บทที่ 3

การควบคุมทั่วไปในระบบสารสนเทศ

โดย

วันชัย พิทักษ์กรณ์

1. สารบัญบท

2. วัตถุประสงค์ในการศึกษา

เพื่อทำความเข้าใจการควบคุมทั่วไปในระบบสารสนเทศ และสามารถนำไปประกอบการประเมินและตรวจสอบการควบคุมทั่วไปในระบบสารสนเทศ สำหรับผู้สอบบัญชีและผู้ตรวจสอบระบบสารสนเทศ ใช้เป็นความรู้พื้นฐานในการตรวจสอบระบบสารสนเทศในกรณีที่ผู้สอบบัญชีจะต้องสอบบัญชีกิจการที่ใช้ระบบสารสนเทศในการประมวลผลข้อมูลและรายงานทางการบัญชีและต้องการที่จะใช้วิธีการสอบบัญชีในลักษณะที่พึ่งพาการควบคุมของระบบสารสนเทศ

ผู้สอบบัญชีและผู้ตรวจสอบระบบสารสนเทศเมื่อศึกษาเนื้อหาของบทนี้แล้วจะสามารถเข้าใจ ความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับการบริหารงานสารสนเทศโดยรวมขององค์กร และสามารถเข้าใจวิธีการควบคุมในการจัดการความเสี่ยงดังกล่าว ซึ่งความรู้ในส่วนนี้มีความสำคัญเป็นอย่างยิ่งสำหรับการสอบบัญชีกิจการที่ใช้ระบบสารสนเทศ

3. คำนำ

เนื้อหาที่สำคัญของบทนี้ คือการให้ความเข้าใจต่อการควบคุมทั่วไปในระบบสารสนเทศ ซึ่งเป็นพื้นฐานของการควบคุมโดยรวมด้านสารสนเทศ แต่ก่อนที่จะทำความเข้าใจต่อรายละเอียดของการควบคุมทั่วไป ในส่วนแรกของบทเป็นการอธิบายความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับการควบคุมทั่วไปในระบบสารสนเทศ แล้วจึงอธิบายรายละเอียดของการควบคุมทั่วไปในระบบสารสนเทศในแต่ละกระบวนการทำงาน ประกอบด้วย

3.1 การกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานสารสนเทศ

3.2 การพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ

3.3 การรักษาความปลอดภัยระบบสารสนเทศ

3.4 การปฏิบัติการคอมพิวเตอร์

3.5 การบริหารจัดการข้อมูล

3.6 การวางแผนเพื่อกู้ระบบสารสนเทศ ในกรณีที่เกิดความเสียหายอย่างรุนแรง

ในส่วนท้ายของบทเป็นการอธิบายหลักการและแนวทางการตรวจสอบการควบคุมทั่วไปในระบบสารสนเทศของกระบวนการทำงานข้างต้น

4. ความหมายและวัตถุประสงค์ของการควบคุมทั่วไป

การควบคุมทั่วไปในระบบสารสนเทศนั้นเป็นการควบคุมภายในกระบวนการทำงานด้านสารสนเทศ ซึ่งไม่ได้เฉพาะเจาะจงว่าเป็นการควบคุมระบบงาน (Application Controls) ใด ซึ่งการควบคุมทั่วไปนั้นเป็นการควบคุมที่อยู่ในความรับผิดชอบของผู้บริหารสารสนเทศ และผู้บริหารระดับสูง และส่วนใหญ่อยู่ในกระบวนงานในฝ่ายสารสนเทศ

การควบคุมทั่วไปในระบบสารสนเทศมีวัตถุประสงค์เพื่อให้มั่นใจว่าการดำเนินการด้านสารสนเทศนั้นสามารถตอบสนองต่อความต้องการด้านสารสนเทศโดยรวมขององค์กร ซึ่งความต้องการขององค์กรประกอบด้วยความต้องการด้านประสิทธิภาพและประสิทธิผลของการดำเนินงาน (Efficiency and Effectiveness) ความปลอดภัยของข้อมูลและระบบสารสนเทศ (Security and Confidentiality) ความถูกต้องครบถ้วนของข้อมูล (Integrity) หรือความพร้อมใช้ของข้อมูลและระบบสารสนเทศ (Availability)

การควบคุมทั่วไปในระบบสารสนเทศ ซึ่งเน้นที่การใช้งานโดยรวมขององค์กรนั้นประกอบด้วย

- 4.1 การกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานสารสนเทศ
- 4.2 การพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ
- 4.3 การรักษาความปลอดภัยระบบสารสนเทศ
- 4.4 การปฏิบัติการคอมพิวเตอร์
- 4.5 การบริหารจัดการข้อมูล
- 4.6 การวางแผนเพื่อกู้ระบบสารสนเทศ ในกรณีที่เกิดความเสียหายอย่างรุนแรง

ซึ่งมีความหมายและวัตถุประสงค์ในแต่ละองค์ประกอบดังนี้

4.1 การกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานสารสนเทศ

การกำหนดนโยบายในภาพรวมของการใช้ระบบสารสนเทศ และการจัดทำแผนงานด้านสารสนเทศเป็นการดำเนินการเพื่อให้มั่นใจว่า การใช้งานสารสนเทศสอดคล้องกับหลักการควบคุมที่ดี และแผนงานด้านสารสนเทศสอดคล้องกับแผนงานทางธุรกิจ กล่าวคือแผนงานสารสนเทศนั้นมีส่วนสนับสนุนกิจกรรมต่าง ๆ ขององค์กรในการทำให้องค์กรบรรลุถึงวัตถุประสงค์และเป้าหมายขององค์กร

การจัดโครงสร้างงานสารสนเทศมุ่งเน้นด้านการแบ่งแยกหน้าที่งานสารสนเทศ และการกำหนดหน้าที่ความรับผิดชอบของฝ่ายงานสารสนเทศที่ชัดเจน เพื่อเป็นพื้นฐานที่สำคัญในการจัดให้มีการควบคุมที่ดี และเพื่อเอื้อให้เกิดการบริหารงานสารสนเทศอย่างมีประสิทธิภาพ ในการแบ่งแยกหน้าที่งานสารสนเทศนั้น เป็นทั้งการแบ่งแยกงานระหว่างฝ่ายสารสนเทศ และฝ่ายธุรกิจ รวมทั้งการแบ่งแยกงานสารสนเทศในฝ่ายสารสนเทศเอง

4.2 การพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ

การควบคุมในส่วนนี้เป็นการควบคุมกระบวนการพัฒนาระบบงานเพื่อให้มั่นใจว่าระบบงานที่พัฒนาขึ้นมาเพื่อใช้ในการประมวลผลข้อมูลต่าง ๆ ในองค์กรนั้น มีความสอดคล้องกับวัตถุประสงค์ในการใช้ระบบสารสนเทศ และระบบที่นำมาใช้งานนั้นทำงานอย่างถูกต้องครบถ้วนตามเงื่อนไขหรือความต้องการขององค์กร

การควบคุมในส่วนนี้ยังรวมถึงการเปลี่ยนแปลงแก้ไขระบบงานต่าง ๆ หลังจากมีการใช้ระบบงานนั้น ๆ แล้ว เพื่อให้มั่นใจว่าการเปลี่ยนแปลงระบบสารสนเทศ มีการดำเนินการอย่างเหมาะสม และการเปลี่ยนแปลงนั้นมีการอนุมัติให้ดำเนินการจากผู้มีอำนาจ ตลอดจนมีการทดสอบการเปลี่ยนแปลงก่อนการนำระบบงานหรือโปรแกรมใหม่มาใช้งาน

4.3 การรักษาความปลอดภัยระบบสารสนเทศ

การควบคุมที่มีความสำคัญมากอีกส่วนหนึ่งก็คือการควบคุมด้านความปลอดภัยระบบสารสนเทศ ในส่วนนี้ ประกอบด้วยการบริหารจัดการด้านความปลอดภัยที่ดี เช่นการกำหนดนโยบายด้านความปลอดภัย การกำหนดระเบียบปฏิบัติต่างๆ ที่เกี่ยวข้องกับความปลอดภัย และกระบวนการการให้ความรู้ในการใช้งานสารสนเทศอย่างปลอดภัยต่อผู้ใช้งานระบบสารสนเทศ

การควบคุมในส่วนนี้ยังรวมถึงการควบคุมความปลอดภัยทางกายภาพของระบบสารสนเทศ การเข้าถึงห้องหรือศูนย์คอมพิวเตอร์ และอุปกรณ์ที่สำคัญ รวมทั้งการจัดให้มีสภาพแวดล้อมในการทำงานที่ดีของเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ตั้งแต่การควบคุมอุณหภูมิ ความชื้น คลื่นแม่เหล็กและฝุ่นละออง เป็นต้น

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

4.4 การปฏิบัติการคอมพิวเตอร์

ในส่วนของการควบคุมการปฏิบัติการคอมพิวเตอร์นั้น เป็นการควบคุมเพื่อให้การดำเนินการใด ๆ เกี่ยวกับระบบคอมพิวเตอร์ ตั้งแต่การเปิดปิดเครื่อง บำรุงรักษาและแก้ไขปัญหาต่าง ๆ การประมวลผลสิ้นวัน การสำรองข้อมูล และการจัดพิมพ์รายงาน เพื่อให้การดำเนินการต่าง ๆ ดังที่กล่าวมาแล้วดำเนินการอย่างมีประสิทธิภาพและประสิทธิผล โดยมีการกำหนดระเบียบปฏิบัติที่ชัดเจน และมีการสอบทานให้การดำเนินการเป็นไปตามระเบียบดังกล่าว

4.5 การบริหารจัดการข้อมูล

การบริหารจัดการข้อมูลสารสนเทศนั้น ประกอบด้วยการกำหนดโครงสร้างข้อมูลขององค์กรและผู้รับผิดชอบข้อมูลที่ชัดเจน การแบ่งประเภทข้อมูลตามความสำคัญของข้อมูล การบริหารด้านความถูกต้องและครบถ้วนของข้อมูล การจัดเก็บข้อมูล และการนำข้อมูลไปใช้งาน โดยมีวัตถุประสงค์เพื่อให้องค์กรมีการใช้ข้อมูลที่ถูกต้องครบถ้วน และตรงกับความต้องการในการใช้ข้อมูลของทุกส่วนในองค์กร

4.6 การวางแผนเพื่อกู้ระบบสารสนเทศ ในกรณีที่เกิดความเสียหายรุนแรงต่อระบบสารสนเทศ

การควบคุมในส่วนนี้เป็นการเตรียมความพร้อมทั้งด้านระบบสำรอง ข้อมูลสำรอง บุคลากร และสถานที่ เพื่อรองรับเหตุการณ์ที่อาจก่อให้เกิดความเสียหายที่รุนแรงต่อระบบคอมพิวเตอร์ จนทำให้ไม่สามารถดำเนินงานต่อไปได้ตามปกติ ซึ่งประกอบด้วย การจัดทำแผน การจัดเตรียมระบบและอุปกรณ์ที่จำเป็น การกำหนดขั้นตอนการกู้ระบบ การทดสอบแผน และการบำรุงรักษาแผนกู้ระบบสารสนเทศ

5. ความเสี่ยงที่เกี่ยวข้องกับการควบคุมทั่วไปในระบบสารสนเทศ

เป็นที่เข้าใจกันโดยทั่วไปว่าการนำระบบสารสนเทศมาใช้ในกิจกรรมต่าง ๆ ขององค์กรนั้น นอกจากจะใช้เพื่อก่อให้เกิดประโยชน์ต่อองค์กรแล้ว ยังจะต้องคำนึงถึงความเสี่ยงที่ตามมากับการนำระบบสารสนเทศมาใช้และจะต้องบริหารจัดการความเสี่ยงต่าง ๆ เหล่านั้นให้อยู่ในระดับที่องค์กรยอมรับได้

ในส่วนนี้จะอธิบายถึงความเสี่ยงต่าง ๆ ที่ตามมาจากการนำระบบสารสนเทศมาใช้ โดยจะเน้นเฉพาะความเสี่ยงที่เกี่ยวข้องกับการควบคุมทั่วไป ซึ่งจะอธิบายแยกตามองค์ประกอบของการควบคุมทั่วไปในระบบสารสนเทศ ดังต่อไปนี้

5.1 ความเสี่ยงด้านการกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานสารสนเทศ

การกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานสารสนเทศนั้น ความเสี่ยงส่วนใหญ่จะเกี่ยวข้องกับการใช้สารสนเทศเพื่อให้เกิดประสิทธิภาพและประสิทธิผลในการปฏิบัติงานโดยรวมขององค์กร ซึ่งประกอบด้วย

5.1.1 แผนงานและการดำเนินการด้านสารสนเทศอาจไม่สอดคล้องกับแผนงานทางธุรกิจ

5.1.2 การดำเนินงานไม่เป็นไปตามแผนที่กำหนดไว้

5.1.3 การใช้งานหรือการดำเนินการด้านสารสนเทศอาจไม่เป็นไปในทางเดียวกัน หรืออาจทำให้ระบบสารสนเทศ ที่นำมาใช้งานไม่มีความสอดคล้องกัน

5.1.4 ระบบงานสารสนเทศอาจไม่สามารถเชื่อมโยงกันและไม่เอื้อต่อการดำเนินการอย่างมีประสิทธิภาพ

5.1.5 งานสารสนเทศอาจไม่มีการแบ่งแยกที่ดี ส่งผลกระทบทำให้ไม่สามารถจัดให้มีการควบคุมภายในด้านสารสนเทศที่ดีได้

5.1.6 งานสารสนเทศอาจถูกจัดวางในตำแหน่งที่เหมาะสม ก่อให้เกิดอุปสรรคในการประสานงานและการให้บริการด้านสารสนเทศ

5.1.1 แผนงานและการดำเนินการด้านสารสนเทศอาจไม่สอดคล้องกับแผนงานทางธุรกิจ

ถ้าองค์กรขาดการวางแผนงานสารสนเทศที่ดี ผลที่ตามมาอาจทำให้องค์กรไม่สามารถใช้ระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศ ใหม่ ๆ เพื่อนำมาใช้ในองค์กรอาจไม่สอดคล้องกับวัตถุประสงค์ในการใช้ระบบสารสนเทศ ขององค์กร ซึ่งถ้าการวางแผนสารสนเทศมิได้คำนึงถึง

วัตถุประสงค์ของการใช้สารสนเทศโดยรวมขององค์กร อาจเป็นไปได้ว่าแผนงานสารสนเทศ และแผนงานทางธุรกิจอาจมุ่งไปที่วัตถุประสงค์ที่แตกต่างกัน

5.1.2 การดำเนินงานไม่เป็นไปตามแผนที่กำหนดไว้

แผนงานอาจไม่ได้รับการดำเนินการตามที่กำหนดไว้ ซึ่งอาจเกิดจากไม่มีการติดตามผลการดำเนินการตามแผน หรืออาจเกิดจากการเปลี่ยนแปลงเป้าหมายหรือปัจจัยภายนอกต่าง ๆ ซึ่งส่งผลกระทบทำให้องค์กรไม่สามารถใช้ระบบสารสนเทศก่อให้เกิดประโยชน์ตามเป้าหมายที่วางไว้

5.1.3 การใช้งานหรือการดำเนินการด้านสารสนเทศอาจไม่เป็นไปในทางเดียวกัน หรืออาจทำให้ระบบสารสนเทศที่นำมาใช้งานไม่มีความสอดคล้องกัน

ถ้าขาดการกำหนดนโยบายและมาตรฐานเกี่ยวกับการใช้ระบบสารสนเทศ อาจส่งผลทำให้การใช้งานสารสนเทศขาดแนวทางที่ชัดเจน และทำให้เกิดอุปสรรคในการบริหารงานสารสนเทศที่มีประสิทธิภาพ ส่งผลทำให้การดำเนินการด้านสารสนเทศอาจไม่เป็นไปในทางเดียวกัน หรืออาจทำให้ระบบสารสนเทศที่นำมาใช้งานไม่มีความสอดคล้องกัน

5.1.4 ระบบงานสารสนเทศอาจไม่สามารถเชื่อมโยงกันและไม่เอื้อต่อการดำเนินการอย่างมีประสิทธิภาพ

ความเสี่ยงอื่น ๆ ที่เกี่ยวข้องกับการวางแผนงานสารสนเทศ ก็คือระบบสารสนเทศที่นำมาใช้งานนั้น อาจไม่สามารถทำงานแบบบูรณาการ (Integrated) ที่สมบูรณ์ เพราะขาดการกำหนดกรอบหรือแนวทางในการนำระบบสารสนเทศ มาใช้งานที่ชัดเจน กล่าวคือ มีการนำระบบมาใช้งานตามความต้องการในแต่ละครั้งคราว ซึ่งมีแนวโน้มว่าการนำระบบดังกล่าวมาใช้งานนั้น อาจไม่ได้คำนึงถึงการทำงานที่ต้องเชื่อมโยงกันกับระบบงานอื่น ๆ ที่มีอยู่ และอาจทำให้เกิดผลกระทบกับการบริหารจัดการข้อมูลโดยรวมของระบบสารสนเทศ

5.1.5 งานสารสนเทศอาจไม่มีการแบ่งแยกที่ดีส่งผลกระทบทำให้ไม่สามารถจัดให้มีการควบคุมภายในด้านสารสนเทศที่ดีได้

ถ้าไม่มีการแบ่งแยกงานสารสนเทศอย่างเหมาะสม เช่นการรวมงานด้านการพัฒนาระบบงานกับงานปฏิบัติการคอมพิวเตอร์ไว้ด้วยกัน อาจทำให้การควบคุมภายในระบบสารสนเทศด้านต่าง ๆ ไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพ เช่น อาจไม่สามารถจัดให้มีการควบคุมการเปลี่ยนแปลงแก้ไขระบบงานที่ดีได้ เนื่องจากผู้พัฒนาระบบงานสามารถดำเนินการแก้ไข

เปลี่ยนแปลงโปรแกรมได้โดยตรง เพราะผู้พัฒนาระบบงานมีสิทธิเข้าถึงโปรแกรมหรือข้อมูลที่ใช้งานจริง ตามสิทธิการใช้งานตามหน้าที่ด้านการปฏิบัติการคอมพิวเตอร์

นอกจากนี้ยังมีงานด้านสารสนเทศอื่น ๆ เช่นการรักษาความปลอดภัยระบบสารสนเทศ หรือการควบคุมคุณภาพงานสารสนเทศ ซึ่งถ้าดำเนินการโดยผู้รับผิดชอบงานสารสนเทศอื่น ๆ แล้วอาจทำให้เกิดการแบ่งแยกหน้าที่ที่ไม่เหมาะสม ซึ่งส่งผลทำให้การรักษาความปลอดภัย หรือการควบคุมคุณภาพงานสารสนเทศด้อยประสิทธิภาพลง

5.1.6 งานสารสนเทศอาจถูกจัดวางในตำแหน่งที่ไม่เหมาะสม ก่อให้เกิดอุปสรรคในการประสานงานและการให้บริการด้านสารสนเทศ

สำหรับด้านการจัดวางตำแหน่งที่เหมาะสมของสายงานสารสนเทศนั้น ถ้าจัดวางตำแหน่งอย่างไม่เหมาะสมเช่น จัดให้งานสารสนเทศอยู่ภายใต้การดูแลของผู้บริหารด้านใดด้านหนึ่ง เช่นด้านการเงินการบัญชี ทั้ง ๆ ที่การใช้สารสนเทศขององค์กรนั้นใช้สารสนเทศในกระบวนการทำงานในทุกด้านของธุรกิจ อาจก่อให้เกิดอุปสรรคด้านการประสานงาน และเกิดความลักลั่นในการให้บริการสารสนเทศอย่างเท่าเทียมกันในองค์กร

5.2 ความเสี่ยงด้านการพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ

ในการพัฒนาระบบงานสารสนเทศและการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศนั้น ความเสี่ยงที่สำคัญคือ ความเสี่ยงที่หลังจากพัฒนาระบบงานเสร็จสิ้นแล้ว ระบบที่จัดทำขึ้นอาจยังไม่สอดคล้องกับความต้องการหรือวัตถุประสงค์ของการพัฒนาระบบงาน และระบบงานที่พัฒนาขึ้นมาใหม่นั้นยังมีข้อบกพร่องภายในระบบหลังจากที่นำมาใช้งานแล้ว

ความเสี่ยงที่เกี่ยวข้องกับการพัฒนาระบบงานและการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ มีดังนี้

5.2.1 ระบบงานใหม่อาจไม่สอดคล้องกับความต้องการทางธุรกิจ

5.2.2 ระบบงานยังมีข้อบกพร่องหลังจากนำมาใช้งานแล้ว

5.2.3 กระบวนการพัฒนาและเปลี่ยนแปลงระบบงานขาดประสิทธิภาพ

5.2.1. ระบบงานใหม่อาจไม่สอดคล้องกับความต้องการทางธุรกิจ

ความเสี่ยงที่เกี่ยวกับความไม่สอดคล้องต่อความต้องการทางธุรกิจของระบบงานที่พัฒนาหรือเปลี่ยนแปลงนับได้ว่าเป็นความเสี่ยงที่สำคัญที่สุด ซึ่งมีโอกาสเกิดขึ้นค่อนข้างสูงทั้งนี้เพราะผู้พัฒนาระบบงานอาจขาดความเข้าใจที่ชัดเจนต่อความต้องการและเงื่อนไขการทำงานของ

ระบบงานใหม่ หรือขาดกระบวนการติดตามตรวจวัดที่มีประสิทธิภาพในการทำให้มั่นใจว่าวัตถุประสงค์หรือเป้าหมายต่าง ๆ ของการพัฒนาระบบงานได้รับการจัดการอย่างครบถ้วนสมบูรณ์ ซึ่งความเสี่ยงนี้จะส่งผลกระทบด้านประสิทธิผลและประสิทธิภาพของการดำเนินการทางธุรกิจโดยตรง แต่อาจไม่มีผลกระทบโดยตรงต่อความครบถ้วนและถูกต้องของข้อมูลต่าง ๆ ที่ประมวลผลโดยระบบฯ

5.2.2. ระบบงานยังมีข้อบกพร่องหลังจากนำมาใช้งานแล้ว

ความเสี่ยงในส่วนถัดมาซึ่งมีผลต่อความถูกต้องและครบถ้วนของการประมวลผล ก็คือความเสี่ยงที่ระบบงานยังมีข้อบกพร่องหลังจากที่ระบบงานถูกนำมาใช้งานจริงแล้ว ทั้งนี้อาจเกิดจากการขาดการทดสอบระบบอย่างเหมาะสมและครบถ้วนเพียงพอ เช่นผู้ทดสอบไม่มีความรู้ความเข้าใจต่อเงื่อนไขต่าง ๆ ของระบบงานอย่างเพียงพอ หรือระยะเวลาที่เตรียมไว้สำหรับการทดสอบมีน้อยเกินไป ในบางกรณีข้อบกพร่องอาจยังไม่เกิดขึ้นโดยทันทีหลังจากนำระบบมาใช้งานในระยะแรก แต่ข้อบกพร่องอาจเกิดขึ้นหลังจากการใช้งานผ่านไปแล้วระยะหนึ่ง ทำให้ การแก้ไขข้อบกพร่องต่าง ๆ เหล่านั้นทำได้ยากยิ่งขึ้น ความเสี่ยงในส่วนนี้มีผลโดยตรงต่อความครบถ้วนถูกต้องของการประมวลผล ซึ่งส่งผลให้ข้อมูลต่าง ๆ ภายในระบบงานขาดความน่าเชื่อถือ โดยเฉพาะอย่างยิ่งถ้าเป็นระบบงานที่เกี่ยวข้องกับข้อมูลทางการบัญชีและการเงิน ดังนั้นผู้สอบบัญชีจะให้ความสำคัญกับความเสี่ยงนี้เป็นพิเศษ

5.2.3. กระบวนการพัฒนาและเปลี่ยนแปลงระบบงานขาดประสิทธิภาพ

ความเสี่ยงอื่น ๆ ที่เกี่ยวข้องกับการพัฒนาและเปลี่ยนแปลงแก้ไขระบบงาน ซึ่งโอกาสเกิดขึ้นค่อนข้างสูงก็คือด้านประสิทธิภาพของการบริหารโครงการการพัฒนาหรือเปลี่ยนแปลงแก้ไขระบบงาน ซึ่งประกอบด้วยความเสี่ยงที่การพัฒนาระบบหรือการเปลี่ยนแปลงอาจล่าช้า ไม่แล้วเสร็จในระยะเวลาที่คาดการณ์ไว้ หรือเป็นการใช้ทรัพยากรหรืองบประมาณมากเกินกว่าที่จัดเตรียมไว้ ทั้งนี้เพราะในระหว่างการดำเนินโครงการนั้นมีปัจจัยหรือเหตุการณ์ที่ไม่คาดหวังเกิดขึ้นเสมอ เช่น วัตถุประสงค์และขอบเขตงานมีการเปลี่ยนแปลง บุคลากรสำคัญของโครงการมีการเปลี่ยนแปลงและปัจจัยภายนอกอื่น ๆ ยิ่งระยะเวลาในการพัฒนาหรือเปลี่ยนแปลงระบบงานฯ มีระยะเวลานานความเสี่ยงเหล่านี้ก็ยิ่งมีโอกาสเกิดขึ้นสูง แต่อย่างไรก็ตามผู้สอบบัญชีอาจไม่ให้ความสำคัญกับความเสี่ยงนี้มากเท่าไร เพราะว่าความเสี่ยงนี้ไม่ค่อยมีผลกระทบโดยตรงต่อความถูกต้องครบถ้วนของการประมวลผลข้อมูลทางบัญชีการเงิน

5.3 ความเสี่ยงด้านการรักษาความปลอดภัยระบบสารสนเทศ

ในด้านการรักษาความปลอดภัยระบบสารสนเทศ นั้น ความเสี่ยงที่สำคัญคือการที่บุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศ สามารถเข้ามาสู่ระบบ และทำให้เกิดความเสียหายต่อข้อมูล โปรแกรมหรือระบบคอมพิวเตอร์ ซึ่งอาจเป็นการเปลี่ยนแปลงข้อมูลหรือโปรแกรม หรืออาจเป็นการทำให้เกิดความเสียหายต่อระบบจนไม่สามารถทำงานต่อไปได้ หรือเป็นการเข้ามาเพื่อลักลอบนำข้อมูลไปใช้ประโยชน์ด้านต่าง ๆ และมีอาจมีผลกระทบต่อความถูกต้อง ครบถ้วนของข้อมูลทางการเงินและรายงานทางบัญชี ซึ่งความเสี่ยงเหล่านี้อาจเกิดขึ้นจากหลายสาเหตุ ซึ่งสามารถแบ่งเป็น 4 กลุ่มที่สำคัญ ดังต่อไปนี้

5.3.1 ความเสี่ยงที่เกี่ยวข้องกับบุคคล

5.3.2 ความเสี่ยงที่เกี่ยวข้องกับกระบวนการทำงาน

5.3.3 ความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยี

5.3.4 ความเสี่ยงที่เกี่ยวข้องกับการรักษาความปลอดภัยทางกายภาพ

5.3.1 ความเสี่ยงที่เกี่ยวข้องกับบุคคล

ในส่วนของความเสี่ยงที่เกี่ยวข้องกับบุคคล อาจมีสาเหตุมาจากประเด็นต่าง ๆ ต่อไปนี้

- ในด้านการบริหารการรักษาความปลอดภัยระบบสารสนเทศ นั้น องค์กรอาจไม่มีการกำหนดนโยบายที่ชัดเจนในการรักษาความปลอดภัย ทำให้ขาดแนวทางในการดำเนินการที่ชัดเจน และทำให้ขาดแนวทางในการใช้ระบบของผู้ใช้งานระบบสารสนเทศ
- การกำหนดหน้าที่ความรับผิดชอบด้านการรักษาความปลอดภัยอาจยังไม่ชัดเจน ซึ่งอาจไม่มีการกำหนดโครงสร้างองค์กรที่ชัดเจนในด้านการรักษาความปลอดภัย และการกำหนดหน้าที่ความรับผิดชอบของเจ้าของข้อมูล เจ้าของระบบงาน ผู้บริหารและเจ้าหน้าที่ด้านความปลอดภัยระบบสารสนเทศ และ ผู้ใช้งานทั่วไป เป็นต้น
- ผู้ใช้งานอาจไม่เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบอย่างชัดเจน ซึ่งอาจจะมีสาเหตุมาจากการขาดนโยบายที่ชัดเจนตามที่กล่าวมาแล้วข้างต้น หรือขาดกระบวนการทำให้เกิดความเข้าใจเช่นการฝึกอบรม หรือการสื่อสารข้อมูลด้านนโยบายอย่างต่อเนื่องสม่ำเสมอ
- บุคลากรที่มีหน้าที่รับผิดชอบด้านการรักษาความปลอดภัยอาจขาดความรู้ความสามารถที่เพียงพอในด้านการจัดการความปลอดภัย ทั้งด้านการบริหารความปลอดภัย ความเสี่ยงด้านความปลอดภัย และความรู้ทางเทคนิคที่จำเป็น

5.3.2 ความเสี่ยงที่เกี่ยวข้องกับกระบวนการทำงาน

ในส่วนของความเสี่ยงที่เกี่ยวข้องกับกระบวนการทำงาน อาจมีสาเหตุมาจากประเด็นต่าง ๆ ต่อไปนี้

- กระบวนการบริหารจัดการในการให้หรือยกเลิกสิทธิในการเข้าถึงระบบสารสนเทศ อาจขาดความรัดกุมเพียงพอ หรือขาดความชัดเจน ในด้านการอนุมัติ การอนุญาต หรือยกเลิกการให้เข้าถึงระบบฯ การดำเนินการ การสอบทานความถูกต้อง หลังจากการดำเนินการ เป็นต้น
- ขาดกระบวนการติดตาม ตรวจสอบ และวิเคราะห์ เหตุการณ์ต่าง ๆ ที่อาจเกี่ยวข้องกับความปลอดภัยระบบสารสนเทศ เพื่อหาแนวทางป้องกันที่เหมาะสมในอนาคต

5.3.3 ความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยี

ในส่วนของความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยี อาจมีสาเหตุมาจากประเด็นต่าง ๆ ต่อไปนี้

