจจุบันยังมีวิธีการพัฒนาระบบงานที่มุ่งเน้นการนำระบบฯ มาใช้งานให้รวดเร็วขึ้น โดยใช้วิธีการพัฒนาที่เรียกว่า Agile Development ซึ่งวิธีนี้จะเป็นการแบ่งระบบงานออกมาเป็นส่วนย่อย ๆ แล้วจัดทำระบบงานและนำมาใช้ทีละส่วน ซึ่งวิธีนี้จะทำให้สามารถนำระบบงานส่วนที่สำคัญมาใช้ก่อน แทนที่จะนำมาใช้ทั้งหมดพร้อมกันเมื่อเสร็จสิ้นโครงการการพัฒนาระบบงานฯ

การพัฒนาระบบงานสารสนเทศนั้น องค์กรจะต้องเตรียมระบบคอมพิวเตอร์ไว้สำหรับการพัฒนาระบบฯ (Development Environment) ที่แยกจากระบบคอมพิวเตอร์ที่ใช้สำหรับประมวลผลข้อมูลจริง (Computer Production Environment) โดยที่การพัฒนาระบบงานจะเริ่มทำในระบบคอมพิวเตอร์สำหรับการพัฒนาก่อน เมื่อพัฒนาและทดสอบระบบงานใหม่เรียบร้อยแล้ว ก็จะย้ายระบบงานไปที่ระบบคอมพิวเตอร์ที่ใช้สำหรับประมวลผลข้อมูลจริง

และในขั้นตอนการเขียนโปรแกรมนั้น โปรแกรมเมอร์จะเขียนโปรแกรมคอมพิวเตอร์โดยใช้ภาษาคอมพิวเตอร์เขียนเป็นรหัสต้นทาง (Source Code) ขึ้นมาก่อน แล้วจึงแปลง (Compile) เป็นรหัสที่คอมพิวเตอร์ใช้สำหรับการประมวลผล หรือ อ็อบเจกต์โคด (Object Code) ซึ่งการโอนย้ายระบบงานนั้น สามารถย้ายได้ 2 วิธี คือ การย้ายรหัสต้นทางจากระบบคอมพิวเตอร์สำหรับการพัฒนาไปที่ระบบคอมพิวเตอร์ที่ใช้สำหรับประมวลผลข้อมูลจริง แล้วจึงแปลงเป็นอ็อบเจกต์โคดเพื่อใช้งาน หรืออีกวิธีก็คือ การแปลงโปรแกรมในระบบคอมพิวเตอร์สำหรับการพัฒนาก่อน แล้วจึงย้ายอ็อบเจกต์โคด ไปที่ระบบคอมพิวเตอร์ที่ใช้สำหรับประมวลผลข้อมูลจริงเพื่อใช้งาน

อย่างไรก็ตาม ไม่ว่าองค์กรจะเลือกวิธีการพัฒนาในวิธีไหน ก็จะต้องจัดให้มีการควบคุมภายในในแต่ละขั้นตอนของการดำเนินการ ซึ่งในส่วนต่อไปนี้จะอธิบายการควบคุมที่ควรมีในการพัฒนาระบบงานเทคโนโลยีสารสนเทศ

การควบคุมด้านการพัฒนาระบบงานเทคโนโลยีสารสนเทศมีวัตถุประสงค์ดังนี้

- เพื่อให้มั่นใจว่าระบบงานที่พัฒนาขึ้นมาใหม่มีความสอดคล้องกับความต้องการทางธุรกิจ และสอดคล้องกับวัตถุประสงค์ของการพัฒนาระบบงาน
- เพื่อให้มั่นใจว่ามีการทดสอบระบบงานใหม่อย่างเหมาะสมเพียงพอ เพื่อให้ระบบงานใหม่ปราศจากข้อบกพร่องก่อนนำระบบงานมาใช้งาน
- เพื่อให้มั่นใจว่าการบริหารโครงการเป็นไปอย่างมีประสิทธิภาพ โดยสามารถดำเนินการเสร็จภายในระยะเวลาที่กำหนด และภายในงบประมาณที่จัดเตรียมไว้

การควบคุมที่เกี่ยวข้องกับการพัฒนาระบบงานเทคโนโลยีสารสนเทศประกอบด้วยกระบวนการที่สำคัญ 2 กระบวนการ คือ การบริหารโครงการ และการพัฒนาระบบงาน ซึ่งในแต่ละส่วนมีความสำคัญไม่น้อยไปกว่ากันโดยที่การบริหารโครงการมุ่งเน้นด้านการควบคุมโครงการให้เป็นไปตามวัตถุประสงค์ของโครงการ และให้โครงการแล้วเสร็จภายในระยะเวลาที่กำหนด ส่วนกระบวนการพัฒนาระบบงานมุ่งเน้นที่รายละเอียดการพัฒนาระบบงานซึ่งเริ่มตั้งแต่การกำหนดวัตถุประสงค์ของโครงการ การรวบรวม รายละเอียดความต้องการ การออกแบบและจัดทำระบบงาน การทดสอบระบบงาน และการเตรียมความพร้อมก่อนนำมาใช้งาน ซึ่งระบวนการทำงานโดยรวมแสดงไว้ในภาพที่ 2.6

ภาพ 2.6 ขั้นตอนการพัฒนาระบบงานเทคโนโลยีสารสนเทศ

ดังนั้น การควบคุมด้านการพัฒนาระบบงานเทคโนโลยีสารสนเทศ ประกอบด้วยการควบคุม 2 ส่วนดังนี้

6.1.1.1 การควบคุมในส่วนของการบริหารโครงการพัฒนาระบบงานเทคโนโลยีสารสนเทศ

6.1.1.2 การควบคุมในขั้นตอนการพัฒนาระบบงานเทคโนโลยีสารสนเทศ

6.1.1.1 การควบคุมในส่วนของการบริหารโครงการพัฒนาระบบงานเทคโนโลยีสารสนเทศ

ในส่วนของการควบคุมการบริหารโครงการพัฒนาระบบงานเทคโนโลยีสารสนเทศนั้น ควรจัดให้มีการควบคุมดังต่อไปนี้

- มีการกำหนดวัตถุประสงค์ของการพัฒนาระบบงานที่ชัดเจน และสอดคล้องกับวัตถุประสงค์และความต้องการทางธุรกิจ ซึ่งจะต้องมีการบันทึกและสื่อสารทำความเข้าใจต่อวัตถุประสงค์ให้กับทุกคนที่เกี่ยวข้องกับการพัฒนาระบบงานนั้น ๆ
- ทีมงานพัฒนาระบบงานเทคโนโลยีสารสนเทศควรประกอบด้วยบุคลากรที่เป็นตัวแทนจากหน่วยงานที่เกี่ยวข้องอย่างครบถ้วน เช่น ถ้าเป็นการพัฒนาระบบงานเทคโนโลยีสารสนเทศนั้นควรจะต้องมีผู้แทนจากหน่วยงานฝ่ายผู้ใช้งานและตัวแทนเทคโนโลยีสารสนเทศผสมผสานกัน
- ผู้ที่ทำหน้าที่ผู้จัดการโครงการจำเป็นต้องมีทักษะในการบริหารโครงการ และควรเป็นผู้ที่มีความรู้และความสามารถที่เหมาะสม ในการพัฒนาระบบงานให้บรรลุถึงวัตถุประสงค์ที่กำหนดไว้ได้อย่างมีประสิทธิภาพ
- จัดให้มีโครงสร้างของทีมงานพัฒนาระบบงานที่เหมาะสมซึ่งประกอบด้วย ผู้จัดการโครงการ เจ้าของโครงการ ผู้สนับสนุนโครงการ ตัวแทนจากในส่วนของผู้ใช้งาน และตัวแทนจากฝ่ายเทคโนโลยีสารสนเทศ

- จัดให้มีการวิเคราะห์เพื่อกำหนดวิธีการพัฒนาระบบงานเทคโนโลยีสารสนเทศที่เหมาะสม เช่น การเลือกระหว่างพัฒนาระบบงานขึ้นมาใหม่ หรือจะใช้ซอฟต์แวร์สำเร็จรูปเป็นพื้นฐานในการพัฒนาโดยคำนึงถึงปัจจัยด้านค่าใช้จ่ายและระยะเวลาในการพัฒนา และนำมาใช้งาน ความน่าเชื่อถือของระบบงาน ความยืดหยุ่นในการปรับปรุงซอฟต์แวร์ให้เข้ากับกระบวนการทำงาน และความสามารถในการเปลี่ยนแปลงแก้ไขระบบงานในอนาคต
- จัดให้มีกระบวนการติดตามความคืบหน้าและการสื่อสารภายในโครงการอย่างสม่ำเสมอ ผ่านการประชุมโครงการและการรายงานความคืบหน้า และมีกระบวนการในการจัดการปัญหาที่ชัดเจนตั้งแต่การบันทึกปัญหาอุปสรรคต่าง ๆ ที่เกิดขึ้นการดำเนินการแก้ไข และการสรุปการแก้ไข

6.1.1.2 การควบคุมในขั้นตอนการพัฒนาระบบงานเทคโนโลยีสารสนเทศ

ในส่วนของการควบคุมในขั้นตอนการพัฒนาระบบงานเทคโนโลยีสารสนเทศนั้น ควรจัดให้มีการควบคุมดังต่อไปนี้

6.1.1.2.1 จัดให้มีการควบคุมในแต่ละขั้นตอนของการพัฒนาระบบงานเทคโนโลยีสารสนเทศ ดังนี้

- **ขั้นตอนการรวบรวมรายละเอียด (Analysis)** เป็นขั้นตอนในการรวบรวมความต้องการของระบบงานใหม่ ซึ่งการควบคุมที่สำคัญ คือ การจัดให้มีกลไกในการรวบรวมความต้องการของระบบที่ชัดเจน และต้องครอบคลุมความต้องการทั้งทางธุรกิจและความต้องการด้านการควบคุม โดยควรที่จะจัดให้มีการสอบทานความต้องการดังกล่าวเพื่อให้มั่นใจว่าความต้องการนั้น ๆ สอดคล้องกับวัตถุประสงค์ของระบบงานใหม่
- **ขั้นตอนการออกแบบระบบงาน (Design)** เป็นการนำความต้องการของระบบงานใหม่มาออกแบบเป็นเทคโนโลยีสารสนเทศซึ่งการควบคุมที่จำเป็นต้องมี คือ การสอบทานเพื่อให้มั่นใจว่าความต้องการที่รวบรวมไว้ในขั้นตอนก่อนหน้านี้ได้รับการออกแบบอย่างถูกต้อง และครอบคลุมทั้งความต้องการทางธุรกิจ และความต้องการด้านการควบคุม
- **ขั้นตอนการจัดทำระบบ (Construction)** การดำเนินการสร้างเทคโนโลยีสารสนเทศ ซึ่งในขั้นตอนนี้การควบคุมที่สำคัญ คือ การทดสอบระบบที่จัดทำขึ้นมาใหม่เพื่อให้ความมั่นใจว่า ความต้องการที่กำหนดโดยผู้ใช้งานนั้นนำมาออกแบบและสร้างอย่างครบถ้วนและถูกต้อง ซึ่งการสร้างระบบอาจเป็นการสร้างขึ้นมาใหม่ทั้งหมดหรือเป็นการนำซอฟต์แวร์สำเร็จรูป มาดัดแปลงเพื่อให้สอดคล้องกับแบบที่ออกไว้ก็ได้
- **ขั้นตอนการทดสอบระบบงาน (Testing)** เป็นขั้นตอนที่สำคัญ ประกอบด้วยการทดสอบโดยผู้พัฒนาระบบเพื่อให้มั่นใจว่าระบบทำงานอย่างถูกต้อง และการทดสอบโดยผู้ใช้งาน เพื่อตรวจรับและรับรองว่าระบบทำงานได้ตรงกับความต้องการของผู้ใช้งาน
- **ขั้นตอนการเตรียมความพร้อมเพื่อนำมาใช้งาน (Implementation)** เป็นขั้นตอนการนำระบบมาใช้งาน โดยมีการควบคุมที่สำคัญคือ ต้องมีการอนุมัติการโอนย้ายระบบไปใช้งานหลังจากผลการทดสอบขั้นสุดท้ายเป็นที่พอใจของเจ้าของระบบแล้วการโอนย้ายเทคโนโลยีสารสนเทศ จึงควรทำภายใต้การควบคุมที่เข้มงวดเพื่อให้มั่นใจว่าโปรแกรมที่นำไปใช้งานเป็นโปรแกรมเดียวกันกับโปรแกรมที่ได้รับการทดสอบ และต้องมีการจัดทำเอกสารประกอบระบบงานอย่างครบถ้วนสมบูรณ์ก่อนนำระบบมาใช้งานจริง และจัดให้มีการสอบทานเพื่อทำให้มั่นใจว่าความต้องการทั้งทางด้านธุรกิจและด้านการควบคุมนั้นได้มีการนำมาปฏิบัติจริง นอกจากนี้ยังเป็นการเตรียมความพร้อมของระบบ เช่น การโอนถ่ายข้อมูลจากระบบงานเดิม (Data Conversion) หรือการเตรียมข้อมูลตั้งต้น รวมทั้งการฝึกอบรมผู้ใช้งาน

6.1.1.2.2 มีการจัดทำเอกสารประกอบระบบงานอย่างครบถ้วน ซึ่งเอกสารควรประกอบด้วย

- **คู่มือประกอบระบบงาน (System Manual)** เป็นเอกสารแสดงรายละเอียดทางเทคนิคของระบบงาน ซึ่งมีไว้เพื่อประกอบการพิจารณาปรับปรุงหรือเปลี่ยนแปลงระบบในอนาคต
- **คู่มือปฏิบัติงาน (Operation Manual)** เป็นเอกสารแสดงรายละเอียดขั้นตอนการปฏิบัติงานต่าง ๆ ของระบบงาน ซึ่งส่วนใหญ่ใช้โดยผู้ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) ในการเปิด-ปิดระบบงาน ประมวลผลงานสิ้นวัน สำรองข้อมูล เป็นต้น
- **คู่มือการใช้งาน (User Manual)** เป็นเอกสารแสดงรายละเอียดการใช้ระบบงานของผู้ใช้งาน ซึ่งใช้สำหรับศึกษาการทำงานของระบบงาน เช่น การทำงานของแต่ละหน้าจอ หรือการใช้ฟังก์ชันต่าง ๆ ที่มีมากับระบบ
- **เอกสารแสดงขั้นตอนการปฏิบัติงาน (User Procedure)** ที่ผู้ใช้งานจะต้องใช้ปฏิบัติ เช่น ก่อนการนำข้อมูลเข้าสู่ระบบจะต้องมีการอนุมัติเอกสารก่อน หรือ ระบุว่าใครเป็นผู้นำเข้าข้อมูล และใครเป็นผู้อนุมัติ เป็นต้น

6.1.1.2.3 เพื่อป้องกันการหยุดชะงักของการใช้เทคโนโลยีสารสนเทศ ประกอบการดำเนินธุรกิจ ก่อนที่จะนำระบบงานใหม่มาใช้งาน ควรพิจารณาวิธีการที่เหมาะสมเพื่อป้องกันเหตุการณ์ข้างต้น ดังมีลักษณะของแต่ละวิธีการนำระบบมาใช้งาน ดังนี้

- การนำระบบงานใหม่มาใช้ทดแทนระบบงานเก่าโดยทันที (Cut Off Implementation) ซึ่งวิธีนี้เป็นการยกเลิกการใช้ระบบงานเก่าทันทีหลังจากระบบงานใหม่เริ่มใช้งานแล้ว ซึ่งวิธีนี้มีความเสี่ยงค่อนข้างสูงแต่ค่าใช้จ่ายจะน้อยที่สุด
- การใช้ระบบงานเก่าพร้อมกับระบบงานใหม่ในระยะเริ่มแรก (Parallel Implementation) เป็นการใช้ระบบงานเก่าพร้อมไปกับการใช้ระบบงานใหม่ในระยะเวลาหนึ่งจนกระทั่งมั่นใจว่าระบบงานใหม่มีความถูกต้อง จึงยกเลิกการใช้ระบบงานเก่า วิธีนี้เป็นวิธีที่ค่อนข้างปลอดภัยสูง แต่จะต้องมีการทำงานและค่าใช้จ่ายมากกว่าเดิม
- การนำระบบงานใหม่มาใช้งานทีละส่วน (Phase Implementation) เช่น เริ่มจากการใช้ส่วนที่ระบบบัญชีก่อน จึงเริ่มนำระบบงานอื่น ๆ มาใช้งานตามลำดับ
- การทดลองใช้ระบบงานใหม่กับหน่วยงานทดลอง (Pilot Implementation) โดยเริ่มทดลองใช้งานระบบงานใหม่กับหน่วยงานย่อยก่อน จนกระทั่งมั่นใจว่าระบบงานใหม่ทำงานได้อย่างถูกต้อง จึงเริ่มทยอยใช้ระบบงานใหม่นี้กับหน่วยงานอื่น ๆ ทั่วทั้งองค์กร

6.1.2 ความเสี่ยง การควบคุม และการตรวจสอบ

ในส่วนนี้เป็นการอธิบายถึงความเสี่ยง การควบคุมความเสี่ยง และการตรวจสอบเพื่อให้มั่นใจถึงประสิทธิภาพและประสิทธิผลของการควบคุมในการจัดการความเสี่ยง ด้านการพัฒนาระบบงานเทคโนโลยีสารสนเทศ ในส่วนที่อาจมีผลกระทบกับความน่าเชื่อถือของรายงานทางการเงิน

ความเสี่ยง	การควบคุม	การตรวจสอบ
ระบบงานยังมีข้อบกพร่องหลังจากนำมาใช้งานแล้ว มีผลทำให้การประมวลผลที่สำคัญอาจไม่ถูกต้องหรือครบถ้วน	• มีการทดสอบระบบงานอย่างมีประสิทธิผล ประกอบด้วย การจัดทำแผนการทดสอบที่ชัดเจนและกำหนดเงื่อนไขการทดสอบ (Test Script) ที่ครอบคลุมความต้องการใช้งาน (Requirements) ทั้งหมดของระบบงาน • ดำเนินการทดสอบระบบฯ ตามแผนการทดสอบอย่างครบถ้วน โดยต้องเป็นการทดสอบที่ดำเนินการโดยบุคคลที่เหมาะสม ได้แก่ การทดสอบรายโปรแกรม (Unit Test) และ การทดสอบระบบโดยรวม (System Test) โดยผู้พัฒนาระบบงาน และการทดสอบเพื่อตรวจรับงานโดยผู้ใช้งาน (User Acceptance Test) โดยผู้ใช้งานจริง • สอบทานผลการทดสอบระบบฯ โดยบุคคลที่เหมาะสม ได้แก่ ผู้ควบคุมคุณภาพระบบงาน และ อนุมัติผลการทดสอบโดยเจ้าของระบบงาน • ต้องมีการดำเนินการที่เหมาะสม ในกรณีที่ผลการทดสอบระบบงานที่ไม่เป็นไปตามผลที่ควรจะเป็น เช่น การแก้ไขและทำการทดสอบซ้ำ หรือการสอบทานเพื่อยอมรับผลทดสอบที่แตกต่างกับผลที่คาดไว้	• เลือกโครงการพัฒนาระบบงานที่สำคัญแล้วตรวจสอบว่ามีการวางแผนการทดสอบและมีการอนุมัติแผนการทดสอบอย่างเหมาะสม • สอบทานแผนการทดสอบและเงื่อนไขการทดสอบว่ามีการสอบทานความครบถ้วนเทียบกับความต้องการใช้งาน • สุ่มตรวจสอบการทดสอบเพื่อให้มั่นใจว่ามีการทดสอบที่เป็นการทดสอบเพื่อตรวจรับงานโดยผู้ใช้งานจริง • ตรวจสอบว่ามีการสอบทานผลการทดสอบอย่างครบถ้วนโดยผู้ควบคุมคุณภาพ และมีการจัดการอย่างเหมาะสมในกรณีที่ผลการทดสอบไม่เป็นไปตามผลที่คาดไว้
ข้อมูลตั้งต้นของระบบงานใหม่อาจไม่ครบถ้วนถูกต้อง ทำให้ผลการประมวลผลอาจไม่ครบถ้วนถูกต้อง	• มีการจัดทำแผนการโอนข้อมูลจากระบบงานเก่าไปยังระบบงานใหม่ (Data Conversion) ที่มีประสิทธิผล โดยมีการสอบทานแผน และการดำเนินการตามแผนโดยบุคคลที่เหมาะสม • มีการตรวจทานเพื่อกระทบยอดข้อมูลระหว่างระบบงานเก่าและระบบงานใหม่ • มีการสอบทานความครบถ้วนถูกต้องของการนำเข้าข้อมูล ในกรณีที่ต้องป้อนข้อมูลตั้งต้นเข้าสู่ระบบงานใหม่	• สอบทานความเหมาะสมของแผนและการอนุมัติแผนการโอนย้ายข้อมูล • ตรวจสอบความครบถ้วนของการกระทบยอดข้อมูลระหว่างระบบงานเก่าและระบบงานใหม่ • สุ่มตรวจสอบข้อมูลที่นำเข้าระบบงานใหม่ว่ามีการสอบทานการนำเข้าข้อมูลอย่างครบถ้วน

