นโยบายความปลอดภัยระบบสารสนเทศ สำหรับบริษัทหลักทรัพย์ไทย

Information System Security Policy For Thai Securities Company

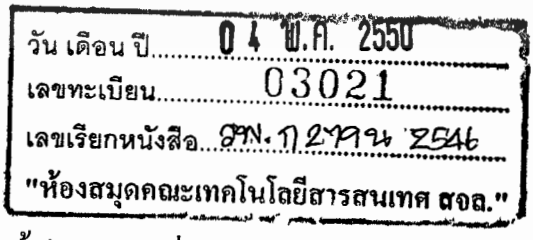
โดย

กฤษฎี ตั้งจิตถนอมสิน

รหัส 44067650

อาจารย์ที่ปรึกษา

จันทร์บูรณ์ สถิตวิริยวงศ์



รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 1 ปีการศึกษา 2546

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	นโยบายความปลอดภัยระบบสารสนเทศสำหรับบริษัทหลักทรัพย์ไทย
นักศึกษา	นาย กฤษฎิ ตั้งจิตถนอมสิน
อาจารย์ที่ปรึกษา	ดร. จันทร์บูรณ์ สถิตวิริยวงศ์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2546

บทคัดย่อ

ธุรกิจของบริษัทหลักทรัพย์ต่างๆในประเทศไทย ต้องดำเนินในภายใต้การดูแลของสำนักงานคณะกรรมการกำกับหลักทรัพย์ และ ตลาดหลักทรัพย์แห่งประเทศไทยแล้ว ซึ่งจำเป็นต้องเป็นไปตามข้อกำหนดต่างๆของธนาคารแห่งประเทศไทยอีกทางหนึ่งด้วย ประกอบกับกระแสนิยมของเรื่อง บรรษัทภิบาล และความจำเป็นด้านการจัดการและดูแลการรักษาความปลอดภัยของระบบสารสนเทศขององค์กร เป็นสิ่งจำเป็นอย่างยิ่งต่อความน่าเชื่อถือและการดำเนินธุรกิจ ต่างๆให้ถูกต้อง ปลอดภัยเป็นไปตาม มาตราฐานที่ยอมรับได้แล้ว ทั้งยังสามารถตรวจสอบ ได้อย่างเป็นระบบ และสอดคล้องกับวัตถุประสงค์ขององค์กร

Title	Information Systems Security Policy for Thai Securities Company
Student	Mr. Krisadee Tangjitthanomsin
Advisor	Dr. Chanboon Sathitwiriyawong
Level of Study	Master of Science in Information Technology
Major	Information Technology Management
Year	2003

ABSTRACT

Corporate governance is defined as ethical corporate behavior by directors or top managements charged with governance (Bank of Thailand (BOT), The Office of the Securities and Exchange Commission (SEC) and The Stock Exchange of Thailand SET)) in creation and presentation of wealth for all stakeholders. The rules and procedures should be established in managing and reporting on business risks. Company objectives are set and monitoring performance.

IT governance is the responsibility of the board of directors and executive management. It is an integral part of governance and consists of the risk management and organizational structures and business processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

ภาพที่

บทที่ 1

บทนำ

1.1 ความเป็นมา

เทคโนโลยีสารสนเทศและการแข่งขันทางธุรกิจ ทำให้การพัฒนาของโลกธุรกิจในปัจจุบันแตกต่างไปจากทศวรรษก่อนๆมาก ในธุรกิจทางการเงินอย่างเช่นบริษัทหลักทรัพย์ก็เช่นเดียวกับ ในอุตสาหกรรมประเภทอื่นๆ ที่ต้องอาศัยระบบสารสนเทศเป็นเครื่องมือสำคัญในการประกอบธุรกิจ ข้อมูลข่าวสารจึงมีความสำคัญมากในการทำงาน จำเป็นจะต้องมีการบริหารและจัดการหรือ ควบคุมให้ข้อมูลมีความถูกต้อง มีความน่าเชื่อถือได้และพร้อมที่จะใช้งานได้อยู่เสมอ แต่ในอีกด้านหนึ่งด้วยเทคโนโลยีอันทันสมัยนี้ มีข้อมูลที่ถูกส่งผ่านเครือข่ายที่เชื่อมโยงกันไปทั่วโลก และอาจถูกดักข้อมูลเพื่อประโยชน์ทางธุรกิจหรืออาชญากรรมประเภทใหม่ๆ ที่อาจจะก่อให้เกิดความเสียหายอย่างมากมายในเชิงธุรกิจได้ หรือแม้กระทั่งความน่าเชื่อถือที่มีต่อลูกค้า จึงมีความเสี่ยงที่เกิดขึ้นเกี่ยวกับการจู่โจมระบบความปลอดภัย และเป็นปัญหาต่อการใช้งานสารสนเทศผ่านระบบเครือข่าย

เทคโนโลยีที่เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศ จึงเพิ่มความสำคัญขึ้นเรื่อยตามความสามารถของเครือข่ายและความสามารถของอุปกรณ์คอมพิวเตอร์ เนื่องจากค่าใช้จ่ายในการดูแลรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ เหล่านี้มีมูลค่าค่อนข้างสูงและยังต้องการผู้เชี่ยวชาญที่เกี่ยวกับการป้องกันรักษาความปลอดภัย ของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ที่มีจำนวนไม่เพียงพอต่อความต้องการในปัจจุบันนี้

ดังนั้น จึงควรจะทราบถึงรูปแบบ ข้อบังคับ และวิธีการต่างๆของมาตรฐานด้านความปลอดภัยซึ่งเป็นที่ยอมรับและเชื่อถือได้ในแวดวงอุตสาหกรรมบริการด้านการเงินด้วยกัน ตามที่ผู้มีบทบาทเกี่ยวข้องตลอดจนมีความน่าไว้วางใจได้ในระดับสากล เพื่อความมั่นใจกับลูกค้าและผู้ลงทุน ซึ่งสอดคล้องกับ นโยบาย และกลยุทธของแต่ละองค์กรเป็นสำคัญ

1.2 วัตถุประสงค์ของการศึกษาโครงการ

เพื่อให้บรรลุวัตถุประสงค์ดังต่อไปนี้

1. นำเสนอแผนงานความปลอดภัยของระบบคอมพิวเตอร์และสารสนเทศ เพื่อใช้เป็นแนวทางและหลักเกณฑ์ในการปฏิบัติงานสำหรับบริษัทหลักทรัพย์ในไทย
2. องค์กรสามารถใช้ระบบสารสนเทศที่ปลอดภัยตามมาตรฐานและเป็นที่ยอมรับเพียงพอเป็นเครื่องมือในการดำเนินงานได้อย่างมั่นใจขึ้น
3. เป็นแนวทางที่มุ่งไปสู่การเป็น บรรษัทภิบาล ที่มีการบริหารจัดการที่ดี
4. เป็นแนวทางปฏิบัติของฝ่ายให้บริการระบบสารสนเทศที่ดี และสามารถตรวจสอบได้
5. เป็นไปตามนโยบายหลักขององค์กร หรือ กฎหมาย ข้อบังคับที่เกี่ยวข้องและสอดคล้องกับวัตถุประสงค์ขององค์กร และของฝ่ายบริการระบบสารสนเทศ

1.3 ขอบเขตของการโครงการ

ศึกษาการปฏิบัติงานของหน่วยงานในบริษัทหลักทรัพย์ ของไทยในด้านที่เกี่ยวกับความปลอดภัยของระบบคอมพิวเตอร์และสารสนเทศ การกำกับดูแล หรือข้อบังคับจากหน่วยงานภาครัฐที่เกี่ยวข้องกับกิจการบริษัทหลักทรัพย์ ซึ่งได้แก่ ธนาคารแห่งประเทศ (ธปท.) ตลาดหลักทรัพย์แห่งประเทศไทย (ตลท.) และ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (กลต.) นอกจากนี้ยังต้องศึกษามาตรฐานต่างๆด้านความรักษาปลอดภัยในระดับสากลที่เหมาะสม และเป็นที่ยอมรับในอุตสาหกรรมการเงิน ซึ่งสอดคล้องกับระบบสารสนเทศที่ใช้ตามกิจการหลักทรัพย์ในประเทศไทย

ขั้นตอนการศึกษา

1. ศึกษาโครงสร้างธุรกิจในภาพรวม
2. ศึกษาระบบสารสนเทศของบริษัทหลักทรัพย์ในไทย
3. ศึกษาข้อบังคับและแนวความคิดต่างๆที่เกี่ยวข้อง
4. ศึกษาแนวทางจาก มาตราฐาน CoBIT และ BS 7799
5. ทำการประเมินความเสี่ยง และ วิเคราะห์ความเสี่ยง
6. จัดทำแผนความปลอดภัยระบบสารสนเทศด้านต่างๆ
7. จัดทำแผนปฏิบัติการกู้คืนและแผนฉุกเฉินเพื่อการดำเนินธุรกิจอย่างต่อเนื่อง
8. ทำการตรวจสอบ และเฝ้าระวังระบบความปลอดภัยสารสนเทศ อย่างเป็นระบบ

1.4 ผลที่คาดว่าจะได้รับจากการศึกษาโครงการ

1. เพื่อเป็นการเตรียมบริษัทหรือองค์กรก้าวสู่มาตรฐานสากล โดยวางแนวทางนโยบาย และการปฏิบัติให้สอดรับกับมาตรฐานที่เป็นที่ยอมรับ
2. เพื่อเสริมสร้างความปลอดภัยในระบบคอมพิวเตอร์ และระบบสารสนเทศขององค์กร
3. สนับสนุนให้พนักงานในองค์กรตระหนักถึงเรื่องความปลอดภัย และเล็งเห็นความเสี่ยงที่อาจจะเกิดขึ้นจากการปฏิบัติงานได้
4. มีระบบความปลอดภัยของระบบสารสนเทศ ที่พร้อมให้บริการ มีการเข้าถึงและใช้งานทรัพยากรได้เสมอ มีข้อมูลที่รักษาความลับ และความถูกต้องสมบูรณ์ข้อมูล
5. มีการป้องกันการใช้งานระบบสารสนเทศโดยไม่ได้รับอนุญาตที่เหมาะสม
6. รองรับการสอบทานและตรวจสอบ ให้เป็นไปตามข้อบังคับจากหน่วยงานที่เกี่ยวข้องและเป็นไปตามมาตรฐานสากลอย่างเป็นระบบและต่อเนื่อง

บทที่ 2

ระบบความปลอดภัยของระบบสารสนเทศ

2.1 ทฤษฎีที่เกี่ยวกับความปลอดภัยระบบสารสนเทศ

จุดประสงค์ของระบบการรักษาความปลอดภัย เพื่อเป็นการรักษาความลับ ป้องกันไม่ให้มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือเกี่ยวข้องและ เพื่อจัดลำดับความสำคัญของข้อมูลในการดำเนินนโยบายป้องกันรักษาข้อมูลเพื่อสอดคล้องกับความสำคัญของข้อมูลซึ่งแสดงความสัมพันธ์ต่อไปนี้

1. เพื่อรักษาความลับของข้อมูล (confidentiality)
2. เพื่อป้องกันการปลอมแปลงข้อมูล (Integrity)
3. เพื่อทำให้ระบบนั้นพร้อมทำงานได้ตามปกติและเต็มประสิทธิภาพเสมอ(Availability)

รูปที่ 2.1 แสดงความสมดุลของวัตถุประสงค์ในการรักษาความปลอดภัย

ระบบรักษาความปลอดภัยที่มีระดับความสามารถในการรักษาความลับที่สูงมากอาจส่งผลกระทบต่อส่วนอื่นด้วย เช่นประสิทธิภาพในการทำงานและความสะดวกในการเข้าถึงหรือการใช้งานระบบ ดังนั้นจึงต้องมีการพิจารณาถึงความเหมาะสมในการเลือกระดับของระบบรักษาความปลอดภัยแบบต่างๆในด้านความสะดวก ปริมาณงาน และประสิทธิภาพของระบบงานนั้นๆอีกด้วย เช่นเดียวกับการเลือกระดับในด้านความสะดวกในการใช้งาน ต้องไม่มากเกินไปจนมีผลกระทบ

กับความถูกต้องและการรักษาความลับข้อมูล การที่ระบบคอมพิวเตอร์ไม่สามารถรักษาความปลอดภัยของข้อมูลนั้น โดยมากเกิดจากความผิดพลาดของระบบการรักษาความปลอดภัยที่มีอยู่ในระบบนั่นเอง สาเหตุของความผิดพลาดอาจเกิดจากหลายสาเหตุนับตั้งแต่การออกแบบสร้างระบบซอฟต์แวร์นั้นไป จนถึงการติดตั้งและนำตัวซอฟต์แวร์ไปใช้งาน รวมทั้งการดูแลรักษาใช้งานระบบซอฟต์แวร์นั้นๆอย่างรัดกุมตามขั้นตอนการใช้งานที่ถูกต้อง อย่างไรก็ตามเราสามารถจะจำแนกสาเหตุของความผิดพลาดหรือข้อบกพร่องต่างๆเป็นหลักใหญ่ๆ ได้ดังนี้คือ

- การเปิดเผยข้อมูลที่เป็นความลับ (Exposure) จากระบบคอมพิวเตอร์โดยที่ข้อมูลนั้นอาจได้รับการเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาต หรือข้อมูลนั้นอาจเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาตด้วยเช่นกัน
- การที่ระบบมีจุดอ่อนภายในตัวอยู่แล้ว (Vulnerabilities) ซึ่งระบบอาจจะถูกโจมตี(Attack)ได้ง่ายโดยใช้จุดอ่อนเหล่านี้เป็นจุดเริ่มต้น
- การที่มีภัยคุกคาม (Threats) ต่อระบบคอมพิวเตอร์ ซึ่งภัยคุกคามนั้นอาจเกิดจากพวกนักจารกรรมข้อมูล (Hacker) หรือเกิดจากภัยธรรมชาติ เช่นน้ำท่วม หรือไฟดับ เป็นต้น หรือแม้กระทั่งอาจเกิดความผิดพลาดในการทำงานหรือการออกแบบตัวฮาร์ดแวร์หรือซอฟต์แวร์เอง

2.2 ภัยคุกคามต่างๆ ต่อระบบความปลอดภัย

ภัยคุกคามที่มีต่อระบบคอมพิวเตอร์นั้น สามารถทำอันตรายต่อส่วนต่างๆ ของระบบได้ไม่ว่าจะเป็น ตัวฮาร์ดแวร์ซอฟต์แวร์ หรือตัวข้อมูล ที่ถูกเก็บไว้ในระบบ เราสามารถจำแนกชนิดของภัยคุกคามได้เป็นชนิดใหญ่ๆ ดังนี้คือ

- การต่อต้านการทำงานของระบบ (Interruption) นั่นก็คือการโจมตีระบบจนทำให้ระบบเสียหายจนไม่สามารถทำหน้าที่ของมันเองได้ตามปกติหรืออย่างเต็มประสิทธิภาพ เช่น การทำลายส่วนฮาร์ดแวร์ การลบบางส่วนของโปรแกรม หรือการเปลี่ยนแปลงแก้ไขโปรแกรม ไฟล์ที่มีผลต่อการทำงานของระบบ เป็นต้น
- การลักลอบเข้ามาในระบบ (Interception) คือการที่มีการเข้ามาในระบบและดำเนินกิจกรรมต่างๆโดยไม่ได้รับอนุญาต การลักลอบนั้นจะทำโดยตัวโปรแกรมหรือโดยบุคคลโดยตรง
- การเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Modification) คือการเปลี่ยนแปลงแก้ไขข้อมูลที่สำคัญที่เก็บภายในระบบฐานข้อมูล (Database) ของระบบ โดยที่ข้อมูลนั้นอาจเอื้อประโยชน์แก่ผู้ทุจริตได้

2.2.1 ภัยคุกคามที่มีต่อระบบต่างๆ (Computer Threats)

- **ภัยต่อระบบฮาร์ดแวร์ (Hardware Security Threats)**

สามารถจำแนกออกเป็น 3 กลุ่มใหญ่ๆ คือ ภัยที่มีต่อระบบการจ่ายไฟฟ้า ภัยที่เกิดจากการทำลายทางกายภาพโดยตรงต่อระบบคอมพิวเตอร์ เช่น น้ำท่วม และภัยจากการลักขโมย

- **ภัยคุกคามที่มีต่อระบบซอฟต์แวร์ (Software Security Threats)**

สามารถจำแนกออกเป็น 3 พวกใหญ่ๆ คือ การลบซอฟต์แวร์ ทำให้เกิดความเสียหายต่อระบบ การขโมยซอฟต์แวร์ เช่นการคัดลอก และการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ ทำให้ข้อมูลสำคัญบิดเบือนไปซึ่งลักษณะของซอฟต์แวร์ที่ถูกเปลี่ยนแปลงเพื่อจุดประสงค์ที่ไม่ดีนั้นสามารถแบ่งออกเป็นพวกใหญ่ๆ ดังนี้

  - ประเภท Trojan Horses เป็นโปรแกรมที่แฝงตัวอยู่ในโปรแกรมอื่นซึ่งอาจทำให้เกิดความเสียหายได้
  - ประเภท Virus มีลักษณะคล้ายโปรแกรมพวก Trojan Horses แต่จะสามารถกระจายตัวมันเองออกไปได้
  - ประเภท Trapdoor เป็นโปรแกรมที่ถูกนักออกแบบใส่ไว้เป็นส่วนหนึ่งของโปรแกรม เพื่อความง่ายต่อการปลดระบบการรักษาความปลอดภัยหลังจากที่ได้มีการนำไปใช้งานแล้ว
  - พวกโปรแกรม ขโมยข้อมูล (Information Leaks) จะทำการเผยแพร่ข้อมูลที่เป็นความลับออกไปโดยไม่ได้รับอนุญาต

- **ภัยที่มีต่อระบบข้อมูล (Data Threats)**

จะทำการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต หรืออาจมีการเปิดเผยข้อมูลบางอย่างซึ่งอาจทำให้ข้อมูลนั้นไม่สารถนำมาใช้งานได้

2.2.2 จุดอ่อนของระบบคอมพิวเตอร์ (Vulnerabilities)

จุดอ่อนที่เราจะต้องทำการป้องกันในระบบคอมพิวเตอร์มีดังนี้

ฮาร์ดแวร์ (Hardware)

- การถูกต่อต้านการทำงาน
- การถูกขโมย
- การถูกการแก้ไข

ซอฟต์แวร์ (Software)

- การถูกต่อต้านการทำงาน
- การถูกลักลอบเข้ามาใช้งาน
- การถูกแก้ไข

ข้อมูล (Data)

- การถูกต่อต้านการทำงาน
- การถูกขโมย
- การถูกลอกเลียนแบบ

2.3 หลักการทั่วไปในการควบคุมและรักษาความปลอดภัยให้กับระบบข้อมูลข่าวสาร

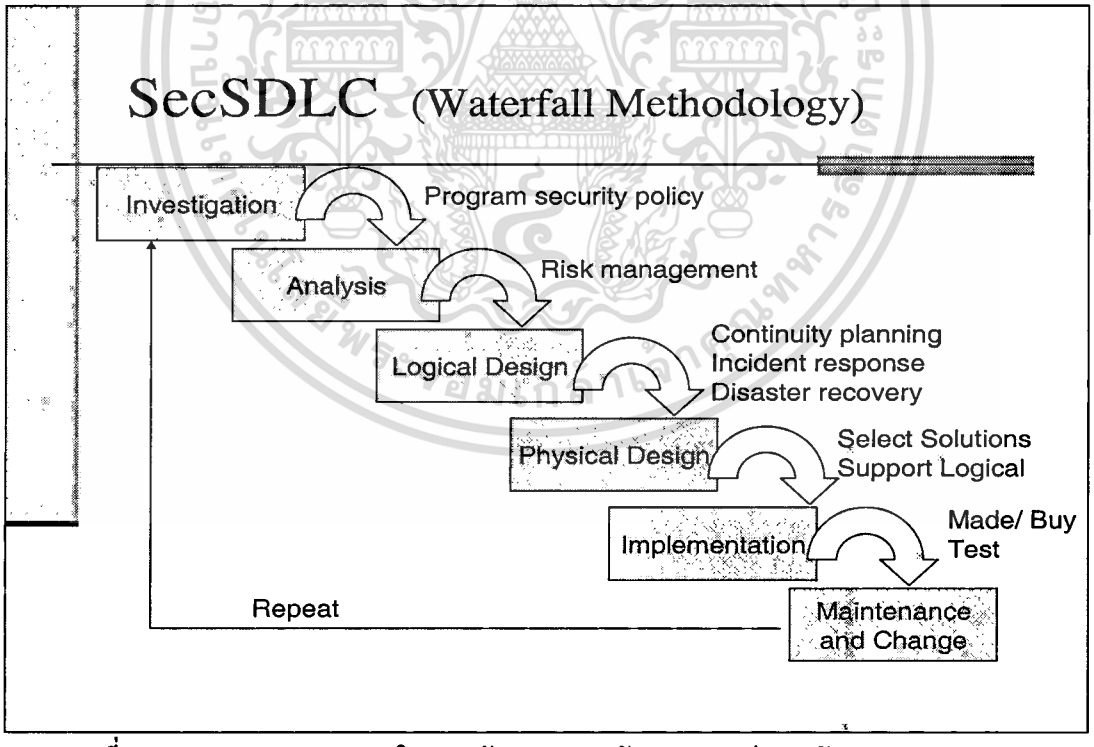
วิธีการในการต่อต้านการถูกโจมตีและการถูกจารกรรมทางข้อมูลได้แก่การควบคุม (Control) ส่วนต่างๆ ของระบบอย่างรัดกุม วิธีการที่ใช้ในการควบคุมมีดังนี้คือ

- **การใช้วิธีการเข้ารหัสข้อมูล (Encryption Techniques)** การใช้วิธีนี้จะเป็นวิธีที่เหมาะสมที่สุดวิธีหนึ่งในการป้องกันข้อมูลที่เป็นความลับให้แก่บุคคลที่ต้องการ โดยทั่วไปจะมีอยู่ 2 วิธีคือ
  1. การเข้ารหัสข้อมูลแบบใช้กุญแจรหัสสมมาตร (Symmetric-Key Encryption)
  2. การเข้ารหัสข้อมูลแบบใช้ กุญแจรหัสอสมมาตร (Asymmetric-Key Encryption)
- **การควบคุมการรักษาความปลอดภัยโดยตัวซอฟต์แวร์ (Software Control)** ระบบการควบคุมความปลอดภัยของซอฟต์แวร์ สามารถป้องกันการโจมตีจากระบบภายนอกได้ภายในระดับวิธีการที่ใช้มีอยู่ 3 วิธีคือ
  1. การควบคุมจากระบบภายในของซอฟต์แวร์เอง (Internal Program Controls) คือการที่โปรแกรมส่วนย่อยๆที่เป็นส่วนประกอบของซอฟต์แวร์นั้นควบคุมสิทธิในการเข้าถึง
  2. การควบคุมความปลอดภัยระบบปฏิบัติการ (Operating System Controls) คือการควบคุมสิทธิในการเข้าถึงและการใช้ข้อมูลในส่วนต่างๆภายในระบบคอมพิวเตอร์ของผู้ใช้คนหนึ่ง
  3. การควบคุมตั้งแต่การออกแบบและสร้างซอฟต์แวร์ (Development Controls) ระบบการรักษาความปลอดภัยและระบบการทำงานของซอฟต์แวร์นั้นจะต้องได้รับการสร้างและทดสอบอย่างถูกหลักวิธีการของวิศวกรรมซอฟต์แวร์ (Software Engineering)
- **การควบคุมความปลอดภัยของระบบโดยใช้ฮาร์ดแวร์ (Hardware Controls)** เช่นการใช้ Smart card การใช้กุญแจล็อค ซึ่งเป็นวิธีการที่มีประสิทธิภาพและราคาถูก

การใช้นโยบายในการควบคุม (Policies) นโยบายของหน่วยงานก็มีผลสำคัญอย่างยิ่งในการรักษาความปลอกภัยของข้อมูล ดังนั้นหน่วยงานที่มีส่วนเกี่ยวข้องจะต้องกำหนดแผนในการป้องกันและแผนในการกู้ภัยที่อาจจะเปิดขึ้นได้ **การป้องกันทางกายภาพ (Physical Controls)** เช่น การล็อคห้องคอมพิวเตอร์ อย่างแน่นหนาเมื่อไม่มีการใช้งานแล้ว การใช้ยามเฝ้า การทำ Backup Disks และเก็บไว้ในส่วนที่ปลอดภัย

2.4 The Security Systems Development Life Cycle

การพัฒนาระบบรักษาความปลอดภัย เช่นเดียวกับการ พัฒนาระบบอื่นๆที่ต้องจัดทำโครงการที่มีขั้นตอนแบ่งไว้เหมือนกับ System Development Life Cycle (SDLC) ที่ใช้ในการพัฒนาระบบทางด้านเทคโนโลยีสารสนเทศทั่วไป จึงดัดแปลงมาให้เหมาะสมกับ ขั้นตอนของการพัฒนาระบบรักษาความปลอดภัยด้วย โดยใช้ตัวย่อว่า SecSDLC ซึ่งมีกระบวนการพื้นฐานพอสังเขปดังแสดงในภาพเบื้องล่างนี้



ภาพที่ 2.2 แสดงกระบวนการในการพัฒนาระบบรักษาความปลอดภัยของสารสนเทศ

2.4.1 Investigation เป็นขั้นตอนแรกที่เกี่ยวข้องกับฝ่ายบริหาร กล่าวถึงวัตถุประสงค์ หลักการ และ แนวความคิดเชิง นโยบาย และการทำงบประมาณ ต่างๆที่จะจัดทำขึ้นสำหรับภายในองค์กรที่เกี่ยวข้องกับด้านความปลอดภัยสารสนเทศ และรวมไปถึงการจัดตั้งคณะทำงานด้านนี้ขึ้นมาโดยเฉพาะ ให้มีบทบาทหน้าที่และ ความรับผิดชอบเกี่ยวกับระบบสารสนเทศที่ต้องมีนโยบาย และแผนปฏิบัติงาน หรือ Program Security Policy และแม้กระทั่งการติดตาม เฝ้าระวังการตรวจสอบระบบสารสนเทศให้มีความปลอดภัยที่เชื่อถือได้เพียงพอต่อการดำเนินธุรกิจอย่างมั่นใจ

2.4.2 Analysis คือขั้นตอน วิเคราะห์ ข้อมูล เอกสารและผลจากการเข้าไปศึกษาในขั้นตอนแรกที่ได้มา ทำการพิจารณาเปรียบเทียบ นโยบายเดิม และมาตรการต่างๆด้านความปลอดภัย ที่ใช้อยู่ในปัจจุบัน มีการควบคุม และให้ความสำคัญ มีการจัดการหรือข้อควรปฏิบัติที่เกิดขึ้นจริง อย่างเหมาะสมหรือไม่ แม้นกระทั่งความเชื่อมโยง หรือผลกระทบกับ กฎระเบียบข้อบังคับที่เปลี่ยนแปลง เพิ่มเติมขึ้นมาใหม่ มีการรองรับให้เหมาะสมเพียงพอหรือไม่ โดยเน้นที่การจัดทำ Risk Management ซึ่งมีผลกระทบกับสารสนเทศ และการดำเนินธุรกิจอย่างต่อเนื่องอย่างแท้จริง

2.4.3 Logical Design การออกแบบด้านความปลอดภัยในมุมของ Logical ให้เป็นตามสิ่งที่ได้มาจากขั้นตอนแรกๆทั้ง2 ส่วนให้สามารถจัดการกับปัญหาด้านความปลอดภัยให้ครอบคลุมและเน้นย้ำตามความสำคัญที่ให้ไว้ มักกล่าวเน้นเรื่องของการทำ Continuity Planning กับ Incident Response และ การวางแผนสำหรับ Disaster Recovery เป็นสิ่งสำคัญ

2.4.4 Physical Design ขั้นตอนนี้เป็นออกแบบ จัดหาและเลือกใช้ เทคโนโลยีเพื่อสนับสนุนการออกแบบที่ได้จากขั้นตอนที่แล้ว และได้ทำการตกลงเป็นที่ยอมรับเรียบร้อยไปแล้ว ซึ่งอาจจะมีความเปลี่ยนแปลงด้านความต้องการที่เปลี่ยนไป เพื่อให้ได้ทางเลือกที่เหมาะสมที่สุดและเกิดประโยชน์สูงสุดกับองค์กรด้วยก่อนที่จะตัดสินใจเลือกเทคโนโลยีที่ตรงกับที่ออกแบบ

2.4.5 Implementation ขั้นตอนนี้ก็จะเป็นการจัดทำ หรือ จัดซื้อ เพื่อให้ได้มาซึ่งระบบรักษาความปลอดภัยของระบบสารสนเทศขององค์กร แล้วทำการทดสอบ การใช้ และประเมินผล รวมทั้งการจัดฝึกอบรมกับผู้เกี่ยวข้องโดยเฉพาะ

2.4.6 Maintenance and Change กระบวนการสุดท้ายของSecSDLC นี้มีความสำคัญที่สุด เพราะต้องมีการเฝ้าตรวจ ทดสอบ และปรับปรุงซ่อมแซมระบบรักษาความปลอดภัยสารสนเทศ ให้ทันสมัย และใช้งานได้ ไม่เป็นจุดอ่อน อยู่สม่ำเสมอ การคุกคามต่อระบบสารสนเทศที่มากมาย หรือไม่เคยพบเจอ มาก่อนเพิ่มขึ้นอยู่ทุกๆวัน จนกว่าระบบที่ออกแบบไว้ไม่สามารถรองรับด้านความปลอดภัยที่เปลี่ยนแปลงไปได้ จึงจำเป็นต้องย้อนกลับไปเริ่มกระบวนในขั้นตอนแรกใหม่ เพื่อให้เกิดระบบรักษาความปลอดภัยรุ่นใหม่ที่รองรับสถานการณ์นั้นได้

บทที่ 3

ระบบสารสนเทศของบริษัทหลักทรัพย์ในไทย

3.1 การดำเนินธุรกิจของบริษัทหลักทรัพย์[1]

บริษัทหลักทรัพย์ หมายถึง บริษัทหรือสถาบันการเงินที่ได้รับใบอนุญาตให้ประกอบธุรกิจหลักทรัพย์ ดังนี้

การเป็นนายหน้าซื้อขายหลักทรัพย์

- การเป็นนายหน้าหรือตัวแทนเพื่อซื้อ ขาย หรือแลกเปลี่ยนหลักทรัพย์ให้แก่บุคคลอื่น
- ได้รับค่านายหน้า ค่าธรรมเนียม หรือผลตอบแทนอื่น

การค้าหลักทรัพย์

- การซื้อ ขาย หรือแลกเปลี่ยนหลักทรัพย์ในนามตนเอง
- ทำการค้านอกตลาดหลักทรัพย์ หรือศูนย์ซื้อขายหลักทรัพย์

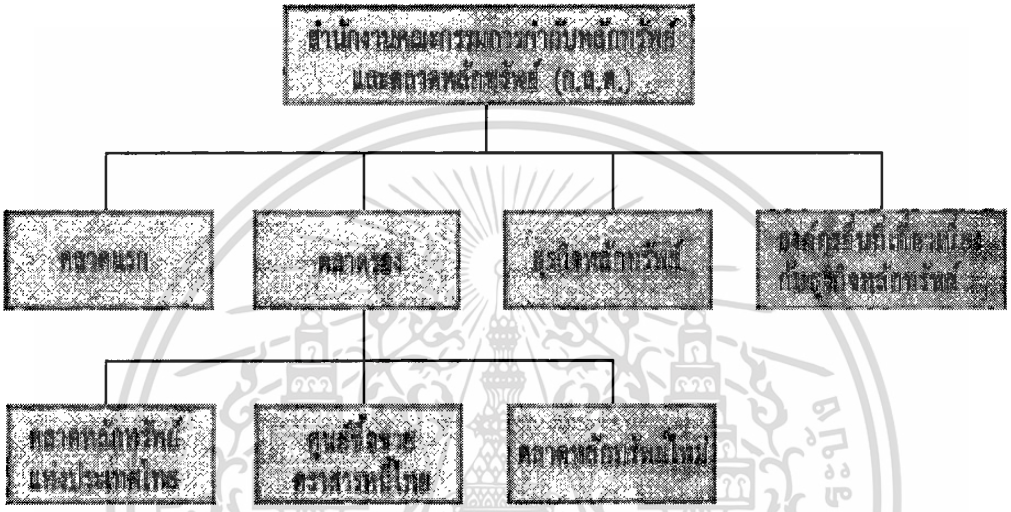
การเป็นที่ปรึกษาการลงทุน

- การให้คำแนะนำไม่ว่าทางตรง และทางอ้อม แก่ประชาชน เกี่ยวกับ
    - คุณค่าของหลักทรัพย์ หรือ
    - ความเหมาะสมในการลงทุนในหลักทรัพย์ หรือ
    - การซื้อขายหลักทรัพย์ใดๆ

---

[1] ที่มา : **ฝ่ายกำกับธุรกิจนายหน้าและค้าหลักทรัพย์** สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ http://www.sec.or.th/mktsup/profile/license.shtml

- ได้รับค่าธรรมเนียม หรือผลตอบแทนอื่น
- ไม่รวมการให้คำปรึกษาในลักษณะที่คณะกรรมการ ก.ล.ต. กำหนด (เช่น การจัดอันดับความน่าเชื่อถือ)



ภาพที่ 3.1 โครงสร้างองค์กรที่เกี่ยวข้องกับบริษัทหลักทรัพย์ในไทย

3.1.1 การจัดจำหน่ายหลักทรัพย์

- การรับหลักทรัพย์ทั้งหมด หรือบางส่วนจากบริษัทหรือเจ้าของหลักทรัพย์ไปเสนอขายต่อประชาชน
- ได้รับค่าธรรมเนียม หรือผลตอบแทนอื่น

บุคคลที่ทำหน้าที่ติดต่อกับผู้ลงทุนในธุรกิจหลักทรัพย์ ในตลาดทุนได้แก่

- **เจ้าหน้าที่การตลาด/ผู้ขายหน่วยลงทุน/ตัวแทนสนับสนุน**
- **ผู้ทำหน้าที่ชักชวนลูกค้าหรือวางแผนการลงทุน หรือเป็นตัวแทนด้านการตลาดกองทุนส่วนบุคคล**
- **ผู้ให้คำแนะนำการลงทุนในหลักทรัพย์**

3.1.2 การซื้อขายหลักทรัพย์ในตลาดหลักทรัพย์แห่งประเทศไทย [2]

ตลาดหลักทรัพย์เปิดให้มีการซื้อขายครั้งแรกเมื่อวันที่ 30 เมษายน 2518 ภายใต้วิธีการซื้อขายแบบประมูลราคาอย่างเปิดเผย (Open Auction) ด้วยวิธีเคาะกระดานในห้องค้าหลักทรัพย์ (Trading Floor) ในวันที่ 31 พฤษภาคม 2534 ตลาดหลักทรัพย์ได้นำระบบการซื้อขายด้วยคอมพิวเตอร์ที่เรียกว่าระบบASSET (Automated System for the Stock Exchange of Thailand) มาใช้แทน ทั้งนี้เพื่อให้เกิดความยุติธรรม ความรวดเร็วและรองรับกับปริมาณการซื้อขายที่ขยายตัวเพิ่มขึ้น ซึ่งระบบคอมพิวเตอร์ดังกล่าวเป็นระบบกระจายศูนย์ (Distributed System) ผู้ลงทุนสามารถทำการซื้อขายหลักทรัพย์โดยผ่านระบบการซื้อขายของตลาดหลักทรัพย์ได้ 2 วิธี ได้แก่

2.5.1.1 Automatic Order Matching (AOM)

เป็นวิธีการซื้อขายที่ผู้ซื้อและผู้ขาย ส่งการเสนอซื้อและเสนอขายด้วยคอมพิวเตอร์ผ่านเข้ามายังระบบการซื้อขายของตลาดหลักทรัพย์ โดยที่ระบบคอมพิวเตอร์ของตลาดหลักทรัพย์จะทำการเรียงลำดับและจับคู่คำสั่งซื้อขายให้โดยอัตโนมัติ

- **การจัดเรียงลำดับคำสั่งซื้อขาย** เมื่อสามารถส่งคำสั่งซื้อขายเข้ามา ระบบการซื้อขายจะเก็บคำสั่งซื้อขายไว้ตั้งแต่เวลาที่ส่งคำสั่งซื้อขายจนถึงสิ้นวันทำการ และจัดเรียงคำสั่งซื้อขายตามลำดับของราคาและเวลาที่ดีที่สุด (Price then Time Priority) โดยมีหลักการคือ

  (1) คำสั่งซื้อที่มีราคาเสนอซื้อสูงที่สุดจะถูกจัดเรียงไว้ในลำดับที่หนึ่ง และถ้ามีราคาเสนอซื้อที่สูงกว่าถูกส่งเข้ามาใหม่ จะจัดเรียง ราคาเสนอซื้อที่สูงกว่าเป็นการเสนอซื้อในลำดับแรกก่อนและถ้ามีการเสนอซื้อในแต่ละราคามากกว่าหนึ่งรายการให้จัดเรียงตามเวลาโดยการเสนอซื้อที่ปรากฏในระบบการซื้อขายก่อนจะถูกจัดไว้เป็นการเสนอซื้อในลำดับก่อน

  (2) คำสั่งขายที่มีราคาเสนอขายต่ำที่สุดจะถูกจัดเรียงไว้ในลำดับที่หนึ่ง และถ้ามีราคาเสนอขายที่ต่ำกว่าถูกส่งเข้ามาใหม่จะจัดเรียงราคาเสนอขายที่ต่ำกว่าเป็นการเสนอขายในลำดับแรกก่อนละถ้ามีการเสนอขายในแต่ละราคามากกว่าหนึ่งรายการให้จัดเรียงตามเวลาโดยการเสนอขายที่ปรากฏในระบบการซื้อขายก่อนจะถูกจัดไว้เป็นการเสนอขายในลำดับก่อน

---

[2] ที่มา : ตลาดหลักทรัพย์แห่งประเทศไทย (ตลท.)

http://www.set.or.th/th/about/how/trading/system_p1.html

- **การคำนวณหาราคาเปิด (Opening Price) และการคำนวณหาราคาปิด (Close Price)** ตลาดหลักทรัพย์ได้กำหนดให้คำนวณราคาเปิดหรือปิดใช้วิธี Call Market ในเวลาเปิดหรือปิดทำการซื้อขายที่ได้จากวิธี การแบบสุ่มเลือกเวลา (Random Time) โดยตลาดหลักทรัพย์จะกำหนดช่วงเวลาให้บริษัทสมาชิกส่งคำสั่งซื้อขายที่ระบุราคาแบบไม่มีเงื่อนไข ยกเว้นคำสั่งซื้อขายแบบ ATO (คำสั่งที่ต้องการซื้อขายหลักทรัพย์ที่ราคาเปิด) หรือ ATC (คำสั่งที่ต้องการซื้อ ขายหลักทรัพย์ที่ราคาปิด) เข้ามาในระบบการซื้อขายของตลาดหลักทรัพย์โดยยังไม่มีการจับคู่ แต่ระบบการซื้อขายจะนำคำสั่ง ซื้อขายทั้งหมดมาคำนวณเพื่อหาราคาเปิดหรือราคาปิด จากนั้นเมื่อถึงช่วงเวลาที่กำหนดระบบจะมีการ Random เพื่อหาเวลาเปิดหรือปิดการซื้อขาย

ตลาดหลักทรัพย์ได้นำวิธี Call Market มาใช้ในการคำนวณหา ราคาเปิด / ปิด ดังนี้

(1) เป็นราคาที่ทำให้เกิดการซื้อขายมากที่สุดเมื่อแรกเปิดทำการซื้อขายประจำวัน

(2) ในกรณีที่ราคาตาม (1) มีมากกว่าหนึ่งราคา ให้ใช้ราคาที่ใกล้เคียงราคาซื้อขายครั้งสุดท้ายในวันทำการก่อนหน้ามากที่สุด

(3) ในกรณีที่ราคาตาม (2) มีมากกว่าหนึ่งราคา ให้ใช้ราคาที่สูงกว่า

- **การจับคู่การซื้อขาย (Matching)** เมื่อคำสั่งซื้อขายผ่านเข้ามาในระบบซื้อขายแล้ว ระบบซื้อขายจะตรวจสอบว่าคำสั่งนั้นสามารถจับคู่กับคำสั่งด้านตรงข้ามได้ทันทีหรือไม่ ถ้าคำสั่งนั้นสามารถจับคู่ได้ทันที ระบบก็จะทำการจับคู่ให้ แต่ถ้าคำสั่งนั้นไม่สามารถจับคู่ได้ ระบบจะจัดเรียงคำสั่ง ซื้อขายนั้นตามหลักการ Price then Time Priority ตามที่กล่าวข้างต้น

3.1.2.2. Put-through (PT)

เป็นการซื้อขายที่ผู้ซื้อและผู้ขายได้ทำการต่อรองเพื่อตกลงซื้อขายกัน (Dealing) แล้วจึงบันทึกรายการซื้อขายนั้นเข้ามา ในระบบซื้อขาย (Put-through) โดยที่การซื้อขายแบบ PT จะไม่นำกฎเกณฑ์ในเรื่องการกำหนด Ceiling & Floor และ ช่วงราคา (Spread) มาใช้ และบริษัทสมาชิกสามารถประกาศโฆษณา (Advertise) การเสนอซื้อหรือ เสนอขายของตน ผ่านระบบการซื้อขายได้ การซื้อขายภายใต้ระบบ PT สามารถแบ่งออกได้เป็น 2 ประเภทคือ