- ไม่มีการกำหนดมาตรฐานทางเทคนิคในการติดตั้งระบบคอมพิวเตอร์และระบบเครือข่ายที่เหมาะสม เพื่อเป็นแนวทางในการกำหนดค่าตัวแปรด้านความปลอดภัยของระบบฯ
- ระบบปฏิบัติการคอมพิวเตอร์ ระบบจัดการฐานข้อมูลและระบบเครือข่ายไม่ได้รับการติดตั้งให้มีการรักษาความปลอดภัยที่เพียงพอ กล่าวคือการกำหนดค่าตัวแปรด้านความปลอดภัย (Security Parameters) อาจไม่เป็นไปตามมาตรฐานการรักษาความปลอดภัยที่ดี เช่น ค่าตัวแปรด้านการใช้รหัสผ่าน (Password Parameters) ค่าตัวแปรด้านการกำหนดสิทธิในการใช้งาน (System Authorization Parameters) และค่าตัวแปรด้านการบันทึกกิจกรรมของระบบฯ (Audit Logging Parameters)
- ขาดเครื่องมือที่สำคัญในการบริหารและจัดการความปลอดภัยที่มีประสิทธิภาพ เช่น การติดตั้งไฟร์วอลล์ (Firewall) และซอฟต์แวร์ในการตรวจจับเหตุการณ์ต่าง ๆ ด้านการบุกรุกระบบคอมพิวเตอร์และระบบเครือข่าย
- การเปลี่ยนแปลงที่รวดเร็วของเทคโนโลยี ทำให้เกิดเทคนิคการเจาะระบบใหม่ ๆ ที่เทคโนโลยีในปัจจุบันไม่สามารถป้องกันได้
- เทคโนโลยีขององค์กรเก่าหรือล้าสมัย ทำให้ไม่สามารถปฏิบัติงานด้านการรักษาความปลอดภัยได้อย่างมีประสิทธิภาพ

5.3.4 ความเสี่ยงที่เกี่ยวข้องกับการรักษาความปลอดภัยทางกายภาพ

ในด้านการรักษาความปลอดภัยทางกายภาพอาจยังมีข้อบกพร่อง ทั้งในด้านการออกแบบ เช่นการออกแบบสถานที่ของศูนย์คอมพิวเตอร์ การติดตั้งอุปกรณ์ด้านความปลอดภัย และอุปกรณ์เกี่ยวกับการจัดการสภาพแวดล้อมของการทำงานของระบบคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งภายในศูนย์คอมพิวเตอร์ เช่นอุปกรณ์ควบคุมอุณหภูมิ ความชื้น อุปกรณ์ป้องกันอัคคีภัยเป็นต้น ซึ่งส่งผลกระทบต่อประสิทธิภาพและความถูกต้องของการประมวลผลในระบบสารสนเทศ

5.4 ความเสี่ยงด้านการปฏิบัติการคอมพิวเตอร์

เนื่องจากการปฏิบัติการคอมพิวเตอร์ส่วนใหญ่เป็นการปฏิบัติงานในภาพรวมของการประมวลผล ซึ่งเกี่ยวกับรายการทุกรายการที่นำเข้าและประมวลผลโดยระบบคอมพิวเตอร์ ดังนั้นหากเกิดข้อผิดพลาดขึ้นก็จะส่งผลกระทบในวงกว้างต่อระบบสารสนเทศ กล่าวคืออาจส่งผลทำให้ข้อมูลทั้งหมดผิดพลาด ซึ่งความเสี่ยงในส่วนของการปฏิบัติการคอมพิวเตอร์นี้ ประกอบด้วย

- การเปิดปิดระบบคอมพิวเตอร์และการเปิดปิดระบบงานที่ไม่เหมาะสม เช่น การปิดระบบงานขณะที่ยังมีผู้ใช้งานบางคนยังนำเข้าข้อมูลไม่ครบ หรืออยู่ระหว่างการประมวลผล อาจส่งผลทำให้ข้อมูลในระบบไม่ครบถ้วน
- การประมวลผลสิ้นวันอาจไม่ถูกต้องครบถ้วนเนื่องจากประมวลผลผิดลำดับขั้นตอนที่กำหนดไว้ หรือข้ามขั้นตอนบางขั้นตอนที่สำคัญ ทำให้การประมวลผลไม่ถูกต้องครบถ้วน
- การสำรองข้อมูลอาจไม่ครบถ้วน หรือข้อมูลที่สำรองไว้ในอุปกรณ์สำรองข้อมูลไม่ปลอดภัยหรือเสียหาย ไม่สามารถนำมาใช้ในการกู้ระบบเมื่อมีความจำเป็น
- ปัญหาต่าง ๆ ที่เกี่ยวกับการใช้งานระบบคอมพิวเตอร์หรือระบบเครือข่ายอาจไม่ได้รับการแก้ไขอย่างทันท่วงที
- ระบบคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอาจไม่ได้รับการบำรุงรักษาและปรับปรุงให้อยู่ในสภาพพร้อมใช้งานอยู่ตลอดเวลา

5.5 ความเสี่ยงด้านการบริหารจัดการข้อมูล

ข้อมูลในระบบสารสนเทศนับได้ว่าเป็นหัวใจสำคัญของการใช้ระบบสารสนเทศ ซึ่งถ้าข้อมูลไม่มีคุณภาพ อาจส่งผลต่อการดำเนินกิจกรรมต่าง ๆ ภายในองค์กรในหลายด้านด้วยกัน เช่น ประสิทธิภาพของการดำเนินงาน การรายงานทางการเงิน การตัดสินใจในการบริหาร เป็นต้น ซึ่งความเสี่ยงที่เกี่ยวกับการบริหารจัดการข้อมูล สามารถสรุปโดยรวมได้ว่า ข้อมูลอาจขาดความครบถ้วนและถูกต้อง ขาดความปลอดภัย หรืออาจไม่มีข้อมูลให้ใช้เมื่อต้องการ ทั้งนี้อาจเกิดขึ้นจากหลายสาเหตุ ดังต่อไปนี้

- ขาดการศึกษาความต้องการใช้ข้อมูล และขาดการจัดทำโครงสร้างของข้อมูลในองค์กรที่ชัดเจน
- ขาดข้อมูลสำหรับการบริหารจัดการข้อมูลสารสนเทศ
- ไม่มีการกำหนดผู้รับผิดชอบที่ชัดเจนในการบริหารความถูกต้องและความปลอดภัยของข้อมูล
- ไม่มีการแบ่งชั้นความสำคัญของข้อมูล ทำให้ไม่สามารถบริหารความถูกต้องครบถ้วนและความปลอดภัยของข้อมูลอย่างเหมาะสม
- กระบวนการที่เกี่ยวข้องกับการบริหารจัดการข้อมูลอาจไม่ชัดเจน เช่น กระบวนการสอบทานความถูกต้องครบถ้วนของข้อมูล กระบวนการจัดเก็บข้อมูล และกระบวนการนำข้อมูลมาใช้งาน
- ขาดเครื่องมือ หรือโปรแกรมที่มีประสิทธิภาพในการใช้ข้อมูลประกอบการดำเนินการหรือประกอบการตัดสินใจทางการบริหาร

5.6 ความเสี่ยงด้านการวางแผนเพื่อกู้ระบบสารสนเทศ ในกรณีที่เกิดความเสียหายอย่างรุนแรง

การทำให้ระบบสารสนเทศมีความต่อเนื่องในการให้บริการนั้น มีความจำเป็นอย่างยิ่งโดยเฉพาะสำหรับองค์กรที่ต้องพึ่งพาระบบสารสนเทศในการดำเนินธุรกิจ ซึ่งถ้าระบบหยุดชะงักอาจส่งผลทำให้ธุรกิจหยุดชะงัก และอาจส่งผลถึงความอยู่รอดขององค์กรในระยะยาว

สำหรับความเสี่ยงด้านการวางแผนเพื่อกู้ระบบสารสนเทศ ในกรณีที่เกิดความเสียหายอย่างรุนแรงนั้นอาจไม่มีผลโดยตรงต่อความถูกต้องและครบถ้วนของรายงานทางการเงินและรายงานทางบัญชี แต่ผู้สอบบัญชีก็ควรให้ความสำคัญต่อความเสี่ยงในส่วนนี้ เพราะถ้าเกิดความเสียหายต่อระบบสารสนเทศที่รุนแรงถึงขนาดที่องค์กรไม่สามารถดำเนินกิจกรรมหลักขององค์กรได้ อาจจะส่งผลถึงความอยู่รอดทางธุรกิจขององค์กร เช่นการสูญเสียลูกค้าส่วนใหญ่ สูญเสียความสามารถในการประกอบกิจกรรมสำคัญ ซึ่งอาจทำให้ไม่สามารถแข่งขันต่อไปได้

ความเสี่ยงที่สำคัญที่เกี่ยวข้องกับการวางแผนเพื่อกู้ระบบสารสนเทศ ในกรณีที่เกิดความเสียหายอย่างรุนแรง ประกอบด้วย

2.6.1 อาจเกิดอุบัติเหตุหรืออุบัติภัยทำให้เกิดผลเสียหายต่อเทคโนโลยีคอมพิวเตอร์หรือระบบเครือข่าย ทำให้ธุรกิจหยุดชะงัก

2.6.2 ระบบสารสนเทศ อาจหยุดชะงัก เนื่องจากขาดการบำรุงรักษาเทคโนโลยีคอมพิวเตอร์และระบบเครือข่ายทำให้เทคโนโลยีคอมพิวเตอร์ หรือระบบเครือข่ายขัดข้อง

2.6.3 ไม่สามารถกู้ระบบสารสนเทศหรือระบบเครือข่ายได้ภายในระยะเวลาที่เหมาะสม หรืออาจไม่สามารถกู้ระบบสารสนเทศกลับมาใช้ใหม่ได้เลย เนื่องจาก

- ไม่มีการสำรองข้อมูลหรือสำรองข้อมูลไม่ครบถ้วน
- ไม่มีเทคโนโลยีคอมพิวเตอร์หรือระบบเครือข่ายสำรองที่สามารถกู้ระบบได้ภายในระยะเวลาที่เหมาะสม
- บุคลากรที่มีหน้าที่กู้ระบบอาจขาดความเข้าใจในขั้นตอนการดำเนินการ

6. การควบคุมด้านการกำหนดนโยบาย การวางแผนและการจัดโครงสร้างงานสารสนเทศ

การควบคุมด้านการกำหนดนโยบาย การวางแผนและการจัดโครงสร้างงานสารสนเทศเป็นพื้นฐานสำคัญในการกำหนดกรอบในการควบคุมของกิจกรรมสารสนเทศต่าง ๆ ภายในองค์กร ซึ่งถ้าไม่มีการกำหนดพื้นฐานที่ดี การควบคุมในส่วนต่าง ๆ อาจไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพ สำหรับในการควบคุมในส่วนนี้มีวัตถุประสงค์และแนวทางการควบคุมดังต่อไปนี้

6.1 การควบคุมด้านการกำหนดนโยบายสารสนเทศ

การควบคุมด้านการกำหนดนโยบายสารสนเทศมีวัตถุประสงค์ของการควบคุมเพื่อให้การใช้ระบบสารสนเทศเป็นไปในแนวทางและมาตรฐานเดียวกัน และสนับสนุนให้เกิดประสิทธิภาพในการบริหารและการควบคุมงานด้านสารสนเทศขององค์กรโดยรวม ซึ่งมีแนวทางการควบคุม ดังนี้

6.1.1 ควรมีการกำหนดนโยบายการใช้ระบบสารสนเทศ เพื่อใช้เป็นแนวทางสำหรับการบริหารจัดการงานต่าง ๆ ด้านสารสนเทศ ประกอบด้วย นโยบายด้านการรักษาความปลอดภัยระบบสารสนเทศ นโยบายด้านการพัฒนาระบบงาน มาตรฐานของระบบคอมพิวเตอร์ที่นำมาใช้งานภายในองค์กร เช่นมาตรฐานด้านซอฟต์แวร์ ฮาร์ดแวร์ เป็นต้น ผู้บริหารระดับสูงขององค์กรควรเป็นผู้อนุมัตินโยบายดังกล่าว และควรมีการประกาศใช้อย่างเป็นทางการ

6.1.2 สำหรับมาตรฐานด้านซอฟต์แวร์ที่เป็นระบบงานสารสนเทศ (Application) นั้น อาจรวมถึงการกำหนดมาตรฐานด้านความสามารถของซอฟต์แวร์ เช่น ด้านการเชื่อมโยงระหว่างระบบงาน ด้านการควบคุมภายในต่าง ๆ เป็นต้น และถ้าเป็นมาตรฐานด้านซอฟต์แวร์ระบบปฏิบัติการ ก็ควรกำหนดเป็นรุ่นหรือเวอร์ชั่นของซอฟต์แวร์ที่อนุญาตให้นำมาใช้งาน ทั้งนี้เพราะหากว่าไม่มีการกำหนดมาตรฐานดังกล่าว และนำซอฟต์แวร์ต่างรุ่นต่างเวอร์ชั่นมาใช้งานแล้วนั้น อาจก่อให้เกิดปัญหาทั้งทางด้านประสิทธิภาพในการใช้งานโดยรวม การบำรุงรักษา และการแก้ไขปัญหา และควรมีการสอบทานเพื่อปรับปรุงนโยบายและมาตรฐานอย่างสม่ำเสมอ แต่ไม่ควรปรับปรุงบ่อยเกินไป เช่นอาจจะสอบทานทุก 1 หรือ 2 ปี เป็นต้น

6.2 การควบคุมด้านการวางแผนงานสารสนเทศ

การควบคุมด้านการวางแผนงานด้านสารสนเทศมีวัตถุประสงค์ของการควบคุมเพื่อ

- ให้มั่นใจว่ากลยุทธ์และแผนการดำเนินงานด้านสารสนเทศ สอดคล้องและสนับสนุนวัตถุประสงค์ เป้าหมายและกลยุทธ์ทางธุรกิจขององค์กร
- เพื่อให้การทำงานโดยรวมของระบบสารสนเทศ ทำงานสอดประสานกันอย่างเป็นบูรณาการ และมีประสิทธิภาพสูงสุด
- เพื่อให้มีการสื่อสารและทำความเข้าใจต่อแผนงานสารสนเทศให้กับบุคคลหรือหน่วยงานที่เกี่ยวข้องอย่างชัดเจน
- เพื่อให้มีการติดตามการปฏิบัติตามแผนงานอย่างสม่ำเสมอ

ดังมีแนวทางการควบคุมดังต่อไปนี้

6.2.1 การกำหนดผู้รับผิดชอบในการวางแผนงานด้านสารสนเทศ

6.2.2 จัดให้มีกระบวนการการวางแผนงานสารสนเทศ

6.2.3 การอนุมัติ การสื่อสารและควบคุมแผนงานสารสนเทศ

6.2.4 การติดตามการดำเนินงานตามแผนงานสารสนเทศ

6.2.1 การกำหนดผู้รับผิดชอบในการวางแผนงานด้านสารสนเทศ

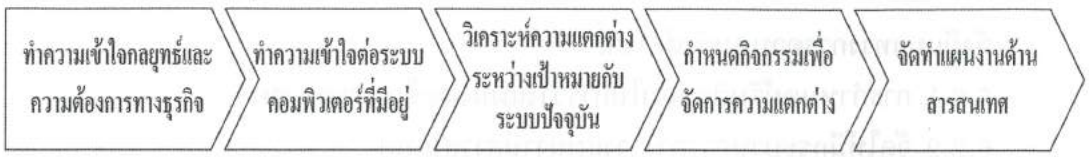
ในการวางแผนงานด้านสารสนเทศนั้น มิใช่เป็นการรับผิดชอบเฉพาะผู้บริหารงานสารสนเทศเท่านั้น ทั้งนี้เพราะการใช้สารสนเทศเป็นการใช้งานโดยรวมเพื่อก่อให้เกิดประโยชน์สูงสุดต่อองค์กร โดยเฉพาะอย่างยิ่งเพื่อทำให้บทบาทที่สำคัญของระบบสารสนเทศ ในการสนับสนุนให้กิจกรรมทางธุรกิจดำเนินการอย่างมีประสิทธิภาพและประสิทธิผล และก่อให้เกิดสินค้าและการบริการที่ทันสมัย เพื่อทำให้องค์กรมีความได้เปรียบในการแข่งขัน ดังนั้นผู้ที่รับผิดชอบในการวางแผนงานสารสนเทศควรเริ่มตั้งแต่ผู้บริหารระดับสูง ผู้บริหารสายงานธุรกิจต่าง ๆ และผู้บริหารงานสารสนเทศ ซึ่งสามารถสรุปบทบาทหน้าที่ได้ดังนี้

- **ผู้บริหารระดับสูง** เป็นผู้รับผิดชอบหลักในการกำหนดแนวทางและกลยุทธ์ในการใช้สารสนเทศสนับสนุนวัตถุประสงค์ เป้าหมายและกลยุทธ์โดยรวมขององค์กร
- **ผู้บริหารสายงานต่าง ๆ** รับผิดชอบในการศึกษาและให้ข้อมูลเกี่ยวกับการนำสารสนเทศมาใช้ให้เกิดประโยชน์ในสายงานธุรกิจที่ตัวเองเป็นผู้รับผิดชอบ รวมทั้งให้ข้อมูลเกี่ยวกับการดำเนินธุรกิจต่อผู้บริหารสารสนเทศ เพื่อนำไปใช้ประกอบการจัดทำแผนงานสารสนเทศในรายละเอียด

- ผู้บริหารสายงานสารสนเทศ รับผิดชอบในการจัดทำแผนงานในรายละเอียด สำหรับการดำเนินงานด้านต่าง ๆ เกี่ยวกับระบบสารสนเทศ นอกจากนี้ยังมีหน้าที่ในการให้ความรู้ต่อผู้บริหารสายงานต่าง ๆ เกี่ยวกับระบบสารสนเทศที่เกี่ยวข้องกับการดำเนินกิจการธุรกิจขององค์กร

6.2.2 จัดให้มีกระบวนการวางแผนงานสารสนเทศ

การวางแผนงานสารสนเทศนั้นมีวัตถุประสงค์เพื่อจัดให้มีแผนการดำเนินการด้านสารสนเทศที่ตอบสนองต่อความต้องการทางธุรกิจ ขั้นตอนสำคัญในการวางแผนงานด้านสารสนเทศแสดงไว้ในภาพ 3 - 1 กระบวนการวางแผนงานสารสนเทศ



ภาพ 3-1 กระบวนการวางแผนงานสารสนเทศ

การวางแผนควรเริ่มจากการทำความเข้าใจต่อกลยุทธ์ วัตถุประสงค์และเป้าหมายทางธุรกิจ และทำการกำหนดลักษณะของระบบข้อมูล ระบบงาน เทคโนโลยี และ โครงสร้างงานและบุคลากรที่จำเป็นต่อการดำเนินการเพื่อให้บรรลุถึงวัตถุประสงค์ดังกล่าว ซึ่งต้องคำนึงถึงเทคโนโลยีใหม่ ๆ ที่สามารถนำเข้ามาใช้ในอนาคตด้วย หรือการประมวลผลข้อมูลใดบ้าง โดยกำหนดให้เป็นระบบสารสนเทศ เป้าหมาย (Target Computerised System)

จากนั้นเป็นการทำความเข้าใจต่อระบบคอมพิวเตอร์ที่มีอยู่ในปัจจุบัน (Existing Computerised System) ว่า ระบบสารสนเทศ (Information System) ระบบงาน (Application) เทคโนโลยี (Technology) และโครงสร้างองค์กรและบุคลากร (Organisation Structure and Human Resource) มีลักษณะและรายละเอียดอย่างไร

จากนั้นก็เริ่มดำเนินการวิเคราะห์ความแตกต่าง (Gap Analysis) ระหว่างระบบเป้าหมายกับระบบปัจจุบัน ว่ามีความแตกต่างกันอย่างไร เพื่อนำมากำหนดเป็นกิจกรรมเพื่อแปลงจากระบบปัจจุบันเป็นระบบที่ควรเป็นในอนาคต ซึ่งอาจเป็นกิจกรรมในการพัฒนาระบบงานใหม่ การติดตั้งเทคโนโลยีใหม่ หรือการพัฒนาศักยภาพของบุคลากร เป็นต้น

สุดท้ายเป็นการรวบรวมกิจกรรมต่าง ๆ มาจัดทำเป็นแผนการดำเนินงานด้านสารสนเทศ ซึ่งควรครอบคลุมแผนการดำเนินการด้านระบบสารสนเทศ ระบบงาน เทคโนโลยี และโครงสร้างองค์กรและบุคลากร อย่างครบถ้วน

6.2.3 การอนุมัติ การสื่อสารและควบคุมแผนงานสารสนเทศ

เมื่อจัดทำแผนเสร็จเรียบร้อยแล้ว ควรจัดให้มีการอนุมัติแผนอย่างเป็นทางการ ซึ่งในขั้นตอนการอนุมัตินั้นควรประกอบด้วยความเห็นชอบของทั้งผู้บริหารระดับสูง และผู้บริหารสารสนเทศ ซึ่งในกรณีที่องค์กรมีคณะกรรมการสารสนเทศ ก็ควรให้คณะกรรมการดังกล่าวเป็นผู้อนุมัติแผน แต่ถ้าไม่มีคณะกรรมการฯ ก็ควรให้ผู้บริหารระดับสูงเป็นผู้อนุมัติ

ลำดับถัดมาคือการสื่อสารเพื่อทำความเข้าใจกับผู้ที่เกี่ยวข้องกับการดำเนินการตามแผนฯ ซึ่งรวมทั้งผู้บริหารสายงานสารสนเทศต่าง ๆ และผู้บริหารสายงานธุรกิจที่เกี่ยวข้อง

ในระหว่างการดำเนินการตามแผนนั้น ก็จะต้องจัดให้มีการติดตามความคืบหน้าและจัดทำสรุปการดำเนินการเพื่อรายงานให้ผู้บริหารในแต่ละระดับ เช่นผู้บริหารสารสนเทศและผู้บริหารระดับสูงเพื่อติดตามให้การดำเนินการเป็นไปตามแผนงานที่กำหนด

6.2.4 การติดตามการดำเนินงานตามแผนงานสารสนเทศ

ควรมีการติดตามการดำเนินงานตามแผนอย่างสม่ำเสมอ และประเมินเปรียบเทียบผลสำเร็จของแผนตามเป้าหมายที่กำหนดไว้ สำหรับในส่วนที่การดำเนินงานไม่เป็นไปตามแผนก็ควรมีการดำเนินการแก้ไขหรือปรับปรุง หรือระบุสาเหตุที่ชัดเจน

6.3 การควบคุมด้านการจัดโครงสร้างงานสารสนเทศ

การควบคุมด้านการจัดโครงสร้างงานสารสนเทศมีวัตถุประสงค์ของการควบคุมเพื่อให้มั่นใจว่าสายงานสารสนเทศอยู่ในตำแหน่งที่เหมาะสมและเอื้อให้เกิดการดำเนินการด้านสารสนเทศที่มีประสิทธิภาพและประสิทธิผลในการสนับสนุนการดำเนินการทางธุรกิจ และมีการแบ่งแยกงานสารสนเทศที่เหมาะสมและเอื้อให้เกิดการควบคุมภายในที่ดี

เพื่อบรรลุถึงวัตถุประสงค์ด้านการควบคุมดังกล่าวข้างต้น ควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

6.3.1 การจัดวางตำแหน่งของสายงานสารสนเทศ

6.3.2 การแบ่งแยกงานสารสนเทศ

6.3.3 งานที่ควรพิจารณาให้อยู่นอกฝ่ายสารสนเทศ

6.3.1 การจัดวางตำแหน่งของสายงานสารสนเทศ

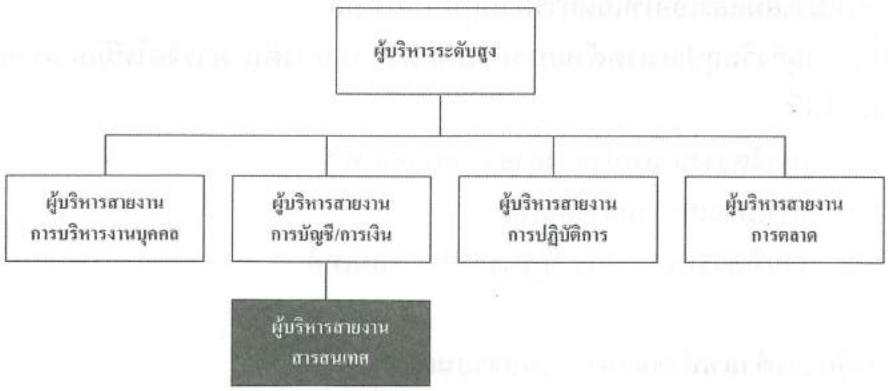
ในการจัดวางตำแหน่งงานด้านสารสนเทศนั้น สิ่งที่ควรคำนึงถึงเป็นลำดับแรกก็คือลักษณะการใช้งานสารสนเทศขององค์กร กล่าวคือถ้าองค์กรใช้ระบบสารสนเทศ ในกระบวนการ

ทำงานแทบทุกกระบวนการทำงาน และทุกสายงาน ก็ควรจัดวางตำแหน่งงานสารสนเทศให้อยู่ในระดับที่ค่อนข้างสูงในองค์กร เช่นจัดให้อยู่ในระดับเดียวกันกับผู้บริหารสายงานอื่น ๆ และขึ้นตรงกับผู้บริหารระดับสูง ดังแสดงไว้ในภาพ 3 - 2 ตัวอย่างของผังโครงสร้างองค์กรแสดงตำแหน่งของสายงานสารสนเทศ กรณีขึ้นตรงกับผู้บริหารระดับสูง

ภาพ 3-2 ตัวอย่างของผังโครงสร้างองค์กรแสดงตำแหน่งของสายงานสารสนเทศ กรณีขึ้นตรงกับผู้บริหารระดับสูง

ทั้งนี้เพื่อเอื้อให้มีการบริการด้านสารสนเทศที่เท่าเทียมกัน และทำให้การประสานงานระหว่างผู้บริหารสายงานสารสนเทศ และผู้บริหารสายงานอื่น ๆ เป็นไปอย่างมีประสิทธิภาพ

แต่ถ้าลักษณะการใช้ระบบสารสนเทศ ขององค์กรเป็นการใช้งานเฉพาะด้าน เช่นใช้ระบบสารสนเทศ เฉพาะงานด้านการบัญชีการเงิน ถ้าจัดให้งานสารสนเทศอยู่ภายใต้การกำกับดูแลของผู้บริหารงานด้านการบัญชีการเงิน ตามภาพ 3 - 3 ก็อาจยังคงการบริหารงานด้านสารสนเทศได้อย่างมีประสิทธิภาพตรงกับความต้องการใช้ระบบสารสนเทศ ขององค์กร



ภาพ 3-3 ตัวอย่างของผังโครงสร้างองค์กรแสดงตำแหน่งของสายงานสารสนเทศ กรณีขึ้นตรงกับผู้บริหารสายงานการบัญชีการเงิน

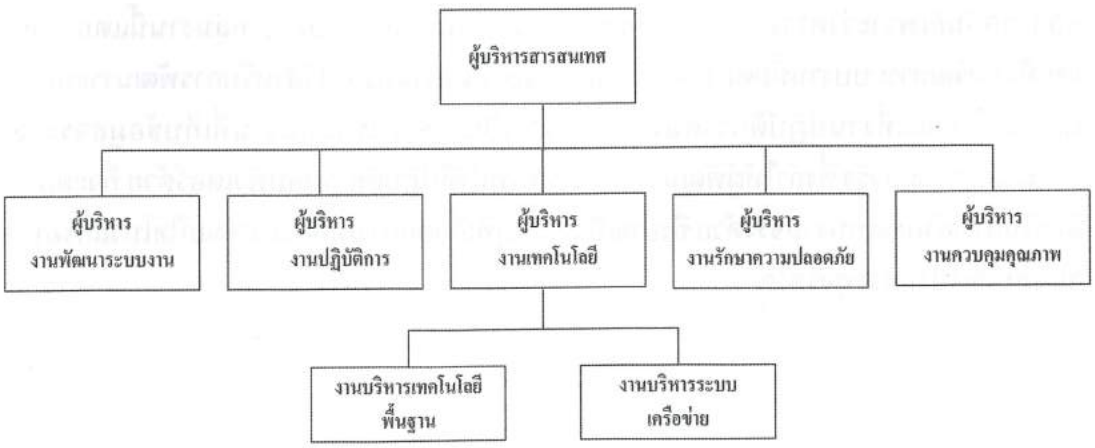
สำหรับองค์กรที่ใช้ระบบสารสนเทศ เป็นกลยุทธ์สำคัญในการดำเนินธุรกิจ โดยเฉพาะอย่างยิ่งเป็นกลไกสำคัญในการแข่งขัน อาจจำเป็นต้องมีการจัดตั้งคณะกรรมการด้านสารสนเทศ (IT Steering Committee) ซึ่งประกอบด้วยผู้บริหารระดับสูงและผู้บริหารสายงานต่าง ๆ เพื่อทำหน้าที่กำหนดแนวทางในการจัดการด้านสารสนเทศ และกำกับดูแลให้การใช้ระบบสารสนเทศสอดคล้องกับกลยุทธ์ทางธุรกิจมากขึ้น อีกทั้งเอื้อให้เกิดการประสานงานระหว่างผู้บริหารสารสนเทศและผู้บริหารสายงานต่าง ๆ มีประสิทธิภาพยิ่งขึ้น

6.3.2 การแบ่งแยกงานสารสนเทศ

หลักการการควบคุมที่ดีด้านการจัดโครงสร้างองค์กรก็คือการแบ่งแยกหน้าที่งานสารสนเทศ ซึ่งงานสารสนเทศในองค์กรส่วนใหญ่ ประกอบด้วย