ความเสี่ยง	การควบคุม	การตรวจสอบ
การโอนย้ายโปรแกรมที่พัฒนาใหม่ เพื่อนำไปใช้งานอาจไม่ครบถ้วนถูกต้อง	• มีการสอบทานความครบถ้วนและถูกต้องของการโอนย้ายโปรแกรมของระบบงานใหม่ไปใช้งานจริง	• ตรวจสอบการอนุมัติและการดำเนินการโอนย้ายโปรแกรมเพื่อให้มั่นใจว่าเป็นการโอนย้าย โปรแกรมที่ถูกต้องและผ่านการทดสอบแล้วไปใช้งาน
ผู้ใช้งานอาจขาดความเข้าใจที่เพียงพอในการทำงานของระบบงานใหม่ อาจส่งผลทำให้เกิดข้อผิดพลาดในการทำงานร่วมกับระบบงานใหม่	• มีแผนการสื่อสารและอบรมให้บุคลากรที่เกี่ยวข้องทราบและเข้าใจต่อการทำงานของระบบงานใหม่ • มีการติดตามการดำเนินการตามแผนงาน • มีการสำรวจอัตราการรับรู้และเข้าใจการใช้งานระบบงานใหม่	• สอบทานแผนและการอนุมัติแผนการสื่อสารและอบรม เพื่อให้มั่นใจว่ามีการติดตามการดำเนินการตามแผน และสุ่มตรวจสอบการสำรวจอัตราการรับรู้ของผู้ใช้งานต่อระบบงานใหม่

6.2 การเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ

6.2.1 ความรู้ทั่วไป

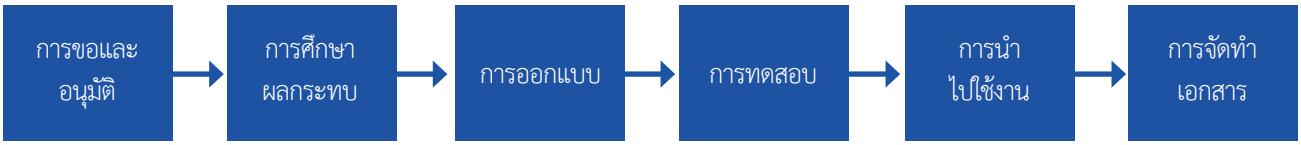
ในส่วนนี้เป็นการอธิบายองค์ประกอบต่าง ๆ ของการเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ เพื่อประกอบการทำความเข้าใจในการพัฒนาเทคโนโลยีสารสนเทศ และสามารถนำไปใช้ในการตรวจสอบการพัฒนาเทคโนโลยีสารสนเทศ

การเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศในส่วนนี้จะครอบคลุมการเปลี่ยนแปลงแก้ไขเทคโนโลยีสารสนเทศทั้งในการเปลี่ยนแปลงระบบงานเทคโนโลยีสารสนเทศ เทคโนโลยีพื้นฐาน เช่น ฮาร์ดแวร์และอุปกรณ์ต่าง ๆ และการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ระบบ (System Software) ซึ่งการเปลี่ยนแปลงเทคโนโลยีสารสนเทศนั้นเป็นการเปลี่ยนแปลงลักษณะการทำงานของระบบ ซึ่งอาจเกิดจากความต้องการปรับปรุงการทำงานภายใน และอาจเกิดขึ้นจากการเปลี่ยนแปลงเนื่องจากปัจจัยภายนอก เช่น มีการเปลี่ยนแปลงในกฎระเบียบ หรือมาตรฐานการทำงาน

ทั้งนี้ ทุกการเปลี่ยนแปลงจะต้องมีการควบคุมที่ดี เพราะการเปลี่ยนแปลงอาจส่งผลกระทบทำให้การทำงานของระบบที่มีการเปลี่ยนแปลงนั้นมีข้อผิดพลาด หรืออาจส่งผลกระทบต่อการทำงานของระบบงานอื่นได้ ดังนั้นองค์กรจำเป็นจะต้องจัดให้มีการควบคุม

การควบคุมด้านการเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศมีวัตถุประสงค์ เพื่อให้มั่นใจว่าระบบงานที่เปลี่ยนแปลงแก้ไขสอดคล้องกับความต้องการทางธุรกิจ และสอดคล้องกับวัตถุประสงค์ของการพัฒนาระบบงาน และให้มั่นใจว่ามีการทดสอบระบบงานใหม่อย่างเหมาะสมเพียงพอ เพื่อให้ระบบงานใหม่ปราศจากข้อบกพร่องก่อนนำระบบงานมาใช้งาน เพื่อบรรลุถึงวัตถุประสงค์ด้านการควบคุมดังกล่าวข้างต้น ควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

การควบคุมการเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศนั้นมีความสำคัญไม่น้อยกว่าการควบคุมในส่วนของการพัฒนาระบบงาน เพราะการเปลี่ยนแปลงมีผลทำให้เกิดความเสี่ยงเกี่ยวกับความถูกต้องของระบบงานและข้อมูลที่ใช้ในการปฏิบัติงานโดยเฉพาะอย่างยิ่งระบบงานที่มีการเปลี่ยนแปลงแก้ไขบ่อยครั้ง ซึ่งการควบคุมในขั้นตอนต่าง ๆ ของการเปลี่ยนแปลงแก้ไขระบบงานมีความคล้ายคลึงกันกับการควบคุมด้านการพัฒนาระบบงาน หากแต่ว่าขนาดของโครงการเป็นขนาดที่เล็กกว่าการพัฒนาระบบงาน ขั้นตอนการเปลี่ยนแปลงแก้ไขระบบงาน แสดงไว้ในภาพที่ 2.7 ดังต่อไปนี้



ภาพ 2.7 ขั้นตอนการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ

ในขั้นตอนของการเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ ควรจัดให้มีการควบคุมดังต่อไปนี้

- จะต้องมีการขอและอนุมัติการเปลี่ยนแปลงแก้ไขเทคโนโลยีสารสนเทศอย่างเป็นทางการ ซึ่งโดยส่วนใหญ่ใช้ใบคำขอการเปลี่ยนแปลงที่เป็นแบบฟอร์มที่เตรียมไว้ล่วงหน้า โดยมีการบันทึกรายละเอียดของการเปลี่ยนแปลงอย่างชัดเจน เช่น ผู้ขอ ผู้อนุมัติ วันที่ขอ วันที่ต้องการให้แล้วเสร็จ เหตุผลของการแก้ไข เป็นต้น โดยผู้บริหารที่ได้รับการแต่งตั้งเป็นเจ้าของระบบงานเป็นผู้อนุมัติการเปลี่ยนแปลง
- มีการศึกษาความเป็นไปได้ทางเทคนิค ความคุ้มค่าของการเปลี่ยนแปลง และผลกระทบที่อาจเกิดขึ้น ก่อนเริ่มลงมือเปลี่ยนแปลงแก้ไข
- การวิเคราะห์และออกแบบ ควรดำเนินการอย่างสอดคล้องกับหลักการการควบคุมการพัฒนาระบบงานที่ดี ตามที่อธิบายไว้ในส่วนของการควบคุมการพัฒนาระบบงาน
- การเปลี่ยนแปลงแก้ไขจะต้องได้รับการทดสอบอย่างเพียงพอ ก่อนที่จะนำระบบหรือโปรแกรมที่แก้ไขไปใช้งาน โดยที่การทดสอบขั้นสุดท้ายก่อนการโอนย้ายระบบไปใช้งาน ต้องทำโดยตัวแทนของเจ้าของระบบงาน
- การโอนย้ายระบบหรือโปรแกรมที่แก้ไขไปใช้งานจะต้องมีการควบคุมเพื่อให้มั่นใจว่าโปรแกรมที่ย้ายไปใช้งานนั้นเป็นโปรแกรมเดียวกันกับโปรแกรมที่ได้รับการทดสอบแล้ว ถ้าเป็นการเปลี่ยนแปลงแก้ไขที่อาจมีผลกระทบกับการทำงานอย่างมีนัยสำคัญ ควรพิจารณาเลือกวิธีการนำระบบงานใหม่มาใช้งานที่เหมาะสม ตามที่อธิบายไว้ในส่วนของการควบคุมการพัฒนาระบบงาน
- มีการปรับปรุงแก้ไขเอกสารประกอบระบบงานทั้งหมดให้สะท้อนถึงการเปลี่ยนแปลงแก้ไขและเพื่อการจัดให้มีการควบคุมที่ดีในกระบวนการการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ ระบบคอมพิวเตอร์ขององค์กรควรจะต้องมีอย่างน้อย 2 ส่วน คือ ส่วนของระบบคอมพิวเตอร์สำหรับการพัฒนา และส่วนที่เป็นระบบคอมพิวเตอร์ที่ใช้สำหรับประมวลผลข้อมูลจริง

ข้อควรคำนึงเพิ่มเติมในด้านการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศคือ บางครั้งการเปลี่ยนแปลงอาจต้องทำในกรณีเร่งด่วน ซึ่งอาจทำให้ไม่สามารถดำเนินการตามขั้นตอนการเปลี่ยนแปลงที่ระบุไว้ข้างต้นโดยมีการพิจารณาดำเนินการแตกต่างกันไปตามความเหมาะสมของแต่ละกรณีที่จำเป็นต้องมีการเปลี่ยนแปลงแก้ไขระบบงานในลักษณะเร่งด่วน ซึ่งบางองค์กรอาจจะจัดให้มีขั้นตอนพิเศษเฉพาะสำหรับการเปลี่ยนแปลงในกรณีดังกล่าว

6.2.2 ความเสี่ยง การควบคุม และการตรวจสอบ

ในส่วนนี้เป็นการอธิบายถึงความเสี่ยง การควบคุมความเสี่ยง และการตรวจสอบเพื่อให้มั่นใจถึงประสิทธิภาพและประสิทธิผลของการควบคุมในการจัดการความเสี่ยง ด้านการเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ ในส่วนที่อาจมีผลกระทบกับความน่าเชื่อถือของรายงานทางการเงิน

ความเสี่ยง	การควบคุม	การตรวจสอบ
โปรแกรมหรือระบบงานที่มีการแก้ไขอาจยังมีข้อบกพร่องหลังจากนำมาใช้งานแล้ว มีผลทำให้การประมวลผลที่สำคัญอาจไม่ถูกต้องหรือครบถ้วน	• การทดสอบโปรแกรมหรือระบบงานโดยบุคคลที่เหมาะสม เช่น การทดสอบเพื่อตรวจรับงาน (User Acceptance Test) โดยผู้ใช้งานจริง ในกรณีที่เป็นการเปลี่ยนแปลงโปรแกรมของระบบงานหรือการทดสอบโดยผู้เชี่ยวชาญในกรณีที่เป็นการเปลี่ยนแปลงเทคโนโลยีพื้นฐานหรือการเปลี่ยนแปลงซอฟต์แวร์ระบบ (System Software) • สอบทานผลการทดสอบระบบงานโดยบุคคลที่เหมาะสม ได้แก่ ผู้ควบคุมคุณภาพระบบงาน และอนุมัติผลการทดสอบ โดยเจ้าของระบบงาน • ต้องมีการดำเนินการที่เหมาะสม ในกรณีที่ผลการทดสอบระบบงานที่ไม่เป็นไปตามผลที่ควรจะเป็น เช่น การแก้ไขและทำการทดสอบซ้ำ หรือการสอบทานเพื่อยอมรับผลทดสอบที่แตกต่างกับผลที่คาดไว้	• เลือกตัวอย่างจากรายการโปรแกรมหรือระบบงานที่มีการเปลี่ยนแปลง แล้วตรวจสอบว่าการเปลี่ยนแปลงนั้น ๆ ผ่านการทดสอบอย่างเหมาะสมหรือไม่ • ตรวจสอบว่ามีการสอบทานผลการทดสอบอย่างครบถ้วนโดยผู้ควบคุมคุณภาพ และมีการจัดการอย่างเหมาะสมในกรณีที่ผลการทดสอบไม่เป็นไปตามผลที่คาดไว้
อาจมีการเปลี่ยนแปลงโปรแกรมหรือระบบงานที่ไม่ได้รับการอนุมัติอย่างเหมาะสมเกิดขึ้น	• มีการกำหนดเป็นนโยบายและระเบียบปฏิบัติที่ชัดเจนโดยระบุผู้มีอำนาจในการอนุมัติการเปลี่ยนแปลงในระบบงานใด และเทคโนโลยีพื้นฐานใด • มีการจัดทำแบบฟอร์มที่ใช้ในแต่ละขั้นตอน เช่น การจัดทำคำขอและการอนุมัติการเปลี่ยนแปลง เป็นต้น • มีการกำหนดสิทธิการเข้าถึงฟังก์ชันหรือชุดคำสั่งที่ใช้สำหรับการเปลี่ยนแปลงให้เฉพาะผู้ที่จำเป็นในการดำเนินการในแต่ละขั้นตอนของการเปลี่ยนแปลง	• เลือกตัวอย่างจากรายการโปรแกรมหรือระบบงานที่มีการเปลี่ยนแปลง แล้วตรวจสอบว่าการเปลี่ยนแปลงนั้น ๆ ผ่านการอนุมัติที่เหมาะสมหรือไม่ • สุ่มตรวจสอบการดำเนินการตามขั้นตอนจากเอกสารหรือแบบฟอร์มประกอบการดำเนินการของแต่ละขั้นตอน • ตรวจสอบสิทธิและอำนาจการดำเนินการในกรณีที่มีการใช้ซอฟต์แวร์ในการควบคุมขั้นตอนในการเปลี่ยนแปลง • ตรวจสอบความเหมาะสมของผู้ที่มีสิทธิเข้าถึงฟังก์ชันหรือชุดคำสั่งที่ใช้สำหรับการเปลี่ยนแปลง
การโอนย้ายโปรแกรมที่พัฒนาใหม่ เพื่อนำไปใช้งานอาจไม่ครบถ้วนถูกต้อง	• มีการสอบทานความครบถ้วนและถูกต้องของการโอนย้ายโปรแกรมของระบบงานใหม่ไปใช้งานจริง	• ตรวจสอบการอนุมัติและการดำเนินการโอนย้ายโปรแกรมเพื่อให้มั่นใจว่าเป็นการโอนย้ายโปรแกรมที่ถูกต้องและผ่านการทดสอบแล้วไปใช้งาน

ความเสี่ยง	การควบคุม	การตรวจสอบ
ข้อมูลตั้งต้นของระบบงานใหม่อาจไม่ครบถ้วนถูกต้อง ในกรณีที่ต้องมีการเปลี่ยนแปลงข้อมูลเพิ่มเติมจากการเปลี่ยนแปลงแก้ไขโปรแกรมหรือระบบงาน	• มีการจัดทำแผนการโอนเปลี่ยนแปลงข้อมูล ที่มีประสิทธิผล โดยมีการสอบทานแผน และการดำเนินการตามแผนโดยบุคคลที่เหมาะสม • มีการสอบทานข้อมูลที่มีการเปลี่ยนแปลงอย่างครบถ้วนถูกต้อง	• สอบทานความเหมาะสมของแผนและการอนุมัติแผนการเปลี่ยนแปลงข้อมูล • ตรวจสอบว่ามีการสอบทานข้อมูลที่มีการเปลี่ยนแปลงอย่างครบถ้วนถูกต้อง
การเปลี่ยนแปลงระบบจัดการฐานข้อมูล โครงสร้างฐานข้อมูล หรือความสัมพันธ์กันระหว่างข้อมูล อาจไม่ได้รับการอนุมัติ หรือเปลี่ยนแปลงไม่ครบถ้วนถูกต้อง	• ทุกการเปลี่ยนแปลง ระบบจัดการฐานข้อมูล และโครงสร้างของข้อมูลต้องได้รับการอนุมัติอย่างเหมาะสม • มีการสอบทานและทดสอบความครบถ้วนถูกต้องของการเปลี่ยนแปลง	• สุ่มเลือกการเปลี่ยนแปลงจากบันทึกของระบบ และสอบทานความเหมาะสมของการอนุมัติการเปลี่ยนแปลง • ตรวจสอบเพื่อให้มั่นใจว่า มีการสอบทานและทดสอบอย่างเหมาะสม
การเปลี่ยนแปลงระบบปฏิบัติการคอมพิวเตอร์และระบบเครือข่ายอาจไม่ได้รับการอนุมัติหรือเปลี่ยนแปลงไม่ครบถ้วนถูกต้อง	• ทุกการเปลี่ยนแปลงระบบปฏิบัติการคอมพิวเตอร์และระบบเครือข่ายต้องได้รับการอนุมัติอย่างเหมาะสม • มีการสอบทานและทดสอบความครบถ้วนถูกต้องของการเปลี่ยนแปลง	• สุ่มเลือกการเปลี่ยนแปลงจากบันทึกของระบบ และสอบทานความเหมาะสมของการอนุมัติการเปลี่ยนแปลง • ตรวจสอบเพื่อให้มั่นใจว่า มีการสอบทานและทดสอบอย่างเหมาะสม

7. การรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

ความเสี่ยงที่สำคัญในการใช้เทคโนโลยีสารสนเทศ คือความเสี่ยงด้านความปลอดภัยของข้อมูลและเทคโนโลยีสารสนเทศ ดังนั้น ผู้บริหารองค์กรจะต้องจัดให้มีกลไกการรักษาความปลอดภัยเทคโนโลยีสารสนเทศที่ครอบคลุมการใช้งานเทคโนโลยีสารสนเทศอย่างรอบด้าน ซึ่งประกอบด้วย

7.1 การบริหารและจัดการความปลอดภัยเทคโนโลยีสารสนเทศ (Security Management and Administration)

7.2 การรักษาความปลอดภัยทางกายภาพ (Physical Security)

7.3 การรักษาความปลอดภัยเชิงตรรกะ (Logical Security)

โดยมีรายละเอียดดังต่อไปนี้

7.1 การบริหารและจัดการความปลอดภัยเทคโนโลยีสารสนเทศ

7.1.1 ความรู้ทั่วไป

การบริหารและจัดการการรักษาความปลอดภัยเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อ

- ให้มั่นใจว่าการใช้เทคโนโลยีสารสนเทศเป็นไปตามมาตรฐานการรักษาความปลอดภัยที่ดี
- ให้มั่นใจว่าบุคลากรมีความรู้ความเข้าใจเกี่ยวกับการรักษาความปลอดภัยอย่างเพียงพอและสม่ำเสมอ
- ให้มั่นใจว่าการจัดการด้านความปลอดภัย เช่น การให้หรือเปลี่ยนแปลงสิทธิในการใช้ระบบคอมพิวเตอร์สอดคล้องกับความต้องการในการใช้ระบบคอมพิวเตอร์โดยรวมขององค์กร
- ให้มั่นใจว่ามีการติดตามสอบทานเหตุการณ์ที่เกี่ยวกับการรักษาความปลอดภัยอย่างสม่ำเสมอ และมีการรายงานเหตุการณ์ต่าง ๆ ให้กับผู้รับผิดชอบอย่างทันท่วงทีและสม่ำเสมอ

เพื่อบรรลุถึงวัตถุประสงค์ของการควบคุมข้างต้น ผู้บริหารองค์กรควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

7.1.1.1 การจัดทำและดำเนินการด้านนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

7.1.1.2 การจัดทำและปฏิบัติงานตามระเบียบปฏิบัติด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

7.1.1.3 การสร้างความเข้าใจและจิตสำนึกด้านความปลอดภัยเทคโนโลยีสารสนเทศ

7.1.1.1 การจัดทำและดำเนินการด้านนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

การบริหารความปลอดภัยเทคโนโลยีสารสนเทศที่ดีเริ่มจากการที่ผู้บริหารจะต้องจัดให้มีนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการดำเนินการและปฏิบัติงานของบุคลากรโดยรวมขององค์กร ทั้งผู้ที่รับผิดชอบโดยตรงด้านการรักษาความปลอดภัย และผู้ใช้งานทั่วไป

นโยบายด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศที่ดี ควรประกอบด้วย

- การกำหนดบทบาทหน้าที่และความรับผิดชอบด้านการรักษาความปลอดภัยของผู้ที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ ประกอบด้วย ผู้บริหารสูงสุด ผู้บริหารสายงานต่าง ๆ ผู้ใช้งานทั่วไป ผู้บริหารเทคโนโลยีสารสนเทศ เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศต่าง ๆ ผู้บริหารและเจ้าหน้าที่ด้านความปลอดภัยเทคโนโลยีสารสนเทศ และผู้สอบบัญชีเทคโนโลยีสารสนเทศ
- ระบุข้อกำหนดการทำงานด้านต่าง ๆ ของเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการรักษาความปลอดภัย เช่น ข้อกำหนดด้านรหัสผู้ใช้งานและรหัสผ่าน (User ID and Password) การติดตั้งและกำหนดตัวแปรด้านความปลอดภัยในระบบปฏิบัติการคอมพิวเตอร์ อุปกรณ์เครือข่าย และไฟร์วอลล์ (Firewall) การปรับปรุงระบบปฏิบัติการทางด้านการรักษาความปลอดภัย (Security Patching) และระเบียบปฏิบัติด้านการให้ ปรับปรุงและยกเลิก สิทธิการเข้าถึงและใช้งานเทคโนโลยีสารสนเทศ
- การกำหนดเจ้าของข้อมูล เจ้าของระบบงานเทคโนโลยีสารสนเทศ และการกำหนดบทบาทความรับผิดชอบของเจ้าของข้อมูลและเจ้าของระบบงานฯ
- การแบ่งชั้นของข้อมูล ซึ่งเป็นการจัดระดับชั้นของข้อมูลตามความสำคัญของข้อมูลต่อองค์กร เพื่อจัดทำแนวทางในการรักษาความปลอดภัยของข้อมูลในแต่ระดับชั้นที่เหมาะสม
- การติดตามและการกำหนดบทลงโทษถ้ามีการละเมิดหรือไม่ปฏิบัติตามนโยบาย ตัวอย่างของนโยบายด้านการใช้รหัสผ่าน (Password) ที่ดีนั้น ควรมีคุณสมบัติดังต่อไปนี้
    - มีการกำหนดความยาวขั้นต่ำ เช่น 8 ตัวอักษรขึ้นไป เป็นต้น
    - มีการกำหนดอายุการใช้งานของรหัสผ่าน เช่น จะต้องเปลี่ยนรหัสผ่านทุก 3 หรือ 6 เดือน เป็นต้น
    - กำหนดให้ใช้ตัวเลขผสมตัวอักษร
    - มีการกำหนดจำนวนครั้งสูงสุดที่สามารถใส่รหัสผ่านผิดก่อนที่ระบบจะยกเลิกการใช้งาน