(1) การซื้อขายระหว่างสมาชิก (Two-firm Put-through) มีหลักเกณฑ์ที่สำคัญดังนี้

หากมีการตกลงซื้อขายกันแล้ว ให้สมาชิกผู้ขายบันทึกรายการซื้อขายเข้ามาในระบบการซื้อขายก่อน จากนั้นให้สมาชิกผู้ซื้อทำการรับรองรายการซื้อขาย (Approve) โดยจะต้องบันทึกรายการซื้อขายเข้ามาในระบบภายใน 15 นาที นับตั้งแต่มีการตกลงซื้อขายกัน หากบันทึกรายการซื้อขายดังกล่าวไม่ทันในช่วงเวลาซื้อขายนั้นๆ ให้บันทึกเข้ามาภายใน 15 นาทีแรกของช่วงเวลาซื้อขาย

ถัดไป หลังจากผู้ซื้อ Approve รายการแล้ว รายการซื้อขายดังกล่าวจะถูกบันทึกเข้ามายังระบบซื้อขายของตลาดหลักทรัพย์

(2) การซื้อขายโดยสมาชิกผู้ซื้อและผู้ขายเป็นรายเดียวกัน (One-firm Put-through) มีหลักเกณฑ์ที่สำคัญดังนี้หากมีการตกลงซื้อขายกัน ให้สมาชิกบันทึกรายการซื้อขายเข้ามายังตลาดหลักทรัพย์ภายใน 15นาที นับตั้งแต่มีการตกลงซื้อขายกัน หาก Key รายการซื้อขายดังกล่าวไม่ทันในช่วงเวลาซื้อขายนั้นๆ ให้ Key เข้ามาภายใน 15 นาทีแรกของช่วงเวลาซื้อขายถัดไป

- **การกำหนดราคาเสนอซื้อขายสูงสุดและต่ำสุดของหลักทรัพย์ (Ceiling & Floor)** ตลาดหลักทรัพย์กำหนดให้ราคาเสนอซื้อเสนอขายหลักทรัพย์ในแต่ละวันสามารถเปลี่ยนแปลงเพิ่มขึ้นหรือลดลงได้สูงสุดได้ไม่เกินร้อยละ 30 ของราคาซื้อขายครั้งสุดท้ายในวันทำการก่อนหน้า แต่อย่างไรก็ตามข้อกำหนดดังกล่าวได้รับการยกเว้นในกรณีต่อไปนี้
  - เริ่มการซื้อขายวันแรกในตลาดหลักทรัพย์
  - เป็นการซื้อขายวันแรกที่มีการขึ้นเครื่องหมาย XD, XR, XS หรือ XA
  - หลักทรัพย์นั้นไม่มีการซื้อขายติดต่อกันเกินกว่า 15 วันทำการ
  - หลักทรัพย์นั้นมีราคาต่ำกว่า 1 บาท

สำหรับราคาซื้อขายใบสำคัญแสดงสิทธิที่จะซื้อหุ้นหรือหน่วยลงทุน (Warrant) สามารถเปลี่ยนแปลงเพิ่มขึ้นสูงสุดหรือลดลงต่ำสุดไม่เกินร้อยละ 30 ของหุ้นสามัญคูณด้วยสิทธิในการซื้อหุ้นหรือหน่วยลงทุนที่จะได้รับจากการใช้สิทธิของใบสำคัญแสดงสิทธิจำนวน 1 สิทธิ

ยกเว้นในกรณีที่หุ้นสามัญมี Ceiling & Floor เป็น 100% ของราคาซื้อขายครั้งสุดท้ายในวันทำการก่อนหน้า ก็ให้ใบสำคัญแสดงสิทธิที่จะซื้อหุ้นหรือหน่วยลงทุน สามารถเปลี่ยนแปลงเพิ่มขึ้นสูงสุดหรือลดลงต่ำสุดไม่เกินร้อยละ 100 ของหุ้นสามัญคูณ ด้วยสิทธิในการซื้อหุ้น หรือหน่วยลงทุนที่จะได้รับจากการใช้สิทธิของใบสำคัญแสดงสิทธิจำนวน 1 สิทธิ

3.1.3 การซื้อขายผ่านระบบอินเทอร์เน็ต (Internet Trading)

การซื้อขายหลักทรัพย์ผ่านอินเทอร์เน็ตเป็นช่องทางการลงทุนซื้อขายที่มีประสิทธิภาพช่องทางหนึ่งโดยผู้ลงทุนสามารถส่งคำสั่งซื้อขายไปยังโบรกเกอร์ ผ่านระบบอิเล็กทรอนิกส์ไม่ว่าจะอยู่

ที่ใดก็ตามได้ทั่วโลกอย่างสะดวกและรวดเร็วนอกจากนี้ ผู้ลงทุนยังสามารถค้นหาข้อมูลซื้อขายที่ต้องการได้ เช่น ข้อมูลซื้อขายในอดีต รวมทั้งข้อมูล Real-time

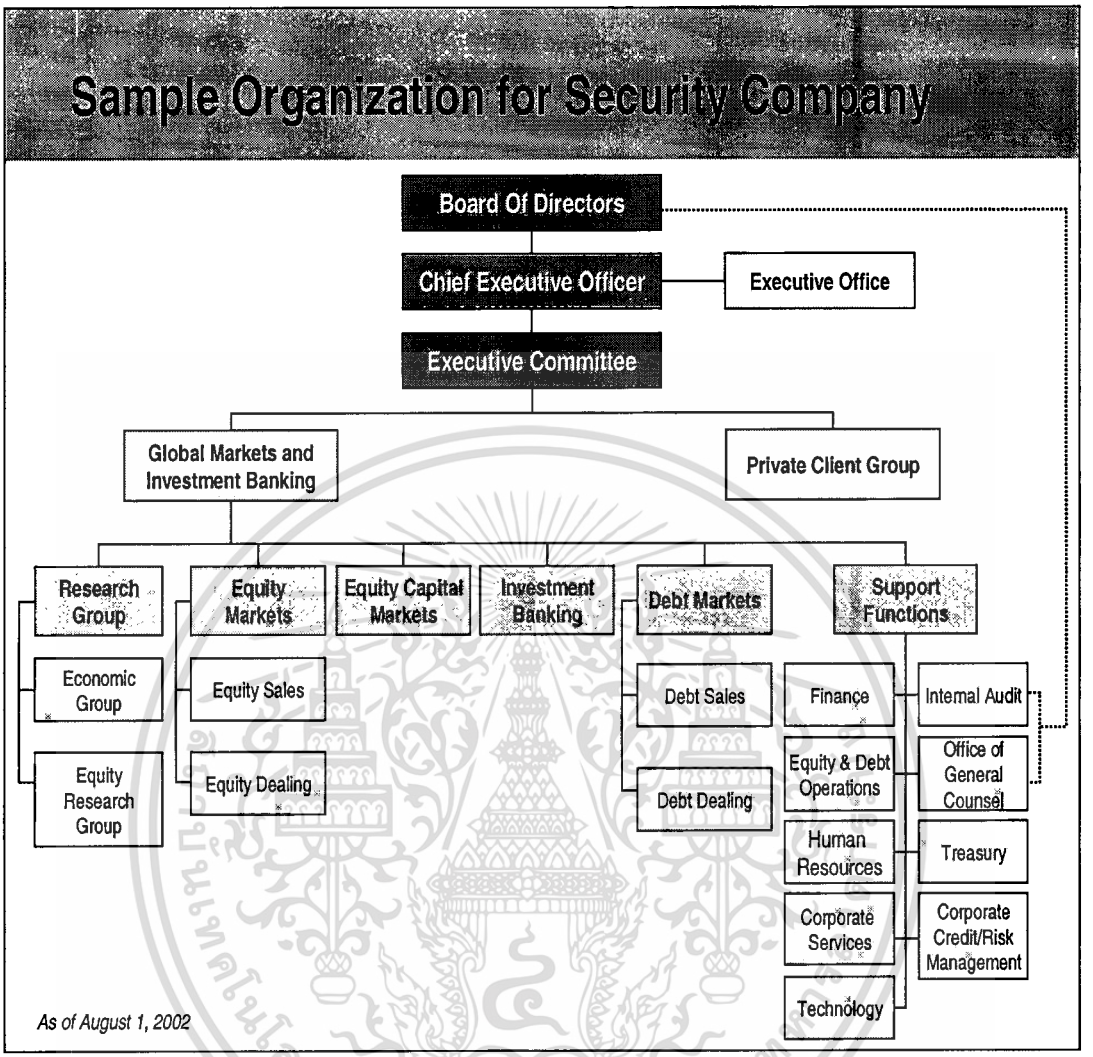
ตลาดหลักทรัพย์อนุญาตให้สามารถซื้อขายหลักทรัพย์จดทะเบียนทุกประเภทในตลาดหลักทรัพย์ และตลาด MAI ผ่านอินเทอร์เน็ตได้ โดยโบรกเกอร์จะต้องรับผิดชอบต่อผลที่เกิดจากคำสั่งซื้อขายหลักทรัพย์ของลูกค้า การซื้อขายหลักทรัพย์ผ่านอินเทอร์เน็ต จะต้องซื้อขายด้วยวิธี AOM (Automatic Order Matching) บนกระดานหลัก กระดานหน่วยย่อย และกระดานต่างประเทศ และให้ส่งคำส่งซื้อขายได้เฉพาะคำสั่งที่ระบุราคา (Limit Order) โดยคำสั่งซื้อขายที่ส่งเข้ามาในแต่ละวัน ถ้าไม่ได้รับการจับคู่ซื้อขาย จะถูกยกเลิก ณ สิ้นวัน ทั้งนี้ หลักเกณฑ์การชำระราคาและส่งมอบหลักทรัพย์ให้เป็นไปตามการซื้อขายหลักทรัพย์ตามปกติ (T+3)และผู้ลงทุนที่ซื้อขายหลักทรัพย์ผ่านอินเทอร์เน็ตสามารถตรวจสอบสถานการณ์ซื้อขายของตนผ่านทางระบบอินเทอร์เน็ตได้

3.2 ระบบสารสนเทศและบริการต่างๆ ขององค์กร

ด้วยลักษณะเฉพาะในการดำเนินธุรกิจที่มีความเกี่ยวข้องกับข้อมูลที่เชื่อมโยงกับตลาดหลักทรัพย์แห่งประเทศไทย ตลอดช่วงเวลาในการทำการซื้อขายหลักทรัพย์ในราคาและจำนวนในช่วงเวลานั้น ปัจจัยสำคัญหลักจึงอยู่ที่การประมวลผลและการติดต่อสื่อสารที่แม่นยำมีประสิทธิภาพและเชื่อถือได้สูงมากๆ จึงจำเป็นอย่างยิ่งที่จะต้องจัดการระบบเทคโนโลยีสารสนเทศให้สอดคล้องเหมาะสมต่อการดำเนินธุรกิจเช่นนี้ สภาพการณ์กับข่าวสารและข้อมูลจากภายนอก ผนวกกับฐานข้อมูลความรู้ต่างๆที่รวบรวมสะสมเอาไว้ มีความสำคัญ ต่อการช่วยตัดสินใจทางธุรกิจอย่างมาก

โดยหลักๆแล้วบริษัทหลักทรัพย์ในประเทศไทยมักแบ่งหน่วยงานออกเป็น 3 ฝ่ายหลักๆ คือ ส่วน Front Office ส่วน Back Office และส่วนวิเคราะห์วิจัยข้อมูล ซึ่งก็จะมีลักษณะของงานและความต้องการบริการทางเทคโนโลยีสารสนเทศที่แตกต่างกันไปบ้าง และบางส่วนก็สามารถใช้งานต่อเนื่องกัน หรือทำงานร่วมกันได้ หรือในบางบริษัทที่มีสำนักงานสาขาอยู่หลายๆที่หลายภูมิภาค ก็ต้องมีเครือข่ายที่กว้างไกลและกระจายไปทั่วประเทศอีกด้วย

จึงมีความจำเป็นที่ฝ่ายสนับสนุนทางด้านเทคโนโลยีสารสนเทศ ต้องจัดเตรียม อุปกรณ์ การบริการ และจัดการบริหารทรัพยากรที่ต้องการให้แก่หน่วยธุรกิจ เพื่อตอบสนองนโยบายหลักขององค์กร อย่างมีประสิทธิภาพและเชื่อถือได้เป็นอย่างดี ไม่ว่าจะเป็นงาน สำนักงานอัตโนมัติทั่วไป การติดต่อสื่อสารและเครือข่ายคอมพิวเตอร์ การประมวลผลข้อมูล และการทำธุรกรรมทางอิเลคทรอนิคส์ต่างๆให้มีความปลอดภัย จากภัยคุกคามทั้งจากภายในและภายนอกองค์กร ให้เหมาะสมและเพียงพอในการดำเนินธุรกิจหลักทรัพย์ได้อย่างต่อเนื่อง

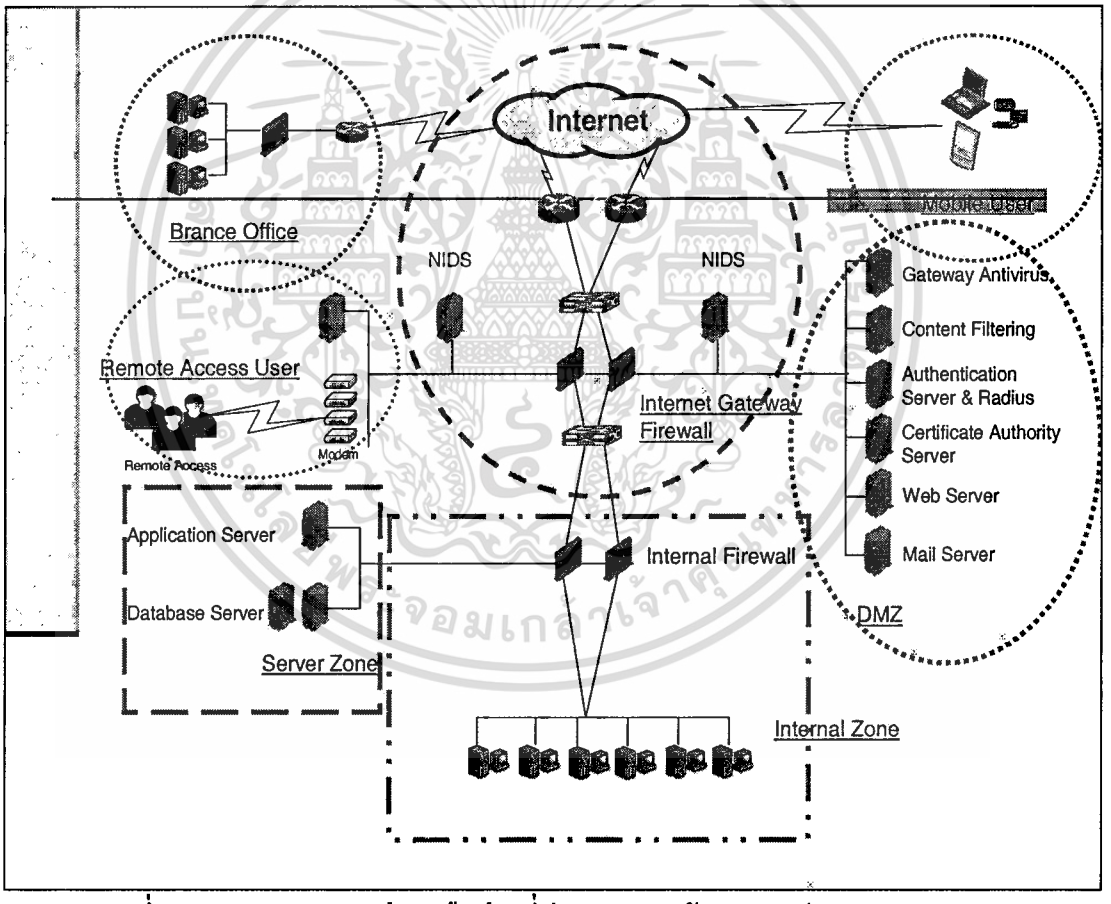


ภาพที่ 3.2 แสดงตัวอย่างผังโครงสร้างองค์กรของบริษัทหลักทรัพย์

3.3 ความจำเป็นของระบบสารสนเทศต่อธุรกิจ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานของบริษัทหลักทรัพย์ ทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผลระบบงานสำคัญต่างๆ โดยเฉพาะระบบงานที่เกี่ยวข้อง กับการประกอบธุรกิจหลักทรัพย์ประเภทการเป็นนายหน้าซื้อขายหลักทรัพย์ เช่น ระบบซื้อขายหลักทรัพย์ (front office system) และระบบปฏิบัติการหลักทรัพย์ (back office system) เป็นต้น เทคโนโลยีสารสนเทศทำให้การดำเนินงานของบริษัทหลักทรัพย์มีความสะดวกรวดเร็ว มีประสิทธิภาพ และเพิ่มโอกาสแข่งขันในทางธุรกิจได้

อย่างไรก็ดี การใช้เทคโนโลยีสารสนเทศก็มีความเสี่ยงหลายประการที่ควรคำนึงถึง โดยหากบริษัทหลักทรัพย์ไม่มีการบริหารจัดการ และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอ ก็อาจส่งผลกระทบต่อการดำเนินงานหรือสร้างความเสียหายต่อบริษัทหลักทรัพย์เองและลูกค้าได้ ดังนั้น การควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศจึงเป็นเรื่องที่ควรให้ความสำคัญกับนโยบายที่จะกำกับดูแลและตรวจสอบเกี่ยวกับการบริหารจัดการ และการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์อย่างจริงจัง เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการประกอบธุรกิจหลักทรัพย์เกิดประโยชน์สูงสุด และเพื่อลดโอกาสความเสียหายที่อาจเกิดขึ้น



ภาพที่ 3.3 แสดงภาพตัวอย่างเครือข่ายที่มีการจัดการด้านความปลอดภัยสารสนเทศ

กระแสการเปลี่ยนแปลงต่างๆ ไม่ว่าจะเป็นการเข้าสู่ยุคโลกาภิวัตน์ การแข่งขันระหว่างตลาดหุ้นของประเทศต่างๆและความสนใจของนักลงทุน ที่หันเหจากธุรกิจอุตสาหกรรมแบบเดิมๆ ไปสู่กิจการ

เทคโนโลยีขั้นสูง และตราสารใหม่ๆ รวมทั้งวิกฤติทางการเงินตั้งแต่ พ.ศ. 2540ส่งผลกระทบ ต่อตลาดหุ้นทั่วโลกอย่างรุนแรง การเปลี่ยนแปลงที่เกิดขึ้นนี้ ทำให้บริษัทหลักทรัพย์ไทย อยู่ในสภาวะที่เสียเปรียบเพราะเกิดจากสาเหตุต่อไปนี้

- ธุรกิจหลักทรัพย์ไทย ได้รับผลกระทบกระเทือน ที่รุนแรงจากวิกฤติเศรษฐกิจ
- การแข่งขันที่เพิ่มมากขึ้น กับตลาดหลักทรัพย์ในประเทศต่างๆ ในเอเชีย
- ทางเลือกใหม่ๆ ในการลงทุนมีมากขึ้น

แต่ภายใต้วิกฤตินี้ นักลงทุน มีโอกาสได้รับผลตอบแทน จากการลงทุนสูงขึ้น (เมื่อเศรษฐกิจเริ่มดีขึ้น) จากการปฏิรูประบบการเงิน การปรับปรุงโครงสร้างหนี้ การหวนกลับมา ของนักลงทุนต่างประเทศที่จะลงทุนอย่างเฉพาะเจาะจงมากขึ้น และจากการพัฒนาตราสารใหม่ๆท่ามกลางการแข่งขันดังกล่าว เพื่อให้สามารถฟันฝ่าอุปสรรค และมีความแข็งแกร่งในอนาคต และเป็นตลาดทุนชั้นนำแห่งหนึ่ง ในเอเชีย โดยจะมีสินค้าที่มีคุณภาพ เป็นตัวแทนของเศรษฐกิจไทย มีเครื่องมือป้องกันความเสี่ยง ที่ได้ผล และการกำกับดูแลตลาด และการดูแลกิจการที่ดีตามมาตรา ฐานสากล โดยจะเน้นการปรับปรุงในเชิงคุณภาพ แทนที่จะแข่งขันโดยตรงกับตลาดอื่นๆ

ในเรื่องของขนาดและ ปริมาณ ควรที่จะพัฒนาให้มีการบริการทางการเงิน ที่มีคุณภาพสูงครบถ้วนทุกชนิด พร้อมกับ เครื่องมือทางการบริหารความเสี่ยงที่มีประสิทธิภาพ บริษัทจดทะเบียนต้องเปิดเผยข้อมูลอย่างโปร่งใส และถูกต้องตามมาตรฐานสากลในการกำกับดูแล และ ส่งเสริมให้มีการดูแลกิจการที่ดี มีการลดความเสี่ยงในการลงทุน และได้รับความคุ้มครองสิทธิประโยชน์มากขึ้น บริษัทจดทะเบียนมีคุณภาพดีขึ้น และมีค่าใช้จ่ายในการระดมทุนต่ำลง ในขณะที่การกำกับดูแลบริษัทหลักทรัพย์จะมีประสิทธิภาพเพิ่มขึ้น และบริษัทหลักทรัพย์มีปริมาณธุรกิจเพิ่มขึ้น

.

บทที่ 4
นโยบาย มาตรฐาน และ ข้อบังคับต่างๆที่เกี่ยวข้อง

การจัดทำแผนระบบรักษาความปลอดภัยของเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในไทย มีความจำเป็นทั้งทางด้านการดำเนินธุรกิจของเหล่าบริษัทหลักทรัพย์เอง ทั้งยังเกี่ยวเนื่องจากการกำกับดูแลของฝ่ายควบคุม ของรัฐที่มีข้อกำหนด กฎหมายและระเบียบปฏิบัติ จากทั้ง 2 หน่วยงานหลัก คือ ตลาดหลักทรัพย์แห่งประเทศไทย (ตลท.) และ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (กลต.) ที่ต้องทำงานร่วมกันอย่างใกล้ชิด

นอกเหนือจากหน่วยงานภาครัฐทั้งสองแล้ว เพื่อบรรลุวัตถุประสงค์ด้าน บรรษัทภิบาล ซึ่งเป็นภาพลักษณะและคุณสมบัติที่บริษัทด้านการเงิน และหลักทรัพย์ควรจะมีอย่างเป็นมาตรฐานที่ยอมรับและเชื่อถือได้ในระดับสากล จึงจำเป็นอยู่ดีที่ต้องผนวกกับข้อกำหนด และมาตรฐานของสากลที่นิยมและอ้างอิงถึงได้อย่างเป็นสากลในอุตสาหกรรมการเงิน ก็คือ มาตราฐานการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ที่เด่นมากในเรื่อง IT Governance ที่เป็นหนทางสนับสนุนการทำบรรษัทภิบาล นั่นเอง ส่วนกระบวนการในการวางแผนเชิงการจัดการที่วงการ เทคโนโลยีสารสนเทศยอมรับกันเป็นสากล ก็คือมาตรฐานของ ISO17799 ซึ่งมีการพัฒนามาจาก BS7799 (2000)

ในบทนี้จึงกล่าวถึงการศึกษาที่ได้มาจากมาตรฐานและข้อกำหนดที่เกี่ยวข้องดังต่อไปนี้

4.1 แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ ของ กลต.[3]

ด้วย กลต. มีเป้าหมายในการกำกับดูแลการประกอบธุรกิจของบริษัทหลักทรัพย์ให้มีความน่าเชื่อถือ มีประสิทธิภาพ และให้มีการดำเนินงานและการให้บริการที่ได้มาตรฐานสากล โดยปัจจุบันสำนักงานได้พัฒนากรอบในการกำกับดูแลบริษัทหลักทรัพย์ ซึ่งให้ความสำคัญกับความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการประกอบธุรกิจของบริษัทหลักทรัพย์ (Risk-Based Approach) โดยความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงหนึ่งที่สำนักงานให้ความสำคัญเนื่องด้วยความเสี่ยงดังกล่าว อาจทำให้การประกอบธุรกิจของบริษัทหลักทรัพย์ขาดความน่าเชื่อถือและไม่มีประสิทธิภาพ ซึ่งจะส่งผลกระทบต่อการประกอบธุรกิจของบริษัทหลักทรัพย์เองและลูกค้า ดังนั้น สำนักงานจึงมีนโยบายที่จะกำกับดูแล และตรวจสอบเกี่ยวกับการบริหารจัดการและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์อย่างจริงจัง โดยให้ความสำคัญกับการ

---

[3] ที่มา : เอกสารเผยแพร่ สำนักเลขาธิการ กลต. 2544

บริหารจัดการและการควบคุมความเสี่ยงที่เกี่ยวข้องกับระบบซื้อขายหลักทรัพย์ ระบบปฏิบัติการหลักทรัพย์ และระบบงานสำคัญอื่น ในเรื่องดังต่อไปนี้

4.1.1. โครงสร้างหน่วยงานและภารบริหารจัดการ หากหน่วยงานเทคโนโลยีสารสนเทศมิได้มีการจัดโครงสร้างและการบริหารจัดการที่ดีเพียงพอ ก็อาจก่อให้เกิดความเสี่ยงด้าน infrastructure risk ได้ ซึ่งสำนักงานให้ความสำคัญในเรื่องของการแบ่งแยกอำนาจหน้าที่ การกำหนดนโยบาย แผนงานและขั้นตอนการปฏิบัติงาน และการกำกับดูแลและควบคุมการปฏิบัติงานเป็นหลัก ดังนี้

4.1.1.1 การแบ่งแยกอำนาจหน้าที่ การแบ่งแยกอำนาจหน้าที่และความรับผิดชอบภายในหน่วยงานเทคโนโลยีสารสนเทศนั้น ควรเป็นไปตามหลักการควบคุมภายในที่ดี โดยไม่ควรมอบหมายให้บุคลากรคนหนึ่งคนใดรับผิดชอบการปฏิบัติงานตลอดกระบวนการ ซึ่งการมอบหมายให้บุคลากรคนหนึ่งคนใดปฏิบัติงานหลายหน้าที่ควบคู่กันในบางกรณี ยังอาจเป็นช่องทางให้ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขหรือเปลี่ยนแปลงได้โดยง่าย (integrity risk) เช่น การมอบหมายเจ้าหน้าที่พัฒนาระบบงาน (system developer) ซึ่งควรปฏิบัติงานเฉพาะในส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (test environment) ให้ปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับส่วนของการใช้งานจริง (production environment) ควบคู่กัน ซึ่งมีความเสี่ยงในกรณีที่เจ้าหน้าที่พัฒนาระบบงานอาจแก้ไขเปลี่ยนแปลงข้อมูลจริงหรือการทำงานของระบบคอมพิวเตอร์ได้โดยง่ายเนื่องจากมีความรู้ความเข้าใจในการทำงานของโปรแกรมต่าง ๆ และโครงสร้างของข้อมูล เป็นต้น

แนวทางการกำกับดูแล สำนักงานให้ความสำคัญกับระบบการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในหน่วยงานเทคโนโลยีสารสนเทศ โดยไม่ควรมอบหมายให้บุคลากรคนหนึ่งคนใดรับผิดชอบการปฏิบัติงานตลอดกระบวนการ ทั้งนี้ หากบริษัทหลักทรัพย์มีข้อจำกัดด้านบุคลากรโดยมีความจำเป็นต้องมอบหมายให้บุคลากรคนหนึ่งคนใดปฏิบัติงานหลายหน้าที่ควบคู่กัน บริษัทหลักทรัพย์ก็ควรกำหนดมาตรการหรือวิธีการกำกับดูแลและควบคุมการปฏิบัติงานของบุคลากรรายดังกล่าวให้รอบคอบและรัดกุมเพียงพอ เช่น กำหนดให้มีบันทึกการทำงาน (log files) ของบุคลากรรายดังกล่าว และมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ เป็นต้น

4.1.1.2 การกำหนดนโยบาย แผนงานและขั้นตอนการปฏิบัติงาน การกำหนดนโยบาย แผนงาน และขั้นตอนการปฏิบัติงานที่ชัดเจน จะทำให้บุคลากรสามารถปฏิบัติงานได้อย่างถูกต้องครบถ้วน และเป็นไปในแนวทางเดียวกัน ซึ่งจะส่งผลให้การปฏิบัติงานโดยรวมมีประสิทธิภาพ นอกจากนี้ ยังลดโอกาสการปฏิบัติงานผิดพลาดในกรณีที่มีการสับเปลี่ยนหน้าที่และความรับผิดชอบหรือมีการมอบหมายงานให้บุคลากรรายใหม่

แนวทางการกำกับดูแล สำนักงานให้ความสำคัญกับความครบถ้วนและความชัดเจนของนโยบาย แผนงานและขั้นตอนการปฏิบัติงาน โดยเฉพาะนโยบาย แผนงาน และขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลและระบบคอมพิวเตอร์ การพัฒนา แก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการปฏิบัติงานประจำอื่นที่สำคัญ

4.1.1.3 การกำกับดูแลและตรวจสอบการปฏิบัติงาน การกำกับดูแลและตรวจสอบการปฏิบัติงานของพนักงานระดับปฏิบัติการอย่างใกล้ชิดโดยผู้บังคับบัญชา จะทำให้การปฏิบัติงานโดยรวมมีความถูกต้องและละเอียดรอบคอบมากขึ้น ซึ่งจะเป็นการลดโอกาสการเกิดข้อผิดพลาดและป้องกันการปฏิบัติงานนอกเหนืออำนาจหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย

แนวทางการกำกับดูแล สำนักงานให้ความสำคัญกับการรายงานการปฏิบัติงานและการตรวจสอบการปฏิบัติงาน เพื่อให้มั่นใจได้ว่าการปฏิบัติงานถูกต้อง ครบถ้วน เป็นไปตามนโยบายและขั้นตอนการปฏิบัติงาน และอยู่ในกรอบอำนาจหน้าที่และความรับผิดชอบตามที่บริษัทกำหนดไว้ นอกจากนี้ ในกรณีที่บริษัทหลักทรัพย์ได้ใช้บริการงานสนับสนุนด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอกไม่ว่าทั้งหมดหรือบางส่วน สำนักงานก็ให้ความสำคัญกับระบบการกำกับดูแลและควบคุมการปฏิบัติงานของบุคคลภายนอกเช่นกัน โดยบริษัทหลักทรัพย์ควรมีระบบการตรวจสอบการปฏิบัติงานของบุคคลภายนอกอย่างรอบคอบและรัดกุมเพียงพอ เช่น มีการตรวจสอบบันทึกการทำงาน (log files) ของบุคคลภายนอก และกำหนดให้บุคคลภายนอกรายงานการปฏิบัติงาน เป็นต้น

4.1.2. **การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์** ในการดำเนินธุรกิจ บริษัทหลักทรัพย์มักจะรับรู้ข้อมูลของลูกค้าซึ่งเป็นข้อมูลที่ไม่ควรเปิดเผย เช่น ข้อมูลวงเงิน ข้อมูลการซื้อขายหลักทรัพย์ของลูกค้า และข้อมูลทรัพย์สินของลูกค้า เป็นต้น นอกจากนี้ บริษัทหลักทรัพย์ยังรับรู้ข้อมูลบางอย่างที่อาจเป็นสาระสำคัญต่อการเปลี่ยนแปลงราคาหลักทรัพย์ เช่น ข้อมูลที่ได้จากการประกอบธุรกิจการเป็นที่ปรึกษาทางการเงินและการจัดจำหน่ายหลักทรัพย์ เป็นต้น ซึ่งในปัจจุบันบริษัทหลักทรัพย์ได้จัดเก็บข้อมูลสำคัญตามที่กล่าวข้างต้นไว้ในระบบคอมพิวเตอร์และในสื่อบันทึกข้อมูลทางอิเล็กทรอนิกส์เป็นส่วนใหญ่ ดังนั้น การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์ จึงเป็นเรื่องที่สำนักงานให้ความสำคัญอย่างมาก โดยในการกำกับดูแลและตรวจสอบ สำนักงานจะให้ความสำคัญกับการควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย และการควบคุมการใช้ข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการป้องกันการบุกรุกระบบเครือข่าย ดังนี้

4.1.2.1 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย

(Physical Security) เนื่องด้วยข้อมูลที่เกี่ยวข้องกับการดำเนินธุรกิจได้ถูกจัดเก็บไว้ในระบบคอมพิวเตอร์และในสื่อบันทึกข้อมูลทางอิเล็กทรอนิกส์เป็นส่วนใหญ่ตามที่กล่าวข้างต้น ดังนั้น การควบคุมการเข้าออกศูนย์คอมพิวเตอร์ซึ่งเป็นสถานที่ตั้งของเครื่องแม่ข่ายที่ใช้เก็บฐานข้อมูล และยังเป็นสถานที่ในการประมวลผลและจัดทำรายงานต่างๆ จึงมีความสำคัญอย่างมากในการป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (access risk) แก้ไขเปลี่ยนแปลง (integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ (availability risk) นอกจากนี้ ระบบป้องกันความเสียหายภายในศูนย์คอมพิวเตอร์ก็มีความสำคัญในการป้องกันมิให้ข้อมูลและระบบคอมพิวเตอร์ได้รับความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (availability risk)

แนวทางการกำกับดูแล สำนักงานให้ความสำคัญกับการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ที่รัดกุมเพียงพอ โดยควรจำกัดสิทธิการเข้าออกศูนย์คอมพิวเตอร์เฉพาะผู้ที่มีหน้าที่เกี่ยวข้อง และควรมีการตรวจสอบการเข้าออกศูนย์คอมพิวเตอร์อย่างสม่ำเสมอ นอกจากนี้ สำนักงานยังให้ความสำคัญกับการจัดให้มีระบบป้องกันความเสียหายภายในศูนย์คอมพิวเตอร์จากปัจจัยสภาวะแวดล้อมและภัยพิบัติต่างๆ เช่น ระบบป้องกันไฟไหม้ ระบบควบคุมอุณหภูมิ ระบบไฟฟ้าสำรอง เป็นต้น ทั้งนี้ หากบริษัทหลักทรัพย์จัดให้มีสถานที่อื่นใดนอกเหนือจากศูนย์คอมพิวเตอร์ เพื่อใช้เป็นสถานที่ตั้งเครื่องแม่ข่ายที่ใช้เก็บฐานข้อมูล หรือเป็นสถานที่ประมวลผลและจัดทำรายงานต่างๆ บริษัทหลักทรัพย์ก็ควรจัดให้มีระบบควบคุมการเข้าออก รวมทั้งระบบป้องกันความเสียหายภายในสถานที่ดังกล่าวอย่างรอบคอบและรัดกุมเพียงพอด้วยเช่นกัน

4.1.2.2 การควบคุมการใช้ข้อมูลและระบบงานคอมพิวเตอร์ และการป้องกันการบุกรุกผ่านระบบเครือข่าย (Logical Security) กรณีการเข้าถึง ล่วงรู้หรือแก้ไขเปลี่ยนแปลงข้อมูลและการทำงานของระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องนั้น (access risk และ integrity risk) อาจเกิดจากบุคคลภายในบริษัทหลักทรัพย์เอง ซึ่งอาจมีสาเหตุมาจากการมิได้มีระบบป้องกันที่ดีพอ เช่น มิได้มีการกำหนดรหัสผ่านในการเข้าสู่ระบบงานอย่างรัดกุม หรือกำหนดสิทธิให้แก่ผู้ใช้งานภายในเพื่อเข้าถึงข้อมูลและระบบงานคอมพิวเตอร์ที่มากเกินความจำเป็น เป็นต้น นอกจากนี้เทคโนโลยีในปัจจุบันได้พัฒนาให้มีการเชื่อมต่อระบบเครือข่ายภายในกับภายนอกมากขึ้น ซึ่งหากบริษัทหลักทรัพย์มิได้มีวิธีการควบคุมที่รอบคอบและรัดกุมเพียงพอ การเชื่อมต่อในลักษณะดังกล่าวก็อาจเป็นช่องทางให้บุคคลภายนอกสามารถเข้าถึงข้อมูลและการทำงานของระบบคอมพิวเตอร์ผ่านระบบเครือข่ายได้ (access risk) อีกทั้งไวรัสหรือ malicious code อื่นๆ ก็อาจผ่านเข้ามาทางการเชื่อมต่อระบบเครือข่ายและสร้างความเสียหายแก่ข้อมูลและระบบคอมพิวเตอร์ได้เช่นกัน (availability risk)

แนวทางการกำกับดูแล สำนักงานให้ความสำคัญกับการจัดให้มีระบบการตรวจสอบผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์ (authentication) และการกำหนดให้มีการใส่รหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์ โดยรหัสผ่านดังกล่าว ควรมีการกำหนดความยาวขั้นต่ำ อายุ จำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิด และควรกำหนดรหัสผ่านให้มีความยากแก่การคาดเดา นอกจากนี้ บริษัทหลักทรัพย์ก็ควรมีการกำหนดสิทธิผู้ใช้งานให้เหมาะสมกับหน้าที่ความรับผิดชอบ และสำหรับกรณีที่บริษัทหลักทรัพย์มีการเชื่อมต่อระบบเครือข่ายภายในกับภายนอก สำนักงานก็ให้ความสำคัญกับการจัดให้มีระบบป้องกันการบุกรุกจากบุคคลภายนอก เช่น Firewall เป็นต้น และระบบป้องกันไวรัสหรือ malicious code อื่นๆ ทั้งนี้ ระบบต่างๆ ตามที่กล่าว รวมทั้งการใช้รหัสผ่านและสิทธิของผู้ใช้งาน ก็ควรมีการตรวจสอบอย่างสม่ำเสมอ

4.1.3 การควบคุมการพัฒนา การแก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ (Change Management) โดยทั่วไประบบงานคอมพิวเตอร์ มักมีการพัฒนา แก้ไขหรือเปลี่ยนแปลงอยู่ตลอดเวลา ด้วยเหตุนี้ วิธีการจัดการและการควบคุมเกี่ยวกับการพัฒนา แก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ จึงเป็นเรื่องที่สำนักงานให้ความสำคัญ โดยหากมิได้มีวิธีการจัดการและการควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจทำให้ระบบงานคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องหรืออาจไม่เป็นไปตามความต้องการของผู้ใช้งานได้ (integrity risk)

แนวทางการกำกับดูแล สำนักงานให้ความสำคัญกับวิธีการจัดการและการควบคุมที่รอบคอบและรัดกุมเพียงพอ โดยหากการพัฒนา แก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์มีการร้องขอจากผู้ใช้งาน การร้องขอนั้น ก็ควรได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่ ควรจัดทำให้เป็นลายลักษณ์อักษร และควรกำหนดให้มีการทดสอบก่อนการใช้งานจริงทั้งจากเจ้าหน้าที่พัฒนาระบบและผู้ใช้งานเพื่อให้มั่นใจว่าระบบงานคอมพิวเตอร์ที่ได้รับการพัฒนา แก้ไขหรือเปลี่ยนแปลง มีการทำงานที่มีประสิทธิภาพ มีการประมวลผลที่ถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน นอกจากนี้ ควรจัดให้มีเอกสารประกอบการพัฒนา แก้ไขหรือเปลี่ยนแปลงโปรแกรมของระบบงานคอมพิวเตอร์ที่มีรายละเอียดเพียงพอเกี่ยวกับโปรแกรมที่ใช้อยู่ปัจจุบัน ทั้งนี้ การแก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์ในหลายกรณีอาจส่งผลกระทบต่อการปฏิบัติตามกฎเกณฑ์ของสำนักงาน ดังนั้น จึงควรมีการสอบทานกฎเกณฑ์ที่เกี่ยวข้องก่อนการพัฒนา แก้ไขหรือเปลี่ยนแปลงระบบงานคอมพิวเตอร์

4.1.4 การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน ในการดำเนินธุรกิจ มีหลายกรณีที่อาจทำให้ข้อมูลหรือระบบงานคอมพิวเตอร์เสียหาย เช่น การติดไวรัส สภาวะแวดล้อมหรือภัยพิบัติต่างๆ หรืออาจเกิดจากการปฏิบัติงานที่ผิดพลาดของผู้ใช้งาน เป็นต้น

ดังนั้น สำนักงานจึงให้ความสำคัญกับการสำรองข้อมูลและระบบงานคอมพิวเตอร์ รวมทั้งการเตรียมพร้อมกรณีฉุกเฉินต่างๆ ดังนี้

4.1.4.1 การสำรองข้อมูลและระบบงานคอมพิวเตอร์ หากมิได้มีการสำรองข้อมูลและระบบงานคอมพิวเตอร์ที่เพียงพอในกรณีที่เกิดเหตุการณ์ที่ทำให้ข้อมูลหรือระบบงานคอมพิวเตอร์เสียหาย บริษัทหลักทรัพย์ก็อาจไม่มีข้อมูลหรือระบบงานคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ (availability risk) ซึ่งอาจส่งผลกระทบต่อการดำเนินงานของบริษัทหลักทรัพย์เองและอาจก่อให้เกิดความเสียหายต่อลูกค้าได้

แนวทางการกำกับดูแล สำนักงานให้ความสำคัญกับความครบถ้วนของการสำรองข้อมูลและระบบงานคอมพิวเตอร์ วิธีการเก็บรักษาสื่อที่ใช้บันทึกข้อมูลและระบบงานคอมพิวเตอร์ และการทดสอบความถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบงานคอมพิวเตอร์ที่ได้สำรองไว้

4.1.4.2 การเตรียมพร้อมกรณีฉุกเฉิน การสำรองข้อมูลและระบบงานคอมพิวเตอร์เพียงอย่างเดียวอาจไม่เพียงพอแก่การป้องกันการหยุดชะงักของการดำเนินธุรกิจ ดังนั้น การจัดให้มีแผนฉุกเฉินเพื่อรองรับในกรณีที่อาจเกิดเหตุการณ์ฉุกเฉิน จะทำให้การควบคุมความเสี่ยงด้าน availability risk มีประสิทธิภาพมากขึ้น