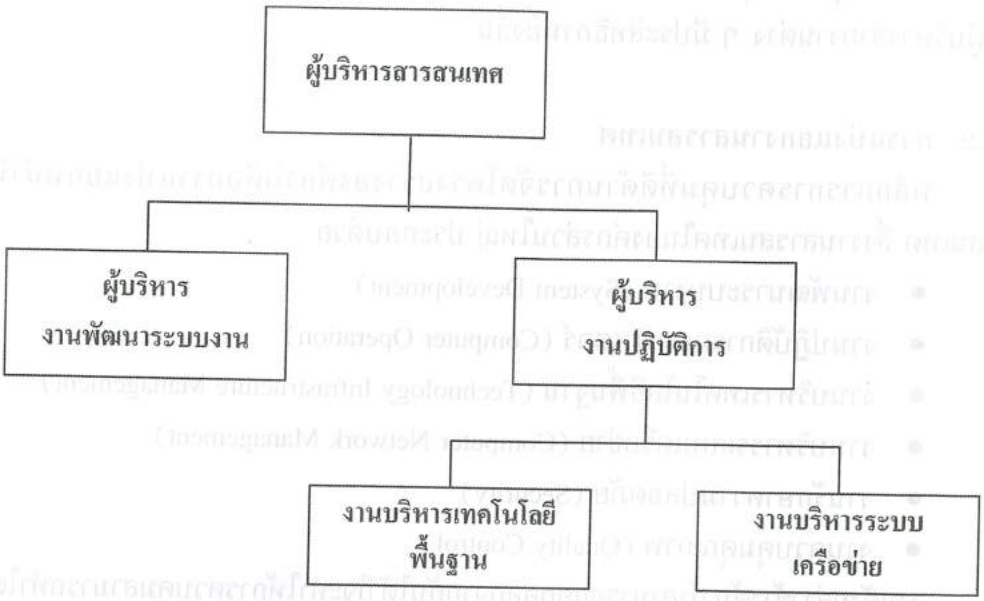
- งานพัฒนาระบบงาน (System Development)
- งานปฏิบัติการคอมพิวเตอร์ (Computer Operation)
- งานบริหารเทคโนโลยีพื้นฐาน (Technology Infrastructure Management)
- งานบริหารระบบเครือข่าย (Computer Network Management)
- งานรักษาความปลอดภัย (Security)
- งานควบคุมคุณภาพ (Quality Control)

งานดังกล่าวข้างต้น ถ้าสามารถแยกออกจากกันได้ ก็จะทำให้การควบคุมสามารถทำได้อย่างมีประสิทธิภาพและประสิทธิผลมากขึ้น แต่ในความเป็นจริงคงจะแบ่งแยกได้เฉพาะองค์กรที่มีขนาดใหญ่ หรือมีการลงทุนด้านระบบสารสนเทศ ที่สูงเท่านั้น ซึ่งสามารถแสดงเป็นผังโครงสร้างองค์กรดังแสดงในภาพ 3 - 4



ภาพ 3-4 ตัวอย่างผังโครงสร้างองค์กรแสดงการแบ่งแยกหน้าที่งานสารสนเทศ สำหรับองค์กรขนาดใหญ่

สำหรับองค์กรที่มีขนาดเล็กและมีการใช้ระบบสารสนเทศ ในปริมาณที่น้อยจะไม่สามารถแบ่งแยกงานต่าง ๆ เหล่านี้ได้ทุกงาน แต่ก็ยังมีความจำเป็นที่จะต้องแบ่งแยกหน้าที่สำหรับงานที่สำคัญบางงาน เช่นงานพัฒนาระบบงาน และงานด้านการปฏิบัติการคอมพิวเตอร์ ส่วนงานด้านอื่น ๆ นั้นอาจจะพิจารณาให้อยู่ในส่วนใดส่วนหนึ่งภายในสองงานดังแสดงในภาพ 3 - 5



ภาพ 3-5 ตัวอย่าง ผังโครงสร้างองค์กรแสดงการแบ่งแยกหน้าที่งานสารสนเทศสำหรับองค์กรขนาดเล็ก

ความจำเป็นที่จะต้องแยกงานพัฒนาระบบงานและงานปฏิบัติการคอมพิวเตอร์ออกจากกันก็เพราะว่าความต้องการในการใช้ระบบคอมพิวเตอร์ของ 2 กลุ่มงานนี้แตกต่างกัน โดยที่งานพัฒนาระบบงานนั้นต้องการใช้ระบบคอมพิวเตอร์ที่เตรียมไว้สำหรับการพัฒนาระบบงานเท่านั้น ในขณะที่งานปฏิบัติการคอมพิวเตอร์จำเป็นจะต้องใช้ระบบงานที่เก็บข้อมูลจริงและประมวลผลข้อมูลจริง ซึ่งถ้าให้ผู้พัฒนาระบบงานทำหน้าที่ปฏิบัติการคอมพิวเตอร์ด้วย ก็จะต้องให้สิทธิในการเข้าถึงระบบงานจริงด้วย ซึ่งอาจเป็นสาเหตุที่เอื้อต่อการเปลี่ยนแปลงแก้ไขโปรแกรมหรือข้อมูลที่ส่อไปในทางทุจริตได้

6.3.3 งานที่ควรพิจารณาให้อยู่นอกฝ่ายสารสนเทศ

งานที่สำคัญ 2 งานที่ในปัจจุบันมีแนวโน้มที่จะจัดวางตำแหน่งไว้ภายนอกสายงานสารสนเทศ คืองานด้านการรักษาความปลอดภัยระบบสารสนเทศ และงานด้านการควบคุมคุณภาพงานสารสนเทศ

สำหรับงานด้านการรักษาความปลอดภัยระบบสารสนเทศ นั้น ถ้าจัดให้อยู่ภายนอกสายงานสารสนเทศจะทำให้การรักษาความปลอดภัยเข้มแข็งมากขึ้น โดยที่ผู้บริหารความปลอดภัยระบบสารสนเทศ ไม่ได้ขึ้นตรงกับผู้บริหารสายงานสารสนเทศ ดังนั้นการดำเนินกิจกรรมต่าง ๆ ในงานสารสนเทศจะได้รับการควบคุมดูแลด้านความปลอดภัยที่เป็นอิสระมากขึ้น ทำให้การดำเนินการเป็นไปตามนโยบาย และหลักการรักษาความปลอดภัยมากขึ้น ซึ่งจะจัดไว้ในส่วนใดขององค์กรนั้นขึ้นอยู่กับความเหมาะสมของแต่ละองค์กร

สำหรับงานด้านการควบคุมคุณภาพ ซึ่งประกอบด้วยการควบคุมคุณภาพของระบบงานสารสนเทศที่พัฒนาโดยสายงานพัฒนาระบบสารสนเทศ และคุณภาพของการให้บริการต่าง ๆ ด้านสารสนเทศต่อผู้ใช้งานในองค์กร ซึ่งถ้างานควบคุมคุณภาพยังอยู่ภายใต้การบริหารงานของฝ่ายสารสนเทศ อาจทำให้การควบคุมคุณภาพขาดความเป็นอิสระ ซึ่งมีผลต่อประสิทธิภาพในการควบคุมคุณภาพของงานสารสนเทศดังกล่าว

7. การควบคุมด้านการพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ

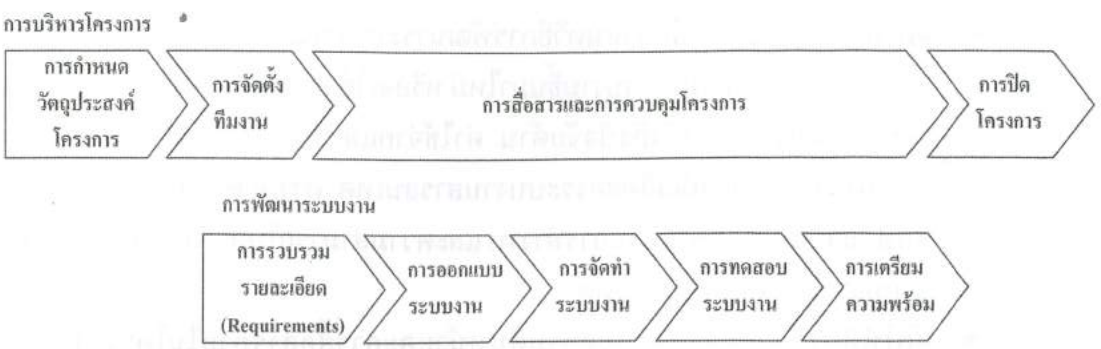
ระบบงานสารสนเทศ (Application System) เป็นกลไกหลักในการประมวลผลข้อมูลเพื่อใช้ในกิจกรรมต่าง ๆ ขององค์กร ซึ่งการทำงานของระบบสารสนเทศจะต้องมีความถูกต้องและตรงกับความต้องการขององค์กร และกระบวนงานด้านสารสนเทศที่เกี่ยวข้องกับความถูกต้องและความสอดคล้องกับความต้องการขององค์กรประกอบด้วย กระบวนการพัฒนาระบบงานสารสนเทศและกระบวนการแก้ไขเปลี่ยนแปลงระบบงานสารสนเทศ ซึ่งมีวัตถุประสงค์และแนวทางการควบคุมในกระบวนงานดังกล่าว ดังต่อไปนี้

7.1 การควบคุมด้านการพัฒนาระบบงานสารสนเทศ

การควบคุมด้านการพัฒนาระบบงานสารสนเทศมีวัตถุประสงค์ดังนี้

- เพื่อให้มั่นใจว่าระบบงานที่พัฒนาขึ้นมาใหม่มีความสอดคล้องกับความต้องการทางธุรกิจ และสอดคล้องกับวัตถุประสงค์ของการพัฒนาระบบงาน
- เพื่อให้มั่นใจว่ามีการทดสอบระบบงานใหม่อย่างเหมาะสมเพียงพอ เพื่อให้ระบบงานใหม่ปราศจากข้อบกพร่องก่อนนำระบบงานมาใช้งาน
- เพื่อให้มั่นใจว่าการบริหารโครงการเป็นไปอย่างมีประสิทธิภาพ โดยสามารถดำเนินการเสร็จภายในระยะเวลาที่กำหนด และภายในงบประมาณที่จัดเตรียมไว้

การควบคุมที่เกี่ยวข้องกับการพัฒนาระบบงานสารสนเทศประกอบด้วยกระบวนการที่สำคัญ 2 กระบวนการคือ การบริหารโครงการ และการพัฒนาระบบงาน ซึ่งในแต่ละส่วนมีความสำคัญไม่น้อยไปกว่ากันโดยที่การบริหารโครงการมุ่งเน้นด้านการควบคุมโครงการให้เป็นไปตามวัตถุประสงค์ของโครงการ และให้โครงการแล้วเสร็จภายในระยะเวลาที่กำหนด ส่วนกระบวนการพัฒนาระบบงานมุ่งเน้นที่รายละเอียดการพัฒนาระบบงานซึ่งเริ่มตั้งแต่การกำหนดวัตถุประสงค์ของโครงการ การรวบรวมรายละเอียดความต้องการ การออกแบบและจัดทำระบบงาน การทดสอบระบบงาน และการเตรียมความพร้อมก่อนนำมาใช้งาน ซึ่งกระบวนการทำงานโดยรวมแสดงไว้ในภาพ 3 - 6



ภาพ 3-6 ขั้นตอนของการพัฒนาระบบงานสารสนเทศ

ดังนั้นการควบคุมด้านการพัฒนาระบบงานสารสนเทศ ประกอบด้วยการควบคุม 2 ส่วน ดังนี้

7.1.1 การควบคุมในส่วนของการบริหารโครงการพัฒนาระบบงานสารสนเทศ

7.1.2 การควบคุมในขั้นตอนการพัฒนาระบบงานสารสนเทศ

7.1.1 การควบคุมในส่วนของการบริหารโครงการพัฒนาระบบงานสารสนเทศ

ในส่วนของการควบคุมการบริหารโครงการพัฒนาระบบงานสารสนเทศนั้น ควรจัดให้มีการควบคุมดังต่อไปนี้

- มีการกำหนดวัตถุประสงค์ของการพัฒนาระบบงานสารสนเทศที่ชัดเจน และสอดคล้องกับวัตถุประสงค์และความต้องการทางธุรกิจ ซึ่งจะต้องมีการบันทึกและสื่อสารทำความเข้าใจต่อวัตถุประสงค์ให้กับทุกคนที่เกี่ยวข้องกับการพัฒนาระบบงานนั้น ๆ
- ทีมงานพัฒนาระบบงานสารสนเทศควรประกอบด้วยบุคลากรที่เป็นตัวแทนจากหน่วยงานที่เกี่ยวข้องอย่างครบถ้วน เช่นถ้าเป็นการพัฒนาระบบงานสารสนเทศนั้นควรจะต้องมีผู้แทนจากหน่วยงานฝ่ายผู้ใช้งาน และตัวแทนจากหน่วยงานสารสนเทศผสมผสานกัน
- ผู้ที่ทำหน้าที่ผู้จัดการโครงการจำเป็นต้องมีทักษะในการบริหารโครงการ และควรเป็นผู้ที่มีความรู้และความสามารถที่เหมาะสมในการพัฒนาระบบงานให้บรรลุถึงวัตถุประสงค์ที่กำหนดไว้ ได้อย่างมีประสิทธิภาพ
- จัดให้มีโครงสร้างของทีมงานพัฒนาระบบงานที่เหมาะสม ซึ่งประกอบด้วย ผู้จัดการโครงการ เจ้าของโครงการ ผู้สนับสนุนโครงการ ตัวแทนจากสายงานในส่วนของผู้ใช้งาน และตัวแทนจากสายงานสารสนเทศ

- จัดให้มีการวิเคราะห์เพื่อกำหนดวิธีการพัฒนาระบบงานสารสนเทศที่เหมาะสม เช่น การเลือกระหว่างพัฒนาระบบงานขึ้นมาใหม่ หรือจะใช้ซอฟต์แวร์สำเร็จรูปเป็นพื้นฐานในการพัฒนา โดยคำนึงถึงปัจจัยด้าน ค่าใช้จ่ายและระยะเวลาในการพัฒนา และนำมาใช้งานความน่าเชื่อถือของระบบงานสารสนเทศ ความยืดหยุ่นในการปรับปรุงซอฟต์แวร์ให้เข้ากับกระบวนการทำงาน และความสามารถในการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศในอนาคต
- จัดให้มีกระบวนการติดตามความคืบหน้าและการสื่อสารภายในโครงการอย่างสม่ำเสมอ ผ่านการประชุมโครงการและการรายงานความคืบหน้า และมีกระบวนการในการจัดการปัญหาที่ชัดเจน ตั้งแต่การบันทึกปัญหาอุปสรรคต่าง ๆ ที่เกิดขึ้น การดำเนินการแก้ไข และการสรุปการแก้ไข

7.1.2 การควบคุมในขั้นตอนการพัฒนาระบบงานสารสนเทศ

ในส่วนของการควบคุมในขั้นตอนการพัฒนาระบบงานสารสนเทศนั้น ควรจัดให้มีการควบคุม ดังต่อไปนี้

7.1.2.1 จัดให้มีการควบคุมในแต่ละขั้นตอนของการพัฒนาระบบงานสารสนเทศ ดังนี้

1) **ขั้นตอนการรวบรวมรายละเอียด (Analysis)** ขั้นตอนนี้เป็นขั้นตอนในการรวบรวมความต้องการของระบบงานสารสนเทศใหม่ (System Requirements) ซึ่งการควบคุมที่สำคัญคือการจัดให้มีกลไกในการรวบรวมความต้องการของระบบที่ชัดเจน และต้องครอบคลุมความต้องการทั้งทางธุรกิจ และความต้องการด้านการควบคุม โดยควรที่จะจัดให้มีการสอบทานความต้องการดังกล่าวเพื่อให้มั่นใจว่าความต้องการนั้น ๆ สอดคล้องกับวัตถุประสงค์ของระบบงานใหม่
2) **ขั้นตอนการออกแบบระบบงาน (Design)** ในขั้นตอนนี้เป็นการนำความต้องการของระบบงานสารสนเทศใหม่มาออกแบบเป็นระบบสารสนเทศ ซึ่งการควบคุมที่จำเป็นต้องมีก็คือการสอบทานเพื่อให้มั่นใจว่าความต้องการที่รวบรวมไว้ในขั้นตอนก่อนหน้านี้ ได้รับการออกแบบอย่างถูกต้อง และครอบคลุมทั้งความต้องการทางธุรกิจและความต้องการด้านการควบคุม
3) **ขั้นตอนการจัดทำระบบงาน (Construction)** เป็นขั้นตอนการดำเนินการสร้างระบบงานสารสนเทศ ซึ่งในขั้นตอนนี้การควบคุมที่สำคัญคือการทดสอบระบบงานสารสนเทศที่จัดทำขึ้นมาใหม่ เพื่อให้ความมั่นใจว่า ความต้องการที่กำหนดโดย

ผู้ใช้งานนั้น นำมาออกแบบและสร้างอย่างครบถ้วนและถูกต้อง ซึ่งการสร้างระบบงานสารสนเทศอาจเป็นการสร้างขึ้นมาใหม่ทั้งหมด หรือเป็นการนำซอฟต์แวร์สำเร็จรูปมาดัดแปลงเพื่อให้สอดคล้องกับแบบที่ออกไว้ก็ได้

4) **ขั้นตอนการทดสอบระบบงาน (Testing)** ขั้นตอนนี้เป็นขั้นตอนที่สำคัญ ประกอบด้วยการทดสอบโดยผู้สร้างระบบงานสารสนเทศเพื่อให้มั่นใจว่าระบบงานสารสนเทศทำงานอย่างถูกต้อง และการทดสอบโดยผู้ใช้งาน เพื่อตรวจรับและรับรองว่าระบบงานทำงานได้ตรงกับความต้องการของผู้ใช้งาน

5) **ขั้นตอนการเตรียมความพร้อมเพื่อนำมาใช้งาน (Implementation)** เป็นขั้นตอนการนำระบบงานสารสนเทศมาใช้งาน โดยมีการควบคุมที่สำคัญคือ ต้องมีการอนุมัติการโอนย้ายระบบงานสารสนเทศไปใช้งาน หลังจากผลการทดสอบขั้นสุดท้ายเป็นที่พอใจของเจ้าของระบบงานสารสนเทศแล้ว การโอนย้ายระบบงานสารสนเทศ ก็ควรทำภายใต้การควบคุมที่เข้มงวดเพื่อให้มั่นใจว่าโปรแกรมที่นำไปใช้งานเป็นโปรแกรมเดียวกันกับโปรแกรมที่ได้รับการทดสอบ และต้องมีการจัดทำเอกสารประกอบระบบงานอย่างครบถ้วนสมบูรณ์ก่อนนำระบบมาใช้งานจริง และจัดให้มีการสอบทานเพื่อทำให้มั่นใจว่าความต้องการทั้งทางด้านธุรกิจและด้านการควบคุมนั้น ได้มีการนำมาปฏิบัติจริง นอกจากนี้ยังเป็นการเตรียมความพร้อมของระบบ เช่นการโอนถ่ายข้อมูลจากระบบงานสารสนเทศเดิม หรือการเตรียมข้อมูลตั้งต้น รวมทั้งการฝึกอบรมผู้ใช้งาน

7.1.2.2 มีการจัดทำเอกสารประกอบระบบงานอย่างครบถ้วน ซึ่งเอกสารควรประกอบด้วย

- คู่มือประกอบระบบงานสารสนเทศ (Information System Manual) ซึ่งเป็นเอกสารแสดงรายละเอียดทางเทคนิคของระบบงานสารสนเทศ ซึ่งมีไว้เพื่อประกอบการพิจารณาปรับปรุงหรือเปลี่ยนแปลงระบบในอนาคต
- คู่มือปฏิบัติงาน (Operation Manual) ซึ่งเป็นเอกสารแสดงรายละเอียดขั้นตอนการปฏิบัติงานต่าง ๆ ของระบบงานสารสนเทศ ซึ่งส่วนใหญ่ใช้โดยผู้ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) ในการเปิดปิดระบบงานสารสนเทศ ประมวลผลงานสิ้นวัน สำรองข้อมูลเป็นต้น
- คู่มือการใช้งาน (User Manual) เป็นเอกสารแสดงรายละเอียดการใช้ระบบงานสารสนเทศของผู้ใช้งาน ซึ่งใช้สำหรับศึกษาการทำงานของระบบงานสารสนเทศ เช่น การทำงานของแต่ละหน้าจอ หรือการใช้ฟังก์ชั่นต่าง ๆ ที่มีมากับระบบ

- เอกสารแสดงขั้นตอนการปฏิบัติงาน (User Procedure) ที่ผู้ใช้งานจะต้องปฏิบัติ เช่นก่อนการนำข้อมูลเข้าสู่ระบบจะต้องมีการอนุมัติเอกสารก่อน หรือ ระบุว่าใครเป็นผู้นำเข้าข้อมูล และใครเป็นผู้อนุมัติ เป็นต้น

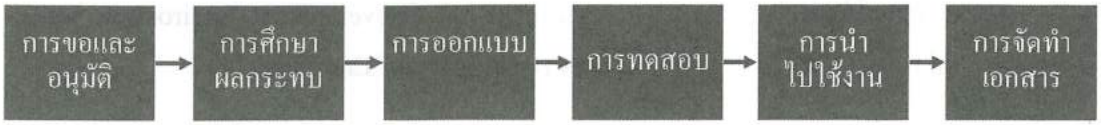
7.1.2.3 เพื่อป้องกันการหยุดชะงักของการใช้ระบบสารสนเทศ ประกอบการดำเนินธุรกิจ ก่อนที่จะนำระบบงานสารสนเทศใหม่มาใช้งาน ควรพิจารณาวิธีการที่เหมาะสมเพื่อป้องกันเหตุการณ์ข้างต้น ดังมีลักษณะของแต่ละวิธีการนำระบบมาใช้งาน ดังนี้

- การนำระบบงานใหม่มาใช้ทดแทนระบบงานสารสนเทศเก่าโดยทันที (Cut Off Implementation) ซึ่งวิธีนี้เป็นการยกเลิกการใช้ระบบงานเก่าทันทีหลังจากระบบงานสารสนเทศใหม่เริ่มใช้งานแล้ว ซึ่งวิธีนี้มีความเสี่ยงค่อนข้างสูง แต่ค่าใช้จ่ายจะน้อยที่สุด
- การใช้ระบบงานสารสนเทศเก่าพร้อมกับระบบงานใหม่ในระยะเริ่มแรก (Parallel Implementation) เป็นการใช้ระบบงานสารสนเทศเก่าพร้อมไปกับการใช้ระบบงานสารสนเทศใหม่ ไประยะเวลาหนึ่งจนกระทั่งมั่นใจว่าระบบงานสารสนเทศใหม่มีความถูกต้อง จึงยกเลิกการใช้ระบบงานสารสนเทศเก่า วิธีนี้เป็นวิธีที่ค่อนข้างปลอดภัยสูง แต่จะต้องมีการทำงานและค่าใช้จ่ายมากกว่าเดิม
- การนำระบบงานสารสนเทศใหม่มาใช้งานทีละส่วน (Phase Implementation) เช่น เริ่มจากการใช้ส่วนที่ระบบบัญชีก่อน จึงเริ่มนำระบบงานสารสนเทศอื่น ๆ มาใช้งานตามลำดับ
- การทดลองใช้ระบบงานสารสนเทศใหม่กับหน่วยงานทดลอง (Pilot Implementation) โดยเริ่มทดลองใช้งานระบบงานสารสนเทศใหม่กับหน่วยงานย่อยก่อน จนกระทั่งมั่นใจว่าระบบงานสารสนเทศใหม่ทำงานได้อย่างถูกต้อง จึงเริ่มทยอยใช้ระบบงานสารสนเทศใหม่นี้กับหน่วยงานอื่น ๆ ทั่วทั้งองค์กร

7.2 การควบคุมด้านการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ

การควบคุมด้านการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศมีวัตถุประสงค์ เพื่อให้มั่นใจว่าระบบงานที่เปลี่ยนแปลงแก้ไขสอดคล้องกับความต้องการทางธุรกิจ และสอดคล้องกับวัตถุประสงค์ของการพัฒนาระบบงานสารสนเทศ และให้มั่นใจว่ามีการทดสอบระบบงานสารสนเทศใหม่อย่างเหมาะสมเพียงพอ เพื่อให้ระบบงานสารสนเทศใหม่ปราศจากข้อบกพร่องก่อนนำระบบงานสารสนเทศมาใช้งาน

การควบคุมการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศนั้นมีความสำคัญไม่น้อยกว่าการควบคุมในส่วนของการพัฒนาระบบงานสารสนเทศ เพราะการเปลี่ยนแปลงมีผลทำให้เกิดความเสี่ยงเกี่ยวกับความถูกต้องของระบบงานสารสนเทศและข้อมูลที่ใช้ในการปฏิบัติงาน โดยเฉพาะอย่างยิ่งระบบงานสารสนเทศที่มีการเปลี่ยนแปลงแก้ไขบ่อยครั้ง ซึ่งการควบคุมในขั้นตอนต่าง ๆ ของการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศมีความคล้ายคลึงกันกับการควบคุมด้านการพัฒนาระบบงานสารสนเทศ หากแต่ว่าขนาดของโครงการเป็นขนาดที่เล็กกว่าการพัฒนาระบบงานสารสนเทศ ขั้นตอนการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ แสดงไว้ในภาพ 3 - 7



ภาพ 3-7 ขั้นตอนการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ

เพื่อบรรลุถึงวัตถุประสงค์ด้านการควบคุมดังกล่าวข้างต้น ควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

- จะต้องมีการขอและอนุมัติการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ อย่างเป็นทางการ ซึ่งโดยส่วนใหญ่ใช้ใบคำขอการเปลี่ยนแปลงที่เป็นแบบฟอร์มที่เตรียมไว้ล่วงหน้า โดยมีการบันทึกรายละเอียดอย่างชัดเจน เช่นผู้ขอ ผู้อนุมัติ วันที่ขอ วันที่ต้องการให้แล้วเสร็จ เหตุผลของการแก้ไข เป็นต้น โดยผู้บริหารที่ได้รับการแต่งตั้งเป็นเจ้าของระบบงานเป็นผู้อนุมัติการเปลี่ยนแปลง
- มีการศึกษาความเป็นไปได้ทางเทคนิค ความคุ้มค่าของการเปลี่ยนแปลง และผลกระทบที่อาจเกิดขึ้น ก่อนเริ่มลงมือเปลี่ยนแปลงแก้ไข
- การวิเคราะห์และออกแบบ ควรดำเนินการอย่างสอดคล้องกับหลักการการควบคุมการพัฒนาระบบงานสารสนเทศที่ดี ตามที่อธิบายไว้ในส่วนของการควบคุมการพัฒนาระบบงานสารสนเทศ
- การเปลี่ยนแปลงแก้ไขจะต้องได้รับการทดสอบอย่างเพียงพอ ก่อนที่จะนำระบบงานสารสนเทศหรือโปรแกรมที่แก้ไขไปใช้งาน โดยที่การทดสอบขั้นสุดท้ายก่อนการโอนย้ายระบบสารสนเทศไปใช้งาน ต้องทำโดยตัวแทนของเจ้าของระบบงานสารสนเทศ
- การโอนย้ายระบบงานสารสนเทศหรือโปรแกรมที่แก้ไขไปใช้งานจะต้องมีการควบคุมเพื่อให้มั่นใจว่า ระบบงานสารสนเทศที่ย้ายไปใช้งานนั้นเป็นระบบงานสารสนเทศ

เดียวกันกับระบบงานสารสนเทศที่ได้รับการทดสอบแล้ว ถ้าเป็นการเปลี่ยนแปลงแก้ไขที่อาจมีผลกระทบกับการทำงานอย่างมีนัยสำคัญ ควรพิจารณาเลือกวิธีการนำระบบงานสารสนเทศใหม่มาใช้งานที่เหมาะสม ตามที่อธิบายไว้ในส่วนของการควบคุมการพัฒนาระบบงานสารสนเทศ

- มีการปรับปรุงแก้ไขเอกสารประกอบระบบงานสารสนเทศทั้งหมดให้สะท้อนถึงการเปลี่ยนแปลงแก้ไข

และเพื่อการจัดให้มีการควบคุมที่ดีในกระบวนการการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ ระบบคอมพิวเตอร์ขององค์กรควรจะต้องมีอย่างน้อย 2 ส่วน คือส่วนที่เตรียมไว้สำหรับการพัฒนาและเปลี่ยนแปลง (Development Environment) และส่วนที่เตรียมไว้สำหรับการใช้งานจริง (Production Environment)

8. การควบคุมด้านการรักษาความปลอดภัยระบบสารสนเทศ

ความเสี่ยงที่สำคัญในการใช้ระบบสารสนเทศ ก็คือความเสี่ยงด้านความปลอดภัยของข้อมูลและระบบสารสนเทศ ดังนั้นผู้บริหารองค์กรจะต้องจัดให้มีกลไกการรักษาความปลอดภัยระบบสารสนเทศที่รัดกุม โดยการควบคุมด้านความปลอดภัยระบบสารสนเทศนั้นเกี่ยวข้องกับการใช้งานของผู้ใช้งานทั้งองค์กร ดังนั้นการควบคุมควรประกอบด้วยในส่วนของการบริหารจัดการความปลอดภัยโดยรวม การรักษาความปลอดภัยทางกายภาพ (Physical Security) และการรักษาความปลอดภัยเชิงตรรกะ (Logical Security) ซึ่งกลไกการควบควบคุมดังกล่าวมีวัตถุประสงค์และแนวทางการควบคุมในกระบวนงานดังกล่าว ดังต่อไปนี้

8.1 การควบคุมด้านการบริหารและจัดการการรักษาความปลอดภัยระบบสารสนเทศ

การควบคุมด้านการบริหารและจัดการการรักษาความปลอดภัยระบบสารสนเทศมีวัตถุประสงค์เพื่อ

- ให้มั่นใจว่าการใช้ระบบคอมพิวเตอร์เป็นไปตามมาตรฐานการรักษาความปลอดภัยที่ดี
- ให้มั่นใจว่าบุคลากรมีความรู้ความเข้าใจเกี่ยวกับการรักษาความปลอดภัยอย่างเพียงพอ และสม่ำเสมอ
- ให้มั่นใจว่าการจัดการด้านความปลอดภัย เช่นการให้หรือเปลี่ยนแปลงสิทธิในการใช้ระบบคอมพิวเตอร์ สอดคล้องกับความต้องการในการใช้ระบบคอมพิวเตอร์โดยรวมขององค์กร
- ให้มั่นใจว่ามีการติดตามสอบทานเหตุการณ์ที่เกี่ยวกับการรักษาความปลอดภัยอย่างสม่ำเสมอ และมีการรายงานเหตุการณ์ต่าง ๆ ให้กับผู้รับผิดชอบอย่างทันท่วงทีและสม่ำเสมอ

เพื่อบรรลุถึงวัตถุประสงค์ของการควบคุมข้างต้น ผู้บริหารองค์กรควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