ผู้บริหารสูงสุดควรเป็นผู้อนุมัติให้ความเห็นชอบในการบังคับใช้นโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ และจัดให้มีการเผยแพร่นโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ ให้กับบุคลากรที่เกี่ยวข้องรับทราบและเข้าใจหน้าที่ความรับผิดชอบ และสิ่งที่ควรปฏิบัติอย่างสม่ำเสมอ และควรจัดให้มีการปรับปรุงนโยบายการรักษาความปลอดภัยอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความเสี่ยงและเทคนิคการควบคุมอยู่ตลอดเวลา

7.1.1.2 การจัดทำและปฏิบัติงานตามระเบียบปฏิบัติด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ

เพื่อทำให้นโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ สามารถนำไปปฏิบัติได้อย่างสอดคล้องกับนโยบาย ควรจะจัดทำระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อเป็นแนวทางในทางปฏิบัติในรายละเอียด ซึ่งระเบียบปฏิบัติที่สำคัญประกอบด้วย

ระเบียบปฏิบัติด้านการจัดการรหัสผู้ใช้งาน (Users Administration Procedure) ซึ่งใช้สำหรับเป็นแนวทางในการจัดการด้านการสร้าง เปลี่ยนแปลง และยกเลิกรหัสผู้ใช้งาน ซึ่งประกอบด้วยขั้นตอนการขอและอนุมัติ การดำเนินการและการสอบทาน การยกเลิกและการสอบทานรหัสผู้ใช้งานเป็นประจำสม่ำเสมอ

ระเบียบปฏิบัติด้านการติดตามเหตุการณ์ที่อาจเกี่ยวข้องกับความปลอดภัยเทคโนโลยีสารสนเทศ (Security Incident Monitoring Procedure) ซึ่งระบุรายละเอียดของขั้นตอนการติดตามเหตุการณ์ ตั้งแต่การระบุเหตุการณ์ การกำหนดเงื่อนไขในการติดตาม การวิเคราะห์เหตุการณ์ การจัดการเบื้องต้น และการจัดทำรายงาน

7.1.1.3 การสร้างความเข้าใจและจิตสำนึกด้านความปลอดภัยเทคโนโลยีสารสนเทศ

เนื่องจากส่วนที่มีความเสี่ยงในด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศที่สำคัญที่สุดส่วนหนึ่งคือส่วนที่เกี่ยวข้องกับพฤติกรรมในการใช้งานของผู้ใช้งาน ซึ่งผู้ใช้งานอาจมีความเข้าใจต่อความเสี่ยง และการควบคุมที่แตกต่างกัน และอาจส่งผลให้มีการใช้งานระบบคอมพิวเตอร์อย่างไม่ปลอดภัย เนื่องมาจากความไม่เข้าใจถึงขั้นตอนการทำงานที่ถูกต้องเป็นไปตามนโยบายและหลักการการควบคุมที่ดี หรืออาจใช้งานโดยขาดจิตสำนึกที่ดีด้านการรักษาความปลอดภัย

ดังนั้นองค์กรควรจัดให้มีการสร้างความเข้าใจและจิตสำนึกด้านความปลอดภัยเทคโนโลยีสารสนเทศให้กับบุคลากรทุกคนที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ ซึ่งการสร้างความรู้และจิตสำนึกดังกล่าวอาจทำได้โดยการจัดให้มีการฝึกอบรมเพื่อสร้างความเข้าใจ (Awareness Training) อย่างต่อเนื่องและสม่ำเสมอ ซึ่งองค์กรส่วนมากจะเริ่มให้การฝึกอบรมดังกล่าวตั้งแต่วันแรก ๆ ที่บุคลากรเริ่มเข้ามาร่วมงานกับองค์กร เช่น ในช่วงการปฐมนิเทศ เป็นต้น

อย่างไรก็ตาม การสร้างความเข้าใจและจิตสำนึกนั้นอาจใช้วิธีการต่าง ๆ นอกเหนือจากการฝึกอบรม เช่น การประชาสัมพันธ์ข่าวสารจากผู้บริหาร จากหน่วยงานรักษาความปลอดภัยเทคโนโลยีสารสนเทศ การทำกิจกรรมวีดิทัศน์แสดงตัวอย่างภัยต่าง ๆ เป็นต้น

7.1.2 ความเสี่ยง การควบคุม และการตรวจสอบ

ในส่วนนี้เป็นการอธิบายถึงความเสี่ยง การควบคุมความเสี่ยง และการตรวจสอบเพื่อให้มั่นใจถึงประสิทธิภาพและประสิทธิผลของการควบคุมในการจัดการความเสี่ยง ด้านการบริหารและจัดการความปลอดภัยเทคโนโลยีสารสนเทศ ในส่วนที่อาจมีผลกระทบกับความน่าเชื่อถือของรายงานทางการเงิน

ความเสี่ยง	การควบคุม	การตรวจสอบ
การใช้เทคโนโลยีสารสนเทศอาจขาดความปลอดภัย และไม่เป็นไปในแนวทางเดียวกัน	• มีการกำหนดและอนุมัตินโยบายที่ชัดเจนในด้านการดำเนินงาน และการใช้งานเทคโนโลยีสารสนเทศ	• สอบถามถึงความมีอยู่จริงของนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ • สอบทานนโยบาย เพื่อให้มั่นใจว่าครอบคลุมการดำเนินการและการใช้งานเทคโนโลยีสารสนเทศอย่างเหมาะสม และมีการอนุมัติเพื่อบังคับใช้โดยผู้บริหารระดับสูง
บุคลากรอาจขาดการรับรู้ และเข้าใจในแนวทางการปฏิบัติตามที่กำหนดไว้ในนโยบาย	• มีแผนการสื่อสารและอบรมให้บุคลากรที่เกี่ยวข้องทราบและเข้าใจแนวทางการปฏิบัติงานตามนโนบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ และมีการติดตามการปฏิบัติตามแผนสื่อสารและแผนอบรม • มีการสำรวจอัตราการรับรู้และเข้าใจในนโยบายฯ อย่างสม่ำเสมอ	• สอบทานแผนการสื่อสารและการอบรม เพื่อให้มั่นใจว่า ครอบคลุมบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างครบถ้วนและเหมาะสม • ตรวจสอบการติดตามการปฏิบัติตามนโยบายและแผน เพื่อให้มั่นใจว่ามีการติดตามอย่างสม่ำเสมอ
อาจไม่มีการกำหนดโครงสร้างองค์กรที่ชัดเจนในด้านการรักษาความปลอดภัย และการกำหนดหน้าที่ความรับผิดชอบของเจ้าของข้อมูล เจ้าของระบบงาน ผู้บริหาร และเจ้าหน้าที่ด้านความปลอดภัยเทคโนโลยีสารสนเทศ และผู้ใช้งานทั่วไป เป็นต้น	• มีการกำหนดบทบาทหน้าที่ด้านความปลอดภัยเทคโนโลยีสารสนเทศอย่างชัดเจน โดยครอบคลุมหน้าที่ที่สำคัญ เช่น ผู้บริหารและเจ้าหน้าที่ด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ เจ้าของข้อมูล เจ้าของระบบงาน และผู้ใช้งาน	สอบทานโครงสร้างงานเทคโนโลยีสารสนเทศ และเอกสารระบุหน้าที่ความรับผิดชอบ เพื่อให้มั่นใจว่ามีการกำหนดหน้าที่อย่างชัดเจน
บุคลากรที่มีหน้าที่รับผิดชอบด้านการรักษาความปลอดภัยอาจขาดความรู้ความสามารถที่เพียงพอในด้านการจัดการความปลอดภัย ทั้งด้านการบริหารความปลอดภัย ความเสี่ยงด้านความปลอดภัย และความรู้ทางเทคนิคที่จำเป็น	• มีแผนการอบรมด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ และความรู้เชิงเทคนิคที่จำเป็นให้กับบุคลากรด้านการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ อย่างเพียงพอเหมาะสม • มีการติดตามการดำเนินการตามแผนการอบรมข้างต้นอย่างสม่ำเสมอ	• สอบทานความเหมาะสมของแผนการอบรม เพื่อให้มั่นใจว่าแผนการอบรมสอดคล้องกับเทคโนโลยีสารสนเทศที่มีใช้และจะนำมาใช้ในองค์กร • ตรวจสอบการติดตามการดำเนินการตามแผน เพื่อให้มั่นใจว่ามีการติดตามการฝึกอบรมอย่างสม่ำเสมอ

ความเสี่ยง	การควบคุม	การตรวจสอบ
รหัสผู้ใช้งานอาจไม่ถูกต้อง หรืออาจมีรหัสผู้ใช้งานที่ไม่มีความจำเป็นค้างอยู่ในระบบ	• มีกระบวนงานสำหรับ การให้หรือยกเลิกสิทธิในการเข้าถึงเทคโนโลยีสารสนเทศที่ชัดเจน • มีกระบวนการสอบทานความถูกต้องครบถ้วนของรหัสผู้ใช้งานและสิทธิการใช้งานอย่างสม่ำเสมอ	• สอบทานความเหมาะสมของกระบวนการให้หรือยกเลิกสิทธิ • สุ่มตรวจสอบรหัสผู้ใช้งานที่มีอยู่ในระบบว่าเป็นผู้ใช้งานที่ผ่านการอนุมัติและดำเนินการตามกระบวนงานที่กำหนดไว้ • ตรวจสอบการสอบทานความถูกต้องครบถ้วนของรหัสผู้ใช้งาน เพื่อให้มั่นใจว่ามีการดำเนินการอย่างสม่ำเสมอ
เหตุการณ์ต่าง ๆ ที่อาจเกี่ยวข้องกับความปลอดภัยเทคโนโลยีสารสนเทศ อาจไม่ได้รับการจัดการอย่างเหมาะสมและทันเวลา	• จัดให้มีการบันทึกเหตุการณ์ด้านความปลอดภัยทั้งโดยระบบ และโดยคนอย่างเหมาะสม • มีกระบวนการติดตาม เฝ้าระวัง และวิเคราะห์ เหตุการณ์ต่าง ๆ ที่อาจเกี่ยวข้องกับความปลอดภัยเทคโนโลยีสารสนเทศ เพื่อหาแนวทางป้องกันที่เหมาะสมในอนาคต	• ตรวจสอบว่ามีการบันทึกด้านความปลอดภัยทั้งโดยระบบ และโดยคนอย่างครบถ้วน เช่น การสอบทานการกำหนดพารามิเตอร์ที่เกี่ยวกับการบันทึกเหตุการณ์ของระบบคอมพิวเตอร์ เป็นต้น • สอบทานความเหมาะสมของกระบวนการติดตามเฝ้าระวัง และวิเคราะห์เหตุการณ์ต่าง ๆ เพื่อให้มั่นใจว่ามีการสอบทานบันทึกเหตุการณ์อย่างสม่ำเสมอ และมีการวิเคราะห์เพื่อหาสาเหตุและแนวทางแก้ไขในกรณีที่มีเหตุการณ์เกิดขึ้นซ้ำ ๆ กัน

7.2 การรักษาความปลอดภัยทางกายภาพ

7.2.1 ความรู้ทั่วไป

การควบคุมด้านการรักษาความปลอดภัยทางกายภาพมีวัตถุประสงค์ดังนี้

- เพื่อป้องกันมิให้บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงเครื่องคอมพิวเตอร์ และอุปกรณ์ที่สำคัญ ทำให้เกิดความเสียหายเกิดขึ้น
- เพื่อป้องกันอุบัติเหตุจากอัคคีภัยหรือภัยอื่น ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์
- เพื่อให้มีสภาพแวดล้อมที่เอื้อต่อการประมวลผลที่มีประสิทธิภาพ

เพื่อบรรลุถึงวัตถุประสงค์ของการควบคุมข้างต้น ผู้บริหารองค์กรควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

7.2.1.1 การควบคุมการเข้าถึงทางกายภาพของเครื่องคอมพิวเตอร์และอุปกรณ์

7.2.1.2 การควบคุมด้านสภาวะแวดล้อมการทำงานของเครื่องคอมพิวเตอร์และอุปกรณ์

7.2.1.1 การควบคุมการเข้าถึงทางกายภาพของระบบคอมพิวเตอร์และอุปกรณ์

การควบคุมที่สำคัญมีรายละเอียดดังต่อไปนี้

- จัดให้ห้องคอมพิวเตอร์อยู่ในสถานที่เหมาะสม เช่น ไม่เป็นที่พลุกพล่านด้วยผู้คนจำนวนมาก และหากอยู่ในอาคารก็ไม่ควรอยู่ชั้นที่สูงหรือต่ำเกินไป
- ควรมีการออกแบบแบ่งเป็นสัดส่วนตามความต้องการด้านการรักษาความปลอดภัย และตามลักษณะการใช้งาน เช่น ส่วนเฉพาะสำหรับพนักงานปฏิบัติการคอมพิวเตอร์ หรือส่วนเฉพาะของเจ้าหน้าที่เครือข่าย เป็นต้น
- ควรมีการติดตั้งระบบควบคุมการเข้าออกศูนย์คอมพิวเตอร์ซึ่งสามารถบันทึกการเข้าออกของบุคลากรแต่ละคนได้ เช่น การติดตั้งอุปกรณ์การควบคุมการเข้าออกแบบอิเล็กทรอนิกส์ เป็นต้น
- ควรจัดให้มีระเบียบการให้และยกเลิกบัตรหรืออุปกรณ์อื่น ๆ ที่ใช้ในการเปิดปิดประตูเข้าออกศูนย์คอมพิวเตอร์
- สำหรับการขอเข้าห้องคอมพิวเตอร์เป็นการชั่วคราว เช่น ช่างเทคนิคของบริษัทผู้ค้าคอมพิวเตอร์ ผู้สอบบัญชี ผู้เยี่ยมชม เป็นต้น ควรจัดให้มีการอนุญาตอย่างเหมาะสม และมีการบันทึกข้อมูลการเข้าออกอย่างเพียงพอ และมีเจ้าหน้าที่ขององค์กรเฝ้าสังเกตการณ์อยู่ตลอดเวลา
- สำหรับอุปกรณ์สำคัญที่อยู่ภายนอกห้องคอมพิวเตอร์ ควรจัดให้มีการป้องกันความปลอดภัยทางกายภาพสำหรับเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่สำคัญเหล่านั้นอย่างเหมาะสม

7.2.1.2 การควบคุมด้านสภาวะแวดล้อมการทำงานของเครื่องคอมพิวเตอร์และอุปกรณ์

การควบคุมประกอบด้วย

- จัดให้มีการติดตั้งและทดสอบอุปกรณ์ควบคุมสภาวะแวดล้อมของการทำงานของระบบคอมพิวเตอร์ในห้องคอมพิวเตอร์อย่างเพียงพอ เช่น มีการติดตั้งระบบปรับอุณหภูมิ ความชื้นและคลื่นแม่เหล็ก และอุปกรณ์ในการควบคุมความคงที่และจัดให้มีไฟฟ้าใช้อย่างต่อเนื่อง
- ไม่ควรติดตั้งระบบดับเพลิงที่ใช้น้ำเป็นปัจจัยสำคัญในการดับไฟ เช่น การติดตั้งระบบดับเพลิงด้วยน้ำ (Water Sprinkle) เป็นต้น
- ระบบปรับอากาศควรจะต่อเข้ากับระบบไฟฟ้าจากแหล่งเดียวกันกับระบบคอมพิวเตอร์ เพื่อทำให้มั่นใจว่าระบบปรับอากาศสามารถทำงานได้ในกรณีไฟฟ้าปกติขัดข้องและระบบคอมพิวเตอร์จะต้องใช้ไฟฟ้าจากแหล่งไฟฟ้าสำรอง

7.2.2 ความเสี่ยง การควบคุม และการตรวจสอบ

ในส่วนนี้เป็นการอธิบายถึงความเสี่ยง การควบคุมความเสี่ยง และการตรวจสอบเพื่อให้มั่นใจถึงประสิทธิภาพและประสิทธิผลของการควบคุมในการจัดการความเสี่ยงด้านการรักษาความปลอดภัยทางกายภาพในส่วนที่อาจมีผลกระทบกับความน่าเชื่อถือของรายงานทางการเงิน

ความเสี่ยง	การควบคุม	การตรวจสอบ
เครื่องคอมพิวเตอร์และอุปกรณ์ที่สำคัญอาจสูญหาย หรือใช้การไม่ได้	• จัดให้เครื่องคอมพิวเตอร์และอุปกรณ์ที่สำคัญอยู่ในห้องที่ปลอดภัย • มีการกำหนดให้เฉพาะผู้ที่จำเป็นเท่านั้นที่สามารถเข้าห้องคอมพิวเตอร์ และมีกระบวนการที่ชัดเจนในการให้และยกเลิกสิทธิในการเข้าห้องคอมพิวเตอร์ • มีระเบียบปฏิบัติสำหรับการอนุญาตให้เข้า-ออกชั่วคราว • มีการบันทึกการเข้าออกห้องคอมพิวเตอร์และมีการสอบทานบันทึกอย่างสม่ำเสมอ • มีการรักษาความปลอดภัยเครื่องคอมพิวเตอร์และอุปกรณ์ที่อยู่นอกห้องคอมพิวเตอร์	• สังเกตการณ์ด้านความปลอดภัยของห้องคอมพิวเตอร์ เพื่อให้มั่นใจว่า ห้องคอมพิวเตอร์มีการติดตั้งระบบป้องกันความปลอดภัยอย่างเหมาะสม • สอบทานกระบวนการให้และยกเลิกบัตรหรือรหัสผ่านที่ใช้สำหรับการเข้าออกห้องคอมพิวเตอร์ เพื่อให้มั่นใจว่า เฉพาะผู้ที่มีความจำเป็นเข้าไปปฏิบัติงานในห้องคอมพิวเตอร์มีสิทธิเข้าออกห้องคอมพิวเตอร์ • สุ่มสังเกตการณ์ด้านความปลอดภัยของเครื่องคอมพิวเตอร์และอุปกรณ์ที่อยู่นอกห้องคอมพิวเตอร์
เครื่องคอมพิวเตอร์และอุปกรณ์อื่นอาจทำงานไม่เต็มประสิทธิภาพเพราะอยู่ในสภาพแวดล้อมที่ไม่เหมาะสม	• มีการติดตั้งอุปกรณ์ควบคุมสภาพแวดล้อมของห้องคอมพิวเตอร์อย่างเหมาะสม ประกอบด้วย การควบคุมอุณหภูมิ ความชื้น ฝุ่นละออง เป็นต้น • ดำเนินการตรวจสอบความพร้อมใช้ของอุปกรณ์ควบคุมสภาพแวดล้อมอย่างสม่ำเสมอ	• สังเกตการณ์ความครบถ้วนเหมาะสมของการติดตั้งอุปกรณ์ควบคุมสภาพแวดล้อมของห้องคอมพิวเตอร์ • ตรวจสอบการบำรุงรักษาอุปกรณ์ควบคุมควบคุมสภาพแวดล้อม เปรียบเทียบกับวันที่การบำรุงรักษาตามคู่มือกับวันที่บำรุงรักษาจริง

7.3 การควบคุมด้านการรักษาความปลอดภัยเชิงตรรกะ

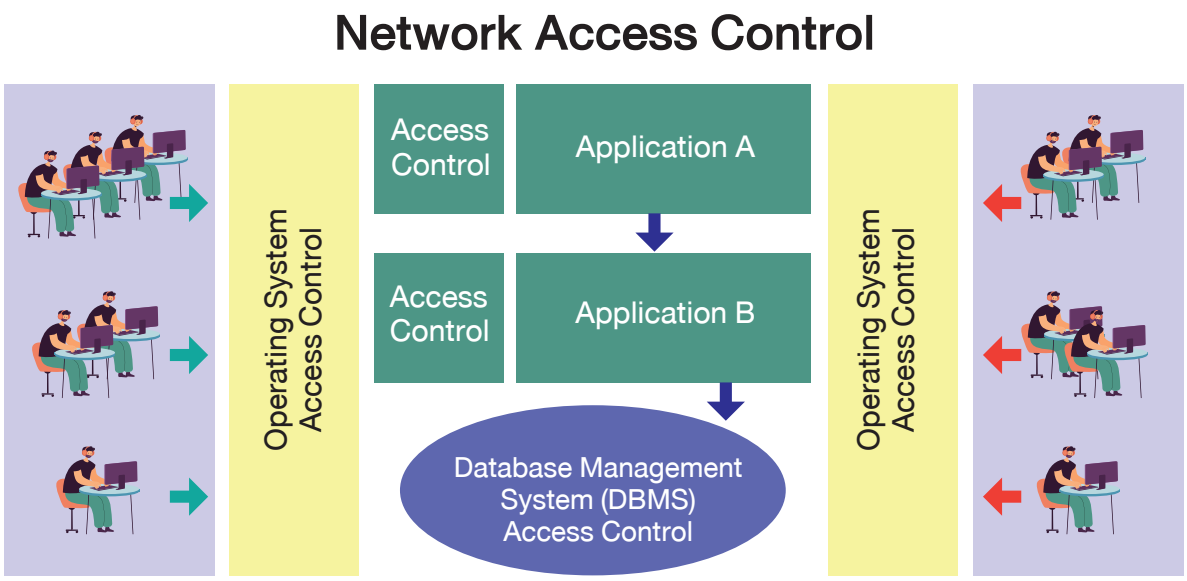
7.3.1 ความรู้ทั่วไป

การควบคุมด้านการรักษาความปลอดภัยเชิงตรรกะมีวัตถุประสงค์เพื่อ

- ป้องกันมิให้บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงเครื่องคอมพิวเตอร์ โปรแกรม ข้อมูล และคำสั่งต่าง ๆ ที่จัดเก็บหรือใช้งานอยู่ในระบบคอมพิวเตอร์
- เพื่อป้องกันมิให้ความลับของข้อมูลที่สำคัญรั่วไหลไปสู่บุคคลหรือองค์กรอื่น ๆ
- เพื่อทำให้เกิดความต่อเนื่องในการใช้ระบบคอมพิวเตอร์ โดยการป้องกันมิให้มีการโจมตีจากบุคคลหรือโปรแกรมที่มุ่งหวังทำให้เกิดความเสียหายต่อระบบ

เพื่อบรรลุถึงวัตถุประสงค์ของการควบคุมข้างต้น ผู้บริหารองค์กรควรจัดให้มีการควบคุมตามแนวทาง ดังต่อไปนี้

การควบคุมในด้านการรักษาความปลอดภัยเชิงตรรกะเป็นการทำงานผ่านกลไกทางเทคนิคของระบบคอมพิวเตอร์ ซึ่งภายในระบบคอมพิวเตอร์นั้น มีการควบคุมด้านความปลอดภัยเทคโนโลยีสารสนเทศอยู่หลายส่วนด้วยกัน ซึ่งสามารถอธิบายได้ดังภาพที่ 2.8 ต่อไปนี้



ภาพ 2.8 ส่วนต่าง ๆ ของการรักษาความปลอดภัยทาง Logical ของระบบคอมพิวเตอร์

การควบคุมด้านการรักษาความปลอดภัยเชิงตรรกะสามารถแบ่งออกเป็น 4 ส่วนคือ

ส่วนที่ 1 ของการรักษาความปลอดภัยคือส่วนที่ดำเนินการโดยระบบปฏิบัติการคอมพิวเตอร์ (Computer Operating System) ซึ่งทำหน้าที่ยืนยันตัวบุคคลที่จะเข้ามาใช้งาน (Authentication) ตรวจสอบสิทธิในการใช้งาน (Authorisation) และบันทึกกิจกรรมการใช้งาน (Audit Logging)

ส่วนที่ 2 เป็นส่วนของการรักษาความปลอดภัยระบบฐานข้อมูล ซึ่งทำงานโดยระบบจัดการฐานข้อมูล (Database Management System – DBMS) ซึ่งทำหน้าที่รักษาความปลอดภัยตารางข้อมูล (Data Table) ต่าง ๆ ที่จัดเก็บอยู่ในระบบคอมพิวเตอร์

ส่วนที่ 3 เป็นส่วนของการรักษาความปลอดภัยภายในระบบงานคอมพิวเตอร์ (Application System) ซึ่งทำงานโดยโปรแกรมของแต่ละระบบงาน โดยทำหน้าที่กำหนดสิทธิในการใช้งานฟังก์ชันต่าง ๆ ที่มีอยู่ในระบบงานนั้น ๆ

ส่วนสุดท้ายเป็นส่วนของการควบคุมในกรณีที่มีการต่อเชื่อมระบบคอมพิวเตอร์เป็นระบบเครือข่ายคอมพิวเตอร์ (Computer Network) ซึ่งทำหน้าที่รักษาความปลอดภัยด้านการสื่อสารและการเข้าถึงภายในระบบเครือข่าย

ในส่วนนี้ซึ่งเป็นเรื่องเกี่ยวกับการควบคุมทั่วไปของเทคโนโลยีสารสนเทศด้านการรักษาความปลอดภัยเชิงตรรกะนั้น จะครอบคลุมเฉพาะส่วนที่เป็นระบบต่าง ๆ ดังนี้

7.3.1.1 ระบบปฏิบัติการคอมพิวเตอร์ (Operating System)

7.3.1.2 ระบบจัดการฐานข้อมูล (DBMS)

7.3.1.3 ระบบเครือข่ายคอมพิวเตอร์ (Computer Network)

สำหรับส่วนของการรักษาความปลอดภัยในระบบงานคอมพิวเตอร์นั้นจะอยู่ในส่วนของการควบคุมระบบงาน (Application Controls)

7.3.1.1 ระบบปฏิบัติการคอมพิวเตอร์

ในส่วนของระบบปฏิบัติการคอมพิวเตอร์นั้นเป็นการรักษาความปลอดภัยซึ่งทำงานโดยโปรแกรมควบคุมการเข้าถึง (Access Control) ซึ่งการทำงานของโปรแกรมดังกล่าวขึ้นอยู่กับข้อมูลและค่าตัวแปรที่กำหนดไว้ล่วงหน้า เช่น ข้อมูลรหัสผู้ใช้งานและรหัสผ่าน (User ID/Password) และข้อมูลสิทธิการใช้งาน เป็นต้น ซึ่งการทำงานของการควบคุมความปลอดภัยในส่วนของระบบปฏิบัติการนั้นควรเริ่มจากการกำหนดมาตรฐานเกี่ยวกับการติดตั้งและการกำหนดค่าตัวแปรด้านความปลอดภัยของระบบปฏิบัติการคอมพิวเตอร์ และดำเนินการติดตั้งและปรับปรุงตามค่าตัวแปรมาตรฐานดังกล่าว แล้วดำเนินการตามแนวทางการควบคุมใน 3 ส่วนต่อไปนี้

7.3.1.1.1 การยืนยันตัวบุคคล (Authentication)

7.3.1.1.2 การตรวจสอบสิทธิการใช้งาน (Authorisation)

7.3.1.1.3 การบันทึกกิจกรรมการใช้งาน (Audit Logging)

ซึ่งทั้ง 3 ส่วนควรมีการควบคุม ดังต่อไปนี้

7.3.1.1.1 การยืนยันตัวบุคคล

- รหัสผู้ใช้งานควรกำหนดให้เป็นรายตัวบุคคล และไม่ควรอนุญาตให้มีการใช้งานร่วมกัน
- มีการกำหนดกฎเกณฑ์การใช้รหัสผ่าน เช่น การกำหนดความยาวขั้นต่ำ กำหนดอายุการใช้งานของรหัสผ่านทุก 60 วัน เป็นต้น มีการระงับการใช้งานชั่วคราวในกรณีใส่รหัสผิดเกินจำนวนครั้งที่กำหนดไว้ ไม่จดบันทึกรหัสผ่านไว้ในที่ต่าง ๆ และให้ถือว่ารหัสผ่านเป็นข้อมูลส่วนตัวของผู้ใช้งานเอง ซึ่งห้ามให้รหัสผ่านนี้กับผู้ใดไม่ว่าจะเป็นการชั่วคราวหรือถาวร
- มีการกำหนดลักษณะเฉพาะของการใช้งานของรหัสแต่ละกลุ่มการใช้งาน เช่น กลุ่มผู้ใช้งาน (End User) ควรจะอนุญาตให้ใช้งานเฉพาะตามที่ระบุไว้ในเมนูของระบบงานเท่านั้น
- จัดให้มีการควบคุมการใช้งานรหัสผู้ใช้งานและรหัสผ่านที่มาพร้อมกับการติดตั้งระบบ โดยเปลี่ยนรหัสผ่านหรือระงับการใช้งานรหัสผู้ใช้งานเหล่านี้ภายหลังการติดตั้งเสร็จเรียบร้อยแล้ว
- จัดให้มีการควบคุมการใช้งานรหัสผู้ใช้งานที่มีสิทธิในการใช้งานสูง (Privilege Users) โดยเฉพาะอย่างยิ่งรหัสผู้ใช้งานที่มีสิทธิในการใช้งานสูงสุด (Super User) โดยจำกัดจำนวนรหัสผู้ใช้งานเหล่านี้ให้น้อยที่สุดตามความจำเป็น และจัดให้มีการบันทึกกิจกรรมที่ทำโดยการใช้รหัสผู้ใช้เหล่านี้และควรมีการสอบทานกิจกรรมต่าง ๆ เหล่านี้อย่างสม่ำเสมอ
- มีการสอบทานข้อมูลการเข้าถึงระบบคอมพิวเตอร์อย่างสม่ำเสมอ เพื่อให้มั่นใจว่ารหัสผู้ใช้งานทั้งหมดเป็นรหัสที่มีเจ้าของและจำเป็นในการใช้งานจริง

7.3.1.1.2 การตรวจสอบสิทธิการใช้งาน

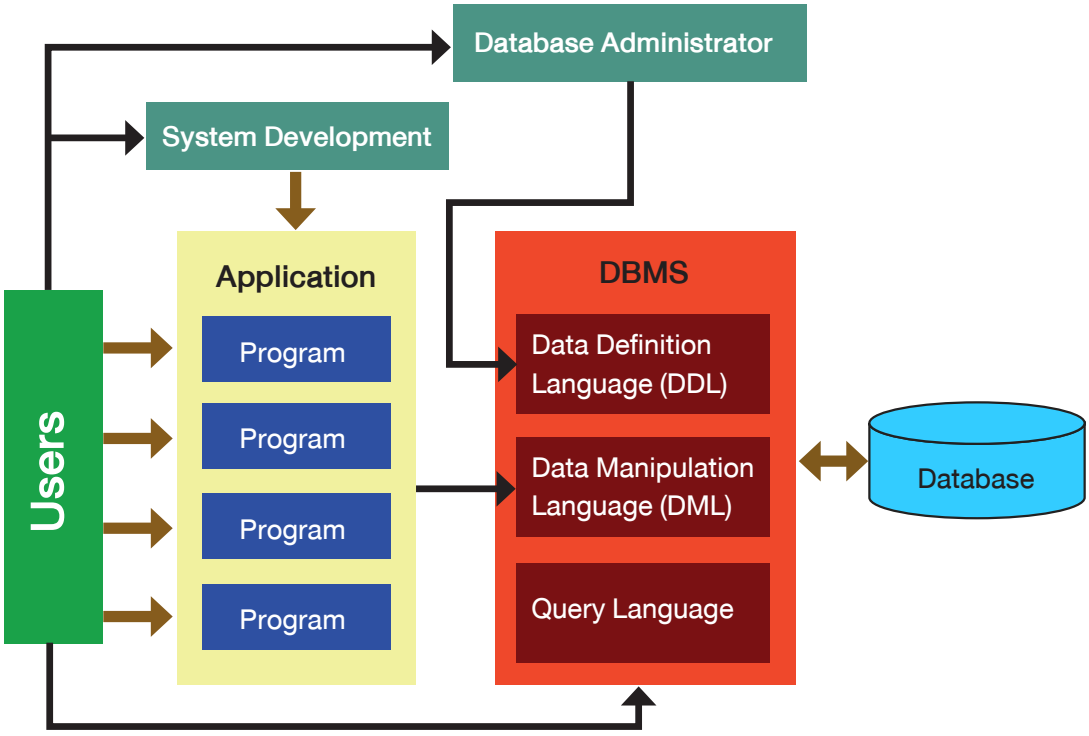
- การกำหนดสิทธิในการใช้งานตามความจำเป็นในการใช้งานเท่านั้น ตามหน้าที่ความรับผิดชอบของผู้ใช้งานแต่ละคน
- เจ้าหน้าที่ด้านการพัฒนาระบบงาน เช่น นักวิเคราะห์ระบบและโปรแกรมเมอร์ ไม่ควรได้รับอนุญาตให้ใช้ข้อมูลและโปรแกรมที่เป็นข้อมูลและโปรแกรมจริง
- อนุญาตให้ผู้ที่จำเป็นในการใช้งานเท่านั้นที่ได้สิทธิในการใช้ทรัพยากรที่มีอยู่ในระบบคอมพิวเตอร์ เช่น แฟ้มข้อมูลที่ใช้งานโดยระบบ (System Files) โปรแกรมที่ทำหน้าที่พิเศษ (System Utilities) และอุปกรณ์ต่อพ่วงต่าง ๆ

7.3.1.1.3 การบันทึกกิจกรรมการใช้งาน

- จัดให้มีการบันทึกกิจกรรมหรือเหตุการณ์ที่สำคัญในระบบคอมพิวเตอร์ เช่น เหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัย หรือกิจกรรมที่ทำโดยผู้ใช้รหัสที่มีสิทธิสูง หรือการใช้โปรแกรมที่สำคัญ หรือการใช้หรือเปลี่ยนแปลงข้อมูลที่สำคัญ
- จัดให้มีการสอบทานกิจกรรมดังกล่าวข้างต้นอย่างสม่ำเสมอโดยผู้ที่มีความรู้ที่เพียงพอและเป็นอิสระจากกิจกรรมต่าง ๆ เหล่านั้น

7.3.1.2 ระบบจัดการฐานข้อมูล

ในส่วนของการจัดการฐานข้อมูลนั้น เป็นการควบคุมการใช้งานและการเข้าถึงฐานข้อมูลซึ่งมีลักษณะการทำงานดังภาพต่อไปนี้



ภาพที่ 2.9 ส่วนต่างๆ ของการรักษาความปลอดภัยทาง Logical ของระบบจัดการฐานข้อมูล

จากภาพที่ 2.9 ระบบฐานข้อมูลสามารถแบ่งได้เป็น ฐานข้อมูล (Database) และระบบจัดการฐานข้อมูล (Database Management System – DBMS) ซึ่งการควบคุมส่วนใหญ่อยู่ที่การทำงานของระบบจัดการฐานข้อมูล ซึ่งแบ่งโปรแกรมออกเป็น 3 ส่วนคือ

โปรแกรมคำสั่งสำหรับกำหนดนิยามของฐานข้อมูล (Data Definition Language – DDL)

– ทำหน้าที่จัดการเกี่ยวกับโครงสร้างของฐานข้อมูล ซึ่งประกอบด้วยชุดคำสั่งเกี่ยวกับการสร้างและเปลี่ยนแปลงตารางข้อมูล (Table) สร้างมุมมอง (View) รวมถึงการกำหนดสิทธิในการใช้ข้อมูล

โปรแกรมคำสั่งสำหรับจัดการข้อมูล (Data Manipulation Language – DML)

– ทำหน้าที่จัดการเกี่ยวกับข้อมูล ซึ่งประกอบด้วยชุดคำสั่งเกี่ยวกับการอ่าน เขียน ปรับปรุง หรือลบข้อมูล

โปรแกรมคำสั่งสำหรับจัดการอ่านข้อมูล (Query Language)

– ทำหน้าที่ช่วยในการเรียกข้อมูลในฐานข้อมูลมาเพื่อจัดทำเป็นรายงานแบบง่าย ๆ

สำหรับการทำงานกับระบบฐานข้อมูลของผู้ที่เกี่ยวข้อง มีลักษณะดังนี้

ผู้จัดการฐานข้อมูล (Database Administrator) ทำหน้าที่บริหารจัดการโครงสร้างฐานข้อมูล ปรับปรุงฐานข้อมูล จัดการด้านความปลอดภัยฐานข้อมูล ซึ่งใช้งานระบบจัดการฐานข้อมูลผ่านโปรแกรมคำสั่งสำหรับกำหนดนิยามของฐานข้อมูล

ผู้พัฒนาระบบงาน ทำหน้าที่เขียนโปรแกรมเพื่ออ่านหรือปรับปรุงข้อมูลในฐานข้อมูลสำหรับการใช้งานของผู้ใช้งานผ่านโปรแกรมต่าง ๆ เหล่านั้น

ผู้ใช้งาน ซึ่งเป็นผู้ใช้ฐานข้อมูลทางอ้อมผ่านโปรแกรมคอมพิวเตอร์ที่เขียนโดยผู้พัฒนาระบบงาน ซึ่งโปรแกรมเหล่านี้ติดต่อกับระบบจัดการฐานข้อมูลผ่านโปรแกรม DML นอกจากนี้ผู้ใช้งานยังสามารถอ่านข้อมูลจากฐานข้อมูลโดยตรงผ่านโปรแกรม Query Language

ในส่วนของการควบคุมความปลอดภัยในระบบฐานข้อมูลนั้น ประกอบด้วย

- การบริหารจัดการรหัสผู้ใช้งานและรหัสผ่านให้สอดคล้องกับมาตรฐานการรักษาความปลอดภัยที่ดี
- การกำหนดสิทธิในการใช้คำสั่งต่าง ๆ ที่อยู่ในโปรแกรม DDL และ DML ให้สอดคล้องกับความจำเป็นตามหน้าที่ความรับผิดชอบ
- การกำหนดสิทธิในการใช้ตารางข้อมูล (Data Table) และมุมมองข้อมูล (Data View) ตามความจำเป็นตามหน้าที่ความรับผิดชอบ

7.3.1.3 ระบบเครือข่ายคอมพิวเตอร์

ในส่วนของระบบเครือข่ายนั้น ในส่วนแรกมีองค์ประกอบที่สำคัญของระบบเครือข่ายที่มีส่วนเกี่ยวข้องกับการควบคุมด้านความปลอดภัย ซึ่งองค์ประกอบที่สำคัญประกอบด้วย

- ระบบปฏิบัติการของเซิฟเวอร์ในส่วนที่เกี่ยวข้องกับระบบเครือข่าย (Network Operating System) ซึ่งทำหน้าที่ในการรับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์กับภายนอก ระบบปฏิบัติการจะทำงานร่วมกับแผงวงจรเครือข่าย (Network Card) เพื่อทำให้ระบบคอมพิวเตอร์สามารถติดต่อกับระบบคอมพิวเตอร์เครื่องอื่น ๆ ได้
- สายสัญญาณหรือการส่งแบบไร้สาย (Cable and Wireless) เป็นสื่อที่ข้อมูลใช้เป็นเส้นทางในการสื่อสารระหว่างระบบคอมพิวเตอร์ เช่น สายโทรศัพท์ (Twisted Pair) สายโคแอ็ก (Coaxial) สายไฟเบอร์ออฟติค (Fibre Optic) หรือผ่านคลื่นในรูปแบบต่าง ๆ เป็นต้น
- อุปกรณ์เครือข่ายที่เกี่ยวกับความปลอดภัย เช่น เราต์เตอร์ (Routers) ไฟร์วอลล์ (Firewall) เป็นต้น

สำหรับการควบคุมที่เกี่ยวกับระบบเครือข่ายนั้น ควรประกอบด้วยการควบคุมที่สำคัญดังต่อไปนี้

- การออกแบบระบบเครือข่ายเทคโนโลยีสารสนเทศควรคำนึงถึงความปลอดภัย กล่าวคือ มีการกำหนดขอบเขตของระบบเครือข่ายเทคโนโลยีสารสนเทศที่ชัดเจน มีการแบ่งขอบเขตของระบบเครือข่าย (Zoning) ตามความสำคัญและตามลักษณะการใช้งาน และมีการติดตั้งอุปกรณ์และซอฟต์แวร์ป้องกันความปลอดภัยอย่างเพียงพอสำหรับแต่ละเขตของระบบเครือข่าย
- เลือกใช้สื่อรับส่งสัญญาณที่เหมาะสมทั้งด้านความปลอดภัย ประสิทธิภาพ และต้นทุน เช่น สายไฟเบอร์ออฟติค (Fiber Optic) มีราคาแพงแต่ให้ความเร็วสูงและมีความปลอดภัยในระดับสูง
- จัดให้มีการควบคุมการใช้โมเด็ม (Modem) เฉพาะที่จำเป็น และไม่อนุญาตให้ติดตั้งโมเด็มก่อนได้รับอนุญาตอย่างเป็นทางการ
- มีการปรับปรุงค่าตัวแปรของอุปกรณ์เครือข่ายและกฎเกณฑ์ของไฟร์วอลล์ให้สอดคล้องกับลักษณะการใช้งานและความเสี่ยง
- มีการแปลงรหัสข้อมูลระหว่างการรับส่งที่เหมาะสม

7.2.2 ความเสี่ยง การควบคุม และการตรวจสอบ

ในส่วนนี้เป็นการอธิบายถึงความเสี่ยง การควบคุมความเสี่ยง และการตรวจสอบเพื่อให้มั่นใจถึงประสิทธิภาพและประสิทธิผลของการควบคุมในการจัดการความเสี่ยงด้านการรักษาความปลอดภัยเชิงตรรกะ ในส่วนที่อาจมีผลกระทบกับความน่าเชื่อถือของรายงานทางการเงิน