แนวทางการกำกับดูแล สำนักงานให้ความสำคัญกับการจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉินต่างๆ ซึ่งแผนดังกล่าวควรมีรายละเอียดที่ชัดเจนเกี่ยวกับขั้นตอนปฏิบัติและผู้รับผิดชอบ ควรมีการสื่อสารให้ผู้เกี่ยวข้องเข้าใจและรับทราบหน้าที่ความรับผิดชอบ รวมทั้งควรมีการทดสอบแผนดังกล่าวเพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ

4.1.5 **การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์** การปฏิบัติงานประจำด้านคอมพิวเตอร์ที่สำคัญคือ การควบคุมการประมวลผลข้อมูล ซึ่งการประมวลผลข้อมูลที่ถูกต้องและครบถ้วนมีความสำคัญต่อการประกอบธุรกิจของบริษัทหลักทรัพย์ ซึ่งหากมิได้มีวิธีการปฏิบัติและการควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจทำให้ข้อมูลไม่ถูกต้องหรือไม่ครบถ้วน (integrity risk) ซึ่งอาจก่อให้เกิดความเสียหายต่อบริษัทหลักทรัพย์เองและลูกค้าได้ นอกจากที่กล่าว ยังมีงานประจำอื่นที่สำคัญ เช่น การดูแลการทำงานของระบบคอมพิวเตอร์ การย้ายโปรแกรมที่พัฒนาแล้วสู่ระบบงานจริง การสำรองข้อมูลและระบบงานคอมพิวเตอร์ เป็นต้น ซึ่งหากมิได้มีวิธีการปฏิบัติและควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจก่อให้เกิดความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ เช่น ความเสี่ยงด้าน

integrity risk ในกรณีที่ย้ายโปรแกรมที่พัฒนาแล้วสู่ระบบงานจริงไม่ครบถ้วน ความเสี่ยงด้าน availability risk ในกรณีที่มิได้มีการดูแลการทำงานของระบบคอมพิวเตอร์อย่างเพียงพอ เป็นต้น

แนวทางการกำกับดูแล สำนักงานให้ความสำคัญกับการกำกับดูแลและควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์อย่างใกล้ชิดของผู้บังคับบัญชา การปฏิบัติงานที่มีขั้นตอนที่ชัดเจนและสามารถตรวจสอบได้ รวมทั้งควรจัดให้มีระบบการรายงาน และการตรวจสอบการปฏิบัติงานประจำดังกล่าวอย่างสม่ำเสมอ

4.2 บรรษัทภิบาล (Corporate governance) และ IT Governance

4.2.1 ระบบการดูแลกิจการที่ดี (บรรษัทภิบาล) [4]

ตลาดหลักทรัพย์ได้ดำเนินการในการกำหนดกฎเกณฑ์ที่สำคัญเกี่ยวกับบริษัทจดทะเบียน3 เรื่อง คือ คุณภาพของการเปิดเผยข้อมูล คณะกรรมการตรวจสอบ และกรอบการพัฒนาระบบการดูแลกิจการที่ดีเพื่อส่งเสริมตลาดทุนในประเทศไทย และเพื่อดึงดูดนักลงทุนต่างชาติ

4.2.1.1. คุณภาพของการเปิดเผยข้อมูล

- บริษัทจดทะเบียนจะต้องจัดให้มีผู้สอบบัญชีที่ได้รับความเห็นชอบจาก ก.ล.ต.ทำการสอบทานงบการเงินรายไตรมาสและงบการเงินประจำปีที่จัดส่งให้กับตลาดหลักทรัพย์
- ส่งเสริมให้กรรมการบริษัทกำหนดขอบเขตความรับผิดชอบของกรรมการในการรายงานงบการเงินของบริษัทโดยกรรมการมีหน้าที่ดูแลให้มีข้อมูลทางบัญชีที่ถูกต้องครบถ้วนและโปร่งใส เพื่อสร้างความมั่นใจแก่ผู้ถือหุ้น

4.2.1.2 คณะกรรมการตรวจสอบ (Audit Committee)

ตลาดหลักทรัพย์ได้ทำการศึกษาแนวทางในการกำหนดให้บริษัทจดทะเบียนจัดตั้งคณะกรรมการตรวจสอบมาตั้งแต่ พ.ศ. 2538 ก่อนเกิดวิกฤตเศรษฐกิจในประเทศไทยและได้ประกาศใช้เมื่อ พ.ศ. 2540 โดยกำหนดให้บริษัทจดทะเบียนทุกบริษัท ต้องจัดตั้งคณะกรรมการตรวจสอบภายในปี 2542 คณะกรรมการตรวจสอบประกอบด้วยกรรมการที่เป็นอิสระ อย่างน้อย 3 คน โดยมีความรับผิดชอบดังนี้

- สอบทานให้บริษัทมีรายงานทางการเงินอย่างถูกต้องและเพียงพอ
- สอบทานให้บริษัทมีระบบควบคุมภายในและการตรวจสอบภายในที่เหมาะสมและมีประสิทธิผล

---

[4] ที่มา : เอกสารเผยแพร่ สำนักเลขาธิการ กลต. สิงหาคม 2544

- สอบทานให้บริษัทปฏิบัติตามข้อกำหนด/กฎหมายที่เกี่ยวข้อง
- คัดเลือกและเสนอแต่งตั้งผู้สอบบัญชี
- จัดทำรายงานกำกับดูแลกิจการของคณะกรรมการตรวจสอบ ฯลฯ

4.2.1.3 แนวทางการพัฒนาระบบการดูแลกิจการที่ดี

ตลาดหลักทรัพย์ได้จัดทำแนวทางการปฏิบัติสำหรับกรรมการบริษัทจดทะเบียน (Code of Best Practice for Directors of Listed Companies) เพื่อเป็นแนวทางสำหรับการปฏิบัติงานของกรรมการ และให้คณะกรรมการรายงานในรายงานประจำปีว่าได้ปฏิบัติตามหรือไม่ ถ้าไม่ปฏิบัติตามขอให้ระบุเหตุผลด้วย ตลาดหลักทรัพย์ร่วมกับ ก.ล.ต. ได้จัดตั้งคณะกรรมการว่าด้วยการดูแลกิจการที่ดี (Good Corporate Governance Committee) ประกอบด้วยผู้แทนจากองค์กรวิชาชีพต่างๆ เพื่อวางแนวทางการพัฒนาระบบการกำกับดูแลกิจการที่ดีสำหรับบริษัทจดทะเบียนในตลาดหลักทรัพย์ โดยเน้นเรื่องต่างๆ ดังต่อไปนี้

- คณะกรรมการบริษัทควรประกอบด้วยกรรมการอิสระหนึ่งในสามของกรรมการทั้งหมด เพื่อให้เป็นที่แน่ใจว่ามีการถ่วงดุล ซึ่งกันและกัน
- กำหนดขอบเขตหน้าที่ของคณะกรรมการและฝ่ายบริหารอย่างชัดเจน เนื่องจากในปัจจุบันนี้ยังไม่มีการระบุให้ชัดเจน
- การควบคุมภายในที่ได้ผล และการบริหารความเสี่ยงที่มีประสิทธิภาพ ซึ่งเป็นปัจจัยหนึ่งที่สำคัญสำหรับธุรกิจในปัจจุบัน ในกรณีนี้ ตลาดหลักทรัพย์จึงได้ร่วมกับสมาคมนักบัญชีและผู้ตรวจสอบบัญชีแห่งประเทศไทย กำหนดแนวทางการสร้างระบบการควบคุมภายใน (Internal Control) ของบริษัทจดทะเบียนที่มีประสิทธิภาพ
- บริษัทจดทะเบียนควรแต่งตั้งเลขานุการคณะกรรมการบริษัท (Company Secretary) เพื่อรับผิดชอบกิจกรรมของคณะกรรมการบริษัท และดูแลว่าคณะกรรมการทำตามกฎระเบียบและข้อบังคับของตลาดหลักทรัพย์หรือไม่
- ร่างข้อพึงปฏิบัติทางจริยธรรม และ จรรยาบรรณสำหรับกรรมการผู้บริหาร และพนักงาน สมาคมส่งเสริมสถาบันกรรมการบริษัทไทย (Thai Institute of Directors Association) ได้จัดตั้งขึ้นเมื่อวันที่ 1 เดือนตุลาคม พ.ศ. 2542 โดยได้รับการสนับสนุนจาก ก.ล.ต. ธนาคารแห่งประเทศไทย และธนาคารโลก มีจุดมุ่งหมายในการส่งเสริมให้มีการรับรู้ถึงหน้าที่และความรับผิดชอบของกรรมการบริษัท รวมทั้งเพิ่มพูนมาตรฐานงานในหน้าที่ ทักษะ ความสามารถ และความรู้

นอกจากนี้ ตลาดหลักทรัพย์ได้กำหนดแนวทางปฏิบัติในการประชุมผู้ถือหุ้น เพื่อให้เป็นที่แน่ใจว่าผู้ถือหุ้นมีข้อมูลที่เพียงพอในการตัดสินใจ นอกจากนั้นแล้ว บริษัทควรจะมีข้อบังคับในการลงคะแนนเสียงโดยผู้รับมอบอำนาจ และข้อมูลอื่นๆ ที่จำเป็นต้องใช้ในการประชุมผู้ถือหุ้นไว้ด้วย

4.2.2 IT Governance

ในปัจจุบันองค์กรต่างๆ ต่างเล็งเห็นถึงประโยชน์ของเทคโนโลยีที่จะนำมาใช้ในการดำเนินงาน อย่างไรก็ดี องค์กรที่ได้รับความสำเร็จอย่างแท้จริงจากการนำเทคโนโลยีใช้ให้เกิดประโยชน์จะได้แก่องค์กรที่ผู้บริหารมีความรู้ความเข้าใจที่จะจัดการกับความเสี่ยงด้านการนำเทคโนโลยีมาใช้ในองค์กรอย่างเหมาะสมการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีจึงกลายเป็นส่วนที่มีนัยสำคัญในการบริหารจัดการความเสี่ยงขององค์กรโดยรวม โดยเฉพาะองค์กรที่มุ่งสู่การเป็นบรรษัทภิบาล (Corporate Governance) สถาบัน เทคโนโลยีสารสนเทศภิบาล (IT Governance Institute)[5] ได้ให้ความจำกัดความเกี่ยวกับเรื่องนี้ไว้ดังนี้

" IT Governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and process that ensure that the organization's strategies and objectives."

แสดงให้เห็นส่วน สำคัญหลักอยู่3ส่วนคือ สภาวะผู้นำ(Leadership) การจัดโครงสร้างหน่วยงาน (Organizational Structure) และกระบวนการต่างๆ (Process)

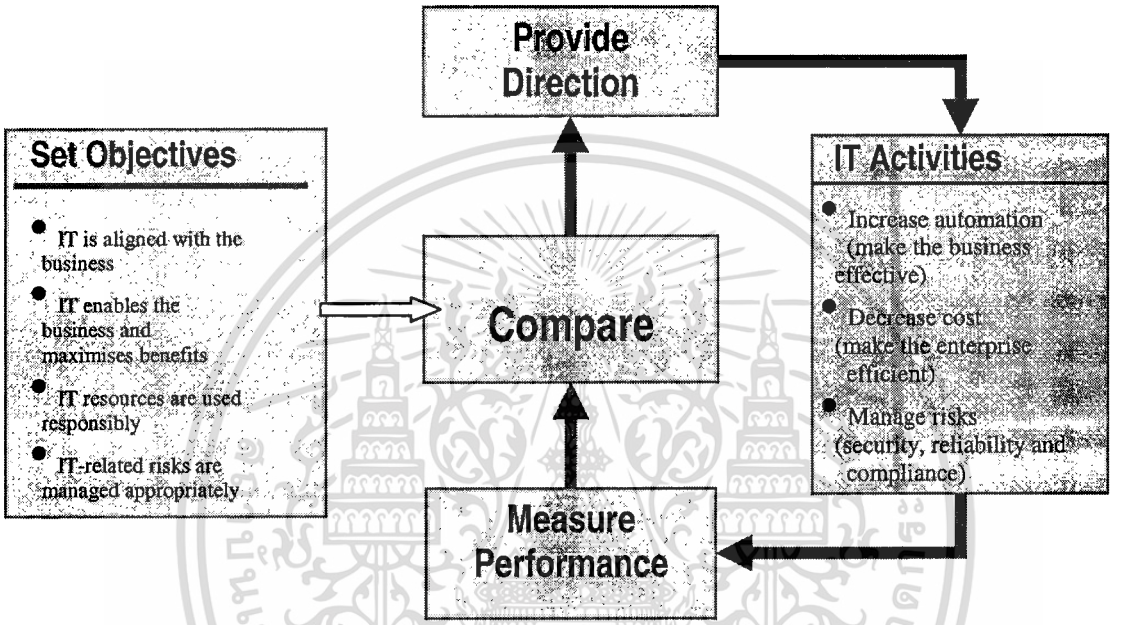
4.2.2.1 สภาวะผู้นำ ฝ่ายบริหารระดับสูงจำเป็นต้องมีความเป็นมืออาชีพ ซึ่งมีสภาวะผู้นำ ที่มีวิสัยทัศน์ที่กว้างไกล ต้องมีความอิสระในการตัดสินใจเพียงพอ ต่อการกำหนด วัตถุประสงค์ขององค์กรอย่างเหมาะสมและถูกต้อง พร้อมที่จะให้แนวทางที่ชัดเจนต่อผู้ปฏิบัติงานไป สานต่อได้อย่างมีประสิทธิภาพ อีกทั้งยังต้องมีหน้าที่สอดส่องดูแลการบริหารงานอย่างเข้มแข็ง ซึ่งต้องสามารถประเมินผลการบริหารงานได้อีกด้วย

4.2.2.2 การจัดสรรโครงสร้างองค์กร ต้องมีการจัดสรรหน่วยงานที่สอดคล้องตามวัตถุประสงค์ขององค์กรได้ เน้นไปที่การแยกหรือจัดตั้งหน่วยงาน ที่ทำหน้าที่ประเมินความเสี่ยงขององค์กร และหน่วยงานตรวจสอบ หรือควบคุมภายในที่มีความอิสระ จากหน่วยงานด้านเทคโนโลยีสารสนเทศ

---

[5] ที่มา : COBIT 3rd Edition Control Objectives , IT Governance Institute, 2000

4.2.2.3 กระบวนการ ซึ่งหมายถึงกระบวนการสำคัญและมีประสิทธิภาพในการบรรลุวัตถุประสงค์ ซึ่งครอบคลุมตั้งแต่ผู้บริหารระดับสูง จนถึงพนักงานทุกระดับในองค์กร ส่วนกระบวนการควบคุมและตรวจสอบ รวมทั้งประเมินผล ที่มีความเป็นอิสระเพื่อลดความเสี่ยงที่อาจเกิดขึ้น รวมทั้งสร้างให้เกิดความตะหนักถึงการควบคุมที่ดีในทุกระดับขององค์กร



ภาพที่ 4.1 IT Governance Framework

จากภาพแสดงถึงแนวคิดหรือกรอบการทำงาน เทคโนโลยีสารสนเทศภิบาล (IT Governance Framework) ที่เริ่มด้วยการตั้งวัตถุประสงค์ขึ้นมาก่อน ในที่นี้ก็จะกล่าวถึงการปรับแต่งงานด้านเทคโนโลยีให้สนับสนุนเป้าหมายทางธุรกิจ เพื่อเพิ่มความสามารถทางธุรกิจให้เกิดประโยชน์สูงสุด ารจัดสรรและบริหารทรัพยากรการความรับผิดชอบงานด้านเทคโนโลยีสารสนเทศ และการบริการความเสี่ยงที่เกี่ยวข้องหรืออาจเกิดขึ้นต่อระบบสารสนเทศขององค์กร

จากนั้นก็จะทำการกำหนดแนวทาง และวางมาตรการในเชิงปฏิบัติ และกิจกรรมต่างๆให้กับงานด้านเทคโนโลยีสารสนเทศที่เน้นไปที่การเพิ่มกระบวนการให้เป็นอัตโนมัติมากขึ้น เพื่อเพิ่มประสิทธิผล และการลดค่าใช้จ่าย เพื่อเพิ่มประสิทธิภาพ และสุดท้ายก็จัดให้มีการบริการความเสี่ยง

ขั้นตอนต่อมาก็จะทำการวัดผลประเมินค่าที่ได้จาก การปฏิบัติตามแนวทางที่วางไว้มาเปรียบเทียบกับเป้าหมายที่กำหนดไว้ในตอนแรก นำค่านั้นมาวิเคราะห์ และจัดหาแนวทางเพื่อปรับปรุงและพัฒนา

มาตรการต่างในการดำเนินงานด้านเทคโนโลยีให้เป็นไปตามเป้าหมาย และให้พัฒนาให้ดีขึ้นอย่างต่อเนื่อง

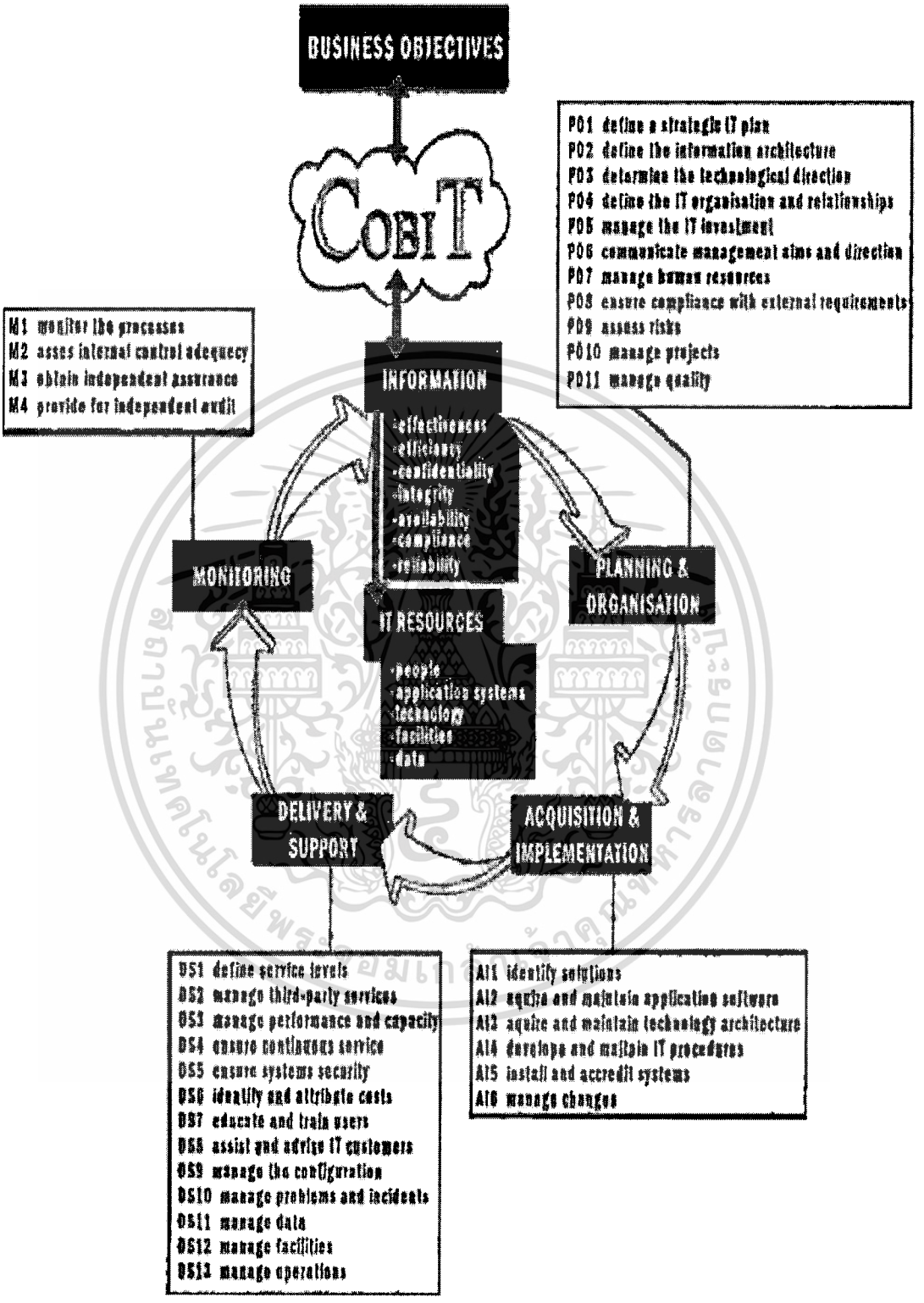
4.3 CoBIT (Control Objectives for Information and Related Technology)

เป็นทั้งแนวคิดและแนวทางการปฏิบัติ (Framework) เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่างๆที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดี (Best Practice) ซึ่งสามารถนำไปปรับใช้ได้ในทุกองค์กรสำหรับกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยโครงสร้างของCoBIT ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจBusiness Process ซึ่งแบ่งเป็น 4 กระบวนการหลัก (Domain)

- การวางแผนและการจัดการองค์กร (Planning and Organization)
- การจัดหาและติดตั้ง (Acquisition and Implementation)
- การส่งมอบและบำรุงรักษา (Delivery and Support)
- การติดตามผล (Monitoring)

ในแต่ละกระบวนการหลักข้างต้น CoBIT แสดงวัตถุประสงค์ของการควบคุมหลัก (High-level Control Objectives) รวมถึง34 หัวข้อ และในแต่ละหัวข้อจะประกอบด้วยวัตถุประสงค์ของการควบคุมย่อยลงไปอีกขั้นหนึ่ง (Detailed Control Objectives) รวมถึง 318หัวข้อย่อย พร้อมทั้งแนวทางการตรวจสอบ (Audit Guidelines) สำหรับแต่ละหัวข้ออีกด้วย ในแต่ละหัวข้อของวัตถุประสงค์ของการควบคุมCoBITแสดงถึงความสัมพันธ์ต่อปัจจัย 2 ประการ ได้แก่

- คุณภาพของระบบข้อมูล ประการ (Information Criteria)
- ทรัพยากรด้านเทคโนโลยี (IT Resources) 5 ประเภท



ภาพที่ 4.2 แสดงความสัมพันธ์ CoBIT Framework

4.3.1 คุณภาพของระบบข้อมูล 7 ประการ (Information Criteria)

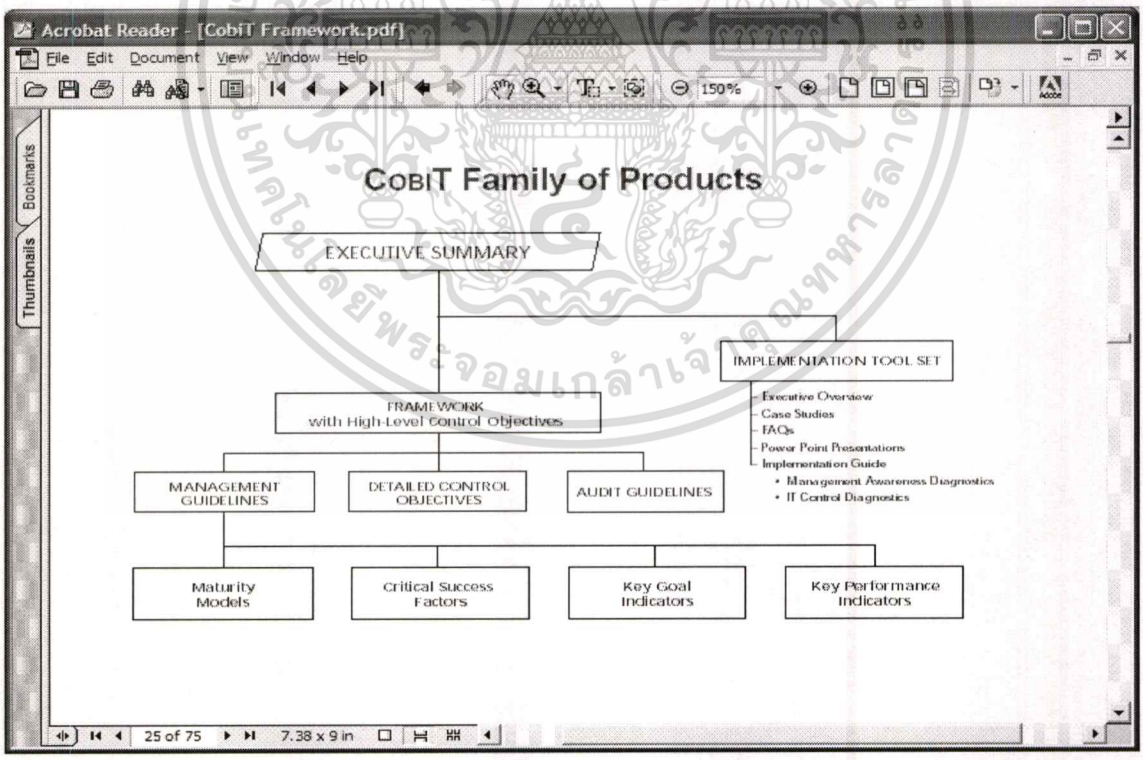
- ประสิทธิภาพ (Effectiveness) หมายถึงข้อมูลที่ใช้เกี่ยวข้องกับกระบวนการทางธุรกิจ รวมทั้งมีการส่งมอบข้อมูลแก่ผู้ใช้อย่าง ถูกต้อง ตรงเวลา สม่ำเสมอ (Consistent) และใช้ประโยชน์ได้ (Usable)
- ประสิทธิผล (Efficiency) หมายถึง มีการใช้ประโยชน์จากทรัพยากรอย่างเต็มที่เพื่อให้ได้มาซึ่งข้อมูลสารสนเทศ
- ความลับ (Confidentiality) หมายถึง การป้องกันการเปิดเผยข้อมูลที่สำคัญต่อบุคคลหรือหน่วยงานที่ไม่ได้รับอนุญาต
- ความสมบูรณ์ (Integrity) หมายถึงความครบถ้วนถูกต้องของข้อมูล ตลอดจนเป็นข้อมูลใช้ได้ (Validity) ในแง่ของความคาดหมายและการให้ความสำคัญของธุรกิจ (business values and expectations)
- การมีใช้เมื่อต้องการ (Availability) หมายถึง เป็นข้อมูลที่เรียกใช้ได้เมื่อต้องการและจำเป็นใช้ทั้งในปัจจุบันและอนาคต และรวมทั้งการป้องกันภัยให้กับทรัพยากรต่างๆที่จำเป็นและการรักษาระดับความสามารถในการทำงานของทรัพยากรเหล่านั้น
- การปฏิบัติตามระบบ (Compliance) หมายถึง การที่ข้อมูลได้จัดทำขึ้นตามกฎ ระเบียบ ข้อบังคับ หลักเกณฑ์ ข้อตกลง หรือกฎหมาย ที่มีขึ้นเพื่อบังคับใช้ทั้งจากหน่วยงานภายในและภายนอกองค์กร เช่น ข้อบังคับของตลาดหลักทรัพย์ ประมวลกฎหมายภาษีอากร หลักการบัญชีที่ยอมรับโดยทั่วไป เป็นต้น
- ความน่าเชื่อถือของข้อมูล (Reliability of Information) หมายถึงความสามารถในการจัดหาข้อมูลที่เหมาะสมให้แก่ผู้บริหารของกิจการเพื่อสามารถดำเนินธุรกิจและเพื่อให้สามารถจัดทำรายงานทางการเงินและรายงานที่จำเป็นอื่นๆภายใต้ความรับผิดชอบของผู้บริหาร

4.3.2. ทรัพยากรด้านเทคโนโลยี (IT Resources) 5 ประเภท

- ข้อมูล (Data) รวมความถึงข้อมูลในรูปแบบต่างๆทั้งที่มีโครงสร้างและไม่มีโครงสร้าง ข้อมูลด้านกราฟฟิค และข้อมูลที่เป็นเสียง

- ระบบงาน (Application System) ได้แก่ขั้นตอนและขบวนการปฏิบัติงานทั้งที่ทำด้วยมือและโปรแกรมคอมพิวเตอร์
- (Technology) ได้แก่ เครื่องคอมพิวเตอร์ (hardware) โปรแกรมระบบ (Operating Systems) ระบบบริหารฐานข้อมูล (database management system) ระบบเครือข่าย (Networking) และระบบมัลติมีเดีย
- (Facilities) ได้แก่ทรัพยากรต่างๆที่ใช้เป็นสถานที่ติดตั้งหรือจัดวาง ตลอดจนสาธารณูปโภคที่จำเป็นเพื่อการปฏิบัติงานของระบบสารสนเทศ
- บุคลากร (People) ได้แก่บุคคลากรที่มีความรู้ความชำนาญในการบริหารและปฏิบัติงานสำหรับการดูแลและจัดทำระบบสารสนเทศ

ปัจจุบัน CobiT ได้กลายเป็นมาตรฐานเปิดที่บุคคลทั่วไปสามารถนำศึกษาและนำไปใช้ได้โดยไม่มีค่าลิขสิทธิ์ ผู้สนใจสามารถดาวน์โหลด CobiT ได้ที่ www.isaca.org



รูปที่ 4.3 แสดงความสัมพันธ์ของ CoBIT ในชุดต่างๆ

4.4 BS 7799 (ISO17799)

ISO17799 เป็นที่รู้จักกันว่าเป็นมาตรฐานด้านการจัดการความปลอดภัยสารสนเทศในระดับสากล ซึ่งเผยแพร่โดย องค์การมาตรฐานสากล (International Organization for Standardization) หรือ ISO ในเดือนธันวาคม ค.ศ. 2000 ซึ่งให้ไว้เป็นแนวความคิด และขอบเขตแนวทางโดยสังเขป เพื่อที่จะนำไปประยุกต์ใช้กับองค์กรหรือ ธุรกิจได้หลากหลาย เพื่อจะได้นำไปใช้ในการจัดการกับระบบรักษาความปลอดภัยกับสารสนเทศได้เหมาะสมได้หลายระดับ

โดยนิยามให้ ข้อมูลสารสนเทศที่มีอยู่ในรูปแบบต่างๆ ถือเป็นทรัพย์สินที่มีคุณค่ายิ่งต่อองค์กร จึงมีเป้าหมายที่จำเป็นที่ต้องจัดการป้องกันอย่างเหมาะสม เพื่อความมั่นใจในการดำเนินธุรกิจได้อย่างต่อเนื่อง ทั้งยังสามารถจำกัดความสูญเสียต่อธุรกิจให้น้อยที่สุดในขณะที่ได้ผลตอบแทนการลงทุนคุ้มค่าที่สุด โดยเน้นไปที่สามประเด็นหลักตามกฎของการรักษาความปลอดภัย คือ การรักษาความลับ (Confidentiality) บูรณภาพของสารสนเทศ (Integrity) และความพร้อมใช้งาน (Availability)

4.4.1 ความเป็นมา

ISO17799 ถูกพัฒนาโดยตรงมาจากBS 7799 ซึ่งเป็นมาตรการจัดการด้านรักษาความปลอดภัยสารสนเทศอันเป็นที่ยอมรับอย่างแพร่หลายและต่อเนื่อง ของสถาบันมาตรา ฐานของอังกฤษ (BSI) โดยเริ่มจากการรวมกลุ่มกันทำงานด้าน ความปลอดภัยระบบสารสนเทศซึ่งมีความจำเป็นอยู่แล้วในบางอุตสาหกรรม ตั้งแต่ปี ค.ศ. 1990 จนพัฒนาต่อมาจนได้มาตรา ฐานฉบับแรกของ BS 7799 ที่สามารถใช้งานได้ในปี ค.ศ. 1995 และได้มีการปรับปรุงอีกในปี 1998 และ 1999

ทุกวันนี้ เมื่อความจำเป็นด้านความปลอดภัยของระบบสารสนเทศเป็นสิ่งสำคัญมากขึ้นสำหรับนักคอมพิวเตอร์ จนต้องการมาตรฐานในระดับสากล จึงพัฒนาต่อยอด ออกมาเป็นมาตรา ฐาน ISO เช่นเดียวกับมาตรฐานด้านอื่นๆที่ใช้กันในระดับองค์กรสากล

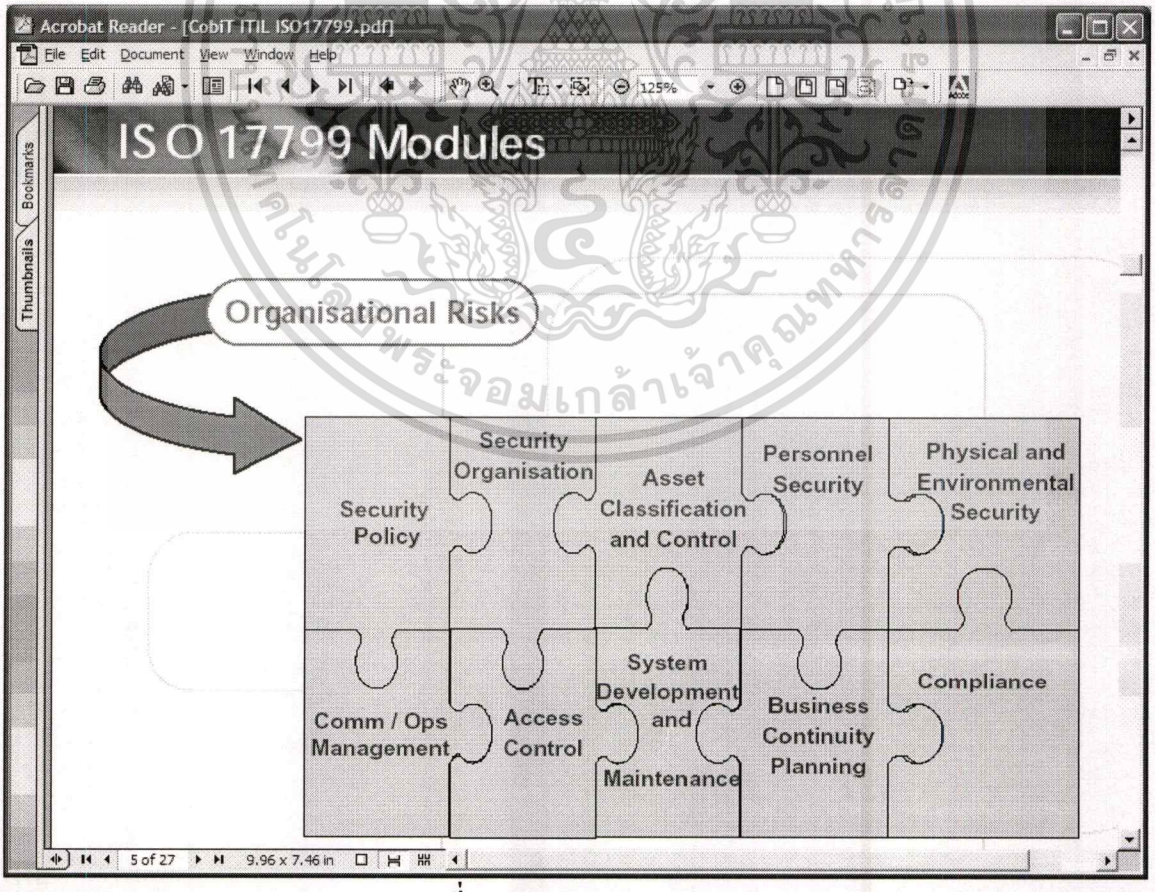
โดยทั่วไปการรักษาความปลอดภัยกับข้อมูลสารสนเทศต้องตัดสินใจและจัดวางความสำคัญระหว่างคามต้องการทางธุรกิจและปัจจัยสำคัญทางด้านความปลอดภัยทั้ง 3ด้านให้สมดุลกัน ซึ่งมักจะใช้ แนวทางปฏิบัติที่ได้ผลและข้อแนะนำ มาเป็นเกณฑ์หรือเป้าหมาย ที่เกี่ยวกับการป้องกัน การตรวจจับ และการปิดช่องทางในการรุกล้ำหรือ คุกคามสู่ระบบสารสนเทศ รวมทั้งการกู้คืนข้อมูลที่ทำสำเนาไว้มาใช้ในยามจำเป็น ตลอดจน การจัดโครงสร้างองค์กรและกลไกการจัดการกระบวนการด้านความปลอดภัยของสารสนเทศในองค์กรให้เหมาะสม ด้วยเช่นกัน

ความรู้และความเข้าใจต่อการคุกคามข้อมูลสารสนเทศ เป็นสิ่งจำเป็นอย่างยิ่งต่อสถานการณ์ปัจจุบัน จึงต้องมีการจัดหาวิธีการประเมินความเสี่ยง และควบคุมปัจจัยเสี่ยงต่างได้อย่างเหมาะสม

4.4.2 มุ่งเน้นที่นโยบาย

เนื่องด้วยระบบรักษาความปลอดภัยคอมพิวเตอร์ เป็นเรื่องด้านการจัดการมากกว่าส่วนที่เป็นเทคโนโลยี การนำมาตรฐานนี้มาใช้ควรจะประยุกต์ให้เข้ากับความต้องการตามแต่ลักษณะเฉพาะกันไป ดังนั้นจึงมุ่งเน้นไปที่การวางนโยบาย และการกำหนดบทบาทของส่วนที่มีหน้าที่เกี่ยวข้องกับความปลอดภัย และเพื่อให้เกิดความตระหนักด้านความปลอดภัยระบบสารสนเทศในองค์กร ตั้งแต่ระดับผู้บริหารและผู้ปฏิบัติการ ไปจนถึงผู้ใช้งานระบบทั่วไป เป็นแนวทางหลักในการจัดทำแผนและมาตรการในทางปฏิบัติอีกที

ความจำเป็นที่ต้องจัดทำนโยบายเพื่อสนองตอบการดำเนินธุรกิจที่มั่นคงปลอดภัย และน่าเชื่อถือได้ก็มุ่งเน้นไปที่ 3 ปัจจัยหลักของความปลอดภัย ทั้ง3 ส่วนคือ Availability Integrity และ Confidentiality แล้วต้องคำนึงถึงการสนับสนุนกระบวนการทางธุรกิจด้วย นอกจากนี้นโยบายด้านความปลอดภัยระบบสารสนเทศ ควรจะมีองค์ประกอบของ การประเมินและจัดการความเสี่ยง การตอบสนองข้อกฎหมาย หรือข้อบังคับต่างๆที่เกี่ยวข้อง และ วัตถุประสงค์ขององค์กรด้วย



ภาพที่ 4.4 ISO 17799 Modules

4.4.3 ปัจจัยหลัก 10 หัวข้อของ ISO17799

- **Security Policy** กล่าวเน้นไปที่หลักการและวัตถุประสงค์ของการรักษาความปลอดภัยสารสนเทศ ให้มั่นใจว่าสามารถปกป้อง และคุ้มกันการเข้าถึงข้อมูลทั้งทางกายภาพ และบูรณภาพของสารสนเทศ และทรัพยากรอื่นๆ จากผู้ไม่ได้รับอนุญาตได้ มีหัวข้อย่อยดังนี้
  - Outline authority of Security Function
  - Consequences of violating policy
  - Supporting documentation
  - Scope
- **Organization Security** กล่าวถึงการกำหนดความรับผิดชอบด้านความปลอดภัย ได้แก่
  - Development of policy
  - Training and Awareness
  - Review Incidents
  - Risk Assessment
  - Liaison with other groups and agencies
  - Review third party contracts
  - Security -smart
- **Asset Classification and Control** การควบคุมและจัดแยกแยะหมวดหมู่ทรัพยากร โดยการระบุความเป็นเจ้าของ และการติดป้ายหมายเลขทรัพย์สินประเภทต่างๆให้ชัดเจน ให้กับอุปกรณ์ เช่น
  - Utilities
  - Paper Files
  - Audio
  - Fax Machines
  - Postal Machines
- **Personnel Security** มีส่วนที่ต้องพิจารณาดังนี้
  - Background Checks (Temporary and Contract Staff)
  - Non – Disclosure Agreements
  - Training of Users
  - Incident Handling and Reporting

- Discipline / Rewards

- **Physical and Environmental Security**
  - Physical Access Controls to Buildings and Secure Areas
    - Key Card and Key Management
    - Receiving doors – Courier Delivery
    - Secure Telephone rooms and Modem shelves
  - Equipment Location Environmental Controls
  - Utility failures
    - Power
    - Water
    - Gas
  - Secure Cable runs
  - Equipment Maintenance Schedules and third party maintenance enforcement
  - Protection of Equipment and Data taken off-site
    - Cable locks
    - Encryption
    - Firewalls
    - Backup tapes to off-site storage
  - Clean Desk Policy
  - Disposal of old Equipment
- **Communications and Operations Management**
  - Documented procedures for:
    - Normal operations
    - Error Processing
    - Restart
  - Change Control
  - Audit Logs
  - Segregation of duties and areas
    - Prevent fraud

        - Error Detection
        - Keep Development and Production Separate
    - Operating System Patches
    - External Facilities Management Security
    - System Capacity Monitor and Planning
    - Anti-virus updates
    - Firewalls
    - Backups – generations
    - Disposal of old Media (paper, tape ,CD)
    - Email use, Retention and Privacy and Virus Risk
    - Integrity of Communications links to other courts, areas
        - Encryption
        - Digital Signatures
        - Non-repudiation and Replay
- **Access Control**
    - Policy on rights and privileges
    - Registration, Detection, Update and regular review of access levels
        - Guest ID's
        - Dual ID's
    - Password Management
        - Forced reset
        - Difficulty
    - Unattended Equipment timeout
    - Remote Login
        - Ports
        - Limited menus
- **System Development and Maintenance**
    - Structured Development Methodology