8.1.1 การจัดทำและดำเนินการด้านนโยบายการรักษาความปลอดภัยระบบสารสนเทศ

8.1.2 การจัดทำและปฏิบัติงานตามระเบียบปฏิบัติด้านการรักษาความปลอดภัยระบบสารสนเทศ

8.1.3 การสร้างความเข้าใจและจิตสำนึกด้านความปลอดภัยระบบสารสนเทศ

8.1.1 การจัดทำและดำเนินการด้านนโยบายการรักษาความปลอดภัยระบบสารสนเทศ

การบริหารความปลอดภัยระบบสารสนเทศที่ดีเริ่มจากการที่ผู้บริหารจะต้องจัดให้มีนโยบายการรักษาความปลอดภัยระบบสารสนเทศ เพื่อเป็นแนวทางในการดำเนินการและปฏิบัติงานของบุคลากรโดยรวมขององค์กร ทั้งผู้ที่รับผิดชอบโดยตรงด้านการรักษาความปลอดภัยและผู้ใช้งานทั่วไป

นโยบายด้านการรักษาความปลอดภัยที่ดี ควรประกอบด้วย

- การกำหนดบทบาทหน้าที่และความรับผิดชอบด้านการรักษาความปลอดภัยของผู้ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ประกอบด้วย ผู้บริหารสูงสุด ผู้บริหารสายงานต่าง ๆ ผู้ใช้งานทั่วไป ผู้บริหารสารสนเทศ เจ้าหน้าที่ด้านสารสนเทศต่าง ๆ ผู้บริหารและเจ้าหน้าที่ด้านความปลอดภัยระบบสารสนเทศ และผู้ตรวจสอบสารสนเทศ
- ระบุข้อกำหนดการทำงานด้านต่าง ๆ ของระบบสารสนเทศ ที่เกี่ยวข้องกับการรักษาความปลอดภัย เช่น ข้อกำหนดด้านรหัสผู้ใช้งานและรหัสผ่าน (User ID and Password) การติดตั้งและกำหนดตัวแปรด้านความปลอดภัยในระบบปฏิบัติการคอมพิวเตอร์ อุปกรณ์เครือข่าย และไฟร์วอลล์ (Firewall) การปรับปรุงระบบปฏิบัติการทางด้านการรักษาความปลอดภัย (Security Patching) และระเบียบปฏิบัติด้านการให้ปรับปรุงและยกเลิกสิทธิการเข้าถึงและใช้งานระบบสารสนเทศ
- การกำหนดเจ้าของข้อมูล และเจ้าของระบบงานสารสนเทศ และการกำหนดบทบาทและความรับผิดชอบของเจ้าของข้อมูลและเจ้าของระบบงาน
- การแบ่งชั้นของข้อมูล ซึ่งเป็นการจัดระดับชั้นของข้อมูลตามความสำคัญของข้อมูลต่อองค์กร เพื่อจัดทำแนวทางในการรักษาความปลอดภัยของข้อมูลในแต่ระดับชั้นที่เหมาะสม
- การติดตามและการกำหนดบทลงโทษถ้ามีการละเมิดหรือไม่ปฏิบัติตามนโยบาย

ตัวอย่างของนโยบายด้านการใช้รหัสผ่าน (Password) ที่ดีนั้น ควรมีคุณสมบัติดังต่อไปนี้

- มีการกำหนดความยาวขั้นต่ำ เช่น 8 ตัวอักษรขึ้นไป เป็นต้น
- มีการกำหนดอายุการใช้งานของรหัสผ่าน เช่นจะต้องเปลี่ยนรหัสผ่านทุก 3 หรือ 6 เดือน เป็นต้น
- กำหนดให้ใช้ตัวเลขผสมตัวอักษร
- มีการกำหนดจำนวนครั้งสูงสุดที่ใส่รหัสผ่านผิด

ผู้บริหารสูงสุดควรเป็นผู้อนุมัติให้ความเห็นชอบในการบังคับใช้นโยบายการรักษาความปลอดภัยระบบสารสนเทศ และจัดให้มีการเผยแพร่นโยบายการรักษาความปลอดภัยระบบสารสนเทศ ให้กับบุคลากรที่เกี่ยวข้องรับทราบและเข้าใจหน้าที่ความรับผิดชอบ และสิ่งที่ควรปฏิบัติอย่างสม่ำเสมอ และควรจัดให้มีการปรับปรุงนโยบายการรักษาความปลอดภัยอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความเสี่ยงและเทคนิคการควบคุมอยู่ตลอดเวลา

8.1.2 การจัดทำและปฏิบัติงานตามระเบียบปฏิบัติด้านการรักษาความปลอดภัยระบบสารสนเทศ

เพื่อทำให้นโยบายการรักษาความปลอดภัยระบบสารสนเทศ สามารถนำไปปฏิบัติได้อย่างสอดคล้องกับนโยบาย ควรจะจัดทำระเบียบปฏิบัติที่เกี่ยวข้อง เพื่อเป็นแนวทางในทางปฏิบัติในรายละเอียด ซึ่งระเบียบปฏิบัติที่สำคัญ ประกอบด้วย

ระเบียบปฏิบัติด้านการจัดการรหัสผู้ใช้งาน (Users Administration Procedure) ซึ่งใช้สำหรับเป็นแนวทางในการจัดการด้านการสร้าง เปลี่ยนแปลงและยกเลิกรหัสผู้ใช้งาน ซึ่งประกอบด้วยขั้นตอน การขอและอนุมัติ การดำเนินการและการสอบทาน การยกเลิก และการสอบทานรหัสผู้ใช้งานเป็นประจำสม่ำเสมอ

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

8.1.3 การสร้างความเข้าใจและจิตสำนึกด้านความปลอดภัยระบบสารสนเทศ

เนื่องจากส่วนที่มีความเสี่ยงในด้านการรักษาความปลอดภัยระบบสารสนเทศที่สำคัญที่สุดส่วนหนึ่งก็คือ ส่วนที่เกี่ยวข้องกับพฤติกรรมในการใช้งานของผู้ใช้งาน ซึ่งผู้ใช้งานอาจมีความเข้าใจต่อความเสี่ยง และการควบคุมที่แตกต่างกัน และอาจส่งผลให้มีการใช้งานระบบคอมพิวเตอร์อย่างไม่ปลอดภัย เนื่องมาจากความไม่เข้าใจถึงขั้นตอนการทำงานที่ถูกต้อง เป็นไปตามนโยบายและหลักการการควบคุมที่ดี หรืออาจใช้งานโดยขาดจิตสำนึกที่ดีด้านการรักษาความปลอดภัย

ดังนั้นองค์กรควรจัดให้มีการสร้างความเข้าใจและจิตสำนึกด้านความปลอดภัยระบบสารสนเทศ ให้กับบุคลากรทุกคนที่เกี่ยวข้องกับการใช้ระบบสารสนเทศ ซึ่งการสร้างความรู้และจิตสำนึกดังกล่าวอาจทำได้โดยการจัดให้มีการฝึกอบรมเพื่อสร้างความเข้าใจ (Awareness Training)

อย่างต่อเนื่องและสม่ำเสมอ ซึ่งองค์กรส่วนมากจะเริ่มให้การฝึกอบรมดังกล่าวตั้งแต่วันแรก ๆ ที่บุคลากรเริ่มเข้ามาร่วมงานกับองค์กร เช่นในช่วงการปฐมนิเทศ เป็นต้น

อย่างไรก็ตาม การสร้างความเข้าใจและจิตสำนึกนั้นอาจใช้วิธีการต่าง ๆ นอกเหนือจากการฝึกอบรม เช่นการประชาสัมพันธ์ข่าวสารจากผู้บริหาร จากหน่วยงานรักษาความปลอดภัยระบบสารสนเทศ การทำกิจกรรม วีดีทัศน์แสดงตัวอย่างภัยต่าง ๆ เป็นต้น

8.2 การควบคุมด้านการรักษาความปลอดภัยทางกายภาพ

การควบคุมด้านการรักษาความปลอดภัยทางกายภาพมีวัตถุประสงค์ดังนี้

- เพื่อป้องกันมิให้บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงเครื่องคอมพิวเตอร์ และอุปกรณ์ที่สำคัญ และทำให้เกิดความเสียหายเกิดขึ้น
- เพื่อป้องกันอุบัติเหตุจากอัคคีภัยหรือภัยอื่น ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์
- เพื่อให้มีสภาพแวดล้อมที่เอื้อต่อการประมวลผลที่มีประสิทธิภาพ

เพื่อบรรลุถึงวัตถุประสงค์ของการควบคุมข้างต้น ผู้บริหารองค์กรควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

8.2.1 การควบคุมการเข้าถึงทางกายภาพของระบบคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

8.2.2 การควบคุมด้านสภาวะแวดล้อมการทำงานของระบบคอมพิวเตอร์

8.2.1 การควบคุมการเข้าถึงทางกายภาพของระบบคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

การควบคุมที่สำคัญมีรายละเอียดดังต่อไปนี้

- จัดให้ห้องคอมพิวเตอร์อยู่ในสถานที่ที่เหมาะสม เช่นไม่เป็นที่ที่พลุกพล่านด้วยผู้คนจำนวนมาก และถ้าอยู่ในอาคาร ก็ไม่ควรอยู่ชั้นที่สูงหรือต่ำเกินไป
- ควรมีการออกแบบแบ่งเป็นสัดส่วนตามความต้องการด้านการรักษาความปลอดภัย และตามลักษณะการใช้งาน เช่นส่วนเฉพาะสำหรับพนักงานปฏิบัติการคอมพิวเตอร์ หรือส่วนเฉพาะของเจ้าหน้าที่เครือข่าย เป็นต้น
- ควรมีการติดตั้งระบบควบคุมการเข้าออกศูนย์คอมพิวเตอร์ซึ่งสามารถบันทึกการเข้าออกของบุคลากรแต่ละคนได้ เช่นการติดตั้งอุปกรณ์การควบคุมการเข้าออกแบบอิเล็คทรอนิคส์ เป็นต้น

- ควรจัดให้มีระเบียบการในการให้และยกเลิกบัตรหรืออุปกรณ์อื่น ๆ ที่ใช้ในการเปิดปิดประตูเข้าออกห้องคอมพิวเตอร์
- สำหรับการขอเข้าห้องคอมพิวเตอร์เป็นการชั่วคราว เช่นช่างเทคนิคของบริษัทผู้ค้าคอมพิวเตอร์ ผู้ตรวจสอบ ผู้เยี่ยมชม เป็นต้น ควรจัดให้มีการอนุญาตอย่างเหมาะสม และมีการบันทึกข้อมูลการเข้าออกอย่างเพียงพอ และมีเจ้าหน้าที่ขององค์กรเฝ้าสังเกตการณ์อยู่ตลอดเวลา
- สำหรับอุปกรณ์ที่สำคัญที่อยู่ภายนอกห้องคอมพิวเตอร์ ก็ควรจัดให้มีการป้องกันความปลอดภัยทางกายภาพสำหรับเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่สำคัญเหล่านั้นอย่างเหมาะสม

8.2.2 การควบคุมด้านสภาวะแวดล้อมการทำงานของระบบคอมพิวเตอร์

การควบคุมประกอบด้วย

- จัดให้มีการติดตั้งและทดสอบอุปกรณ์ควบคุมสภาวะแวดล้อมของการทำงานของระบบคอมพิวเตอร์ในห้องคอมพิวเตอร์อย่างเพียงพอ เช่นมีการติดตั้งระบบปรับอุณหภูมิ ความชื้นและคลื่นแม่เหล็ก และอุปกรณ์ในการควบคุมความคงที่และจัดให้มีไฟฟ้าใช้อย่างต่อเนื่อง
- ไม่ควรติดตั้งระบบดับเพลิงที่ใช้น้ำเป็นปัจจัยสำคัญในการดับไฟ เช่นการติดตั้งระบบดับเพลิงด้วยน้ำ (Water Sprinkle) เป็นต้น
- ระบบปรับอากาศควรจะต่อเข้ากับระบบไฟฟ้าจากแหล่งเดียวกันกับระบบคอมพิวเตอร์ เพื่อทำให้มั่นใจว่าระบบปรับอากาศสามารถทำงานได้ในกรณีไฟฟ้าปกติขัดข้องและระบบคอมพิวเตอร์จะต้องใช้ไฟฟ้าจากแหล่งไฟฟ้าสำรอง

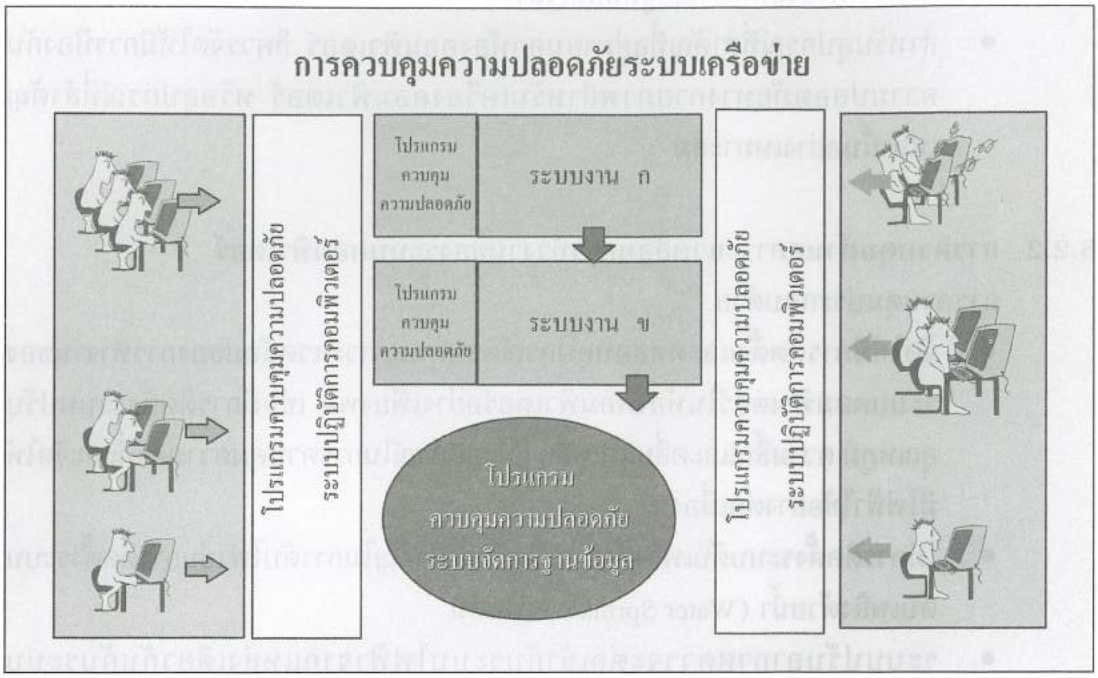
8.3 การควบคุมด้านการรักษาความปลอดภัยเชิงตรรกะ

การควบคุมด้านการรักษาความปลอดภัยเชิงตรรกะมีวัตถุประสงค์เพื่อ

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

เพื่อบรรลุถึงวัตถุประสงค์ของการควบคุมข้างต้น ผู้บริหารองค์กรควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

การควบคุมในด้านการรักษาความปลอดภัยเชิงตรรกะเป็นการทำงานผ่านกลไกทางเทคนิคของระบบคอมพิวเตอร์ ซึ่งภายในระบบคอมพิวเตอร์นั้น มีการควบคุมด้านความปลอดภัยระบบสารสนเทศ อยู่หลายส่วนด้วยกัน ซึ่งสามารถอธิบายได้ดังภาพที่ 3-8



ภาพ 3-8 ส่วนต่าง ๆ ของการรักษาความปลอดภัยเชิงตรรกะ

การควบคุมด้านการรักษาความปลอดภัยเชิงตรรกะสามารถแบ่งออกเป็น 4 ส่วนคือ

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

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

ส่วนที่ 3 เป็นส่วนของการรักษาความปลอดภัยภายในระบบงานสารสนเทศ (Application System) ซึ่งทำงานโดยโปรแกรมของแต่ละระบบงาน โดยทำหน้าที่กำหนดสิทธิในการใช้งานฟังก์ชั่นต่าง ๆ ที่มีอยู่ในระบบงานนั้น ๆ

ส่วนสุดท้ายเป็นส่วนของการควบคุมในกรณีที่มีการต่อเชื่อมระบบคอมพิวเตอร์เป็นระบบเครือข่ายคอมพิวเตอร์ (Computer Network) ซึ่งทำหน้าที่รักษาความปลอดภัยด้านการสื่อสารและการเข้าถึงภายในระบบเครือข่าย

สำหรับส่วนของการรักษาความปลอดภัยในระบบงานสารสนเทศนั้นจะอยู่ในส่วนของการควบคุมระบบงาน (Application Control)

รายละเอียดเกี่ยวกับความเสี่ยง การควบคุมและการตรวจสอบ สามารถศึกษาได้ในบทอื่น ๆ ของชุดวิชานี้

9. การควบคุมด้านการปฏิบัติการคอมพิวเตอร์

ก่อนที่จะทำความเข้าใจการควบคุมการปฏิบัติการระบบสารสนเทศ ลำดับแรกควรทำความเข้าใจการทำงานปฏิบัติการระบบสารสนเทศเสียก่อนว่า งานดังกล่าวมีรายละเอียดอย่างไร ซึ่งงานปฏิบัติการระบบสารสนเทศ ประกอบด้วยงานดังต่อไปนี้

- งานเปิดปิด เครื่องและระบบคอมพิวเตอร์
- งานติดตามดูแลและสนับสนุนการใช้งาน
- งานประมวลผลสิ้นวันและการจัดพิมพ์รายงาน
- งานสำรองและกู้ข้อมูล
- งานบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ

งานเปิดปิด เครื่องและระบบคอมพิวเตอร์ ก่อนเริ่มปฏิบัติงานกับระบบคอมพิวเตอร์ พนักงานปฏิบัติการจะต้องเปิดเครื่องคอมพิวเตอร์ และระบบงานสารสนเทศเสียก่อน มิฉะนั้นจะไม่มีผู้ใช้งานคนใดสามารถใช้ได้ และก่อนจบงานก็จะต้องปิดระบบงาน ซึ่งจะต้องมีกระบวนการตรวจเช็คก่อนว่าผู้ใช้งานทุกคนใช้งานหรือป้อนข้อมูลเสร็จสิ้นหมดแล้ว ก่อนจะทำการปิดระบบงานและปิดเครื่องคอมพิวเตอร์ ตามลำดับ

งานติดตามดูแลและสนับสนุนการใช้งาน เป็นการติดตามการใช้งานและให้ความช่วยเหลือและสนับสนุนการใช้งาน ซึ่งประกอบด้วยการรับรู้รับแจ้งเหตุการณ์หรือปัญหาต่าง ๆ ตรวจสอบเหตุการณ์หรือปัญหา บันทึกรายละเอียด ประสานงานเพื่อการจัดการแก้ไข และสรุปปิดเหตุการณ์และปัญหาที่เกิดขึ้น

งานประมวลผลสิ้นวันและการจัดพิมพ์รายงาน เมื่อปิดระบบงานเรียบร้อยแล้ว พนักงานปฏิบัติการคอมพิวเตอร์ก็จะเริ่มการประมวลผลสิ้นวัน โดยส่วนใหญ่จะเป็นการประมวลผลโปรแกรมตามลำดับก่อนหลังที่ถูกกำหนดไว้ล่วงหน้าโดยผู้ออกแบบระบบงาน และถ้ามีการจัดพิมพ์รายงานสิ้นวัน พนักงานปฏิบัติการคอมพิวเตอร์ก็จะจัดการพิมพ์รายงานโดยใช้แบบฟอร์มที่จัดเตรียมไว้ล่วงหน้า

งานสำรองและกู้ข้อมูล เป็นงานที่ดำเนินการระหว่างการประมวลผลสิ้นวัน ซึ่งครอบคลุมการสำรองข้อมูลจากระบบคอมพิวเตอร์มาไว้ที่อุปกรณ์สำรองข้อมูลเช่น เทป หรือแผ่นดิสก์ เป็นต้น และการนำข้อมูลสำรองไปจัดเก็บไว้ในสถานที่ปลอดภัยทั้งในและนอกศูนย์คอมพิวเตอร์ และในกรณีที่จะต้องกู้ข้อมูล พนักงานปฏิบัติการคอมพิวเตอร์ ก็จะทำหน้าที่นำข้อมูลสำรองที่เก็บไว้มาแทนข้อมูลในระบบงานจริง

งานบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ เป็นการบำรุงรักษาระบบฯ ตามระยะเวลา หรือจัดให้มีการซ่อมแซมเปลี่ยนแปลงเมื่อเกิดเหตุขัดข้อง

การทำงานของระบบคอมพิวเตอร์นั้นจำเป็นที่จะต้องมีการควบคุมดูแล ซึ่งความรับผิดชอบในการทำงานในส่วนนี้เป็นหน้าที่ของผู้ปฏิบัติการคอมพิวเตอร์ (Computer Operator) ซึ่งถ้ามีข้อผิดพลาดเกิดขึ้นจะส่งผลกระทบต่อระบบสารสนเทศโดยรวม เช่น ถ้าผู้ปฏิบัติการคอมพิวเตอร์ประมวลผลโปรแกรมผิดลำดับ อาจทำให้ข้อมูลรายการต่าง ๆ ผิดทั้งหมดก็ได้ และโดยส่วนมากผู้ปฏิบัติการคอมพิวเตอร์จะไม่ใช่ผู้เชี่ยวชาญด้านคอมพิวเตอร์ ทำให้โอกาสเกิดข้อผิดพลาดในการทำงานสูงขึ้น

เพื่อให้ง่ายต่อการทำความเข้าใจ จะแบ่งการควบคุมด้านการปฏิบัติการคอมพิวเตอร์ออกเป็น 3 กลุ่ม ประกอบด้วย

9.1 การควบคุมด้านการประมวลผลของระบบสารสนเทศ

9.2 การสำรองข้อมูลและการนำข้อมูลสำรองกลับมาใช้

9.3 การควบคุมด้านการปฏิบัติการคอมพิวเตอร์ อื่น ๆ

ซึ่งมีวัตถุประสงค์และแนวทางการควบคุมดังต่อไปนี้

9.1 การควบคุมด้านการประมวลผลของระบบสารสนเทศ

การควบคุมด้านการประมวลผลของระบบสารสนเทศ มีวัตถุประสงค์เพื่อทำให้การประมวลผลระบบสารสนเทศมีความถูกต้อง ครบถ้วน ตรงเวลา และตรงกับความต้องการของผู้ใช้งาน และเพื่อให้เจ้าหน้าที่ผู้ปฏิบัติการระบบสารสนเทศมีความรู้ความเข้าใจในการปฏิบัติการคอมพิวเตอร์และระบบงานต่าง ๆ อย่างเพียงพอ

เพื่อบรรลุถึงวัตถุประสงค์ของการควบคุมข้างต้น ผู้บริหารองค์กรควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

- กำหนดให้มีระเบียบการปฏิบัติงานที่ชัดเจนสำหรับงานการประมวลผลของระบบสารสนเทศ
- มีการจัดทำตารางการประมวลผลสิ้นวันอย่างเป็นทางการ และผู้ปฏิบัติการระบบสารสนเทศใช้ตารางดังกล่าวในการดำเนินการประมวลผลสิ้นวัน และบันทึกรายละเอียดต่าง ๆ ของการประมวลผลไว้ในตารางนี้
- ผู้ควบคุมงานปฏิบัติการระบบสารสนเทศสอบทานตารางการประมวลผลสิ้นวัน เพื่อทำให้มั่นใจว่าการประมวลผลสิ้นวันได้รับการประมวลผลอย่างครบถ้วนถูกต้องและเป็นไปตามที่กำหนดไว้

- จัดให้มีการประเมินความรู้ความสามารถของผู้ปฏิบัติการระบบสารสนเทศ และจัดให้มีการฝึกอบรมเพื่อทำให้มั่นใจว่า ผู้ปฏิบัติการระบบสารสนเทศมีความรู้ความเข้าใจต่อการประมวลผลของระบบสารสนเทศ และความรู้ด้านระบบงานต่าง ๆ ที่องค์กรมีใช้งานอยู่อย่างเพียงพอ

9.2 การสำรองข้อมูลและการนำข้อมูลสำรองกลับมาใช้

การควบคุมด้านการสำรองข้อมูลและการนำข้อมูลสำรองกลับมาใช้มีวัตถุประสงค์เพื่อทำให้มีการสำรองข้อมูลอย่างเพียงพอ และสามารถนำข้อมูลสำรองกลับมาใช้อย่างถูกต้อง ครบถ้วน ตรงเวลา และตรงกับความต้องการในการใช้ข้อมูลขององค์กร

เพื่อบรรลุถึงวัตถุประสงค์ของการควบคุมข้างต้น ผู้บริหารองค์กรควรจัดให้มีการควบคุมตามแนวทางดังต่อไปนี้

- กำหนดให้มีระเบียบการปฏิบัติงานที่ชัดเจนสำหรับการสำรองข้อมูลและการนำข้อมูลสำรองกลับมาใช้
- มีการจัดทำตารางการสำรองข้อมูลและโปรแกรมอย่างเป็นทางการ และผู้ปฏิบัติการระบบสารสนเทศใช้ตารางดังกล่าวในการดำเนินการสำรองข้อมูล และบันทึกรายละเอียดต่าง ๆ ของการสำรองข้อมูลไว้ในตารางนี้
- ผู้ควบคุมงานปฏิบัติการระบบสารสนเทศสอบทานตารางการสำรองข้อมูล เพื่อทำให้มั่นใจว่าการสำรองข้อมูลเป็นไปอย่างอย่างครบถ้วนถูกต้องและเป็นไปตามที่กำหนดไว้
- มีการจัดเก็บข้อมูลสำรองไว้ในที่ที่ปลอดภัย ทั้งที่เก็บไว้ที่ศูนย์คอมพิวเตอร์ภายในและที่นำไปจัดเก็บไว้ที่สถานที่จัดเก็บภายนอก

9.3 การควบคุมด้านการปฏิบัติการคอมพิวเตอร์ อื่น ๆ

การปฏิบัติการคอมพิวเตอร์อื่น ๆ ประกอบด้วยกระบวนงาน ดังต่อไปนี้

- งานเปิดปิด เครื่องและระบบคอมพิวเตอร์
- งานติดตามดูแลและสนับสนุนการใช้งาน
- การจัดพิมพ์รายงาน
- งานบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ

ซึ่งมีวัตถุประสงค์ของการควบคุมในแต่ละกระบวนงาน เพื่อให้ระบบคอมพิวเตอร์สามารถให้บริการผู้ใช้งานอย่างมีประสิทธิภาพ และตรงกับความต้องการในการใช้งาน ซึ่งมีแนวทางในการควบคุมดังนี้

- จัดให้มีการตกลงกันระหว่างผู้รับบริการหรือผู้ใช้งานและผู้ให้บริการหรือผู้บริหารงานปฏิบัติการระบบสารสนเทศ เพื่อกำหนดเป็นระดับการให้บริการ (Service Level Agreement) เพื่อเป็นแนวทางในการบริหารการบริการของผู้บริหารงานปฏิบัติการระบบสารสนเทศ
- จัดให้มีระบบการรายงานผลการดำเนินการตามระดับการให้บริการที่ตกลงไว้ เพื่อทำให้มั่นใจว่าการให้บริการเป็นไปตามที่ตกลงไว้ โดยที่รายงานดังกล่าวควรมีการจัดส่งให้ทั้งผู้บริหารของผู้ให้บริการและผู้บริหารในสายงานผู้รับบริการ
- กำหนดให้มีระเบียบการปฏิบัติงานที่ชัดเจนสำหรับงานปฏิบัติการระบบสารสนเทศที่สำคัญ ดังต่อไปนี้
  - งานเปิดปิด เครื่องและระบบคอมพิวเตอร์
  - งานติดตามดูแลและสนับสนุนการใช้งาน
  - การจัดพิมพ์รายงาน
  - งานบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่าง ๆ
- ถ้ามีการปฏิบัติการนอกเหนือจากที่กำหนดไว้ในระเบียบปฏิบัติจะต้องมีการบันทึกเหตุผลของการดำเนินการและการอนุมัติ ไว้อย่างชัดเจน
- จัดให้มีการสอบทานการทำงานของผู้ปฏิบัติการระบบสารสนเทศอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการดำเนินการดังกล่าวเป็นไปตามที่กำหนดไว้ในระเบียบปฏิบัติอย่างเคร่งครัด
- จัดให้มีการประเมินความรู้ความสามารถของผู้ปฏิบัติการระบบสารสนเทศ และจัดให้มีการฝึกอบรมเพื่อทำให้มั่นใจว่าผู้ปฏิบัติการระบบสารสนเทศมีความรู้ความเข้าใจต่อการปฏิบัติการระบบสารสนเทศ และความรู้ด้านระบบงานต่าง ๆ ที่องค์กรมีใช้งานอยู่ อย่างเพียงพอต่อการปฏิบัติการระบบสารสนเทศอย่างมีประสิทธิภาพและปราศจากข้อผิดพลาด
- จัดให้มีช่องทางและผู้รับผิดชอบโดยตรงในการรับแจ้งและจัดการกับปัญหาต่าง ๆ ที่เกิดขึ้นกับระบบสารสนเทศ และกำหนดเป็นระเบียบปฏิบัติที่ชัดเจนในการแจ้ง บันทึก และติดตามแก้ไขปัญหา
- มีการบันทึกรายละเอียดของปัญหาโดยละเอียด ประกอบด้วย วันและเวลาที่เกิดปัญหา ผู้แจ้งและผู้รับแจ้ง ลักษณะของปัญหา ผลการวิเคราะห์ และผลการแก้ไขปัญหา

- มีการวิเคราะห์แนวโน้มของปัญหาต่าง ๆ เพื่อวางมาตรการแก้ไขปัญหาระยะยาว และป้องกันมิให้ปัญหาเกิดขึ้นอย่างซ้ำซ้อน
- มีการจัดทำตารางการพิมพ์รายงานอย่างเป็นทางการ และผู้ปฏิบัติการระบบสารสนเทศใช้ตารางดังกล่าวในการดำเนินการพิมพ์รายงาน และบันทึกรายละเอียดต่าง ๆ ของการพิมพ์รายงานไว้ในตารางนี้
- มีกระบวนการที่ทำให้มั่นใจว่าผู้ใช้รายงานได้รับรายงานอย่างถูกต้องและครบถ้วน เช่น จัดให้มีการเซ็นรับรายงานโดยผู้ใช้งาน หรือการจัดส่งรายงานในรูปแบบอิเล็กทรอนิกส์
- จัดให้มีตารางการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงโดยละเอียดแยกเป็นรายการต่างหาก และดำเนินการให้มีการบำรุงรักษาตามตารางที่กำหนดไว้อย่างเคร่งครัด
- มีการควบคุมการทำงานของช่างผู้ทำการบำรุงรักษาอย่างใกล้ชิด ในระหว่างที่ดำเนินการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