ความเสี่ยง	การควบคุม	การตรวจสอบ
ระบบปฏิบัติการคอมพิวเตอร์ ระบบจัดการฐานข้อมูล และระบบเครือข่ายอาจไม่ปลอดภัยเนื่องจาก การติดตั้งไม่เป็นไปตามแนวทางการรักษาความปลอดภัยที่ดี หรือไม่สอดคล้องกับนโยบายรักษาความปลอดภัยเทคโนโลยีสารสนเทศขององค์กร	• จัดให้มีมาตรฐานด้านความปลอดภัยเชิงเทคนิค (Technical Security Standard or Baseline) ตามนโยบายรักษาความปลอดภัย เพื่อใช้เป็นแนวทางในการติดตั้งและปรับปรุงแก้ไขระบบปฏิบัติการคอมพิวเตอร์ • มีการสอบทานความสอดคล้องกันระหว่างมาตรฐานฯ และการติดตั้งจริงในเครื่องคอมพิวเตอร์แต่ละเครื่องอย่างสม่ำเสมอ	• สอบทานความมีอยู่จริงและความเหมาะสมของมาตรฐานด้านความปลอดภัยเชิงเทคนิค • ตรวจสอบเพื่อให้มั่นใจว่ามีการสอบทานความสอดคล้องกันระหว่างมาตรฐานฯ และการติดตั้งจริงในเครื่องคอมพิวเตอร์แต่ละเครื่องอย่างสม่ำเสมอ
ระบบปฏิบัติการคอมพิวเตอร์ ระบบจัดการฐานข้อมูลและระบบเครือข่าย ไม่มีความปลอดภัยที่เพียงพอ เนื่องจาก การกำหนดค่าตัวแปร (Security Parameters) อาจไม่เป็นไปตามมาตรฐานการรักษาความปลอดภัยที่ดี เช่น ค่าตัวแปรด้านการใช้รหัสผ่าน (Password Parameters) ค่าตัวแปรด้านการกำหนดสิทธิในการใช้งาน (System Authorisation Parameters) และค่าตัวแปรด้านการบันทึกกิจกรรมของระบบฯ (Audit Logging Parameters)	• มีการกำหนดค่าพารามิเตอร์ด้านความปลอดภัยอย่างเหมาะสมและสอดคล้องกับมาตรฐานด้านความปลอดภัยเชิงเทคนิค	• สุ่มตรวจสอบค่าพารามิเตอร์ด้านความปลอดภัยว่าสอดคล้องกับมาตรฐานด้านความปลอดภัยเชิงเทคนิคหรือไม่ ซึ่งอย่างน้อยควรครอบคลุมค่าพารามิเตอร์เกี่ยวกับการควบคุมรหัสผ่าน การเข้าถึงโปรแกรมและข้อมูลที่สำคัญของระบบฯ และ การบันทึกกิจกรรมระบบฯ
อาจมีรหัสผู้ใช้งานที่ไม่มีความจำเป็นอยู่ในระบบ	• มีกระบวนการที่ชัดเจนในการให้เปลี่ยนแปลงและยกเลิกรหัสผู้ใช้งานเมื่อหมดความจำเป็นในการใช้งาน • มีการสอบทานรหัสผู้ใช้งานอย่างสม่ำเสมอ	• ตรวจสอบความมีอยู่จริงและสอบทานความเหมาะสมของกระบวนการการให้และยกเลิกรหัสผู้ใช้งาน • สุ่มตรวจสอบการดำเนินการตามกระบวนการให้เปลี่ยนแปลงและยกเลิกรหัสผู้ใช้งาน โดยเลือกรหัสผู้ใช้งานในระบบย้อนกลับไปถึงเอกสารที่ใช้ในการอนุมัติเพื่อสร้างหรือเปลี่ยนแปลงแก้ไขรหัสผู้ใช้งานนั้น ๆ • ตรวจสอบเพื่อให้มั่นใจว่ามีการสอบทานรหัสผู้ใช้งานอย่างสม่ำเสมอ • เปรียบเทียบรหัสผู้ใช้งานกับรายชื่อผู้ที่จำเป็นในการใช้ระบบ เพื่อให้มั่นใจว่าไม่มีรหัสผู้ใช้งานที่ไม่จำเป็นหลงเหลืออยู่ในระบบฯ

ความเสี่ยง	การควบคุม	การตรวจสอบ
บุคคลที่ไม่มีความจำเป็นอาจเข้าถึงทรัพยากรระบบที่สำคัญ เช่น โปรแกรม หรือข้อมูลที่สำคัญได้	• มีการกำหนดตารางสิทธิเพื่อใช้ในการกำหนดการเข้าถึงทรัพยากรระบบอย่างเหมาะสม • มีการสอบทานสิทธิของแต่ละรหัสผู้ใช้งานอย่างสม่ำเสมอ	• ตรวจสอบความมีอยู่จริงและสอบทานความเหมาะสมของตารางสิทธิ • ตรวจสอบเพื่อให้มั่นใจว่ามีการสอบทานสิทธิของแต่ละรหัสผู้ใช้งานอย่างสม่ำเสมอ • สุ่มตรวจสอบพารามิเตอร์ที่เกี่ยวกับการเข้าถึงทรัพยากรที่สำคัญ เช่นโปรแกรม และข้อมูลที่สำคัญเพื่อให้มั่นใจว่าเฉพาะผู้ที่มีความจำเป็นเท่านั้นที่สามารถเข้าถึงทรัพยากรเหล่านั้นได้
เหตุการณ์ที่อาจเป็นความเสี่ยงด้านความปลอดภัยเทคโนโลยีสารสนเทศ อาจไม่ถูกตรวจพบและจัดการอย่างทันท่วงที	• กำหนดให้ระบบบันทึกกิจกรรมที่สำคัญ • มีการสอบทานบันทึกกิจกรรมฯ อย่างสม่ำเสมอ และมีการดำเนินการที่เหมาะสมสำหรับกิจกรรมที่ล่อแหลมต่อความปลอดภัยของระบบฯ	• ตรวจสอบพารามิเตอร์ด้านการบันทึกกิจกรรมของระบบฯ เพื่อให้มั่นใจว่ามีการบันทึกกิจกรรมที่สำคัญ • ตรวจสอบการสอบทานบันทึกกิจกรรมฯ เพื่อให้มั่นใจว่ามีการสอบทานอย่างสม่ำเสมอ และมีการดำเนินการอย่างทันท่วงทีในกรณีที่พบกิจกรรรมที่มีความล่อแหลมต่อความปลอดภัย
ผู้ที่ไม่ได้รับอนุญาตอาจเข้าถึงข้อมูลสำคัญของระบบจัดการฐานข้อมูล	• จัดให้มีการควบคุมความปลอดภัยระบบฐานข้อมูลครอบคลุม - รหัสผู้ใช้และรหัสผ่าน - การเข้าถึงชุดคำสั่ง และข้อมูล - การบันทึกกิจกรรม	• สุ่มตรวจสอบพารามิเตอร์ด้านความปลอดภัยของระบบจัดการฐานข้อมูลเปรียบเทียบกับค่ามาตรฐานด้านความปลอดภัยหรือนโยบายขององค์กร • สุ่มตรวจสอบสิทธิการเข้าถึงฐานข้อมูลเพื่อให้มั่นใจว่าผู้ที่มีความจำเป็นเท่านั้นสามารถเข้าถึงข้อมูล • ตรวจสอบเพื่อให้มั่นใจว่ามีการสอบทานบันทึกกิจกรรมในระบบจัดการฐานข้อมูลอย่างสม่ำเสมอ
ระบบเครือข่ายอาจไม่มีความปลอดภัยเพียงพอ	• จัดให้มีการควบคุมความปลอดภัยระบบเครือข่ายซึ่งครอบคลุม - การออกแบบระบบเครือข่ายให้มีการแบ่งตามความต้องการในการใช้งาน - การจัดวางอุปกรณ์ด้านความปลอดภัยในตำแหน่งที่เหมาะสม - การกำหนดพารามิเตอร์ของอุปกรณ์ด้านความปลอดภัย - การติดตั้งซอฟต์แวร์ด้านความปลอดภัยระบบเครือข่าย	• สอบทานการออกแบบระบบเครือข่ายเพื่อให้มั่นใจว่ามีการแบ่งแยกระบบเครือข่ายออกตามลักษณะการใช้งาน และมีการติดตั้งอุปกรณ์ด้านความปลอดภัย เช่น เราต์เตอร์และไฟร์วอลล์ อย่างเหมาะสม • ตรวจสอบการควบคุมรหัสผู้ใช้งานและรหัสผ่านของเราต์เตอร์และไฟร์วอลล์ • ตรวจสอบความเหมาะสมของการกำหนดข้อมูล เช่น เส้นทางของข้อมูล การให้บริการต่าง ๆ และกฎเกณฑ์การกลั่นกรองรายการ (Rule Base) ของเราต์เตอร์และไฟร์วอลล์

8. การปฏิบัติการคอมพิวเตอร์

8.1 ความรู้ทั่วไป

ก่อนที่จะทำความเข้าใจการควบคุมการปฏิบัติการเทคโนโลยีสารสนเทศ ลำดับแรกควรทำความเข้าใจการทำงานปฏิบัติการเทคโนโลยีสารสนเทศเสียก่อนว่างานดังกล่าวมีรายละเอียดอย่างไร ซึ่งงานปฏิบัติการเทคโนโลยีสารสนเทศประกอบด้วยงานดังต่อไปนี้

- งานเปิด-ปิด เครื่องและระบบคอมพิวเตอร์
- งานติดตามดูแลและสนับสนุนการใช้งาน
- งานประมวลผลสิ้นวันและการจัดพิมพ์รายงาน
- งานสำรองและกู้ข้อมูล
- งานบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ

งานเปิด-ปิด เครื่องและระบบคอมพิวเตอร์ ก่อนเริ่มปฏิบัติงานกับระบบคอมพิวเตอร์ พนักงานปฏิบัติการจะต้องเปิดเครื่องคอมพิวเตอร์ และระบบงานเทคโนโลยีสารสนเทศเสียก่อน มิฉะนั้นจะไม่มีผู้ใช้งานคนใดสามารถใช้ได้ และก่อนจบงานก็จะต้องปิดระบบงาน ซึ่งจะต้องมีกระบวนการตรวจสอบก่อนว่าผู้ใช้งานทุกคนใช้งานหรือป้อนข้อมูลเสร็จสิ้นหมดแล้ว ก่อนจะทำการปิดระบบงานและปิดเครื่องคอมพิวเตอร์ ตามลำดับ

งานติดตามดูแลและสนับสนุนการใช้งาน เป็นการติดตามการใช้งานและให้ความช่วยเหลือและสนับสนุนการใช้งาน ซึ่งประกอบด้วยการรับรู้รับแจ้งเหตุการณ์หรือปัญหาต่าง ๆ ตรวจสอบเหตุการณ์หรือปัญหา บันทึกรายละเอียด ประสานงานเพื่อการจัดการแก้ไข และสรุปปิดเหตุการณ์และปัญหาที่เกิดขึ้น

งานประมวลผลสิ้นวันและการจัดพิมพ์รายงาน เมื่อปิดระบบงานเรียบร้อยแล้ว พนักงานปฏิบัติการคอมพิวเตอร์จะเริ่มการประมวลผลสิ้นวัน โดยส่วนใหญ่จะเป็นการประมวลผลโปรแกรมตามลำดับก่อนหลังที่ถูกกำหนดไว้ล่วงหน้าโดยผู้ออกแบบระบบงาน และถ้ามีการจัดพิมพ์รายงานสิ้นวัน พนักงานปฏิบัติการคอมพิวเตอร์ก็จะจัดการพิมพ์รายงานโดยใช้แบบฟอร์มที่จัดเตรียมไว้ล่วงหน้า

งานสำรองและกู้ข้อมูล เป็นงานที่ดำเนินการระหว่างการประมวลผลสิ้นวัน ซึ่งครอบคลุมการสำรองข้อมูลจากระบบคอมพิวเตอร์มาไว้ที่อุปกรณ์สำรองข้อมูล เช่น เทป หรือแผ่นดิสก์ เป็นต้น และการนำข้อมูลสำรองไปจัดเก็บไว้ในสถานที่ปลอดภัยทั้งในและนอกศูนย์คอมพิวเตอร์ และในกรณีที่จะต้องกู้ข้อมูล พนักงานปฏิบัติการคอมพิวเตอร์ จะทำหน้าที่นำข้อมูลสำรองที่เก็บไว้มาแทนข้อมูลในระบบงานจริง

งานบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ เป็นการบำรุงรักษาระบบฯ ตามระยะเวลา หรือจัดให้มีการซ่อมแซมเปลี่ยนแปลงเมื่อเกิดเหตุขัดข้อง

การทำงานของระบบคอมพิวเตอร์นั้นจำเป็นที่จะต้องมีการควบคุมดูแล ซึ่งความรับผิดชอบในการทำงานในส่วนนี้เป็นหน้าที่ของผู้ปฏิบัติการคอมพิวเตอร์ ซึ่งถ้ามีข้อผิดพลาดเกิดขึ้นจะส่งผลกระทบต่อเทคโนโลยีสารสนเทศโดยรวม เช่น ถ้าผู้ปฏิบัติการคอมพิวเตอร์ประมวลผลโปรแกรมผิดลำดับ อาจทำให้ข้อมูลรายการต่าง ๆ ผิดทั้งหมดก็ได้ และโดยส่วนมากผู้ปฏิบัติการคอมพิวเตอร์จะไม่ใช่ผู้เชี่ยวชาญด้านคอมพิวเตอร์ ทำให้โอกาสเกิดข้อผิดพลาดในการทำงานสูงขึ้น

เพื่อให้ง่ายต่อการทำความเข้าใจจะแบ่งการควบคุมด้านการปฏิบัติการคอมพิวเตอร์ออกเป็น 3 กลุ่ม ประกอบด้วย

8.1.1 การควบคุมด้านการประมวลผลของเทคโนโลยีสารสนเทศ

8.1.2 การสำรองข้อมูลและการนำข้อมูลสำรองกลับมาใช้

8.1.3 การควบคุมด้านการปฏิบัติการคอมพิวเตอร์ อื่น ๆ

ซึ่งมีวัตถุประสงค์และแนวทางการควบคุมดังต่อไปนี้

8.1.1 การควบคุมด้านการประมวลผลของเทคโนโลยีสารสนเทศ

การควบคุมด้านการประมวลผลของเทคโนโลยีสารสนเทศ มีวัตถุประสงค์เพื่อทำให้การประมวลผลเทคโนโลยีสารสนเทศมีความถูกต้อง ครบถ้วน ตรงเวลา และตรงกับความต้องการของผู้ใช้งาน และเพื่อให้เจ้าหน้าที่ผู้ปฏิบัติการเทคโนโลยีสารสนเทศมีความรู้ความเข้าใจในการปฏิบัติการคอมพิวเตอร์ และระบบงานต่าง ๆ อย่างเพียงพอ

เพื่อบรรลุถึงวัตถุประสงค์ของการควบคุมข้างต้น ผู้บริหารองค์กรควรจัดให้มีการควบคุมตามแนวทาง ดังต่อไปนี้

- กำหนดให้มีระเบียบการปฏิบัติงานที่ชัดเจนสำหรับงานการประมวลผลของเทคโนโลยีสารสนเทศ
- มีการจัดทำตารางการประมวลผลสิ้นวันอย่างเป็นทางการ และผู้ปฏิบัติการเทคโนโลยีสารสนเทศใช้ตารางดังกล่าวในการดำเนินการประมวลผลสิ้นวัน และบันทึกรายละเอียดต่าง ๆ ของการประมวลผลไว้ในตารางนี้
- ผู้ควบคุมงานปฏิบัติการเทคโนโลยีสารสนเทศสอบทานตารางการประมวลผลสิ้นวันเพื่อทำให้มั่นใจว่าการประมวลผลสิ้นวันได้รับการประมวลผลอย่างครบถ้วนถูกต้อง และเป็นไปตามที่กำหนดไว้
- จัดให้มีการประเมินความรู้ความสามารถของผู้ปฏิบัติการเทคโนโลยีสารสนเทศ และจัดให้มีการฝึกอบรมเพื่อทำให้มั่นใจว่าผู้ปฏิบัติการเทคโนโลยีสารสนเทศมีความรู้ ความเข้าใจต่อการประมวลผลของเทคโนโลยีสารสนเทศ และความรู้ด้านระบบงานต่าง ๆ ที่องค์กรมีใช้งานอยู่ อย่างเพียงพอ

8.1.2 การสำรองข้อมูลและการนำข้อมูลสำรองกลับมาใช้

การควบคุมด้านการสำรองข้อมูลและการนำข้อมูลสำรองกลับมาใช้มีวัตถุประสงค์เพื่อทำให้มีการสำรองข้อมูลอย่างเพียงพอ และสามารถนำข้อมูลสำรองกลับมาใช้อย่างถูกต้อง ครบถ้วน ตรงเวลา และตรงกับความต้องการในการใช้ข้อมูลขององค์กร

เพื่อบรรลุถึงวัตถุประสงค์ของการควบคุมข้างต้น ผู้บริหารองค์กรควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

- กำหนดให้มีระเบียบการปฏิบัติงานที่ชัดเจนสำหรับการสำรองข้อมูลและการนำข้อมูลสำรองกลับมาใช้
- มีการจัดทำตารางการสำรองข้อมูลและโปรแกรมอย่างเป็นทางการ และผู้ปฏิบัติการเทคโนโลยีสารสนเทศใช้ตารางดังกล่าวในการดำเนินการสำรองข้อมูล และบันทึกรายละเอียดต่าง ๆ ของการสำรองข้อมูลไว้ในตารางนี้
- ผู้ควบคุมงานปฏิบัติการเทคโนโลยีสารสนเทศสอบทานตารางการสำรองข้อมูล เพื่อทำให้มั่นใจว่าการสำรองข้อมูลเป็นไปอย่างครบถ้วนถูกต้องและเป็นไปตามที่กำหนดไว้
- มีการจัดเก็บข้อมูลสำรองไว้ในที่ที่ปลอดภัย ทั้งที่เก็บไว้ที่ศูนย์คอมพิวเตอร์ภายใน และที่นำไปจัดเก็บไว้ที่สถานที่จัดเก็บภายนอก

8.1.3 การควบคุมด้านการปฏิบัติการคอมพิวเตอร์ อื่น ๆ

การปฏิบัติการคอมพิวเตอร์อื่น ๆ ประกอบด้วยกระบวนงาน ดังต่อไปนี้

- งานเปิด-ปิด เครื่องและระบบคอมพิวเตอร์
- งานติดตามดูแลและสนับสนุนการใช้งาน
- การจัดพิมพ์รายงาน
- งานบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ

ซึ่งมีวัตถุประสงค์ของการควบคุมในแต่ละกระบวนงาน เพื่อให้ระบบคอมพิวเตอร์สามารถให้บริการผู้ใช้งานอย่างมีประสิทธิภาพและตรงกับความต้องการในการใช้งาน ซึ่งมีแนวทางในการควบคุมดังนี้

- จัดให้มีการตกลงกันระหว่างผู้รับบริการหรือผู้ใช้งานและผู้ให้บริการหรือผู้บริหารงานปฏิบัติการเทคโนโลยีสารสนเทศ เพื่อกำหนดเป็นระดับการให้บริการ (Service Level Agreement) เพื่อเป็นแนวทางในการบริหารการบริการของผู้บริหารงานปฏิบัติการเทคโนโลยีสารสนเทศ
- จัดให้มีระบบการรายงานผลการดำเนินการตามระดับการให้บริการที่ตกลงไว้เพื่อทำให้มั่นใจว่าการให้บริการเป็นไปตามที่ตกลงไว้ โดยที่รายงานดังกล่าวควรมีการจัดส่งให้ทั้งผู้บริหารของผู้ให้บริการและผู้บริหารของผู้รับบริการ
- กำหนดให้มีระเบียบการปฏิบัติงานที่ชัดเจนสำหรับงานปฏิบัติการเทคโนโลยี เทคโนโลยีสารสนเทศที่สำคัญ ดังต่อไปนี้
  - งานเปิด-ปิด เครื่องและระบบคอมพิวเตอร์
  - งานติดตามดูแลและสนับสนุนการใช้งาน
  - การจัดพิมพ์รายงาน
  - งานบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ
- ถ้ามีการปฏิบัติการนอกเหนือจากที่กำหนดไว้ในระเบียบปฏิบัติจะต้องมีการบันทึกเหตุผลของการดำเนินการและการอนุมัติ ไว้อย่างชัดเจน
- จัดให้มีการสอบทานการทำงานของผู้ปฏิบัติการเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการดำเนินการดังกล่าวเป็นไปตามที่กำหนดไว้ในระเบียบปฏิบัติอย่างเคร่งครัด
- จัดให้มีการประเมินความรู้ความสามารถของผู้ปฏิบัติการเทคโนโลยีสารสนเทศ และจัดให้มีการฝึกอบรมเพื่อทำให้มั่นใจว่าผู้ปฏิบัติการเทคโนโลยีสารสนเทศมีความรู้ความเข้าใจต่อการปฏิบัติการเทคโนโลยีสารสนเทศ และความรู้ด้านระบบงานต่าง ๆ ที่องค์กรมีใช้งานอยู่อย่างเพียงพอต่อการปฏิบัติการเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพและปราศจากข้อผิดพลาด
- จัดให้มีช่องทางและผู้รับผิดชอบโดยตรงในการรับแจ้งและจัดการกับปัญหาต่าง ๆ ที่เกิดขึ้นกับเทคโนโลยีสารสนเทศ และกำหนดเป็นระเบียบปฏิบัติที่ชัดเจนในการแจ้งบันทึก และติดตามแก้ไขปัญหา
- มีการบันทึกรายละเอียดของปัญหาโดยละเอียดประกอบด้วย วันและเวลาที่เกิดปัญหา ผู้แจ้งและผู้รับแจ้ง ลักษณะของปัญหา ผลการวิเคราะห์ และผลการแก้ไขปัญหา
- มีการวิเคราะห์แนวโน้มของปัญหาต่าง ๆ เพื่อวางมาตรการแก้ไขปัญหาระยะยาว และป้องกันมิให้ปัญหาเกิดขึ้นอย่างซ้ำซ้อน
- มีการจัดทำตารางการพิมพ์รายงานอย่างเป็นทางการ และผู้ปฏิบัติการเทคโนโลยี เทคโนโลยีสารสนเทศใช้ตารางดังกล่าวในการดำเนินการพิมพ์รายงาน และบันทึกรายละเอียดต่าง ๆ ของการพิมพ์รายงานไว้ในตารางนี้
- มีกระบวนการที่ทำให้มั่นใจว่าผู้ใช้รายงานได้รับรายงานอย่างถูกต้องและครบถ้วน เช่น จัดให้มีการเซ็นรับรายงานโดยผู้ใช้งาน หรือการจัดส่งรายงานในรูปแบบอิเล็กทรอนิกส์
- จัดให้มีตารางการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงโดยละเอียดแยกเป็นรายการต่างหาก และดำเนินการให้มีการบำรุงรักษาตามตารางที่กำหนดไว้อย่างเคร่งครัด
- มีการควบคุมการทำงานของช่างผู้ทำการบำรุงรักษาอย่างใกล้ชิด ในระหว่างที่ดำเนินการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

8.2 ความเสี่ยง การควบคุม และการตรวจสอบ

ในส่วนนี้เป็นการอธิบายถึงความเสี่ยง การควบคุมความเสี่ยง และการตรวจสอบเพื่อให้มั่นใจถึงประสิทธิภาพและประสิทธิผลของการควบคุมในการจัดการความเสี่ยง ด้านการปฏิบัติการคอมพิวเตอร์ ในส่วนที่อาจมีผลกระทบกับความน่าเชื่อถือของรายงานทางการเงิน

ความเสี่ยง	การควบคุม	การตรวจสอบ
การประมวลผลคอมพิวเตอร์อาจไม่ถูกต้องครบถ้วน	• กำหนดให้มีระเบียบการปฏิบัติงานที่ชัดเจนสำหรับงานการประมวลผลของเทคโนโลยีสารสนเทศ • มีการจัดทำตารางการประมวลผลสิ้นวันอย่างเป็นทางการ และผู้ปฏิบัติการเทคโนโลยีสารสนเทศใช้ตารางดังกล่าวในการดำเนินการประมวลผลสิ้นวัน และบันทึกรายละเอียดต่าง ๆ ของการประมวลผลไว้ในตาราง • ผู้ควบคุมงานสอบทานตารางการประมวลผลสิ้นวัน เพื่อตรวจสอบความครบถ้วนถูกต้องของการประมวลผล	• สอบทานความมีอยู่จริงและความเหมาะสมของระเบียบการปฏิบัติงานที่ชัดเจนสำหรับงานการประมวลผล • ตรวจสอบเพื่อให้มั่นใจว่า ผู้ควบคุมงานสอบทานตารางการประมวลผลสิ้นวันอย่างสม่ำเสมอ
การสำรองข้อมูลอาจไม่ถูกต้องครบถ้วน	• กำหนดให้มีระเบียบการปฏิบัติงานที่ชัดเจนสำหรับการสำรองข้อมูล • มีการจัดทำตารางการสำรองข้อมูลอย่างเป็นทางการ และผู้ปฏิบัติการเทคโนโลยีสารสนเทศใช้ตารางดังกล่าวในการสำรองข้อมูล และบันทึกรายละเอียดต่าง ๆ ของการสำรองข้อมูลไว้ในตาราง • ผู้ควบคุมงานสอบทานตารางการสำรองข้อมูล เพื่อตรวจสอบความครบถ้วนถูกต้องของการสำรองข้อมูล	• สอบทานความมีอยู่จริงและความเหมาะสมของระเบียบการปฏิบัติงานที่ชัดเจนสำหรับงานการสำรองข้อมูล • ตรวจสอบเพื่อให้มั่นใจว่าผู้ควบคุมงานสอบทานตารางการสำรองข้อมูลอย่างสม่ำเสมอ
ข้อมูลที่สำรองไว้อาจไม่สามารถนำกลับมาใช้ได้	• มีการทดสอบการนำข้อมูลที่สำรองไว้กลับมาใช้อย่างสม่ำเสมอ	• ตรวจสอบเพื่อให้มั่นใจว่ามีการทดสอบการนำข้อมูลที่สำรองไว้ กลับมาใช้อย่างสม่ำเสมอ

9. การควบคุมด้านการบริหารจัดการข้อมูล

9.1 ความรู้ทั่วไป

ข้อมูลเทคโนโลยีสารสนเทศเป็นปัจจัยสำคัญของการบริหารงานองค์กร ดังนั้นองค์กรจึงควรจัดให้มีการควบคุมที่ดีเพื่อทำให้องค์กรมีข้อมูลที่ถูกต้อง ครบถ้วน และพร้อมใช้เมื่อมีความจำเป็น ซึ่งแนวทางการควบคุมควรประกอบด้วยการดำเนินการด้านต่าง ๆ ดังนี้

9.1.1 การจัดทำโครงสร้างข้อมูลองค์กร

9.1.2 การกำหนดผู้รับผิดชอบต่อข้อมูล

9.1.3 การแบ่งประเภทข้อมูลตามระดับความสำคัญ

9.1.1 การจัดทำโครงสร้างข้อมูลองค์กร

ปัญหาที่สำคัญของการบริหารจัดการข้อมูลภายในองค์กร คือ ผู้บริหารข้อมูลไม่มีข้อมูลเพียงพอที่จะบริหารข้อมูลได้อย่างมีประสิทธิภาพ ดังนั้นวัตถุประสงค์ของการจัดทำโครงสร้างข้อมูล ก็เพื่อจัดให้มีรายละเอียดเกี่ยวกับข้อมูลขององค์กรอย่างถูกต้องและเพียงพอสำหรับบริหารข้อมูลขององค์กรให้มีประสิทธิภาพ ซึ่งแนวทางการดำเนินการควบคุม มีดังนี้

- จัดทำผังทางเดินของข้อมูล (Data Flow Diagram) เพื่อแสดงแหล่งกำเนิดของข้อมูล การประมวลผลข้อมูล การจัดเก็บข้อมูล และการใช้ข้อมูล
- ควรมีการปรับปรุงผังทางเดินของข้อมูลให้ทันสมัยอยู่เสมอ เมื่อมีการเปลี่ยนแปลงเกิดขึ้นกับข้อมูล
- มีการจัดทำรายละเอียดของข้อมูลหรือคำบรรยายข้อมูล (Data Dictionary) โดยระบุคำจำกัดความหรือคำอธิบายข้อมูลรูปแบบเฉพาะของข้อมูล (Format) และเงื่อนไขของข้อมูล (Condition) เช่น ข้อมูลเป็นตัวเลขระหว่าง 1 ถึง 100 เท่านั้น เป็นต้น
- มีการวิเคราะห์โครงสร้างของข้อมูลเป็นประจำ เพื่อสอบทานความซ้ำซ้อนของข้อมูล (Redundancy) ความสม่ำเสมอของข้อมูล (Consistency) และความถูกต้องของข้อมูล (Integrity)

9.1.2 การกำหนดผู้รับผิดชอบต่อข้อมูล

องค์กรที่สามารถบริหารจัดการข้อมูลได้ดี จะมีการกำหนดให้มีเจ้าของข้อมูลซึ่งเป็นผู้รับผิดชอบที่ชัดเจนต่อข้อมูล เช่น กำหนดให้ผู้บริหารฝ่ายบุคคลเป็นเจ้าของข้อมูลพนักงาน หรือผู้บริหารฝ่ายบัญชีเป็นเจ้าของข้อมูลบัญชี เพื่อให้มีบุคคลที่รับผิดชอบต่อความถูกต้อง ความครบถ้วน และความปลอดภัยของข้อมูล ซึ่งแนวทางการดำเนินการควบคุมมีดังนี้

- กำหนดให้มีเจ้าของข้อมูลที่ชัดเจนเพื่อให้เป็นผู้รับผิดชอบโดยตรงกับความถูกต้อง ความครบถ้วนและความปลอดภัยของข้อมูล โดยจัดให้มีการกำหนดเงื่อนไขว่าจะให้ผู้บริหารท่านใดเป็นเจ้าของข้อมูลใด เช่น กำหนดให้ผู้บริหารฝ่ายงานที่เป็นแหล่งกำเนิดข้อมูล เป็นเจ้าของข้อมูล หรือกำหนดให้ผู้บริหารฝ่ายงานที่อาจได้รับผลเสียหายมากที่สุดถ้าข้อมูลเกิดความเสียหายเป็นเจ้าของข้อมูล เป็นต้น
- กำหนดหน้าที่ความรับผิดชอบของเจ้าของข้อมูล ซึ่งควรครอบคลุมถึงความรับผิดชอบต่อความถูกต้องครบถ้วนของข้อมูล ความปลอดภัยของการใช้ข้อมูล การจัดเก็บและการสำรองข้อมูล โดยหน้าที่ของเจ้าของข้อมูลนั้นไม่ได้เป็นผู้ดำเนินการด้านต่าง ๆ ดังกล่าวข้างต้นเอง แต่มีบทบาทเป็นผู้กำหนดระเบียบปฏิบัติ กำหนดความต้องการและเงื่อนไขการใช้ข้อมูล ประสานงานกับผู้ปฏิบัติงานให้ดำเนินการตามระเบียบปฏิบัติและตามความต้องการ การติดตามดูแลให้การดำเนินการด้านข้อมูลเป็นไปตามเงื่อนไขที่กำหนดดังกล่าวข้างต้น รวมถึงการอนุญาตให้ผู้อื่นนำข้อมูลไปใช้

9.1.3 การแบ่งประเภทข้อมูลตามระดับความสำคัญ

องค์กรควรจัดให้มีการแบ่งประเภทข้อมูลเพื่อให้การบริหารจัดการข้อมูลมีความสอดคล้องกับระดับความสำคัญของข้อมูล ซึ่งส่วนมากจะให้เจ้าของข้อมูลเป็นผู้กำหนดว่าข้อมูลที่ตนเองรับผิดชอบนั้นจัดอยู่ในประเภทใด ตัวอย่างประเภทข้อมูล ได้แก่

- ข้อมูลสาธารณะ (Public Information) เป็นข้อมูลที่สามารถเปิดเผยให้สาธารณะรับทราบได้ เช่น ข้อมูลคุณสมบัติของสินค้า ข้อมูลงบการเงินที่ได้รับการรับรองจากผู้สอบบัญชีแล้ว เป็นต้น
- ข้อมูลภายใน (Internal Information) เป็นข้อมูลที่ใช้ภายในองค์กร ซึ่งทุกหน่วยงาน และบุคลากรทุกคนสามารถใช้ได้ เช่น ข้อมูลเกี่ยวกับระเบียบปฏิบัติภายใน ข้อมูลโครงสร้างองค์กร เป็นต้น
- ข้อมูลเฉพาะด้านหรือฝ่ายงาน (Specific / Department Information) เป็นข้อมูลที่ถูกกำหนดให้ใช้เฉพาะด้าน หรือเฉพาะหน่วยงาน เช่น ข้อมูลด้านการผลิต จะเป็นข้อมูลที่ใช้ได้เฉพาะสายงานผลิต เป็นต้น
- ข้อมูลลับเฉพาะ (Confidential Information) เป็นข้อมูลที่ใช้เฉพาะบางคน หรือเป็นข้อมูลที่เมื่อถูกเปิดเผยแล้วอาจส่งผลกระทบต่อการบริหารงานโดยรวม เช่น ข้อมูลเงินเดือน เป็นต้น
- ข้อมูลลับสูงสุด (Highly Confidential / Restricted Information) เป็นข้อมูลที่ต้องรักษาให้เป็นความลับอย่างยิ่ง เพราะถ้าถูกเปิดเผยแล้วอาจส่งผลกระทบรุนแรงต่อองค์กร เช่น ข้อมูลความลับทางการค้า ข้อมูลสูตรการผลิตเฉพาะสินค้า เป็นต้น

การจัดประเภทของข้อมูลมีความจำเป็นอย่างยิ่งถ้าต้องการให้การบริหารจัดการข้อมูลมีประสิทธิภาพและประสิทธิผลมากที่สุด โดยภายหลังจากจัดให้มีการจัดประเภทข้อมูลแล้ว ควรนำข้อมูลนี้ไปวิเคราะห์และจัดทำแนวทางบริหารจัดการข้อมูลให้เหมาะสมกับระดับความสำคัญของข้อมูลแต่ละประเภท ซึ่งแนวทางการดำเนินการควบคุมมีดังนี้

- กำหนดประเภทของข้อมูลและเงื่อนไขการจัดประเภทข้อมูลดังแสดงไว้เป็นตัวอย่างข้างต้น และนำเสนอผู้บริหารระดับสูงเพื่อให้เป็นผู้เห็นชอบ
- รวบรวมข้อมูลที่มีอยู่ในองค์กรทั้งหมดมาจัดเป็นกลุ่มเพื่อนำมาใช้จัดประเภท เช่น กลุ่มข้อมูลพนักงาน กลุ่มข้อมูลลูกค้า กลุ่มข้อมูลผลิตภัณฑ์ กลุ่มข้อมูลบัญชีการเงิน เป็นต้น
- วิเคราะห์เพื่อคัดแยกข้อมูลที่มีลักษณะเฉพาะออกจากกลุ่มข้อมูล เช่น ข้อมูลเงินเดือนมีความต้องการเฉพาะด้านการรักษาความลับ ควรแยกออกจากกลุ่มข้อมูลพนักงาน เป็นต้น
- ดำเนินการประเมินความเสี่ยงและผลกระทบที่เกี่ยวกับข้อมูลแต่ละกลุ่ม และข้อมูลที่มีลักษณะเฉพาะ เพื่อจัดประเภทของข้อมูลแต่ละกลุ่มและข้อมูลเฉพาะ โดยให้เจ้าของข้อมูลเป็นผู้ให้ความเห็นชอบกับการจัดประเภทดังกล่าว
- จัดทำความต้องการด้านการบริหารจัดการข้อมูล เช่น การรักษาความปลอดภัย การจัดเก็บและสำรองข้อมูล การจัดการความถูกต้องครบถ้วนของข้อมูล โดยระบุว่าในแต่ละประเภทจะต้องมีเงื่อนไขการดำเนินการด้านความปลอดภัย การจัดเก็บและการสำรอง รวมทั้งความถูกต้องอย่างไร
- จัดให้มีการสอบทานเพื่อติดตามว่าการดำเนินการด้านข้อมูลแต่ละประเภทเป็นไปตามแนวทางที่กำหนดไว้หรือไม่

9.2 ความเสี่ยง การควบคุม และการตรวจสอบ

ส่วนนี้จะอธิบายถึงความเสี่ยง การควบคุมความเสี่ยง และการตรวจสอบเพื่อให้มั่นใจถึงประสิทธิภาพและประสิทธิผลของการควบคุมการจัดการความเสี่ยงที่เกิดจากการบริหารจัดการข้อมูลที่มีผลกระทบกับความน่าเชื่อถือของรายงานทางการเงิน โดยรายละเอียดแสดงอยู่ในตารางนี้

ความเสี่ยง	การควบคุม	การตรวจสอบ
ขาดข้อมูลที่มีคุณภาพสำหรับสนับสนุนการบริหารและการควบคุมที่มีประสิทธิผล	• จัดโครงสร้างของข้อมูลอย่างเป็นระบบ เช่น การจัดให้มีสถาปัตยกรรมข้อมูล (Information Architecture) • กำหนดผู้รับผิดชอบต่อข้อมูลที่ชัดเจน และกำหนดหน้าที่ความรับผิดชอบอย่างเป็นทางการ • มีการวิเคราะห์ความต้องการใช้ข้อมูลเพื่อการบริหารและควบคุมองค์กรอย่างสม่ำเสมอ	• สอบทานโครงสร้างองค์กรและเอกสารที่เกี่ยวข้องกับการกำหนดหน้าที่ความรับผิดชอบเพื่อให้มั่นใจว่ามีการกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับข้อมูลที่เหมาะสม • ตรวจสอบเพื่อให้มั่นใจว่ามีการวิเคราะห์ความต้องการการใช้ข้อมูลขององค์กรอย่างสม่ำเสมอ

ความเสี่ยง	การควบคุม	การตรวจสอบ
ข้อมูลขององค์กรอาจไม่ถูกต้องครบถ้วนและปลอดภัย	• มีการกำหนดนโยบายเทคโนโลยีสารสนเทศให้มีการแบ่งประเภทของข้อมูลตามความเหมาะสมของลักษณะการใช้ข้อมูลขององค์กร • มีการกำหนดแนวทางการบริหารจัดการความถูกต้องครบถ้วน ความปลอดภัยและความพร้อมใช้ของข้อมูลแต่ละประเภท	• สอบทานนโยบายเทคโนโลยีสารสนเทศเพื่อให้มั่นใจว่ามีการกำหนดเรื่องการแบ่งประเภทของข้อมูล • สอบทานความเหมาะสมของการแบ่งประเภทข้อมูล • สอบทานความเหมาะสมของการกำหนดแนวทางการบริหารจัดการ ความถูกต้องครบถ้วน ความปลอดภัยและความพร้อมใช้ของข้อมูล • ตรวจสอบเพื่อให้มั่นใจว่ามีการปฏิบัติตามแนวทางการบริหารจัดการข้อมูลอย่างสม่ำเสมอ
การเปลี่ยนแปลงข้อมูลโดยตรง โดยใช้เครื่องมือหรือโปรแกรมอื่น ๆ ที่ไม่ใช่โปรแกรมในระบบงานเทคโนโลยีสารสนเทศอาจไม่ได้รับการอนุมัติ หรือเปลี่ยนแปลงไม่ครบถ้วนถูกต้อง	• ทุกการเปลี่ยนแปลงต้องได้รับการอนุมัติอย่างเหมาะสม • มีการสอบทานความครบถ้วนถูกต้องของการเปลี่ยนแปลง	• สุ่มเลือกการเปลี่ยนแปลงจากบันทึกของระบบ และสอบทานความเหมาะสมของการอนุมัติการเปลี่ยนแปลง • ตรวจสอบเพื่อให้มั่นใจว่ามีการสอบทานและทดสอบอย่างเหมาะสม

10. ผลกระทบจากการขาดการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่ดี

ส่วนนี้จะอธิบายถึงผลกระทบจากการขาดการควบคุมทั่วไปที่ดีของเทคโนโลยีสารสนเทศในส่วนที่เกี่ยวกับการจัดทำรายงานทางการเงินซึ่งมีเนื้อหาที่สำคัญดังนี้

10.1 การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ กับการจัดทำรายงานทางการเงิน

10.2 การประเมินผลกระทบต่อการสอบบัญชีกิจการที่ใช้เทคโนโลยีสารสนเทศจัดทำรายงานทางการเงิน ในกรณีที่มีข้อบกพร่องของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

10.3 ตัวอย่างข้อบกพร่องของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่อาจมีผลกระทบต่อรายงานทางการเงิน

10.1 การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ กับการจัดทำรายงานทางการเงิน

ปัจจุบันองค์กรต่าง ๆ มีการนำเทคโนโลยีสารสนเทศมาใช้สนับสนุนการปฏิบัติงาน และการจัดทำรายงานทางการเงินกันอย่างกว้างขวาง ในส่วนที่เกี่ยวกับรายงานทางการเงินนั้น เทคโนโลยีสารสนเทศมีส่วนเกี่ยวข้องตั้งแต่การรวบรวมและบันทึกรายการทางธุรกิจ การประมวลผลต่าง ๆ การคำนวณและการประมาณการ การแปลงรายการทางธุรกิจให้เป็นรายการทางบัญชี และการจัดทำรายงานโดยใช้โปรแกรมคอมพิวเตอร์ เพื่อประมวลผลข้อมูลทั้งข้อมูลหลัก (Master Data) และข้อมูลรายการ (Transaction Data) ฉะนั้นถ้าไม่มีการจัดให้มีการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่เพียงพอและมีประสิทธิผลแล้ว อาจทำให้โปรแกรมที่นำมาใช้งานหรือข้อมูลที่นำมาประมวลผลขาดความถูกต้องครบถ้วน ซึ่งจะส่งผลให้การควบคุมที่เกี่ยวกับรายงานทางการเงินขาดประสิทธิผลตามไปด้วย โดยเฉพาะอย่างยิ่งการควบคุมที่ใช้ระบบงานเทคโนโลยีสารสนเทศเป็นกลไกสำคัญดังต่อไปนี้

- การควบคุมโดยอัตโนมัติ (Automated Controls)
- การประมวลผลแบบอัตโนมัติโดยระบบคอมพิวเตอร์ (Automated Processing)
- รายงานหรือข้อมูลที่จัดทำโดยระบบคอมพิวเตอร์ (Computer Generated Reports/Data)

การควบคุมโดยอัตโนมัติ (Automated Controls) หมายถึง การควบคุมที่ดำเนินการอัตโนมัติโดยโปรแกรมคอมพิวเตอร์และไม่มีบุคคลเข้าไปเกี่ยวข้อง ตัวอย่างเช่น การตรวจสอบวงเงินลูกค้าระหว่างการนำเข้าข้อมูลคำสั่งซื้อ การอนุมัติรายการซื้อสินค้าผ่านบัตรเครดิตโดยโปรแกรมคอมพิวเตอร์ หรือการใช้โปรแกรมตรวจสอบข้อมูลคำสั่งซื้อ รายการรับสินค้า และข้อมูลใบแจ้งหนี้ ก่อนสั่งจ่ายเงินโดยระบบฯ หรือการใช้ระบบคอมพิวเตอร์ควบคุมราคาสินค้า ณ จุดจำหน่ายสินค้า เป็นต้น

การประมวลผลแบบอัตโนมัติโดยระบบคอมพิวเตอร์ (Automated Processing) หมายถึง การใช้โปรแกรมคอมพิวเตอร์ประมวลผลรายการต่าง ๆ โดยอัตโนมัติ เช่น การคำนวณดอกเบี้ย การคำนวณมูลค่าของสินค้าคงคลัง การคำนวณค่าเสื่อมราคา หรือการปรับปรุงรายการต่าง ๆ เช่น การปรับปรุงยอดคงเหลือของบัญชีออมทรัพย์ การปรับปรุงยอดลูกหนี้คงค้างจากรายการชำระเงิน การบันทึกและประมวลทางบัญชี เป็นต้น

รายงานหรือข้อมูลที่จัดทำโดยระบบคอมพิวเตอร์ (Computer Generated Reports/Data) หมายถึง รายงานหรือข้อมูลที่จัดทำโดยระบบ ซึ่งผู้บริหารใช้รายงานหรือข้อมูลต่าง ๆ เหล่านี้ เพื่อควบคุมกิจกรรมต่าง ๆ ขององค์กร เช่น รายงานแบ่งอายุลูกหนี้ รายงานสรุปการซื้อขาย รายงานรายละเอียดวัตถุดิบที่ใช้ไปในการผลิต เป็นต้น

ถ้าโปรแกรมหรือข้อมูลที่ใช้สำหรับการควบคุมดังกล่าวข้างต้นขาดความถูกต้องครบถ้วน อาจส่งผลทำให้รายงานทางการเงินขาดความน่าเชื่อถือตามไปด้วย ซึ่งตารางต่อไปนี้แสดงให้เห็นถึงผลกระทบที่เกิดขึ้นกับโปรแกรมและข้อมูลที่ใช้ประมวลผลรายการทางการเงิน ในกรณีที่มีข้อบกพร่องของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