- Peer Review
- Technical Review

- Input Data Validation
- Output Controls
- Balancing
- System File and Database Protection
- Test Data Integrity
- Covert Channel Analysis

- **System Continuity Management**
  - Identify Risks
  - BIA
  - BCP
  - DRP
  - Writing and Testing Plans
  - Maintaining Plans
- **Compliance**
  - Safeguard of Privacy
  - Legislative Changes
  - Non Business use of Equipment
  - Collection of Evidence
  - Admissibility of Evidence
  - Audit Support

สิ่งที่จะเสริมให้นโยบายมีผลในทางปฏิบัติมากยิ่งขึ้นก็คือการ การตรวจปรับปรุงทบทวนและบำรุงรักษานโยบายให้เหมาะสมกับองค์กร มากขึ้นเรื่อยๆ และการให้ความรู้และปลูกฝังจิตสำนึกด้านความปลอดภัยให้กับผู้ใช้งานทุกระดับ หรือแม้นแต่ลูกค้าและคู่ค้าก็เป็นสิ่งสำคัญอย่างยิ่ง

ขั้นตอนหลักๆในการจัดเตรียมนโยบายด้วย ISO17799 จะเริ่มที่ การรวบรวมและนิยาม ระบบและกระบวนทางธุรกิจ ทั้งหมดที่มี กำหนดและระบุข้อมูลในทุกๆรูปแบบที่ใช้ แล้วมาแยกแยะหมวดหมู่ข้อมูลต่างๆ หาจุดวิกฤติและ ข้อมูลที่อ่อนไหวง่าย ให้ได้ก่อน

4.5 แนวโน้มสำหรับบริษัทหลักทรัพย์

ได้มีการสำรวจอย่างต่อเนื่องพบว่าทั้ง CoBIT Version3 และ ISO 17799 ที่นิยมใช้เป็นสิ่งอ้างอิงในการสร้างนโยบายและมาตราการรักษาความปลอดภัยระบบสารสนเทศในแต่ละองค์กร มีความคาบเกี่ยวกันค่อนข้างมาก แต่ลักษณะที่มุ่งเน้นแตกต่างกันไปบ้างในรายละเอียดปลีกย่อย และวัตถุประสงค์ในการใช้งาน

แต่เนื่องด้วย CoBIT เป็น Frame Work ที่เกิดขึ้นจาก สมาคมผู้ควบคุมและตรวจสอบระบบสารสนเทศ หรือ ISACA (Information Systems Audit and Control Association) ซึ่งมีสำนักงานสาขากับจำนวนสมาชิกที่มีอาชีพด้านการตรวจสอบระบบเทคโนโลยีสารสนเทศ อยู่ทั่วโลก และมุ่งเน้นมากขึ้นในเรื่อง IT Governance มีการทำวิจัย และโครงการด้านนี้มาต่อเนื่องเป็นเวลานาน และเป็นที่นิยมมากในระดับสากล โดยเฉพาะอุตสาหกรรมด้านการเงิน จึงมีรายละเอียดที่การตรวจสอบและเกณฑ์ต่างๆในเชิงปฏิบัติอยู่ครบถ้วนกว่า ISO 17799 มีจะมุ่งเน้นไปทางการอ้างอิงถึงวิธีการจัดการระบบโดยทั่วไป ซึ่งชัดเจนครบถ้วนด้านการปกป้องสารสนเทศ ไม่เฉพาะกับอุตสาหกรรม หรือธุรกิจใดๆมากนัก

จึงทำให้บริษัทหลักทรัพย์ในประเทศไทย นิยมที่จะนำเอามาเป็นแบบแผนในการออกแบบนโยบาย ตามกรอบงาน ของ ISO17799 ในเบื้องต้น แล้วเสริมด้วยรายละเอียดเพื่อการตรวจสอบระบบและ แนวทางในการปฏิบัติ ในหัวข้อย่อยๆต่างๆที่อ้างอิงจาก CoBIT เพื่อจะได้ยึดถือเป็นแนวทางเดียวกันกับผู้ตรวจสอบ ที่จะต้องเข้ามาร่วมในการประเมินระบบความปลอดภัยเป็นระยะอยู่แล้ว อีกทั้งยังเป็นหนทางในการไปสู่เป้าหมายขององค์กรที่เป็น บรรษัทภิบาล โดยอาศัย IT Governance เป็นสิ่งขับเคลื่อน

บทที่ 5
การบริหารความเสี่ยง

การบริหารความเสี่ยงของธุรกิจของบริษัทหลักทรัพย์ถือว่าเป็นเรื่องที่ต้องทำกันเป็นประจำอยู่เสมอ แต่ที่จะเน้นย้ำในโครงการนี้คือด้านเทคโนโลยีสารสนเทศ

5.1 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ[6]

มีแนวทางที่น่าสนใจและได้นำเสนอโดยสำนักงานคณะกรรมการกำกับและดูแลตลาดหลักทรัพย์ (กลต.) จัดทำขึ้นเผยแพร่ไว้ดังนี้

จากการศึกษาค้นคว้า ประกอบกับการตรวจสอบบริษัทหลักทรัพย์เกี่ยวกับการบริหารจัดการและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงานพิจารณาแล้วเห็นว่าความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการประกอบธุรกิจของบริษัทหลักทรัพย์ สามารถแบ่งออกเป็น 4 ประเภทหลัก ดังนี้

5.1.1. Access Risk : เป็นความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์[7] โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากบริษัทหลักทรัพย์มิได้มีวิธีการจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้อง กับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นในการใช้งาน การมิได้มีการกำหนด

---

[6] ที่มา: เอกสารเผยแพร่ สำนักเลขาธิการ กลต. การกำกับดูแลบริษัทหลักทรัพย์ตามแนว Risk-Based Approach (RBA) : 2544

[7] ระบบคอมพิวเตอร์ หมายถึง โปรแกรม ระบบงาน เครือข่าย และอุปกรณ์คอมพิวเตอร์

รหัสผ่าน(password)ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การมิได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์ เป็นต้น

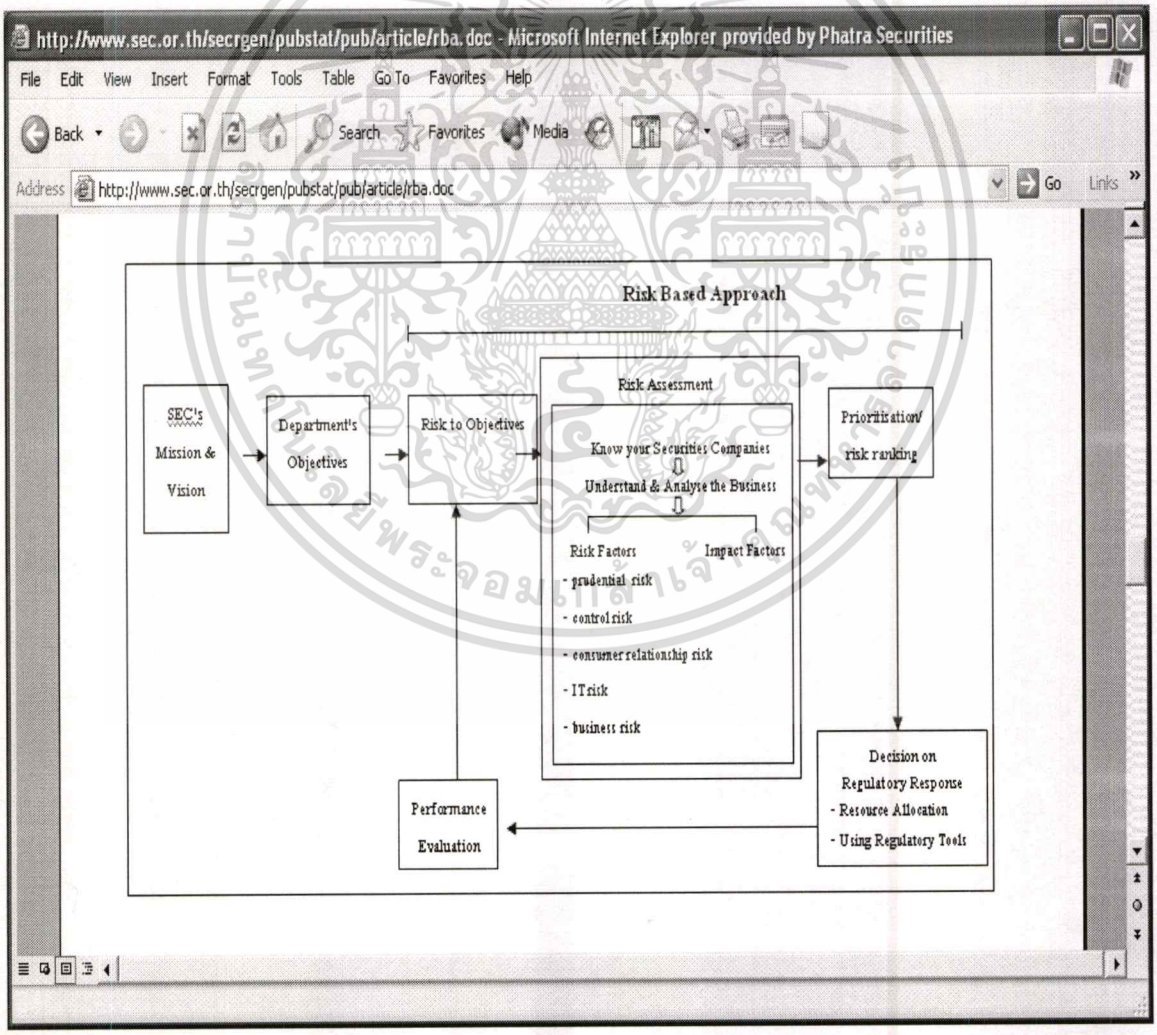
5.1.2. Integrity Risk : เป็นความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่บริษัทหลักทรัพย์มิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและ ระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไขเปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการมิได้มีระบบการควบคุมและตรวจสอบอย่างเพียงพอเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

5.1.3. Availability Risk : เป็นความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหรือการดำเนินธุรกิจของบริษัทหลักทรัพย์หยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากการมิได้ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการมิได้มีการสำรองข้อมูลและระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ หากบริษัทหลักทรัพย์มิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูล และการทำงานของระบบคอมพิวเตอร์เสียหายได้

5.1.4. Infrastructure Risk : เป็นความเสี่ยงเกี่ยวกับการที่บริษัทหลักทรัพย์มิได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี รวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์ และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจโดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการมิได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการมิได้จัดให้มี

ระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการดำเนินธุรกิจ และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่บผิดชอบ

นอกจากความเสี่ยง 4 ประเภทหลักตามที่กล่าวข้างต้น ยังมีความเสี่ยงเกี่ยวกับการที่ผู้บริหารของบริษัทหลักทรัพย์มิได้รับข้อมูลที่เกี่ยวข้องอย่างถูกต้องและทันเวลาเพื่อใช้ประกอบการตัดสินใจทางธุรกิจ ดังนั้น บริษัทหลักทรัพย์ก็ควรพิจารณาว่าข้อมูลใดบ้างที่จำเป็นแก่การตัดสินใจ รวมทั้งจัดให้มีระบบการตรวจสอบความถูกต้องของข้อมูล และจัดเตรียมข้อมูลดังกล่าวให้พร้อม เพื่อประโยชน์ในการดำเนินธุรกิจของบริษัทหลักทรัพย์เอง ทั้งนี้ ในการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ สำนักงานจะประเมินเฉพาะความเสี่ยง 4 ประเภทหลักตามที่กล่าวข้างต้น โดยไม่ประเมินความเสี่ยงที่ระบุในย่อหน้านี้



ภาพที่ 5.1 แสดงแนวทางในการประเมินความเสี่ยงบริษัทหลักทรัพย์ของ กลต.

5.2 ขั้นตอนการบริหารความเสี่ยง

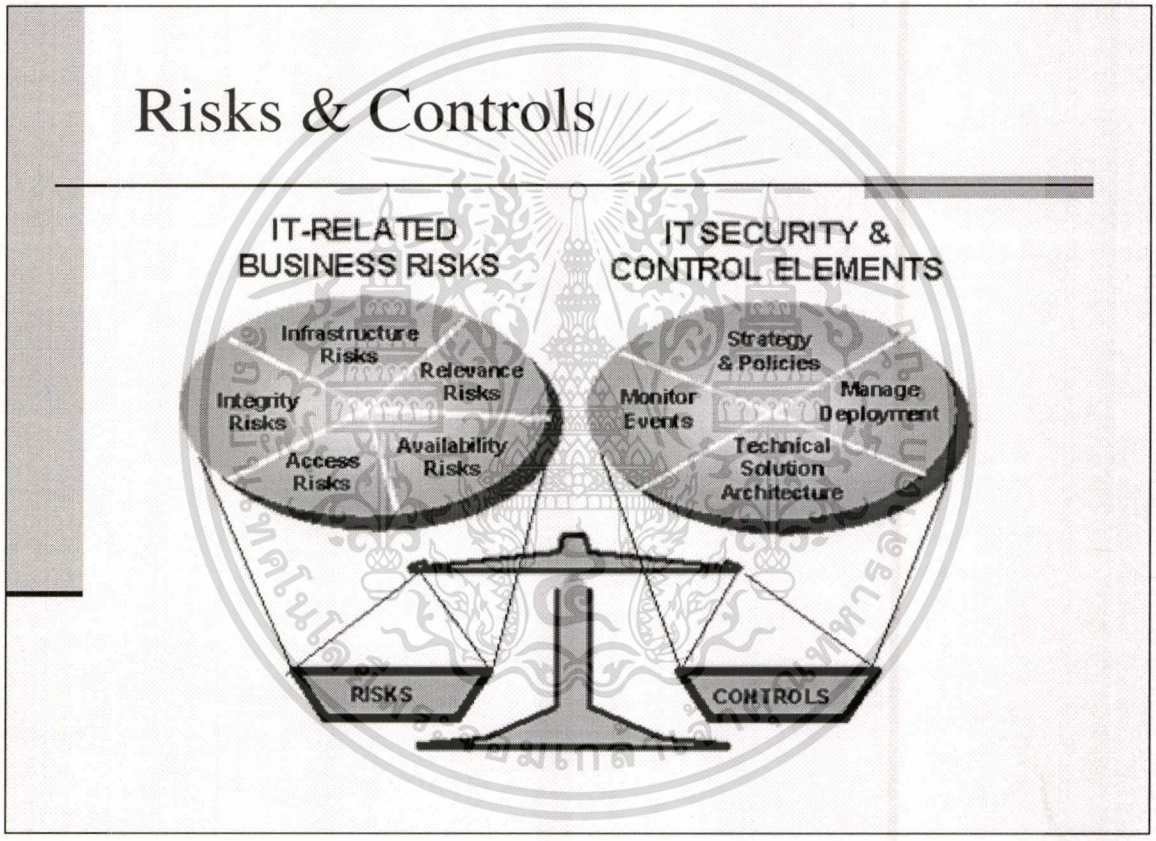
จากข้อมูลต่าง ๆ ของบริษัทหลักทรัพย์ที่มีผลกระทบต่อ risk factors และ impact factors อาจมีการเปลี่ยนแปลงได้ตลอดเวลา เช่น มีการเพิ่ม/ลดประเภทธุรกิจที่ทำ ปรับเปลี่ยนกลยุทธ์ในการประกอบธุรกิจ เปลี่ยนแปลงวิธีการปฏิบัติงาน/ระบบควบคุมการปฏิบัติงาน ทำการเพิ่ม/ลดทุน หรือเปลี่ยนแปลงผู้ถือหุ้นรายใหญ่/ผู้บริหาร/พนักงาน เป็นต้น การประเมินบริษัทหลักทรัพย์โดยใช้ RBA จึงจะมีการทบทวนผลการประเมินเป็นประจำ รวมทั้งอาจต้องมีการทบทวนใหม่เมื่อมีเหตุการณ์เปลี่ยนแปลงที่มีผลกระทบอย่างมีนัยสำคัญต่อปัจจัยที่ใช้ในการประเมิน โอกาสที่จะเกิดความเสี่ยงและผลกระทบ จึงได้ศึกษาถึงขั้นตอนหลักๆ ในการทำการบริหารความเสี่ยงตามลำดับคือ

1. การกำหนดวัตถุประสงค์
2. การระบุความเสี่ยง
3. การประเมินความเสี่ยง จะประเมินจากปัจจัยในเรื่อง
   - ผลกระทบของความเสี่ยง (Impact) และ
   - โอกาสที่จะเกิดขึ้น (occurrence)
4. การจัดลำดับความเสี่ยง แบ่งเป็น 3 ระดับ คือ
   - ความเสี่ยงต่ำ (L)
   - ความเสี่ยงปานกลาง (M)
   - ความเสี่ยงสูง (H)
5. การบริหารจัดการความเสี่ยง

5.3 การประเมินความเสี่ยงทางด้าน เทคโนโลยีสารสนเทศ

การประเมินและวิเคราะห์ความเสี่ยง จำเป็นต้องมีการทำ Information Security Risk Assessment นั่นหมายถึง การวิเคราะห์ความเสี่ยงของระบบนั่นเอง โดยผู้จัดทำต้องตอบคำถามต่างๆ เช่น ระบบมีส่วนไหนบ้างที่มีโอกาสล่มหรือโดน Hacker เข้ามาถล่ม หรือแอบขโมยข้อมูล และภัยที่จะเกิดขึ้นกับระบบจะมาจากทางไหนได้ และถ้ามีเหตุเกิดขึ้นกับระบบเช่น ระบบล่มหรือโดน Hacker เข้ามา Hack จะก่อให้เกิด ความเสียหายในครั้งนั้นจะมากน้อยเพียงใด นอกจากนี้โอกาสที่จะเกิดเหตุความถี่หรือจำนวนครั้งที่เกิดมีมากน้อยเพียงใดและมีเราควรจะทำอย่างไรเพื่อที่จะไม่ให้เกิดปัญหากับระบบหรือลดความรุนแรงของปัญหาที่เกิดขึ้น หรือ เราอาจจะทำการ ถ่ายเทความเสี่ยงไปให้บุคคลที่ 3

อย่างไรและถ้าสรุปได้ว่าจำเป็นต้องมีการซื้อ Firewall หรือ IDS ในการป้องกันระบบ ค่าใช้จ่ายทั้งหมด รวมถึงค่า Implement และ Maintenance นั้นเป็นจำนวนเท่าไรและเมื่อเปรียบเทียบระหว่าง Cost/Benefit ระหว่าง มูลค่าของความเสียหายที่เกิดขึ้น กับค่าใช้จ่ายที่เราต้องลงทุนในการป้องกันระบบว่าคุ้มกันหรือไม่ เมื่อได้คำตอบทั้งหมดก็จะทำให้องค์กรเห็นว่า ควรที่จะลงทุนในการป้องกัน Asset ขององค์กรหรือไม่อย่างไร



ภาพที่ 5.2 แสดงความสมดุลของการจัดการความเสี่ยง และการควบคุมเทคโนโลยีสารสนเทศ

การวิเคราะห์ความเสี่ยงของระบบนั้น ประกอบไปด้วยขั้นตอนใหญ่ ๆ ทั้งหมด 6 ขั้นตอน คือ

1. Inventory, Definition, and Requirements คือการเข้ามาเก็บข้อมูลและเรียนรู้ทำความเข้าใจถึง Business Process ขององค์กร ตลอดจนทำ Inventory ของ hardware และ software ที่ใช้งาน เพื่อเตรียมข้อมูลให้พร้อมในขั้นตอนต่อไป

2. Vulnerability & Threat Assessment ซึ่งเป็นการวิเคราะห์ช่องโหว่และภัยต่าง ๆ ที่อาจเกิดขึ้นกับระบบ ทั้งระดับ Network, Hosts ตลอดจน application โดยเฉพาะอย่างยิ่ง Web application เนื่องจากการโจมตีทุ ส่วนใหญ่เกิดขึ้นกับ Web sever ที่อ่อนแอ ดังนั้นจึงจำเป็นต้องใช้เครื่องมือที่มีความสามารถมาทำการวิเคราะห์เจาะหาช่องโหว่

3. Evaluation of Control หมายถึง การประเมินมูลค่าของ Control ที่ถูกนำมาใช้ในการลดผลกระทบของความเสี่ยง ในขั้นตอนนี้เราควรประเมินมูลค่าเป็นตัวเงินสำหรับ Control ต่างๆ ที่เราต้องการนำมาใช้เช่น มูลค่าของ Firewall หรือ Intrusion Detection ตลอดจนโปรแกรม Anti-virus หรือการจ้างบริษัท System Integrator (SI) มาจัดการติดตั้งเป็นต้น

4. Analysis, Decision and Documentation หมายถึงการวิเคราะห์ข้อมูลจากขั้นตอนที่หนึ่งถึงสามเพื่อนำมาตัดสินในในการเลือกใช้ Control ให้เหมาะสมกับมูลค่าของทรัพย์สิน ที่เรามีความจำเป็นต้องป้องกัน การตัดสินใจควรจะมาจากบุคคลหลายๆคนที่มีความเกี่ยวข้อง ตั้งแต่ผู้บริหารจนถึงผู้ที่ทำงานอยู่กับระบบเป็นประจำ การที่ทุกคนมาร่วมกันคิด จะทำให้การตัดสินใจนั้นมีความใกล้เคียงกับความเป็นจริงขององค์กรมากขึ้น จากนั้นเราก็ควรจัดทำเอกสารเก็บรวบรวมผลจากการทำ Assessment และผลสรุปการตัดสินใจเลือกติดตั้ง Control ที่เหมาะสมเพื่อนำไปใช้ในขั้นตอนต่อไป

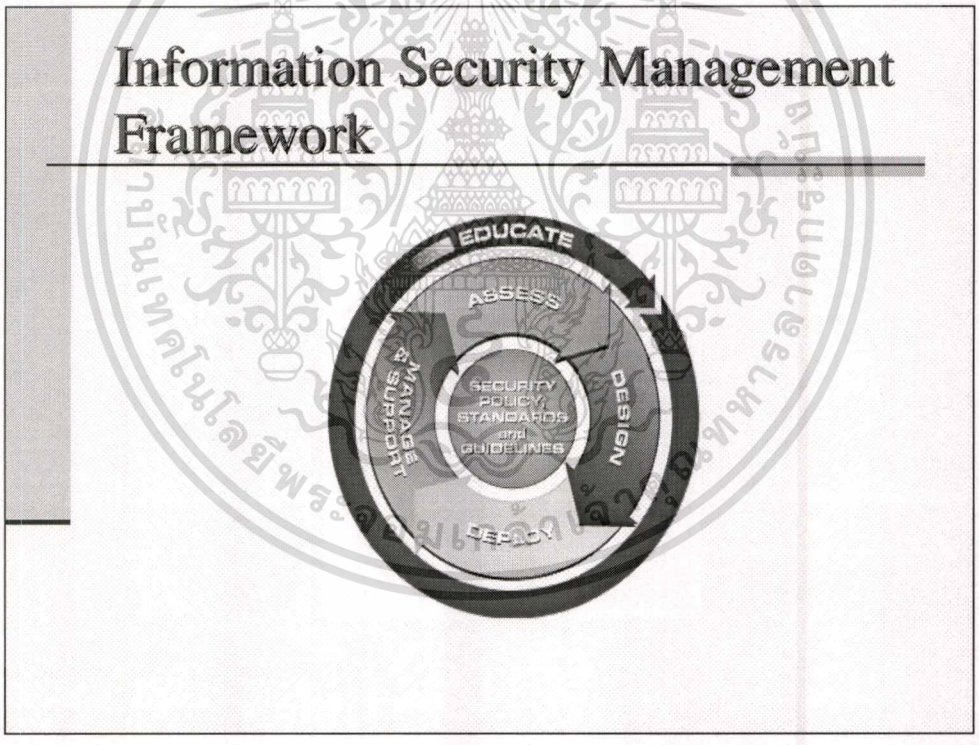
5. Communication หมายถึง การที่จะทำอย่างไรให้บุคคลอื่นหรือ แผนกอื่นๆ ในองค์กร มีความเข้าใจว่าเรากำลังต้องการที่จะลดความเสี่ยงให้กับระบบขององค์กร โดยควรแสดงให้เห็นถึงผลจากการที่เราลองเจาะระบบในขั้นตอนที่สอง และชี้ให้เห็นถึงช่องโหว่ที่เราตรวจพบตลอดจนผลที่ได้รับในทางลบหากไม่มีการติดตั้ง Control ต่างๆ ให้เหมาะสม

6. Monitoring เป็นการดูแลอยู่ตลอดหลังจากการที่เราได้ติดตั้ง Control ต่างๆ ไปแล้ว เพราะเมื่อองค์กรมีการเปลี่ยนแปลง การบริหารความเสี่ยง ก็ต้องมีการปรับให้เข้ากับสถานการณ์ใหม่ๆ ที่เกิดขึ้น บางครั้งบางระบบถึงขนาดต้องทำใหม่ทั้งหมดจากขั้นตอนที่หนึ่งเลยก็มี ดังนั้นจึงควรปรับแต่งขั้นตอนในการบริหารความเสี่ยงให้เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไปของระบบด้วย

บทที่ 6

การจัดทำแผนความปลอดภัยระบบสารสนเทศสำหรับบริษัทหลักทรัพย์ไทย

จากการศึกษาข้อกำหนด และมาตราฐาน ทางด้านความปลอดภัยต่างๆที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์ในประเทศไทยตามที่กล่าวในบทต้นที่ผ่านมาแล้วนั้น การจัดทำแผนความปลอดภัยระบบสารสนเทศสำหรับบริษัทหลักทรัพย์ไทย ต้องมีความเข้าใจในการจัดการงานด้านนี้ที่ต้องอาศัยกรอบการทำงานเพื่อการจัดการด้าน ความปลอดภัยระบบสารสนเทศที่ใช้กันแพร่หลาย และสอดคล้องกับ SecSDLC ดังที่กล่าวมาแล้ว



ภาพที่ 6.1 แสดงกรอบงานการบริหารความปลอดภัยระบบสารสนเทศ

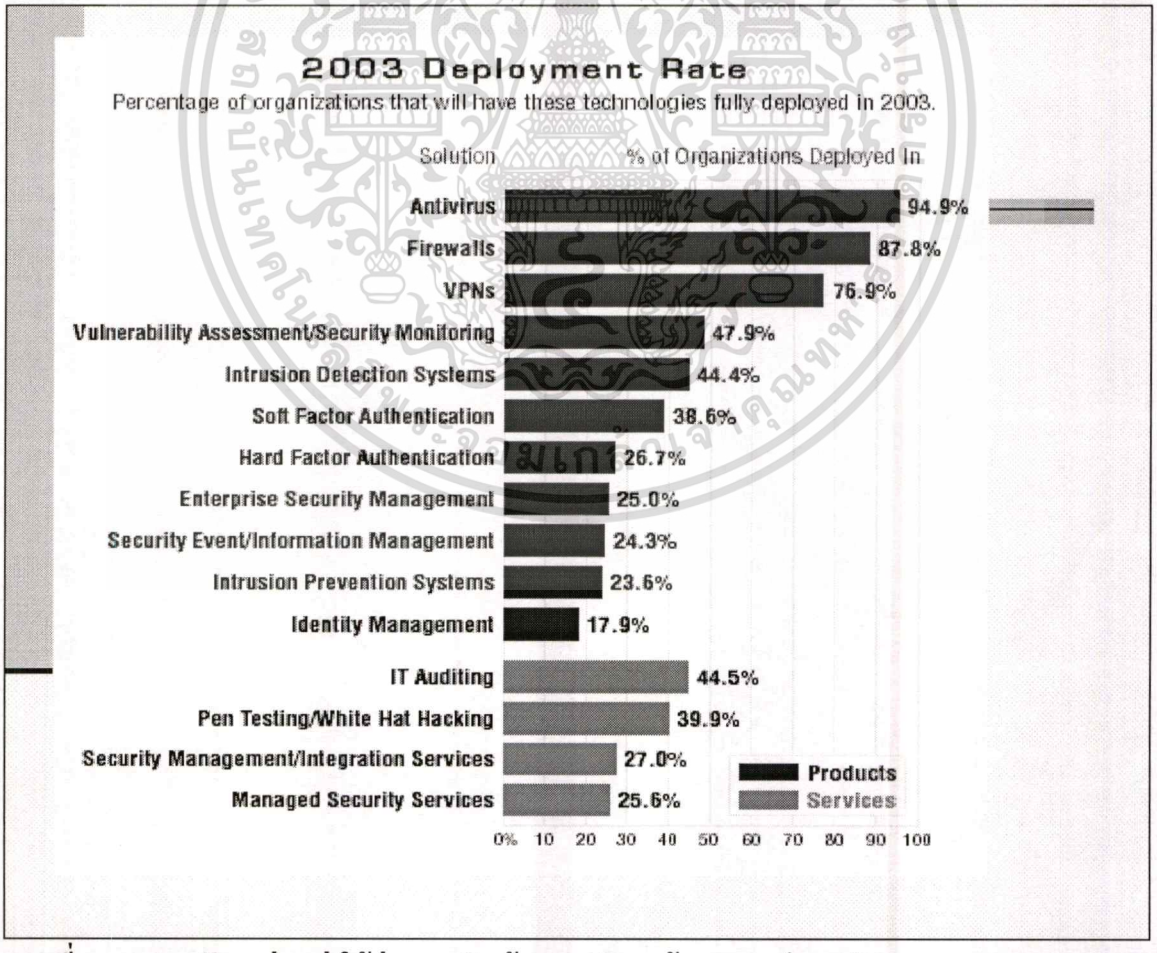
ขั้นตอนการบริหารจัดการความปลอดภัยระบบสารสนเทศเริ่มที่การประเมิน (Assess) ก่อน เพื่อให้ได้ทราบถึงสถานการณ์ปัจจุบันที่แน่ชัด โดยอ้างอิงกับ นโยบาย มาตรฐาน และ ข้อแนะนำต่างๆ

ที่เกี่ยวกับความปลอดภัยระบบสารสนเทศที่บริษัทหลักทรัพย์นั้นใช้ในปัจจุบัน ด้วยขั้นตอนการประเมินความเสี่ยงจากสภาพในปัจจุบัน และตามที่คาดการณ์ไว้

จากนั้นก็เป็นการ ออกแบบให้เหมาะสมกับองค์กร ที่ได้ทำการประเมินมา (Design) แล้วการนำไปบังคับใช้ (Deploy)และการ จัดการพร้อมทั้งความส่งเสริม สนับสนุน (Manage and Support) เพื่อให้การควบคุมและการบริหารจัดการความปลอดภัยระบบสารสนเทศเป็นไปอย่างเหมาะสม

สิ่งต้องทำอย่างต่อเนื่อง และสม่ำเสมอ ก็คือเรื่องการสร้างความเข้าใจและจิตสำนึก พร้อมทั้งการให้ความรู้และแนวทางที่ถูกต้อง และทันสมัย ซึ่งต้องทำอย่างต่อเนื่องให้กับทุกๆคนในทุกระดับชั้นของบริษัท เพื่อดำรงไว้ ซึ่งความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่สามรถปกป้องไว้และเชื่อใจได้ของสารสนเทศที่มีความจำเป็นยิ่งๆ ขึ้นในการดำเนินธุรกิจหลักทรัพย์เช่นนี้

จึงทำให้การบริหารจัดการความปลอดภัยระบบสารสนเทศ เป็นสิ่งที่ต้องเฝ้าทำงานและปรับปรุงอยู่สม่ำเสมอและเป็นระบบอย่างต่อเนื่องเป็นวัฐจักร



ภาพที่ 6.2 แสดงอัตราส่วนค่าใช้จ่ายของสินค้าและ บริการด้านความปลอดภัยระบบสารสนเทศ

จากการแบ่งประเภทของนโยบายด้านความปลอดภัยของ The National Institute of Standards and Technology 800-14 ซึ่งแบ่งเอาไว้ 3 ประเภทคือ

- General or Security program policies จะกล่าวถึง นโยบายความปลอดภัยทั่วๆไป และนโยบายความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ซึ่งจะต้องเป็นไปตามแนวทางและวิสัยทัศน์ของผู้บริหารระดับสูง โดยกำหนดผ่านกลยุทธที่เลือกแล้วออกมาเป็นระดับนโยบายขององค์กร แล้วแตกย่อยไปเป็นนโยบายของฝ่ายสารสนเทศ เป็นตามขั้นตอน
- Issue - Specific Security policies เป็นนโยบายที่เฉพาะมาที่กระบวนการและปฏิบัติงานด้านเทคโนโลยีสารสนเทศที่ใช้งานกันเป็นประจำ
- Systems –specific Security policies ระบุชัดเจนลงไปเป็น มาตรฐาน หรือ ข้อบังคับต่างๆในรายละเอียดมากขึ้น แบ่งได้ 2 กลุ่มคือ Access Control Lists และ Configuration Rules

ตารางที่ 6.1 เปรียบเทียบแผนความปลอดภัยและการป้องกันระบบสารสนเทศรูปแบบต่างๆ

Security Components	People	Information	Systems	Networks	Internets
Technology	Access Contre	Encryption Backups	Host IDS Patches Monitoring Redundancy	Network IDS Proxy servers Firewalls	Virus Scans Spam - Filter
Management	Policy & Law	Education Training	Standards Procedures	Standards Procedures	Policy & Law
Security Plan Covering	Organization Policy (6.1) Policy (6.6)	Policy (6.1) Policy (6.5) BCP (7.2) IR (7.3)	Policy (6.2) Policy (6.5)	Policy (6.3) Policy (6.6)	Policy (6.4) Policy (6.3)

6.1 นโยบาย ความปลอดภัยระบบสารสนเทศ

1.ข้อมูลสารสนเทศถือเป็นทรัพย์สินของบริษัท พนักงานทุกคนมีหน้าที่สำคัญที่จะต้องปกป้องรักษาให้คงสภาพและ เป็นทรัพย์สินอันทำประโยชน์สูงสุดต่อบริษัท

2.พนักงานทุกคนที่จะต้องรับทราบ และทำความเข้าใจ โดยถือว่านโยบายนี้มีความสำคัญ ที่ต้องปฏิบัติสม่ำเสมอเป็นการยอมรับโดยชอบในการปกป้องรักษาข้อมูลที่เป็นทรัพย์สินของบริษัท

3.บริษัทมีหน้าที่การดูแลรักษาความปลอดภัยต่อข้อมูลสารสนเทศ และเข้าใจสถานภาพความเป็นความลับ บูรณภาพ และคุณค่าแห่งสาระสำคัญ

4.บริษัทจัดทำคู่มือปฏิบัติงาน เพื่อให้การดูแลรักษาข้อมูลสารสนเทศ เป็นแนวทางปฏิบัติเดียวกัน

5.บริษัทต้องแจ้งให้บริษัทคู่ค้า/คู่สัญญาได้เข้าใจและรับทราบถึงนโยบายรักษาความปลอดภัยด้วย เพื่อให้บริษัทคู่ค้า/คู่สัญญา ได้เข้าใจในนโยบายรักษาความปลอดภัย

6.กลุ่มผู้รักษาความปลอดภัยข้อมูลสารสนเทศ ต้องได้รับมอบอำนาจและการสนับสนุนจากผู้บริหาร ในการดำเนินนโยบายรักษาความปลอดภัย

7.บริษัทจะต้องปฏิบัติภายใต้กฎหมาย ระเบียบ รวมทั้งพันธกรณีใดๆ ที่เกี่ยวข้อง

การแบ่งแยกหน้าที่

การแยกการบริหารหรือการจัดการ ออกจากหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงแก้ไข จากผู้ไม่มีอำนาจ

- ผู้ใช้ข้อมูลจะต้องไม่เป็นผู้อนุมัติการนำข้อมูลสารสนเทศไปใช้งาน
- ต้องมีการควบคุม ตรวจสอบการเข้าถึงข้อมูลและผู้ใช้

6.1.1. คณะบริหารงานความปลอดภัยสารสนเทศ

เพื่อการปฏิบัติงานเป็นไปโดยราบรื่น คณะทำงาน อาจประกอบด้วย ผู้บริหารระดับอาวุโส เช่น ผู้บริหารหน่วยงาน เช่น ฝ่ายสารสนเทศ ฝ่ายตรวจสอบภายใน ฝ่ายบริหารบุคคล ฝ่ายกฎหมาย ฝ่ายประชาสัมพันธ์ และคณะทำงานรักษาความปลอดภัยข้อมูลสารสนเทศ เพื่อที่จะสนับสนุนเป้าหมายการรักษาความปลอดภัย ซึ่งกำหนดโดยคณะทำงานรักษาความปลอดภัยของข้อมูลสารสนเทศ และให้ความร่วมมือต่อคณะทำงาน ดำเนินการในส่วนที่เกี่ยวข้องกับการรักษาความปลอดภัย อันมีผลกระทบต่อข้อมูลสารสนเทศอันเป็นทรัพย์สินของบริษัท อนุมัติเอกสารที่จัดทำขึ้นตามข้อกำหนดของมาตรฐานและนโยบายรักษาความปลอดภัย ให้ความร่วมมือในการควบคุมการปฏิบัติการรักษาความปลอดภัย

นอกจากนี้ยังมีหน้าที่ที่สำคัญที่ควรพิจารณาดังนี้

- ให้คำแนะนำ ความเสี่ยงและข้อพึงปฏิบัติให้แก่บริษัท
- ทบทวนข้อบังคับที่เกี่ยวกับมาตรฐานและนโยบายรักษาความปลอดภัย
- จัดทำข้อกำหนดการส่งผ่านข้อมูลสารสนเทศไปยังหน่วยงานภายนอก
- ดูแลรักษาสัญญาที่จัดทำขึ้นโดยหน่วยงานรักษาความปลอดภัยภายนอก เช่น ผู้ให้บริการข่าวสารสารสนเทศ คณะผู้เชี่ยวชาญรักษาความปลอดภัย

6.1.2. การประเมินความเสี่ยงของการบริหาร

เป็นการกำหนดการคุกคามทรัพย์สิน ภัยพิบัติ และผลกระทบและการตัดสินใจในระดับความเสี่ยงที่อาจเกิดขึ้นโดยพิจารณาได้ดังหัวข้อต่อไปนี้

- การรับผิดชอบในการกำหนดและพิจารณาประเมินผลความเสี่ยง
- รายงานผลความเสี่ยงและแผนการนำไปปฏิบัติจะต้องจัดเป็นเอกสาร และอนุมัติโดยคณะทำงานบริหารรักษาความปลอดภัยข้อมูลสารสนเทศ
- การประเมินผลความเสี่ยง จะถูกกำหนดเป็นข้อบังคับเพื่อให้ครอบคลุมถึงการควบคุมการรักษาความปลอดภัย หรือการนำไปปฏิบัติงาน
- การควบคุมรักษาความปลอดภัยข้อมูลสารสนเทศ จะถูกนำไปปฏิบัติภายใต้ความระมัดระวัง และให้ความสำคัญ ต่อข้อมูลสารสนเทศอย่างสมเหตุสมผล
- การประเมินผลความเสี่ยง จะต้องมีการทบทวนและปรับปรุงอย่างน้อย 1 ปี

6.1.3.บทบาทการเป็นเจ้าของข้อมูล และความรับผิดชอบ

ผู้บริหารจะต้องรับผิดชอบในเรื่องดังต่อไปนี้

- กำหนดระดับชั้นของเอกสารตามการใช้งานอย่างชัดเจน
- จัดทำนโยบายรักษาความปลอดภัยรวมทั้งแผนการดูแลรักษาที่เหมาะสม
- ควบคุม และอนุมัติการเข้าถึงข้อมูล ทรัพยากรระบบ แผนงานธุรกิจ และ เอกสารประกอบที่เกี่ยวข้อง
- ตัดสินใจเกี่ยวกับระดับความสำคัญเข้าถึงข้อมูลระบบ รวมถึงข้อกำหนดบริษัท
- กำหนดข้อปฏิบัติการตรวจทานที่นำมาใช้ในการบันทึกข้อมูลอย่างถูกต้อง
- อนุมัติข้อปฏิบัติการตรวจทาน และควบคุมการเปลี่ยนข้อมูลสารสนเทศที่กู้คืนมาจากการคุกคาม
- กำหนดคุณลักษณะที่เหมาะสมของทดสอบความต้องการของข้อมูลสารสนเทศตามแผนการกู้คืนข้อมูล

- สร้างความเข้าใจ และการยอมรับว่ายังคงมีความเสี่ยงที่ยังคงสภาพในข้อมูล สารสนเทศ

6.1.4.บทบาทและความรับผิดชอบของผู้ดูแล

ผู้ดูแลต้องดูแลทั้งส่วนกายภาพ ข้อมูล และลิขสิทธิ์หรือทรัพย์สินที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ซึ่งถือว่าเป็นสมบัติขององค์กรที่ต้องดูแลด้วย ระบบทุกระบบต้องมีผู้ที่ได้รับมอบหมายให้ดูแล โดยผู้ดูแลมีหน้าที่รับผิดชอบดังนี้

- การคุ้มครองข้อมูลประกอบด้วยการติดตั้งระบบป้องกัน การเข้าถึงข้อมูลของผู้ไม่มีสิทธิ์ จะต้องมีการทำสำเนาหรือสำรองข้อมูลที่มีความสำคัญ เพื่อไม่ให้สูญหาย
- การปฏิบัติงานและการบำรุงรักษาระบบควบคุมความปลอดภัยเป็นไปตามที่กำหนด
- การติดตั้ง ปฏิบัติงาน ติดตามตรวจสอบ และบำรุงรักษา ระบบสารสนเทศให้เป็นไปตามที่กำหนด
- ให้แน่ใจว่าการเตือนเมื่อมีผู้บุกรุก จะแจ้งเตือนได้ทันเวลาตามที่กำหนด
- ดูแลข้อผิดพลาด หรือการทำงานที่ผิดปรกติ ของระบบคอมพิวเตอร์ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความปลอดภัย

6.1.5.การจัดกลุ่มข้อมูล และการควบคุม

เพื่อสร้างความมั่นใจสูงสุดในการป้องกันข้อมูลซึ่งถือเป็นทรัพย์สินของบริษัท จึงจำเป็นต้องมีการจัดกลุ่มข้อมูลตามลำดับความสำคัญ บริษัทจะต้องจัดกลุ่มข้อมูลในความรับผิดชอบโดยจะถือเป็นทรัพย์สินประเภทหนึ่งของบริษัท หากมีการจัดเก็บข้อมูลไม่ว่าจะเป็นทางสื่อประสม หรือทางระบบด้วยระดับความสำคัญ"**ลับที่สุด**" และได้มีการเปลี่ยนแปลงเป็นระดับความสำคัญ "ลับ" ดังนั้นจะต้องมีการเปลี่ยนแปลงสื่อประสมหรือระบบนั้นด้วย ถ้ามีการเพิ่มขั้นตอน รวมทั้งวิธีปฏิบัติที่ซับซ้อนขึ้น ซึ่งเก็บรวมรวมข้อมูลด้วยระดับความสำคัญที่แตกต่างกัน จะต้องเปิดเผยสาระสำคัญนี้ด้วย

ข้อมูลภายในองค์การ

ข้อมูลประเภทนี้เป็นการจัดกลุ่มข้อมูลที่สามารถเผยแพร่ภายในองค์กรได้โดยไม่มีผลกระทบองค์กร เช่น ข้อมูลพนักงาน ข้อมูลผู้ถือหุ้น ข้อมูลหุ้นส่วนธุรกิจ และ/หรือข้อมูลลูกค้า
ข้อมูลประเภทนี้สามารถเผยแพร่ภายในองค์กร และตัวแทนผู้จำหน่ายสินค้าที่เป็นคู่สัญญา

ข้อมูลจำเพาะ

ข้อมูลจำเพาะ ไม่ว่าจะเป็นข้อมูลทางเทคนิค ข้อมูลทางการเงิน ข้อมูลกลยุทธ์ทางธุรกิจ หรือข้อมูลทางการบริหาร เมื่อไม่มีการใช้งานแล้ว (ยกเลิกการใช้งาน) หรืออยู่ระหว่างการเจรจา จะต้องทำลายเพื่อมิให้มีการเปิดเผยไปยังคู่แข่ง ข้อมูลจำเพาะที่แสดงคำบรรยายคุณลักษณะ เช่นข้อมูลแสดงผลกำไรโดยเปรียบเทียบ จะไม่เผยแพร่เนื่องจากอาจจะมีผลกระทบความมั่นคงขององค์กร การ

เผยแพร่ข้อมูลประเภทนี้จะจำกัดเฉพาะพนักงานภายในองค์กรเท่านั้น หรือกลุ่มบุคคลซึ่งมีข้อสัญญาในการเผยแพร่ข่าวสารข้อมูลเท่านั้น

ข้อมูลลับที่สุด

การจัดกลุ่มข้อมูลระดับ "ลับที่สุด" จะเป็นข้อมูลซึ่งหากถูกนำไปเผยแพร่โดยผู้ไม่สิทธิจะมีผลกระทบ ต่อความมั่นคงขององค์กร ผู้ถือหุ้น หุ้นส่วนธุรกิจ และ/หรือลูกค้าขององค์กร ซึ่งเผยแพร่เฉพาะกลุ่มบุคคลที่มีรายชื่อเท่านั้น

6.1.6. การลด หรือเพิ่มระดับชั้นความสำคัญของข้อมูล

การพิจารณาลดระดับความสำคัญ องค์กรจะต้องกำหนดประเภทของข้อมูลให้หน่วยงานที่เกี่ยวข้องดำเนินการ โดยกำหนดระยะเวลาอย่างน้อยปีละ 1 ครั้ง การลดระดับชั้นความสำคัญของข้อมูลจะต้องประกาศเป็นวิธีปฏิบัติงาน การแจ้งผลการพิจารณาลดระดับชั้นความสำคัญของข้อมูล จะต้องแจ้งวันที่มีผลบังคับใช้ด้วย

6.1.7. การควบคุมการใช้งานเอกสารข้อมูล และ สื่อประสม

ข้อมูลทุกประเภทจะต้องกำหนดการนำไปใช้งานตามระดับชั้นความสำคัญของข้อมูล

- **ข้อมูล "ลับที่สุด"**

ข้อมูลประเภทนี้จะต้องไปรับการพิจารณาอนุมัติจากฝ่ายบริหารก่อนนำไปใช้งาน หรือเผยแพร่ และต้องระบุจำนวนหน้าไว้อย่างชัดเจน เช่น หน้า 2 ของจำนวนทั้งหมด 5 หน้า การจัดทำสำเนาข้อมูลเอกสาร "ลับที่สุด" จะต้องได้รับการอนุมัติจากผู้บริหารทุกครั้งโดยต้องมีเลขที่หน้าของเอกสารตรงกับเอกสารต้นฉบับ และมีการลงลายมือในสำเนาข้อมูลเอกสาร "ลับที่สุด" ทุกหน้า

กรณีพิมพ์ข้อมูลเอกสารทางเครื่องพิมพ์ ผู้จัดทำจะต้องดูแลเอกสารดังกล่าวอย่างระมัดระวังเอกสารทุกฉบับที่สั่งพิมพ์ ผู้จัดทำต้องลงลายมือทุกครั้งโดยต้องได้รับการอนุมัติเป็นลายลักษณ์อักษร ส่วนการจัดส่งข้อมูลเอกสาร "ลับที่สุด" ทางระบบคอมพิวเตอร์ จะจัดส่งเฉพาะผู้เกี่ยวข้องที่มีรายชื่อเท่านั้น และจะไม่มีการจัดส่งข้อมูลเอกสาร "ลับที่สุด" ไปยังสาธารณะชน

การส่งข้อมูลเอกสารทางเครื่องโทรสาร การจัดส่งข้อมูลเอกสาร "ลับที่สุด" จะต้องจัดส่งโดยกำหนดผู้รับปลายทางเสมอ โดยผู้ได้รับมอบหมายเท่านั้น ต้องดำเนินการโดยรัดกุม

การขนย้ายข้อมูลเอกสาร การขนย้ายข้อมูลเอกสาร "ลับสุดยอด" จะต้องได้รับอนุมัติจากผู้บริหาร ซึ่งรวมถึงการเคลื่อนย้ายอุปกรณ์เครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงต่าง ๆ เช่น Hard disk, floppy disk

การส่งข้อมูลทางเครือข่าย หากต้องส่งข้อมูลเอกสาร "ลับที่สุด" ทางเครือข่าย จะต้องส่งโดยการเข้ารหัสเสมอ ซึ่งให้รวมถึงการจัดส่งทาง Internet คู่สายโทรศัพท์ เครื่องโทรสาร หรือเครือข่าย

อื่น ๆ และต้องไม่ถูกจัดเก็บไว้ในระบบ Internet หรือ Intranet server ยกเว้น server ที่กำหนดรหัสการเข้าถึงข้อมูล การจัดส่งข้อมูลเอกสาร "ลับที่สุด" จากเครื่องคอมพิวเตอร์หนึ่งไปยังอีกเครื่องหนึ่ง ผู้จัดเก็บข้อมูลจะต้องจัดส่งด้วยความระมัดระวังรอบคอบการจัดเก็บข้อมูลไว้ใน Laptop, Notebook, palmtop, หรือเครื่องคอมพิวเตอร์ประเภทอื่น ๆ จะต้องเข้ารหัสทุกครั้ง

- **การขนย้ายข้อมูล หรือการนำกลับมาใช้งาน**

ก่อนขนย้ายหรือทำลายข้อมูล จะต้องพิจารณาอนุมัติทุกครั้งโดยต้องลงบันทึก หากมีความต้องการนำกลับมาใช้งาน และให้เป็นไปตามกฎ ระเบียบปฏิบัติ เพื่อการตรวจสอบ

6.1.8. การใช้ทรัพยากรคอมพิวเตอร์ในทางมิชอบ

พนักงานจะไม่ใช้ทรัพยากรคอมพิวเตอร์ของบริษัทกับกิจกรรมที่ไม่ใช่งานของบริษัท ครอบคลุมถึงการใช้งานนอกเวลาการทำงานของบริษัท ทรัพยากรคอมพิวเตอร์และเครือข่ายของบริษัทถือเป็นเครื่องมือทางธุรกิจ จะต้องไม่ถูกนำไปใช้ในลักษณะที่จะก่อให้เกิดความเสื่อมเสียต่อบริษัท หรือจดหมายลูกโซ่แสดงความคิดเห็นส่วนตัว ในนามบริษัท การใช้เข้าสู่อินเทอร์เน็ตซึ่งจะต้องอยู่ภายใต้นโยบายความปลอดภัยสารสนเทศของบริษัท และกฎหมายที่เกี่ยวข้องกับการอ้างอิงในความปลอดภัยของจดหมายอิเลคทรอนิคส์

6.1.9. สิทธิในทรัพย์สินทางปัญญา

ทรัพย์สินทางปัญญาที่ถูกพัฒนาขึ้นโดยพนักงานบริษัทในช่วงระยะเวลาการจ้างงาน(และใช้ทรัพยากรของบริษัท) ซึ่งครอบคลุมถึงแบบอย่างของธุรกิจ ผลิตภัณฑ์ เทคโนโลยี เทคนิค วิธีการปฏิบัติงาน บริการ ผลการวิจัย และการพัฒนาถือเป็นทรัพย์สินของบริษัทเพียงผู้เดียว

ข้อกำหนดนี้จะรวมถึง การประพันธ์ สิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้า และทรัพย์สินทางปัญญาอื่นๆทั้งหมดที่ปรากฏอยู่ในบันทึก แผนงาน กลยุทธ์ ผลิตภัณฑ์ โปรแกรมคอมพิวเตอร์และเอกสารอื่นๆของบริษัท ระบบการสื่อสารและข้อความที่เกิดทางอิเลคทรอนิคส์ รวมทั้งสำเนาข้อมูลถือเป็นทรัพย์สินของบริษัทด้วยเช่นกัน

6.1.10. ความปลอดภัยทางในสถานที่ทำงาน

มีการกำหนดขอบเขตการป้องกันในด้านความปลอดภัย สำหรับพื้นที่ใช้ในการดำเนินธุรกิจและสถานที่ใช้ในการประมวลผลข้อมูลสารสนเทศไว้อย่างชัดเจน และเหมาะสมกับขอบเขตที่เป็นสถานที่ทำงานทั้งหมดโดยมีการพิจารณาขอบเขตการป้องกันใหม่อย่างน้อยที่สุดทุกๆ 1 ปี

ทางเข้าออกทุกทางจะต้องถูกปิดเมื่อไม่ได้ใช้งานและควรจะต้องพิจารณาถึงเรื่องการป้องกันการเข้าสู่อาคารจากภายนอกทางหน้าต่าง ระบบป้องกันการบุกรุกมีสัญญาณเชื่อมต่อไปถึงสถานี

6.2.3. การระบุรหัสเพื่อเข้าสู่ระบบ

วัตถุประสงค์ : ผู้ใช้งานทุกคนที่เข้าใช้ฐานข้อมูลของบริษัทต้องมีรหัสส่วนตัว (USER ID) สำหรับใช้งานเฉพาะตนเอง

- กระบวนการมอบ user id และ password ให้ผู้ใช้งานต้องทำอย่างเป็นทางการ
- การใช้ user id และ password ร่วมกันไม่สามารถทำได้หากไม่มีการอนุมัติจากเจ้าของบริษัทหรือกลุ่มผู้ดูแลความปลอดภัยของฐานข้อมูลก่อน
- หากมีข้อจำกัดการปฏิบัติงานจนทำให้เกิดความจำเป็นในการใช้ user id และ password ร่วมกันมีกระบวนการควบคุมต่างๆ ต่อไปนี้จะต้องถูกนำมาใช้งาน
  - การควบคุมร่วมกันระหว่างกลุ่มผู้ใช้งานที่มีการใช้ user id และ password ร่วมกัน
  - การสร้างข้อมูลสำหรับกระบวนการตรวจสอบ
  - การกำหนดให้ใช้งาน 1 user id ต่อ 1 ครั้ง

โปรแกรมควบคุมการเข้าใช้ระบบ

ควรมีการติดตั้งโปรแกรมควบคุมการเข้าใช้ระบบและโปรแกรมระบบที่มีคุณลักษณะในเรื่องเกี่ยวกับความปลอดภัยเพื่อจำกัดการเข้าใช้งานในระบบและฐานข้อมูลของบุคคลที่ไม่ได้รับอนุญาตเพื่อควบคุมการเข้าใช้งานระบบดังนี้

- ป้องกันไม่ให้ทำการแก้ไขหรือลบโดยไม่ได้รับอนุญาต
- บังคับให้ผู้ใช้งานต้องทำการใส่รหัสผ่านเพื่อระบุตัวตนก่อนเข้าสู่ระบบและมีวิธีการตรวจสอบความถูกต้องของรหัสผ่านของผู้ใช้งานดังกล่าวด้วย
- มีระบบตรวจสอบข้อมูล

6.2.4. การควบคุมและจัดการเกี่ยวกับ password

วัตถุประสงค์ : การใช้ password เป็นวิธีการที่นำมาใช้ในการพิสูจน์ตัวตนของผู้ใช้งาน การจัดสรร password จำเป็นต้องมีกระบวนการควบคุมการจัดการอย่างเป็นทางการ

- ระบบจัดการเกี่ยวกับ password ต้องมีการนำไปใช้งานเพื่อให้เกิดความเชื่อถือของการเข้าใช้งานระบบ user id ของแต่ละบุคคล
- passwords ทั้งหมดจะต้องมีความยาวอย่างน้อย 8 ตัวอักษร (alphanumeric)และไม่ใช้คำที่เกี่ยวข้องกับเจ้าของ password อันอาจจะทำให้ผู้อื่นสามารถคาดเดาได้หรือนำข้อมูลส่วนตัวทั่วๆไปมาตั้งเป็น password เช่น ชื่อ หมายเลขโทรศัพท์ คำศัพท์ในพจนานุกรม

- ไม่มีการเขียนไว้เป็นลายลักษณ์อักษรเว้นเสียแต่ว่าจะมีการจัดเก็บในที่ที่มีความปลอดภัย
- เก็บไว้ในรูปแบบที่มีการเข้ารหัสโดยใช้วิธีการเข้ารหัสแบบทางเดียว (Hash)
- ไม่ควรให้หรือเปิดเผย password ไว้ในที่ต่าง ๆ
- หากมีการใส่ password ผิดเกิน 3 ครั้ง ระบบจะระงับการใช้ User ID นั้น
- password ชั่วคราวควรถูกเปลี่ยน เมื่อเข้าสู่ระบบครั้งแรก
- ไม่มีระบบการแสดงค่า password โดยอัตโนมัติ

การเปลี่ยน password

- ควรเปลี่ยน password เป็นประจำ นานที่สุดไม่ควรเกิน 4 เดือน
- password ของ user id ที่มีสิทธิพิเศษในการเข้าใช้งานระบบที่มีความสำคัญจะต้องถูกเปลี่ยนบ่อยครั้งกว่า password ที่ใช้งานปกติ

6.2.5. โครงสร้างของระบบความปลอดภัย

วัตถุประสงค์ : โครงสร้างของระบบปฏิบัติการหรือโปรแกรมระบบอื่นๆจะต้องมีการรักษาความปลอดภัยอย่างเคร่งครัดก่อนนำไปใช้งานจริง

- การจัดการข้อมูลที่มีความไวต่อการเปลี่ยนแปลงของบริษัทไม่ควรทำผ่าน display screens ของทุกระบบ เพื่อผู้ที่ไม่มีสิทธิใช้งานจะได้ไม่สามารถเข้าดูได้โดยง่าย
- โครงสร้างของระบบปฏิบัติการจะต้องประกอบด้วย function ที่จำเป็นต่อการปฏิบัติงานเป็นอย่างน้อย
- ต้องมีการจัดทำกระบวนการรักษาความปลอดภัยใหม่ทุกครั้งที่มีการ upgrade หรือ update ระบบ
- ต้องมีการพิสูจน์ความถูกต้องและพิสูจน์ตัวตนของโปรแกรมระบบปฏิบัติการที่มีการ update ที่มาจากแหล่งที่เชื่อถือได้ก่อนนำไปติดตั้งใช้งานจริง
- โปรแกรมที่ได้รับการปรับปรุงความปลอดภัย(security patch) จะต้องถูกรนำมาติดตั้งภายใน 30 วัน หลังจากมีประกาศใช้อย่างเป็นทางการ

การยุติการใช้ระบบ

- การยุติการใช้ระบบจะต้องมีการปิดระบบปฏิบัติการและการติดต่อสื่อสาร เพื่อป้องกันการใช้ที่ไม่ได้รับอนุญาต

- สำหรับระบบที่ไม่สามารถตั้งค่ายุติการใช้ระบบได้ ผู้ใช้ระบบคนสุดท้ายจะต้องคอยสอดส่องดูแลเพื่อให้เกิดความแน่ใจว่า จะไม่มีการเข้าสู่ระบบโดยผู้ใช้งานคนอื่นที่ไม่ได้รับอนุญาติ

การยุติการเชื่อมต่อ

- การจำกัดเวลาการเชื่อมต่อจะต้องมีการกำหนดให้เหมาะสมกับการใช้งานแต่ละประเภท
- ระบบปฏิบัติการที่มีความสำคัญจะต้องมีการกำหนดเวลาการยุติการเชื่อมต่อ

6.2.6. การใช้โปรแกรมประเภท Utilities และ Tools

วัตถุประสงค์ : การใช้โปรแกรมประเภท Utilities และ Tools ที่มีอยู่ในเครือข่าย โปรแกรมประยุกต์ หรือโปรแกรมระบบ จะต้องถูกจำกัดขอบเขตในการใช้และควบคุมการใช้

- การใช้โปรแกรมประเภท Utilities และ Tools จะต้องได้รับอนุญาตจากผู้ดูแลระบบ และกลุ่มคณะทำงานรักษาความปลอดภัยข้อมูลสารสนเทศก่อน และจะได้อนุญาตให้ใช้ตามความจำเป็นพื้นฐาน
- โปรแกรมประเภท Utilities และ Tools จะต้องมีการควบคุมไม่ให้มีการเข้าถึงโดยไม่มีสิทธิ
- การใช้โปรแกรมประเภท Utilities และ Tools ต้องมีการแบ่งแยกออกจากโปรแกรมประยุกต์ และรวมถึงการแบ่งแยกหน้าที่ในการดำเนินงาน การแบ่งแยกบัญชีผู้ที่มีสิทธิใช้งาน
- ระยะเวลาในการใช้โปรแกรมประเภท Utilities และ Tools จะต้องถูกจำกัดการใช้งาน
- การใช้โปรแกรมประเภท Utilities และ Tools จะต้องมีบันทึก(log) และมีการสอบทานอย่างน้อยทุก 1สัปดาห์โดยกลุ่มความปลอดภัยสารสนเทศ
- ผู้ดูแลระบบจะต้องกำหนดสิทธิการใช้ในโปรแกรมประเภท Utilities และ Tools
- ลบโปรแกรมที่ไม่มีความจำเป็นในการใช้ออกจาก โปรแกรมประเภท Utilities และ Tools

6.2.7. ร่องรอยเพื่อการตรวจสอบ

วัตถุประสงค์ : เพื่อสามารถสืบหาและป้องกันอย่างมีประสิทธิภาพใน กิจกรรมที่บุกรุก การเข้าถึงที่ไม่มีสิทธิ การใช้ทรัพยากรของบริษัทในทางผิด และการสืบสวนกิจกรรมหรือรูปแบบที่ไม่ปรกติ การฉ้อโกง จะต้องมีการบันทึกกิจกรรมของบุคคลหรือพนักงานเพื่อให้มั่นใจว่ามีบูรณภาพและไม่สามารถปฏิเสธการรับผิดได้

ความรับผิดชอบ

ผู้ใช้หรือผู้ดูแลทรัพย์สินสารสนเทศที่อยู่ในระบบ เครือข่าย หรือระเบียบของสื่อบันทึกข้อมูลที่ครอบคลุมถึงหลักฐานทางกายภาพ จะต้องรวมกับกลุ่มความปลอดภัยสารสนเทศกำหนดเงื่อนไขสารสนเทศที่จำเป็นเพื่อใช้ในการตรวจสอบ

สิ่งที่ต้องบันทึก

- บันทึก(log) จะต้องประกอบด้วยสารสนเทศที่มีเพียงพอเพื่อที่สืบหากิจกรรมเครือข่ายหรือระบบที่มิชอบ
- ทรัพยากรเทคโนโลยีสารสนเทศทั้งหมดที่มีการทำงาน จะต้องมีบันทึกความปลอดภัย(Security log) และบันทึกเพื่อการตรวจสอบ(Audit log)

การเก็บบันทึก

- บันทึกความปลอดภัย(Security log) จะต้องมีการเก็บเป็นระยะเวลา 3 ปี
- บันทึกเพื่อการตรวจสอบ(Audit log) จะต้องมีการเก็บเป็นระยะเวลา 3 ปี
- กิจกรรมการดูแลและบำรุงรักษา(Vendor Maintance Activity) จะต้องมีการเก็บเป็นระยะเวลาอย่างน้อย 2 ปี
- สารสนเทศที่รายงานถึงความผิดปรกติหรือปัญหาความปลอดภัยสารสนเทศ จะต้องมีการเก็บเป็นระยะเวลา 3 ปี

บันทึกความปลอดภัย

คอมพิวเตอร์ทุกเครื่องที่มีผู้ใช้งานหลายคน จะต้องมีการบันทึกกิจกรรมของผู้ใช้อย่างน้อยที่สุดดังนี้

- ความพยายามในการเข้าสู่ระบบ (สำเร็จหรือไม่สำเร็จ)
- การออกจากระบบ
- การใช้แฟ้มข้อมูลหรือทรัพยากรที่นอกเหนือจากสิทธิที่ได้รับอนุญาตให้ใช้ (ถ้าเป็นไปได้)
- การเปลี่ยนแปลงค่าต่างๆของระบบปฏิบัติการ
- การเปลี่ยนแปลงโปรแกรมของระบบปฏิบัติการ
- การเปลี่ยนแปลงความปลอดภัยของระบบทั้งหมด รวมถึงการเพิ่มผู้ใช้
- ข้อผิดพลาดที่เกิดขึ้นของคอมพิวเตอร์ โปรแกรม การสื่อสาร และการปฏิบัติงาน
- บันทึกจะต้องไม่แสดงรหัสผ่านของผู้ใช้ อย่างน้อยที่สุดจะต้องมีการเข้ารหัส(encrypted) รหัสผ่านของผู้ใช้

บันทึกเพื่อการตรวจสอบ

บันทึกเพื่อการตรวจสอบ(Audit log) อย่างน้อยที่สุดจะต้องสามารถระบุถึงสิ่งสำคัญของเหตุการณ์ (รหัสผู้ใช้ IP Address) ประเภทของเหตุการณ์ ความสำเร็จหรือล้มเหลวของเหตุการณ์ วันและเวลาของเหตุการณ์ที่เกิดขึ้น

การดูแลและบำรุงรักษาระบบ

การดูแลและบำรุงรักษาจะต้องมีการบันทึกอยู่ในบันทึกระบบ (system log) อย่างน้อยที่สุดต้องมีการบันทึก ชื่อของผู้ที่มาดูแลและบำรุงรักษา/ชื่อบริษัท และเหตุผลในการดูแลและบำรุงรักษา วันที่เริ่มและจบการดูแลและบำรุงรักษา และ เวลาที่มีการเชื่อมต่อ Modem(ถ้าได้ใช้)

ความถี่ในการสอบทานบันทึกความปลอดภัย(Security log) /บันทึกเพื่อการตรวจสอบ (Audit log) กลุ่มความปลอดภัยสารสนเทศจะต้องมีการสอบทานบันทึกความปลอดภัย (Security log) อย่างน้อยที่สุดทุกๆ 1 วัน และสอบทานบันทึกเพื่อการตรวจสอบ (Audit log) อย่างน้อยที่สุดทุก ๆ1 สัปดาห์ ผู้ดูแลทรัพย์สินสารสนเทศจะต้องมีการสอบทานบันทึกเพื่อการตรวจสอบ (Audit log)อย่างน้อยที่สุดทุก 1 สัปดาห์

6.2.8. การบริหารจัดการในเรื่องความปลอดภัยและระบบงาน

วัตถุประสงค์ : หน้าที่ความรับผิดชอบในการใช้งาน ดูแลและบำรุงรักษาของระบบความปลอดภัยจะต้องมีการมอบหมาย อนุมัติ และบันทึกลงในเอกสาร

การบริหารการจัดการข้าม Domain จะไม่อนุญาตให้ทำนอกเหนือจากได้รับอนุญาตจากผู้ดูแล Domain นั้น configuration plan ของระบบที่มีความสำคัญของบริษัทจะต้องมีการบันทึกและปรับปรุงข้อมูลให้ทันสมัย ในข้อมูลดังต่อไปนี้

- รายละเอียดรุ่นของ Software
- ข้อมูลรายละเอียดของผู้ขาย(vendor)
- รายละเอียดการตั้งค่าต่างๆของระบบ
- รายละเอียดการตั้งค่าความปลอดภัยของระบบ

กระบวนการการจัดการเอกสาร

กระบวนการจะต้องมีรายละเอียดของการปฏิบัติงานดังนี้

- ผู้ปฏิบัติงานที่มีสิทธิเท่านั้นจะได้รับอนุญาตให้ปฏิบัติงานกับอุปกรณ์คอมพิวเตอร์นั้น
- กระบวนการทำงานและสารสนเทศต้องมีการควบคุมโดยสิทธิและมีการเรียงลำดับความสำคัญ
- ตารางการทำงาน การมีผลต่อระบบอื่นที่เกี่ยวข้อง เวลาในการบำรุงรักษา
- วิธีการจัดการกับข้อผิดพลาด หรือเงื่อนไขที่ได้รับการยกเว้นอื่นในขณะปฏิบัติงาน จะต้องรวมวิธีการป้องกันไว้ด้วย

- สิ่งที่ได้จากกระบวนการทำงานที่เป็นความลับ จะต้องมีการแยกสถานที่ทำกระบวนการดังกล่าวเฉพาะ รวมถึงต้องมีวิธีการทำลายสิ่งที่ได้จากกระบวนการทำงานที่ไม่ประมวลผลไม่สำเร็จ
- กระบวนกู้กลับคืนและเริ่มทำงานของระบบที่ใช้ในกรณีที่เกิดความผิดพลาดของระบบ
- บันทึกกิจกรรมต่างของระบบ

กระบวนการจะต้องมีการสร้างกิจกรรมดูแลรักษาระบบ (system housekeeping activities) ซึ่งประกอบด้วยกระบวนการสารสนเทศและอุปกรณ์การติดต่อสื่อสาร ซึ่งรวมถึง

- กระบวนการเปิดและปิดคอมพิวเตอร์
- การสำรองข้อมูล
- การบำรุงรักษาระบบและอุปกรณ์
- การจัดการห้องคอมพิวเตอร์
- การจัดการจดหมายอิเลคทรอนิคส์

6.2.9. การจัดการทรัพยากร

วัตถุประสงค์ : หน้าที่งานเทคโนโลยีสารสนเทศในการบริหารและปฏิบัติงานทรัพยากรจะต้องสนับสนุนหน้าที่การสื่อสารสารสนเทศและการประมวลผลสารสนเทศประจำวันของบริษัท โดยมีความเพียงพอ ความวางใจได้ ความเชื่อถือได้ของทรัพยากร

- ผู้ดูแลทรัพยากรของบริษัทจะต้องมีกระบวนการที่จัดการ เฝ้าตรวจสอบ และมีมาตรการตรวจวัดในทรัพยากรของบริษัท
- บริการการสื่อสารสารสนเทศและการประมวลผลสารสนเทศต้องถูกวัดและเฝ้าตรวจสอบให้ได้ตรงตามมาตรฐานระดับการให้บริการการจัดการระบบ
- อุปกรณ์เครื่องมือจะต้องถูกประเมิน นำมาใช้ สนับสนุน และบำรุงรักษา ให้ตรงตามคำแนะนำผู้ขาย เพื่อให้แน่ใจว่าระบบจะมีความน่าเชื่อถือ ความเพียงพอในการใช้ และบูรณภาพ
- บุคคลที่มีสิทธิในซ่อมบำรุงรักษาเท่านั้นจะเป็นผู้ซ่อมแซมและบำรุงรักษาอุปกรณ์เครื่องมือ
- ต้องมีการบันทึกข้อสงสัยหรือความผิดพลาดที่เกิดขึ้นทั้งหมด และวิธีการป้องกันและการวิธีการแก้ไขที่ถูกต้อง

การจัดการความสามารถในการทำงาน

บริการหรือระบบของธุรกิจที่มีความสำคัญที่ประกอบด้วยข้อมูลที่มีความสำคัญจะต้องมีการวางแผนในการใช้เนื้อที่(capacity plan) มีการเฝ้าคอยตรวจสอบความต้องการการใช้เนื้อที่ในปัจจุบันว่าเพียงพอต่อการทำงานในอนาคตหรือไม่ และปรับวิเคราะห์ความต้องการใช้เนื้อที่ให้เหมาะสมเพื่อให้เกิดประสิทธิผลในการทำงาน โครงการที่จะเกิดขึ้นในธุรกิจใหม่ๆต้องมีการรายละเอียดของความ

ต้องการของระบบทั้งในปัจจุบัน และแนวโน้ม ในอนาคต ผู้ที่รับผิดชอบในสื่อบันทึกข้อมูลจะต้องมีหน้าที่ความรับผิดชอบในการลบหรือทำลายข้อมูลที่เหมาะสม

6.2.10. อุปกรณ์คอมพิวเตอร์ที่เคลื่อนย้ายได้

วัตถุประสงค์ : อุปกรณ์คอมพิวเตอร์ที่เคลื่อนย้ายได้จะต้องถูกควบคุมตามมาตรฐานและนโยบายของบริษัทในการป้องกันข้อมูลที่เป็นความลับและให้คงความเป็นบูรณภาพ

การแจกจ่ายอุปกรณ์คอมพิวเตอร์ที่เคลื่อนย้ายได้

- คำขอที่ต้องการใช้ Portable Pc เพื่อการใช้งาน จะต้องถูกตรวจสอบเสียก่อน
- สำหรับผู้ใช้คนใหม่จำเป็นจะต้องมีการเปลี่ยนรหัสเก่าผ่านเพื่อใช้งานใหม่
- ต้องมีการประเมินความเสี่ยงกับอุปกรณ์คอมพิวเตอร์ที่เคลื่อนย้ายได้ประเภทใหม่ๆ และต้องมีการประเมินความเสี่ยงใหม่อย่างน้อยทุกๆ 6 เดือน

ความปลอดภัยทางด้านกายภาพ

- พนักงานที่มีการนำทรัพย์สินของบริษัทที่มีความสำคัญ หรือเป็นความลับ เพื่อนำกลับบ้านไปทำงานต่อจะต้องมีการเก็บรักษาในตู้ที่มีการล็อคกุญแจ ในกรณีที่ไม่ได้ใช้งาน
- ห้องทำงานแต่ละห้องจะต้องถูกล็อคกรณีที่ไม่ได้ทำงานชั่วขณะ และในกรณีไม่ได้ทำงานเป็นระยะเวลายาว Laptop หรือ Notebook จะต้องมีการปิดเครื่องและป้องกันการลักลอบการใช้โดยใช้รหัสผ่านตอนเปิดเครื่อง
- อุปกรณ์คอมพิวเตอร์ที่เคลื่อนย้ายได้(portable,notebook,palmtop และ อุปกรณ์คอมพิวเตอร์อื่นที่เคลื่อนย้ายได้) จะต้องมีอุปกรณ์ล็อคติดไว้กับโต๊ะทำงานในกรณีที่ไม่ใช้
- เครื่องคอมพิวเตอร์ที่เคลื่อนย้ายได้(portable computer) ที่ให้บุคคลภายนอกใช้ จะต้องมีการมีอุปกรณ์ล็อค เพื่อป้องกันการขโมย

6.3 Network Security

6.3.1. การควบคุมการเข้าถึงเครือข่าย

วัตถุประสงค์ : การเข้าถึงการบริการเครือข่ายทั้งภายในและภายนอกจำเป็นต้องมีการควบคุมเพื่อให้แน่ใจว่าผู้ใช้บริการและการให้บริการของเครือข่ายจะมิได้ทำให้ระบบป้องกันเครือข่ายของบริษัทเสียหาย

กลุ่มรักษาความปลอดภัยของข้อมูลที่ได้รับอนุญาตเท่านั้นที่สามารถจะเข้าถึงเครือข่ายของบริษัทได้

การเข้าถึง/การป้องกันจะต้อง

- เป็นไปตาม "หลักการของการให้สิทธิ์ให้น้อยที่สุด" โดยปฏิเสธการเชื่อมต่อซึ่งไม่ได้รับการอนุญาตโดยชัดเจน
- ยินยอมให้เฉพาะการเชื่อมต่อภายในแก่ปลายทางที่ได้รับอนุมัติเท่านั้น
- ยินยอมให้เชื่อมต่อเฉพาะการบริการที่ได้รับอนุญาตเท่านั้น
- ซ่อนโครงสร้างข้อมูลเครือข่ายภายในและข้อมูลอื่น ๆ ยกเว้นที่จำเป็นสำหรับเกื้อการบริการโดยระบบป้องกัน
- เชื่อมต่อกับทุกกิจกรรมที่สำเร็จ
- จัดเตรียมระบบเตือนภัยสำหรับการทำลายความมั่นคงของระบบ
- การบริหารเป็นไปโดยระบบและผู้บริหารที่ได้รับอนุญาตตามกฎหมาย
- การบริหารเป็นไปโดยอิสระ จากการครอบครองของผู้จัดการระบบ
- จะต้องมีอักษรลับเพื่อป้องกันการติดต่อสื่อสารระหว่างผู้บริหารและระบบป้องกัน
- จะต้องผ่านการทดสอบการโจมตีของข้อมูลก่อนนำไปใช้งานจริงอย่างน้อยปีละ 1 ครั้ง และหากเป็นไปได้ควรมีการทดสอบแบบอัตโนมัติ
- ในกรณีเชื่อมต่อผ่าน โมเด็ม ถ้าเป็นระบบสำคัญจะต้องใช้วิธีการ call back กลับไปที่ผู้ใช้
- การเชื่อมต่อผ่าน Remote Access server ใช้ Radius Server เข้ามากำหนดสิทธิการใช้ โดยสิทธิจะกำหนดที่ Directory Service และที่ Access Server จะไม่มีการเก็บ User ID และ Password เอาไว้

6.3.2.ขอบเขตของเครือข่าย

วัตถุประสงค์ : ขอบเขตของเครือข่ายควรจะถูกกำหนดระดับการรักษาความปลอดภัยโดยอนุญาตให้เฉพาะผู้เกี่ยวข้องที่ได้รับอนุญาตและถูกกฎหมายเท่านั้น

การแบ่งแยกเครือข่าย

ขอบเขตความปลอดภัยของข้อมูลจะได้รับการดูแลโดยเครือข่ายข้อมูลของบริษัท กลุ่มเครือข่ายรักษาความปลอดภัยในระดับต่าง ๆ และ การเชื่อมต่อจากภายนอก เครือข่ายจะถูกแบ่งเป็น

หลาย ๆ กลุ่มระหว่างการให้บริการข้อมูล ผู้ใช้บริการ และ ระบบข้อมูล ถ้ามีความจำเป็นต้องเชื่อมต่อระหว่าง 2 เครือข่าย จะมีระดับการรักษาความปลอดภัยที่แตกต่างกัน เครือข่ายที่มีระบบการรักษาความปลอดภัยที่ต่ำกว่าจะต้องได้มาตรฐานของระดับที่สูงกว่า และการเชื่อมต่อจะต้องได้รับการอนุมัติโดยผู้บริหารหรือผู้ได้รับมอบหมายของระดับที่สูงกว่า

การเชื่อมต่อเครือข่าย

- การเชื่อมต่อ sessions หรือ วงจรไฟฟ้าจะต้องถูกอนุมัติให้ใช้งาน
- การเชื่อมต่อที่ไม่ได้ใช้งาน และบางส่วนของเครือข่าย จะต้องถูกตัดขาดจากเครือข่ายที่ใช้งานอยู่ เพื่อที่จะลดความเสี่ยงในการเข้าถึงเครือข่ายของบริษัท
- การวิเคราะห์ nodes วงจร ทางเดินการสื่อสาร และ protocols ต้องมีการพิจารณาระเบียบบันทึกและมีการทบทวน อย่างน้อย 1 ครั้ง/ปี

การบริการเครือข่าย

- คุณภาพการป้องกันของบริการเครือข่ายจะต้องกำหนดไว้เป็นลายลักษณ์อักษรและเก็บรักษาไว้ในที่ปลอดภัย
- การเข้าสู่บริการเครือข่ายจะต้องเป็นไปตามข้อกำหนดเท่านั้น สำหรับการเชื่อมต่อที่ไม่สามารถระบุสิทธิการใช้บริการ จะถูกปฏิเสธการใช้บริการโดยเด็ดขาด

เส้นทางการบริหาร ต้องมีการควบคุมเส้นทางเครือข่ายย่อย เพื่อที่จะแน่ใจว่า การเชื่อมต่อคอมพิวเตอร์และการส่งผ่านของข้อมูล จะไม่เปิดเผยความลับและความเชื่อถือของบริษัท

6.3.3.การบริหารเครือข่าย

วัตถุประสงค์ : เพื่อป้องกันเครือข่าย ช่องทางการสื่อสาร และการส่งข้อมูลในส่วนที่เป็นความลับ ให้สามารถสนับสนุนการการดำเนินงานของธุรกิจ ด้วยเครือข่ายที่มีประสิทธิภาพและนโยบายที่รัดกุม

- เครือข่ายและอุปกรณ์เครือข่ายต้องมีอำนาจในการบริหาร nominated เจ้าของและเครือข่าย (ผู้ปกป้อง) อำนาจในการบริหารเครือข่าย (ผู้ปกป้อง) จะต้องรับผิดชอบเครือข่ายและการจัดการ การทำงาน และ การควบคุมดูแลการสื่อสาร
- ความรับผิดชอบในการดำเนินงานของเครือข่ายจะต้องแยกจากระบบการทำงานอย่างเหมาะสม
- ผู้บริหารที่ได้รับมอบหมาย จะต้องรับผิดชอบในการทบทวนเครือข่ายและการสื่อสารและมีการติดตาม ตรวจสอบ กิจกรรมที่นอกเหนือจากปกติอย่างสม่ำเสมอ
- ศูนย์ควบคุมการทำงานของเครือข่ายจะตั้งอยู่ในสิ่งแวดล้อมที่ดูปลอดภัย ซึ่งการเข้าใช้งานจะต้องจำกัดเฉพาะผู้ที่ได้รับอำนาจเท่านั้น

- การเข้าใช้งานทั้งหมดในการบริหารจะปฏิบัติตามกฎของลำดับความสำคัญ และจะถูกปฏิเสธหากสิทธิการใช้งานไม่ตรงกับที่ระบุไว้
- การบริหารแบบ cross domain (ไขว้กัน) จะไม่ได้รับการอนุญาต ยกเว้น ผ่านการสื่อสารระหว่างระบบการบริหารและผู้มีอำนาจ
- การป้องกัน การตรวจหา และการวัดอุปสรรค จะถือว่าเป็นการใช้งานเป็นการป้องกันอย่างมี เช่น การป้องกันระบบเครือข่าย และการตรวจหาการใช้ข้อมูลที่ผิด
- จะต้องทบทวนเครือข่ายทั้งหมดอย่างน้อยทุก 1 ครั้ง/สัปดาห์ โดยฝ่ายเครือข่าย (Network Dept.)

การอนุมัติการเชื่อมต่อ

- การเชื่อมต่อเครือข่าย หรือ โซนเครือข่ายที่มีระดับของการป้องกันแตกต่างกันจะต้องได้รับอนุมัติ และทำเป็นเอกสาร โดยฝ่ายบริหารและคณะทำงานรักษาความปลอดภัยข้อมูลสารสนเทศ
- ความต้องการการเชื่อมต่อทั้งหมดจะต้องสอดคล้องกับวัตถุประสงค์และระยะเวลาของบริษัท
- จะต้องกำหนดกระบวนการสร้างและยกเลิกการเชื่อมต่อ
- การทบทวนการรักษาความปลอดภัยจะต้องนำไปปฏิบัติเพื่อที่จะเข้าไปเข้าสู่มาตรการรักษาความปลอดภัยสำหรับการเชื่อมต่อใหม่ๆ
- การเชื่อมต่อที่ได้รับการอนุมัติจะต้องทบทวนอย่างน้อย 1 ครั้ง/6 เดือน

6.3.4. **Network Encryption**

วัตถุประสงค์ : เพื่อให้มั่นใจว่า ข้อมูล ของบริษัท จะได้รับการปกป้องตามความคาดหมาย สำหรับเครือข่ายที่อยู่ในระดับที่มีความเสี่ยงต่อความความไว้วางใจ จะต้องได้รับการเข้ารหัส

- การควบคุม cryptographic ที่เข้มงวดจะนำมาใช้เพื่อรับรองและปกป้องความลับของ เครือข่าย
- Cryptographic Algorithms ที่ได้รับการอนุมัติ และจะเป็นกฎและมาตรฐานในการใช้งาน
- การใช้ cryptographic key และการบริการจะเป็นไปตามกฎและมาตรฐานที่ระบุไว้ใน Cryptographic Key Management.