10. การควบคุมด้านการบริหารจัดการข้อมูล

ข้อมูลสารสนเทศถือว่าเป็นปัจจัยสำคัญในการบริหารงานองค์กร ดังนั้นองค์กรควรจัดให้มีการควบคุมที่ดีเพื่อทำให้องค์กรมีข้อมูลที่ถูกต้อง ครบถ้วน และพร้อมใช้เมื่อมีความจำเป็น ซึ่งแนวทางการควบคุมควรประกอบด้วยการดำเนินการด้านต่าง ๆ ดังนี้

10.1 การจัดทำโครงสร้างข้อมูลองค์กร

10.2 การกำหนดผู้รับผิดชอบต่อข้อมูล

10.3 การแบ่งประเภทข้อมูลตามระดับความสำคัญ

10.1 การจัดทำโครงสร้างข้อมูลองค์กร

ปัญหาที่สำคัญในด้านการบริหารจัดการข้อมูลสารสนเทศภายในองค์กรคือ การที่ผู้บริหารข้อมูลไม่มีข้อมูลเพียงพอที่จะบริหารข้อมูลได้อย่างมีประสิทธิภาพ ดังนั้นวัตถุประสงค์ของการจัดทำโครงสร้างของข้อมูล ก็เพื่อจัดให้มีข้อมูลเกี่ยวกับข้อมูลสารสนเทศขององค์กรอย่างถูกต้องและเพียงพอในการบริหารข้อมูลสารสนเทศขององค์กรอย่างมีประสิทธิภาพ ซึ่งมีแนวทางในการดำเนินการควบคุมดังนี้

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

10.2 การกำหนดผู้รับผิดชอบต่อข้อมูล

ในองค์กรที่สามารถบริหารจัดการด้านข้อมูลสารสนเทศที่ดี จะมีการกำหนดให้มีเจ้าของข้อมูลซึ่งเป็นผู้รับผิดชอบที่ชัดเจนต่อข้อมูลสารสนเทศ เช่นกำหนดให้ผู้บริหารฝ่ายบุคคลเป็นเจ้าของข้อมูลพนักงาน หรือผู้บริหารฝ่ายบัญชีเป็นเจ้าของข้อมูลบัญชี เพื่อให้มีบุคคลที่รับผิดชอบ

ต่อข้อมูลด้านความถูกต้อง ความครบถ้วน และความปลอดภัย โดยมีแนวทางในการดำเนินการควบคุมดังนี้

- กำหนดให้มีเจ้าของข้อมูลที่ชัดเจนเพื่อเป็นผู้รับผิดชอบโดยตรงด้านความถูกต้องความครบถ้วนและความปลอดภัยของข้อมูล โดยจัดให้มีการกำหนดเงื่อนไขว่าจะให้ผู้บริหารท่านใดเป็นเจ้าของข้อมูลใด เช่นกำหนดให้ผู้บริหารฝ่ายงานที่เป็นแหล่งกำเนิดข้อมูล เป็นเจ้าของข้อมูล หรือกำหนดให้ผู้บริหารฝ่ายงานที่อาจได้รับผลเสียหายมากที่สุดถ้าข้อมูลเกิดความเสียหาย เป็นเจ้าของข้อมูล เป็นต้น
- กำหนดหน้าที่ความรับผิดชอบของเจ้าของข้อมูล ซึ่งควรครอบคลุมด้านความถูกต้องครบถ้วนของข้อมูล ความปลอดภัยในการใช้ข้อมูล การจัดเก็บและการสำรองข้อมูล ซึ่งหน้าที่ของเจ้าของข้อมูลนั้นไม่ได้เป็นผู้รับผิดชอบในการดำเนินการด้านต่าง ๆ ดังกล่าวเอง แต่เป็นบทบาทด้านการกำหนดระเบียบปฏิบัติ การกำหนดความต้องการและเงื่อนไขในการใช้ข้อมูล ประสานงานกับผู้ปฏิบัติให้ดำเนินการตามระเบียบปฏิบัติและตามความต้องการ การติดตามดูแลให้การดำเนินการด้านข้อมูลเป็นไปตามเงื่อนไขดังกล่าวข้างต้น รวมถึงการอนุญาตให้ผู้อื่นนำข้อมูลไปใช้

10.3 การแบ่งประเภทข้อมูลตามระดับความสำคัญ

เพื่อให้การบริหารจัดการต่าง ๆ ด้านข้อมูลสารสนเทศมีความสอดคล้องกับระดับความสำคัญของข้อมูลสารสนเทศ ควรจัดให้มีการแบ่งประเภทข้อมูล โดยส่วนมากจะให้เจ้าของข้อมูลเป็นผู้กำหนดว่าข้อมูลที่ตนเองรับผิดชอบนั้นจัดอยู่ในประเภทใด ซึ่งตัวอย่างของประเภทของข้อมูลได้แก่

- ประเภทข้อมูลสาธารณะ (Public Information) คือข้อมูลที่สามารถเปิดเผยให้สาธารณะรับทราบได้ เช่นข้อมูลคุณสมบัติของสินค้า หรือข้อมูลงบการเงินที่ได้รับการรับรองจากผู้สอบบัญชีแล้ว เป็นต้น
- ประเภทข้อมูลภายใน (Internal Information) คือข้อมูลที่ใช้ภายในองค์กร และทุกหน่วยงานหรือบุคลากรทุกคนสามารถใช้ได้ เช่นข้อมูลเกี่ยวกับระเบียบปฏิบัติภายใน หรือข้อมูลด้านโครงสร้างองค์กร เป็นต้น
- ประเภทข้อมูลเฉพาะด้านหรือฝ่ายงาน (Specific/Department Information) ซึ่งเป็นข้อมูลที่ถูกกำหนดให้ใช้เฉพาะด้าน หรือเฉพาะหน่วยงาน เช่นข้อมูลด้านการผลิตน่าจะเป็นข้อมูลที่ใช้เฉพาะสายงานผลิตเป็นต้น
- ประเภทข้อมูลลับเฉพาะ (Confidential Information) เป็นข้อมูลที่ใช้เฉพาะบางคนหรือเป็นข้อมูลที่เมื่อถูกเปิดเผยแล้วอาจส่งผลกระทบต่อการบริหารงานโดยรวม เช่นข้อมูลเงินเดือน เป็นต้น

- ประเภทข้อมูลลับสูงสุด (Highly Confidential/Restricted Information) เป็นข้อมูลที่ต้องรักษาให้เป็นความลับอย่างยิ่ง เพราะถ้าถูกเปิดเผยแล้วอาจส่งผลกระทบรุนแรงต่อองค์กร เช่นข้อมูลความลับทางการค้า หรือ ข้อมูลสูตรการผลิตเฉพาะสินค้า เป็นต้น

การจัดประเภทข้อมูลมีความจำเป็นอย่างยิ่งถ้าจะทำให้การบริหารจัดการข้อมูลมีประสิทธิภาพและประสิทธิผลมากที่สุด ซึ่งกล่าวอีกนัยหนึ่งก็คือหลังจากจัดให้มีการจัดประเภทข้อมูลแล้วก็ควรจะนำข้อมูลนี้ไปวิเคราะห์และจัดทำแนวทางบริหารจัดการข้อมูลให้เหมาะสมกับระดับความสำคัญของแต่ละประเภทของข้อมูล

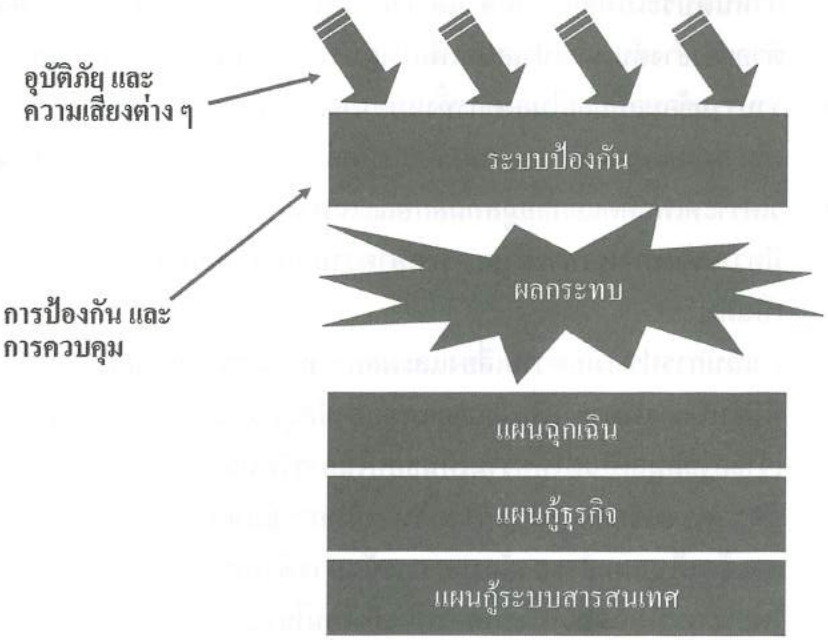
โดยมีแนวทางในการดำเนินการควบคุมดังนี้

- กำหนดประเภทของข้อมูล และเงื่อนไขในการจัดประเภทข้อมูล ดังแสดงไว้เป็นตัวอย่างข้างต้น และนำเสนอเพื่อให้ผู้บริหารระดับสูงเป็นผู้เห็นชอบ
- รวบรวมข้อมูลที่มีอยู่ในองค์กรทั้งหมดมาจัดเป็นกลุ่มของข้อมูลที่จะนำมาใช้จัดประเภท เช่น กลุ่มข้อมูลพนักงาน กลุ่มข้อมูลลูกค้า และ กลุ่มข้อมูลบัญชีการเงิน เป็นต้น
- วิเคราะห์เพื่อคัดแยกข้อมูลที่มีลักษณะเฉพาะออกจากกลุ่มข้อมูล เช่นข้อมูลเงินเดือนมีความต้องการเฉพาะด้านการรักษาความลับ ควรแยกออกจากกลุ่มข้อมูลพนักงาน เป็นต้น
- ดำเนินการประเมินความเสี่ยงและผลกระทบที่เกี่ยวกับข้อมูลแต่ละกลุ่ม และข้อมูลที่มีลักษณะเฉพาะ เพื่อจัดประเภทของข้อมูลแต่ละกลุ่มและข้อมูลเฉพาะ โดยให้เจ้าของข้อมูลเป็นผู้ให้ความเห็นชอบในการจัดประเภทดังกล่าว
- จัดทำความต้องการด้านการบริหารจัดการข้อมูล เช่นการรักษาความปลอดภัย การจัดเก็บและสำรองข้อมูล การจัดการด้านความถูกต้องครบถ้วนของข้อมูล โดยระบุว่าในแต่ละประเภทจะต้องมีเงื่อนไขในการดำเนินการด้านความปลอดภัย การจัดเก็บและสำรองความถูกต้องอย่างไร
- จัดให้มีการสอบทานเพื่อติดตามว่า การดำเนินการด้านข้อมูลในแต่ละประเภทเป็นไปตามแนวทางที่กำหนดไว้หรือไม่

11. การควบคุมด้านการวางแผนเพื่อกู้ระบบในกรณีเกิดความเสียหายอย่างรุนแรง

การควบคุมด้านการวางแผนเพื่อกู้ระบบในกรณีเกิดความเสียหายอย่างรุนแรงต่อระบบสารสนเทศมีวัตถุประสงค์เพื่อทำให้มีระบบสารสนเทศใช้อย่างต่อเนื่อง และสามารถกู้ระบบสารสนเทศกลับมาใช้ใหม่ภายในระยะเวลาที่เหมาะสม

ความจำเป็นในการจัดให้มีการควบคุมด้านความต่อเนื่อง ซึ่งในส่วนนี้เน้นทางด้านการวางแผนนำระบบกลับมาใช้ใหม่ นั้นสามารถแสดงได้โดยภาพ 3-9



ภาพ 3-9 การบริหารความต่อเนื่องระบบสารสนเทศ

ภาพ 3-9 เป็นแผนภาพแสดงความจำเป็นในการจัดให้มีแผนกู้ระบบสารสนเทศ ซึ่งเริ่มจากสมมติให้องค์กรเปรียบเป็นแฮมเบอร์เกอร์ โดยการดำเนินกิจกรรมต่าง ๆ ขององค์กรนั้นอาจเกิดภัยหรือความเสี่ยงเกิดขึ้นและอาจมีผลกระทบต่อองค์กรอยู่ตลอดเวลา เช่น ไฟไหม้ น้ำท่วม การจลาจล เครื่องเสีย หรือไฟฟ้าขัดข้อง เป็นต้น

เพื่อจัดการกับความเสี่ยงและภัยต่าง ๆ ที่อาจเกิดขึ้น องค์กรส่วนใหญ่จะจัดให้มีการป้องกัน เช่น การสร้างระบบรักษาความปลอดภัย การออกแบบให้มีการสำรองอุปกรณ์ต่าง ๆ เป็นต้น แต่อย่างไรก็ตามภัยหรือความเสี่ยงต่าง ๆ อาจเล็ดลอดการป้องกันต่าง ๆ นั้นเข้ามาได้ ซึ่งจะก่อให้เกิดผลกระทบต่าง ๆ มากมาย เช่น ผลกระทบทางการเงินโดยตรง ผลกระทบทำให้ธุรกิจหยุดชะงัก ผลกระทบด้านภาพพจน์ เป็นต้น

เมื่อเกิดเหตุการณ์เกิดขึ้นสิ่งแรกที่องค์กรควรจะต้องมี คือแผนจัดการเหตุการณ์เร่งด่วนเฉพาะหน้า ได้แก่แผนอพยพพนักงาน การปฐมพยาบาลเบื้องต้น การประชาสัมพันธ์ เพื่อลดผลกระทบเบื้องต้น แต่ว่าแผนดังกล่าวไม่สามารถกู้ธุรกิจให้กลับมาดำเนินการต่อได้ ดังนั้นองค์กรต้องจัดทำแผนเพื่อนำธุรกิจกลับมาดำเนินการใหม่ให้ได้ ซึ่งองค์ประกอบที่สำคัญที่ขาดไม่ได้ก็คือ การจัดทำแผนกู้ระบบสารสนเทศ

การควบคุมที่สำคัญมีรายละเอียดดังต่อไปนี้

1) มีการประเมินความเสี่ยงที่ระบบคอมพิวเตอร์อาจหยุดชะงัก และส่งผลกระทบให้การดำเนินธุรกิจหยุดชะงักเป็นระยะเวลานาน พร้อมทั้งจัดให้มีการป้องกันและจัดการเพื่อมิให้ความเสี่ยงต่าง ๆ เหล่านี้เกิดขึ้น
2) ประเมินผลกระทบที่อาจเกิดขึ้นถ้าระบบหยุดชะงักในแต่ละระยะเวลา เช่น ถ้าระบบหยุดชะงักเป็นเวลา 1 ชั่วโมงจะก่อให้เกิดผลกระทบทั้งทางการเงินและที่ไม่ใช่ตัวเงินมากเท่าไร และถ้าเพิ่มระยะเวลาขึ้นไปเป็น 2 ชั่วโมง ครึ่งวัน 1 วัน 2 วันหรือ 1 อาทิตย์ จนกระทั่งเราสามารถกำหนดระยะเวลาในการที่เราต้องกู้ระบบกลับมาใช้ใหม่ให้ได้ เพื่อกำหนดเป็นเป้าหมายในการกู้ระบบ (Recovery Time Target)
3) หลังจากที่ทราบถึงเป้าหมายด้านระยะเวลาที่ต้องกู้ระบบกลับมาให้ได้แล้ว จะต้องจัดทำกลยุทธ์ในการกู้ระบบสารสนเทศ ซึ่งประกอบด้วยกลยุทธ์ในการสำรองข้อมูล กลยุทธ์ในการจัดหาสถานที่สำรองเพื่อใช้ในการกู้ระบบ และแผนการในการกู้ระบบฯ
4) การสำรองข้อมูลควรจะต้องสอดคล้องกับระยะเวลาที่จะต้องกู้ระบบฯ เช่นถ้าจะต้องกู้ระบบกลับมาให้ได้ภายในระยะเวลาที่สั้น เช่นภายใน 1 ชั่วโมง การสำรองข้อมูลอาจจำเป็นต้องเป็นการสำรองข้อมูลที่ค่อนข้างถี่และเกือบใกล้เคียงกับการทำงานจริง เช่นการสำรองแบบ real time mirroring โดยเมื่อรายการได้รับการปรับปรุงในระบบงานจริง ก็จะทำการปรับปรุงรายการที่อยู่ที่เครื่องสำรองด้วย แต่ถ้าระยะเวลาสำหรับการกู้ระบบค่อนข้างนาน การสำรองข้อมูลอาจทำเป็นรายวันก็ได้

5) ข้อมูลสำรองควรเก็บไว้ทั้งในและนอกสถานที่เพื่อรองรับกรณีที่เกิดความสูญเสียกับศูนย์คอมพิวเตอร์และข้อมูลที่สำรองไว้ เราจะยังคงมีข้อมูลสำรองที่เก็บไว้อีกที่หนึ่ง สถานที่จัดเก็บข้อมูลสำรองภายนอกก็จะต้องมีการรักษาความปลอดภัยระดับที่ใกล้เคียงกับที่ศูนย์คอมพิวเตอร์ และควรมีระยะทางที่ห่างจากศูนย์คอมพิวเตอร์หลักพอสมควร

6) การเตรียมสถานที่หรือศูนย์คอมพิวเตอร์สำรองก็ควรเลือกให้มีความสอดคล้องกับระยะเวลาในการกู้ระบบฯ เช่นกัน ซึ่งเรามีทางเลือกดังต่อไปนี้

- สถานที่สำรองแบบพร้อมใช้ทันที (Hot Site) เป็นศูนย์คอมพิวเตอร์ที่มีทุกอย่างครบเกือบเท่าเทียมกันกับศูนย์คอมพิวเตอร์หลัก ซึ่งเมื่อมีความต้องการกู้ระบบก็สามารถใช้ศูนย์คอมพิวเตอร์สำรองนี้ได้เกือบทันที แต่ก็ต้องใช้เงินลงทุนค่อนข้างสูง
- สถานที่สำรองแบบมีแต่สถานที่ (Cold Site) เป็นสถานที่ที่เตรียมไว้สำหรับการกู้ระบบ แต่อาจมีเพียงสถานที่ว่าง ๆ เตรียมไว้เท่านั้น และเมื่อถึงเวลาที่จะต้องกู้ระบบฯ อาจต้องดำเนินการติดตั้งเครื่องคอมพิวเตอร์ ระบบเครือข่าย ระบบงานสารสนเทศ และข้อมูล ซึ่งอาจใช้ระยะเวลาที่ค่อนข้างนาน แต่ก็มีข้อดีที่การใช้เงินลงทุนไม่สูง
- สถานที่สำรองแบบผสม (Warm Site) เป็นสถานที่ที่อยู่ระหว่างกลางของแบบที่1 และแบบที่ 2 ข้างต้น จะเอนเอียงไปตามแบบใดนั้นขึ้นอยู่กับความจำเป็นด้านระยะเวลาที่ต้องกู้ระบบฯกลับมาใช้ใหม่

7) นอกจากมีทางเลือกด้านลักษณะของศูนย์คอมพิวเตอร์สำรองข้างต้นแล้ว เรายังมีทางเลือกของการจัดหาหรือจัดสร้างอีกด้วยดังนี้

- สร้างศูนย์สำรองขึ้นมาเอง วิธีนี้เป็นวิธีที่มีการลงทุนสูง แต่ให้ความปลอดภัยและรวดเร็วกว่าในการกู้ระบบฯ
- เช่าสถานที่เพื่อใช้เป็นศูนย์สำรองชั่วคราว วิธีนี้เหมาะสำหรับระยะเวลาการกู้ระบบที่นานกว่า และมีค่าใช้จ่ายค่อนข้างต่ำ
- ซื้อบริการจากบริษัทที่ให้บริการด้านศูนย์สำรอง วิธีนี้เป็นที่นิยมสำหรับบริษัทขนาดกลางที่ไม่ต้องการลงทุนสร้างศูนย์คอมพิวเตอร์สำรองเอง แต่ยังต้องการระยะเวลาการกู้ระบบที่รวดเร็ว
- ทำข้อตกลงเป็นศูนย์สำรองซึ่งกันและกันระหว่าง 2 องค์กร วิธีนี้เป็นไปได้ค่อนข้างยากในทางปฏิบัติ เพราะมีปัญหาด้านความลับของข้อมูล และทั้ง 2 องค์กร

- จะต้องมีระบบสารสนเทศ ที่คล้ายคลึงกัน และหากมีการปรับปรุงระบบสารสนเทศ ในองค์กรหนึ่ง อีกองค์กรหนึ่งก็ต้องปรับปรุงตาม

8) หลังจากมีข้อมูลสำรองและศูนย์สำรองแล้ว เราจำเป็นต้องเตรียมอีกส่วนหนึ่งที่มีความสำคัญมาก ก็คือบุคลากรและขั้นตอนการกู้ระบบสารสนเทศ ซึ่งมีข้อควรพิจารณาดังต่อไปนี้
   - มีการกำหนดทีมงานในการกู้ระบบ ซึ่งเป็นทีมงานที่จะต้องรับผิดชอบงานด้านต่าง ๆ ระหว่างการกู้ระบบ ซึ่งประกอบด้วย ผู้บริหารงานกลาง ทีมสื่อสารข้อมูลทั้งภายนอกและภายใน ทีมกู้ระบบคอมพิวเตอร์และระบบเครือข่าย ทีมกู้ระบบงานสารสนเทศและข้อมูล และทีมงานด้านอื่น ๆ ที่จำเป็น
   - กำหนดรายละเอียดการทำงานในแต่ละขั้นตอนตั้งแต่ การประเมินสถานการณ์และประกาศเหตุการณ์สุดวิสัย การรองรับเหตุการณ์เฉพาะหน้า การสื่อสารและประสานงานทั้งภายในและภายนอก การติดตั้งระบบด้านต่าง ๆ ที่ศูนย์สำรอง และการนำระบบงานกลับไปใช้ที่ศูนย์คอมพิวเตอร์หลักตามปกติ
   - ฝึกอบรมให้ทีมงานต่าง ๆ เข้าใจถึงขั้นตอนการทำงานของการกู้ระบบสารสนเทศ
9) ต้องทำการทดสอบแผนการกู้ระบบอย่างสม่ำเสมอเช่นทุกปี และมีการประเมินผลการทดสอบว่าสามารถกู้ระบบฯ กลับมาได้ภายในระยะเวลาที่กำหนดไว้หรือไม่ และทำการปรับปรุงแผนฯ ตามความจำเป็น
10) จัดให้มีระเบียบปฏิบัติในการปรับปรุงข้อมูลต่าง ๆ เช่นข้อมูลด้านการติดต่อสื่อสารข้อมูลของระบบงาน ที่จำเป็นในการกู้ระบบ ให้เป็นปัจจุบันและสอดคล้องกับระบบคอมพิวเตอร์หลัก

12. ผลกระทบจากการขาดการควบคุมทั่วไประบบสารสนเทศที่ดี

การขาดหรือมีข้อบกพร่องในการควบคุมทั่วไประบบสารสนเทศนั้นอาจส่งผลกระทบต่อการใช้ระบบสารสนเทศขององค์กรในหลายด้าน เช่น ด้านประสิทธิภาพและประสิทธิผล ด้านความปลอดภัยของข้อมูล ด้านความถูกต้องและครบถ้วน และด้านความต่อเนื่องของระบบสารสนเทศ ซึ่งสุดท้ายก็จะมีผลกระทบต่อการดำเนินธุรกิจ เช่น ทำให้รายงานทางการเงินและรายงานทางการบริหารไม่ถูกต้อง ทำให้การตัดสินใจทางธุรกิจผิดพลาดเนื่องจากข้อมูลที่ใช้ประกอบการตัดสินใจมีข้อผิดพลาด ธุรกิจหยุดชะงัก เกิดการทุจริตเนื่องจากระบบรักษาความปลอดภัยขาดความเข้มแข็งและข้อมูลสำคัญรั่วไหลทำให้เสียเปรียบในการแข่งขัน

ในส่วนนี้จะเป็นการอธิบายเพิ่มเติมในรายละเอียดในกรณีที่มีข้อบกพร่องในการควบคุมทั่วไประบบสารสนเทศในแต่ละองค์ประกอบของการควบคุมทั่วไประบบสารสนเทศ ในรูปแบบตาราง ดังต่อไปนี้

ตาราง 3.1 แสดงผลกระทบในการขาดการควบคุมทั่วไประบบสารสนเทศที่ดี

การควบคุมทั่วไประบบสารสนเทศ	ผลกระทบในการขาดการควบคุมทั่วไประบบสารสนเทศที่ดี
การควบคุมด้านการกำหนดนโยบายสารสนเทศ	ถ้าไม่มีการกำหนดนโยบายสารสนเทศที่ชัดเจน อาจส่งผลทำให้การใช้ระบบสารสนเทศไม่เป็นไปในแนวทางเดียวกัน หรือขาดระบบสารสนเทศที่สามารถเชื่อมโยงกันอย่างสมบูรณ์ ซึ่งผลกระทบส่วนใหญ่เป็นผลกระทบด้านประสิทธิภาพและประสิทธิผลของการใช้ระบบสารสนเทศ ซึ่งจะส่งผลกระทบต่อประสิทธิภาพและประสิทธิผลทางธุรกิจ
การควบคุมด้านการวางแผนงานสารสนเทศ	ถ้าขาดการวางแผนสารสนเทศที่ดี จะส่งผลทำให้แผนงานสารสนเทศและการลงทุนด้านสารสนเทศอาจไม่สอดคล้องกับวัตถุประสงค์ทางธุรกิจขององค์กร ซึ่งเป็นผลกระทบด้านประสิทธิภาพและประสิทธิผลทางธุรกิจ

การควบคุมทั่วไประบบสารสนเทศ	ผลกระทบในการขาดการควบคุมทั่วไประบบสารสนเทศที่ดี
การควบคุมด้านการจัดโครงสร้างงานสารสนเทศ	ในด้านการจัดโครงสร้างงานสารสนเทศนั้น ถือเป็นพื้นฐานในการจัดให้มีการควบคุมทั่วไประบบสารสนเทศที่ดี ดังนั้น ถ้ามีข้อบกพร่องในการจัดโครงสร้างงานสารสนเทศ โดยเฉพาะอย่างยิ่งด้านการแบ่งแยกหน้าที่งานสารสนเทศ ก็จะทำให้ไม่สามารถจัดให้มีการควบคุมที่ดีภายในองค์ประกอบต่าง ๆ ของการควบคุมทั่วไประบบสารสนเทศ เช่นถ้าไม่มีการแบ่งแยกงานระหว่างผู้ปฏิบัติการคอมพิวเตอร์และผู้พัฒนาระบบงานสารสนเทศ อาจทำให้ไม่สามารถดำเนินการควบคุมในส่วนของการพัฒนาระบบงานสารสนเทศที่ดีได้
การควบคุมด้านการพัฒนาระบบงานสารสนเทศ	ถ้าขาดการควบคุมที่ดีด้านการพัฒนาระบบงานสารสนเทศ อาจจะส่งผลทำให้ระบบงานหรือโปรแกรมที่นำมาใช้อาจขาดความถูกต้อง ซึ่งจะมีผลกระทบอย่างมากต่อความถูกต้องและครบถ้วนของรายงานทางการเงินและรายงานทางการบริหาร นอกจากนี้ยังมีผลกระทบทางด้านประสิทธิภาพและประสิทธิผลของการพัฒนาระบบสารสนเทศ เช่นระบบสารสนเทศเสร็จไม่ทันเวลา หรือใช้งบประมาณเกินกำหนด หรือระบบงานที่พัฒนาใหม่ไม่สอดคล้องกับความต้องการอย่างครบถ้วน ซึ่งในส่วนนี้เป็นผลกระทบด้านประสิทธิภาพและประสิทธิผลทางธุรกิจ ผลกระทบอีกส่วนหนึ่งในการพัฒนาระบบสารสนเทศจากการที่ไม่มีการกำหนดให้ระบบสารสนเทศที่พัฒนาใหม่นั้นมีการรักษาความปลอดภัยอย่างเพียงพอ อาจส่งผลกระทบด้านความปลอดภัยของข้อมูลในระบบสารสนเทศ หรือแม้กระทั่งอาจเกิดการทุจริตได้

การควบคุมทั่วไประบบสารสนเทศ	ผลกระทบในการขาดการควบคุมทั่วไประบบสารสนเทศที่ดี
การควบคุมด้านการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ	ข้อบกพร่องในการควบคุมการเปลี่ยนแปลงแก้ไขระบบสารสนเทศมีผลกระทบคล้ายกันกับการพัฒนาระบบงานสารสนเทศ แต่ขนาดของผลกระทบจะมากน้อยขึ้นอยู่กับขนาดของการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ แต่โดยส่วนใหญ่เป็นผลกระทบด้านความถูกต้องของโปรแกรมที่มีการแก้ไข และส่งผลกระทบต่อความถูกต้องของรายงานทางการเงินและรายงานทางการบริหาร
การควบคุมด้านการบริหารและจัดการการรักษาความปลอดภัยระบบสารสนเทศ	ในด้านการบริหารและจัดการการรักษาความปลอดภัยระบบสารสนเทศนั้นเป็นพื้นฐานเพื่อให้ระบบสารสนเทศมีความปลอดภัย ซึ่งส่วนใหญ่เป็นการกำหนดนโยบายด้านความปลอดภัย และด้านความรู้และความเข้าใจของผู้ใช้งานโดยรวม ซึ่งผลกระทบในกรณีที่ขาดนโยบายที่ดีหรือผู้ใช้งานขาดความรู้และให้ความสำคัญ จะทำให้การใช้งานไม่มีความปลอดภัย ซึ่งมีผลกระทบด้านการรั่วไหลของข้อมูลที่สำคัญ การเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่ได้รับอนุญาตซึ่งส่งผลต่อความถูกต้องของรายงานต่าง ๆ อาจทำให้เพิ่มโอกาสในการทำทุจริต และสุดท้ายอาจทำให้ระบบสารสนเทศหยุดชะงักเนื่องจากโปรแกรมที่ไม่พึงประสงค์ต่าง ๆ เช่นไวรัสคอมพิวเตอร์ โปรแกรมโทรจัน เป็นต้น
การควบคุมด้านการรักษาความปลอดภัยทางกายภาพ	ผลกระทบในการขาดการรักษาความปลอดภัยทางกายภาพที่ดีนั้น ส่วนใหญ่เป็นผลกระทบด้านความปลอดภัยของทรัพย์สิน ประสิทธิภาพของระบบสารสนเทศในกรณีห้องคอมพิวเตอร์มีสภาพแวดล้อมที่ไม่เอื้อต่อการทำงานของเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ

การควบคุมทั่วไประบบสารสนเทศ	ผลกระทบในการขาดการควบคุมทั่วไประบบสารสนเทศที่ดี
การควบคุมด้านการรักษาความปลอดภัยเชิงตรรกะ	การควบคุมด้านการรักษาความปลอดภัยเชิงตรรกะเป็นการควบคุมทางเทคนิคด้านระบบปฏิบัติการคอมพิวเตอร์ ระบบจัดการฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์ ซึ่งมุ่งเน้นไปที่การทำให้ระบบมีความปลอดภัย ดังนั้นถ้าการควบคุมในส่วนนี้มีข้อบกพร่องจะส่งผลกระทบต่อความปลอดภัยในส่วนที่เกี่ยวข้องกับการทำงาน ไม่ว่าจะเป็นระบบปฏิบัติการคอมพิวเตอร์ ระบบจัดการฐานข้อมูล หรือระบบเครือข่ายคอมพิวเตอร์ ซึ่งผลกระทบประกอบด้วยผลกระทบด้านความถูกต้องของข้อมูล ความลับรั่วไหล และระบบหยุดชะงักจากการโจมตีจากโปรแกรมที่ประสงค์ร้ายต่าง ๆ
การควบคุมด้านการประมวลผลของระบบสารสนเทศ	ถึงแม้ว่าโปรแกรมที่ใช้ในการประมวลผลถูกต้อง แต่ถ้าการประมวลผลซึ่งสั่งการโดยผู้ปฏิบัติการคอมพิวเตอร์มีข้อผิดพลาด เช่นประมวลผลผิดลำดับโปรแกรม หรือข้ามการประมวลผลบางโปรแกรมไป ก็จะทำให้การประมวลผลระบบสารสนเทศโดยรวมขาดความถูกต้อง จะส่งผลกระทบต่อความถูกต้องของข้อมูล และรายงานด้านต่าง ๆ
การควบคุมด้านการสำรองข้อมูลและการนำข้อมูลกลับมาใช้	การควบคุมในส่วนการสำรองข้อมูลและการนำข้อมูลกลับมาใช้นั้นโดยส่วนใหญ่ส่งผลกระทบต่อความต่อเนื่องและพร้อมใช้งานของระบบสารสนเทศ ซึ่งส่งผลกระทบต่อการหยุดชะงักของการดำเนินธุรกิจที่ใช้ระบบสารสนเทศเป็นกลไกสำคัญ นอกจากนี้เป็นผลกระทบด้านความถูกต้องของข้อมูลในระบบสารสนเทศ ในกรณีที่การนำข้อมูลสำรองกลับมาใช้เกิดข้อผิดพลาดขึ้น ซึ่งจะส่งผลกระทบต่อความถูกต้องของข้อมูลและรายงานต่าง ๆ

การควบคุมทั่วไประบบสารสนเทศ	ผลกระทบในการขาดการควบคุมทั่วไประบบสารสนเทศที่ดี
การควบคุมด้านการปฏิบัติการคอมพิวเตอร์ อื่น ๆ	การปฏิบัติการคอมพิวเตอร์ อื่น ๆ ซึ่งประกอบด้วยการเปิดปิดระบบสารสนเทศ การบำรุงรักษาเครื่องคอมพิวเตอร์ การจัดพิมพ์รายงาน การแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้นในการใช้ระบบสารสนเทศนั้นถ้ามีข้อบกพร่องในการควบคุม ก็จะส่งผลกระทบต่อประสิทธิภาพและประสิทธิผลในการใช้ระบบสารสนเทศ
การควบคุมด้านการบริหารจัดการข้อมูล	ในด้านการบริหารจัดการข้อมูลนั้น ผลกระทบในส่วนแรกจากการขาดประสิทธิภาพของการควบคุมที่ดี ก็คือความถูกต้องครบถ้วนของข้อมูล ซึ่งส่งผลกระทบต่อความถูกต้องของการรายงานต่าง ๆ ผลกระทบในส่วนที่สองคือผลกระทบต่อการใช้ข้อมูลเพื่อก่อให้เกิดประสิทธิภาพและประสิทธิผลต่อองค์กรในทางธุรกิจ กล่าวคือถ้าขาดข้อมูลที่มีคุณภาพหรือขาดเครื่องมือในการใช้ข้อมูลที่มีประสิทธิภาพ ก็จะทำให้การใช้ข้อมูลขาดประสิทธิภาพตามไปด้วย
การควบคุมด้านการวางแผนเพื่อกู้ระบบในกรณีเกิดความเสียหายอย่างรุนแรง	ถ้าองค์กรไม่มีการวางแผนเพื่อกู้ระบบในกรณีเกิดความเสียหายอย่างรุนแรง หรือแผนที่มีอยู่ขาดความครบถ้วนสมบูรณ์จะส่งผลกระทบต่อความต่อเนื่องในการใช้ระบบสารสนเทศในการสนับสนุนการทำงานของธุรกิจ กล่าวคือไม่สามารถกู้ระบบสารสนเทศกลับมาใช้ใหม่ได้ภายในระยะเวลาที่เหมาะสม และเมื่อองค์กรไม่สามารถกู้ระบบกลับมาได้ก็อาจส่งผลกระทบต่อความอยู่รอดขององค์กร

13. การตรวจสอบด้านการควบคุมทั่วไประบบสารสนเทศ

การตรวจสอบการควบคุมทั่วไประบบสารสนเทศนั้น เป็นการตรวจสอบเพื่อให้มั่นใจว่ามีการจัดให้มีการควบคุมอย่างเพียงพอในกระบวนการทำงานด้านสารสนเทศ และการควบคุมที่มีอยู่นั้น มีการดำเนินการอย่างมีประสิทธิผล ซึ่งหลักการหรือแนวทางการตรวจสอบการควบคุมทั่วไประบบสารสนเทศจะใช้แนวทางของการตรวจสอบแบบอิงกับความเสี่ยง (Risk Base Audit Approach) ซึ่งผู้ตรวจสอบจะต้องศึกษาทำความเข้าใจต่อความเสี่ยงและการควบคุมอย่างเพียงพอก่อนกำหนดวิธีการตรวจสอบ

ในส่วนนี้จะอธิบายการตรวจสอบด้านการควบคุมทั่วไประบบสารสนเทศ ซึ่งจะแบ่งออกเป็น 2 ส่วนดังต่อไปนี้

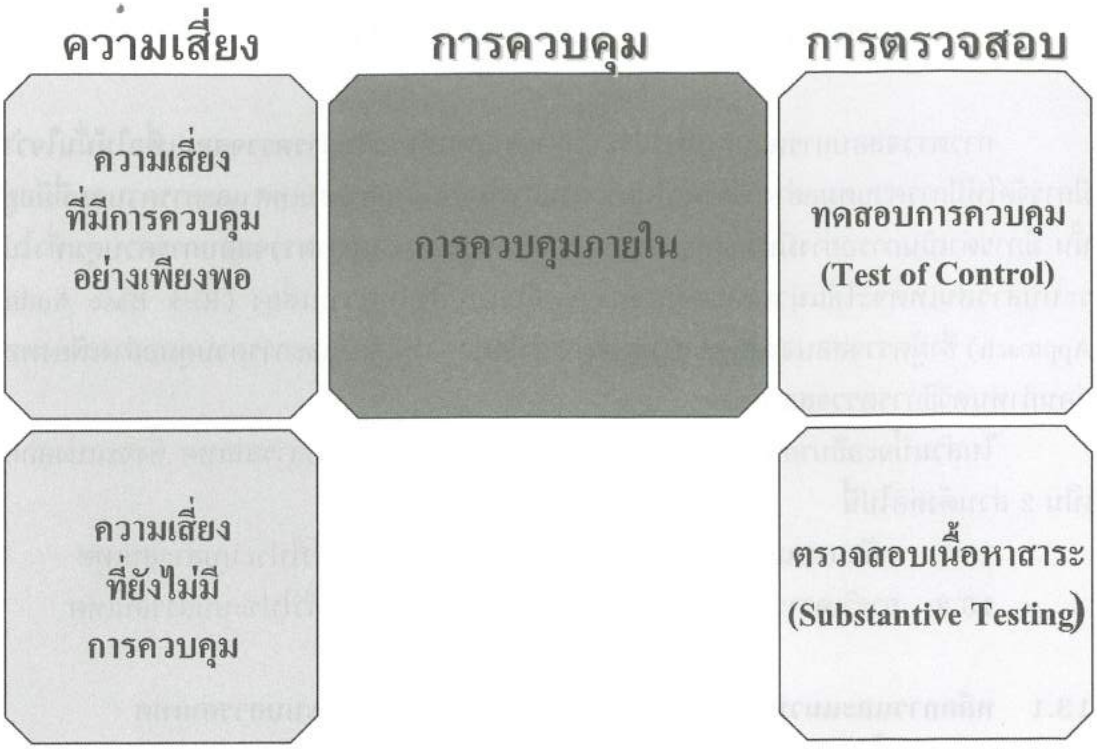
13.1 หลักการและแนวทางในการตรวจสอบการควบคุมทั่วไประบบสารสนเทศ

13.2 การวิเคราะห์และสรุปผลการตรวจสอบการควบคุมทั่วไประบบสารสนเทศ

13.1 หลักการและแนวทางในการตรวจสอบการควบคุมทั่วไประบบสารสนเทศ

หลักการพื้นฐานของการตรวจสอบแบบอิงกับความเสี่ยงนั้นสามารถสรุปเป็นคำกล่าวว่า "ผู้ตรวจสอบจำเป็นต้องมีความรู้ความเข้าใจอย่างเพียงพอต่อความเสี่ยงและการควบคุมภายในก่อนกำหนดวิธีการตรวจสอบ"

จากคำกล่าวข้างต้นเราสามารถนำมากำหนดเป็นวิธีการตรวจสอบ ซึ่งสามารถอธิบายได้ดังภาพ 3-10



ภาพ 3-10 การตรวจสอบแบบอิงกับความเสี่ยง

การตรวจสอบแบบอิงกับความเสี่ยงเริ่มต้นจากผู้ตรวจสอบทำความเข้าใจต่อความเสี่ยงของส่วนงานที่กำลังจะทำการตรวจสอบ แล้วจึงทำความเข้าใจต่อการควบคุมภายใน จากนั้นทำการวิเคราะห์ความเสี่ยงและการควบคุม โดยประเมินว่าความเสี่ยงใดมีการควบคุมที่เพียงพอ และความเสี่ยงใดยังไม่มีการควบคุมที่เพียงพอ หลังจากนั้นจึงเริ่มวางแผนการตรวจสอบโดยความเสี่ยงที่มีการควบคุมแล้วนั้นก็จะวางแผนเพื่อทดสอบประสิทธิผลของการควบคุม และถ้าผลการตรวจสอบการควบคุมไม่เป็นที่น่าพอใจ กล่าวคือการควบคุมอาจไม่มีประสิทธิผลที่น่าเชื่อถือ หรือถ้าความเสี่ยงนั้น ๆ ยังไม่มีการควบคุม ก็จะวางแผนเพื่อตรวจสอบเนื้อหาสาระ

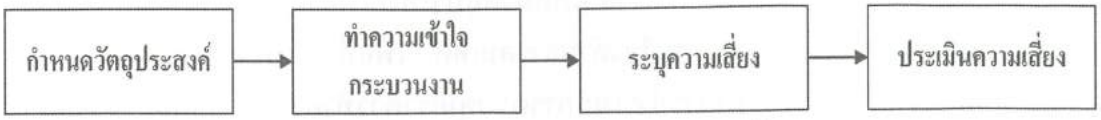
จากหลักการตรวจสอบแบบอิงกับความเสี่ยงนี้ สามารถสรุปเป็นกิจกรรมหลักที่ผู้ตรวจสอบจะต้องดำเนินการก่อนเริ่มทำการตรวจสอบคือ

13.1.1 การประเมินความเสี่ยงระบบสารสนเทศ

13.1.2 การประเมินการควบคุมระบบสารสนเทศ

ซึ่งมีรายละเอียดในการดำเนินการดังนี้

13.1.1 การประเมินความเสี่ยงระบบสารสนเทศ



ภาพ 3-11 ขั้นตอนการประเมินความเสี่ยง

การประเมินความเสี่ยงในการตรวจสอบระบบสารสนเทศนั้น สิ่งแรกที่ควรจะต้องทำความเข้าใจก็คือวัตถุประสงค์ของการตรวจสอบ ถ้าเป็นการสอบบัญชี วัตถุประสงค์ของการตรวจสอบอาจมุ่งความสำคัญให้กับความถูกต้องครบถ้วนน่าเชื่อถือของข้อมูลทางการบัญชีที่ประมวลผลด้วยระบบคอมพิวเตอร์ แต่ถ้าเป็นการตรวจสอบอื่น ๆ เช่นการตรวจสอบการปฏิบัติการ (Operational Audit) การตรวจสอบการบริหาร (Management Audit) วัตถุประสงค์ของการตรวจสอบก็จะแตกต่างกันออกไป แต่หลักการก็คือจะต้องเข้าใจวัตถุประสงค์ของการตรวจสอบเสียก่อน

หลังจากเข้าใจวัตถุประสงค์ของการตรวจสอบแล้ว ลำดับถัดไปก็เป็นการทำความเข้าใจสภาพแวดล้อมและกระบวนการทำงานของส่วนงานที่จะทำการประเมินความเสี่ยง ซึ่งจะช่วยให้เราสามารถระบุความเสี่ยงได้ตรงกับความเป็นจริงมากที่สุด และหลังจากเข้าใจสภาพแวดล้อมและกระบวนการทำงานแล้ว ลำดับถัดไปเป็นการระบุความเสี่ยงในแต่ละส่วนของกระบวนการทำงาน โดยใช้คำนิยามความเสี่ยงที่ว่า "ความเสี่ยงคือเหตุการณ์ใด ๆ ที่เกิดขึ้นแล้วส่งผลกระทบต่อการบรรลุวัตถุประสงค์" ดังนั้นถ้าเราวิเคราะห์รายละเอียดของกระบวนการทำงานในแต่ละขั้นตอน และสภาพแวดล้อมของการดำเนินงาน เราก็จะสามารถระบุความเสี่ยงในรายละเอียดได้อย่างครบถ้วน

ตัวอย่างเช่น วัตถุประสงค์ของการตรวจสอบระบบสารสนเทศคือ "เพื่อความมั่นใจว่าข้อมูลรายได้ที่นำมาลงบัญชีรวบรวมและประมวลผลอย่างถูกต้องครบถ้วน" หลังจากที่เราทำการศึกษาการบริหารงานระบบคอมพิวเตอร์ ลักษณะของระบบคอมพิวเตอร์ การดำเนินการในรายละเอียดของระบบงานคอมพิวเตอร์ที่เกี่ยวข้องกับข้อมูลรายได้แล้วเราก็สามารถระบุความเสี่ยงที่อาจจะทำให้ข้อมูลรายได้ขาดความครบถ้วนถูกต้อง เช่น การนำข้อมูลรายได้เข้าสู่ระบบอาจไม่ถูกต้อง หรือไม่ครบถ้วน และโปรแกรมที่ใช้ในการประมวลผลข้อมูลรายได้อาจไม่ถูกต้อง เป็นต้น

หลังจากที่เราสามารถระบุความเสี่ยงได้ครบถ้วนแล้ว เราต้องประเมินความเสี่ยงแต่ละความเสี่ยง ซึ่งอาจประเมินทั้งทางด้านโอกาสเกิด (Likelihood) และผลกระทบ (Impact) ซึ่งเป็นผลกระทบต่อวัตถุประสงค์ของการตรวจสอบ วัตถุประสงค์ของการประเมินความเสี่ยงก็คือการกลั่นกรองความเสี่ยง เพื่อให้การตรวจสอบมุ่งประเด็นไปที่ความเสี่ยงที่อยู่ในระดับสูงก่อน และเป็นข้อมูลสำหรับการวิเคราะห์เปรียบเทียบกับการควบคุมภายใน เพื่อระบุความเพียงพอของการควบคุม

13.1.2 การประเมินการควบคุมระบบสารสนเทศ

การประเมินการควบคุมระบบสารสนเทศมีวัตถุประสงค์เพื่อวิเคราะห์ความเพียงพอของการควบคุมภายในในการรองรับความเสี่ยงด้านสารสนเทศ เพื่อที่จะจัดทำแผนการตรวจสอบที่อิงกับความเสี่ยง ซึ่งก่อนที่จะทำการประเมินการควบคุมเราควรทำความเข้าใจต่อคำนิยามของการควบคุมเสียก่อน ซึ่งก็คือ "กระบวนการที่ดำเนินการโดยบุคลากรในองค์กรโดยมุ่งหวังที่จะเพิ่มโอกาสในการบรรลุวัตถุประสงค์ขององค์กร"

หลังจากที่ทราบวัตถุประสงค์ของการตรวจสอบ สภาพแวดล้อมของระบบสารสนเทศ กระบวนการทำงานต่าง ๆ ความเสี่ยงและระดับความเสี่ยง แล้ว เราสามารถเริ่มศึกษาการควบคุมภายในด้านสารสนเทศ ซึ่งเราทราบจากบทก่อนหน้านี้ว่าประกอบด้วยการควบคุมทั่วไป (General Controls) และการควบคุมระบบงาน (Application Control) โดยเริ่มต้นจากความเสี่ยง แล้วทำการวิเคราะห์การทำงานในส่วนต่าง ๆ ว่ามีกลไกหรือกระบวนการทำงานใดที่สามารถลดหรือจัดการความเสี่ยงดังกล่าวได้ ทั้งนี้ขึ้นอยู่กับลักษณะและระดับความเสี่ยงของแต่ละความเสี่ยง

การประเมินความเสี่ยงระดับนี้เป็นการประเมินการควบคุมตามลักษณะการออกแบบของการควบคุมนั้น ๆ (Control Design) โดยยังมิได้ทำการทดสอบประสิทธิผล และความสม่ำเสมอของการดำเนินการควบคุม โดยลักษณะการประเมินนั้นอาจประเมินจากระเบียบปฏิบัติหรือขั้นตอนการทำงานที่ถูกออกแบบไว้โดยยังมิต้องสุ่มรายการที่เกี่ยวกับการควบคุมมาตรวจสอบเพื่อประเมินประสิทธิผลของการควบคุม

ในการประเมินการควบคุมด้านสารสนเทศนั้น อาจมีความแตกต่างกันเล็กน้อยในทางเทคนิคระหว่างการประเมินการควบคุมทั่วไประบบสารสนเทศ และการประเมินการควบคุมระบบงาน ซึ่งการประเมินการควบคุมทั่วไประบบสารสนเทศนั้น ส่วนใหญ่เป็นการประเมินโดยใช้แบบสอบถามหรือแบบประเมินสำเร็จรูป (Control Questionnaire หรือ Control Checklist) ทั้งนี้เพราะการดำเนินงานด้านการควบคุมทั่วไปส่วนใหญ่จะมีขั้นตอนการทำงานที่ไม่ค่อยแตกต่างกันในแต่ละองค์กร แต่สำหรับการประเมินการควบคุมระบบงานนั้น ผู้ประเมินจะต้องทำความเข้าใจระบบงานวิเคราะห์กระบวนการทำงานแล้วจึงดำเนินการประเมินการควบคุม ทั้งนี้เพราะกระบวนการทำงานในแต่ละองค์กรอาจไม่เหมือนกัน ทั้งที่เป็นกระบวนการทำงานด้านเดียวกันและใช้ซอฟต์แวร์ยี่ห้อเดียวกัน

ผลที่ได้รับจากการประเมินความเสี่ยงและการควบคุม สามารถนำไปใช้กำหนดโปรแกรมการตรวจสอบ โดยที่ถ้าความเสี่ยงใดมีการควบคุมที่เพียงพอ ผู้ตรวจสอบก็จะวิเคราะห์การควบคุมนั้นแล้วกำหนดเป็นแนวทางหรือโปรแกรมการตรวจสอบ เพื่อทดสอบว่าการควบคุมนั้นดำเนินการอย่างสม่ำเสมอและมีประสิทธิผลหรือไม่ และสำหรับความเสี่ยงที่ไม่มีการควบคุม ผู้ตรวจสอบก็จะ

วิเคราะห์เพื่อหาวิธีการทดสอบจากรายการหรือข้อมูลจริง เพื่อที่จะค้นให้พบว่า มีความเสี่ยงเกิดขึ้นหรือไม่จากการที่ไม่มีการควบคุมที่เพียงพอ หรือความเสี่ยงที่เกิดขึ้นมีระดับความมีนัยสำคัญมากน้อยเพียงใด

13.2 การวิเคราะห์และสรุปผลการตรวจสอบการควบคุมทั่วไประบบสารสนเทศ

ในส่วนนี้จะอธิบายการวิเคราะห์และการสรุปผลการตรวจสอบการควบคุมทั่วไประบบสารสนเทศ ซึ่งจะแยกอธิบายตามองค์ประกอบของการควบคุมทั่วไประบบสารสนเทศ ดังต่อไปนี้

13.2.1 การตรวจสอบการควบคุมด้านการกำหนดนโยบายสารสนเทศ
13.2.2 การตรวจสอบการควบคุมด้านการวางแผนงานสารสนเทศ
13.2.3 การตรวจสอบการควบคุมด้านการจัดโครงสร้างงานสารสนเทศ
13.2.4 การตรวจสอบการควบคุมด้านการพัฒนาระบบงานสารสนเทศ
13.2.5 การตรวจสอบการควบคุมด้านการรักษาความปลอดภัยระบบสารสนเทศ
13.2.6 การตรวจสอบการควบคุมด้านการปฏิบัติการคอมพิวเตอร์
13.2.7 การตรวจสอบการควบคุมด้านการบริหารจัดการข้อมูล
13.2.8 การตรวจสอบการควบคุมด้านการวางแผนเพื่อกู้ระบบในกรณีเกิดความเสียหายอย่างรุนแรง

ดังมีรายละเอียดการวิเคราะห์และสรุปผลการตรวจสอบในแต่ละองค์ประกอบ ดังนี้

13.2.1 การตรวจสอบการควบคุมด้านการกำหนดนโยบายสารสนเทศ

ความเสี่ยงที่เกี่ยวข้อง

- การใช้งานหรือการดำเนินการด้านสารสนเทศอาจไม่เป็นไปในทางเดียวกัน
- ขาดแนวทางในการใช้งานระบบสารสนเทศอย่างมีประสิทธิผลและปลอดภัย

การวิเคราะห์การควบคุม

ทำความเข้าใจการกำหนดนโยบาย และวิเคราะห์ความมีอยู่ของการควบคุมต่อไปนี้

- มีการจัดทำนโยบายการใช้ระบบสารสนเทศ ซึ่งครอบคลุมการทำงานของผู้ที่เกี่ยวข้องกับระบบสารสนเทศอย่างครบถ้วน
- มีการอนุมัติและเผยแพร่นโยบายการใช้ระบบสารสนเทศอย่างเหมาะสม
- มีกระบวนการติดตามการปฏิบัติตามนโยบายอย่างสม่ำเสมอ

การตรวจสอบการควบคุม

- ตรวจสอบความมีอยู่จริงของนโยบายสารสนเทศ และสอบทานรายละเอียดของนโยบายว่าครอบคลุมการใช้งานของผู้ที่เกี่ยวข้องกับระบบสารสนเทศอย่างครบถ้วน และนโยบายจะต้องมีการระบุถึง บทบาทหน้าที่และความรับผิดชอบของแต่ละคน ระบุสิ่งที่ควรและไม่ควรปฏิบัติ และระบุบทลงโทษที่ชัดเจน
- ตรวจสอบว่ามีการอนุมัตินโยบายสารสนเทศอย่างเหมาะสม เช่นอนุมัติโดยผู้บริหารระดับสูง และตรวจสอบ ว่ามีการทำความเข้าใจให้ผู้ที่เกี่ยวข้องสามารถรับรู้และเข้าใจสาระสำคัญของนโยบายอย่างทั่วถึง เช่นมีการประกาศอย่างเป็นทางการหรือสื่อสารผ่านช่องทางการสื่อสารต่าง ๆ ขององค์กร
- ตรวจสอบความมีอยู่จริงของกระบวนการติดตามการปฏิบัติตามนโยบาย และตรวจสอบความสม่ำเสมอของการดำเนินการตามกระบวนการดังกล่าว

แนวทางการสรุปผลการตรวจสอบ

การที่จะสรุปได้ว่าการควบคุมในส่วนนี้มีความพียงพอและมีประสิทธิผลก็ต่อเมื่อ มีการกำหนดนโยบายที่ครอบคลุมการใช้งานของผู้ที่เกี่ยวข้องกับระบบสารสนเทศอย่างครบถ้วน นโยบายได้รับการอนุมัติจากผู้บริหารระดับสูงและเผยแพร่ให้ผู้ที่เกี่ยวข้องได้รับรู้และเข้าใจอย่างชัดเจน และมีการติดตามการปฏิบัติตามนโยบายอย่างสม่ำเสมอ

13.2.2 การตรวจสอบการควบคุมด้านการวางแผนงานสารสนเทศ

ความเสี่ยงที่เกี่ยวข้อง

- แผนงานและการดำเนินการด้านสารสนเทศอาจไม่สอดคล้องกับแผนงานทางธุรกิจ
- การดำเนินงานไม่เป็นไปตามแผนที่กำหนดไว้
- ระบบงานสารสนเทศอาจไม่สามารถเชื่อมโยงกันและไม่เอื้อต่อการดำเนินการอย่างมีประสิทธิภาพ

การวิเคราะห์การควบคุม

ทำความเข้าใจการวางแผนงานสารสนเทศ และวิเคราะห์ความมีอยู่ของการควบคุมต่อไปนี้

- มีการกำหนดผู้รับผิดชอบในการวางแผนอย่างชัดเจน ประกอบด้วยผู้บริหารธุรกิจและผู้บริหารสารสนเทศ

- มีการกำหนดกระบวนการที่ชัดเจนในการวางแผนงานสารสนเทศ และมีขั้นตอนการพิจารณาแผนงานทางธุรกิจประกอบการวางแผนงานสารสนเทศ
- มีการอนุมัติและเผยแพร่แผนการอย่างเหมาะสม
- มีกระบวนการติดตามความคืบหน้าของแผนอย่างสม่ำเสมอ
- มีการกำหนดมาตรฐานด้านการเชื่อมโยงกันของระบบคอมพิวเตอร์ เพื่อเป็นแนวทางในการดำเนินการด้านการพัฒนาหรือสร้างระบบงาน

การตรวจสอบการควบคุม

- ตรวจสอบว่ามีการกำหนดหน้าที่ความรับผิดชอบด้านการวางแผนงานสารสนเทศที่ชัดเจน โดยผู้ที่มีหน้าที่รับผิดชอบในการวางแผนงานสารสนเทศควรประกอบด้วยผู้บริหารสารสนเทศและผู้บริหารธุรกิจ
- สอบทานกระบวนการวางแผน เพื่อให้มั่นใจว่ากระบวนการวางแผนมีการนำแผนงานทางธุรกิจเป็นข้อมูลในการวางแผนงานสารสนเทศและแผนงานสารสนเทศครอบคลุมแผนงานด้านต่าง ๆ อย่างครบถ้วน ได้แก่ แผนงานด้านข้อมูลสารสนเทศ แผนงานด้านระบบงาน แผนงานด้านโครงสร้างพื้นฐานของระบบสารสนเทศ และแผนงานด้านบุคลากร
- ตรวจสอบว่ามีการอนุมัติแผนงานสารสนเทศอย่างเหมาะสม เช่นอนุมัติโดยคณะกรรมการสารสนเทศ (IT Steering Committee) หรืออนุมัติโดยผู้บริหารระดับสูง เป็นต้น
- สอบทานการสื่อสารและให้ความเข้าใจในแผนงานสารสนเทศ โดยตรวจสอบว่ามีการสื่อสารและทำความเข้าใจต่อแผนงานสารสนเทศต่อผู้บริหารที่มีส่วนเกี่ยวข้องกับการดำเนินงานตามแผนอย่างเพียงพอ
- สอบทานกระบวนการติดตามแผน โดยสอบทานรายงานความคืบหน้า หรือบันทึกการประชุมที่เกี่ยวกับการดำเนินงานตามแผน เพื่อให้มั่นใจว่าผู้บริหารรับรู้และติดตามการดำเนินการตามแผนอย่างสม่ำเสมอ รวมถึงการสุ่มตรวจสอบกรณีที่การดำเนินการไม่เป็นไปตามแผน เพื่อให้มั่นใจว่ามีการระบุสาเหตุและแนวทางการแก้ไขโดยผู้ที่เกี่ยวข้องอย่างเหมาะสม

แนวทางการสรุปผลการตรวจสอบ

การที่จะสรุปได้ว่าการควบคุมในส่วนนี้มีความพียงพอและมีประสิทธิผลก็ต่อเมื่อ มีการกำหนดกระบวนการวางแผนที่ชัดเจน และผู้ที่เกี่ยวข้องมีตัวแทนจากฝ่ายธุรกิจและฝ่ายสารสนเทศอย่างเหมาะสม แผนงานสารสนเทศได้รับการอนุมัติจากผู้บริหารระดับสูงและเผยแพร่ให้ผู้ที่เกี่ยวข้องได้รับรู้และเข้าใจอย่างชัดเจน และมีการติดตามผลการดำเนินการตามแผนอย่างสม่ำเสมอ

13.2.3 การตรวจสอบการควบคุมด้านการจัดโครงสร้างงานสารสนเทศ

ความเสี่ยงที่เกี่ยวข้อง

- งานสารสนเทศอาจไม่มีการแบ่งแยกหน้าที่ที่ดีส่งผลกระทบทำให้ไม่สามารถจัดให้มีการควบคุมภายในด้านสารสนเทศที่ดีได้
- งานสารสนเทศอาจถูกจัดวางในตำแหน่งที่ไม่เหมาะสม ก่อให้เกิดอุปสรรคในการประสานงานและให้บริการด้านสารสนเทศ

การวิเคราะห์การควบคุม

ทำความเข้าใจการจัดโครงสร้างงานสารสนเทศ และวิเคราะห์ความมีอยู่ของการควบคุมต่อไปนี้

- มีการแบ่งแยกงานอย่างชัดเจน โดยเฉพาะอย่างยิ่งระหว่างงานพัฒนาระบบงานกับงานปฏิบัติการคอมพิวเตอร์ ซึ่งการแบ่งแยกหน้าที่งานควรแบ่งทั้งในเชิงโครงสร้างและเชิงหน้าที่ความรับผิดชอบ
- ถ้าไม่สามารถแบ่งแยกหน้าที่งานได้อย่างชัดเจน ควรจัดให้มีการควบคุมทดแทน เช่น การสอบทานบันทึกกิจกรรมการดำเนินงานของผู้ปฏิบัติงานโดยผู้สอบทานอิสระ
- มีการจัดวางตำแหน่งงานสารสนเทศอย่างเหมาะสมโดยวิเคราะห์จากลักษณะการใช้ระบบสารสนเทศขององค์กร

การตรวจสอบการควบคุม

- สอบทานโครงสร้างงานสารสนเทศ และคำอธิบายหน้าที่งานของหน่วยงานต่าง ๆ เพื่อให้มั่นใจว่ามีการแบ่งแยกหน้าที่งานอย่างเหมาะสม ซึ่งคำนึงถึงหลักการการแบ่งแยกหน้าที่งานสารสนเทศที่สำคัญ ดังนี้
  - เจ้าหน้าที่สารสนเทศไม่ควรดำเนินการในงานที่รับผิดชอบโดยผู้ใช้งาน เช่น การนำเข้าข้อมูล และการปรับปรุงแฟ้มข้อมูลหลักของระบบงาน เป็นต้น

- งานปฏิบัติการคอมพิวเตอร์จะต้องแยกจากงานพัฒนาและเปลี่ยนแปลงแก้ไขระบบสารสนเทศ
- สอบทานการจัดวางตำแหน่งงานสารสนเทศว่าอยู่ในตำแหน่งที่เหมาะสมซึ่งสามารถให้บริการและสื่อสารกับหน่วยงานด้านผู้ใช้ระบบอย่างเหมาะสม เช่นในกรณีที่มีการใช้สารสนเทศในทุกสายงานธุรกิจ ผู้บริหารงานสารสนเทศไม่ควรรายงานโดยตรงกับผู้บริหารสายงานใดสายงานหนึ่ง แต่ควรรายงานโดยตรงกับผู้บริหารระดับสูงขึ้นไป เป็นต้น

แนวทางการสรุปผลการตรวจสอบ

การที่จะสรุปได้ว่าการควบคุมในส่วนนี้มีความพียงพอและมีประสิทธิผลก็ต่อเมื่อ มีการแบ่งแยกหน้าที่งานอย่างชัดเจน โดยเฉพาะอย่างยิ่งการแบ่งแยกหน้าที่ระหว่างผู้พัฒนาและเปลี่ยนแปลงระบบงาน กับผู้ปฏิบัติการคอมพิวเตอร์ และถ้าไม่มีการแบ่งแยกที่ชัดเจน ก็ควรมีการควบคุมทดแทน เช่นการสอบทานการทำงานโดยบุคคลอื่น สำหรับงานที่ขาดการแบ่งแยกหน้าที่

13.2.4 การตรวจสอบการควบคุมด้านการพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ

ความเสี่ยงที่เกี่ยวข้อง

- ระบบงานใหม่อาจไม่สอดคล้องกับความต้องการทางธุรกิจ
- ยังมีข้อบกพร่องภายในระบบงานใหม่หลังจากนำมาใช้งานแล้ว
- กระบวนการพัฒนาและเปลี่ยนแปลงระบบงานขาดประสิทธิภาพ ส่งผลทำให้การพัฒนาล่าช้า และใช้งบประมาณเกินจากที่กำหนด

การวิเคราะห์การควบคุม

ทำความเข้าใจการพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ และวิเคราะห์ความมีอยู่ของการควบคุมต่อไปนี้

- มีการกำหนดทีมงานผู้พัฒนาและเปลี่ยนแปลงแก้ไขระบบงาน ประกอบด้วยผู้บริหารธุรกิจและผู้บริหารสารสนเทศ
- มีการกำหนดกระบวนการพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานที่ชัดเจน ซึ่งประกอบด้วยการกำหนดเป้าหมาย ขอบเขต การรวบรวมความต้องการ การออกแบบและจัดทำ ซึ่งสอดคล้องกับความต้องการทางธุรกิจ

- มีกระบวนการทดสอบระบบงานอย่างเหมาะสม เช่น การทดสอบโปรแกรม (Unit Test) การทดสอบระบบ (Integrated Test) และการทดสอบเพื่อตรวจรับระบบโดยผู้ใช้งาน (User Acceptance Test)
- มีกระบวนการจัดเตรียมการนำระบบงานมาใช้งานอย่างเหมาะสม ครอบคลุมการเตรียมข้อมูลหรือการแปลงข้อมูล และการย้ายโปรแกรมไปใช้งานจริง
- มีกระบวนการบริหารโครงการที่มีประสิทธิภาพ ครอบคลุมการวางแผน การติดตามผลการดำเนินโครงการ การสื่อสารภายในโครงการ เป็นต้น

การตรวจสอบการควบคุม

- สุ่มเลือกโครงการพัฒนาระบบงาน หรือการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ แล้วดำเนินการตรวจสอบในประเด็นต่อไปนี้
  - ตรวจสอบการอนุมัติการริเริ่มโครงการ หรือการขอให้มีการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ ว่ามีการอนุมัติอย่างเหมาะสม เช่น การอนุมัติโดยเจ้าของระบบงาน หรือคณะกรรมการสารสนเทศ เป็นต้น
  - ตรวจสอบการกำหนดทีมงาน ว่าประกอบด้วยผู้บริหารหรือเจ้าหน้าที่ที่เกี่ยวข้องอย่างครบถ้วน เช่นการพัฒนาระบบงานสารสนเทศต้องมีผู้บริหารและเจ้าหน้าที่ในส่วนของผู้ใช้งาน และผู้บริหารด้านสารสนเทศ เป็นต้น
  - ตรวจสอบว่ามีการกำหนดหน้าที่ความรับผิดชอบของทีมงานอย่างชัดเจน
  - ตรวจสอบการดำเนินโครงการเพื่อให้มั่นใจว่า มีการกำหนดวัตถุประสงค์ที่ชัดเจน มีการสอบทานเปรียบเทียบวัตถุประสงค์กับความต้องการ มีการสอบทานเปรียบเทียบความต้องการกับการออกแบบ และมีการทดสอบโดยผู้ใช้งาน
  - สอบทานความมีอยู่จริง และความเหมาะสมของกระบวนการทดสอบ และสอบทานการดำเนินการทดสอบ เพื่อให้มั่นใจว่ามีการดำเนินการอย่างเหมาะสมครอบคลุม การวางแผนการทดสอบ การดำเนินการทดสอบ และการอนุมัติการทดสอบ
  - ตรวจสอบว่าก่อนนำระบบไปใช้งาน มีการทดสอบและรับรองผลการทดสอบโดยผู้บริหารหรือตัวแทนผู้ใช้งาน และผลการทดสอบที่ยังไม่ได้รับการยอมรับโดยผู้ใช้งาน ได้มีการดำเนินการแก้ไขและทดสอบอย่างครบถ้วนแล้ว

- ตรวจสอบการเตรียมการก่อนนำระบบงานมาใช้งาน ว่ามีการอนุมัติและดำเนินการโอนย้ายระบบงานอย่างเหมาะสม มีการสอบทานการเตรียมข้อมูลตั้งต้น หรือการถ่ายโอนจากระบบงานเก่า มีการฝึกอบรมผู้ใช้งานอย่างเพียงพอ และมีการจัดทำเอกสารประกอบระบบงานอย่างครบถ้วน
- สอบทานความเหมาะสมของกระบวนการบริหารโครงการว่ามีการดำเนินการติดตามผลการดำเนินโครงการอย่างเหมาะสม ประกอบด้วยการติดตามความคืบหน้าของโครงการ และ การบริหารงบประมาณโครงการ

แนวทางการสรุปผลการตรวจสอบ

การที่จะสรุปได้ว่าการควบคุมในส่วนนี้มีความพียงพอและมีประสิทธิผลก็ต่อเมื่อ มีการกำหนดกระบวนการพัฒนาระบบงานที่ชัดเจน และครอบคลุมกระบวนการย่อยอย่างครบถ้วนมีการทดสอบระบบงานก่อนนำมาใช้งาน และมีการกำหนดวิธีการบริหารโครงการที่มีประสิทธิภาพ

13.2.5 การตรวจสอบการควบคุมด้านการรักษาความปลอดภัยระบบสารสนเทศ

ความเสี่ยงที่เกี่ยวข้อง

- องค์กรอาจไม่มีการกำหนดนโยบายที่ชัดเจนในการรักษาความปลอดภัย ทำให้ขาดแนวทางในการดำเนินการที่ชัดเจน และทำให้ขาดแนวทางในการใช้ระบบของผู้ใช้งานระบบสารสนเทศ
- การกำหนดหน้าที่ความรับผิดชอบด้านการรักษาความปลอดภัยอาจยังไม่ชัดเจน ซึ่งอาจไม่มีการกำหนดโครงสร้างองค์กรที่ชัดเจนในด้านการรักษาความปลอดภัย และการกำหนดหน้าที่ความรับผิดชอบของเจ้าของข้อมูล เจ้าของระบบงาน ผู้บริหาร และเจ้าหน้าที่ด้านความปลอดภัยระบบสารสนเทศ ผู้ใช้งานทั่วไป
- ผู้ใช้งานอาจไม่เข้าใจถึงบทบาทหน้าที่ความรับผิดชอบอย่างชัดเจน ซึ่งอาจจะมีสาเหตุมาจากการขาดนโยบายที่ชัดเจนตามที่กล่าวมาแล้วข้างต้น หรือขาดกระบวนการทำให้เกิดความเข้าใจ เช่นการฝึกอบรม หรือการสื่อสารข้อมูลด้านนโยบายอย่างต่อเนื่องสม่ำเสมอ
- บุคลากรที่มีหน้าที่รับผิดชอบด้านการรักษาความปลอดภัยอาจขาดความรู้ความสามารถที่เพียงพอในด้านการจัดการความปลอดภัย ทั้งด้านการบริหารความปลอดภัย ความเสี่ยงด้านความปลอดภัย และความรู้ทางเทคนิคที่จำเป็น

- กระบวนการบริหารจัดการในการให้หรือยกเลิกสิทธิในการเข้าถึงระบบสารสนเทศ อาจขาดความรัดกุมเพียงพอ หรือขาดความชัดเจน ในด้านการอนุมัติ การอนุญาต หรือยกเลิกการให้เข้าถึงระบบฯ การดำเนินการ การสอบทานความถูกต้องหลังจากการดำเนินการ เป็นต้น
- ขาดกระบวนการติดตาม ตรวจสอบ และวิเคราะห์ เหตุการณ์ต่าง ๆ ที่อาจเกี่ยวข้องกับความปลอดภัยของระบบสารสนเทศ เพื่อหาแนวทางป้องกันที่เหมาะสมในอนาคต
- ไม่มีการกำหนดมาตรฐานทางเทคนิคในการติดตั้งระบบคอมพิวเตอร์และระบบเครือข่ายที่เหมาะสม เพื่อเป็นแนวทางในการกำหนดค่าตัวแปรด้านความปลอดภัยของระบบสารสนเทศ
- ระบบคอมพิวเตอร์และระบบเครือข่ายไม่ได้รับการติดตั้งให้มีการรักษาความปลอดภัยที่เพียงพอ กล่าวคือการกำหนดค่าตัวแปรด้านความปลอดภัย (Security Parameters) อาจไม่เป็นไปตามมาตรฐานการรักษาความปลอดภัยที่ดี เช่นค่าตัวแปรด้านการใช้รหัสผ่าน (Password Parameters) เช่นความยาวของรหัสผ่าน และค่าตัวแปรด้านการบันทึกกิจกรรมของระบบฯ (Audit Logging Parameters) เช่น การกำหนดระยะเวลาในการจัดเก็บ เป็นต้น
- ขาดเครื่องมือที่สำคัญในการบริหารและจัดการความปลอดภัยที่มีประสิทธิภาพ เช่น การติดตั้งไฟร์วอลล์ (Firewall) และซอฟต์แวร์ในการตรวจจับเหตุการณ์ต่าง ๆ ด้านการบุกรุกระบบคอมพิวเตอร์และระบบเครือข่าย
- การรักษาความปลอดภัยทางกายภาพยังมีข้อบกพร่อง ทั้งในด้านการออกแบบ เช่น การออกแบบสถานที่ของศูนย์คอมพิวเตอร์ การติดตั้งอุปกรณ์ด้านความปลอดภัย และอุปกรณ์เกี่ยวกับการจัดการสภาพแวดล้อมของการทำงานของระบบคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งภายในศูนย์คอมพิวเตอร์ เช่นอุปกรณ์ควบคุมอุณหภูมิ ความชื้น อุปกรณ์ป้องกันอัคคีภัย

การวิเคราะห์การควบคุม

ทำความเข้าใจการรักษาความปลอดภัยระบบสารสนเทศ และวิเคราะห์ความมีอยู่ของการควบคุมต่อไปนี้

- มีการกำหนดนโยบายการรักษาความปลอดภัยที่ชัดเจนและมีการอนุมัติ เผยแพร่และบังคับใช้อย่างเหมาะสม

- มีการกำหนดหน้าที่ความรับผิดชอบสำหรับงานด้านการรักษาความปลอดภัย ครอบคลุมทุกคนที่เกี่ยวข้อง ตั้งแต่ผู้บริหารระดับสูง ผู้บริหารสารสนเทศ รวมถึงผู้ใช้งานทั่วไป
- มีกระบวนการเผยแพร่นโยบาย และจัดให้มีการฝึกอบรมด้านการรักษาความปลอดภัยอย่างสม่ำเสมอ
- จัดให้มีการวางแผนการพัฒนาความรู้และการฝึกอบรมให้กับบุคลากรที่ทำหน้าที่รักษาความปลอดภัยระบบสารสนเทศอย่างเพียงพอ
- มีกระบวนการบริหารจัดการในการให้หรือยกเลิกสิทธิอย่างเหมาะสม
- มีกระบวนการติดตาม ตรวจสอบ และวิเคราะห์เหตุการณ์ต่าง ๆ ที่อาจเกี่ยวข้องกับความปลอดภัยระบบสารสนเทศ
- มีการกำหนดมาตรฐานทางเทคนิคในการติดตั้งระบบคอมพิวเตอร์ ระบบจัดการฐานข้อมูล และระบบเครือข่ายที่เหมาะสม เพื่อเป็นแนวทางในการกำหนดค่าตัวแปรด้านความปลอดภัยของระบบสารสนเทศ
- มีกระบวนการติดตั้งและสอบทานค่าตัวแปรด้านความปลอดภัย เพื่อให้มั่นใจว่าการติดตั้งค่าตัวแปรด้านความปลอดภัยเป็นไปตามมาตรฐานที่กำหนด
- มีการประเมินความเสี่ยงและความจำเป็นในการติดตั้งอุปกรณ์ที่จำเป็นในการรักษาความปลอดภัย และดำเนินการติดตั้งอย่างเหมาะสม
- ออกแบบศูนย์คอมพิวเตอร์โดยใช้หลักความปลอดภัย และติดตั้งอุปกรณ์ควบคุมความปลอดภัยและสภาพแวดล้อมอย่างเหมาะสมเพียงพอ

การตรวจสอบการควบคุม

- สอบทานความมีอยู่จริงของนโยบายการรักษาความปลอดภัย และสอบทานความครบถ้วนเหมาะสมของเนื้อหารายละเอียดของนโยบายโดยอาจเปรียบเทียบกับมาตรฐานต่าง ๆ เช่นมาตรฐานของ ISO 27001 หรือ กฎระเบียบภายนอกที่เกี่ยวข้อง เช่นกฎเกณฑ์ของธนาคารแห่งประเทศไทย เป็นต้น
- ตรวจสอบว่ามีการอนุมัตินโยบายการรักษาความปลอดภัยอย่างเหมาะสม ซึ่งควรเป็นผู้บริหารระดับสูงที่เป็นผู้อนุมัติ และตรวจสอบเพื่อให้มั่นใจว่ามีการเผยแพร่นโยบายการรักษาความปลอดภัยที่ครอบคลุมถึงผู้ที่เกี่ยวข้องอย่างครบถ้วน เช่นมีการประกาศใช้อย่างเป็นทางการ หรือจัดให้มีช่องทางการเข้าถึงนโยบายการรักษาความปลอดภัยผ่านทางอิเล็กทรอนิกส์อย่างเพียงพอ

- สอบทานเอกสารแสดงหน้าที่ความรับผิดชอบเช่นนโยบายการรักษาความปลอดภัย หรือเอกสารอธิบายลักษณะงาน เป็นต้น เพื่อให้มั่นใจว่ามีการกำหนดหน้าที่ความรับผิดชอบด้านการรักษาความปลอดภัยอย่างเหมาะสม โดยมีการกำหนดหน้าที่ความรับผิดชอบของ ผู้บริหารระดับสูง ผู้บริหารสายงานต่าง ๆ ทางธุรกิจ ผู้บริหารและเจ้าหน้าที่ด้านความปลอดภัยระบบสารสนเทศ ผู้บริหารสายงานสารสนเทศ เจ้าหน้าที่ด้านสารสนเทศ ผู้ใช้งานทั่วไป ผู้ตรวจสอบด้านสารสนเทศ และผู้ให้บริการด้านสารสนเทศภายนอก เป็นต้น
- สอบทานแผนงานด้านการฝึกอบรมด้านการรักษาความปลอดภัยให้กับผู้ใช้งาน และตรวจสอบอัตราการเข้ารับการอบรมตามแผนงานที่กำหนดไว้ เช่นการจัดให้มีการอบรมด้านความปลอดภัยระบบสารสนเทศประจำปี และการจัดให้มีหัวข้อด้านการรักษาความปลอดภัยระบบสารสนเทศในการอบรมพนักงานใหม่ เป็นต้น
- สอบทานแผนงานการฝึกอบรมด้านการรักษาความปลอดภัยของบุคลากร ด้านความปลอดภัยระบบสารสนเทศ และสอบทานอัตราการเข้ารับการอบรมตามแผนงานที่กำหนดไว้ ครอบคลุมผู้บริหารและเจ้าหน้าที่ด้านความปลอดภัยระบบสารสนเทศ และเจ้าหน้าที่สารสนเทศที่เกี่ยวข้อง
- สอบทานความมีอยู่จริง ของกระบวนการบริหารจัดการในการให้หรือยกเลิกสิทธิ ซึ่งกระบวนการบริหารจัดการในการให้หรือยกเลิกสิทธิควรครอบคลุม การขอสิทธิสำหรับพนักงานใหม่ การเปลี่ยนแปลงสิทธิ การเปลี่ยนแปลงรหัสผ่าน และการยกเลิกสิทธิกรณีที่พนักงานลาออกหรือเปลี่ยนแปลงหน้าที่งาน เป็นต้น
- ตรวจสอบการปฏิบัติตามกระบวนการการบริหารจัดการในการให้หรือยกเลิกสิทธิ โดยสุ่มตัวอย่างจากเอกสารการขอสิทธิ การเปลี่ยนแปลง หรือการยกเลิกสิทธิ แล้วตรวจสอบว่ามีการอนุมัติ และดำเนินการอย่างเหมาะสมและเป็นไปตามระเบียบปฏิบัติหรือไม่
- ตรวจสอบโดยการขอข้อมูลที่เกี่ยวกับสิทธิการใช้งาน เช่นรหัสผู้ใช้งาน และสิทธิของผู้ใช้งานที่กำหนดไว้ในระบบ แล้วตรวจสอบกับรายชื่อพนักงานในปัจจุบัน เพื่อดูความเหมาะสมของรหัสผู้ใช้งานและสิทธิที่กำหนดไว้
- สอบทานความมีอยู่จริง ของกระบวนการติดตาม ตรวจสอบ และวิเคราะห์ เหตุการณ์ต่าง ๆ ที่อาจเกี่ยวข้องกับความปลอดภัยระบบสารสนเทศ และตรวจสอบการดำเนินการตามกระบวนการติดตาม ตรวจสอบ และวิเคราะห์เหตุการณ์ต่าง ๆว่าดำเนินการอย่างสม่ำเสมอหรือไม่

- สอบทานความเหมาะสมของมาตรฐานทางเทคนิค ครอบคลุมมาตรฐานด้านระบบปฏิบัติการคอมพิวเตอร์ ระบบบริหารจัดการฐานข้อมูล และการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ โดยเปรียบเทียบกับมาตรฐานที่เป็นที่ยอมรับโดยทั่วไป และตรวจสอบว่ามีการอนุมัติมาตรฐานดังกล่าวอย่างเหมาะสม
- สอบทานกระบวนการการสอบทานการติดตั้งระบบคอมพิวเตอร์เพื่อให้เป็นไปตามมาตรฐาน โดยตรวจสอบว่า ในการติดตั้งหรือปรับปรุงระบบปฏิบัติการคอมพิวเตอร์ ระบบบริหารจัดการฐานข้อมูล และการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์นั้น มีการใช้มาตรฐานที่กำหนดไว้เป็นแนวทางในการติดตั้งและปรับปรุง และมีการสอบทานหลังจากการติดตั้งและปรับปรุงทุกครั้งอย่างเหมาะสม อนึ่งผู้สอบทานควรเป็นคนละคนกันกับผู้ปฏิบัติ
- ตรวจสอบด้านความปลอดภัยทางกายภาพของระบบสารสนเทศ โดย
  - สอบทานการออกแบบห้องคอมพิวเตอร์ ว่ามีความปลอดภัยเพียงพอหรือไม่ โดยมีจำนวนจุดเข้าออกที่เหมาะสม และแต่ละจุดเข้าออกจะต้องมีระบบรักษาความปลอดภัย เช่นระบบเปิดปิดประตูโดยใช้บัตรผ่านและรหัสผ่านที่ปลอดภัย
  - ตรวจสอบว่าผู้ที่ได้รับอนุญาตให้ผ่านเข้าออกห้องคอมพิวเตอร์เป็นผู้ที่มีความจำเป็นในการเข้าไปปฏิบัติหน้าที่ภายในห้องคอมพิวเตอร์ โดยเปรียบเทียบรายชื่อผู้ที่มีสิทธิเข้าออกห้องคอมพิวเตอร์ กับรายชื่อผู้ที่มีความจำเป็นในการเข้าปฏิบัติงานในห้องคอมพิวเตอร์ เป็นต้น
  - สังเกตการณ์การการติดตั้งอุปกรณ์ด้านความปลอดภัยและสภาพแวดล้อม เช่น จัดให้มีอุปกรณ์ป้องกันไฟไหม้ มีการติดตั้งระบบควบคุมไฟฟ้า และระบบไฟฟ้าสำรองที่เพียงพอ มีระบบปรับอุณหภูมิห้องคอมพิวเตอร์ เป็นต้น และตรวจสอบกระบวนการทดสอบอุปกรณ์ดังกล่าวอย่างสม่ำเสมอ

แนวทางการสรุปผลการตรวจสอบ

การที่จะสรุปได้ว่าการควบคุมในส่วนนี้มีความพียงพอและมีประสิทธิผลก็ต่อเมื่อ มีการกำหนดนโยบายและมาตรฐานด้านความปลอดภัยที่เหมาะสมและมีการอนุมัติและเผยแพร่ทำความเข้าใจกับทุกคนที่เกี่ยวข้องกับระบบสารสนเทศ มีการปรับปรุงค่าพารามิเตอร์ทางเทคนิคตามมาตรฐานอย่างครบถ้วน มีการรักษาความปลอดภัยทางกายภาพต่อระบบสารสนเทศที่สำคัญและปรับปรุงสภาพแวดล้อมของศูนย์คอมพิวเตอร์ให้เอื้อต่อการประมวลผลที่มีประสิทธิภาพ

13.2.6 การตรวจสอบการควบคุมด้านการปฏิบัติการคอมพิวเตอร์

ความเสี่ยงที่เกี่ยวข้อง

- การทำงานด้านปฏิบัติการคอมพิวเตอร์อาจเกิดข้อผิดพลาดและส่งผลกระทบต่อความถูกต้องและปลอดภัยของระบบสารสนเทศ
- การสำรองข้อมูลอาจไม่ครบถ้วน และสื่อการเก็บข้อมูลสำรองไม่ได้จัดเก็บให้มีความปลอดภัยเพียงพอ

การวิเคราะห์การควบคุม

ทำความเข้าใจการปฏิบัติการคอมพิวเตอร์ และวิเคราะห์ความมีอยู่ของการควบคุมต่อไปนี้

- มีการกำหนดขั้นตอนการปฏิบัติงานที่ชัดเจน และมีการสอบทานการปฏิบัติงานอย่างสม่ำเสมอ
- จัดให้มีการฝึกอบรมผู้ปฏิบัติการคอมพิวเตอร์อย่างเพียงพอทั้งทางด้านเทคนิคการปฏิบัติงาน เทคนิคคอมพิวเตอร์ และความรู้เกี่ยวกับระบบงาน
- มีการกำหนดขั้นตอนที่ชัดเจนในการสำรองข้อมูล
- มีการจัดเก็บสื่อสำรองข้อมูลไว้ในที่ที่ปลอดภัย ทั้งในและนอกสถานที่

การตรวจสอบการควบคุม

- สอบทานความมีอยู่จริงและความครบถ้วนเหมาะสมของขั้นตอนการปฏิบัติงาน และตรวจสอบการปฏิบัติตามขั้นตอนการปฏิบัติงานว่ามีการปฏิบัติอย่างครบถ้วนสม่ำเสมอ ซึ่งควรครอบคลุมการปฏิบัติงานในด้านต่าง ๆ ดังต่อไปนี้
  - การเปิดปิดระบบคอมพิวเตอร์ และระบบงานสารสนเทศ
  - การประมวลผลสิ้นวัน
  - การสำรองข้อมูลและการนำข้อมูลสำรองกลับมาใช้
  - การจัดพิมพ์และแจกจ่ายรายงาน
- ตรวจสอบว่ามีการสอบทานการปฏิบัติงานข้างต้นโดยผู้ควบคุมงานอย่างต่อเนื่องและสม่ำเสมอ
- สอบทานแผนงานการฝึกอบรมที่สอดคล้องกับความต้องการในการปฏิบัติการคอมพิวเตอร์ และตรวจสอบว่ามีการดำเนินการอบรมตามแผนการอบรมอย่างครบถ้วน

แนวทางการสรุปผลการตรวจสอบ

การที่จะสรุปได้ว่าการควบคุมในส่วนนี้มีความพียงพอและมีประสิทธิผลก็ต่อเมื่อ มีการกำหนดขั้นตอนการทำงานด้านการปฏิบัติการคอมพิวเตอร์ที่ชัดเจนและครอบคลุมทุกงานที่สำคัญ มีการสอบทานการปฏิบัติงานของผู้ปฏิบัติการคอมพิวเตอร์อย่างสม่ำเสมอ และมีการฝึกอบรมผู้ปฏิบัติงานอย่างสม่ำเสมอ และจัดเก็บสื่อสำรองข้อมูลไว้ในที่ที่ปลอดภัยทั้งในและนอกสถานที่

13.2.7 การตรวจสอบการควบคุมด้านการบริหารจัดการข้อมูล

ความเสี่ยงที่เกี่ยวข้อง

- ขาดผู้รับผิดชอบที่ชัดเจนในการบริหารความถูกต้องและความปลอดภัยของข้อมูล
- การรักษาความปลอดภัยอาจไม่สอดคล้องกับระดับความสำคัญของข้อมูล
- การสำรองข้อมูลอาจไม่สอดคล้องกับระดับความสำคัญของข้อมูล
- ไม่มีข้อมูลเกี่ยวกับข้อมูลสารสนเทศขององค์กรที่เพียงพอทำให้การบริหารข้อมูลสารสนเทศขององค์กรขาดประสิทธิภาพ

การวิเคราะห์การควบคุม

ทำความเข้าใจการบริหารจัดการข้อมูล และวิเคราะห์ความมีอยู่ของการควบคุมต่อไปนี้

- มีการกำหนดผู้รับผิดชอบที่ชัดเจนในการบริหารจัดการข้อมูลสารสนเทศขององค์กร
- มีการกำหนดระดับชั้นข้อมูล และแบ่งแยกข้อมูลตามระดับชั้นข้อมูลอย่างถูกต้องตามระดับความสำคัญ
- มีการกำหนดความต้องการด้านการรักษาความปลอดภัย การจัดเก็บและสำรองข้อมูล และการบริหารความถูกต้องของข้อมูลแต่ละระดับ เพื่อให้มีการบริหารด้านดังกล่าวอย่างเหมาะสม
- จัดทำโครงสร้างของข้อมูลสารสนเทศขององค์กร รวมถึงผังทางเดินของข้อมูล และคำอธิบายข้อมูล

การตรวจสอบการควบคุม

- ตรวจสอบการกำหนดเจ้าของข้อมูล ดังต่อไปนี้
  - มีการกำหนดเจ้าของข้อมูลอย่างเหมาะสม ซึ่งการกำหนดเจ้าของข้อมูลพิจารณาจากผู้มีส่วนได้เสียต่อข้อมูลนั้น ๆ

- มีการกำหนดบทบาทของเจ้าของข้อมูลอย่างชัดเจน ซึ่งอย่างน้อยควรประกอบด้วยความรับผิดชอบ ด้านความถูกต้องครบถ้วนของข้อมูล ความปลอดภัยของข้อมูล และความพร้อมใช้ของข้อมูล เป็นต้น

- ตรวจสอบการแบ่งประเภทข้อมูล ดังต่อไปนี้
  - มีการกำหนดประเภทของข้อมูลตามระดับความสำคัญอย่างเหมาะสม โดยผู้ที่กำหนดระดับความสำคัญควรเป็นผู้ที่ถูกกำหนดให้เป็นเจ้าของข้อมูลนั้น ๆ
  - มีการกำหนดความต้องการในด้านการรักษาความปลอดภัย การจัดเก็บและสำรองข้อมูลเพื่อความพร้อมใช้ และการบริหารความครบถ้วนถูกต้องของข้อมูล
  - ตรวจสอบกระบวนการติดตามว่ามีกระบวนการติดตามโดยเจ้าของข้อมูลเพื่อให้มั่นใจว่าความต้องการด้านต่าง ๆ ของข้อมูลได้รับการจัดการอย่างเหมาะสม
- ตรวจสอบการจัดทำโครงสร้างของข้อมูล ดังต่อไปนี้
  - มีการจัดทำผังโครงสร้างของข้อมูลโดยรวมขององค์กร โดยระบุ แหล่งกำเนิดข้อมูล ผังการไหลของข้อมูลจากแหล่งกำเนิดไปยังผู้ใช้ข้อมูล การจัดเก็บรักษาข้อมูล เป็นต้น

แนวทางการสรุปผลการตรวจสอบ

การที่จะสรุปได้ว่าการควบคุมในส่วนนี้มีความเพียงพอและมีประสิทธิผลก็ต่อเมื่อมีการกำหนดผู้รับผิดชอบต่อข้อมูลหรือเจ้าของข้อมูลที่ชัดเจน มีการกำหนดบทบาทของเจ้าของข้อมูลให้ครอบคลุมการดูแลด้านการรักษาความปลอดภัย การจัดเก็บและสำรองข้อมูล และการบริหารความถูกต้องของข้อมูล รวมทั้งการจัดทำโครงสร้างข้อมูลซึ่งประกอบด้วยผังทางเดินข้อมูล และคำอธิบายข้อมูล

13.2.8 การตรวจสอบการควบคุมด้านการวางแผนเพื่อกู้ระบบในกรณีเกิดความเสียหายอย่างรุนแรง

ความเสี่ยงที่เกี่ยวข้อง

- ไม่สามารถกู้ระบบสารสนเทศหรือระบบเครือข่ายได้ภายในระยะเวลาที่เหมาะสม หรืออาจไม่สามารถกู้ระบบสารสนเทศกลับมาใช้ใหม่ได้เลย เนื่องจาก ไม่มีการสำรองข้อมูลหรือสำรองข้อมูลไม่ครบถ้วน และไม่มีระบบคอมพิวเตอร์หรือระบบเครือข่ายสำรองที่สามารถกู้ระบบได้ภายในระยะเวลาที่เหมาะสม

- บุคลากรที่มีหน้าที่กู้ระบบอาจขาดความเข้าใจในขั้นตอนการดำเนินการ
- อาจเกิดอุบัติเหตุหรืออุบัติภัยทำให้เกิดผลเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่าย ทำให้ธุรกิจหยุดชะงัก
- ระบบสารสนเทศอาจหยุดชะงัก เนื่องจากขาดการบำรุงรักษาระบบคอมพิวเตอร์และระบบเครือข่ายทำให้ระบบคอมพิวเตอร์ หรือระบบเครือข่ายขัดข้อง

การวิเคราะห์การควบคุม

ทำความเข้าใจการวางแผนเพื่อกู้ระบบในกรณีเกิดความเสียหายอย่างรุนแรง และวิเคราะห์ความมีอยู่ของการควบคุมต่อไปนี้

- จัดทำแผนที่สอดคล้องกับความเสี่ยงและผลกระทบเพื่อกู้ระบบกลับมาใช้ใหม่ภายในระยะเวลาที่เหมาะสม ทดสอบและปรับปรุงแผนให้ทันสมัยอย่างสม่ำเสมอ
- อบรมให้ผู้ที่มีหน้าที่กู้ระบบสารสนเทศมีความเข้าใจในขั้นตอนการกู้ระบบอย่างเพียงพอ และสม่ำเสมอ
- มีการซ้อมการกู้แผนอย่างสม่ำเสมอ
- จัดให้มีระบบป้องกันและการออกแบบที่เผื่อเหลือเผื่อขาด
- จัดให้มีกระบวนการบำรุงรักษาอุปกรณ์อย่างสม่ำเสมอ ตั้งแต่การกำหนดแผนการดำเนินการ เป็นต้น

การตรวจสอบการควบคุม

- สอบทานความมีอยู่จริงและความครบถ้วนเหมาะสมของแผนกู้ระบบสารสนเทศ โดยตรวจสอบดังต่อไปนี้
  - มีกระบวนการจัดทำแผนอย่างเหมาะสม โดยจะต้องมีการประเมินผลกระทบต่อธุรกิจในกรณีที่เกิดเหตุการณ์ที่ทำให้ระบบหยุดชะงัก และการกำหนดเป้าหมายด้านระยะเวลาที่จะต้องนำระบบกลับมาใช้ใหม่ และการกำหนดขั้นตอนการกู้ระบบ จะต้องสอดคล้องกับเป้าหมายที่กำหนดไว้
  - รายละเอียดของแผนกู้ระบบสารสนเทศควรจะครอบคลุมเรื่องต่าง ๆ อย่างครบถ้วน เช่น ขั้นตอนการประเมินและประกาศเหตุการณ์ การสื่อสารระหว่างเกิดเหตุการณ์ การจัดการเหตุการณ์ฉุกเฉิน ขั้นตอนการกู้ระบบ การทดสอบและปรับปรุงแผนกู้ระบบสารสนเทศ เป็นต้น

- ตรวจสอบว่ามีการฝึกอบรมสำหรับผู้ที่มีหน้าที่กู้ระบบสารสนเทศอย่างเพียงพอและสม่ำเสมอซึ่งผู้ที่ถูกระบุไว้เป็นผู้ที่จะต้องปฏิบัติงานตามขั้นตอนต่าง ๆ ตามที่ระบุไว้ในแผนการกู้ระบบสารสนเทศ จะต้องได้รับการฝึกอบรมตามขั้นตอนต่าง ๆ อย่างครบถ้วน และสม่ำเสมอ เช่นอย่างน้อยปีละครั้ง เป็นต้น
- ตรวจสอบว่ามีการทดสอบแผนการกู้ระบบสารสนเทศอย่างสม่ำเสมอ และสอบทานผลการทดสอบว่าเป็นไปตามเป้าหมายที่กำหนดไว้หรือไม่ และในกรณีที่จะต้องมีการปรับปรุงแผนหลังการทดสอบ ให้ตรวจสอบเพิ่มเติมว่ามีการดำเนินการปรับปรุงแผนกู้ระบบสารสนเทศตามที่ระบุไว้หรือไม่
- ตรวจสอบว่ามีแผนการสอบทานและปรับปรุงแผนให้ทันสมัยอย่างสม่ำเสมอ เช่น ปีละครั้งหรือไม่ และสุ่มตรวจสอบข้อมูลที่ระบุไว้ในแผน เช่นบุคลากรที่กำหนดในแผน หรือข้อมูลการติดต่อกับบุคลากรดังกล่าว โดยเปรียบเทียบกับข้อมูลปัจจุบันว่าสอดคล้องตรงกันหรือไม่
- สอบทานระบบป้องกัน และสอบทานการออกแบบเพื่อหลีกเลี่ยงจุดล่อแหลมที่เมื่อเกิดปัญหาจะทำให้หยุดชะงักทั้งระบบ (Single Point of Failure)
- สอบทานการมีอยู่ของกระบวนการบำรุงรักษาอุปกรณ์คอมพิวเตอร์และเครือข่าย และสอบทานการปฏิบัติการตามกระบวนการการบำรุงรักษาอุปกรณ์คอมพิวเตอร์และเครือข่าย ว่ามีการดำเนินการอย่างต่อเนื่องสม่ำเสมอหรือไม่

แนวทางการสรุปผลการตรวจสอบ

การที่จะสรุปได้ว่าการควบคุมในส่วนนี้มีความเพียงพอและมีประสิทธิผลก็ต่อเมื่อมีการกำหนดแผนกู้ระบบสารสนเทศที่สอดคล้องกับความต้องการทางธุรกิจ มีการฝึกอบรมให้ผู้กู้ระบบอย่างเพียงพอ และมีการทดสอบแผนกู้ระบบอย่างสม่ำเสมอ รวมทั้งมีการออกแบบที่เหมาะสมและการบำรุงรักษาเครื่องคอมพิวเตอร์และระบบเครือข่ายอย่างสม่ำเสมอ

14. บทสรุป

การควบคุมทั่วไปในระบบสารสนเทศนั้นเป็นการควบคุมภายในกระบวนการทำงานด้านสารสนเทศ ซึ่งไม่ได้เฉพาะเจาะจงว่าเป็นการควบคุมระบบงาน (Application Controls) ใด ซึ่งการควบคุมทั่วไปนั้นเป็นการควบคุมที่อยู่ในความรับผิดชอบของผู้บริหารสารสนเทศ และผู้บริหารระดับสูง และส่วนใหญ่อยู่ในกระบวนงานในฝ่ายสารสนเทศ

การควบคุมทั่วไปในระบบสารสนเทศมีวัตถุประสงค์เพื่อให้มั่นใจว่าการดำเนินการด้านสารสนเทศนั้น สามารถตอบสนองต่อความต้องการด้านสารสนเทศโดยรวมขององค์กร ซึ่งความต้องการขององค์กรประกอบด้วยความต้องการด้านประสิทธิภาพและประสิทธิผลของการดำเนินงาน (Efficiency and Effectiveness) ความปลอดภัยของข้อมูลและระบบสารสนเทศ (Security and Confidentiality) ความถูกต้องครบถ้วนของข้อมูล (Integrity) หรือความพร้อมใช้ของข้อมูลและระบบสารสนเทศ (Availability)

การควบคุมทั่วไประบบสารสนเทศ ซึ่งเน้นที่การใช้งานโดยรวมขององค์กรนั้น ประกอบด้วย

- การกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานสารสนเทศ
- การพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ
- การรักษาความปลอดภัยระบบสารสนเทศ
- การปฏิบัติการคอมพิวเตอร์
- การบริหารจัดการข้อมูล
- การวางแผนเพื่อกู้ระบบสารสนเทศ ในกรณีที่เกิดความเสียหายอย่างรุนแรง

ความเสี่ยงที่สำคัญในแต่ละองค์ประกอบของการควบคุมทั่วไประบบสารสนเทศ มีดังต่อไปนี้

- **ด้านการกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานสารสนเทศ** เพื่อรองรับความเสี่ยงเกี่ยวกับการใช้งานที่ไม่สอดคล้องกัน แผนงานสารสนเทศอาจไม่สอดคล้องกับแผนงานทางธุรกิจ และการแบ่งแยกงานที่ไม่ชัดเจนของงานสารสนเทศ
- **ด้านการพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ** เพื่อรองรับความเสี่ยงเกี่ยวกับ ความไม่ถูกต้องของการทำงานของโปรแกรมในระบบงานต่าง ๆ ระบบงานที่พัฒนาหรือเปลี่ยนแปลงใหม่อาจไม่สอดคล้องกับความต้องการขององค์กร และประสิทธิภาพของการพัฒนาระบบงาน

- **ด้านการรักษาความปลอดภัยระบบสารสนเทศ** เพื่อรองรับความเสี่ยงเกี่ยวกับการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูล และการโจมตีจากโปรแกรมที่ประสงค์ร้าย
- **ด้านการปฏิบัติการคอมพิวเตอร์** เพื่อรองรับความเสี่ยงเกี่ยวกับความไม่ถูกต้องและประสิทธิภาพของงานปฏิบัติการคอมพิวเตอร์ ซึ่งประกอบด้วย การประมวลผลโปรแกรม การสำรองข้อมูลและนำข้อมูลกลับมาใช้ และการปฏิบัติงานด้านอื่น ๆ เช่น การเปิดปิดระบบสารสนเทศ การจัดการปัญหาด้านการใช้ระบบสารสนเทศ และการบำรุงรักษาเครื่องคอมพิวเตอร์
- **ด้านการบริหารจัดการข้อมูล** เพื่อรองรับความเสี่ยงเกี่ยวกับ ความไม่ถูกต้องของข้อมูล และการรักษาความปลอดภัยที่ไม่สอดคล้องกับระดับความสำคัญของข้อมูล
- **ด้านการวางแผนเพื่อกู้ระบบสารสนเทศ ในกรณีที่เกิดความเสียหายอย่างรุนแรง** เพื่อรองรับความเสี่ยงเกี่ยวกับการหยุดชะงักของระบบสารสนเทศซึ่งส่งผลกระทบทำให้ธุรกิจหยุดชะงัก

และเพื่อจัดการความเสี่ยงข้างต้น ผู้บริหารมีหน้าที่ในการจัดให้มีการควบคุมทั่วไประบบสารสนเทศนั้น ซึ่งสามารถสรุปได้ดังนี้

- **ด้านการกำหนดนโยบาย การวางแผนงาน และการจัดโครงสร้างงานสารสนเทศ** โดยการจัดทำ อนุมัติ และเผยแพร่นโยบายสารสนเทศ เพื่อเป็นกรอบการใช้งานระบบสารสนเทศโดยรวม และจัดให้มีกระบวนการวางแผนและผู้มีส่วนร่วมในการวางแผน เพื่อทำให้มั่นใจว่าแผนสารสนเทศและแผนธุรกิจมีความสอดคล้องกัน และจัดให้มีการแบ่งแยกงานสารสนเทศอย่างเหมาะสมโดยเฉพาะอย่างยิ่งการแบ่งแยกงานพัฒนาระบบงานสารสนเทศออกจากงานปฏิบัติการคอมพิวเตอร์
- **ด้านการพัฒนาและเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ** โดยกำหนดกระบวนการพัฒนาและแก้ไขเปลี่ยนแปลงระบบงานที่ชัดเจน รวมทั้งกระบวนการบริหารโครงการพัฒนาระบบงานอย่างมีประสิทธิภาพ ซึ่งสิ่งที่ควรเน้นเป็นพิเศษคือการทดสอบโปรแกรมก่อนนำมาใช้งาน
- **ด้านการรักษาความปลอดภัยระบบสารสนเทศ** โดยการกำหนดนโยบายด้านการรักษาความปลอดภัย กำหนดระเบียบปฏิบัติ และสร้างสำนึกด้านความปลอดภัยที่ดีกับผู้ใช้งาน การกำหนดค่าพารามิเตอร์ทางเทคนิคให้สอดคล้องกับมาตรฐานการรักษาความปลอดภัยที่ดี และจัดให้มีการรักษาความปลอดภัยทางกายภาพสำหรับศูนย์คอมพิวเตอร์

- **ด้านการปฏิบัติการคอมพิวเตอร์** โดยการกำหนดขั้นตอนการทำงานที่ชัดเจน สอบทานการปฏิบัติตามขั้นตอนอย่างสม่ำเสมอ และฝึกอบรมให้กับผู้ปฏิบัติการคอมพิวเตอร์อย่างเพียงพอ
- **ด้านการบริหารจัดการข้อมูล** โดยการกำหนดให้มีผู้รับผิดชอบต่อข้อมูลที่ชัดเจน และมีการจัดประเภทของข้อมูลตามระดับความสำคัญ และจัดทำโครงสร้างข้อมูลขององค์กร เพื่อเป็นข้อมูลที่ใช้ในการบริหารจัดการด้านข้อมูล
- **ด้านการวางแผนเพื่อกู้ระบบสารสนเทศ ในกรณีที่เกิดความเสียหายอย่างรุนแรง** โดยการจัดทำแผนกู้ระบบสารสนเทศที่สามารถกู้ระบบภายในระยะเวลาที่เหมาะสม สอดคล้องกับความต้องการขององค์กร และจัดให้มีการทดสอบแผนงานอย่างสม่ำเสมอ

ส่วนสุดท้ายของบทนี้คือการตรวจสอบการควบคุมทั่วไป ซึ่งใช้หลักการการตรวจสอบแบบอิงกับความเสี่ยง ซึ่งผู้ตรวจสอบจะต้องทำความเข้าใจและประเมินความเสี่ยงและการควบคุมด้านการควบคุมทั่วไประบบสารสนเทศอย่างเพียงพอก่อนกำหนดวิธีการตรวจสอบ ซึ่งระหว่างการตรวจสอบนั้นผู้ตรวจสอบจะทำการทดสอบความมีอยู่จริงของการควบคุม และทดสอบประสิทธิภาพของการควบคุมดังกล่าว

15. แบบฝึกหัดปรนัย และแนวคำตอบ

15.1 แบบฝึกหัดปรนัย

1. ข้อใดมิใช่ การแบ่งแยกหน้าที่งานสารสนเทศที่ดี
   ก. การแบ่งแยกหน้าที่งานพัฒนาระบบงาน และ งานปฏิบัติการคอมพิวเตอร์
   ข. การแบ่งแยกหน้าที่งานการรักษาความปลอดภัย และ งานพัฒนาระบบงาน
   ค. การแบ่งแยกหน้าที่งานการรักษาความปลอดภัย และงานปฏิบัติการคอมพิวเตอร์
   ง. การแบ่งแยกหน้าที่งานพัฒนาระบบงาน และงานการเปลี่ยนแปลงระบบงาน

2. ในลักษณะองค์กรที่ยังไม่มีการใช้ระบบสารสนเทศและธุรกรรมส่วนใหญ่เกิดขึ้นในสำนักงานใหญ่ ท่านคิดว่าการนำระบบงานใหม่มาใช้ลักษณะใดมีความเหมาะสมมากที่สุด
   ก. การนำระบบงานใหม่มาใช้ใหม่แบบ คู่ขนาน (Parallel Implementation)
   ข. การนำระบบงานใหม่มาใช้ใหม่แบบ ทดแทนทันที (Cut-Off Implementation)
   ค. การนำระบบงานใหม่มาใช้ใหม่แบบ ทีละส่วนขององค์กร (Pilot Implementation)
   ง. การนำระบบงานใหม่มาใช้ใหม่แบบ ทีละส่วนของระบบ (Phase Implementation)

3. ในกระบวนการพัฒนาระบบงานนั้น ขั้นตอนใดเป็นขั้นตอนที่สำคัญที่สุดในการทำให้มั่นใจว่าระบบงานที่พัฒนาตรงกับความต้องการของผู้ใช้งาน
   ก. การทดสอบเพื่อตรวจรับระบบโดยผู้ใช้งาน
   ข. การรวบรวมความต้องการของผู้ใช้งาน เทียบกับวัตถุประสงค์
   ค. การออกแบบให้ครอบคลุมความต้องการทั้งหมด
   ง. การกำหนดวัตถุประสงค์และสื่อสารให้ทุกคนในโครงการ

4 การกำหนดให้มีการควบคุมความลับของ Password เช่นการกำหนดความยาวขั้นต่ำ และการกำหนดอายุการใช้งาน เป็นการควบคุมประเภทใด
   ก. การควบคุมเชิงป้องกัน (Preventive Control)
   ข. การควบคุมเชิงตรวจพบ(Detective Control)
   ค. การควบคุมเชิงแก้ไข(Corrective Control)
   ง. การควบคุมแบบผสมผสานกัน

5. งานใดที่มิใช่งานในหน้าที่ของผู้ปฏิบัติการคอมพิวเตอร์
   ก. การประมวลผลรายการ ณ สิ้นวัน
   ข. การสำรองข้อมูล
   ค. การแก้ไขปัญหาด้านระบบสารสนเทศ
   ง. การบำรุงรักษาระบบคอมพิวเตอร์

6. ในการตรวจสอบแบบอิงกับความเสี่ยง (Risk-Based Audit Approach) นั้นผู้ตรวจสอบให้ความสำคัญกับกรณีใดเป็นพิเศษ
   ก. ความเสี่ยงทุกความเสี่ยงจะต้องมีการควบคุมเสมอ
   ข. การตรวจสอบจะต้องขึ้นอยู่กับระดับการควบคุมภายในที่มีอยู่
   ค. การตรวจสอบจะต้องขึ้นอยู่กับระดับความเสี่ยงที่มีอยู่
   ง. ผู้ตรวจสอบจะต้องเข้าใจความเสี่ยงและการควบคุมก่อนกำหนดวิธีการตรวจสอบ

7. ในกระบวนการทำงานของผู้ปฏิบัติการคอมพิวเตอร์ กระบวนการใดที่มีผลต่อความถูกต้องของข้อมูลมากที่สุด
   ก. การประมวลผลข้อมูล
   ข. การสำรองข้อมูล
   ค. การพิมพ์ และจัดส่งรายงาน
   ง. การย้ายโปรแกรม

8. ข้อใดเป็นผลกระทบที่น้อยที่สุดจากความเสี่ยงที่เกี่ยวกับการควบคุมด้านการปฏิบัติการคอมพิวเตอร์
   ก. การทำงานทางธุรกิจขาดประสิทธิภาพ
   ข. ข้อมูลและรายงานทางการเงินอาจไม่ถูกต้อง
   ค. ข้อมูลที่สำคัญรั่วไหล
   ง. ธุรกิจหยุดชะงัก

9. ข้อใดต่อไปนี้ที่มิใช่การควบคุมทั่วไปของระบบคอมพิวเตอร์สารสนเทศ (Computer General Controls)
   ก. การจัดโครงสร้างงานคอมพิวเตอร์
   ข. การแบ่งแยกงานภายในระบบงานต่าง ๆ
   ค. การเปลี่ยนแปลงแก้ไขโปรแกรม
   ง. การจัดทำแผนรองรับเหตุการณ์ฉุกเฉิน

10. ผู้ที่มีความรับผิดชอบ **โดยตรง** ในการจัดให้มีนโยบายการรักษาความปลอดภัยระบบสารสนเทศ คือ
   ก. ผู้บริหารระดับสูง
   ข. ผู้บริหารความปลอดภัย (Security Officer)
   ค. ผู้ดำเนินการด้านการรักษาความปลอดภัย (Security Administrator)
   ง. ผู้บริหารงานสารสนเทศ

แนวคำตอบ

1. ง
2. ง
3. ก
4. ก
5. ค
6. ง
7. ก
8. ค
9. ข
10. ก

16. แบบฝึกหัดอัตนัย และแนวคำตอบ

ข้อ 1 ข้อบกพร่องในการควบคุมทั่วไประบบสารสนเทศส่วนใดบ้างที่มีผลกระทบต่อความถูกต้องของรายงานทางการเงิน พร้อมอธิบายพอสังเขป

ข้อ 2 ในการพัฒนาระบบงานสารสนเทศนั้น ควรกำหนดให้มีการควบคุมขั้นตอนใดบ้าง

แนวคำตอบ

ข้อ 1 ข้อบกพร่องในการควบคุมทั่วไปในส่วนต่อไปนี้ มีผลกระทบต่อความถูกต้องของรายงานทางการเงิน

การควบคุมทั่วไประบบสารสนเทศ	ผลกระทบในการขาดการควบคุมทั่วไประบบสารสนเทศที่ดี
การควบคุมด้านการพัฒนาระบบงานสารสนเทศ	ถ้าขาดการควบคุมที่ดีด้านการพัฒนาระบบงานสารสนเทศ อาจจะส่งผลทำให้ระบบงานหรือโปรแกรมที่นำมาใช้อาจขาดความถูกต้อง ซึ่งจะมีผลกระทบอย่างมากต่อความถูกต้องและครบถ้วนของรายงานทางการเงินและรายงานทางการบริหาร
การควบคุมด้านการเปลี่ยนแปลงแก้ไขระบบงานสารสนเทศ	ข้อบกพร่องในการควบคุมการเปลี่ยนแปลงแก้ไขระบบสารสนเทศมีผลกระทบต่อความถูกต้องของโปรแกรมที่มีการแก้ไข และส่งผลกระทบต่อความถูกต้องของรายงานทางการเงินและรายงานทางการบริหาร
การควบคุมด้านการบริหารและจัดการการรักษาความปลอดภัยระบบสารสนเทศ	ผลกระทบในกรณีที่ขาดนโยบายที่ดีหรือผู้ใช้งานขาดความรู้และให้ความสำคัญ จะทำให้การใช้งานไม่มีความปลอดภัย ซึ่งมีผลกระทบด้านการรั่วไหลของข้อมูลที่สำคัญ การเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่ได้รับอนุญาตซึ่งส่งผลต่อความถูกต้องของรายงานต่าง ๆ

การควบคุมทั่วไประบบสารสนเทศ	ผลกระทบในการขาดการควบคุมทั่วไประบบสารสนเทศที่ดี
การควบคุมด้านการรักษาความปลอดภัยเชิงตรรกะ	การควบคุมด้านการรักษาความปลอดภัยเชิงตรรกะเป็นการควบคุมทางเทคนิคด้านระบบปฏิบัติการคอมพิวเตอร์ ระบบจัดการฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์ ซึ่งมุ่งเน้นไปที่การทำให้ระบบมีความปลอดภัย ดังนั้นถ้าการควบคุมในส่วนนี้มีข้อบกพร่องจะส่งผลกระทบต่อความปลอดภัยในส่วนที่เกี่ยวข้องกับการทำงานของส่วนนั้น ๆ ไม่ว่าจะเป็นระบบปฏิบัติการคอมพิวเตอร์ ระบบจัดการฐานข้อมูล หรือระบบเครือข่ายคอมพิวเตอร์ ซึ่งผลกระทบประกอบด้วยผลกระทบด้านความถูกต้องของข้อมูล ความลับรั่วไหล และระบบหยุดชะงักจากการโจมตีจากโปรแกรมที่ประสงค์ร้ายต่าง ๆ
การควบคุมด้านการประมวลผลของระบบสารสนเทศ	ถึงแม้ว่าโปรแกรมที่ใช้ในการประมวลผลถูกต้อง แต่ถ้าการประมวลผลซึ่งสั่งการโดยผู้ปฏิบัติการคอมพิวเตอร์มีข้อผิดพลาด เช่นประมวลผลผิดลำดับโปรแกรม หรือข้ามการประมวลผลบางโปรแกรมไป ก็จะทำให้การประมวลผลระบบสารสนเทศโดยรวมขาดความถูกต้อง จะส่งผลกระทบต่อความถูกต้องของข้อมูล และรายงานด้านต่าง ๆ
การควบคุมด้านการสำรองข้อมูลและการนำข้อมูลกลับมาใช้	ในกรณีที่การนำข้อมูลสำรองกลับมาใช้เกิดข้อผิดพลาดเกิดขึ้น จะส่งผลกระทบต่อความถูกต้องของข้อมูลและรายงานต่าง ๆ
การควบคุมด้านการบริหารจัดการข้อมูล	ในด้านการบริหารจัดการข้อมูลนั้น ผลกระทบในส่วนแรกจากการขาดประสิทธิผลของการควบคุมที่ดีนั้น ก็คือความถูกต้องครบถ้วนของข้อมูล ซึ่งส่งผลกระทบต่อความถูกต้องของการรายงานต่าง ๆ

ข้อ 2 ในการพัฒนาระบบงานสารสนเทศนั้น ควรกำหนดให้มีการควบคุมในขั้นตอนต่อไปนี้

- **ขั้นตอนการรวบรวมรายละเอียด (Analysis)** ขั้นตอนนี้เป็นขั้นตอนในการรวบรวมความต้องการของระบบงานใหม่ (System Requirements) ซึ่งการควบคุมที่สำคัญคือการจัดให้มีกลไกในการรวบรวมความต้องการของระบบที่ชัดเจน และต้องครอบคลุมความต้องการทั้งทางธุรกิจ และความต้องการด้านการควบคุม โดยควรที่จะจัดให้มีการสอบทานความต้องการดังกล่าวเพื่อให้มั่นใจว่าความต้องการนั้น ๆ สอดคล้องกับวัตถุประสงค์ของระบบงานใหม่
- **ขั้นตอนการออกแบบระบบงาน (Design)** ในขั้นตอนนี้เป็นการนำความต้องการของระบบงานใหม่มาออกแบบเป็นระบบสารสนเทศ ซึ่งการควบคุมที่จำเป็นต้องมีก็คือการสอบทานเพื่อให้มั่นใจว่าความต้องการที่รวบรวมไว้ในขั้นตอนก่อนหน้านี้ ได้รับการออกแบบอย่างถูกต้อง และครอบคลุมทั้งความต้องการทางธุรกิจ และความต้องการด้านการควบคุม
- **ขั้นตอนการจัดทำระบบงาน (Construction)** เป็นขั้นตอนการดำเนินการสร้างระบบสารสนเทศ ซึ่งในขั้นตอนนี้การควบคุมที่สำคัญคือการทดสอบระบบที่จัดทำขึ้นมาใหม่ เพื่อให้ความมั่นใจว่า ความต้องการที่กำหนดโดยผู้ใช้งานนั้น นำมาออกแบบและสร้างอย่างครบถ้วนและถูกต้อง ซึ่งการสร้างระบบอาจเป็นการสร้างขึ้นมาใหม่ทั้งหมด หรือเป็นการนำซอฟต์แวร์สำเร็จรูปมาดัดแปลงเพื่อให้สอดคล้องกับแบบที่ออกไว้ก็ได้
- **ขั้นตอนการทดสอบระบบงาน (Testing)** ขั้นตอนนี้เป็นขั้นตอนที่สำคัญ ประกอบด้วยการทดสอบโดยผู้สร้างระบบเพื่อให้มั่นใจว่าระบบทำงานอย่างถูกต้อง และการทดสอบโดยผู้ใช้งาน เพื่อตรวจรับและรับรองว่าระบบทำงานได้ตรงกับความต้องการของผู้ใช้งาน
- **ขั้นตอนการเตรียมความพร้อมเพื่อนำมาใช้งาน (Implementation)** เป็นขั้นตอนการนำระบบมาใช้งาน โดยมีการควบคุมที่สำคัญคือ ต้องมีการอนุมัติการโอนย้ายระบบไปใช้งานหลังจากผลการทดสอบขั้นสุดท้ายเป็นที่พอใจของเจ้าของระบบแล้ว การโอนย้ายระบบสารสนเทศ ก็ควรทำภายใต้การควบคุมที่เข้มงวดเพื่อให้มั่นใจว่าโปรแกรมที่นำไปใช้งานเป็นโปรแกรมเดียวกันกับโปรแกรมที่ได้รับการทดสอบ และต้องมีการจัดทำเอกสารประกอบระบบงานอย่างครบถ้วนสมบูรณ์ก่อนนำระบบมาใช้งานจริง และจัดให้มีการสอบทานเพื่อทำให้มั่นใจว่าความต้องการทั้งทางด้านธุรกิจและด้านการควบคุม นั้นได้มีการนำมาปฏิบัติจริง นอกจากนี้ยังเป็นการเตรียมความพร้อมของระบบ เช่นการโอนถ่ายข้อมูลจากระบบงานเดิม (Data Conversion) หรือการเตรียมข้อมูลตั้งต้น รวมทั้งการฝึกอบรมผู้ใช้งาน

17. บรรณานุกรมบท

ณฐพร พันธุ์อุดม และคณะ. 2549. แนวทางการควบคุมภายในที่ดี. ตลาดหลักทรัพย์แห่งประเทศไทย

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

The IT Governance Institute Committee and COBIT Steering Committee. 2000. **COBIT 3rd Edition – Control Objectives.** n.p.

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

James A. Hall and Tommie Singleton. August 2004. **Information Technology Auditing and Assurance 2nd edition.** South-Western Publishing

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