ความเสี่ยง	การควบคุม	การตรวจสอบ
การกำหนดนโยบายการวางแผนงาน และการจัดโครงสร้างงานเทคโนโลยีสารสนเทศ	• มีการกำหนดนโยบายเทคโนโลยีสารสนเทศให้มีการแบ่งประเภทของข้อมูลตามความเหมาะสมของลักษณะการใช้ข้อมูลขององค์กร • มีการกำหนดแนวทางการบริหารจัดการความถูกต้องครบถ้วน ความปลอดภัยและความพร้อมใช้ของข้อมูลแต่ละประเภท	ส่งผลกระทบต่อประสิทธิผลของการควบคุมอื่น ซึ่งมีผลกระทบทางอ้อมต่อความถูกต้องครบถ้วนของโปรแกรมและข้อมูล
การกำหนดนโยบายการวางแผนงาน และการจัดโครงสร้างงานเทคโนโลยีสารสนเทศ	• การทดสอบโปรแกรมไม่มีประสิทธิผลหรือทดสอบไม่ครบถ้วน • ไม่มีการควบคุมการโอนย้ายโปรแกรมไปใช้งานที่รัดกุม	โปรแกรมที่ใช้งานอาจไม่ถูกต้อง
	• ขาดการควบคุมการโอนย้ายข้อมูลจากระบบเก่าไปสู่ระบบใหม่	ข้อมูลอาจไม่ถูกต้อง
การรักษาความปลอดภัยเทคโนโลยีสารสนเทศ	• โปรแกรมอาจถูกเปลี่ยนแปลงโดยบุคคลที่ไม่ได้รับอนุญาต	โปรแกรมอาจไม่ถูกต้อง
	• ข้อมูลอาจถูกเปลี่ยนแปลงโดยบุคคลที่ไม่ได้รับอนุญาต	ข้อมูลอาจไม่ถูกต้องครบถ้วน
การปฏิบัติการคอมพิวเตอร์	• ขาดการควบคุมการประมวลผลสิ้นวัน	การประมวลผลอาจไม่ถูกต้อง
	• ขาดการควบคุมการกู้คืนข้อมูลสำรองที่ดี	ข้อมูลอาจไม่ถูกต้องครบถ้วน
การบริหารจัดการข้อมูล	• มีข้อบกพร่องของการบริหารจัดการข้อมูล	ข้อมูลอาจไม่ถูกต้องครบถ้วน

10.2 การประเมินผลกระทบต่อการสอบบัญชีกิจการที่ใช้เทคโนโลยีสารสนเทศจัดทำรายงานทางการเงิน ในกรณีที่มีข้อบกพร่องของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

ผู้สอบบัญชีต้องทำความเข้าใจก่อนว่าการสอบบัญชีสำหรับกิจการที่ใช้เทคโนโลยีสารสนเทศประมวลผลรายการทางการเงินนั้น ผู้สอบบัญชีไม่จำเป็นต้องตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศในทุกกิจการ แต่ผู้สอบบัญชีอาจเลือกวิธีการตรวจสอบโดยเชื่อมั่นต่อการควบคุมโดยระบบงานเทคโนโลยีสารสนเทศซึ่งประกอบด้วย การควบคุมโดยอัตโนมัติ การประมวลผลแบบอัตโนมัติโดยระบบคอมพิวเตอร์ และรายงานหรือข้อมูลที่จัดทำโดยระบบคอมพิวเตอร์ ดังที่อธิบายแล้วข้างต้น

แต่ผู้สอบบัญชีจะเชื่อมั่นต่อการควบคุมข้างต้นได้ก็ต่อเมื่อกิจการนั้นมีการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่ดี ดังนั้น ผู้สอบบัญชีจะต้องตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศของกิจการนั้น ๆ เสียก่อน โดยอาจจะทำงานร่วมกับผู้ตรวจสอบเทคโนโลยีสารสนเทศ และถ้าพบว่าการควบคุมทั่วไปของเทคโนโลยีสารสนเทศของกิจการมีข้อบกพร่อง ผู้สอบบัญชีจะต้องประเมินว่าข้อบกพร่องนั้นมีผลกระทบต่อการควบคุมโดยระบบงานเทคโนโลยีสารสนเทศหรือไม่ ก่อนที่จะทำการสอบบัญชีโดยให้ความเชื่อมั่นกับการควบคุมโดยระบบงานเทคโนโลยีสารสนเทศ

ในทางปฏิบัติ ผู้สอบบัญชีจะระบุรายละเอียดว่าจะตรวจสอบการควบคุมโดยระบบงานเทคโนโลยีสารสนเทศเรื่องใด เช่น การควบคุมโดยอัตโนมัติที่เกี่ยวกับความถูกต้องของราคาสินค้า หรือ การประมวลผลแบบอัตโนมัติโดยระบบคอมพิวเตอร์ที่เกี่ยวกับการคำนวณต้นทุนสินค้า หรือ รายงานยอดลูกหนี้คงค้างที่จัดทำโดยระบบคอมพิวเตอร์ เพื่อให้ผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถกำหนดขอบเขตของการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศได้ชัดเจนขึ้น และเมื่อตรวจพบข้อบกพร่องของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ ก็จะสามารถประเมินผลกระทบต่อการควบคุมโดยระบบงานเทคโนโลยีสารสนเทศได้ตรงประเด็นมากขึ้น โดยการประเมินผลกระทบที่เกิดจากข้อบกพร่องของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ เป็นการประเมินว่าผู้สอบบัญชีสามารถเชื่อมั่นต่อการควบคุมโดยระบบงานเทคโนโลยีสารสนเทศตามที่ผู้สอบบัญชีวางแผนไว้ได้หรือไม่ ทั้งนี้ขึ้นอยู่กับลักษณะของข้อบกพร่องของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่ตรวจพบ

10.3 ตัวอย่างข้อบกพร่องของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศที่อาจมีผลกระทบต่อรายงานทางการเงิน

ตารางนี้เป็นตัวอย่างการประเมินผลกระทบของการควบคุมระบบงานโดยระบบงานเทคโนโลยีสารสนเทศจากข้อบกพร่องของการควบคุมที่ตรวจพบจากการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

การควบคุมทั่วไป	ข้อบกพร่องของการควบคุม	การประเมินผลกระทบต่อการควบคุมระบบงาน
การพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ	• การทดสอบโปรแกรมไม่มีประสิทธิผล หรือทดสอบไม่ครบถ้วน • ไม่มีการควบคุมที่รัดกุมด้านการโอนย้ายโปรแกรมไปใช้งาน	โปรแกรมที่ใช้ควบคุมระบบงานอาจไม่ถูกต้อง ทำให้การควบคุมโดยระบบงานอาจไม่มีประสิทธิผล ผู้ตรวจสอบเทคโนโลยีสารสนเทศควรตรวจสอบเพิ่มเติมในรายละเอียดว่าโปรแกรมที่ใช้ควบคุมระบบงานที่ผู้สอบบัญชีต้องการความเชื่อมั่นนั้นได้รับการทดสอบอย่างเพียงพอเหมาะสมหรือไม่ ถ้าไม่ผู้ตรวจสอบเทคโนโลยีสารสนเทศจำเป็นต้องตรวจสอบความถูกต้องของโปรแกรมด้วยวิธีอื่น ๆ เช่น การใช้คอมพิวเตอร์ช่วยตรวจสอบหรือตรวจสอบว่าโปรแกรมนั้นมีการเปลี่ยนแปลงแก้ไขหรือไม่ ซึ่งอาจตรวจสอบได้จากวันที่และเวลาของโปรแกรมนั้น (Program Date and Time stamp)

การควบคุมทั่วไป	ข้อบกพร่องของการควบคุม	การประเมินผลกระทบต่อการควบคุมระบบงาน
	• ขาดการควบคุมการโอนย้ายข้อมูลจากระบบงานเก่าไปสู่ระบบงานใหม่	ข้อมูลอาจไม่ถูกต้อง ลำดับแรก ผู้ตรวจสอบเทคโนโลยีสารสนเทศจะต้องวิเคราะห์เพื่อทำความเข้าใจว่า การควบคุมระบบงานที่ผู้สอบบัญชีต้องการความเชื่อมั่นนั้นต้องใช้ข้อมูลอะไรบ้าง ก่อนที่จะดำเนินการตรวจสอบความถูกต้องของข้อมูล ซึ่งวิธีตรวจสอบเพื่อพิสูจน์ว่าข้อมูลตั้งต้นที่โอนย้ายมาจากระบบงานเก่าถูกต้องครบถ้วนหรือไม่ มีหลายวิธี เช่น • เปรียบเทียบข้อมูลในระบบงานเก่าและระบบงานใหม่จากข้อมูลที่สำรองไว้ (ถ้ามี) • เปรียบเทียบข้อมูลยอดยกมาในระบบงานใหม่กับยอดคงเหลือของระบบงานเก่า ในกรณีนี้ผู้ตรวจสอบเทคโนโลยีสารสนเทศจะต้องมีความเข้าใจที่เพียงพอต่อระบบงานเพื่อจะได้สามารถกำหนดวิธีการตรวจสอบที่เหมาะสม
	• โปรแกรมอาจถูกเปลี่ยนแปลงโดยบุคคลที่ไม่ได้รับอนุญาต	โปรแกรมอาจไม่ถูกต้อง สามารถตรวจสอบว่ามีการเปลี่ยนแปลงโปรแกรมที่ใช้ในการควบคุมระบบงานหรือไม่ จากการตรวจสอบ วันที่และเวลาของโปรแกรมเช่นเดียวกับที่กล่าวข้างต้น ผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถตรวจสิทธิการเข้าถึงโปรแกรมดังกล่าว โดยการสอบทานพารามิเตอร์ด้านการเข้าถึงโปรแกรมจากระบบสอบทานบันทึกกิจกรรมระบบ (System Activity Log) ว่ามีการเปลี่ยนแปลงโปรแกรมโดยไม่ได้รับอนุญาตหรือไม่
	• ข้อมูลอาจถูกเปลี่ยนแปลงโดยบุคคลที่ไม่ได้รับอนุญาต	ข้อมูลอาจไม่ถูกต้องครบถ้วน ผู้ตรวจสอบเทคโนโลยีสารสนเทศควรตรวจสอบว่ามีการเปลี่ยนแปลงข้อมูลที่ใช้สำหรับการควบคุมระบบงานหรือไม่ จากการตรวจสอบ วันที่และเวลาของแฟ้มข้อมูล เช่นเดียวกับที่กล่าวข้างต้น ผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถตรวจสิทธิการเข้าถึงแฟ้มข้อมูลดังกล่าว โดยการสอบทานพารามิเตอร์ด้านการเข้าถึงแฟ้มข้อมูลจากระบบสอบทานบันทึกกิจกรรมระบบ (System Activity Log) ว่ามีการเปลี่ยนแปลงแฟ้มข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาตหรือไม่

การควบคุมทั่วไป	ข้อบกพร่องของการควบคุม	การประเมินผลกระทบต่อการควบคุมระบบงาน
	• มีบัญชีผู้ใช้งานที่ไม่มีความจำเป็นต้องใช้งานแล้ว แต่ยังคงอยู่ในระบบ	บัญชีผู้ใช้งานอาจถูกนำมาใช้โดยบุคคลที่ไม่เหมาะสม หรือไม่ได้รับอนุญาต ผู้ตรวจสอบเทคโนโลยีสารสนเทศควรตรวจสอบว่ามีการเข้ามาใช้บัญชีดังกล่าวภายหลังจากบัญชีผู้ใช้งานนั้นหมดความจำเป็นแล้วหรือไม่ เช่น บัญชีของผู้ใช้งานที่ลาออกแล้ว ยังมีการเข้าใช้งานภายหลังวันที่การลาออกมีผลแล้วหรือไม่ ถ้ามีการเข้าใช้งาน ผู้ตรวจสอบเทคโนโลยีสารสนเทศต้องสอบทานสิทธิในการเข้าถึงโปรแกรมและข้อมูลที่อาจมีผลกระทบต่อการควบคุมระบบงาน หรือความถูกต้องครบถ้วนของรายงานทางการเงินหรือไม่ และมีการใช้สิทธิดังกล่าวหรือไม่ โดยอาจดูจากบันทึกกิจกรรมของระบบ เป็นต้น
	• การกำหนดสิทธิการเข้าถึงโปรแกรมหรือข้อมูลไม่เหมาะสม	ตรวจสอบว่ามีการใช้สิทธิที่ไม่เหมาะสมหรือไม่ โดยสอบทานจากบันทึกกิจกรรมของระบบฯ ถ้ามีการเข้าไปเปลี่ยนแปลงโปรแกรมหรือข้อมูล ผู้ตรวจสอบเทคโนโลยีสารสนเทศควรตรวจสอบว่ามีการเปลี่ยนแปลงที่อาจมีผลกระทบต่อการควบคุมระบบงาน หรือความถูกต้องครบถ้วนของรายงานทางการเงินหรือไม่ และตรวจสอบในรายละเอียดเพิ่มเติมถึงผลที่อาจเกิดขึ้นจากการเปลี่ยนแปลงดังกล่าว
	• ขาดการควบคุมการประมวลผลสิ้นวัน	การประมวลผลอาจไม่ถูกต้อง ผู้ตรวจสอบเทคโนโลยีสารสนเทศควรสุ่มเลือกตารางการประมวลผลสิ้นวัน เพื่อสอบทานว่ามีรายการประมวลผลที่ผิดปกติหรือไม่ หากมีการประมวลผลที่ผิดปกตินั้นได้รับการแก้ไขอย่างเหมาะสมหรือไม่ ผู้ตรวจสอบเทคโนโลยีสารสนเทศอาจใช้เทคนิคการตรวจสอบโดยใช้คอมพิวเตอร์ช่วยมาใช้ในการตรวจสอบ เพื่อให้มั่นใจว่าการประมวลผลมีความถูกต้อง เช่น การใช้เทคนิคการประมวลผลคู่ขนาน (Parallel Simulation) หรือเทคนิคการทำข้อมูลทดสอบ (Test Data) เป็นต้น
	• มีข้อบกพร่องของการบริหารจัดการข้อมูล	ข้อมูลอาจไม่ถูกต้องครบถ้วน เนื่องจากข้อบกพร่องของการบริหารจัดการข้อมูล อาจส่งผลกระทบต่อความถูกต้องและครบถ้วนของข้อมูลโดยรวม ซึ่งอาจไม่สามารถระบุได้ชัดเจนว่าจะกระทบกับข้อมูลใดเป็นการเฉพาะเจาะจง ดังนั้น การประเมินผลกระทบนั้นอาจจะต้องดำเนินการโดยสอบถามผู้สอบบัญชีว่าต้องการได้ความเชื่อมั่นจากการควบคุมระบบงานใดบ้าง และมีข้อมูลใดที่มีความสำคัญต่อการควบคุมดังกล่าว แล้วจึงทำการตรวจสอบในรายละเอียดว่าข้อมูลเหล่านั้นมีความครบถ้วนและถูกต้องหรือไม่

11. หลักการและขั้นตอนการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

การตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศเป็นการตรวจสอบเพื่อให้มั่นใจว่าองค์กรมีการควบคุมอย่างเพียงพอในกระบวนการทำงานด้านเทคโนโลยีสารสนเทศ และการควบคุมที่มีอยู่นั้นมีการดำเนินการอย่างมีประสิทธิภาพและประสิทธิผล โดยหลักการหรือแนวทางการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศจะใช้แนวทางของการตรวจสอบแบบอิงกับความเสี่ยง (Risk-Based Audit Approach) ที่กำหนดให้ผู้สอบบัญชีต้องศึกษาและทำความเข้าใจต่อความเสี่ยงและการควบคุมอย่างเพียงพอก่อนเริ่มดำเนินการตรวจสอบ

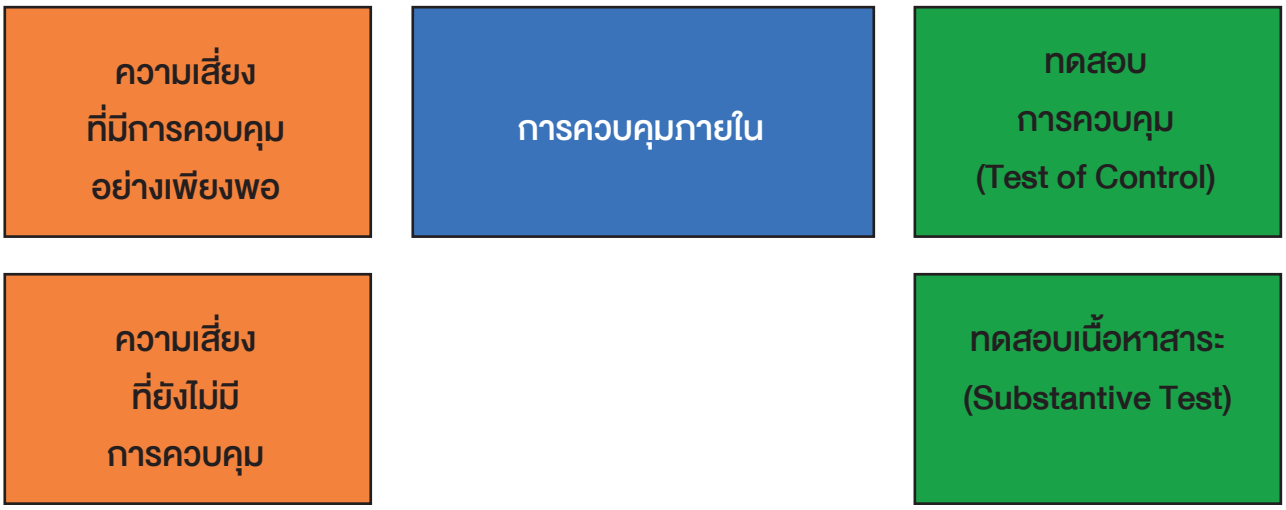
ส่วนนี้จะอธิบายการตรวจสอบด้านการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ ซึ่งจะแบ่งออกเป็น 2 ส่วนดังนี้

11.1 หลักการและแนวทางการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

11.2 ขั้นตอนการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

11.1 หลักการและแนวทางการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

ด้วยหลักการพื้นฐานของการตรวจสอบแบบอิงกับความเสี่ยง (Risk-Based Audit Approach) ที่กล่าวว่า “ผู้สอบบัญชีจำเป็นต้องมีความรู้ความเข้าใจอย่างเพียงพอต่อความเสี่ยงและการควบคุมภายในก่อนเริ่มดำเนินการตรวจสอบ” สามารถนำมากำหนดเป็นวิธีการตรวจสอบได้ ดังภาพต่อไปนี้



ภาพที่ 2.10 การตรวจสอบแบบอิงกับความเสี่ยง (Risk-Based Audit Approach)

การตรวจสอบแบบอิงกับความเสี่ยงเริ่มจากผู้สอบบัญชีทำความเข้าใจกับความเสี่ยงของส่วนงานที่กำลังจะตรวจสอบแล้วจึงทำความเข้าใจกับการควบคุมภายใน จากนั้นจึงวิเคราะห์ความเสี่ยงและการควบคุม โดยประเมินว่าความเสี่ยงใดมีการควบคุมที่เพียงพอ และความเสี่ยงใดยังไม่มีการควบคุมที่เพียงพอ หลังจากนั้นจึงเริ่มวางแผนการตรวจสอบโดยความเสี่ยงที่มีการควบคุมแล้วนั้น ผู้สอบบัญชีจะวางแผนเพื่อทดสอบประสิทธิภาพของการควบคุม ส่วนความเสี่ยงที่ยังไม่มีการควบคุม ผู้สอบบัญชีจะวางแผนการตรวจสอบเนื้อหาสาระ ทั้งนี้ หากผลการตรวจสอบการควบคุมของความเสี่ยงใดไม่เป็นที่น่าพอใจ กล่าวคือการควบคุมอาจไม่มีประสิทธิภาพที่น่าเชื่อถือ ผู้สอบบัญชีจะต้องวางแผนการตรวจสอบเนื้อหาสาระสำหรับความเสี่ยงนั้น ๆ เพิ่มเติม

จากหลักการตรวจสอบแบบอิงกับความเสี่ยงที่กล่าวข้างต้น สามารถสรุปเป็นกิจกรรมหลักที่ผู้สอบบัญชีจะต้องดำเนินการก่อนเริ่มดำเนินการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ ซึ่งอาจจะต้องทำงานร่วมกับผู้ตรวจสอบเทคโนโลยีสารสนเทศ ดังนี้

11.1.1 การประเมินความเสี่ยงเทคโนโลยีสารสนเทศ

11.1.2 การประเมินการควบคุมเทคโนโลยีสารสนเทศ

11.1.1 การประเมินความเสี่ยงเทคโนโลยีสารสนเทศ

ขั้นตอนการประเมินความเสี่ยงเทคโนโลยีสารสนเทศสามารถแสดงได้ดังนี้

ภาพที่ 2.11 ขั้นตอนการประเมินความเสี่ยงเทคโนโลยีสารสนเทศเพื่อการตรวจสอบ

สิ่งแรกที่ผู้สอบบัญชีและผู้ตรวจสอบเทคโนโลยีสารสนเทศควรจะต้องทำความเข้าใจในการประเมินความเสี่ยงในการตรวจสอบเทคโนโลยีสารสนเทศก็คือวัตถุประสงค์ของการตรวจสอบ ถ้าเป็นการสอบบัญชีวัตถุประสงค์ของการตรวจสอบอาจมุ่งความสำคัญให้กับความถูกต้องครบถ้วนน่าเชื่อถือของข้อมูลทางการบัญชีที่ประมวลผลด้วยระบบงานเทคโนโลยีสารสนเทศ แต่ถ้าเป็นการตรวจสอบอื่น ๆ เช่น การตรวจสอบการปฏิบัติการ (Operational Audit) การตรวจสอบการบริหาร (Management Audit) วัตถุประสงค์ของการตรวจสอบก็จะแตกต่างออกไป แต่หลักการก็คือจะต้องเข้าใจวัตถุประสงค์ของการตรวจสอบเสียก่อน

ภายหลังจากเข้าใจวัตถุประสงค์ของการตรวจสอบแล้ว ลำดับถัดไปเป็นการทำความเข้าใจกับสภาพแวดล้อมและกระบวนการทำงานของส่วนงานที่จะประเมินความเสี่ยง ซึ่งจะช่วยให้ผู้สอบบัญชีสามารถระบุความเสี่ยงได้ตรงกับความเป็นจริงมากที่สุด เมื่อเข้าใจสภาพแวดล้อมและกระบวนการทำงานแล้ว ลำดับถัดไปจึงเป็นการระบุความเสี่ยงในแต่ละส่วนของกระบวนการทำงาน โดยความเสี่ยงดังกล่าวข้างต้น หมายถึง “เหตุการณ์ใด ๆ ที่เกิดขึ้นแล้วส่งผลกระทบต่อการบรรลุวัตถุประสงค์” ดังนั้นถ้าผู้สอบบัญชีได้วิเคราะห์รายละเอียดของกระบวนการทำงานในแต่ละขั้นตอน และสภาพแวดล้อมของการดำเนินงานแล้วก็จะสามารถระบุความเสี่ยงในรายละเอียดได้อย่างครบถ้วน โดยอาจจะปรึกษาหรือทำงานร่วมกับผู้ตรวจสอบเทคโนโลยีสารสนเทศเพื่อให้ได้ความเข้าใจในบทบาทของเทคโนโลยีสารสนเทศที่ครบถ้วน

ตัวอย่างเช่น วัตถุประสงค์ของการตรวจสอบเทคโนโลยีสารสนเทศ คือ “เพื่อความมั่นใจว่าข้อมูลรายได้ที่นำมาลงบัญชีมีการรวบรวมและประมวลผลอย่างถูกต้องครบถ้วน” หลังจากที่ผู้สอบบัญชีทำการศึกษาการบริหารงานระบบคอมพิวเตอร์ ลักษณะของระบบคอมพิวเตอร์ การดำเนินการในรายละเอียดของระบบงานคอมพิวเตอร์ที่เกี่ยวข้องกับข้อมูลรายได้แล้ว ผู้สอบบัญชีจะสามารถระบุความเสี่ยงที่อาจทำให้ข้อมูลรายได้ขาดความครบถ้วนถูกต้อง เช่น การนำข้อมูลรายได้เข้าสู่ระบบอาจไม่ถูกต้อง หรือไม่ครบถ้วน และโปรแกรมที่ใช้ประมวลผลข้อมูลรายได้อาจไม่ถูกต้อง เป็นต้น

ภายหลังจากที่ผู้สอบบัญชีสามารถระบุความเสี่ยงได้ครบถ้วนแล้ว ผู้สอบบัญชีจะต้องประเมินความเสี่ยงแต่ละรายการ โดยประเมินทั้งทางด้านโอกาสเกิด (Likelihood) และผลกระทบ (Impact) ซึ่งเป็นผลกระทบต่อวัตถุประสงค์ของการตรวจสอบ โดยวัตถุประสงค์ของการประเมินความเสี่ยงคือการกลั่นกรองความเสี่ยงเพื่อให้การตรวจสอบมุ่งประเด็นไปที่ความเสี่ยงที่อยู่ในระดับสูงก่อน และเป็นข้อมูลสำหรับการวิเคราะห์เปรียบเทียบกับการควบคุมภายในเพื่อระบุความเพียงพอของการควบคุม

11.1.2 การประเมินการควบคุมเทคโนโลยีสารสนเทศ

การประเมินการควบคุมเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อวิเคราะห์ความเพียงพอของการควบคุมภายในที่รองรับความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อที่ผู้สอบบัญชีและผู้ตรวจสอบเทคโนโลยีสารสนเทศจะใช้จัดทำแผนการตรวจสอบที่อิงกับความเสี่ยง ซึ่งก่อนที่จะประเมินการควบคุมผู้สอบบัญชีควรทำความเข้าใจกับคำนิยามของการควบคุมก่อนว่าเป็น “กระบวนการที่ดำเนินการโดยบุคลากรในองค์กรโดยมุ่งหวังที่จะเพิ่มโอกาสของการที่องค์กรจะบรรลุวัตถุประสงค์ที่ตั้งไว้”

ภายหลังจากที่ทราบวัตถุประสงค์ของการตรวจสอบสภาพแวดล้อมของเทคโนโลยีสารสนเทศ กระบวนการทำงานต่าง ๆ ความเสี่ยงและระดับความเสี่ยงแล้ว ผู้สอบบัญชีและผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถเริ่มศึกษาการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ซึ่งประกอบด้วย การควบคุมทั่วไป (General Controls) และการควบคุมระบบงาน (Application Control) โดยเริ่มต้นจากความเสี่ยง จากนั้นจึงวิเคราะห์การทำงานในส่วนต่าง ๆ ว่ามีกลไกหรือกระบวนการทำงานใดที่สามารถลดหรือจัดการความเสี่ยงดังกล่าวได้ ทั้งนี้ขึ้นอยู่กับลักษณะและระดับความเสี่ยงของแต่ละรายการ

การประเมินความเสี่ยงระดับนี้เป็นการประเมินการควบคุมตามลักษณะการออกแบบการควบคุมนั้น ๆ (Control Design) ที่ยังไม่ได้มีการทดสอบประสิทธิภาพ และความสม่ำเสมอของการดำเนินการควบคุม ซึ่งลักษณะการประเมินนั้นอาจประเมินจากระเบียบปฏิบัติ หรือขั้นตอนการทำงานที่ถูกออกแบบไว้โดยยังไม่ต้องสุ่มรายการที่เกี่ยวกับการควบคุมมาตรวจสอบเพื่อประเมินประสิทธิภาพของการควบคุม

การประเมินการควบคุมด้านเทคโนโลยีสารสนเทศอาจมีความแตกต่างกันเล็กน้อยในทางเทคนิคระหว่างการประเมินการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ และการประเมินการควบคุมระบบงาน ซึ่งส่วนใหญ่การประเมินการควบคุมทั่วไปของเทคโนโลยีสารสนเทศเป็นการประเมินโดยใช้แบบสอบถามหรือแบบประเมินสำเร็จรูป (Control Questionnaire หรือ Control Checklist) ทั้งนี้เพราะการดำเนินงานด้านการควบคุมทั่วไปส่วนใหญ่จะมีขั้นตอนการทำงานที่ไม่ค่อยแตกต่างกันในแต่ละองค์กร แต่สำหรับการประเมินการควบคุมระบบงานนั้น ผู้ประเมินจะต้องทำความเข้าใจกับระบบงาน วิเคราะห์กระบวนการทำงานแล้วจึงดำเนินการประเมินการควบคุม เพราะกระบวนการทำงานในแต่ละองค์กรอาจไม่เหมือนกัน ทั้งที่เป็นกระบวนการทำงานด้านเดียวกันและใช้ซอฟต์แวร์ยี่ห้อเดียวกัน

ผลที่ได้รับจากการประเมินความเสี่ยงและการควบคุม ผู้สอบบัญชีและผู้ตรวจสอบเทคโนโลยีสารสนเทศสามารถนำไปใช้กำหนดโปรแกรมการตรวจสอบ โดยที่ถ้าความเสี่ยงใดมีการควบคุมที่เพียงพอ ผู้สอบบัญชีและผู้ตรวจสอบเทคโนโลยีสารสนเทศจะวิเคราะห์การควบคุมนั้นแล้วกำหนดเป็นแนวทางหรือโปรแกรมการตรวจสอบเพื่อทดสอบว่าการควบคุมนั้นดำเนินการอย่างสม่ำเสมอและมีประสิทธิภาพหรือไม่ และสำหรับความเสี่ยงที่ไม่มีการควบคุม ผู้สอบบัญชีและผู้ตรวจสอบเทคโนโลยีสารสนเทศจะวิเคราะห์หาวิธีการทดสอบจากรายการหรือข้อมูลจริงเพื่อค้นหาว่า มีความเสี่ยงเกิดขึ้นหรือไม่จากการที่ไม่มีการควบคุมที่เพียงพอ หรือความเสี่ยงที่เกิดขึ้นมีระดับความมีนัยสำคัญมากน้อยเพียงใด

11.2 ขั้นตอนการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

ขั้นตอนในทางปฏิบัติของการตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศสำหรับกิจการที่ใช้เทคโนโลยีสารสนเทศประมวลผลรายการทางการเงิน เพื่อให้ผู้สอบบัญชีมีความเชื่อมั่นในการควบคุมโดยระบบคอมพิวเตอร์นั้น มีดังนี้

11.2.1 วางแผนการตรวจสอบ

10.2.1.1 รวบรวมข้อมูลเบื้องต้นด้านเทคโนโลยีสารสนเทศขององค์กร ซึ่งประกอบด้วย

- ข้อมูลด้านเทคโนโลยีสารสนเทศที่องค์กรนำมาใช้งาน เช่น ระบบงาน ระบบคอมพิวเตอร์ ระบบจัดการฐานข้อมูลและระบบเครือข่าย เป็นต้น
- โครงสร้างฝ่ายเทคโนโลยีสารสนเทศ และหน้าที่ความรับผิดชอบของแต่ละส่วนงาน
- นโยบายหรือระเบียบปฏิบัติที่เกี่ยวกับงานด้านเทคโนโลยีสารสนเทศ เช่น นโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศ นโยบายการพัฒนาระบบเทคโนโลยีสารสนเทศ ระเบียบปฏิบัติด้านการเปลี่ยนแปลงแก้ไขระบบเทคโนโลยีสารสนเทศ และระเบียบปฏิบัติด้านการปฏิบัติการคอมพิวเตอร์ เป็นต้น
- ระบบเทคโนโลยีสารสนเทศที่องค์กรนำมาใช้สนับสนุนและประมวลผลรายการทางธุรกิจและรายการทางการเงินรวมทั้งความเชื่อมโยงของระบบต่าง ๆ เหล่านั้น

11.2.1.2 ผู้ตรวจสอบเทคโนโลยีสารสนเทศประเมินสภาพแวดล้อมของการควบคุมด้านเทคโนโลยีสารสนเทศ (Computer Control Environment) เพื่อใช้เป็นแนวทางประกอบการตัดสินใจของผู้สอบบัญชีในการให้ความเชื่อมั่นที่มีต่อการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ

11.2.1.3 ผู้ตรวจสอบเทคโนโลยีสารสนเทศทำความเข้าใจความต้องการของผู้สอบบัญชีในส่วนที่ผู้สอบบัญชีต้องการความเชื่อมั่นที่มีต่อการควบคุมระบบงานโดยระบบงานเทคโนโลยีสารสนเทศ ซึ่งประกอบด้วยการควบคุมโดยอัตโนมัติ การประมวลผลแบบอัตโนมัติโดยระบบคอมพิวเตอร์ และรายงานหรือข้อมูลที่จัดทำโดยระบบคอมพิวเตอร์

11.2.1.4 ผู้ตรวจสอบเทคโนโลยีสารสนเทศกำหนดขอบเขตของการตรวจสอบโดยใช้ข้อมูลด้านเทคโนโลยีสารสนเทศและความต้องการของผู้สอบบัญชี เพื่อสรุปว่าจะดำเนินการตรวจสอบเรื่องใดบ้าง และเทคโนโลยีสารสนเทศใดบ้าง

11.2.2 ดำเนินการตรวจสอบ

- ระบุความเสี่ยงที่อาจมีผลกระทบต่อการควบคุมโดยระบบงานเทคโนโลยีสารสนเทศที่ผู้สอบบัญชีต้องการความเชื่อมั่น
- ระบุการควบคุมที่มีอยู่จริงขององค์กร และกำหนดแนวทางการทดสอบการควบคุม
- รวบรวมหลักฐานประกอบการตรวจสอบการควบคุม
- วิเคราะห์ประสิทธิผลของการควบคุม ซึ่งเป็นการตรวจสอบว่าการควบคุมที่องค์กรกำหนดไว้นั้น มีการดำเนินการอย่างสม่ำเสมอและต่อเนื่องหรือไม่
- ในกรณีที่ตรวจพบข้อบกพร่องของการควบคุม ผู้ตรวจสอบเทคโนโลยีสารสนเทศจะประเมินผลกระทบที่อาจมีต่อความน่าเชื่อถือของการควบคุมโดยระบบงานเทคโนโลยีสารสนเทศ และความน่าเชื่อถือของรายงานทางการเงิน

11.2.3 สรุปผลและรายงานผลการตรวจสอบ

- สรุปผลการตรวจสอบ และการประเมินผลกระทบต่อความน่าเชื่อถือของการควบคุมระบบงานโดยระบบงานเทคโนโลยีสารสนเทศ และความน่าเชื่อถือของรายงานทางการเงิน
- นำสนอผลการตรวจสอบ โดยมีสาระสำคัญอยู่ที่ความน่าเชื่อถือของการควบคุมระบบงานโดยระบบงานเทคโนโลยีสารสนเทศที่ผู้สอบบัญชีต้องการความเชื่อมั่น

12. บทสรุป

การควบคุมทั่วไปของเทคโนโลยีสารสนเทศเป็นการควบคุมภายในของกระบวนการทำงานด้านเทคโนโลยีสารสนเทศ ซึ่งไม่ได้เฉพาะเจาะจงว่าเป็นการควบคุมระบบงาน (Application Controls) ใดระบบงานหนึ่ง ซึ่งการควบคุมทั่วไปนั้นเป็นการควบคุมที่อยู่ในความรับผิดชอบของผู้บริหารเทคโนโลยีสารสนเทศ และผู้บริหารระดับสูง และส่วนใหญ่อยู่ในกระบวนงานในฝ่ายเทคโนโลยีสารสนเทศ การควบคุมทั่วไปของเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อให้มั่นใจว่าการดำเนินการด้านเทคโนโลยีสารสนเทศนั้นสามารถตอบสนองความต้องการด้านเทคโนโลยีสารสนเทศโดยรวมขององค์กรได้ ซึ่งความต้องการขององค์กรประกอบด้วยความต้องการด้านประสิทธิภาพและประสิทธิผลของการดำเนินงาน (Efficiency and Effectiveness) ความปลอดภัยของข้อมูลและเทคโนโลยีสารสนเทศ (Security and Confidentiality) ความถูกต้องครบถ้วนของข้อมูล (Integrity) หรือความพร้อมใช้ของข้อมูลและเทคโนโลยีสารสนเทศ (Availability) การควบคุมทั่วไปของเทคโนโลยีสารสนเทศ ประกอบด้วย

- การกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานเทคโนโลยีสารสนเทศ
- การพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานเทคโนโลยีสารสนเทศ
- การรักษาความปลอดภัยเทคโนโลยีสารสนเทศ
- การปฏิบัติการคอมพิวเตอร์
- การบริหารจัดการข้อมูล

การที่ผู้สอบบัญชีและผู้ตรวจสอบเทคโนโลยีสารสนเทศจะสามารถตรวจสอบได้อย่างมีประสิทธิผล ผู้สอบบัญชีและผู้ตรวจสอบเทคโนโลยีสารสนเทศจะต้องมีความรู้เบื้องต้นเกี่ยวกับองค์ประกอบของการควบคุมทั่วไปซึ่งครอบคลุมความรู้ทั่วไป ความเสี่ยงและการควบคุม จึงจะสามารถออกแบบการตรวจสอบที่มุ่งเน้นการประเมินประสิทธิผลของการควบคุมเพื่อจัดการความเสี่ยงต่าง ๆ ขององค์ประกอบของการควบคุมทั่วไปเหล่านั้น และเมื่อผู้ตรวจสอบเทคโนโลยีสารสนเทศตรวจพบข้อบกพร่องของการควบคุมทั่วไปของเทคโนโลยีสารสนเทศ ผู้ตรวจสอบเทคโนโลยีสารสนเทศจะต้องประเมินผลกระทบที่เกิดจากข้อบกพร่องดังกล่าวต่อการควบคุมระบบงานโดยระบบงานเทคโนโลยีสารสนเทศ ซึ่งประกอบด้วย การควบคุมโดยอัตโนมัติ (Automated Controls) การประมวลผลแบบอัตโนมัติโดยระบบคอมพิวเตอร์ (Automated Processing) และรายงานหรือข้อมูลที่จัดทำโดยระบบคอมพิวเตอร์ (Computer Generated Reports/Data) ร่วมกับผู้สอบบัญชีเนื่องจากการควบคุมระบบงานเหล่านี้เป็นการควบคุมที่ผู้สอบบัญชีให้ความสนใจและต้องการที่จะได้ความเชื่อมั่นเพื่อที่จะได้ใช้วิธีการตรวจสอบแบบที่เน้นการทดสอบการควบคุม (Test of Control) ซึ่งเป็นวิธีการตรวจสอบที่มีประสิทธิภาพมากกว่าการตรวจสอบเนื้อหาสาระ (Substantive Test)

การตรวจสอบการควบคุมทั่วไปของเทคโนโลยีสารสนเทศสำหรับกิจการที่ใช้เทคโนโลยีสารสนเทศประมวลผลรายการทางการเงินและผู้สอบบัญชีต้องการที่จะเชื่อมั่นในการควบคุมระบบงานโดยระบบงานเทคโนโลยีสารสนเทศ ผู้ตรวจสอบเทคโนโลยีสารสนเทศควรดำเนินการตามขั้นตอนที่สำคัญ ดังนี้

- วางแผนการตรวจสอบ ซึ่งประกอบด้วย การรวบรวมข้อมูลเบื้องต้นด้านเทคโนโลยีสารสนเทศ และการกำหนดขอบเขตของการตรวจสอบตามจำนวนการควบคุมระบบงานที่ผู้สอบบัญชีต้องการความเชื่อมั่น
- ดำเนินการตรวจสอบ ซึ่งประกอบด้วย การระบุความเสี่ยงและการควบคุม เพื่อกำหนดแนวทางการทดสอบการควบคุม และรวบรวมหลักฐานเกี่ยวกับการดำเนินการควบคุมว่ามีประสิทธิผลหรือไม่ ทั้งนี้ ผู้ตรวจสอบเทคโนโลยีสารสนเทศต้องประเมินผลกระทบที่มีต่อการควบคุมระบบงาน และความน่าเชื่อถือของรายงานทางการเงินร่วมกับผู้สอบบัญชี ในกรณีที่ผู้ตรวจสอบเทคโนโลยีสารสนเทศพบว่าการควบคุมมีข้อบกพร่อง
- สรุปผลและรายงานผลการตรวจสอบ เมื่อดำเนินการตรวจสอบเสร็จสิ้นแล้ว ผู้ตรวจสอบเทคโนโลยีสารสนเทศจะต้องสรุปผลและรายงานผลให้กับผู้สอบบัญชีทราบ ซึ่งสาระสำคัญของการสรุปผล คือ การให้ความเห็นว่าผู้สอบบัญชีจะเชื่อมั่นต่อการควบคุมระบบงานโดยระบบงานเทคโนโลยีสารสนเทศได้หรือไม่

13. บรรณานุกรม

ณฐพร พันธ์อุดม และคณะ. (2549). *แนวทางการควบคุมภายในที่ดี.* ตลาดหลักทรัพย์แห่งประเทศไทย.

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์. (2564). *มาตรฐานการสอบบัญชี รหัส 315 (ฉบับปรับปรุง 2564): การระบุและประเมินความเสี่ยงจากการแสดงข้อมูลที่ขัดต่อข้อเท็จจริงที่มีนัยสำคัญ.*

Hall, J. A., & Singleton, T. (2004, August). *Information Technology Auditing and Assurance* (2nd Edition). South-Western Pub.

Otero, A. R. (2019). *Information Technology Control and Audit* (5th Edition). n.p.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004, September). *Enterprise Risk Management – Integrated Framework: Executive Summary.* n.p.

The IT Governance Institute. (2004). *Board Briefing on IT Governance* (2nd Edition). n.p.

The IT Governance Institute, & COBIT Steering Committee. (2000). *COBIT – Control Objectives* (3rd Edition). n.p.

The IT Governance Institute, & COBIT Steering Committee. (2005). *COBIT 4.0 – Control Objectives, Management Guidelines, Maturity Models*. n.p.

คณะผู้ทรงคุณวุฒิจัดทำคู่มือด้านการสอบบัญชีที่ประมวลผลโดยคอมพิวเตอร์

ศ.ดร.ศิริลักษณ์	โรจนกิจอำนวย	ประธานคณะทำงาน
ศ.ดร.นิตยา	วงศ์ภินันท์วัฒนา	คณะทำงาน
ดร.เยาวลักษณ์	ชาติบัญชาชัย	คณะทำงาน
นางปิยะพัชร์	อัศวจินดากรณ์	คณะทำงาน
นางสาวผุสดี	จันทะสุวันนะ	คณะทำงาน
นายพิรุฬน์	กิตติเดชปรีชา	คณะทำงาน
นางสาวรินรัตน์	ภาสเวคิน	คณะทำงาน
นางวราลี	วัฒนวิบูลย์	คณะทำงาน
นายวันชัย	พิทักษ์กรณ์	คณะทำงาน
นางเสาวนีย์	เสตเสถียร	คณะทำงาน
นายอธิษฐ์	ตระกูลเดช	คณะทำงาน

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

เลขที่ 133 ถนนสุขุมวิท 21 (อโศก) แขวงคลองเตยเหนือ
เขตวัฒนา กรุงเทพฯ 10110

0 2685 2500 โทรสาร 0 2685 2501

tfac@tfac.or.th www.tfac.or.th