เครือข่ายส่วนตัว

- ปลายทางของ VPN ทั้งหมดจะมีเครื่องควบคุมการเข้าใช้งาน และจะถูกป้องกันจากการใช้งานที่ไม่ได้รับอนุญาตให้ใช้ช่องทาง VPN
- จะต้องมีการเปลี่ยนรหัสผ่าน สำหรับ Hardware based ทุกครั้งเพื่อสนับสนุนการใช้ของ VPN

- การใช้งานและกลไกของ cryptographic บน VPN จะต้องปฏิบัติตามกฎและมาตรฐานที่ระบุไว้ใน Security Mechanisms.
- VPN ทั้งหมดจะถูกเชื่อมต่อผ่าน อุปกรณ์เชื่อมต่อเครือข่ายที่ปลอดภัย (SNCF)
- VPN จะต้องมีการตรวจสอบเพื่อที่จะบันทึกการเข้าใช้งานทั้งหมดและการใช้งานของช่องทาง VPN

การเชื่อมต่อจากภายนอก

- ฝ่ายสารสนเทศเครือข่ายจะต้องดูแล ระบบเครือข่ายภายนอกที่เชื่อมต่อทั้งหมด
- การเชื่อมต่อ Internet หรือเครือข่ายภายนอกจะต้องได้รับการตรวจสอบยืนยันแล้วเท่านั้น
- สถาปัตยกรรมการเชื่อมต่อจะต้อง
- ทำตามมาตรฐานและนโยบายความปลอดภัยของ องค์กร
- จะต้องสร้างความแตกต่างระหว่าง Physical และ Logical ของเครือข่าย
- การเชื่อมต่อสู่เครือข่ายภายนอกจะต้องได้รับการอนุมัติจากคณะทำงานรักษาความปลอดภัยข้อมูลสารสนเทศ
- ทำตามนโยบายและมาตรฐานใน firewall / gateway
- การประเมินผลการจัดลำดับความปลอดภัยเป็นไปตามสภาพแวดล้อมที่เกิดขึ้นจริง
- ทบทวนกฎระเบียบอย่างน้อยทุก 6 เดือน

การเข้าถึงจากระยะไกล

- การเชื่อมต่อระยะไกลทุกครั้งต้องปฏิบัติตามนโยบายและมาตรฐานความปลอดภัยในการจัดการเครือข่าย
- การเชื่อมต่อทางโทรศัพท์ เพื่อ login เข้าสู่ระบบจะถูกกำหนดสิทธิการใช้งาน
- การเชื่อมต่อระยะไกลทุกครั้งต้องผ่านอุปกรณ์เครือข่ายที่ได้รับอนุญาต
- การเข้าถึงจากระยะไกลต้องถูกพิสูจน์อย่างเพียงพอ สำหรับระบบที่มีความเสี่ยงสูง หรือระบบที่จำเป็นต้องนำการเข้ารหัสที่แข็งแรงมาใช้
- การสื่อสารเครือข่ายจะต้องถูกเข้ารหัสสำหรับการเข้าถึงข้อมูล จากภายนอกระบบเครือข่าย ตามที่กำหนดไว้ในนโยบาย และคู่มือ
- ควบคุมสำหรับบัญชีพิเศษจะต้องทำตามนโยบายและมาตรฐานความปลอดภัยในระบบการบริหารบัญชีผู้ใช้ การควบคุมการบริหารสิทธิพิเศษ
- การเข้าถึงจากระยะไกลจะต้องมีการตรวจสอบ และทบทวนอย่างน้อยทุก ๆ 1 เดือน

6.4 Communication Security

6.4.1. ความปลอดภัยด้าน E-mail

- พนักงานที่มีสิทธิในระบบการสื่อสารอิเลคทรอนิคส์จะต้องได้รับอนุญาตซึ่งมีงานที่เกี่ยวข้องหรือใช้
- ระบบ e-mail จะใช้รหัสประจำตัวพนักงานและรหัสผ่านที่แตกต่างกัน
- การแสดงอย่างผิด ๆ ความไม่ชัดเจน การปิดบัง หรือการแทนที่ แทนตัวผู้ใช้ ที่ไม่ได้รับอนุญาต ชื่อผู้ใช้ ที่อยู่ จะต้องสะท้อนหรือแสดงที่มาที่ชัดเจน
- ข้อมูลที่จัดแบ่งตามสิทธิ ต้องการที่จะทราบ และไม่ถูกส่งด้วย e-mail โดยปราศจากการควบคุมตามนโยบายและวิธีความปลอดภัย

สิทธิผู้ใช้

- ไม่ให้เผยแพร่สื่อต่างๆ ทาง Internet ที่ไม่ได้รับอนุญาตหรือรับรองโดยฝ่ายประชาสัมพันธ์
- ผู้ใช้ไม่ได้รับอนุญาตให้ส่งจดหมายลูกโซ่ หรือจดหมายรบกวนในระบบ e-mail ขององค์กร
- พนักงาน องค์กร ทุกคนจะไม่ใช้ถ้อยคำหยาบคาย ก่อกวน รบกวน ในการพูดคุยโต้ตอบ e-mail

การดูแลรักษา E-mail

- e-mail ทุกฉบับจะต้องถูกสำเนาไว้ที่ Archival Records Department
- ข้อความต้องไม่ยาวเกินไปที่จะสื่อสาร และจะต้องขจัดโดยผู้ใช้ไม่ให้กระทบต่อพื้นที่จัดเก็บ

6.4.2. Electronic Mail Gateway

วัตถุประสงค์ : e-mail จะต้องได้รับการจัดการที่ปลอดภัยในการรับส่งจดหมาย E-mail gateway จะต้องถูกกำหนดเพื่อป้องกันการหาเส้นท้อง หรือสะพานระหว่างเครือข่าย ยกเว้นผ่าน mail transfer protocol E-mail gateway จะต้อง

- รับประกันทุกข้อความไม่มีไวรัสคอมพิวเตอร์
- รับประกันข้อ E-mail ที่มี Attached file
- รับประกันขนาดของไฟล์กรณีที่ใหญ่กว่าที่กำหนด
- ถูกกำหนดให้ป้องกันไม่ให้ข้อมูลทางเครือข่ายของ องค์กร เปิดเผย

- ประมวลเฉพาะที่อยู่ภายใน องค์กร
- ต่อท้ายจดหมายทุกฉบับว่าไม่รับผิดชอบทางด้านกฎหมาย

การติดตามตรวจสอบ E-mail

- พนักงานไม่อาจเข้าไปขัดขวาง หรือยุ่งเกี่ยวช่วยเหลือการเปิดเผยหรือขัดขวางการรับส่ง E-mail ยกเว้นผู้ที่ได้รับสิทธิ
- ผู้ดูแล และกลุ่มความปลอดภัยสารสนเทศ (Custodian and Information security group) เป็นผู้ให้อำนาจในการติดตามตรวจสอบ E-mail
- บุคลากรสนับสนุนด้านเทคนิคจะต้อง
    - ทวนสอบเนื้อหา (Content) E-mail ระหว่างการแก้ปัญหา
    - การทวนสอบเนื้อหาต้องไม่ทำด้วยความอยากรู้อยากเห็น หรือเป็นคำสั่งของบุคคลใด ๆ ที่ไม่ได้ดำเนินการอย่างถูกต้องตามระเบียบ

6.4.3. ความปลอดภัยของการประชุมภาพและเสียง

วัตถุประสงค์ : อุปกรณ์ในการประชุมภาพควรพิจารณาในส่วนการดักฟัง การขัดขวาง อุปกรณ์ในการประชุมต้องไม่อนุญาตให้ตอบรับอัตโนมัติ และป้องกันผู้ไม่มีสิทธิ หรือแปลกปลอมในการบันทึกหรือฟัง หรือร่วมการประชุม

6.5. Application and System Development Security

6.5.1. การวิเคราะห์ความเสี่ยง และความต้องการความปลอดภัย

วัตถุประสงค์ : ความต้องการความปลอดภัยอย่างเป็นทางการ และการควบคุมควรจะถูกนำไปใส่ไว้ทุก ขั้นตอนการพัฒนาที่มีวิกฤติ หรือให้บริการ

- การวิเคราะห์ความเสี่ยง และความต้องการความปลอดภัยควรระบุลงใน Requirement phase Justified agreed และเอกสารในการพัฒนาระบบต่าง ๆ หรือเป็นพื้นฐานในการออกแบบระบบ
- ความปลอดภัย และการควบคุมควรพัฒนาด้วยกระบวนการทางธุรกิจ และตามหน่วยงานควบคุมความปลอดภัยสารสนเทศขององค์กร
- การปรับปรุง พัฒนาเพิ่มเติมระบบที่มีอยู่จะต้องสนับสนุนสิ่งจำเป็นทางธุรกิจ และสิ่งจำเป็นต้องควบคุม
- ระบบหรือโปรแกรมที่พัฒนานอกองค์กรควรกำหนดให้พัฒนาตาม Business Process ความปลอดภัย และการควบคุม
- ความปลอดภัยและการควบคุมควรประกอบด้วยอย่างน้อยดังนี้
    - คำนึงถึงความเสียหายต่อธุรกิจ ต่อกรณีระบบความปลอดภัยเสียหายหรือล้มเหลว
    - การพิสูจน์สิทธิ และควบคุมการเข้าถึง
    - บูรณภาพ และความลับของข้อมูล
    - ความจำเป็นในการตรวจสอบ
    - ตรวจสอบการบุกรุก และรายงานที่ยกเว้น
    - การตรวจสอบความถูกต้องของข้อมูล
    - ไม่ใช้การควบคุมอัตโนมัติในระบบ แต่ต้องการให้สนับสนุนการควบคุมด้วยมือ
    - ปฏิบัติตามนโยบาย และมาตรฐานความปลอดภัยของ องค์กร
    - ไม่ละเมิดกฎหมาย กฎระเบียบขององค์กร
    - การกู้คืนเมื่อเกิดความเสียหาย
    - การถอยกลับ

6.5.2. การใช้ข้อมูลเพื่อการทดสอบ

วัตถุประสงค์ : เพื่อความแน่นอนในการใช้ข้อมูลที่เป็นความลับในการทดสอบ ซึ่งต้องควบคุมและสังเกต ข้อมูลที่ใช้ทดสอบระบบต้องได้รับการอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของธุรกิจ และหน่วยงานควบคุมความปลอดภัยสารสนเทศขององค์กร ควรจัดทำสำเนาไว้

- ข้อมูลผลผลิตสำหรับการทดสอบต้อง
    - ข้อมูลที่ได้จัดชั้นข้อมูลแล้วว่าเป็นข้อมูลเฉพาะและเผยแพร่ภายในบริษัทเท่านั้น
    - ไม่รวมข้อมูลเป็นเป็นรายละเอียด หรือวิกฤติ หรือเป็นส่วนตัว
    - ควบคุมความปลอดภัยเท่าเทียมหรือดีกว่าในระบบการผลิตข้อมูล
- ข้อกำหนดในการทดสอบข้อมูลที่หน่วยงานภายนอกดังนี้
    - ต้องไม่รวมข้อมูลปัจจุบันถ้าเจ้าของธุรกิจไม่ให้ความยินยอม
    - ต้องไม่ขัดแย้งหรือละเมิดกฎหมาย และกฎระเบียบขององค์กร

6.5.3. การแยกข้อมูล และสิ่งแวดล้อมในการพัฒนา

วัตถุประสงค์ : เพื่อลดความเสี่ยงอันอาจเกิดจากเหตุบังเอิญ หรือการใช้งานอย่างประมาทเลินเล่อ รวมทั้งการจัดแบ่งขั้นตอนการพัฒนาและขั้นตอนการปฏิบัติงานซึ่งมีผลกระทบต่อการปฏิบัติงานที่เกี่ยวข้อง ในการทดสอบ และการพัฒนาควรปฏิบัติตามดังต่อไปนี้

- ในการพัฒนา และการทดสอบจะต้องไม่ต่อเชื่อมคอมพิวเตอร์ออกไปภายนอก หรืออยู่ใน Domain ที่ไม่มีการควบคุม
- การรวบรวม การแก้ไข ระบบต่าง ๆ ต้องไม่ถูกเข้าถึงด้วยระบบปฏิบัติการ
- ผู้ใช้ต้องใช้รหัสผ่านที่แตกต่างกันในการเข้าระบบ และเมนูควรแสดงข้อความที่กำหนดความเหมาะสมแล้ว
- ทีมงานพัฒนา และทดสอบไม่ควรเข้าถึงระบบปฏิบัติการ และสารสนเทศของระบบ
- ปราศจากการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานควบคุมความปลอด และเจ้าของข้อมูล
- การควบคุมควรเปลี่ยนรหัสผ่าน หลังจากที่ใช้ ยกเว้นกรณีการบำรุงรักษาเร่งด่วน ซึ่งเปลี่ยนการควบคุม และกระบวนการสนับสนุน

6.5.4. การทดสอบความปลอดภัย

วัตถุประสงค์ : ระบบธุรกิจหรือบริหารสามารถเข้าถึงด้วยบุคคลภายนอก หรือลูกค้า จึงต้องมีการทดสอบระบบความปลอดภัยคอมพิวเตอร์

- การประเมินความปลอดภัยระหว่างเครื่องปลายทางทั้งสอง ควรดำเนินการให้สมบูรณ์ต่อจากนั้นให้ทำอย่างน้อยทุก 1 ปี
- การประเมินความปลอดภัยควรดำเนินการด้วยหน่วยงานที่ไม่ใช่ผู้พัฒนาระบบที่ทำการทดสอบ
- การทดสอบความปลอดภัยควรได้รับการอนุญาตจากเจ้าของธุรกิจ โดยทำตามขั้นตอน

- หน่วยงานภายนอกที่ได้รับการรับรองจากหน่วยงานความปลอดภัยสารสนเทศขององค์กร Information Security Group จึงเป็นผู้ทดสอบได้
- แผนการทดสอบความปลอดภัยอย่างเป็นทางการต้องนำเสนอต่อเจ้าของธุรกิจและที่ประชุมหน่วยงานความปลอดภัยขององค์กร
- การตรวจสอบขั้นยอมรับ ต้องประกอบด้วยการทดสอบความปลอดภัยที่แน่ใจว่าเป็นไปตามความต้องการความปลอดภัย และเอกสารการทดสอบอย่างเป็นทางการอย่างถูกต้อง

6.5.5. การควบคุมการพัฒนาซอฟต์แวร์

วัตถุประสงค์ : การพัฒนาซอฟต์แวร์ จะต้องอยู่ภายใต้การควบคุมดูแล จากฝ่ายสารสนเทศของบริษัท และจะต้องได้รับความยอมรับจากผู้มีอำนาจที่ได้รับการแต่งตั้ง

- การใช้ทรัพยากรในการพัฒนาระบบควรถูกจำกัดให้ได้เฉพาะผู้พัฒนาซึ่งได้รับสิทธิด้วยผู้ดูแล ซึ่งทำตามกระบวนการของเจ้าของธุรกิจ
- การเปลี่ยนแปลงทุกอย่างที่เกี่ยวข้องกับทรัพยากรในการพัฒนาโปรแกรมต้องได้รับสิทธิและบันทึกไว้
- Software ที่ล้าสมัยมากกว่า 6 เดือนต้องมีการจัดทำใหม่
- ทรัพยากรที่พัฒนาโปรแกรมซึ่งประกอบด้วยรายการ โค้ดที่พัฒนาควรแบ่งอย่างน้อยตามกลุ่มเจ้าของ (แต่ละฝ่าย)

6.5.6. การจัดการการเปลี่ยนแปลง

วัตถุประสงค์ : การเปลี่ยนแปลงกระบวนการทำงาน หรือระบบควรควบคุมทั้งหมดด้วยกระบวนการบริหารจัดการที่เป็นทางการ กระบวนการบริหารการเปลี่ยนแปลงต้องประกอบด้วยอย่างน้อย

- เอกสารกระบวนการในการเปลี่ยนแปลงที่ออกให้ด้วยเจ้าของธุรกิจ เพื่อควบคุมให้การเปลี่ยนแปลงเป็นไปตามกำหนด
- การประเมินความเสี่ยงและวิเคราะห์ผลกระทบ ความต้องการทางธุรกิจ ความต้องการด้านเทคนิค ตลอดจนการติดตั้ง ต้องนำมาใช้ทุกครั้งในการเปลี่ยนแปลง
- ขอบเขตของกระบวนการบริหารการเปลี่ยนแปลง
- ให้เหตุผลเพื่อการจัดการเปลี่ยนแปลงและประสานงาน
- ปฏิบัติตามกระบวนการเปลี่ยนแปลงของหน่วยงาน
- มีวิธีการเพื่อการเปลี่ยนแปลง

ทุกการเปลี่ยนแปลงการจัดการต้องมีศูนย์กลางซึ่งเป็นผู้รู้รายละเอียด ซึ่งควรรวบรวมเหตุผลในการเปลี่ยนแปลงเพื่อการเปลี่ยนแปลง และการประสานงานการเปลี่ยนแปลง เอกสารประกอบการเปลี่ยนแปลงสำหรับ โค้ด ข้อมูล Hardware Software เครือข่าย องค์ประกอบระบบ ต้องมีอย่างน้อยดังต่อไปนี้

- จัดหมวดหมู่ของการเปลี่ยนแปลง
- กำหนดบุคลากร
- บันทึกการเปลี่ยน
- การติดตามการเปลี่ยนแปลงระบบการผลิต
- การยกเว้นของระบบทั่วไป
- ควบคุมการเปลี่ยนแปลง และการเปลี่ยนกลับ
- การล้มเหลว และการกู้กลับจากการเปลี่ยนแปลงที่ไม่ประสบความสำเร็จ
- ประสานรายละเอียดการเปลี่ยนแปลงต่อผู้ที่รับผิดชอบทุกคน

สอบทวนการเปลี่ยนแปลง

หลังการเปลี่ยนแปลงแล้วทบสอบ และวิเคราะห์การเปลี่ยนแปลงจัดทำเป็นเอกสารให้สมบูรณ์ ภายใน 30 วันนับจากการเปลี่ยนแปลง การเปลี่ยนแปลงที่เกี่ยวข้องกับระบบ Application ต้องแน่ใจว่าเข้ากันได้กับการควบคุมความปลอดภัย ก่อนการเปลี่ยนแปลง

เจ้าของกระบวนการหรือผู้ปฏิบัติงานที่เกี่ยวข้องกับการเปลี่ยนแปลง จะต้องมีความเข้าใจเป็นอย่างดีในการเปลี่ยนแปลงทั้งส่วนการทำงาน การจัดการ ซึ่งผู้ดูแลการเปลี่ยนแปลงจะต้องให้ข้อมูลทุกอย่างที่จำเป็นกับการเปลี่ยนแปลงนั้นเพื่อทบทวนหรือเข้าใจ

6.5.7. การทดสอบในขั้นการตรวจรับ

วัตถุประสงค์ : การทดสอบในขั้นการตรวจรับเพื่อแน่ใจว่าปฏิบัติอย่างถูกต้องทั้งระบบใหม่หรือระบบที่เปลี่ยนแปลง ระบบใหม่หรือที่เปลี่ยนแปลงควรได้รับการทดสอบระบบ Regression Testing การทดสอบขั้นตรวจรับ และด้วยการทบทวนผลทดสอบ ด้วยส่วนงานที่เกี่ยวข้องซึ่งจะติดตั้งเป็นอันดับต่อไป การทดสอบขั้นการตรวจรับต้องดำเนินการด้วยทีมทดสอบที่ไม่ใช่ทีมผู้พัฒนา ผู้ใช้ในขั้นทดสอบตรวจรับควรจะมีเอกสารประกอบและปฏิบัติตามในการควบคุมสิ่งแวดล้อมในการทดสอบแต่ไม่ถึงขั้นจำกัด

หน้าที่รับผิดชอบ

- แผนการทดสอบ
- หลักการทดสอบ และวัตถุประสงค์การทดสอบ

- สิ่งที่เกิดขึ้นที่จะต้องพิจารณาซึ่งมีผลต่อระบบใหม่บนระบบความปลอดภัยขององค์กร
- การควบคุมความปลอดภัย
- ประสิทธิภาพของคอมพิวเตอร์ที่ต้องการ
- ตรวจสอบความถูกต้องข้อมูล และข้อบกพร่องต่าง ๆ
- จัดเตรียมและทดสอบตามประบวนการและมาตรฐานที่กำหนด
- เพิ่มเติมกรณีมีการแก้ไขข้อบกพร้องที่เกี่ยวข้อง
- กระบวนการที่มีประสิทธิภาพ
- จัดเตรียมความต่อเนื่องการดำเนินธุรกิจ
- กู้กลับหรือเริ่มใหม่ และแผนงานล่วงหน้า
- ผลการทดสอบ

6.6 Workstation Security

6.6.1. Workstation Hardware

ต้องกำหนดมอบหมายความรับผิดชอบต่อความปลอดภัยทางกายภาพของอุปกรณ์ในระบบเครือข่าย และสิ่งบรรจุข้อมูล

- คอมพิวเตอร์และอุปกรณ์ต่าง ๆ ของเครือข่ายต้องอยู่ในสิ่งปลูกสร้างที่มีความปลอดภัย
- ถ้าคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ไม่อยู่ในพื้นที่ควบคุมอาจจะโดนขโมย หรือสูญหายได้
- สื่อที่ใช้บรรจุข้อมูลต้องถูกระวังป้องกันจากสนามแม่เหล็ก หรือความเสี่ยงอื่น ๆ
- คอมพิวเตอร์อุปกรณ์ต่าง ๆ ขององค์กร ต้องไม่ดำเนินการปรับปรุง เพิ่มประสิทธิภาพโดยไม่ได้รับอนุญาตจากเจ้าของระบบ

6.6.2. Workstation Software

- ไม่อนุญาตให้แบ่งปันทรัพยากรในเครือข่าย
- ทรัพยากรคอมพิวเตอร์ทุกรายการต้องไม่ละเมิดลิขสิทธิ์ ในการจัดซื้อ
- ผู้ใช้คอมพิวเตอร์ไม่มีสิทธิในการเปลี่ยนแปลง หรือติดตั้ง Software โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

6.6.3. Un-attend Workstation

วัตถุประสงค์ : การควบคุมจะต้องสามารถยับยั้ง ป้องกัน ให้เกิดความปลอดภัยและบูรณภาพของระบบอย่างสมบูรณ์ พนักงานทุกคนจะต้องใส่ใจในเอกสารที่รับผิดชอบ ไม่ว่าจะเป็นการจัดเก็บด้วยสื่อใด ๆ ก็ตาม หรือการปิดหน้าจอทุกครั้งที่ไม่มีการใช้งาน คอมพิวเตอร์ส่วนบุคคล และ Terminal ไม่ควรทิ้งการบันทึก เมื่อไม่มีผู้ดูแลหรือผู้ใช้ และควรป้องกันด้วยการ Key Lock เมื่อเครื่องตั้งอยู่ในบริเวณที่สาธารณาและรหัสผ่านเมื่อไม่มีผู้ใช้

ในช่วงที่ไม่ใช้คอมพิวเตอร์ช่วงสั้น ๆ ระหว่างชั่วโมงทำงาน ปิดล็อคห้องก็เพียงพอ กรณีนอกชั่วโมงทำงานต้องเก็บเอกสาร สื่อเก็บข้อมูลต่าง ๆ ให้เป็นระเบียบใส่ตู้ล็อกกุญแจให้เรียบร้อย จึงจะออกจากที่ทำงาน คอมพิวเตอร์ และเครื่องพิมพ์ไม่ควรที่จะเลิกบันทึกการใช้งาน เมื่อไม่มีผู้ใช้งานหรือดูแล ควรป้องกันด้วยการล็อกกุญแจ และรหัสผ่านเมื่อตั้งอยู่ในพื้นที่

6.6.4. การควบคุมไวรัสคอมพิวเตอร์

วัตถุประสงค์ : โปรแกรมควบคุมไวรัสติดตั้งเพื่อแน่ใจว่าเพียงพอที่จะจำกัดโอกาสที่ข้อมูลเสียหาย เพราะการแพร่พันธุ์ของไวรัส หรือการทำงานของโปรแกรมที่ไม่ได้รับอนุญาตให้ติดตั้ง

ภาระหน้าที่

- พนักงานทุกคนในองค์มีหน้าที่ต้องรายงานข้อมูลการฝ่าฝืนหรือละเมิดความปลอดภัย และปัญหาต่อหน่วยงานควบคุมความปลอดภัยคอมพิวเตอร์อย่างทันเวลา เพื่อแก้ไข
- รายทันทีเมื่อคอมพิวเตอร์แจ้งเตือนว่าติดไวรัส ต่อหน่วยงานควบคุมความปลอดภัย
- ถ้ารายงานเกี่ยวกับการระบาดของไวรัสยังไม่ออก และพนักงานทราบจากการค้นคว้าให้พนักงานรับทราบเป็นหน้าต้องแจ้งให้หน่วยงานทราบด้วย
- ผู้จัดการควรมีหน้าที่รับผิดชอบให้ธุรกิจสามารถดำเนินการไปได้แม้จะถูกไวรัสโจมตี และกู้ข้อมูลที่ถูกทำลายคืนด้วย ซึ่งประกอบด้วยข้อมูลที่จำเป็น และการสำรองโปรแกรมไว้
- ฝ่ายคอมพิวเตอร์มีหน้าที่รับผิดชอบดังนี้
    - เตือนทุกระบบในองค์กรอย่างทันเวลา และรวดเร็ว
    - ปรับปรุงฐานข้อมูลไวรัส (Virus Signature) ให้ทันสมัยอยู่เสมอ

Virus Control Mechanism

- นำการควบคุมป้องกัน การสืบค้น ต่อโปรแกรมที่ประสงค์ร้ายมาใช้ และนำกระบวนการเตือนหรือรับรู้ที่เหมาะสมมาใช้
- การป้องกันโปรแกรมประสงค์ร้ายควรปฏิบัติตามมาตรการความปลอดภัย การเข้าถึงระบบที่เหมาะสม
- คอมพิวเตอร์ทุกเครื่องควรติดตั้งโปรแกรมค้นหาไวรัส และแก้เมื่อติดไวรัสที่ถูกลิขสิทธิ์และปรับปรุงฐานข้อมูลไวรัสทุก ๆ 2 สัปดาห์
- การเชื่อมต่อจากภายนอกเข้าสู่เครือข่ายทุกจุดควรติดตั้งโปรแกรมค้นหาไวรัสที่ถูกลิขสิทธิ์
- ไฟล์หรือแฟ้มข้อมูลที่นำมาใช้ในระบบงานควรถูกตรวจสอบไวรัสก่อนนำมาใช้ในระบบ
- ควรทบทวนข้อมูลเกี่ยวกับไวรัส และจัดเก็บไว้ข้อมูลประกอบในส่วนสนับสนุนที่อาจทำให้การดำเนินงานธุรกิจมีความเสี่ยงและอาจเกิดวิกฤติได้

การควบคุมไวรัส

ส่วนบริหารจัดควรปรับปรุงเหตุการณ์เกี่ยวกับไวรัสให้ทันสมัยเสมอ เพื่อสามารถแก้ปัญหาได้อย่างรวดเร็วมีประสิทธิภาพ และเป็นขั้นตอน การควบคุมไวรัสควรปฏิบัติตามกำหนดการใน การจัดการควบคุมเกี่ยวกับไวรัส

การสำรองข้อมูล และไฟล์ต่าง ๆ

ข้อมูลที่จัดเก็บอยู่ในคอมพิวเตอร์ทุกเครื่องจะถูกสำรองไว้ที่ระบบควบคุมที่ได้รับสิทธิ

- เป็นความรับผิดชอบของเจ้าของข้อมูลที่ปฏิบัติงานให้สำเร็จ
- เจ้าของข้อมูลควรตรวจสอบว่าข้อมูลที่สำรอง มีความถูกต้องและไม่เปลี่ยนแปลง

บทที่ 7
การจัดทำแผนการเพื่อการดำเนินธุรกิจอย่างต่อเนื่อง และแผนฉุกเฉินการกู้คืน

แผนการเพื่อการดำเนินธุรกิจอย่างต่อเนื่อง(**Business Continuity Planning: BCP**)

7.1. การจัดการ หน้าที่และความรับผิดชอบ

วัตถุประสงค์ : การติดตามงาน ของแผนก IT ของบริษัท เป็นส่วนหนึ่งของหน้าที่ความรับผิดชอบที่ระบุอยู่ในแผนงานธุรกิจ

แผนกวางแผนธุรกิจต่อเนื่อง

เพื่อศึกษาความเป็นไปได้ของกระบวนการทางธุรกิจ โดยแผนกจะประกอบไปด้วย เจ้าของบริษัทซึ่งเป็นผู้เก็บข้อมูลที่มีความสำคัญไว้ แผนกตรวจสอบภายใน แผนกธุรการและแผนกรักษาความปลอดระบบสารสนเทศ

แผนกวางแผนธุรกิจต่อเนื่องจะมีหน้าทีความรับผิดชอบดังต่อไปนี้

- รายงานสถานการณ์ปัจจุบัน ความพร้อม ต่อ ทีมผู้บริหารและฝ่ายจัดการอาวุโสเพื่อพิจารณา
- พัฒนากระบวนการ และขอบเขตของงานเพื่อเป็นแนวทางให้กับทุกหน่วยงานในบริษัทในการพัฒนาแผนการดำเนินการต่อเนื่องของธุรกิจ ที่สามารถสนับสนุนบริการความต้องการต่างๆ ได้
- พิจารณาแผนการดำเนินการทางธุรกิจที่จะเกิดขึ้นในอนาคต
- ดูแลบุคลากรในแผนกการวางแผนธุรกิจ ให้คำปรึกษาและกำหนดขอบเขตการปฏิบัติงาน รวมถึงแผนการการจัดเก็บรักษาข้อมูลต่างๆ
- จัดตั้งทีมเฉพาะกิจสำหรับจัดการปัญหาต่างๆที่อาจจะเกิดขึ้นในการขบวนการกู้คืนข้อมูลทางธุรกิจ
- ดูแลรักษาข้อมูลส่วนกลางที่เกี่ยวข้องกับแผนกวางแผนธุรกิจทั้งหมด
- ประสานงานและร่วมกันตัดสินใจกับทีมอื่นๆที่เกี่ยวข้องในการเก็บและกู้คืน Key
- เป็นผู้ตัดสินใจในส่วนที่เกี่ยวข้องกับแผนกวางแผนธุรกิจต่อเนื่อง
- รวบรวมและเตรียมการทางด้านการเงินสำหรับการกู้คืนข้อมูล
- เป็นผู้ช่วยเหลือฝ่ายกฎหมายในการดูแลเรื่องความเสียหายที่อาจจะเกิดขึ้น
- เป็นผู้ช่วยเหลือฝ่ายประชาสัมพันธ์ เกี่ยวกับงานสื่อสาธารณะอื่นๆ

ผู้มีส่วนเกี่ยวข้องในแผนกวางแผนธุรกิจต่อเนื่อง จะต้องมีผู้ร่วมงานอย่างน้อย 1 คนภายในบริษัทที่มาความเข้าใจอย่างลึกซึ้งเกี่ยวกับโครงสร้างและเนื้อหาของแผนการขั้นต่อไปในโครงสร้างธุรกิจ

หน้าที่สำหรับผู้มีส่วนเกี่ยวข้องในแผนการดำเนินการ

- จัดหาที่ผู้เชียวชาญ ที่ปรึกษาเพื่อสนับสนุนการทำงานร่วมกับ BCPO ในทุกหน้าที่
- ให้คำปรึกษาแก่ผู้บริหารและผู้ที่มีส่วนเกี่ยวข้องเกี่ยวกับแผนการดูแลรักษา สนับสนุนแผนการขั้นต่อไปของธุรกิจ
- ทำสำเนาให้กับผู้ที่มีส่วนรับผิดชอบใน key เพื่อความสะดวกในการดำเนินการ

7.2. การวิเคราะห์ผลกระทบต่อธุรกิจ

วัตถุประสงค์ : การวิเคราะห์ผลกระทบต่อธุรกิจเป็นการวิเคราะห์ในเชิงลึกโดยระบุถึงถึงส่วนงานที่อาจจะเกิดปัญหาขึ้น ภายในบริษัท และสามารถตัดสินใจได้ว่าจะมีผลกระทบ
เอกสารที่เกี่ยวข้องกับการวิเคราะห์ผลกระทบธุรกิจ ผลกระทบต่อการปฏิบัติงาน และมีส่วนเกี่ยวข้องการรายงานการเงิน จะต้องได้รับการอนุมัติจากเจ้าขององค์กร ทีมผู้บริหาร และบุคคลภายในบริษัทผู้มีส่วนเกี่ยวข้อง การศึกษาผลกระทบทางธุรกิจที่เกิดขึ้นจะต้องมีข้อมูลที่เกี่ยวข้องดังต่อไปนี้

- ระบุระยะเวลาในการวิเคราะห์ รวมถึงรายละเอียดการให้บริการให้แก่บริษัท
- รายงานสถานะทางการเงินของแต่ละหน่วยธุรกิจที่มีผลกระทบต่อการปฏิบัติงานและที่มีผลกระทบต่อความสูญเสียของทรัพยากรภายในองค์กร
- ระยะเวลาที่มีผลกระทบโดยตรงต่องานจะต้องดำเนินการต่อไปได้
- คำสั่งที่มีความจำเป็นในการรันโปรแกรมจะต้องสามารถสามารถกู้คืนได้
- จะต้องสามารคาดการณ์ส่วนเพิ่มของการใช้ทรัพยากรที่จำเป็นต่อการดำเนินการต่อเนื่องทางธุรกิจ

7.2.1. แผนการดำเนินการต่อเนื่องทางธุรกิจ

แผนการดำเนินการต่อเนื่องจะต้องสามารถสนับสนุนหน่วยธุรกิจที่สำคัญต่อองค์กรได้ภายใต้ระยะเวลาที่กำหนดในแผนการวิเคราะห์ผลกระทบทางธุรกิจ ลดโอกาสที่จะเกิดความสูญเสียทางการเงิน หรือ รายได้รวม จัดหาบุคลากรที่เหมาะสมในการรักษาความปลอดภัยที่สามารถแก้ไขปัญหาได้ทันทีเมื่อเกิดความผิดพลาดขึ้นและทำให้การปฏิบัติงานไม่ต้องหยุดชะงักลงภายในระยะเวลาที่กำหนด

แผนงานขั้นต่อไป จะต้องมีการพัฒนาและมีเอกสารเพื่อรองรับการดูแลรักษาในอนาคต รองรับการทำสำรองข้อมูลเกี่ยวกับการดำเนินงานทางธุรกิจ ภายในระยะเวลาที่กำหนด สามารถติดตามปัญหาหรือความผิดพลาดที่จะเกิดขึ้น

แผนงานธุรกิจขั้นต่อไป จะต้องมีข้อมูลดังต่อไปนี้เป็นอย่างต่ำ

- จำนวนและความถี่ของ “ad hoc” ที่มีผลต่อโอกาสที่จะเกิดการรบกวนต่อธุรกิจ
- ทีมงานจะต้องประกอบด้วยผู้เชี่ยวชาญเฉพาะด้าน รวมอยู่ในทีมงานด้วย
- มีแผนสำหรับการพัฒนาและติดตั้งระบบใหม่ รวมถึงแผนสำหรับการกู้คืนข้อมูลด้วย
- แผนการสรุปข้อมูลทีเกิดการสูญหาย
- สรุปเวลารวมทั้งหมดสำหรับกระบวนการการกู้คืน

กระบวนการการวางแผนจะเน้นในส่วนที่เกี่ยวกับความต้องการทางธุรกิจเป็นสำคัญ

- แผนงานขั้นต่อไป จะต้องมีการพิจารณาถึงประเด็นต่างๆเหล่านี้
- ขอบข่ายของแผนงานขั้นต่อไป และการจำกัดความชองความผิดพลาดที่อาจจะเกิดขึ้น
- ลำดับขั้นตอนภาวะฉุกเฉิน
- บุคลากรที่มีส่วนรับผิดชอบในการตัดสินใจในภาวะฉุกเฉิน ส่วนประกอบของแผนปฏิบัติการ และทางเลือกอื่นๆ
- ส่วนประกอบของทีมกู้คืนข้อมูลธุรกิจ และรายละเอียดของลูกทีมและ ที่ๆสามารถติดต่อได้
- ทรัพยากรที่เกี่ยวข้อง เมื่อทรัพยากรถูกนำมาใช้ สามารถทราบได้ว่าทรัพยากรนั้นถูกใช้ในลักษณะใด
- แผนปฏิบัติการในกรณีที่ฉุกเฉิน และรายละเอียดของแผนปฏิบัติการของเหตุการณ์ทีเกิดขึ้นว่าส่วนใดที่อาจทำให้เกิดอันตรายธุรกิจหรือต่อชีวิต
- จัดทำระเบียบปฏิบัติและรายละเอียดกิจกรรมต่างๆที่มีผลทางธุรกิจหรือ สถานที่ชั่วคราวที่ใช้เป็นที่จัดเก็บชั่วคราว และสามารถเคลื่อนย้ายกับเข้าสู่ที่เดิมภายในระยะเวลาที่กำหนด
- จัดทำระเบียบปฏิบัติและรายละเอียดของการนำกิจกรรมต่างๆกลับเข้าสู่ภาวะปกติ
- ตารางการดูแลรักษาระบุถึงวิธีการและเวลามรการทำการทดสอบและแนวทางการดูแลรักษา
- จัดทำตารางอบรม เพื่อทำความเข้าใจในแผนการขั้นต่อไปและเพื่อความมั่นใจว่าแผนงานนั้นจะประสบผลสำเร็จ

7.2.2. การประเมินแผนการดำเนินการ

แผนการดำเนินการควรจะมีการประเมินเป็นประจำเพื่อความมั่นใจในประสิทธิภาพเป็นผู้อนุมัติการทดสอบและแผนการดูแลรักษาการประเมินแผนการดำเนินการจะประกอบไปด้วย

- มีการประเมินจะรวมถึงหัวข้อที่เผยแพร่แล้วหัวข้อที่ไม่มีการเผยแพร่

- เอกสารประกอบการชี้แจงจะต้องแจ้งวัตถุประสงค์ในแต่ละหัวข้อรวมถึงรายงานความรับผิดชอบและบรรทัดฐานที่ใช้ในการประเมิน
- มีการแยกประเด็นที่เกี่ยวกับวิธีการและเวลาของแผนที่ใช้ในการทดสอบ
- หาค่าผลการทดสอบก่อนการประเมินและเปรียบเทียบหลักการประเมินรวมถึงเอกสารปรักอบวิธีการขยายแผนงาน

ผู้ร่วมงานในแผนปฏิบัติงานจะต้องแจ้งแก่ตัวแทนของทีมรักษาความปลอดภัยระบบสารสนเทศอย่างน้อย 1 เดือนล่วงหน้าสำหรับการทำการประเมินในแต่ละครั้งการประเมินแผนการปฏิบัติงานอย่างน้อยปีละ 1 ครั้ง

7.2.3. แผนการทบทวนและการดูแลรักษาแผนการปฏิบัติงาน

ทีมผู้บริหารที่มีส่วนเกี่ยวข้องในการรับทราบข้อมูลเกี่ยวกับแผนการปฏิบัติงานจะเป็นผู้ลงนามยอมรับแผนการและรายละเอียดในแผนการปฏิบัติงาน ข้อมูลเกี่ยวกับแผนการปฏิบัติงานจะต้องสามารถนำมาใช้ได้ทันทีที่ต้องการ เมื่อมีการเปลี่ยนแปลงตามรายการต่อไปนี้ทางต้องมีการแจ้งต่อเจ้าหน้าที่ผู้ดูแลแผนงาน

- ข้อมูลของแต่ละบุคคล
- กลยุทธ์ทางธุรกิจ
- สถานที่ ผลกระทบและทรัพยากรที่เปลี่ยนแปลง
- เกี่ยวข้องกับทางกฎหมาย
- ผู้ประสานงาน ผู้ขาย และกลุ่มลูกค้าหลัก
- วิธีการดำเนินการ
- ความเสี่ยงทั้งในทางปฏิบัติการและทางการเงิน

การเปลี่ยนแปลงในแผนการปฏิบัติงานจะต้องดำเนินการแล้วเสร็จภายใน 30 วันนับจากมีการประชุมเพื่อทำการเปลี่ยนแปลงและหรือไม่เกิน 60 วันหลังจากการสรุปผลการประเมินมีการทบทวนแผนการดำเนินการอย่างน้อยปีละ 1 ครั้ง

7.2.4. การสำรองและการกู้คืนข้อมูล

การสำรองและการกู้คืนข้อมูล จะต้องครอบคลุมทุกส่วนของข้อมูลที่เกี่ยวข้องกับการดำเนินธุรกิจและมีการปรับเปลี่ยนแก้ไขให้สอดคล้องกับแผนการรักษาความปลอดภัยที่เจ้าของธุรกิจเป็นผู้กำหนด แผนการสำรองและการกู้คืนข้อมูลจะต้องครอบคลุมข้อมูลทุกส่วนที่เกี่ยวข้องระบบธุรกิจ / การบริการโดยจะต้องมีรายละเอียดสำหรับแต่ละระบบ แต่ละบริการอย่างชัดเจน

