บทที่ 9

การควบคุมระบบสารสนเทศ

(Controls in Information Systems)

เนื้อหาภายในบท

9.1 บททนำ

9.2 การควบคุมระบบสารสนเทศ

สิ่งที่ต้องควบคุมในระบบสารสนเทศ

9.3 โครงสร้างการควบคุม

การควบคุมสภาพแวดล้อม

กระบวนงานควบคุม

ระบบสารสนเทศ

ส่วนประกอบของการควบคุม

การควบคุมการจัดองค์การ

9.4 ประเภทของการควบคุม

กระบวนงานควบคุมการเข้าถึง

กระบวนงานควบคุมการรับเข้า

กระบวนงานควบคุมการประมวลผล

กระบวนงานควบคุมการนำออก

การควบคุมเอกสารและกระบวนงาน

9.5 ความมั่นคง

ความมั่นคงด้านกายภาพ

ความมั่นคงด้านข้อมูล

วิธีการป้องกันข้อมูล

9.6 การวางแผนเพื่อรองรับความไม่แน่นอนที่อาจเกิดขึ้น

กระบวนงานการทำสำรองและการเริ่มใหม่

การเตรียมการสำหรับความเสียหายของศูนย์ประมวลผลข้อมูล

คำถามท้ายบท

วัตถุประสงค์ประจำบท

1. สามารถอธิบายความสำคัญของการควบคุม (controls) ต่อระบบสารสนเทศ
2. สามารถอธิบายความแตกต่างระหว่างการควบคุมและความมั่นคง (security)
3. สามรถอธิบายความหมายของอาชญากรทางคอมพิวเตอร์
4. สามารถอธิบายประเภทของความมั่นคง
5. สามารถอธิบายส่วนประกอบของโครงสร้างการควบคุม
6. สามารถอธิบายการควบคุมกระบวนงาน
7. สามารถอธิบายการควบคุมการเข้าถึงและการควบคุมการรับเข้า
8. สามารถอธิบายการวอธีการป้องกันข้อมูลบนคอมพิวเตอร์
9. สามารถบอกความสำคัญของนโยบายการทำการสำรอง (backup) ต่อคอมพิวเตอร์
10. สามารถอธิบายความสำคัญของการควบคุมการประมวลผลและตรรกะ
11. สามารถอธิบายการเตรียมการเพื่อรองรับเหตุการณ์ความไม่แน่นอนที่อาจเกิดขึ้น

9.1 บททนำ

มีความเสี่ยง(Risks) หลายประการที่เกิดขึ้นในองค์การแล้วทำให้องค์การได้รับความเสียหายและสูญเสียหลายประการเช่น องค์การประสพภาวะขาดทุน การขาดความน่าเชื่อถือทางธุรกิจ ดังนั้นองค์การจึงต้องการการจัดการที่สามารถกำจัดความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศ เพื่อให้องค์การบรรลุผลตามเป้าหมายที่วางแผนไว้

ถึงแม้ว่าความเสี่ยงของระบบสารสนเทศมักถูกมองว่าเกิดจากบุคลากรภายนอกองค์การที่ไม่ได้รับสิทธิ์การใช้ระบบแอบลักลอบเข้าสู่ระบบเพื่อทำให้ระบบได้รับความเสียหาย แต่ยังมีอีกความเสี่ยงหนึ่งซึ่งถือว่าเป็นสาเหตุที่สำคัญนั่นคือความเสี่ยงที่เกิดจากพนักงานภายในองค์การ ซึ่งเกิดจากการกระทำโดยมิได้ตั้งใจ การละเลยในการปฏิบัติงาน การมีเจตนามุ่งร้ายและการจงใจปฏิบัติงานเพื่อการทุจริต นอกจากพนักงานแล้วยังมีสาเหตุที่เกิดจากการเกิดไฟไหม้ น้ำท่วม หรือภัยธรรมชาติต่างๆ

ความเสี่ยงอีกประการหนึ่งที่อาจเกิดขึ้นกับระบบสารสนเทศคือ อาชญากรรมทางคอมพิวเตอร์ (Computer Crime) เป็นการกระทำของบุคคลที่ไม่ได้รับสิทธิ์การใช้จากองค์การแอบลักลอบเข้าสู่ระบบโดยใช้คอมพิวเตอร์เป็นเครื่องมือ การกระทำที่จัดว่าเป็นอาชญากรรมได้แก่

- การลักลอบเข้าไปปรับปรุงระเบียน(records) ทางด้านการเงิน เช่น ปรับปรุงยอดเงินฝากยอดตัวเลขในบัญชีต่างๆ
- การลักลอบขโมยข้อมูลของบริษัท ข้อมูลลูกค้า รายชื่อลูกค้าหรือโปรแกรมคอมพิวเตอร์ต่างๆ
- การทำลายอุปกรณ์คอมพิวเตอร์ หน่วยเก็บข้อมูลหรือซอฟต์แวร์ต่างๆ
- การบุกรุกเข้าไปใช้เครื่องคอมพิวเตอร์ ซอฟต์แวร์ แฟ้มข้อมูล ฐานข้อมูล เป็นต้น

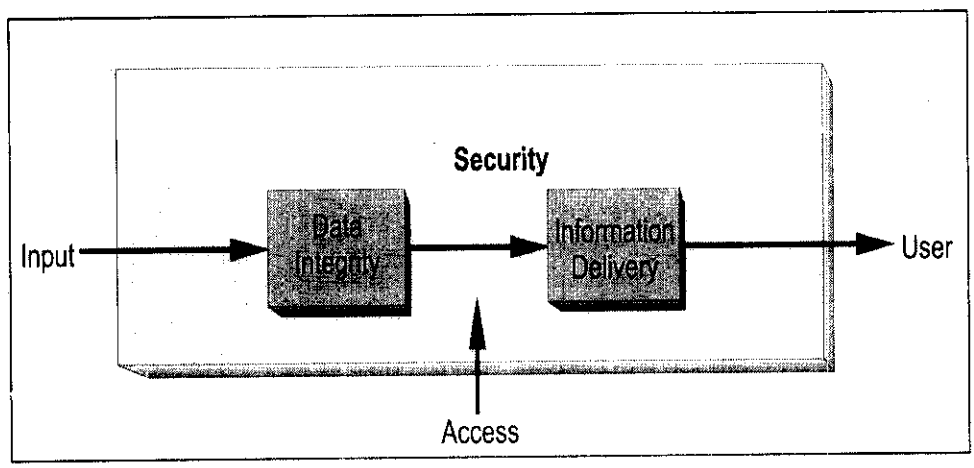
ปัญหาความเสี่งต่างๆที่เกิดขึ้นเหล่านี้ทำความเสียหายให้กับข้อมูลซึ่งเราทราบดีอยู่แล้วว่าการนำข้อมูลที่ไม่ไปประมวลผลทำให้ได้รับสารสนเทศที่ไม่มีคุณภาพซึ่งนำไปสู่การตัดสินใจที่ผิดพลาด เป็นทำให้องค์การได้รับความเสียหาย ดังนั้นในบทนี้จึงกล่าวถึง ระบบการควบคุมและระบบรักษาความมั่นคง เพื่อทำให้ระบบสารสนเทศมีความมั่นคง มีบูรณภาพและมีการจัดส่งที่มีคุณภาพ

9.2 การควบคุมระบบสารสนเทศ (Control of Information Systems)

การควบคุมภายในเป็นการลดความเสี่ยงที่เกิดขึ้นกับระบบสารสนเทศ การควบคุม (Controls) สามารถกำหนดได้ตั้งแต่ขั้นการวางแผนและนโยบายการป้องกันระบบสารสนเทศ เพื่อให้การมีบูรณภาพรวมถึงการจัดส่งข้อมูลและสารสนเทศไปยังผู้ทำการตัดสินใจ การควบคุมจึงต้องพิจารณาตั้งแต่การจัดการ การวางแผน การจัดองค์การ การจัดบุคลากรและการสั่งการในองค์การ

สิ่งที่ต้องควบคุมในระบบสารสนเทศ(Aspects of Information System Control)

ในระบบสารสนเทศมีสิ่งสำคัญ 3 ประการที่ต้องควบคุม ได้แก่ ความมั่นคง บูรณภาพข้อมูลและการจัดส่ง ความมั่นคง (Securitv) เป็นการป้องกันสารสนเทศจากบุคคลที่ไม่ได้รับสิทธิ์ในการใช้ แอบลักลอบเข้าสู่ระบบ รวมถึงอาชญากรรมทางคอมพิวเตอร์ต่างๆ บูรณภาพข้อมูล (Data Integrity) เป็นการป้องกันข้อมูลและสารสนเทศให้มีความถูกต้องและการจัดส่งสารสนเทศ (Information Delivery) เพื่อให้มั่นใจได้ว่าสารสนเทศได้ถูกส่งถึงมือผู้ที่ต้องการนำไปใช้ในการตัดสินใจอย่างถูกต้อง



รูป 9-1 สิ่งที่ต้องควบคุมในระบบสารสนเทศ

สิ่งสำคัญทั้งสามประการดังกล่าวเป็นสิ่งที่ต้องพิจารณาควบคุมในระบบสารสนเทศ หากปราศจากความมั่นคง ระบบสารสนเทศอาจถูกโจมตีจากบุคคลภายนอกและบุคคลภายในองค์การที่พยายามลักลอบเข้ามาทำลายระบบ หากปราศจากบูรณภาพของข้อมูล การประมวลผลก็จะไม่ได้ระบบสารสนเทศที่มีคุณค่าเพราะผู้ใช้ต้องนำระบบสารสนทศไปใช้เพื่อทำการตัดสินใจนั้นไม่มี

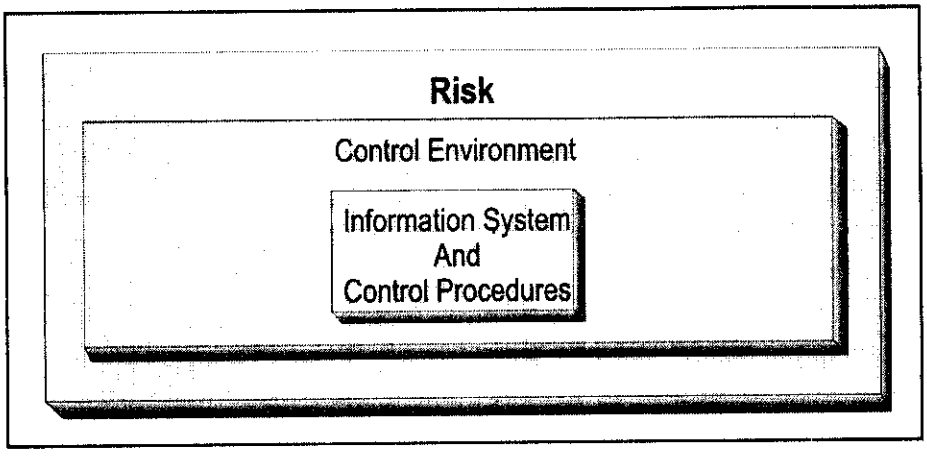
ความเชื่อมั่นในผลลัพธ์ที่ตนเองได้รับ และสุดท้ายหากปราศจากการควบคุมการจัดส่งสารสนเทศไปให้กับบุคคลที่ถูกต้อง ก็ทำให้สารสนเทศรั่วไหล ไม่ถึงมือผู้รับหรือได้รับไม่ทันกาล รูป 9–1 แสดงให้เห็นสิ่งที่ต้องควบคุมในระบบสารสนเทศ และตาราง 9–1 แสดงปัญหาประเภทต่างๆ ที่นำไปสู่การสูญเสียทรัพยากรข้อมูล ซึ่งเท่ากับว่าองค์การขาดความมั่นใจในการใช้ข้อมูลเพื่อทำการตัดสินใจ ปัญหาดังกล่าวได้แก่ ปัญหาด้านความมั่นคง ปัญหาบูรณภาพของข้อมูลและปัญหาการจัดส่ง

ปัญหาด้านความมั่นคง (Security Problems)
-ไฟไหม้ น้ำท่วม หรือภัยธรรมชาติ -การฉ้อโกงหรือการกระทำการใดๆที่ผิดต่อกฎหมาย -การลักลอบเข้าสู่ระบบคอมพิวเตอร์ -การใช้ฐานข้อมูลไปในทางที่ผิดกฎหมายหรือผิดวัตถุประสงค์ -การส่งผ่านข้อมูลทางสายสื่อสารต่างๆ -การสมรู้ร่วมคิดกันฉ้อโกงระหว่างบุคลากรภายในองค์การ
ปัญหาด้านบูรณภาพข้อมูล (Data Integrity)
-ความผิดพลาดจากการประมวลผลที่มีสาเหตุมาจากปัญหาของฮาร์ดแวร์หรือซอฟต์แวร์ - ความผิดพลาดจากความบกพร่องของมนุษย์ -การนำข้อมูลเข้าไม่ถูกต้องเนื่องจากผู้ปฏิบัติงาน หรือจากความผิดปกติของฮาร์ดแวร์ หรือจากการควบคุมการปฏิบัติงานที่ไม่มีประสิทธิภาพ -การสูญหายของข้อมูลระหว่างการส่งผ่านข้อมูล การใช้แฟ้มข้อมูลผิดหรือแฟ้มข้อมูลเก่ามาประมวลผล หรือการพรั่งเผลอลบข้อมูลที่มีความสำคัญโดยไม่ได้ตั้งใจ -การที่ไม่สามารถติดตามการประมวลผลของแต่ละรายการ(transaction)
ปัญหาด้านการจัดส่ง (Information Delivery)
-ผู้ใช้ได้รับระบบสารสนเทศที่ไม่ตรงตามความต้องการ -การเลือกฮาร์ดแวร์และซอฟต์แวร์ที่ไม่เหมาะสม -ข้อมูลถูกนำมาประมวลผลผิดพลาด

ตาราง 9-1 ปัญหาที่ต้องควบคุมประเภทต่างๆ

9.3 โครงสร้างการควบคุม(Control Structure)

วิธีการที่ใช้ในการปกป้องระบบสารสนเทศจากปัญหาทางด้านความมั่นคง บูรณภาพของข้อมูลและการจัดส่งสารสนเทศแสดงดังตาราง 9-1 โครงสร้างการควบคุม (control structure) ประกอบด้วยการควบคุมสภาพแวดล้อมและกระบวนงานการควบคุมที่ใช้ปกป้อง IS จากความเสี่ยง แสดงดังรูป 9-2 ระบบสารสนเทศและกระบวนงานการควบคุมอยู่ภายในการควบคุมสภาพแวดล้อม การควบคุมโครงสร้างช่วยให้ผู้ใช้ระบบสารสนเทศได้ใช้สารสนเทศที่มีความถูกต้องและขีดความสามารถในการตัดสินใจ ทั้งยังช่วยในเรื่องความมั่นคงของระบบด้านสิทธิอำนาจในการเข้าถึงระบบ ในส่วนต่อไปนี้จะเป็นการกล่าวถึงการควบคุมสภาพแวดล้อมและระบบสารสนเทศและการควบคุมกระบวนงาน



รูป 9-2 โครงสร้างการควบคุม

การควบคุมสภาพแวดล้อม (The Control Environment)

การควบคุมสภาพแวดล้อมแสดงดังรูป 9–2 ประกอบด้วยการควบคุมโครงสร้างองค์การ คณะกรรมการและการควบคุมการจัดการ

โครงสร้างองค์การ(Organization structure)

เป็นการจัดโครงสร้างเพื่อการวางแผน การสั่งการและการควบคุมในองค์การและยังเป็นสิ่งสำคัญที่ใช้ควบคุมสภาพแวดล้อม โครงสร้างองค์การเป็นแผนภาพที่มีเส้นลากโยงและมีการแบ่ง

ระดับชั้นตามสายงานที่แสดงอำนาจหน้าที่ในการทำงานระหว่างบุคคลภายในองค์การ มีการระบุตำแหน่งงานซึ่งทำให้เห็นหน้าที่ความรับผิดชอบของงานในแต่ตำแหน่งที่สูงและต่ำกว่าเป็นแบบลำดับชั้น ลำดับชั้นที่สูงกว่าจะควบคุมและสั่งการ ลำดับชั้นที่ต่ำกว่าจะรับคำสั่งไปปฏิบัติเพื่อสนองนโยบาย การควบคุมจึงทำได้ง่ายเพราะสามารถควบคุมได้ตามลำชั้นและสายงาน

คณะกรรมการ(Steering Committee)

เป็นคณะกรรมการซึ่งมีหน้าที่วางระเบียบและวาระการดำเนินงานได้แก่ การพัฒนาแผนการกำหนดนโยบายให้กับองค์การสารสนเทศ เป็นต้น

การควบคุมการจัดการ(Management Control)

เป็นการควบคุมกิจกรรมหลักภายในองค์การ โดยการติดตามดูประสิทธิภาพการทำงานและผลกระทบต่างๆที่เกิดขึ้นกับพนักงานและหน่วยงานภายในองค์การ เป็นการประเมินหรือกำหนดนโยบาย การจัดการ กฎระเบียบ วัตถุประสงค์ การจัดทำแผนและงบประมาณ ในการติดตามผลนี้ทำให้ทราบผลสะท้อนกลับในเรื่องดังกล่าว

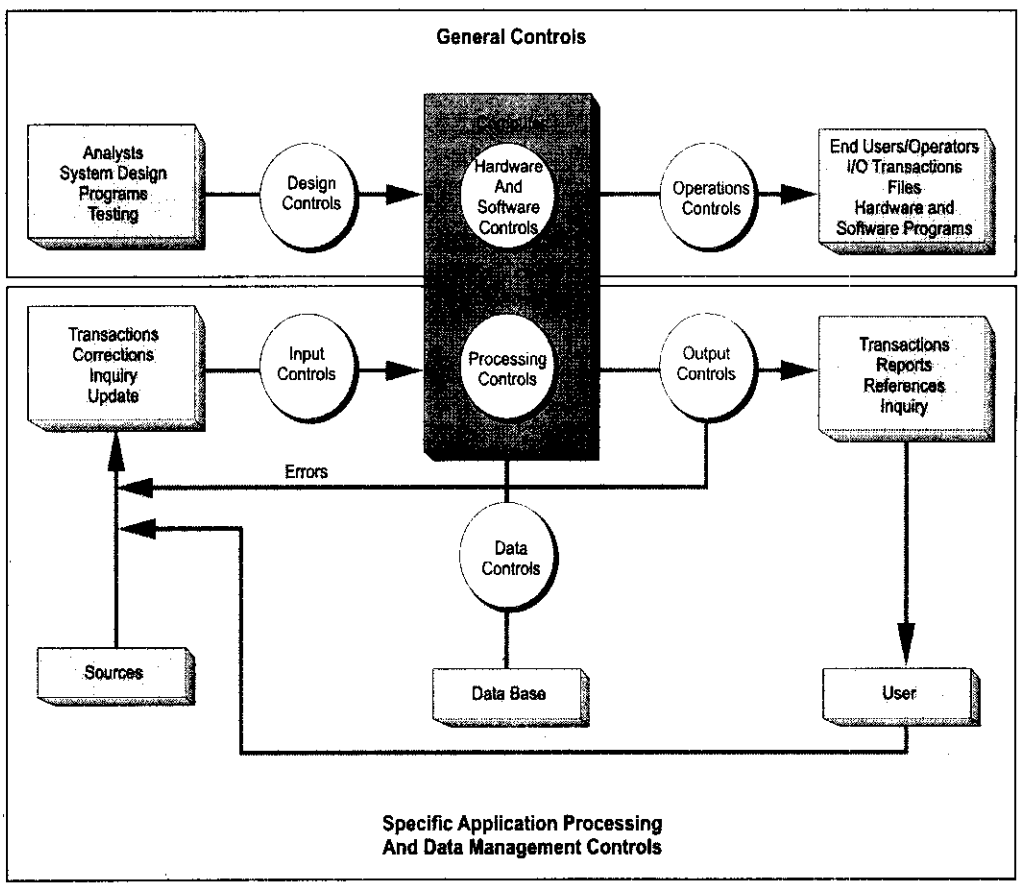
กระบวนงานควบคุม (Control Procedures)

เพื่อหลีกเลี่ยงปัญหาประเภทต่างๆ ที่ได้กล่าวไปแล้วในตอนต้นจึงต้องมีการสร้างกระบวนงานการควบคุม กระบวนงานการควบคุมเป็นนโยบายที่ได้ประยุกต์ขึ้นจากการจัดการเพื่อให้เกิดความมั่นใจว่ากระบวนงานการควบคุมนั้นสำเร็จตามวัตถุประสงค์อย่างแน่นอน การควบคุมทั่วไป (general control) ประยุกต์ใช้กับระบบสารสนเทศในแบบทั่วๆ ไป ส่วนการควบคุมงานประยุกต์ (application controls) ประยุกต์ใช้กับงานประยุกต์แบบเฉพาะอย่างหรืองานประยุกต์ด้านต่างๆ ที่รวมเข้าด้วยกัน

โดยทั่วไปแล้วกระบวนการควบคุมทำให้เกิดความมั่นใจในความถูกต้องด้านการให้สิทธิของรายการ (transaction) และกิจกรรม การจัดแบ่งหน้าที่อย่างชัดเจน (เช่น การแบ่งหน้าที่เขียนโปรแกรมคอมพิวเตอร์ออกจากการควบคุมเครื่องคอมพิวเตอร์) การดูแลให้เกิดความสะดวกปลอดภัยและความเป็นอิสระในการตรวจสอบ

ระบบสารสนเทศ(The Information System)

ระบบสารสนเทศถูกออกแบบมาเพื่อสนับสนุนการทำงานของระบบการจัดการภายในองค์การเช่น การประมวลผลธุรกรรม การรายงาน และการให้ระบบสารสนเทศเพื่อการตัดสินใจ สิ่งดังกล่าวเป็นสิ่งที่บุคลากรภายในองค์การมีความต้องการนำมาใช้ในการปฏิบัติงาน ดังนั้นจึงต้องมีการออกแบบระบบสารสนเทศให้เหมาะสมกับการปฏิบัติงานในแต่ละกิจกรรมของบุคลากรภายในองค์การ



รูป 9– 3 โครงสร้างการควบคุมในระบบสารสนเทศใช้คอมพิวเตอร์

ส่วนประกอบของการควบคุม (Elements of Control Structure)

โครงสร้างการควบคุมในระบบสารสนเทศด้วยคอมพิวเตอร์(Computer Based Information System: CBIS) และส่วนประกอบต่างๆ แสดงดังรูป 9– 3 โดยส่วนประกอบแทนด้วยสี่เหลี่ยมผืน

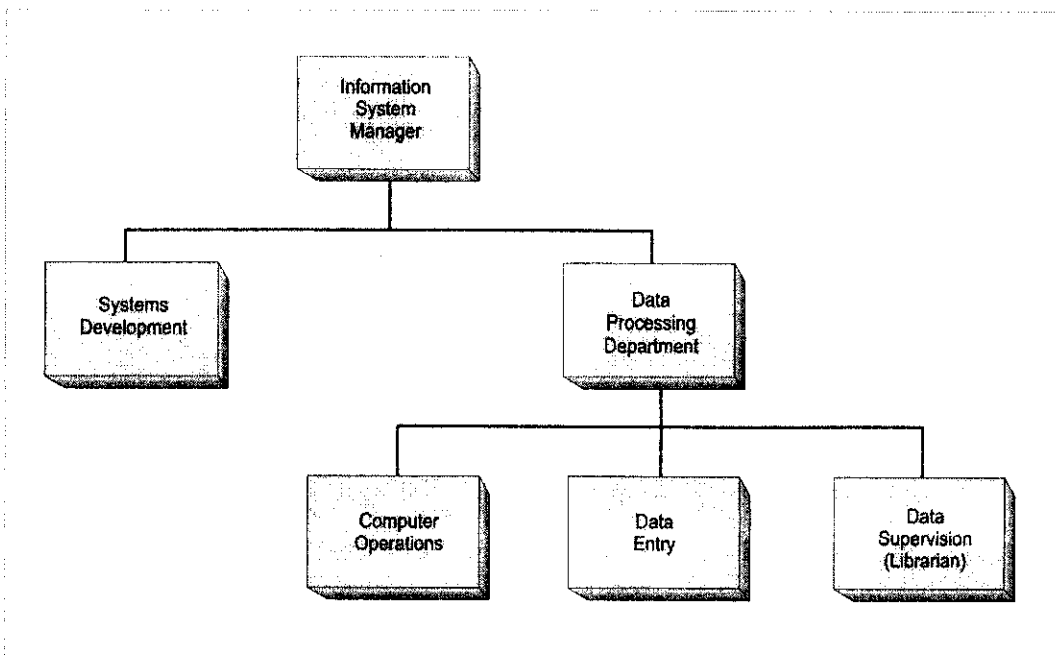
ผ้าและการควบคุมแทนด้วยวงกลม มีการแบ่งการควบคุมออกเป็น 2 ประเภท ได้แก่ การควบคุมทั่วไป(General Control) และการควบคุมงานประยุกต์(Application Controls)

การควบคุมทั่วไป ประกอบด้วย

1. การควบคุมการออกแบบระบบ ซึ่งต้องทำการควบคุมในวงจรการพัฒนาระบบ ควบคุมในขั้นตอนต่างๆ เพื่อให้ได้ระบบสารสนเทศที่ตรงตามความต้องการของผู้ใช้

2. การควบคุมการทำงานของฮาร์ดแวร์และซอฟต์แวร์ เป็นการตรวจสอบฮาร์ดแวร์ให้อยู่ในสภาพที่พร้อมใช้งานและควบคุมความมั่นคง ในส่วนของซอฟต์แวร์เป็นการควบคุมการเข้าถึง เพราะซอฟต์แวร์เป็นส่วนหนึ่งที่สามารถเข้าถึงข้อมูลได้

3. การควบคุมการปฏิบัติงานซึ่งใช้บุคลากรในการควบคุมดูแล เป็นการควบคุมวิธีการปฏิบัติงานให้เป็นไปตามขั้นตอนและวิธีการที่กำหนด โดยต้องมีการจัดทำคู่มือปฏิบัติงานเพื่อการศึกษาระบบงานและเพื่อทราบวิธีแก้ปัญหาที่จะเกิดขึ้น



รูป 9-4 ผังองค์การ

การควบคุมงานประยุกต์ ประกอบด้วย

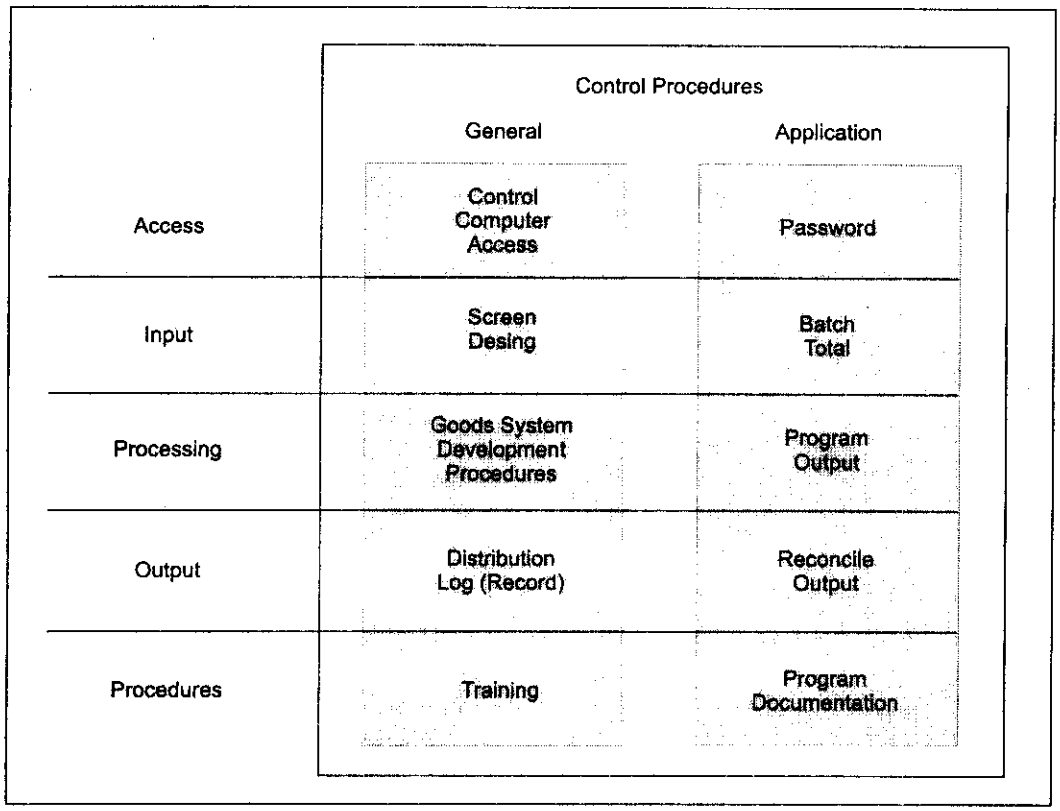
1. การควบคุมการนำเข้า เป็นการตรวจสอบความถูกต้องและสมบูรณ์ของการนำข้อมูลเข้า

2. การควบคุมการประมวลผล เป็นการควบคุมและตรวจสอบการประมวลผลให้ถูกต้องตามตรรกะวิธีที่กำหนด

3. การควบคุมผลลัพธ์เพื่อให้ได้ผลลัพธ์ที่ถูกต้อง ถึงแม้ระบบจะสร้างผลลัพธ์ออกมาได้ แต่ต้องผ่านการตรวจสอบโดยการใส่ค่าข้อมูลทดสอบว่าถูกต้องหรือไม่

4. การควบคุมฐานข้อมูลขององค์การ เป็นการควบคุมการเข้าถึงและการตรวจสอบสิทธิ์การใช้

จากรูป 9–3 ที่ผ่านมาจะเห็นว่าระบบสารสนเทศประกอบด้วยการพัฒนาระบบ ข้อมูลเข้า ระบบคอมพิวเตอร์ การปฏิบัติการ สารสนเทศและฐานข้อมูล ซึ่งรายละเอียดจะกล่าวในหัวข้อต่อไป



รูป 9-5 การควบคุมทั่วไปและการควบคุมงานประยุกต์

การควบคุมการจัดองค์การ

เป็นการจัดผังองค์การ(Organization Chart) เป็นการจัดแบ่งหน่วยงานสารสนเทศออกเป็นแผนกและตำแหน่งงานตามความรับผิดชอบหรือตามวัตถุประสงค์ของงาน เป็นสิ่งสำคัญที่ต้องกระทำเพราะทำให้มองเห็นสายการบังคับบัญชา อำนาจการสั่งการ ความรับผิดชอบและหน้าที่ของบุคคลในแต่ละตำแหน่งที่กำหนด การควบคุมจึงกระทำได้โดยง่าย หน้าที่หลักของแผนกสารสนเทศได้แก่ การปฏิบัติการ การพัฒนาระบบ(การวิเคราะห์ ออกแบบและสร้างระบบ) การนำข้อมูลเข้า การบรรณาธิการข้อมูล เป็นต้น แสดงดังรูป 9-4

9.4 ประเภทของการควบคุม (Types of Controls)

ได้กล่าวถึงไปแล้วว่ากระบวนงานการควบคุมแบ่งออกเป็นการควบคุมทั่วไปและการควบคุมงานประยุกต์ การควบคุมเหล่านี้แบ่งออกเป็นกระบวนงานควบคุมการเข้าถึง กระบวนงานควบคุมการรับเข้า กระบวนงานควบคุมการประมวลผล กระบวนงานควบคุมการนำออกและการควบคุมกระบวนคำสั่งและเอกสารระบบ การจำแนกออกเป็นประเภทต่าง ๆ ข้างต้นแสดงเป็นลักษณะของเมตริกซ์ดังรูป 9-5 กระบวนงานการควบคุมแต่ละประเภททำขึ้นเพื่อให้เกิดความมั่นใจว่าข้อมูลมีความมั่นคงหรือข้อมูลมีบูรภาพหรือการจัดส่งอย่างถูกต้องเพื่อให้ได้สารสนเทศที่เหมาะสมและพึงพอใจตามความต้องการของผู้ตัดสินใจ

กระบวนงานควบคุมการเข้าถึง (Access Control Procedures)

การควบคุมการเข้าถึง(Access Control) เป็นการจำกัดสิทธิ์การใช้ของผู้ใช้ในการเข้าถึงฮาร์ดแวร์ ซอฟต์แวร์ หรือฐานข้อมูล การควบคุมลักษณะนี้เป็นการป้องกันการบุกรุกหรือลักลอบเข้ามาใช้ของบุคคลที่ไม่ได้รับสิทธิ์เป็นการป้องกันการเข้ามาใช้ทรัพยากรระบบอย่างไม่เหมาะสม เช่น เวลาคอมพิวเตอร์ การใช้เนื้อที่จัดเก็บข้อมูลเกินขนาดที่เหมาะสม และการทำให้ระบบสื่อสารหยุดชะงัก เป็นต้น การควบคุมการเข้าถึงมีดังต่อไปนี้

1. การเข้าถึงเอกสารการใช้ซอฟต์แวร์ ต้องมีการกำหนดสิทธ์เป็นบุคคลรายบุคคล ว่าใครบ้างที่มีสิทธิ์เข้าถึง เพราะเอกสารนี้จะแสดงรายละเอียดต่างๆ เช่นวัตถุประสงค์การใช้ วิธีการใช้ เป็นต้น

2. การเข้าถึงอุปกรณ์คอมพิวเตอร์ต้องมีการกำหนดสิทธิ์เป็นบุคคลรายบุคคลว่าใครบ้างสามารถเข้าถึงได้ หรือเมื่อเข้าถึงได้แล้วมีสิทธิ์การใช้แบบอยู่ในระดับใด

3. การเข้าถึงฐานข้อมูลและซอฟต์แวร์ ต้องมีการกำหนดสิทธิ์เป็นบุคคลรายบุคคลว่าใครบ้างสามารถใช้ซอฟต์แวร์ประมวลผลได้ เพราะสามารถใช้ซอฟต์แวร์เข้าถึงข้อมูลในฐานข้อมูลได้ เช่น การเพิ่ม การลบ การปรับเปลี่ยน และการสืบค้นข้อมูล

กระบวนงานควบคุมการรับเข้า (Input Control Procedures)

ควบคุมการรับเข้า (Input Control) เป็นการตรวจสอบความถูกต้องของข้อมูลก่อนที่จะนำเข้าสู่หน่วยเก็บ ป้องกันไม่ให้เกิดปัญหาข้อมูลขยะ ดังคำกล่าวที่ว่าหากเราเก็บข้อมูลที่เป็นขยะเข้าไป ผลลัพธ์ที่ได้ก็ได้ขยะออกมา (Garbage In, Garbage Out :GIGO) นอกจากนั้นยังเป็นการป้องกันการสูญหายของข้อมูล การซ้ำซ้อนกันของข้อมูล หรือการเข้าไปเปลี่ยนแปลง ซึ่งการควบคุมการนำเข้ามักถูกนำไปใช้เป็นข้อกำหนดในการสร้างโปรแกรมประยุกต์ต่างๆ ลักษณะที่ถือว่าทำให้เกิดกรรมวิธีการนำข้อมูลเข้า ได้แก่

- การเก็บรายการ (transaction)
- การปรับปรุงรายการ (transaction)
- การปรับปรุงแฟ้มข้อมูลหรือฐานข้อมูล
- ข้อคำถาม
- การตรวจแก้ข้อผิดพลาด

การควบคุมการนำข้อมูลเข้า(Data Entry Control)

การนำข้อมูลเข้าต้องแน่ใจว่าเป็นข้อมูลที่ถูกต้อง ในการประมวลผลธุรกรรมการตรวจสอบข้อมูลเข้าเป็นสิ่งจำเป็นที่ต้องกระทำ การตรวจสอบรวมถึง system logs การตรวจสอบเขตข้อมูล(field) ระเบียน(record) แฟ้ม(file) และชุดข้อมูล(batch)

1. Field Checks เป็นการตรวจสอบแต่ละเขตข้อมูลตามข้อกำหนดหรือเงื่อนไขของโปรแกรมประยุกต์ เช่น กำหนดให้รับรหัสนักศึกษาจำนวน 10 หลักและมีชนิดเป็นตัวเลข หากการป้อนข้อมูลเข้าไม่เป็นไปตามข้อกำหนดก็ไม่สามารถรับข้อข้อมูลเข้าที่เขตข้อมูลนี้ได้

2. Record Checks เป็นการตรวจสอบความสัมพันธ์ระหว่างเขตข้อมูลที่โปรแกรมประยุกต์กำหนดไว้ เช่น กำหนดให้เขตข้อมูลใดบ้างที่ไม่สามารถละเลยการป้อนข้อมูล หากผู้ใช้ไม่ป้อนข้อมูลให้ครบตามเขตข้อมูลที่กำหนดก็ทำให้ไม่สามารถบักทึกระเบียนนั้นลงสู่หน่วยเก็บได้

3. File Checks เป็นการตรวจสอบเพื่อให้มั่นใจว่าได้นำแฟ้มข้อมูลที่ถูกต้องมาประมวลผล เนื่องจากอาจมีการเก็บข้อมูลตามช่วงเวลาการเกิดของข้อมูล เช่น การเก็บข้อมูลการลงทะเบียนเรียนของนักศึกษามีการแบ่งจัดเก็บตามภาคและปีการศึกษา

4. Batch Checks เป็นการตรวจสอบว่าข้อมูลทุกระเบียนที่รวบรวมไว้ถูกนำเข้าประมวลผล เช่น การจัดเก็บข้อมูลนักศึกษาที่เข้าสอบวิชา CT105 ให้ผู้เข้าสอบที่ข้อสอบชุด A1 ทั้งหมดมี หมายเลข Batch เป็น 101 ส่วนผู้เข้าสอบที่ข้อสอบชุด A2 ทั้งหมดมี หมายเลข Batch เป็น 102 เมื่อทำการประมวลผลก็ประมวลผลแยกชุดข้อมูลกัน

5. หากต้องการตรวจสอบการทำงานการนำเข้าทั้งหมด สามารถตรวจสอบได้จาก logs ซึ่งมี 2 ชนิดได้แก่ Transaction logs เป็นรายการที่ถูกสร้างขึ้นมาเพื่อแสดงรายการของธุรกรรมทั้งหมดที่ได้นำเข้าสู่ระบบ และError logs เป็นรายการที่ถูกสร้างขึ้นมาเพื่อแสดงข้อผิดพลาดที่เกิดขึ้นกับระบบ ซึ่งแสดงรายละเอียดต่างๆ เช่น เวลาและประเภทของข้อผิดพลาดที่เกิดขึ้น

กระบวนงานควบคุมการประมวลผล (Processing Control Procedures)

การควบคุมการประมวลผล (Processing Control) เป็นการควบคุมเพื่อให้ได้ระบบสารสนเทศจากการประมวลผลข้อมูลที่ถูกต้อง การควบคุมการประมวลผลมี 4 ประเภทได้แก่ การควบคุมการประมวลผลและตรรกะ (Processing and Logic Controls) การควบคุมแฟ้มและฐานข้อมูล (File and Database Controls) การควบคุมซอฟต์แวร์ (Software Controls) และการควบคุมฮาร์ดแวร์ (Hardware Controls)

1. การควบคุมการประมวลผลและตรรกะ (Processing and Logic Controls)

เป็นการควบคุมที่ต้องกำหนดในระยะการวิเคราะห์และออกแบบระบบ(Analysis Phase and Design Phase) ซึ่งอยู่ในวงจรการพัฒนาระบบ (System Development Life Cycle) เนื่องจากการวิเคราะห์และออกแบบระบบที่ดีและถูกต้องย่อมนำไปสู่การได้รับสารสนเทศที่ตรงตามความต้องการของผู้ใช้ ซึ่งส่งผลให้ผู้ทำการตัดสินใจได้ใช้ระบบสารสนเทศทำการตัดสินใจอย่างมีคุณภาพ ในทางตรงข้ามหากทำการวิเคราะห์และออกแบบระบบผิดแนวทาง ก็ส่งผลให้ได้รับสารสนเทศที่ไม่ตรงตามความต้องการของผู้ใช้ ทำให้ผู้ทำการตัดสินใจไม่สามารถนำสารสนเทศไปประกอบการตัดสินใจได้

ในส่วนการควบคุมการเขียนโปรแกรมโดยทั่วไปต้องมีการตรวจสอบตั้งแต่การเลือกใช้แฟ้มข้อมูลหรือตารางในฐานข้อมูล การตรวจสอบขั้นตอนการคิด สูตรคณิตศาสตร์ การคำนวณ

แบบต่างๆ เป็นไปตามเงื่อนไขข้อกำหนดหรือไม่ มีการตรวจสอบยอดรวมของระเบียนก่อนและหลังการประมวลผลว่าครบถ้วนหรือไม่ การตรวจความสอดคล้องและความซ้ำซ้อนกันของข้อมูลในฐานข้อมูลเพื่อป้องกันการเกิดปัญหา deadlock เมื่อผู้ใช้หลายๆคนต้องการเข้าถึงข้อมูลเดียวกันในเวลาเดียวกัน

2. การควบคุมแฟ้มข้อมูลและฐานข้อมูล(File and Database Controls)

เป็นการควบคุมการเลือกใช้แฟ้มข้อมูลหรือตารางในฐานข้อมูลมาประมวลผลให้เป็นไปอย่างถูกต้องตรงตามความต้องการ และเมื่อมีการเปลี่ยนแปลงแฟ้ม ต้องมีการตรวจสอบจำนวนของระเบียนที่คงเหลือและจำนวนระเบียนที่ถูกเปลี่ยนแปลง

3. การควบคุมซอฟต์แวร์(Software Controls)

การควบคุมซอฟต์แวร์เป็นการทำเพื่อให้เกิดความมั่นใจว่ารายการและสารสนเทศที่ปรากฏอยู่ในรายงานเพื่อการตัดสินใจนั้นเป็นไปตามวัตถุประสงค์ของการจัดการ ด้วยเหตุนี้เององค์การจะต้องติดตามแผนการพัฒนาซอฟต์แวร์และการทำให้เกิดผล การควบคุมซอฟต์แวร์โดยทั่วไปเข้มงวดด้านการปฏิบัติงานและระบบฐานข้อมูลและจัดเตรียมกระบวนงานการทำสำรอง (backup) การกู้คืน (recovery) และการเริ่มต้นใหม่ (restart)

4. การควบคุมฮาร์ดแวร์(Hardware Controls)

เป็นการตรวจสอบปัญหามากเกินเก็บ (overflow) การอ่าน/เขียน เพื่อให้เกิดความแน่ใจว่าไม่เกิดการสูญหายของข้อมูลและไม่เกิดข้อผิดพลาดในขั้นตอนการนำข้อมูลเข้าและออก สิ่งสำคัญประการหนึ่งคือการตรวจสอบภาวะคู่หรือคี่ (parity check) เพื่อช่วยตรวจตักข้อผิดพลาดของข่าวสาร เป็นบิตที่เติมเข้าไป บิตพาริตี้แบ่งเป็น 2 ชนิดคือ ภาวะคู่ (even parity) และภาวะคี่ (odd parity) บิตพาริตี้ที่เติมนั้นจะมีค่าเป็น 0 หรือ 1 ขึ้นกับว่าเลข 1 ที่เติมเข้าไปนั้นมีจำนวนเท่าใดและเราเลือกใช้พาริตี้คู่หรือคี่

กระบวนงานควบคุมการนำออก (Output Control Procedure)

ผลลัพธ์หรือส่วนนำออกได้แก่ สารสนเทศซึ่งอยู่ในรูปแบบรายงานต่างๆ ข้อมูลที่ผ่านการปรับปรุงหรือข้อคำถามเป็นต้น ก่อนที่ผลลัพธ์จะส่งไปให้ผู้ใช้ ต้องผ่านการตรวจสอบและทดสอบจนมั่นใจว่าถูกต้องตรงตามวัตถุประสงค์ที่ได้กำหนดไว้ ในการทดสอบเป็นการทดสอบฟังก์ชั่นการทำงานทั้งในส่วนของการนำข้อมูลเข้าและประมวลผลว่าถูกต้องหรือตามที่กล่าวมาในหัวข้อก่อนหน้านี้ ส่วนขั้นตอนการจัดส่งนั้นต้องเป็นไปตามระยะเวลาที่กำหนดถึงแม้ว่าจะได้สารสนเทศที่ถูก

ต้องแต่ผู้รับได้รับล่าช้าไม่ทันกาล สารสนเทศนั้นก็ไม่มีประโยชน์กับผู้ใช้แต่อย่างใด นอกจากนั้นต้องจัดส่งสารสนเทศไปให้ถูกสถานที่และบุคคล เนื่องจากสารสนเทศบางชนิดเป็นความลับจึงต้องระมัดระวังในการจัดส่ง กล่าวได้ว่าสารสนเทศที่ดีนั้นต้องมีความถูกต้อง ส่งตรงเวลาและส่งถูกสถานที่และบุคคล

การควบคุมเอกสารและกระบวนงาน (Procedure and Documentation Controls)

การควบคุมเอกสารระบบ (documentation controls) ได้แก่การบำรุงรักษาเอกสารต้นฉบับให้ทันสมัย รวมทั้งบำรุงรักษารายงาน การตรวจสอบ กระบวนงานและควบคุมฐานข้อมูลให้เป็นไปตามเอกสารโครงสร้างข้อมูลและหน้าที่ของแต่ละงาน

การควบคุมกระบวนงาน (procedural controls) เป็นการเขียนคู่มืออย่างเป็นขั้นเป็นตอนตามการปฏิบัติงานของกระบวนงานคอมพิวเตอร์หรือตามขั้นตอนของการนำข้อมูลเข้าของพนักงาน เพื่อให้ผู้ใช้ระบบสารสนเทศปฏิบัติงานตามอย่างราบรื่นไม่ติดขัด การควบคุมกระบวนงานนี้ต้องจัดทำขึ้นเฉพาะแต่ละงานประยุกต์

การจัดแบ่งระบบสารสนเทศตามหน้าที่การปฏิบัติงานที่แสดงดังรูป 9-4 เป็นการควบคุมกระบวนงาน ผู้บริหารฐานข้อมูลมีบทบาทสำคัญเพราะหน้าที่การทำงานนั้นเกี่ยวข้องกับระบบฐานข้อมูลจึงมีบทบาทสำคัญในการควบคุมระบบสารสนเทศและต้องรายงานผลไปยังผู้จัดการสารสนเทศ

10.3 ความมั่นคง (The Security)

การควบคุมที่ได้กล่าวไปแล้วเป็นการควบคุมในเรื่องของบูรณภาพของข้อมูลและการส่งสารสนเทศไปยังผู้ใช้ การควบคุมดังกล่าวเป็นการควบคุมเพื่อหลีกเลี่ยงข้อผิดพลาดที่อาจเกิดขึ้นในส่วนของการนำเข้า การประมวลผลข้อมูลและการนำออก แต่อย่างไรก็ตามความมั่นคงเป็นสิ่งที่จำเป็นเพื่อป้องกันระบบคอมพิวเตอร์ไม่ให้ถูกทำลายความมั่นคงมี 2 ประเภทได้แก่ ความมั่นคงด้านกายภาพ (Physical Security) และความมั่นคงด้านข้อมูล (Data Security)

ความมั่นคงด้านกายภาพ (Physical security)

เป็นการป้องกันส่วนประกอบของฮาร์ดแวร์ (รวมถึงอุปกรณ์การประมวลผลส่วนกลาง เทอร์มินอลและหน่วยเก็บข้อมูล) ไม่ให้บุคคลที่ไม่ได้รับสิทธ์อย่างถูกต้องเข้ามาใช้ และยังรวมถึงการป้องกันการจารกรรม ไฟไหม้ น้ำท่วมหรือภัยธรรมชาติต่างๆ

การป้องกันด้านกายภาพจากการโจรกรรมของผู้ร้ายนั้นสามารถควบคุมการเข้าไปใช้สถานที่ โดยใช้ระบบตรวจสอบเพื่อระบุตัวบุคคลว่าได้สิทธ์หรือไม่ เช่น การตรวจม่านตา(eye prints) การอ่านลายนิ้วมือ(finger prints) การสังเคราะห์เสียง(voice prints) ซึ่งวิธีการเหล่านี้เป็นการใช้ส่วนต่างๆ ของร่างกายของแต่ละบุคคลที่ได้รับสิทธิ์ บางกรณีอาจใช้ระบบล็อคประตูโดยการใช้บัตรแม่เหล็ก เป็นต้น

การป้องกันความเสียหายที่เกิดจากไฟไหม้หรือน้ำท่วมจะต้องถูกกำหนดไว้ในแผนการจัดตั้งองค์กรโดยกำหนดเป็นนโยบาย สิ่งที่ต้องกำหนดได้แก่ติดตั้งอุปกรณ์ตรวบจับควันหรือดับเพลิงชนิดต่างๆตามความเหมาะสมตามห้องหรืออาคาร ห้องหรืออาคารที่มีการติดตั้งอุปกรณ์ทางอิเล็กทรอนิกส์ต้องมีการติดตั้งอุปกรณ์ที่แตกต่างจากห้องอื่นๆ มิควรติดตั้งระบบฉีดดับด้วยน้ำ เพราะจะทำให้อุปกรณ์อิเล็กทรอนิกส์เกิดความเสียหาย

ความมั่นคงด้านข้อมูล (Data Security)

การป้องกันซอฟท์แวร์มีความแตกต่างจากการป้องกันฮาร์ดแวร์อุปกรณ์คอมพิวเตอร์เมื่อได้รับความเสียหายสามารถหามาทดแทนได้ แต่หากเป็นข้อมูลเมื่อได้รับความเสียหายอาจหามาทดแทนไม่ได้ ข้อมูลถือว่าเป็นสิ่งสำคัญสูงสุดจึงจำเป็นต้องกำหนดมาตราการในการป้องกันข้อมูลและซอฟท์แวร์จากบุคคลที่ไม่ได้รับสิทธิ์ซึ่งแอบลักลอบหรือบุกรุกเข้ามาใช้ระบบ

วิธีการหนึ่งที่ใช้ป้องกันคอมพิวเตอร์และข้อมูลคือการใช้รหัสลับ (Password) รหัสลับเป็นการนำอาตัวเลขหรือตัวอักษรมาเรียงต่อกันและผู้ใช้ที่เป็นเจ้าของเท่านั้นจึงจะทราบรหัสลับนี้ ผู้ใช้จะต้องป้อนรหัสลับให้ถูกต้องจึงสามารถเข้าถึงระบบคอมพิวเตอร์ได้ คนทั่วไปรู้จักรหัสลับจากการใช้เครื่องฝาก-ถอนเงินด่วนหรือตู้เอทีเอ็ม(Automatic Teller Machine: ATM) ผู้ใช้ต้องมีรหัสลับที่เรียกว่าหมายเลขเอกลักษณ์บุคคลหรือพิน (Personal Identification Number: PIN) เป็นรหัสที่ใช้ในการเข้าถึงบัญชีธนาคารของตนเองโดยผ่านเครื่องเอทีเอ็ม รหัสโดยทั่วไปมักถูกสร้างจากข้อมูลส่วนตัว เช่น วันเดือนปีเกิด ชื่อสัตว์เลี้ยง ชื่อบุคคลในครอบครัว หมายเลขทะเบียนรถยนต์ เป็นต้น ซึ่งเป็นการง่ายต่อการคาดเดา

วิธการป้องกันข้อมูล(Data Protection Methods)

วิธีการที่ใช้ป้องกันซอฟท์แวร์และข้อมูลในปัจจุบันที่รู้จักกันดีได้แก่ การใช้รหัสลับ ซอฟท์แวร์ตรวจสอบระบบ ซอฟท์แวร์สำเร็จรูปด้านรักษาความปลอดภัย ระบบcall-back อุปกรณ์ป้องกันพอร์ต ระบบการเข้ารหัสข้อมูล และซอฟท์แวร์ป้องกันไวรัส

1. นโยบายรหัสลับ (Password Policies)

เป็นการกำหนดนโยบายในการใช้รหัสลับ ได้แก่ การกำหนดความยาวของรหัสลับเช่น ต้องมีความยาวของตัวอักขระที่ประกอบเป็นรหัสลับมากกว่า 4 ตัว มีการกำหนดระยะการมใช้รหัสลับเช่น 6 เดือนต้องเปลี่ยนรหัสลับใหม่ มีการระงับการใช้บริการโดยมิต้องแจ้งให้ผู้ใช้ทราบล่วงหน้าหากผู้ใช้ละเมิดกฎข้อบังคับ เป็นต้น

2. ซอฟท์แวร์ตรวจสอบระบบ (System Audit Software)

เป็นการตามรอยการลงบันทึกเข้า (login) สู่ระบบคอมพิวเตอร์ ระบบตามรอยนี้เป็นส่วนหนึ่งของ transaction log ที่ได้กล่าวไปแล้ว ในระบบlogนี้สามารถชี้ให้เห็นว่ามีผู้ใช้บริการคนใดเข้ามาใช้ระบบบ้าง เข้ามาใช้ระบบเวลาใด มีการlogin มาจากที่ station ใด ผู้ใช้ที่อยู่ในระบบเข้ามาใช้ทรัพยากรอะไรบ้าง เป็นต้น

3. ซอฟท์แวร์สำเร็จรูปด้านการรักษาความมั่นคง (Security Software Package)

เป็นการป้องกันระบบคอมพิวเตอร์ในหลายความหมายเช่น หากผู้ใช้ไม่ป้อนรหัสลับตามเวลาที่ระบบกำหนด(เช่น 5 วินาที)ระบบจะตัดผู้ใช้ออกจากขั้นตอนการป้อนรหัส หรือหากมีการป้อนรหัสผิดเกินจำนวนครั้งที่กำหนด(เช่น 3 ครั้ง)จะไม่สามารถติดต่อกับระบบได้ ในระบบเครื่องฝากถอนเงินด่วน เมื่อผู้ใช้กดรหัสผิดเกิน3ครั้งติดต่อกันเครื่องจะยึดบัตรเข้าตู้ การป้องกันวิธีนี้เป็นการป้องกันผู้ใช้ที่พยายามเดารหัสของผู้ใช้ตัวจริง

4. การเรียกกลับ (Call-back)

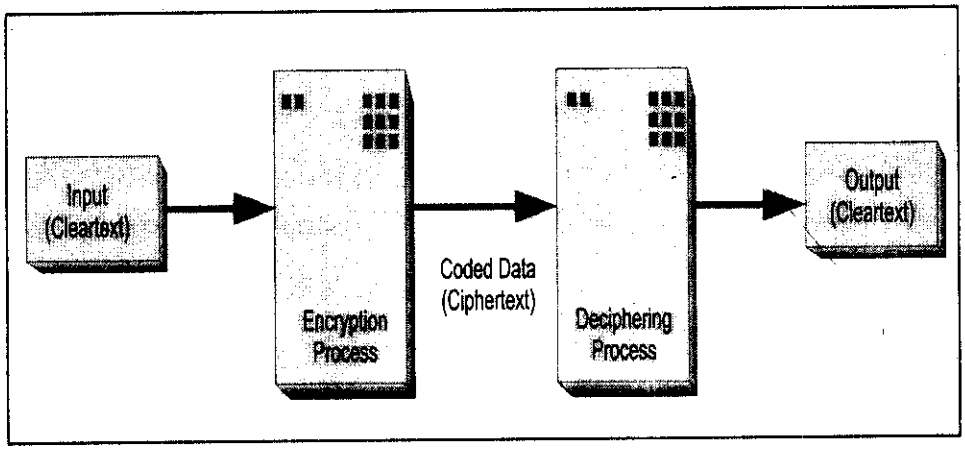
เป็นระบบที่ตอบรับการเรียกใช้ทางโทรศัพท์และการป้อนรหัสลับของผู้ใช้ เมื่อผู้ใช้หมุนโทรศัพท์ติดต่อ ระบบจะตอบกลับไปยังหมายเลขที่ผู้ใช้หมุนมา วิธีนี้เป็นการตรวจสอบหมายเลขโทรศัพท์ว่าผู้ใช้เป็นผู้ใช้ตัวจริงหรือไม่ หากรหัสลับถูกขโมยและถูกใช้โดยผู้ใช้ที่ไม่ได้รับสิทธิ์ เมื่อทำการตรวจสอบรหัสลับกับหมายเลขโทรศัพท์ที่หมุนเข้ามาก็จะทราบได้ว่าเป็นผู้ใช้ตัวจริงหรือไม่ หากไม่ใช่ก็ไม่สามารถเข้าสู่ระบบได้

5. อุปกรณ์ป้องกันพอร์ต (Port Protection Device)

เป็นการกำหนดจุดเชื่อมต่อเข้าสู่ระบบคอมพิวเตอร์โดยการกำหนดพอร์ต ซึ่งอนุญาตให้ผู้ใช้บางคนเท่านั้นที่สามารถลอ็กอินเข้าสู่ระบบคอมพิวเตอร์ได้ทางพอร์ตที่กำหนด หรือมีการกำหนดว่าผู้ใช้ที่ลอ็กอินเข้ามาที่พอร์ตนั้นสามารถใช้ทรัพยากรอะไรจากระบบได้บ้าง

6. ระบบการเข้ารหัสลับข้อมูล (Data Encryption Systems)

เป็นการเปลี่ยนรูปแบบของข้อมูลให้อยู่ในรูปแบบที่คนทั่วไปไม่สามารถอ่านหรือเข้าใจได้ก่อนที่จะส่งข้อมูลนั้นออกไปทางสายสื่อสารหรือทางระบบเครือข่าย เพื่อป้องกันการดักลักลอบขโมยข้อมูล และเมื่อข้อมูลถึงปลายทางผู้ใช้ปลายทางจะมีการถอดรหัสทำให้ข้อมูลเปลี่ยนรูปแบบกลับไปเป็นแบบเดิมก่อนเข้ารหัส หน่วยงานที่กำหนดมาตรฐานนี้ได้แก่ สถาบันมาตรฐานแห่งชาติของสหรัฐอเมริกาหรือแอนซี (The American Nation Standards Institute: ANSI) วิธีการที่เข้ารหัสที่แพร่หลายในปัจจุบันในได้การเข้ารหัสที่เรียกว่ามาตรฐานการเข้ารหัสลับข้อมูลหรือดีอีเอส (Data Encryption Standard: DES) สำหรับระบบการถอดรหัสนั้นแสดงดังรูป 9-6



รูป 9-6 กระบวนการของการเข้ารหัสลับ

7. ไวรัสคอมพิวเตอร์ (Computer Virus)

ปัญหาอย่างหนึ่งที่เกิดขึ้นกับระบบคอมพิวเตอร์คือการถูกโจมตีจากไวรัส ไวรัสคอมพิวเตอร์เป็นโปรแกรมคอมพิวเตอร์ชนิดหนึ่งที่สามารถทำสำเนาตัวเอง เข้าไปติดอยู่ในคอมพิวเตอร์และสามารถแพร่ระบาดไปยังคอมพิวเตอร์อื่น การแพร่ระบาดนั้นมีหลายวิธี ได้แก่ การแพร่ระบาดผ่านแผ่นดิสก์ที่ติดไวรัสจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง การแพร่ผ่านระบบเครือข่ายหรือระบบสื่อ

สารข้อมูล เป็นต้น จุดประสงค์การทำงานของไวรัสแต่ละชนิดขึ้นอยู่กับผู้เขียนโปรแกรมไวรัสแต่ละชนิด เช่น การสร้างโปรแกรมไวรัสไปทำลายโปรแกรมหรือข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ การรบกวนการทำงานโดยการแสดงข้อความที่จอภาพ การทำให้คอมพิวเตอร์หรือระบบสื่อสารทำงานได้ช้าลงหรือผิดปกติ เป็นต้น

ดังนั้นองค์กรจึงต้องมี ซอฟท์แวร์และนโยบายในการป้องกันไวรัส (Anti-Virus Policies and Software) โดยติดตั้งซอฟท์แวร์ที่สามารถตรวจจับและทำลายไวรัสได้รวมถึงหลีกเลี่ยงการใช้ซอฟท์แวร์ที่ไม่ทราบแหล่งกำเนิดที่แน่ชัด

9.6 การวางแผนเพื่อรองรับเหตุบังเอิญที่อาจเกิดขึ้น (Contingency Planning)

จะเกิดอะไรขึ้นหากการควบคุมและความมั่นคงเกิดความล้มเหลวและฮาร์ดแวร์ ซอฟต์แวร์ หรือข้อมูลเกิดความเสียหาย เพื่อตอบคำถามดังกล่าวองค์การต้องวางแผนเพื่อป้องกันสิ่งเหล่านี้ การวางแผนเพื่อรองรับสถานการณ์ฉุกเฉินเป็นการวางแผนเพื่อป้องกันสภาพการณ์และเหตุการณ์ที่ไม่แน่นอนที่อาจเกิดขึ้น โดยในส่วนนี้จะกล่าวถึงการวางแผนรองรับเหตุการณ์ความไม่แน่นอนสองประการที่อาจเกิดขึ้นกับระบบสารสนเทศ ได้แก่ การสูญเสียข้อมูลในหน่วยความจำสำรองและการสูญเสียของศูนย์ประมวลผลข้อมูล ในกรณีแรกถ้าดิสก์ของเครื่องเมนเฟรมหรือฮาร์ดดิสก์ของเครื่องพีซีเกิดการ "พัง (crashed)" (crash เป็นการหยุดทำงานของเครื่องซึ่งเกิดจากการขัดข้องของอุปกรณ์บางส่วน) แผนที่รองรับสถานการณ์นี้คือการทำสำรอง (backup) ดิสก์หรือฮาร์ดดิสก์ หากขาดการจัดทำแผนเพื่อรองรับสถานการณ์ความไม่แน่นอนที่อาจเกิดขึ้นสามารถนำไปสู่ความหายนะ การสูญเสียข้อมูลที่ไม่สามารถกอบกู้กลับคืนมาได้ ส่วนในกรณีที่สองนั้นพิจารณาจากเหตุการณ์การเกิดพายุเฮอริเคน (hurricane) ที่ไมอามี่ (Miami) สหรัฐอเมริกาในปี ค.ศ. 1992 ทำให้ศูนย์สารสนเทศจำนวนมากต้องหยุดทำงาน (shut down) หลายวันทำให้ต้องงดการให้บริการ แผนรองรับเหตุการณ์ความไม่แน่นอนนี้คือองค์การจะปฏิบัติงานต่อไปได้อย่างไร ในหัวข้อนี้จะกล่าวถึงแผนรองรับความไม่แน่นอนสำหรับเหตุการณ์

กระบวนงานการทำสำรองและการเริ่มใหม่ (Backup and Restart Procedures)

ส่วนประกอบที่สำคัญในระบบสารสนเทศคือหน่วยเก็บรอง (secondary storage) เป็นหน่วยเก็บข้อมูลถาวรภายนอกของหน่วยความจำภายในของคอมพิวเตอร์ หน่วยความจำภายในนั้นมีข้อจำกัดและเปลี่ยนแปลงง่าย หน่วยความจำสำรองต้องเก็บข้อมูลและสารสนเทศที่พร้อมสำหรับ

การประมวลผล เทปแม่เหล็กหรือดิสก์ก็ถูกใช้หน่วยเก็บข้อมูลรองและองค์การต้องจัดให้มีการทำสำรองหน่วยเก็บข้อมูลรอง การทำสำรอง (backup) เป็นการทำสำเนาสิ่งที่บรรจุในหน่วยเก็บข้อมูลรอง เป็นการเก็บข้อมูลสำรองไว้ ในกรณีที่หน่วยเก็บที่ใช้งานอยู่เกิดการขัดข้องหรือเสียหายก็ใช้ข้อมูลที่ทำสำรองไว้แทน ในระบบของเครื่องเมนเฟรมพนักงานควบคุมเครื่อง (operator) จะทำการสำรองข้อมูลประจำวันโดยเก็บที่เทปหรือดิสก์ และมักมีการทำสำรองตามระยะเวลาที่องค์การกำหนด

ถึงแม้ว่าข้อมูลที่หน่วยความจำสำรองไม่เกิดการขัดข้องหรือสูญเสีย วิธีการเริ่มต้นใหม่ (restart) ของเครื่องเมนเฟรมเมื่อเครื่องหยุดทำงานหรือ "down" อันเกิดขึ้นจากการทำงานล้มเหลวหรือจากปัญหาอื่น ๆ จะมีกระบวนงานที่เรียกว่า จุดตรวจสอบ / การเริ่มต้นใหม่ (checkpoint / restart) เป็นการใช้จุดตรวจสอบสำเนาของหน่วยความจำปัจจุบันของคอมพิวเตอร์ที่เก็บบันทึกในดิสก์ การเริ่มต้นใหม่เป็นการกำหนดให้เครื่องคอมพิวเตอร์เริ่มทำการ (execute) ต่อหลังจากหยุดทำงาน ณ จุดที่ระบุเอาไว้ นั้นคือคอมพิวเตอร์เกิดการเริ่มต้นใหม่เป็นการเริ่มต้นสำเนาโปรแกรมใหม่ที่จุดตรวจสอบครั้งสุดท้ายในหน่วยความจำและเริ่มต้นการประมวลผลจากจุดนี้ กระบวนงานจุดตรวจสอบ / การเริ่มต้นใหม่สามารถบันทึกการประมวลผลของพนักงานควบคุมเครื่อง สามารถกู้คืน (recover) สิ่งที่เคยเกิดขึ้นในหน่วยความจำคอมพิวเตอร์ให้ย้อนกลับไปดำเนินการใหม่เหมือนไม่เคยเกิดเหตุการณ์ล้มเหลวใดขึ้น

ในระบบฐานข้อมูลจุดตรวจสอบสร้างขึ้นโดยการสร้าง "dumping" เป็นการถ่ายเทข้อมูลโดยการทำสำเนาฐานข้อมูลตามระยะเวลาที่กำหนดโดยถ่ายเทเก็บไว้ที่เทปหรือดิสก์ ระหว่างการถ่ายเทข้อมูลนี้กิจกรรมรายการ (transaction) และฐานข้อมูลอื่น ๆ นั้นจะมีการปิดกั้น (lock) ในระดับแฟ้มที่ดิสก์ หากระบบพังฐานข้อมูลจะจัดโครงสร้างใหม่โดยการทำสำรองการถ่ายเทของครั้งก่อน โดยจัดโครงสร้างฐานข้อมูล ณ เวลาที่เกิดการพัง

การเตรียมการสำหรับความเสียหายของศูนย์ประมวลผลข้อมูล

(Preparing for Loss of Data Processing Center)

การวางแผนเพื่อรองรับเหตุบังเอิญหรืออุบัติเหตุที่อาจเกิดขึ้นนั้นเป็นสิ่งที่มีความสำคัญมาก การทำสำรองหน่วยเก็บรองหรือการกำหนดจุดตรวจสอบ/การเริ่มต้นใหม่ ก็เป็นทางเลือกหนึ่งที่ต้องจัดเตรียมไว้หากหน่วยงานที่ทำหน้าที่หลักในการประมวลผลข้อมูลไม่สามารถปฏิบัติงานได้ ในปี ค.ศ. 1989 ได้เกิดเหตุการณ์แผ่นดินไหวและพายุเฮอริเคนขึ้นที่เมืองซานฟรานซิสโคและชาร์ล

เลสตันประเทศสหรัฐอเมริกา ทำให้องค์การขนาดใหญ่จำนวนมากไม่สามารถปฏิบัติงานด้วยคอมพิวเตอร์ได้เป็นระยะเวลาราวสัปดาห์ โดยที่ไม่มีเครื่องคอมพิวเตอร์ทำงานสำรองแทนเครื่องคอมพิวเตอร์หลัก ดังนั้นจึงต้องมีการจัดเตรียมที่ตั้ง (site) สำรองเพื่อรองรับเหตุการณ์ความไม่แน่นอนและความหายนะที่อาจเกิดขึ้นได้ การจัดเตรียมแผนนี้แบ่งออกเป็น 4 ประเภทได้แก่

1. Hot Site Agreement เป็นที่ตั้งที่จัดตั้งขึ้นมาพอจะเปรียบเทียบได้กับศูนย์คอมพิวเตอร์เมนเฟรม เป็น hot site เตรียมพร้อมสำหรับการทำงานได้ทันทีหากองค์การต้องการ มีค่าใช้จ่ายการประมวลผลสูง

2. Cold Site Agreement เป็นที่ตั้งที่จัดตั้งขึ้นมาพร้อมสามารถติดตั้ง (install) เครื่องคอมพิวเตอร์เมนเฟรมได้ทันที

3. Reciprocal Agreement เป็นการจัดหาการประมวลผลให้กับความหายนะในแต่ละกรณีที่เกิดขึ้น มีค่าใช้จ่ายต่ำ

4. Backup Data Processing Site องค์การสร้างศูนย์คอมพิวเตอร์ไว้อีกแห่งหนึ่งเสมือนกับเป็นศูนย์ประมวลผลข้อมูลที่ศูนย์หลักทุกประการ ทางเลือกนี้องค์การสามารถปฏิบัติงานได้ทันทีหากเกิดความหายนะแต่มีค่าใช้จ่ายที่สูงมาก

คำถามท้ายบท

1. จงอธิบายเพราะเหตุใดการควบคุม (controls) จึงมีความสำคัญในระบบสารสนเทศ
2. จงอธิบายความแตกต่างระหว่างการควบคุมและความมั่นคง (security) พร้อมทั้งยกตัวอย่าง
3. จงอธิบายอาชญากรทางคอมพิวเตอร์คืออะไร
4. จงอธิบายความมั่นคงแบ่งออกเป็นกี่ประเภท อะไรบ้าง
5. จงอธิบายส่วนประกอบของโครงสร้างการควบคุม ส่วนประกอบใดควบคุมสภาพแวดล้อม
6. จงอธิบายการควบคุมกระบวนงาน
7. จงอธิบายการควบคุมการเข้าถึงหมายถึงอะไร ในการนำข้อมูลเข้านั้นต้องมีการควบคุมการรับเข้าอย่างไรบ้าง
8. จงอธิบาย transaction log มีกี่ประเภทอะไรบ้าง
9. จงอธิบายว่านอกจากการใช้รหัสลับ (password) เพื่อป้องกันข้อมูลบนคอมพิวเตอร์แล้วยังมีวิธีการใดอีกบ้าง
10. นโยบายการทำการสำรอง (backup) มีความสำคัญต่อระบบคอมพิวเตอร์อย่างไร และแบ่งเป็นระดับใดบ้าง
11. จงอธิบายความมั่นคงของเครื่องคอมพิวเตอร์ส่วนบุคคลแตกต่างจากเครื่องในระดับเมนเฟรมอย่างไร
12. จงอธิบายสาเหตุที่ต้องเพิ่มความสำคัญด้านความมั่นคงของเครือข่าย
13. จงยกตัวอย่างกระบวนการความมั่นคงด้านเครือข่าย
14. จงอธิบายเพราะเหตุใดจึงต้องควบคุมการประมวลผลและตรรกะ
15. จงอธิบายการเตรียมการเพื่อรองรับเหตุการณ์ความไม่แน่นอนที่อาจเกิดขึ้น