แผนการสำรอง และการกู้คืนข้อมูลจะต้องประกอบไปด้วยส่วนต่างๆดังนี้

- กำหนด ID และความรับผิดชอบของแต่ละฟังก์ชั่นการทำงาน
- ได้รับอนุญาตและรายงานผลกระทบต่อเวลาและระบบ
- ตรวจสอบความถูกต้องของข้อมูลที่ทำการสำรอง
- ความเป็นไปได้ของความผิดพลาดอันเกิดจากการสำรองข้อมูล
- ตรวจสอบความถูกต้องของข้อมูลที่กู้คืน
- ระยะเวลาที่สงวนไว้เพื่อทำการสำรองข้อมูล
- มีการตรวจสอบขั้นตอนการกู้ข้อมูลเป็นประจำ
- เอกสารเกี่ยวกับข้อมูลที่ทำการสำรองและข้อมูลที่กู้คืนมา

7.2.5. Offsite Storage

ผู้ดูแลรักษาข้อมูลจะต้องมีการประชุมร่วมกันเพื่อหาแนวทางในการเก็บข้อมูลทั้งหมดและสามารถกู้คืนกลับมาได้

หน้าที่และความรับผิดชอบข้อมูลต่างๆ ของเจ้าของธุรกิจและทีมผู้บริหาร

- ตัดสินใจเกี่ยวกับโปรแกรมและระบบที่จะใช้ในการเก็บข้อมูล
- กำหนดเอกสารและระเบียบปฏิบัติที่จะใช้ในการกำหนด ID และโปรแกรมสำหรับการ
- ทำการกู้คืน
- รับรองข้อมูล และเอกสารที่หมุนเวียนกันจะเพียงพอต่อการกู้คืนข้อมูลที่จำเป็น
- รับรองข้อมูล ซอฟแวร์และเอกสารเกี่ยวกับสถานที่ตั้งของการเก็บข้อมูลในปัจจุบัน

การสำรองข้อมูลจะต้องมี 2 เวอร์ชั่นคือ Back up file และ เวอร์ชั่นปัจจุบัน สถานที่เก็บข้อมูลสำรองควรจะอยู่ในที่ๆเหมาะสมในการเดินทาง เหมาะสมต่อค่าใช้จ่าย และจะต้องไกลจากส่วนที่จะมีผลกระทบที่อาจจะเกิดขึ้นจากสถานที่เก็บข้อมูลปัจจุบัน มีการจัดการดูแลรักษาสภาพแวดล้อมและความปลอดภัยทางกายภาพอย่างเหมาะสม มีการจัดระบบการขนส่งและการเดินทางที่สะดวกและสอดคล้องกับสื่อที่จะใช้ในการเก็บข้อมูลสำรอง

มีการควบคุมปัจจัยต่างๆสำหรับสถานที่เก็บข้อมูลสำรองดังต่อไปนี้

- เนื้อหาการเข้าถึงข้อมูลทางกายภาพ
- โครงสร้างทางกายภาพที่สามารถทนต่อการเกิดเพลงไหม้ได้ไม่ต่ำกว่า 2 ชั่วโมง
- จะตั้งสถานที่เก็บเอกสารแยกออกจากห้องคอมพิวเตอร์
- อนุญาตให้ผ่านได้เฉพาะผู้ที่มีส่วนเกี่ยวข้อง
- มีการเก็บข้อมูลอย่างถาวร

- มีการบันทึกสื่อข้อมูลทั้งหมดและบันทึกการเคลื่อนย้ายไฟล์ทั้งในและนอกห้องเก็บข้อมูล
- มีการจัดทำบันทึกต่างๆไว้เป็นลายลักษณ์อักษร มีการจัดทำสารบัญ เวอร์ชั่น สถานที่ตั้งของไฟล์ข้อมูล

แผนฉุกเฉินการกู้คืน (Incident Handling Management)

7.3 หน้าที่และความรับผิดชอบ

วัตถุประสงค์ : พนักงานของบริษัททุกคนจะต้องคอยสอดส่องดูแลและรายงานให้แก่แผนกรักษาความปลอดภัยสารสนเทศ หากพบเห็นเหตุการณ์ผิดปกติ หรือเหตุการณ์อันอาจจะก่อให้เกิดความเสียหายกับข้อมูลสารสนเทศทันทีเพื่อให้การแก้ไขเป็นไปอย่างรวดเร็วถูกต้อง

- การกระทำใดๆที่เป็นการพยายามเข้าทำลาย แก้ไข รบกวนข้อมูลนั้น ถ้าหากได้รับรายงานจากแผนกรักษาความปลอดภัยระบบสารสนเทศจะต้องมีลงโทษตามวินัย
- มีการออกระเบียบการลงโทษสำหรับพนักงานที่พยายามฝ่าฝืน เข้าแทรกแซง หรือทำการทดลองใดๆกับข้อมูลโดยไม่ได้รับอนุญาต

การช่วยเหลือ User และการติดตามการแก้ไข

ระบบที่จะใช้ในการเก็บข้อมูล ติดตามการแก้ไขและรายงานสถานการณ์ปัญหาที่เกิดขึ้นจะต้องได้รับการยอมรับว่าสามารถจัดการและแก้ไขปัญหาที่เกิดขึ้นภายในระยะเวลาอันรวดเร็วและเกิดผลกระทบกับผู้ใช้งานระบบให้น้อยที่สุด

ผู้ทำหน้าที่ช่วยเหลือการใช้งานคอมพิวเตอร์ จะเป็นบุคคลแรกในการแก้ปัญหาการใช้งานคอมพิวเตอร์ รายงานการคาดการณ์ที่เกี่ยวกับความปลอดภัยของข้อมูลจะต้องสัมพันธ์กับการทำรายงานการจัดการตรวจสอบ

7.4. การแจกแจงและการจัดลำดับชั้น

วัตถุประสงค์ : เพื่อช่วยในการตัดสินใจกับปัญหาที่อาจจะเกิดขึ้น และถ้าหากเกิดปัญหาขึ้นจะต้องมีขั้นตอนที่จะสามารถแยกแยะและจะลำดับสถานการณ์ของปัญหาได้ แผนกรักษาความปลอดภัยข้อมูลสารสนเทศและแผนก ISS จะเป็นผู้จัดหาขั้นตอนในการกำหนดหัวข้อ การแจกแจง และการจัดลำดับชั้นของเหตุการณ์ที่เกิดขึ้น

การจัดลำดับขั้นของเหตุการณ์จะต้องมีรวมถึงหัวข้อต่างๆดังต่อไปนี้

- ไวรัสประเภทหนอนและไวรัส (Worms and Virus)
- code ที่ประสงค์ร้ายต่อระบบ
- การเจาะทำลายส่วนที่เป็นความลับ
- การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- การเข้าถึงบริการและโปรแกรมอรรถประโยชน์โดยไม่ได้รับอนุญาต
- การทำลายระบบ IT ทำให้เกิดการสูญเสียข้อมูล หรือการรบกวนการให้บริการ

การปฏิเสธการให้บริการหรือไม่สามารถให้บริการแก่ผู้ต้องการใช้ระบบที่เข้าถึงข้อมูลอย่างถูกต้อง ความเสียหายหรือการสูญหายที่เกิดกับ Hardware, Software หรือข้อมูลที่สำคัญ การเข้าถึงข้อมูลหรือระบบเครือข่ายได้อย่างผิดปกติ เช่น ผู้ใช้งานระบบ UNIX สามารถเข้าถึงข้อมูลได้โดยไม่ได้ผ่านการตรวจสอบตามลำดับ รหัสพนักงานที่น่าสงสัย (เช่น พนักงานบางคนที่เข้ามาในระบบและไม่มีการดำเนินการใดๆที่เกี่ยวกับระบบนานกว่า 20 นาที)

- รหัสพนักงานที่ไม่มีอยู่ในระบบ
- ไม่มีรายละเอียดของไฟล์ใหม่เกิดขึ้นหรือไม่สอดคล้องกับไฟล์ที่ดำเนินการ
- ไม่ประสบผลสำเร็จในการ Login
- ไม่มีรายละเอียดบอกถึงการแก้ไขความยาวของไฟล์ หรือวันที่ โดยเฉพาะอย่างยิ่งในไฟล์ที่ใช้ในการปฏิบัติการ (Execute file)
- ไม่คำอธิบายสำหรับการพยายามทดลองเขียนทับไฟล์เก่าหรือการปรับแก้ไฟล์ระบบ
- ไม่มีการอธิบายการแก้ไขข้อมูลหรือการลบข้อมูล
- ระบบมีประสิทธิภาพที่ต่ำลง
- ปัญหาสภาพแวดล้อม (เช่น ทำลายเครื่องสแกนเนอร์ การเข้าระบบจากผู้ที่ไม่มีส่วนเกี่ยวข้องหรือผู้แอบอ้าง)
- ใช่เวลาในการทำงานผิดปกติตามที่ควรจะเป็น (เช่น การเข้าทำงานในเวลาที่ผิดปกติหรือนอกเวลาทำงาน)
- มีรูปแบบการเรียกใช้งานที่เปลี่ยนไป (เช่น มีการเรียกใช้งานโปรแกรมซึ่งพนักงานคนนั้นๆไม่เคยเรียกโปรแกรมนี้เพื่อใช้งานมาก่อน)
- การจารกรรม
- ความผิดพลาดเกิดจากการเข้าถึงข้อมูลทางธุรกิจไม่สมบูรณ์ หรือเข้าถึงอย่างไม่ตรงไปตรงมา
- ปัญหาทั่วๆไปที่พบในระบบ

7.5. การตอบรับและการรายงาน

วัตถุประสงค์ : ผู้ติดต่อประสานงานและผู้ที่มีส่วนรับผิดชอบหรือแผนกที่มีส่วนรับผิดชอบจะต้องมีการติดต่อกับพนักงานของบริษัท

ส่วนที่อาจจะมีการถูกโจมตีได้โดยง่าย หรือเหตุการณ์อื่นๆที่อาจจะผลกระทบจะต้องมีการรายงานอย่างรวดเร็วและเป็นความลับให้แก่แผนกรักษาความปลอดภัยระบบสารสนเทศ การเปิดเผย

ข้อมูลโดยไม่ได้รับความยินยอมจากแผนกดูแลระบบสารสนเทศจะถูกรายงานให้แก่เจ้าของระบบเมื่อตรวจสอบโปรแกรมที่ต้องห้ามหรือโปรแกรมที่ไม่ได้รับอนุญาตจะต้องรายงานให้แก่ผู้บังคับบัญชา

ถ้าพบหลักฐานที่ชัดเจนว่าจะมีผู้เข้ามาทำลายระบบของบริษัทไม่ว่าจะโดยทางคอมพิวเตอร์หรือทางระบบเครือข่าย จะต้องมีการสืบสวนให้กระจ่าง การสืบสวนจะต้องได้ข้อมูลที่ต้องการครบถ้วนและสามารถทำมาใช้จัดการในแต่ละลำดับเหตุการณ์ เช่น เหตุการณ์ที่ไม่สามารถอธิบายได้หรือ มีเปลี่ยนแปลงมาตรการที่ใช้ในการตรวจสอบ

การรายงานภายนอก

การแจ้ง รายงานระบบความปลอดภัย หรือจุดอ่อนให้แก้บุคคลภายนอกโดยไม่ได้รับอนุญาตจะถูกลงโทษตามวินัยและทางกฎหมาย หากทางฝ่ายกฎหมายต้องการรายงานเกี่ยวกับความปลอดภัยให้กับบุคคลภายนอกที่ได้รับอนุญาตจะต้องสามารถดำเนินการได้อย่างทันท่วงที

ถ้าไม่มีความต้องการทางด้านระบบเพิ่มเติมในการประชุมร่วมกันจากทางตัวแทนฝ่ายกฎหมาย ฝ่ายรักษาความปลอดภัยระบบสารสนเทศ และฝ่ายตรวจสอบภายใน จะต้องมีโหวตเกี่ยวกับข้อดีและข้อเสียที่จะให้บุคคลภายนอกทราบก่อนที่จะรายงานเหตุการณ์นั้นออกไป

7.6. การสร้างระเบียบปฏิบัติ

วัตถุประสงค์ : อนุญาตให้ระบบตอบรับ การสร้างระเบียบปฏิบัติจะต้องมั่นใจว่าพนักงานว่าพนักงานสามารถปฏิบัติได้ตามแผนที่ได้วางไว้และระบบจะมีความปลอดภัย

แผนกรักษาความปลอดภัยระบบสารสนเทศและเจ้าของธุรกิจจะเป็นผู้ออกระเบียบปฏิบัติที่ครอบคลุมศักยภาพของระบบและมีรายละเอียดของการกำหนดรายละเอียดและการจำแนกประเภทเมื่อมีการเพิ่มเติมแผนการดำเนินการ จะต้องมีการออกแบบให้ระบบสามารถถูกกู้คืนได้ภายในระยะเวลาอันสั้น และระเบียบปฏิบัติจะต้องครอบคลุมหัวข้อต่อไปนี้

- วิเคราะห์และระบุถึงสาเหตุของเหตุการณ์ที่จะเกิดขึ้น
- เพิ่มเติมแผนระเบียบปฏิบัติ
- วางแผนและติดตั้งระบบที่ใช้แก้ไขความเสียหาย ในกรณีที่จำเป็น
- เก็บข้อมูลหลักฐานการตรวจสอบ
- ติดต่อกับผู้ที่มีผลกระทบหรือมีส่วนเกี่ยวข้องเพื่อทำการกู้คืนโดยตรวจสอบได้จากหลักฐาน
- รายงานเหตุการณ์ที่เกิดขึ้นกับผู้บัญชาการ

การปฏิบัติการที่เกี่ยวกับการแก้ไขหรือการกู้คืนข้อมูลจะต้องดำเนินการอย่างรอบคอบและระมัดระวังและเป็นทางการ ระเบียบปฏิบัติควรจะมั่นใจว่า ระบุเฉพาะผู้มีที่มีส่วนเกี่ยวข้องเท่านั้น

ที่จะสามารถเข้าสู่ระบบและข้อมูล มีเอกสารที่ลงรายละเอียดเกี่ยวกับการปฏิบัติการฉุกเฉินต่างๆ มีรายงานเหตุการณ์ฉุกเฉินให้ผู้ที่มีส่วนเกี่ยวข้องทราบ หรือมีการยืนยันความสมบูรณ์ของระบบว่าสามารถดำเนินการได้อย่างปกติภายในระยะเวลาอันสั้น

หลักฐานการตรวจสอบหรือหลักฐานที่เกี่ยวข้องจะถูกเก็บไว้อย่างปลอดภัยและแยกออกต่างหากเพื่อ

- การวิเคราะห์ภายใน
- เป็นหลักฐานที่เกี่ยวข้องในการพิจารณาสัญญาฉบับใหม่ สำหรับดำเนินการกับผู้ที่ทำลายระบบ
- ใช้เป็นข้อต่อรองเพื่อให้ผู้ให้บริการหรือเจ้าของซอฟต์แวร์ชดใช้ค่าเสียหาย

ถ้ามีความต้องการเปลี่ยนแปลงระบบปฏิบัติการจะต้องมีการจะต้องได้รับความยินยอมและสอดคล้องกับนโยบายแผนหลักในส่วน Application and System Development: Change Management

7.7. การกำหนดเนื้อหาข้อมูลและการกำจัด

วัตถุประสงค์ : การกำหนดเนื้อหาและการกำจัดขั้นตอนต่างๆจะต้องมีการกำหนดขอบเขตและขนาดของงานอย่างชัดเจนว่ามีขนาดเล็กหรือใหญ่ขนาดไหน แยกส่วนที่มีปัญหาน้อยและปัญหามากออกจากกัน และมั่นใจว่าปัญหาที่เกิดขึ้นจะถูกกำจัดออกไปจนหมดสิ้น ด้วยการลบออกหรือการป้องกัน

นโยบายต่อไปนี้จะใช้เป็นการระบุความปลอดภัยของระบบ

- ไม่สามารถเข้าใช้งานระบบจากที่ใดก็ได้โดยผู้ที่ไม่ได้รับอนุญาตจากแผนกรักษาความปลอดภัยระบบสารสนเทศ
- มี่การสำรองข้อมูลในระบบโดยผู้ที่ได้รับอนุญาตจาก เจ้าของระบบ/เจ้าของธุรกิจ หรือทีมรักษาความปลอดภัยข้อมูล

เจ้าของธุรกิจจะเป็นผู้อนุญาตให้สามารถทำการปิดระบบ / การปิดการให้บริการเครือข่าย เป็นผู้อนุญาตระบบสามารถทำงานต่อได้จากการตรวจสอบกิจกรรมทั้งหมดของเจ้าของธุรกิจ

7.8. การกู้คืน

วัตถุประสงค์ : กระบวนการการกู้คืนจะต้องมั่นใจว่าสามารถกู้คืนส่วนที่เกี่ยวข้องทั้งหมดได้ภายในระยะเวลาที่กำหนด โดยเจ้าของธุรกิจจะเป็นผู้ตัดสินใจเกี่ยวกับระดับการให้บริการที่เกี่ยวข้อง เจ้าของธุรกิจจะเป็นผู้อนุญาตให้ทำการกู้คืนส่วนที่เกี่ยวข้องกับการดำเนินธุรกิจเป็นส่วนแรก กระบวนการกู้คืนจะต้องสอดคล้องและใช้งานได้กับความต้องการทางด้านความปลอดภัยของบริษัท ในสถานการณ์ที่ระบบที่เกี่ยวข้องกับธุรกิจหลักและความปลอดภัยมีผลกระทบและใช้เวลาในการ

ดำเนินการเกินกว่าที่คาดการณ์ จะต้องมีการพิจารณานำระบบสำรองมาใช้งานและระบบที่นำมาใช้งานแทนจะต้องมีความสามารถในการดำเนินการได้ภายในระยะเวลาที่กำหนด

สถานที่ประมวลผลและระบบคอมพิวเตอร์สำรอง

- จะต้องมีสถานที่ (แยกต่างหากจากสถานที่ประมวลผลปรกติ) อย่างเพียงพอในการประมวลผลสำหรับระบบงานที่สำคัญ
- ระบบคอมพิวเตอร์สำรองจะต้องมีความสามารถเพียงพอในการประมวลผลระบบงานที่สำคัญ
- ในกรณีที่ใช้บริการของผู้ให้บริการด้านนี้ จะต้องมีสัญญาการใช้บริการที่เป็นลายลักษณ์อักษร
- ถ้าเป็นไปได้ควรจะจัดเก็บข้อมูล และโปรแกรมสำรองไว้ไม่ไกลจากสถานที่ประมวลผลสำรอง
- จะต้องทำการทดสอบการประมวลผลในสถานที่สำรองอย่างสม่ำเสมอ อย่างน้อยปีละครั้ง
- เพื่อความปลอดภัยของข้อมูล ควรจะทำการลบข้อมูลที่ใช้ในการทดสอบออกจากระบบสำรอง และต้องแน่ใจว่า จะไม่สามารถนำข้อมูลที่ลบแล้วมาใช้ใหม่ได้

7.9. การติดตามความคืบหน้า

วัตถุประสงค์ : หลังจากระบบถูกกู้คืนขึ้นมาเรียบร้อยและระบบอยู่ในสภาวะปกติ จะต้องมีการวิเคราะห์และติดตามผลที่เกิดขึ้น

ทุกแผนกที่เกี่ยวข้อง (หรือตัวแทนของแต่ละกลุ่ม) จะต้องมีการประชุมเพื่อสรุปสถานการณ์ที่ประสบมาและเก็บเป็นกรณีศึกษา มีการแยกประเด็นต่างๆต่อไปนี้ออกเป็นข้อย่อยและรวมอยู่ในวาระการประชุม วิเคราะห์สิ่งทีเกิดขึ้นและการแทรกการดำเนินการแก้ไข และค่าใช้จ่าย ทีมรักษาความปลอดภัยระบบสารสนเทศ จะเป็นผู้ประสานงานในการเขียนรายงานที่เกิดขึ้นให้แต่ละบุคคล ถ้าการจัดทำรายงานใช้ได้ จะมีการกำหนดให้เป็นคำแนะนำและนำเสนอในระดับการจัดการต่อไป โดยอาจจะมีการเพิ่มเติมและปรับปรุงนโยบายและระเบียบปฏิบัติถ้าหากว่ามีความจำเป็น

บทที่ 8
สรุปผล ข้อเสนอแนะ

8.1 สรุปผล

พบว่าทั้ง CoBIT Version3 และ ISO 17799 นิยมใช้เป็นสิ่งอ้างอิงในการสร้างนโยบายและมาตราการรักษาความปลอดภัยระบบสารสนเทศในแต่ละองค์กร มีความคาบเกี่ยวกันค่อนข้างมาก แต่ลักษณะที่มุ่งเน้นแตกต่างกันไปบ้างในรายละเอียดปลีกย่อย และวัตถุประสงค์ในการใช้งาน แต่เนื่องด้วย CoBIT เป็น Frame Work ที่เกิดขึ้นจาก สมาคมผู้ควบคุมและตรวจสอบระบบสารสนเทศ หรือ ISACA (Information Systems Audit and Control Association) ซึ่งมีสำนักงานสาขา กับจำนวนสมาชิกที่มีอาชีพด้านการตรวจสอบระบบเทคโนโลยีสารสนเทศ อยู่ทั่วโลก และมุ่งเน้นมากขึ้นในเรื่อง IT Governance มีการทำวิจัย และโครงการด้านนี้มาต่อเนื่องเป็นเวลานาน และเป็นที่นิยมมากในระดับสากล โดยเฉพาะอุตสาหกรรมด้านการเงิน จึงมีรายละเอียดที่การตรวจสอบและเกณฑ์ต่างๆในเชิงปฏิบัติอยู่ครบถ้วนกว่า ISO 17799 มีจะมุ่งเน้นไปทางการอ้างอิงถึงวิธีการจัดการระบบโดยทั่วไป ซึ่งชัดเจนครบถ้วนด้านการปกป้องสารสนเทศ ไม่เฉพาะกับอุตสาหกรรม หรือธุรกิจใดๆมากนัก

จึงทำให้บริษัทหลักทรัพย์ในประเทศไทยนิยมที่จะนำเอามาเป็นแบบแผนในการออกแบบนโยบาย ตามกรอบงาน ของ ISO17799 ในเบื้องต้น แล้วเสริมด้วยรายละเอียดเพื่อการตรวจสอบระบบ และ แนวทางในการปฏิบัติ ในหัวข้อย่อยๆต่างๆที่อ้างอิงจาก CoBIT เพื่อจะได้ยึดถือเป็นแนวทางเดียวกันกับผู้ตรวจสอบ ที่จะต้องเข้ามาร่วมในการประเมินระบบความปลอดภัยเป็นระยะอยู่แล้ว อีกทั้งยังเป็นหนทางในการไปสู่เป้าหมายขององค์กรที่เป็น บรรษัทภิบาล โดยอาศัย IT Governance เป็นสิ่งขับเคลื่อนที่สำคัญ

9.2 ข้อเสนอแนะ

แนวทางปฏิบัติของบริษัทหลักทรัพย์ในประเทศไทยด้านการรักษาความปลอดภัยสารสนเทศ

1. ระบุรายชื่อ บทบาทหน้าที่ และรายละเอียดงานของผู้ที่มีส่วนได้ส่วนเสีย และองค์กรที่มีส่วนรับผิดชอบ ซึ่งเป็นสิ่งที่สำคัญที่จะต้องเข้าใจโครงสร้างขององค์กร และทราบว่าใครเป็น

ผู้รับผิดชอบดูแล นโยบายด้านความปลอดภัย โดยสิ่งที่สำคัญที่สุดคือ นโยบายด้านความปลอดภัยจะต้องได้รับความเห็นร่วมกันในระดับที่เหมาะสม เพื่อให้แน่ใจได้ว่านโยบายด้านความปลอดภัยที่มีนั้นตรงประเด็น โดยองค์กรต้องคำนึงถึงสิ่งที่ต้องการ เป้าหมายและวัตถุประสงค์ขององค์กรได้อย่างเหมาะสม

ผู้ที่จะเข้ามามีส่วนร่วมในการกำหนดนโยบายนี้ ควรจะเปิดให้กว้างให้กับฝ่าย ที่ปฏิบัติงานในด้านต่างๆ และควรมีผู้แทนของฝ่ายดูแลระบบข้อมูล การรักษา ความความปลอดภัย กฎหมาย ทรัพยากรบุคคล ฝ่ายตรวจสอบภายใน ฝ่ายปฏิบัติงาน และฝ่ายพัฒนาองค์กร เพื่อเป็นตัวแทนฝ่ายในองค์กรเพื่อที่จะสามารถแก้ไขปัญหาได้อย่างแท้จริง

2. กำหนดวัตถุประสงค์ทางธุรกิจให้ชัดเจน การเข้าใจวัตถุประสงค์เบื้องต้นของธุรกิจ มีความสำคัญต่อการกำหนดขอบเขตนโยบายด้าน ความปลอดภัย เช่น องค์กรอาจจำเป็นต้องตรวจสอบภายในเป็นพิเศษ มีขั้นตอนการตรวจตรา ตลอดจนการเก็บข้อมูลสำรอง และกู้ข้อมูลตามกฎเกณฑ์ข้อบังคับที่ได้ระบุไว้ ในขณะที่องค์กรอื่นๆ อาจไม่จำเป็นต้องทำเช่นนี้ก็เป็นได้

ในส่วนนี้จะมีประเด็นหลักว่าจะทำอย่างไรให้นโยบายด้านความปลอดภัยเป็นไปอย่างคุ้มค่าและเหมาะสมกับองค์กรนั้นๆ เป็นหลัก ไม่ใช่เพียงแค่ดำเนินการตามที่ที่ปรึกษาด้านระบบความปลอดภัยนำมาเสนอ

3. หลักการด้านความปลอดภัยที่ตรงตามเจตนาของฝ่ายบริหาร โดยเฉพาะหลักการด้านความปลอดภัย ซึ่งควรได้รับการทบทวนและปรับใช้ในขั้นตอน การพัฒนานโยบายด้านความปลอดภัยเท่าที่จำเป็น จุดประสงค์ของหลักการด้านความปลอดภัยคือ ช่วยให้องค์กรของคุณสามารถระบุถึงสาระสำคัญได้อย่างชัดเจน และเรียบง่ายในสิ่งที่เป็นหัวใจของ องค์กร โดยไม่ต้องใส่รายละเอียดด้านเทคนิค หรือภาษาที่ทำให้เข้าใจยาก

4. กำหนดและจัดหมวดหมู่ข้อมูลและทรัพยากรด้านการประมวลผลที่เกี่ยวข้อง โดยมีวิธีการวางนโยบายด้านความปลอดภัยที่จะแนะนำ คือ วิธีการที่ใช้ข้อมูลเป็นศูนย์กลาง ในปัจจุบันระบบเทคโนโลยีสารสนเทศมักจะถือว่า ข้อมูลเป็นสินทรัพย์ที่สำคัญที่สุดประเภทหนึ่ง และควรได้รับการ ดูแลอย่างดี ด้วยเหตุนี้ การจัดหมวดหมู่ข้อมูล และทรัพยากรด้านการประมวลผลจะช่วยให้องค์กรสามารถ ตัดสินรูปแบบการใช้งานและประโยชน์ของมันได้ง่ายขึ้น

5. วิเคราะห์การหมุนเวียนของข้อมูล เพื่อจัดกลุ่มข้อมูลพื้นฐาน โดยเริ่มกระบวนการตั้งแต่เริ่มเก็บข้อมูลไปจนถึงการลบทิ้งข้อมูลแต่ละชิ้น โดยมีการใช้โมเดลที่มีข้อมูลเป็นศูนย์กลางในการวางนโยบายด้านความปลอดภัย วัตถุประสงค์ของการวิเคราะห์การหมุนเวียนของข้อมูลก็เพื่อแสดงให้เห็นถึงจุดในความรับผิดชอบต่างๆ ที่เข้าถึงข้อมูลได้ ตัวอย่างเช่น ในระบบการโอนเงิน ข้อมูลอาจจะไหลผ่านบราวเซอร์ เว็บเซิร์ฟเวอร์ ดาตาเซิร์ฟเวอร์ และ เซิร์ฟเวอร์อื่นๆ หรือระบบป้องกันข้อมูลไฟร์วอลส์ ก่อนจะถูกจัดเก็บไว้ในฐานข้อมูลบนเทปแม่เหล็ก หรือเอกสาร การติดตามการหมุนเวียนของข้อมูลผ่านระบบประมวลผล จะช่วยให้องค์กรสามารถกำหนดรูปแบบ และการจัดวางการควบคุมตามหลักเหตุผล และในเชิงกายภาพเพื่อปกป้องข้อมูลที่มีค่าเหล่านั้น

6. ระบุความเสี่ยงเบื้องต้นที่อาจจะเกิดขึ้นในระบบการทำงาน ซึ่งการคาดคำนวณความเสี่ยงที่อาจจะเกิดขึ้นช่วยชี้ให้เห็นถึงประเภทของความเสี่ยงที่มีอยู่ภายในองค์กร ความเป็นไปได้ที่ความเสี่ยงนั้นๆ จะก่อให้เกิดปัญหาขึ้นจริง ตลอดจนความยุ่งยากซับซ้อน ค่าใช้จ่าย และผลกระทบจากความเสี่ยงเหล่านั้น อย่างไรก็ตาม พึงตระหนักเสมอว่า รูปแบบความเสี่ยงมีความหลากหลาย ตามสภาพการณ์ที่แตกต่างกันไป

7. กำหนดมาตรการความปลอดภัยของระบบเบื้องต้นที่เหมาะสมสำหรับการใช้งาน หลังจากกำหนดตัวข้อมูลและกระบวนการที่เกี่ยวข้อง รวมทั้งได้ประเมินความเสี่ยงแล้ว ขั้นต่อ ไปคือการมองหามาตรการความปลอดภัยทั่วไปที่เหมาะสมกับองค์กร เรื่องนี้จัดว่าต้องใช้บริการในระดับสูง ซึ่งอาจรวมถึงความรับผิดชอบ การอนุญาตให้ใช้ข้อมูล การใช้งานอย่างต่อเนื่อง การแสดงข้อมูล การรับรองข้อมูล การรักษาความลับของข้อมูล การรวบรวมข้อมูล และการตอบรับข้อมูล การเข้าใจว่า องค์กรต้องการบริการด้าน การรักษาความปลอดภัยแบบใด จะช่วยกำหนดรูปแบบของนโยบายด้านความปลอดภัยที่จำเป็น รวมทั้งเนื้อหาเฉพาะและองค์ประกอบของนโยบายเหล่านั้น

8. สร้างโครงร่างนโยบายด้านความปลอดภัยทั่วไป โครงสร้างนโยบายด้านความปลอดภัยสามารถทำได้หลายรูปแบบ เช่นในเรื่ององค์ประกอบและลักษณะของนโยบายด้านความปลอดภัย ขั้นตอนนี้เป็นการระบุหัวข้อจำเพาะที่ จำเป็นสำหรับด้านความปลอดภัยแต่ละชุด

9. ระบุหัวข้อนโยบายด้านความปลอดภัย เป็นขั้นตอนสุดท้ายก่อนลงมือร่างนโยบายด้านความปลอดภัยคือ การระบุหัวข้อสำคัญของนโยบายด้าน ความปลอดภัยว่าจะเน้นในจุดใดบ้าง ทั้งนี้ การระบุหัวข้อดังกล่าวนี้นั้นจะขึ้นอยู่กับผลลัพธ์ของทุกขั้นตอนที่กล่าวมาขั้นต้น

9.3 บทสรุป

องค์ประกอบด้านรักษาความปลอดภัยที่สำคัญที่สุดแต่มักจะเข้าใจกันน้อยที่สุด ก็คือเรื่องของนโยบายด้านความปลอดภัย นโยบายด้านความปลอดภัยเหล่านี้จะระบุความคาดหมายของลูกค้าหรือผู้ใช้ รวมทั้งความต้องการด้านการเก็บรักษาความลับของข้อมูล ความเป็นสมบูรณ์ของข้อมูล และการจัดการ ข้อมูลองค์กรที่เหมาะสม ตลอดจนเงื่อนไขที่จะทำให้ความคาดหมายดังกล่าวบรรลุผล

ในความเป็นจริง นโยบายด้านความปลอดภัยมิใช่ตัวกำหนดความต้องการของผู้ใช้บนระบบข้อมูลคอมพิวเตอร์ แต่เป็นเหมือนสะพานเชื่อมโยงความคาดหมายของผู้ใช้กับความจำเป็นพื้นฐานในการพัฒนาระบบข้อมูล นโยบายด้านความปลอดภัยควรระบุความคาดหมายของลูกค้าให้ชัดเจน และควรตั้งอยู่บนพื้นฐานการประเมินค่าความเสี่ยงหากเหตุการณ์ไม่เป็นไปตามคาด การยึดหลักประเมินความเสี่ยงนี้จะช่วยให้ หลีกเลี่ยงปัญหาจากการวางมาตรการที่เป็นไปไม่ได้ จัดการได้ยาก หรือมีข้อจำกัดมากเกินไป

บรรณานุกรม

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. 2545. **แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ.**

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย. 2545. **ตัวอย่างระเบียบว่าด้วยการใช้งานระบบเครือข่ายคอมพิวเตอร์อย่างปลอดภัย.** [Online].Available: http://www.thaicert.nectec.or.th/paper/basic/policy.php

Hoekstra, A. and Conradie , N. 2002. **CoBIT,ITIL and ISO17799 How to Use them in Conjunction: Global Risk Management Solution** [Presentation]. Pricewaterhouse and Coopers.

Information Systems Audit and Control Association. 2002. **IS Standards, Guidelines and Procedures for Auditing and Control Professionals.**

ISO/IEC 17799. 20002 Information Technology – Code of Practice for Information Security Management. [Online]. Available: http://www.iso.ch

Krutz, L. Ronald, and Vines Dean, R. 2001. **The CISSP Prep Guide: Mastering the Ten Domains of Computer Security.** New York . John Wiley &Sons.

Whitman, M. and Mattord, H. 2002. **Principles of Information Security**. Massachusetts. Thomson Course Tecnology.

ภาคผนวก

<u>โครงการสนับสนุนให้บริษัทจดทะเบียนมีการกำกับดูแลกิจการที่ดี</u> (Good Governance)[8]

แนวความคิด

ในช่วงที่ผ่านมา กลต. และตลาดหลักทรัพย์ฯ ได้พยายามผลักดันให้บริษัทจดทะเบียนตระหนักถึงความสำคัญของการมีการกำกับดูแลกิจการที่ดี (good governance) โดยการออกข้อกำหนดต่าง ๆ หลายเรื่อง เช่น การกำหนดมาตรฐานการเปิดเผยข้อมูล การกำหนดให้มีคณะกรรมการตรวจสอบหรือแนวทางปฏิบัติที่ดีสำหรับกรรมการ เป็นต้น

จากการติดตามและประเมินผลในเรื่องดังกล่าว พบว่า มีบริษัทจดทะเบียนหลายแห่งได้ให้ความสำคัญในเรื่องนี้ และมีการปรับปรุงการดำเนินงานในหลาย ๆ ด้าน จนกล่าวได้ว่ามีการกำกับดูแลกิจการอยู่ในระดับที่น่าพอใจ อย่างไรก็ดี ยังมีบริษัทจดทะเบียนอีกจำนวนหนึ่งที่ยังไม่ได้ให้ความสำคัญในเรื่องดังกล่าวมากพอ รวมทั้งผู้ลงทุนส่วนใหญ่ก็ยังไม่ได้ให้ความสนใจในเรื่องนี้มากนัก ซึ่งสาเหตุหนึ่งอาจจะมาจากการไม่สามารถแยกแยะให้เห็นได้ชัดเจนระหว่างบริษัททั่ว ๆ ไป กับบริษัทที่มีการกำกับดูแลกิจการที่ดี สำนักงาน ก.ล.ต. จึงมีแนวความคิดที่จะส่งเสริมและผลักดันการดำเนินการในเรื่องนี้ให้เห็นผลได้ชัดเจนยิ่งขึ้น โดยการสนับสนุนให้มีการจัดอันดับการกำกับดูแลกิจการ (governance rating) และเปิดเผยให้ผู้ลงทุนทั่วไปได้ทราบ โดยบริษัทที่ได้รับอันดับในระดับที่สำนักงานกำหนด (เช่น ได้คะแนน 7 จาก 10 เป็นต้น) จะได้รับสิทธิประโยชน์ต่าง ๆ ทั้งทางตรงและทางอ้อม ดังนี้

<u>ประโยชน์ทางตรง</u>

(1) สำนักงานจะประกาศยกย่อง เชิดชู บริษัทที่ได้อันดับขั้นต่ำตามเกณฑ์ที่กำหนด ให้ประชาชนทั่วไปได้รับทราบ

(2) สำนักงานจะลดหย่อนค่าธรรมเนียมรายปีที่บริษัทต้องจ่ายให้สำนักงาน ในฐานะที่เป็นบริษัทที่ออกหลักทรัพย์

(3) ในกรณีที่บริษัทประสงค์จะระดมทุน ไม่ว่าโดยการเสนอขายหุ้นหรือตราสารใด ๆ จะสามารถทำได้อย่างสะดวกรวดเร็วและด้วยต้นทุนที่ต่ำลง กล่าวคือ

- ได้รับการพิจารณาเป็นกรณีเร่งด่วน (fast track)
- ได้รับยกเว้นไม่ต้องมีที่ปรึกษาทางการเงินร่วมจัดทำคำขออนุญาต
- ได้รับการลดหย่อนค่าธรรมเนียม filing ที่ต้องจ่ายให้สำนักงาน

---

[8] ที่มา : เอกสารเผยแพร่ ฝ่ายจดทะเบียนหลักทรัพย์ **สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์** (เมษายน 2545)

ทั้งนี้ การลดหย่อนค่าธรรมเนียมตาม (2) และ (3) มีกำหนดเวลาเบื้องต้น 3 ปี หลังจากนั้น สำนักงานจะทบทวนความเหมาะสมในเรื่องนี้อีกครั้งหนึ่ง

<u>ประโยชน์ทางอ้อม</u>

(1) บริษัทจะมีภาพพจน์ที่ดีในสายตาผู้เกี่ยวข้อง ไม่ว่าจะเป็นผู้ถือหุ้น ประชาชนทั่วไป ลูกค้า supplier เจ้าหนี้ ฯลฯ

(2) ราคาหุ้นของบริษัทจะมี premium เพิ่มขึ้น เนื่องจากผู้ลงทุนจะเห็นประโยชน์และความสำคัญของการกำกับดูแลกิจการที่ดีมากขึ้น เช่นเดียวกับแนวโน้มที่เกิดขึ้นในต่างประเทศ ซึ่งผลจากการวิจัยของบางบริษัทพบว่า ผู้ลงทุนต่างประเทศยินดีจ่าย premium ให้กับหุ้นของบริษัทจดทะเบียนในประเทศไทยที่มี governance ดี เพิ่มขึ้นถึง 26%

การดำเนินการต่อไป

- <u>Rating Agency</u>

  สำนักงานได้สอบถามความสนใจในเบื้องต้นกับบริษัทจัดอันดับในประเทศไทยทั้ง 2 แห่ง คือ บริษัท ไทยเรทติ้งแอนด์อินฟอร์เมชั่นเซอร์วิส จำกัด (TRIS) และบริษัท ฟิทช์ เรทติ้งส์ (ประเทศไทย) จำกัด (FITCH) แล้วพบว่า ทั้ง 2 บริษัทให้ความสนใจจะดำเนินการเรื่องนี้ โดยสำนักงานรับจะทำหน้าที่เป็นที่ปรึกษาให้กับทั้ง 2 บริษัทในขั้นตอนการกำหนดแนวทางการจัดอันดับ ทั้งนี้ คาดว่าทั้ง 2 บริษัทจะต้องใช้เวลาในการเตรียมการเรื่องนี้ประมาณ 2-3 เดือน และจะพร้อมเริ่มให้บริการได้ในช่วงปลายปีนี้

- <u>แนวทางการจัดอันดับ</u>

  สำนักงานจะเป็นผู้กำหนดกรอบการจัดอันดับ โดยใช้แนวทางซึ่งเป็นที่ยอมรับในระดับสากล และนำมาปรับปรุงให้เหมาะสมกับสภาพแวดล้อมของไทย โดยจะหารือในเรื่องนี้ร่วมกับผู้ที่เกี่ยวข้อง เช่น ตลาดหลักทรัพย์ฯ บริษัทจัดอันดับ สถาบันกรรมการบริษัทไทย (IOD) บริษัทจดทะเบียน และผู้ลงทุน ซึ่งในเบื้องต้น สำนักงานเห็นว่า แนวทางดังกล่าวจะครอบคลุมเรื่องสำคัญ ๆ ดังต่อไปนี้

  - การให้สิทธิและความเป็นธรรมแก่ผู้ถือหุ้น และผู้มีส่วนได้เสียอื่น ๆ เช่น คู่ค้า เจ้าหนี้ เป็นต้น
  - โครงสร้างผู้ถือหุ้น และการกระจายการถือหุ้น
  - โครงสร้างกรรมการ และการบริหารงาน
  - การเปิดเผยข้อมูลที่โปร่งใส (ครบถ้วน เท่าเทียมกัน และทันต่อเหตุการณ์)

- <u>การผลักดันให้ผู้ลงทุนสนใจเรื่องการกำกับดูแลกิจการที่ดี</u>

ในระยะต่อไป เมื่อเริ่มมีบริษัทที่ได้รับการจัดอันดับในเรื่องนี้มากขึ้น สำนักงานมีแนวความคิดที่จะออกข้อกำหนดให้ผู้ลงทุนสถาบันภายใต้การกำกับดูแลของสำนักงาน เช่น กองทุนรวม กองทุนสำรองเลี้ยงชีพ เปิดเผยว่ากองทุนภายใต้การบริหารของบริษัทจัดการต่าง ๆ มีสัดส่วนการลงทุนในบริษัทที่มีการกำกับดูแลกิจการที่ดีมากน้อยเพียงใด นอกจากนี้ สำนักงานจะเผยแพร่และขอความร่วมมือจากผู้ลงทุนสถาบันอื่น ๆ เช่น กองทุนประกันสังคม กองทุนบำเหน็จบำนาญข้าราชการ (กบข.) และบริษัทประกันชีวิต ให้นำเรื่องการกำกับดูแลกิจการที่ดีมาเป็นปัจจัยสำคัญที่ใช้ประกอบการพิจารณาลงทุนในโอกาสต่อไปด้วย ทั้งนี้ มีข้อสังเกตว่า ปัจจุบันผู้ลงทุนสถาบันทั้ง 5 ประเภทที่กล่าวถึงข้างต้น มีมูลค่า port การลงทุนรวมกันกว่า 700,000 ล้านบาท ซึ่งจะมีผลอย่างยิ่งต่อการผลักดันให้บริษัทจดทะเบียนในประเทศไทยมีการกำกับดูแลกิจการที่ดีมากยิ่งขึ้นในอนาคต

<u>ตัวอย่างผลประโยชน์เป็นตัวเงินสูงสุดที่บริษัทที่มีการกำกับดูแลกิจการที่ดีอาจได้รับ</u>

ค่าใช้จ่าย	บริษัทเล็ก		บริษัทกลาง		บริษัทใหญ่
	ทุนชำระแล้ว				
	500 ล้านบาท	1,000 ล้านบาท	2,000 ล้านบาท	5,000 ล้านบาท	10,000ล้านบาท
1. <u>รายปี</u>	**50,000**	**100,000**	**300,000**	**300,000**	**300,000**
2. <u>เมื่อระดมทุน</u>					
2.1 เสนอขายหุ้น					
- ค่าคำขอ	50,000	50,000	50,000	50,000	50,000
- ค่า filing[1/]	160,000	320,000	640,000	1,600,000	3,200,000
- ค่า F/A[2/]	800,000	1,000,000	1,500,000	2,000,000	2,500,000
รวม	**1,010,000**	**1,370,000**	**2,190,000**	**3,650,000**	**5,750,000**
2.2 เสนอขายหุ้นกู้					
- ค่าคำขอ	10,000	10,000	10,000	10,000	10,000
- ค่า filing[3/]	80,000	160,000	320,000	800,000	1,600,000
- ค่า F/A	800,000	1,000,000	1,500,000	2,000,000	2,500,000
รวม	**890,000**	**1,170,000**	**1,830,000**	**2,810,000**	**4,110,000**

<u>หมายเหตุ</u> : ค่าธรรมเนียมรายปี ค่าธรรมเนียมคำขออนุญาต และค่าธรรมเนียม filing คิดเฉพาะค่าธรรมเนียมที่บริษัทต้องจ่ายให้สำนักงาน ก.ล.ต. เท่านั้น

1/ ใช้สมมุติฐานว่า มูลค่าการเสนอขายหุ้น = 40% ของทุนชำระแล้ว ค่า filing ที่บริษัทจะต้องจ่ายให้สำนักงาน ก.ล.ต. จะเท่ากับ 0.08% ของมูลค่าการเสนอขาย

2/ ค่า F/A หมายถึง ค่าที่ปรึกษาทางการเงิน ซึ่งในทางปฏิบัติ ค่าธรรมเนียมดังกล่าวจะแตกต่างกันตามขนาดของบริษัท

3/ ใช้สมมุติฐานว่า มูลค่าการเสนอขายหุ้นกู้ = 80% ของทุนชำระแล้ว ค่า filing ที่บริษัทต้องจ่ายให้สำนักงาน ก.ล.ต. จะเท่ากับ 0.02% ของมูลค่าการเสนอขาย

CobIT Framework Domain	Code	Process	Information Criteria							IT Resources				
			Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	People	Applications	Technology	Facilities	Data
Planning & Organization	PO1	Define a Strategic IT Plan	P	S						Y	Y	Y	Y	Y
	PO2	Define IT Architecture	P	S	S	S					Y			Y
	PO3	Determine Tech. Direction	P	S								Y	Y	
	PO4	Define IT Org. & Relation	P	S						Y				
	PO5	Management IT investment	P	P					S	Y	Y	Y	Y	
	PO6	Communicate Management aims & direction	P					S		Y				
	PO7	Manage Human Resources	P	P						Y				
	PO8	Ensure compliance with external requirements	P					P	S	Y	Y			Y
	PO9	Assess Risks	P	S	P	P	P	S	S	Y	Y	Y	Y	Y
	PO10	Manage Projects	P	P						Y	Y	Y	Y	
	PO11	Manage Quality	P	P		P			S	Y	Y	Y	Y	
Acquisition & Implementation	AI1	Identify Automated Solutions	P	S							Y	Y	Y	
	AI2	Acquire and Maintain Application Software	P	P		S		S	S		Y			
	AI3	Acquire and Maintain Technology Infrastructure	P	P		S						Y		
	AI4	Develop and Maintain Procedures	P	P		S		S	S	Y	Y	Y	Y	
	AI5	Install and accredit Systems	P			S	S			Y	Y	Y	Y	Y
	AI6	Manage Changes	P	P		P	P		S	Y	Y	Y	Y	Y
Delivery & Support	DS1	Define and Manage Services Levels	P	P	S	S	S	S	S	Y	Y	Y	Y	Y
	DS2	Manage third-party Services	P	P	S	S	S	S	S	Y	Y	Y	Y	Y
	DS3	Manage Performance and Capacity	P	P			S				Y	Y	Y	
	DS4	Ensure Continouse Service	P	S			P			Y	Y	Y	Y	Y
	DS5	Ensure Systems Security			P	P	S	S	S	Y	Y	Y	Y	Y
	DS6	Identify and Allocate Costs		P					P	Y	Y	Y	Y	Y
	DS7	Educate and Train Users	P	S						Y				
	DS8	Assist and Advise Customers	P	P						Y	Y			
	DS9	Manage the Configuration	P				S		S		Y	Y	Y	
	DS10	Manage Problems and Incidents	P	P			S			Y	Y	Y	Y	Y
	DS11	Manage Data				P			P					Y
	DS12	Manage Facilities				P	P						Y	
	DS13	Manage Operations	P	P		S	S			Y	Y	Y	Y	Y
Monitoring	M1	Monitor the Processes	P	P	S	S	S	S	S	Y	Y	Y	Y	Y
	M2	Assess Internal Control Adequacy	P	P	S	S	S	P	S	Y	Y	Y	Y	Y
	M3	Obtain Independent Assurance	P	P	S	S	S	P	S	Y	Y	Y	Y	Y
	M4	Provide for Independent Audit	P	P	S	S	S	P	S	Y	Y	Y	Y	Y

ThaiCERT Thai Computer Emergency Response Team **ThaiCERT: Thai Computer Emergency Response Team**

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย

ตัวอย่างระเบียบ

ว่าด้วยการใช้งานระบบเครือข่ายคอมพิวเตอร์ขององค์กรอย่างปลอดภัย

ด้วย(หน่วยงาน / บริษัท / ห้าง / ร้าน).....ได้จัดให้มีเครือข่ายคอมพิวเตอร์ขึ้น เพื่ออำนวยความสะดวกแก่พนักงานในการปฏิบัติงานให้แก่องค์กร ดังนั้น เพื่อให้การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์ในลักษณะที่ไม่ถูกต้อง เห็นสมควรวางระเบียบไว้ดังต่อไปนี้

บทที่ 1 คำนิยาม

"องค์กร" หมายความว่า ชื่อ (หน่วยงาน / บริษัท / ห้าง / ร้าน).....

"เครือข่ายคอมพิวเตอร์" หมายความถึง เครือข่ายคอมพิวเตอร์ขององค์กร.....

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างขององค์กร / บริษัท / ห้าง / ร้าน

"พนักงาน" หมายความว่า พนักงานและลูกจ้างขององค์กร / บริษัท / ห้าง / ร้าน รวมถึงบุคคลอื่นที่องค์กรมอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ

"ข้อมูล" หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง ข้อมูล หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"ผู้ดูแลเครือข่ายคอมพิวเตอร์" หมายความถึง พนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

บทที่ 2 กำหนดอำนาจหน้าที่ของคณะกรรมการหรือผู้ดูแลความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

ให้มี "คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์" ที่ผู้บังคับบัญชาแต่งตั้งจากพนักงานขององค์กร โดย คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์มีอำนาจหน้าที่ดังต่อไปนี้

- กำกับดูแลและให้คำแนะนำเกี่ยวกับการปฏิบัติงานของผู้ดูแลเครือข่ายคอมพิวเตอร์ในการปฏิบัติตามระเบียบนี้
- ให้คำปรึกษาแก่ผู้ดูแลเครือข่ายคอมพิวเตอร์เกี่ยวกับการปฏิบัติตามระเบียบนี้
- ให้คำแนะนำและคำเสนอแนะต่อผู้บังคับบัญชาในการกำหนดนโยบายและมาตรการเกี่ยวกับการรักษาความปลอดภัยของข้อมูล
- จัดทำรายงานเกี่ยวกับการปฏิบัติตามระเบียบนี้เสนอผู้บังคับบัญชาเป็นครั้งคราวตามความเหมาะสม
- ปฏิบัติหน้าที่อื่นตามที่กำหนดไว้ในระเบียบนี้
- ดำเนินการเรื่องอื่นตามที่ผู้บังคับบัญชามอบหมาย

บทที่ 3 ข้อปฏิบัติของพนักงานในการใช้งานเครือข่ายคอมพิวเตอร์

ข้อ 1 พนักงานมีสิทธิใช้เครือข่ายคอมพิวเตอร์ได้ภายใต้ข้อกำหนดแห่งระเบียบนี้

การฝ่าฝืนข้อกำหนดดังกล่าวในวรรคหนึ่ง และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กรจะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่พนักงานที่ฝ่าฝืนตามความเหมาะสมต่อไป

ข้อ 2 พนักงานพึงใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ เช่น ไม่ download ไฟล์ที่มีขนาดใหญ่โดยไม่จำเป็น และไม่ควรปฏิบัติในระหว่างเวลาทำงานซึ่งมีการใช้เครือข่ายอย่างหนาแน่น

ข้อ 3 พนักงานพึงใช้ข้อความสุภาพ และถูกต้องตามธรรมเนียมปฏิบัติในการใช้เครือข่าย อาทิ เช่น ไม่ใช้การส่ง mail แบบกระจายถึงทุกคนที่เป็นสมาชิกเครือข่ายโดยไม่จำเป็น หรือ การใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น เป็นต้น

ข้อ 4 พนักงานมีหน้าที่ระมัดระวังความปลอดภัยในการใช้เครือข่าย โดยเฉพาะอย่างยิ่งไม่ยอมให้บุคคลอื่นเข้าใช้เครือข่ายคอมพิวเตอร์จากบัญชีผู้ใช้ของตนเอง

ข้อ 5 เพื่อประโยชน์ในการใช้รหัสผ่านส่วนบุคคล พนักงานจะต้อง

- ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้งานเครื่องคอมพิวเตอร์ที่พนักงานครอบครองใช้งานอยู่ ทั้งในระดับ BIOS และระดับระบบปฏิบัติการ (Operating System) โดยรหัสผ่านส่วนบุคคลดังกล่าวต้องมีความยาวไม่น้อยกว่า 6 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
- ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่พนักงานครอบครองอยู่
- ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

ข้อ 6 พนักงานจะต้องไม่ใช้เครือข่ายคอมพิวเตอร์โดยมีวัตถุประสงค์ดังต่อไปนี้

- เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น
- เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
- เพื่อการพาณิชย์
- เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติให้แก่องค์กร ไม่ว่าจะเป็นข้อมูลขององค์กร หรือขององค์กร หรือบุคคลภายนอกก็ตาม
- เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาขององค์กร หรือของบุคคลอื่น
- เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว
- เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่องค์กร เช่น การรับหรือส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ หรือการรับหรือส่งข้อมูลที่ได้รับจากบุคคลภายนอกอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่นไปยังพนักงานหรือบุคคลอื่น เป็นต้น
- เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ขององค์กร หรือของพนักงานอื่นขององค์กร หรือเพื่อให้เครือข่ายคอมพิวเตอร์ขององค์กร ไม่สามารถใช้งานได้ตามปกติ
- เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานขององค์กรไปยังที่อยู่เว็บ (web site) ใด ๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง
- เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายแก่องค์กร

ข้อ 7 เพื่อความปลอดภัยในการใช้เครือข่ายคอมพิวเตอร์โดยส่วนรวม พนักงานจะต้อง

- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนเครือข่ายคอมพิวเตอร์ เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาก่อน
- ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ส่วนบุคคลขององค์กร เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนั้นหรือเครือข่ายคอมพิวเตอร์ขององค์กร ได้
- ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องบริการ (server) ที่ต้องใช้งานตลอด 24 ชั่วโมง
- ตรวจสอบข้อมูลที่ได้รับจากภายนอกองค์กร ทุกครั้งด้วยโปรแกรมคอมพิวเตอร์สำหรับตรวจสอบและกำจัดไวรัสคอมพิวเตอร์ที่องค์กร จัดให้ และหากตรวจพบไวรัสคอมพิวเตอร์ฝังตัวอยู่ในข้อมูลส่วนใดจะต้องรีบจัดการทำลายไวรัสคอมพิวเตอร์หรือข้อมูลนั้นโดยเร็วที่สุด
- ลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ส่วนบุคคลของตนเพื่อเป็นการประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล
- ใช้โปรแกรมคอมพิวเตอร์ที่มีการเข้ารหัสข้อมูลซึ่งองค์กร จัดให้สำหรับใช้ในการติดต่อกับเครือข่ายคอมพิวเตอร์จากภายนอกสถานที่ทำการขององค์กร
- ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์ หรือคณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลของพนักงานและเครือข่ายคอมพิวเตอร์ รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา ผู้ดูแลเครือข่ายคอมพิวเตอร์ หรือคณะกรรมการดังกล่าวด้วย
- ระมัดระวังการใช้งานและสงวนรักษาเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์เหมือนเช่นบุคคลทั่วไปจะพึงปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครือข่ายคอมพิวเตอร์ แล้วแต่กรณี
- ไม่เข้าไปในสถานที่ตั้งของระบบเครือข่ายคอมพิวเตอร์ก่อนได้รับอนุญาต

- คืนทรัพย์สินอันเกี่ยวข้องกับการใช้งานเครือข่ายคอมพิวเตอร์ที่เป็นขององค์กร เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้าหรือออก ฯลฯ ให้แก่องค์กร รวมทั้งขอรับข้อมูลส่วนบุคคลที่อยู่บนเครือข่ายคอมพิวเตอร์คืนจากองค์กรภายในกำหนด 7 วันนับแต่วันพ้นสภาพการเป็นพนักงาน

บทที่ 4 ข้อปฏิบัติของผู้ดูแลเครือข่ายคอมพิวเตอร์

ข้อ 1 ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องดูแลรักษาและปรับปรุงเครือข่ายคอมพิวเตอร์เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งจะต้องสอดส่องดูแลการใช้เครือข่ายคอมพิวเตอร์ของพนักงานเพื่อให้เป็นไปตามระเบียบนี้

หากผู้ดูแลเครือข่ายคอมพิวเตอร์พบว่าพนักงานผู้ใดมีพฤติการณ์ส่อไปในทางที่จะละเมิดข้อกำหนดการใช้เครือข่ายคอมพิวเตอร์แห่งระเบียบนี้ ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องรายงานให้คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปทราบโดยเร็วที่สุด และในกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นแก่องค์กร ผู้ดูแลเครือข่ายคอมพิวเตอร์มีอำนาจในการระงับการใช้งานเครือข่ายคอมพิวเตอร์ของพนักงานดังกล่าวได้ทันที

ข้อ 2 ผู้ดูแลเครือข่ายคอมพิวเตอร์มีหน้าที่ในการเสนอความเห็นและข้อสังเกตต่อคณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ตลอดจนผู้บังคับบัญชาที่เหนือขึ้นไปเพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารเครือข่ายคอมพิวเตอร์ หรือปฏิบัติหน้าที่อื่นที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ตามที่ผู้บังคับบัญชามอบหมาย

ข้อ 3 ผู้ดูแลเครือข่ายคอมพิวเตอร์มีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัสข้อมูลอัตโนมัติหรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ

ข้อ 4 ผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และจะต้องไม่เปิดเผยข้อมูลที่ตน

ได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลเครือข่ายคอมพิวเตอร์ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ

ข้อ 5 เมื่อผู้ดูแลเครือข่ายคอมพิวเตอร์จะต้องคืนทรัพย์สินอันเกี่ยวข้องกับการปฏิบัติหน้าที่ของตนที่เป็นขององค์กร เช่น ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว บัตรผ่านเข้า-ออก ฯลฯ ให้แก่องค์กร ในทันทีที่พ้นหน้าที่ และให้คณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ดำเนินการตรวจสอบการคืนทรัพย์สินของผู้ดูแลเครือข่ายคอมพิวเตอร์ที่พ้นจากหน้าที่โดยละเอียดเพื่อความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์

ข้อ 6 ผู้ดูแลเครือข่ายคอมพิวเตอร์ที่ฝ่าฝืนข้อกำหนดในระเบียบนี้ และก่อหรืออาจก่อให้เกิดความเสียหายแก่องค์กร หรือบุคคลหนึ่งบุคคลใด องค์กร จะพิจารณาดำเนินการทางวินัยและทางกฎหมายแก่ผู้ดูแลเครือข่ายคอมพิวเตอร์นั้นตามความเหมาะสมต่อไป

คำแนะนำเบื้องต้นจากศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย

ThaiCERT : Thai Computer Emergency Response Team)

ให้แนวทางในการรักษาความปลอดภัยและโครงสร้างของการรักษาความปลอดภัย เพื่อสามารถช่วยให้เริ่มจัดทำการรักษาความปลอดภัยระบบสารสนเทศเป็นอย่างน้อยที่ควรจะมี ให้กับเครือข่ายขององค์กร 5 ขั้นตอนดังนี้

1. ปกป้องทรัพย์สินที่มีค่าที่สุด

ส่วนแรกที่ต้องมุ่งเน้นคือการป้องกันระบบที่มีข้อมูลซึ่งเป็นสมบัติมีค่าที่สุดก่อน เช่น บริษัทหนึ่งมีเครื่องเซิร์ฟเวอร์ที่เป็น NT มากกว่า 60 เครื่อง อย่างไรก็ตามข้อมูลทางการเงิน ข้อมูลของลูกค้าและข้อมูลของพนักงานอยู่ในเครื่องเซิร์ฟเวอร์ที่เป็น UNIX เพียง 2 เครื่องเท่านั้น ดังนั้นในกรณีนี้จึงเป็นเรื่องที่รู้กันอยู่แล้วว่าควรจะมุ่งเน้นไปที่ระบบเซิร์ฟเวอร์ที่เป็น UNIX ก่อนที่จะจัดการกับระบบ NTสำหรับการทำให้มีระบบ NT print server ที่ปลอดภัยที่สุดก็เป็นการดี

แต่สิ่งแรกที่ต้องให้ความสำคัญก็คือการหยุดระบบธุรกิจที่สำคัญของเครือข่าย ซึ่งควรจะปรึกษากับฝ่ายบริหาร ก่อนว่าระบบใดที่สำคัญที่สุดในมุมมองทางธุรกิจ

2. ปกป้องที่บริเวณรอบๆ

ต้องมั่นใจว่าจุดใดเป็นจุดที่เข้าถึงเครือข่ายของระบบสารสนเทศ และทำการป้องกันจุดเหล่านั้นแล้ว โดยทั่วไปมีการเลือกใช้เทคโนโลยีมาช่วยอยู่ 2 ชนิด คือ

Firewalls: การติดตั้งไฟล์วอลล์ที่ถูกตั้งค่าไว้อย่างถูกต้องเหมาะสม (ไม่ใช่ค่าที่ถูกตั้งไว้โดย default) และควรกำหนดเส้นทาง (route) ของจุดเชื่อมต่อไปยังเครือข่ายภายนอกที่จะเข้ามายังไฟล์วอลล์ให้มากที่สุดเท่าที่จะเป็นไปได้ เพื่อความแน่ใจว่าการเชื่อมต่อเหล่านั้นถูกป้องกันแล้ว

Intrusion Detection Systems: ส่วนเสริมสำหรับไฟล์วอลล์ก็คือระบบตรวจจับการบุกรุก (Intrusion Detection System) ซึ่งเป็นเครื่องมือสำคัญมากที่สามารถตรวจดูเครือข่ายได้ว่ามีกิจกรรมน่าสงสัยเกิดขึ้นหรือไม่ และจะแจ้งเตือน (alert) คุณเมื่อมีการทำ access compromise เกิดขึ้น ในเอกสารเผยแพร่หัวข้อ Intrusion Detection Systems ของหน่วยงาน NIST ระบุว่าระบบตรวจจับการบุกรุกมีด้วยกัน 3 ชนิดซึ่งแต่ละชนิดมีข้อดีและข้อเสียแตกต่างกัน ระบบทั้ง 3 นั้นได้แก่

- Network-based IDSs
- Host-based IDSs
- Application-based IDS

มีหลายบริษัทที่เสนอขายระบบตรวจจับการบุกรุกซึ่งมีทั้งดีและไม่ดี จึงควรศึกษารายละเอียดและวางแผนให้ดีก่อนที่จะใช้

3. การป้องกันระบบภายในที่สำคัญ

หลังจากที่ทำการป้องกันที่ระบบสำคัญและบริเวณรอบๆเครือข่ายแล้ว ขั้นตอนต่อไปคือ การป้องกันระบบภายในที่สำคัญ (core/internal systems) หลักสำคัญคือค่า default ของการติดตั้งระบบใดๆก็ตามนั้นมักไม่มีความปลอดภัยเลย

- **Microsoft Windows NT/2000**
  - Service Packs and hotfixes ติดตาม service packs และ hotfixes ใหม่ๆอยู่เสมอ
  - Hardening your system ค่า default ของการติดตั้งไม่มีความปลอดภัยเลย ถ้าติดตั้งเซิร์ฟเวอร์ใหม่ ต้องระบุหน้าที่ของเครื่องให้ชัดเจน แล้วปิดหรือยกเลิกการติดตั้งบริการใดๆ หรือพอร์ตใดๆที่ไม่จำเป็น แต่ต้องมั่นใจว่าได้ปรับเปลี่ยนให้ตรงกับความต้องการเฉพาะ
  - Auditing เพื่อให้มั่นใจว่าไม่มีการกระทำที่ไม่ได้รับอนุญาตใดๆเกิดขึ้นในระบบขจึงต้องทำการ enable auditing ไม่ว่าจะเป็นการตรวจจับการกระทำที่ไม่ได้รับอนุญาตหรือเป็นเพียงการแจ้งแก่ผู้ใช้ระบบว่า เครื่อข่ายไม่ได้ลบไฟล์ให้ก็ตาม และจะต้องทำการ enable auditing สำหรับเหตุการณ์ต่างๆเช่น การสร้าง/ลบไฟล์, การล็อกอินผิด, การพยายามเข้าถึงไดเรกทอรีที่ไม่ได้รับอนุญาต เป็นต้น แต่การ audit จะไม่ให้ผลดีเลยถ้าไม่คอยหมั่นตรวจสอบและพิจารณาดู audit logs สม่ำเสมอ
  - Password and account policies หนึ่งในวิธีการหลากหลายที่ผู้บุกรุกมักจะใช้เข้าถึงเครือข่ายคือการแอบใช้ชื่อบัญชีและรหัสผ่านของผู้ใช้ของระบบ ดังนั้นควรบังคับให้มีการตั้งรหัสผ่านและมีนโยบายที่รัดกุมเพื่อลดโอกาสของผู้บุกรุกที่

จะเข้าถึงเครือข่าย วิธีหนึ่งที่จะช่วยลดโอกาสที่จะมีใครขโมยหรือเดารหัสผ่านได้ ก็คือการทำ account lockout ซึ่งจะล็อคชื่อบัญชีของผู้ใช้นั้นถ้ามีการเข้ามาด้วยรหัสผ่านที่ผิดด้วยจำนวนครั้งที่กำหนดไว้ โดยวิธีการนี้จะช่วยป้องกันการโจมตีที่เรียกว่า brute-force password attack ได้

- Vulnerability scanners มีเครื่องมือจำนวนมากในท้องตลาดที่ช่วยให้ระบุได้ว่าจุดไหนที่มีความอ่อนแอในระบบเครือข่าย scanner เหล่านี้สามารถดูได้ว่าระบบทำการ update แล้วหรือไม่ ระบุได้ว่ามีพอร์ตอะไรบ้างที่เปิดอยู่ซึ่งอาจถูกบุกรุกได้ และข้อมูลอื่นๆขึ้นอยู่กับชนิดของ scanner ที่ใช้ การแก้ปัญหาเหล่านี้สามารถทำได้โดยเพียงแค่ติดตั้ง Service Packs, hotfixes ที่ออกมาใหม่อย่างสม่ำเสมอและทำการ disable บริการและพอร์ตที่ไม่จำเป็น

- **UNIX:**

  มีหลายวิธีที่คุณสามารถป้องกันระบบ UNIX จากภัยชนิดนี้ เช่น

  - บังคับใช้รหัสผ่านที่แข็งแรง
  - รักษากฎหรือนโยบายเกี่ยวกับรหัสผ่านให้เคร่งครัด (เช่น การหมดอายุของรหัสผ่าน เป็นต้น)
  - ใช้ไฟล์ shadow ซึ่งเป็นการเก็บรหัสผ่านที่เข้ารหัสไว้ในไฟล์ที่แยกจากไฟล์รหัสผ่านที่เป็น default อยู่แล้ว (/etc/passwd)

ขั้นตอนอื่นๆนอกเหนือจากการทำให้ระบบความปลอดภัยของทั้ง UNIX และ NT มีความแข็งแรงขึ้นแล้วยังมีการกำจัดพอร์ตของ IP service

- **Desktops:**

  หลักสำคัญที่จะต้องมุ่งเน้นคือการตั้งค่าให้ระบบปิดการแชร์ไฟล์และเครื่องพิมพ์ (file and print sharing) การทำ disable เหล่านี้ เป็นการป้องกัน desktops จากการ broadcast ซึ่งเป็นการเปิดเผยให้ผู้อื่นรู้ ตัวตนซึ่งอาจทำให้ถูกโจมตีได้ง่าย ต้องมีการติดตั้งและปรับปรุง service packs, hotfixes,ระบบความปลอดภัยอื่นๆให้ทันสมัยอยู่เสมอ ติดตั้งและคอยดูแลซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอยู่เสมอ

4. สร้างเครือข่ายที่ง่ายไม่ซับซ้อน

ตามหลักการแล้ว ระบบเครือข่ายที่ไม่มีความซับซ้อนจะสามารถจัดการและทำการรักษาความปลอดภัยได้ง่ายกว่าเครือข่ายที่ยุ่งยากซับซ้อน มีตัวอย่างบริษัทหนึ่งที่เชื่อมต่ออินเทอร์เน็ตโดยผ่านไฟล์วอลล์ที่แตกต่างกันถึง 3 ชนิด (Border Manager, Guantlet, และ PIX) ถึงแม้ว่าจะมีบางคนพยายามอ้างว่าการใช้ไฟล์วอลล์ทั้ง 3 ตัวร่วมกันสามารถทำให้ระบบความปลอดภัยมีความเข้มแข็งขึ้น แต่จริงๆแล้วกลับกลายเป็นการรวมความอ่อนแอของระบบเหล่านี้เข้าด้วยกัน เพราะว่าแฮกเกอร์สามารถทำการโจมตีที่จุดที่อ่อนแอที่สุดหรือที่ไหนก็ตามที่ง่ายต่อการบุกรุกเข้าไป ดังนั้นยิ่งถ้าเครือข่ายถูกออกแบบให้ง่ายเท่าไหร่ ก็จะเข้าใจ และสามารถจัดการ รวมทั้งป้องกันมันได้ดีเท่านั้น

5. ศึกษาความรู้เรื่องความปลอดภัยอย่างต่อเนื่อง

เรื่องของการรักษาความปลอดภัยเป็นหัวข้อที่ใหญ่และครอบคลุมถึงสาขาอื่นอีกหลายสาขาจึงเป็นไปไม่ได้ที่คนๆเดียวจะรู้ทุกอย่าง อย่างไรก็ตามคุณควรจะศึกษาและทำความเข้าใจในภัยคุกคามต่างๆ ช่องโหว่ต่างๆ และวิธีแก้ไขปัญหาสำหรับระบบความปลอดภัยของเครือข่ายอย่างต่อเนื่อง

การเริ่มต้นรักษาความปลอดภัยระบบเครือข่ายด้วยขั้นตอน5 ข้อนี้สามารถใช้เป็นจุดเริ่มต้นสำหรับการรักษาความปลอดภัยระบบเครือข่ายได้เป็นอย่างดี ขณะที่ทำตามขั้นตอนเหล่านี้ก็ได้เรียนรู้และเข้าใจระบบความปลอดภัยเพิ่มขึ้น และสามารถแก้ไขปัญหาของจุดที่สำคัญและระบบหลักได้ เป็นการเริ่มต้นอย่างดีเพื่อสร้างระบบเครือข่ายที่มีความปลอดภัยและแข็งแกร่งยั่งยืนต่อไป

การทำ IT AUDIT ในระดับความปลอดภัย C2[9]

Department of Defense Computer Security Center (DoDCSC) หรือศูนย์ความปลอดภัยคอมพิวเตอร์ กระทรวงกลาโหม (สหรัฐอเมริกา) ได้พัฒนา Trusted Computer System Evaluation Criteria (TCSEC) ขึ้นเพื่อใช้เป็นเกณฑ์ในการพิจารณาระบบคอมพิวเตอร์ต่างๆว่ามีความปลอดภัยมากน้อยเพียงใด โดยกระทรวงกลาโหมสหรัฐฯได้อ้างอิงถึงเกณฑ์นี้เพื่อใช้ภายในกระทรวงเอง นอกจากนี้แล้ว TCSEC ยังได้รับการยอมรับกันทั่วไป โดยผู้ใช้และผู้ขายระบบคอมพิวเตอร์และเครือข่ายได้มีการอ้างอิงถึงเกณฑ์นี้กันอย่างแพร่หลายเกณฑ์นี้แบ่งระดับความปลอดภัยของระบบคอมพิวเตอร์เป็น 4 ระดับคือ D, C, B, และ A เรียงตามลำดับจากความปลอดภัยน้อยที่สุดไปถึงความปลอดภัยสูงที่สุด โดยที่ในระดับความปลอดภัย C และ B จะแบ่งออกเป็นระดับความปลอดภัยย่อยๆอีกคือ C1, C2, B1, B2, และ B3

ใน TCSEC ระบุว่าสำหรับระดับความปลอดภัยตั้งแต่ C2 ถึงระดับ A1 นั้น การกระทำต่างๆของผู้ใช้จะต้องสามารถให้มีการ audit ได้ ซึ่งการ audit นี้ก็คือกระบวนการบันทึก, ตรวจสอบ, และวิเคราะห์ทบทวนกิจกรรมที่เกี่ยวข้องกับความปลอดภัยทั้งหลายในระบบ และระดับความปลอดภัย C2 นั้นเป็นที่ยอมรับกันทั่วไปว่ามีความปลอดภัยเพียงพอสำหรับการปฏิบัติงานที่ไม่เกี่ยวข้องกับปฏิบัติการทางทหาร

ในระบบที่มีความปลอดภัยอยู่ในระดับ C2 นั้นผู้ดูแลระบบควรจะสามารถ audit ได้โดยดูจาก identity ของบุคคลหนึ่งๆและควรที่จะ (ไม่จำเป็น--เป็นเพียงคำแนะนำ) สามารถ audit ได้โดยดูจาก identity ของสิ่งหนึ่งๆ

พื้นฐานการ Audit

เราใช้ audit trails (หลักฐานที่สร้างจากกลไกการ audit) ในการตรวจจับและป้องปรามการเจาะเข้ามาในระบบคอมพิวเตอร์และใช้ในการตรวจถึงการใช้งานระบบโดยมิชอบ เราอาจใช้ audit trail ในเหตุการณ์เฉพาะเพียงบางเหตุการณ์หรืออาจใช้ในกิจกรรมทั้งหมดที่เกิดขึ้นบนระบบก็ได้ ทั้งนี้ขึ้นอยู่กับผู้รับผิดชอบในการ audit

---

[9] ที่มา : เอกสารเผยแพร่ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

กลไกการ audit นั้นควรจะบันทึกเหตุการณ์ได้ทั้งในแบบของผู้กระทำ (subject) และผู้ถูกกระทำ (object) (ถึงแม้ว่า TCSEC ไม่ได้ระบุถึงความสามารถในส่วนนี้)

จุดประสงค์ของกลไกการ Audit

กลไกการ audit ของระบบคอมพิวเตอร์นั้นถูกจัดตั้งขึ้นมาด้วยมีจุดประสงค์ด้านความปลอดภัย 5 อย่างด้วยกันคือ

1. กลไกการ audit จะต้องช่วยให้สามารถมีการตรวจสอบวิเคราะห์ถึง

- วิธีการเข้าถึงสู่ object ที่ถูกกระทำแต่ละอย่าง
- ประวัติการเข้าถึงของ process และบุคคลต่างๆ
- การใช้กลไกการป้องกันต่างๆของระบบและประสิทธิภาพของกลไกเหล่านั้น

2. กลไกการ audit จะต้องช่วยให้สามารถค้นพบความพยายามซ้ำแล้วซ้ำเล่าที่จะข้ามผ่านกลไกการป้องกันต่างๆ ทั้งจากผู้ใช้ที่อยู่ภายในและจากบุคคลที่อยู่ภายนอก

3. กลไกการ audit จะต้องช่วยให้สามารถค้นพบการที่ผู้ใช้ใช้ user privilege ที่สูงกว่า privilege ของตนเอง เช่น programmer ใช้ privilege ของ administrator ซึ่งในกรณีนี้ถึงจะไม่มีการข้ามผ่านการควบคุมความปลอดภัยแต่ก็อาจจะสามารถทำให้เกิดการละเมิดความปลอดภัยได้

4. กลไกการ audit จะต้องเป็นตัวป้องปรามผู้ประสงค์ร้ายที่จะเข้ามาพยายามข้ามผ่านกลไกการป้องกันระบบ การที่กลไกการ audit จะสามารถทำหน้าที่ป้องปรามได้นั้นผู้ประสงค์ร้ายจะต้องทราบว่ามีกลไกการ audit ที่ใช้ในการตรวจจับความพยายามที่จะข้ามผ่านกลไกการป้องกันของระบบนี้อยู่

5. กลไกการ audit จะเป็นหลักประกันความมั่นใจของผู้ใช้อีกชั้นหนึ่งว่าความพยายามทั้งหลายที่จะข้ามผ่านกลไกการป้องกันนั้นถูกบันทึกไว้และสามารถตรวจพบได้ ถึงแม้ว่าความพยายามในการข้ามผ่านกลไกการป้องกันนั้นจะประสบผลสำเร็จ ก็ยังสามารถใช้ audit trail เพื่อช่วยในการประเมินความเสียหายและทำให้สามารถควบคุมความเสียหายของระบบได้ดีขึ้น

ผู้ใช้กลไกการ Audit

เราสามารถแบ่งผู้ใช้กลไกการ audit ออกได้เป็นสองกลุ่มคือ กลุ่มแรกประกอบด้วยผู้รับผิดชอบในการ audit ซึ่งเป็นผู้ที่มีหน้าที่ในการจัดการ (administrative) ซึ่งจะเลือกว่าเหตุการณ์ใดในระบบที่ควรจะได้รับการ audit ซึ่งจะตั้ง audit flag เพื่อให้เหตุการณ์เหล่านั้นถูกบันทึกได้ และซึ่งจะวิเคราะห์ audit trail ของเหตุการณ์เหล่านั้น ในบางระบบ หน้าที่ในการ audit นั้นจะรวมเป็นหนึ่งในหน้าที่ของผู้จัดการความปลอดภัยของระบบ (system security administrator) ส่วนในบางระบบ ผู้นี้จะเป็นผู้ดูแลระบบ (system administrator) หรือในบางระบบจะมีผู้ที่มีหน้าที่รับผิดชอบในการ audit โดยเฉพาะ

กลุ่มที่สองของผู้ใช้กลไกการ audit ก็คือผู้ใช้ระบบนั้นๆนั่นเอง ซึ่งประกอบด้วยผู้ดูแล (administrator), ผู้ปฏิบัติงาน (operator), programmer, และผู้ใช้อื่นๆที่เหลือทั้งหมด ผู้ใช้เหล่านี้ถือว่าเป็นผู้ใช้กลไกการ audit เนื่องจากผู้ใช้เหล่านี้และโปรแกรมของผู้ใช้เหล่านี้สร้างเหตุการณ์ที่ถูก audit และนอกจากนี้ยังเนื่องจากว่าผู้ใช้เหล่านี้จะต้องเข้าใจถึงว่ามีกลไกการ audit อยู่ในระบบและเข้าใจว่ากลไกการ audit นี้จะมีผลกระทบอย่างไรต่อตนเอง ซึ่งความเข้าใจทั้งสองนี้เป็นสิ่งสำคัญมาก เพราะหากผู้ใช้ไม่มีความเข้าใจในเรื่องดังกล่าวก็จะทำให้ไม่สามารถบรรลุจุดประสงค์ของกลไกการ audit ที่จะใช้เป็นเครื่องมือในการป้องปรามและเป็นเครื่องช่วยในการให้ความมั่นใจต่อผู้ใช้

ความปลอดภัยของการ Audit

Software ที่ใช้ในการสร้าง audit trail รวมถึงตัว audit trail ที่ถูกสร้างขึ้นมานั้นควรจะได้รับการปกป้องโดยระบบรักษาความปลอดภัยของระบบนั้นและควรจะมีกฎการเข้าถึงที่เข้มงวด กลไกการ audit นั้นควรมีความปลอดภัยดังในหัวข้อต่อไปนี้

1. กลไกการบันทึกเหตุการณ์ควรเป็นส่วนหนึ่งของระบบที่ได้รับการปกป้องและควรจะได้รับการปกป้องจากการแก้ไขหรือการเปิดเผยโดยไม่ได้รับอนุญาต

2. audit trail เองนั้นควรจะได้รับการปกป้องโดยระบบรักษาความปลอดภัยของระบบนั้นนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต (กล่าวคือมีเพียงผู้รับผิดชอบการ audit เท่านั้นที่จะเข้าถึง audit trail ได้) และ audit trail ยังควรจะได้รับการปกป้องจากการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

3. กลไกที่ใช้ในการ เปิด/ปิด กลไกการ audit ควรเป็นส่วนหนึ่งของระบบที่ได้รับการปกป้องผู้ใช้ที่ไม่ได้รับอนุญาตไม่ควรจะเข้าถึงกลไกนี้ได้

อย่างน้อยที่สุด ข้อมูลใน audit trail ควรจะถือว่าเป็นความลับและตัว audit trail ควรถือว่ามีชั้นความลับที่สูงเท่ากับข้อมูลที่มีชั้นความลับสูงที่สุดในระบบนั้นเมื่อตัวกลาง (media บรรจุข้อมูล) ที่บรรจุ audit trail ถูกถอดออกจากระบบแล้วตัวกลางนั้นควรจะได้รับการปกป้องทางกายภาคโดยได้รับการปกป้องเช่นเดียวกันกับข้อมูลที่มีชั้นความลับสูงสุดในระบบนั้น

ความต้องการในการ Audit **ระดับ** C2

เหตุการณ์ที่ควรจะได้รับการ Audit ในระบบที่มีความปลอดภัยอยู่ในระดับ C2 นั้นควรจะมีการ audit เหตุการณ์ต่างๆต่อไปนี้

1. การใช้กลไกการแสดงตัว (identification) และการพิสูจน์ทราบ (authentication)

2. การเพิ่มสิ่งใดสิ่งหนึ่ง (object) เข้าไปยังพื้นที่ของผู้ใช้

3. การลบสิ่งใดสิ่งหนึ่งออกจากพื้นที่ของผู้ใช้

4. การกระทำใดๆที่ผู้ปฏิบัติการ (operators), ผู้ดูแลระบบ (system administrators), และหรือผู้ดูแลความปลอดภัยระบบ (system security administrators) เป็นผู้กระทำ

5. เหตุการณ์ทั้งหมดที่เกี่ยวเนื่องกับความปลอดภัย

6. การสร้างสิ่งที่ถูกพิมพ์ออกมา

ข้อมูลที่ควรได้รับการ Audit

ในระบบที่มีความปลอดภัยอยู่ในระดับ C2 นั้นข้อมูลเหล่านี้ควรได้รับการบันทึกลงบน audit trail

1. วันและเวลาของเหตุการณ์

2. สิ่งชี้บอกที่ชัดเจน (เป็นเอกลักษณ์) ว่าผู้กระทำในเหตุการณ์นั้นเป็นใครหรือกระทำในนามของผู้ใด

3. ชนิดของเหตุการณ์

4. ผลความสำเร็จของเหตุการณ์

5. จุดแรก (เช่น terminal ID) ที่ให้มีการแสดงตัว/พิสูจน์ทราบ

6. ชื่อของสิ่งใดๆ (object) ที่ถูก เพิ่มเข้าไป, เข้าถึง, หรือลบออกจาก พื้นที่ของผู้ใช้

7. รายละเอียดของการแก้ไขต่างๆที่ผู้ดูแลระบบกระทำต่อฐานข้อมูลความปลอดภัยของผู้ใช้/ระบบ

ประวัติผู้เขียน

นาย กฤษฎี ตั้งจิตถนอมสิน

26 มีนาคม พ.ศ. 2507

กรุงเทพมหานคร

กำลังศึกษา วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง