บทที่ 2

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

สำหรับในงานวิจัยนี้ จะใช้แนวความคิดตามมาตรฐานหรือเฟรมเวิร์ค เข้ามาบริหารจัดการในการสร้างนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศภายในองค์การ มาตรฐานในปัจจุบันมีอยู่หลากหลายขึ้นอยู่กับลักษณะข้อมูลและการนำไปใช้ของแต่ละองค์กร แต่สำหรับในกรณีศึกษา องค์การกระจายเสียงและแพร่ภาพสาธารณะจะใช้กรอบแนวความคิดตาม Information Security Management Framework (ISMF) 2.0 และมาตรฐานสากลอย่าง ISO/IEC 27001

กรอบแนวความคิด และทฤษฎี

1. **การรักษาความปลอดภัยทางด้านข้อมูล** (Information Security)

โดยทั่วไป ความปลอดภัย (Security) หมายถึง “ความรู้สึกหรือสถานะที่ปลอดภัย-การปราศจากอันตรายใดๆ” ในมุมมองของผู้บริหารแต่ละท่านความปลอดภัยต้องเกิดจากการวางแผน , การดำเนินงาน , บุคลากร การสั่งการ และการควบคุมที่เหมาะสม โดยจะยกตัวอย่างลักษณะของความปลอดภัยซึ่งประกอบไปด้วย

- การรักษาความปลอดภัยทางด้านกายภาพ (Physical Security) เป็นกลยุทธ์ที่กล่าวถึงการปกป้องบุคคล ทรัพย์สินที่จับต้องได้ และสถานที่ทำงานจากภัยคุกคามที่หลากหลาย เช่น ไฟไหม้ การเข้ามาโดยไม่ได้รับอนุญาต หรือ ภัยธรรมชาติ
- การรักษาความปลอดภัยทางด้านบุคคล (Personal Security) มีความเกี่ยวข้องกับการรักษาความปลอดภัยทางด้านกายภาพซึ่งปกป้องบุคลากรภายในองค์กร
- การรักษาความปลอดภัยในการดำเนินงาน (Operations Security) มุ่งเน้นไปที่การรักษาความสามารถในการดำเนินงานเพื่อให้กิจกรรมขององค์กรไม่สะดุดหยุดชะงัก
- การรักษาความปลอดภัยในการติดต่อสื่อสาร (Communications Security) กล่าวถึงการปกป้องสื่อต่างๆ ,เทคโนโลยี และข่าวสารที่ใช้ติดต่อสื่อสารภายในองค์กร และมีความสามารถในการใช้เครื่องมือนั้นเพื่อให้บรรลุวัตถุประสงค์ขององค์กรอีกด้วย

- การรักษาความปลอดภัยทางด้านเครือข่าย (Network Security) ระบุถึงการปกป้องอุปกรณ์เครือข่าย การเชื่อมต่อ และข่าวสารขององค์กร และความสามารถในการใช้เครือข่ายในการบรรลุภาระในการติดต่อสื่อสารข้อมูลขององค์กร

การรักษาความปลอดภัยทางด้านข้อมูล(Information Security - InfoSec) เป็นการป้องกันข้อมูลและส่วนประกอบที่สำคัญซึ่งรวมถึงระบบงานและอุปกรณ์ที่ถูกใช้กักเก็บหรือ สื่อสารข้อมูล หน่วยงาน US. Government's National Information Assurance Glossary ได้ให้คำนิยามความปลอดภัยทางด้านข้อมูลไว้ว่า "เป็นการป้องกันระบบข้อมูลข่าวสารที่เกิดจากการเข้าใช้โดยไม่ได้รับอนุญาตหรือมีการเปลี่ยนแปลงข้อมูล ในการเก็บ การประมวลผล หรือ การสื่อสาร หรือ ซึ่งรวมถึงการวัดผล ในเรื่องการตรวจตรา และ ต่อต้านต่อภัยคุกคาม" คำนิยามที่เกี่ยวข้องกับความปลอดภัยส่วนใหญ่จะเน้นไปที่การใช้งานที่เฉพาะเจาะจง เช่น การป้องกันการใช้ข้อมูลอิเล็กทรอนิกส์จากผู้ใช้ที่ไม่ได้รับอนุญาต แต่ในความเป็นจริงแล้วเป็นความเข้าใจที่ผิด

องค์ประกอบหลักๆที่ได้รับการยอมรับอย่างกว้างขวางของความปลอดภัยของข้อมูล โดยทั่วไปมักจะพูดถึง C.I.A – Confidentiality, Integrity, Availability คือ

- การรักษาความลับของข้อมูล (Confidentiality) เป็นการทำให้มั่นใจว่าจะมีเพียงผู้ที่ได้รับสิทธิจะเข้าถึงข้อมูลตามขอบเขตของตน ในองค์กรนั้นถือว่าการรักษาความลับของข้อมูลมีความสำคัญมากต่อข้อมูลส่วนบุคคลซึ่งเกี่ยวข้องกับ พนักงาน ลูกค้า หรือ คนไข้ เป็นต้น

- การรักษาบูรณภาพของข้อมูล (Integrity) เป็นลักษณะของการรักษาความสมบูรณ์หรือมีผิดพลาดของข้อมูล ความบูรณภาพของข้อมูลจะถูกคุกคามต่อเมื่อมีการโยกย้ายข้อมูลไปใช้ในทางที่ผิด เกิดความเสียหาย ถูกทำลาย หรือ หยุดชะงักจากเหตุการณ์บางอย่าง

- การรักษาการให้บริการของข้อมูล (Availability) เป็นลักษณะของข้อมูลซึ่งทำให้ผู้ใช้สามารถเข้าถึงข้อมูลโดยปราศจากการแทรกแซงหรือการขัดขวางในทางที่เป็นประโยชน์ ผู้ใช้ในที่นี้อาจจะหมายถึงบุคคลหรือเครื่องคอมพิวเตอร์ก็ได้ การรักษาการบริการของข้อมูลนี้ไม่ใช่กับผู้ใดก็ได้ แต่ต้องเป็นผู้ที่ได้รับสิทธิที่กำหนดเท่านั้น

- การรักษาความเป็นส่วนตัว (Privacy) ข้อมูลที่ได้ถูกรวบรวม ใช้งาน และเก็บไว้ในองค์กรซึ่งถูกใช้สำหรับจุดประสงค์เพื่อเข้าใช้ข้อมูลของผู้เป็นเจ้าของในเวลาซึ่งได้เก็บรวบรวมมา ความหมายของความเป็นส่วนตัวมิได้มุ่งเน้นบนความเป็นอิสระจากการสังเกตการณ์เท่านั้น แต่ยังหมายถึงข้อมูลซึ่งจะถูกใช้สำหรับบุคคลที่มีสิทธิจัดการกับข้อมูลได้เท่านั้น

- การระบุตัวตน (Identification) เป็นกระบวนการในการยอมรับแต่ละราย การระบุตัวตนเป็นขั้นตอนแรกของการเข้าสู่สิ่งที่ได้รับการปกป้อง และนำไปสู่การรับรองตัวตนและการ

ให้สิทธิ การระบุตัวตนและการรับรองตัวตนเป็นหัวใจของการจัดทำระดับของการเข้าถึงหรือการให้สิทธิซึ่งได้รับการอนุญาตเป็นรายๆ การระบุตัวตนเป็นรูปแบบทั่วไปซึ่งนำไปปฏิบัติโดยที่จะหมายถึงการใช้ชื่อผู้ใช้หรือรหัสอื่นๆ

- การรับรองตัวตน (Authentication) จะเกิดขึ้นเมื่อมาตรการควบคุมพิสูจน์ได้ว่าผู้ใช้เป็นเจ้าของรหัสที่ตนเองถือครองเช่น การเข้ารหัสป้องกันการใช้งานอุปกรณ์โดยนำ บัตรรหัสลับมาใช้ร่วมด้วย (Secure ID cards) เพื่อยืนยันการระบุตัวตนของผู้นั้น

- การให้สิทธิ (Authorization) หลังจากการระบุตัวตนของผู้ใช้ซึ่งได้รับการรับรองแล้ว ในขั้นตอนนี้จะเรียกว่าการให้สิทธิ(Authorization) ซึ่งเป็นการประกันว่าผู้ใช้ได้รับสิทธิที่เฉพาะเจาะจงและมีความชัดเจนจากการตรวจสิทธิในการถึง การเปลี่ยนแปลง การลบ เนื้อหาของข้อมูล

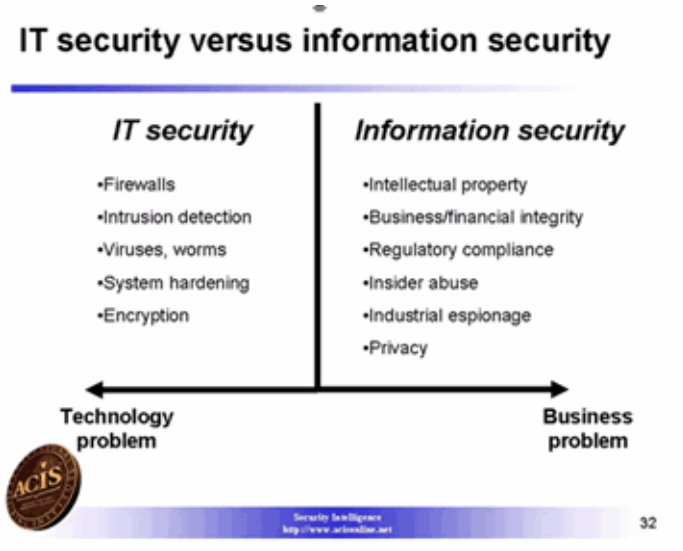
- ความระบุความเป็นเจ้าของในการกระทำ (Accountability) ลักษณะของขั้นตอนนี้จะเกิดขึ้นเมื่อมาตรการควบคุมได้จัดหาสิ่งที่รับประกันว่าทุกๆกิจกรรมที่เกิดขึ้นได้ระบุชื่อผู้ใช้หรือกระบวนการไว้แล้ว

การกำหนดแผนการปฏิบัติการรักษาความปลอดภัยทางด้านข้อมูลที่ประสบความสำเร็จจะต้องประกอบไปด้วยองค์ประกอบที่กล่าวมาข้างต้นซึ่งนำไปใช้ในการลดความเสี่ยงสำหรับทรัพย์สินทางด้านข้อมูล ศิลปะในการบรรลุวัตถุประสงค์ในการลดความเสี่ยงจำเป็นจะต้องมีการสื่อสารและการประสานงานโดยทั่วถึง

2. Information Security Management Framework (ISMF) 2.0

Information Security Management Framework (ISMF) 2.0 เป็นโครงสร้างการจัดการด้านความปลอดภัยสารสนเทศรุ่น 2.0 ซึ่งเป็นรูปแบบการพัฒนาอย่างต่อเนื่องมาจาก ISFM 1.0 โดยโมเดล ISMF Version 2 ได้ปรับมุมมองจาก "IT security" ไปเป็น "Information Security" ซึ่งหมายความว่าได้ปรับมุมมองจากเดิมซึ่งเป็นการเน้นในการแก้ปัญหาด้านเทคโนโลยีและไอทีเป็นหลัก เปลี่ยนไปเป็นการมองถึงปัญหาทางธุรกิจมากขึ้น

ภาพที่ 2.1 การเปรียบเทียบระหว่าง IT Security กับ Information Security



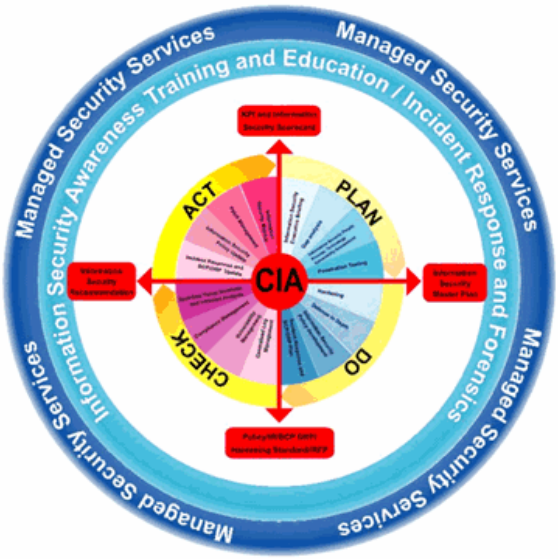
นอกจากนั้นทีมพัฒนา ISMF ยังได้พัฒนาโดยอาศัยหลักของการพัฒนาอย่างต่อเนื่อง (Continuous Improvement) ในการบริหารคุณภาพ (Quality Management) ซึ่งประกอบเป็น 4 แนวความคิดหลัก ประกอบด้วย 1. วางแผน (Plan) 2. ปฏิบัติ (Do) 3. ตรวจสอบ (Check) และ 4. แก้ไข (Act) แต่อย่างไรก็ตามการปรับแนวความคิดด้านการพัฒนาอย่างต่อเนื่องนั้นยังไม่สามารถนำมาใช้ในทางการรักษาความปลอดภัยของข้อมูลได้โดยตรง เนื่องจากแนวคิดด้านการรักษาความปลอดภัยของข้อมูลนั้นไม่ใช่การลดช่องโหว่ลงให้เท่ากับศูนย์ (zero risk) ทั้งนี้เนื่องจากการทำดังกล่าวนั้นอาจทำได้หากแต่ต้องใช้ต้นทุนที่สูงมากจนไม่คุ้มค่า และอาจขัดขวางต่อการทำธุรกิจของบริษัทอีกด้วย ดังนั้นการจัดการด้านรักษาความปลอดภัยของข้อมูลนั้นจึงควรตั้งอยู่บนแนวคิดด้าน Risk Management ซึ่งหมายความว่า การรับมือกับความเสี่ยงหรือความไม่ปลอดภัยของระบบนั้นไม่ใช่การทำได้เพียงแค่ซื้ออุปกรณ์เพิ่มและป้องกันระบบเท่านั้น หากยังมีวิธีการอื่นอีกมากมาย ซึ่งการอยู่เฉยๆไม่ทำอะไรเลย ก็นับเป็นหนึ่งในนั้นด้วย และ ก็นับว่าเป็นสิ่งที่ควรทำในกรณีที่ค่าใช้จ่ายในการป้องกันระบบสูงจนไม่คุ้มกับความเสียหายที่อาจจะเกิดขึ้นเป็นต้น

ภาพที่ 2.2 แนวความคิดด้าน Risk Management

ที่มา http://www.acisonline.com

ดังนั้นโมเดล ISMF version 2 ที่พัฒนาขึ้นจึงได้ยึดแนวความคิดด้าน Risk Management เป็นหลัก ซึ่งสามารถช่วยให้องค์กรสามารถดำเนินการด้านการรักษาความปลอดภัยของข้อมูลได้อย่างเหมาะสม โดยคำนึงถึง Risk Tolerance และ Risk Acceptance เป็นหลัก ซึ่งจะช่วยให้องค์กรได้รับ ROI จากโครงการรักษาความปลอดภัยของข้อมูลได้ในระดับสูงสุด

ภาพที่ 2.3 ขั้นตอนของ Information Security Management Framework (ISMF) 2.0



ที่มา http://www.acisonline.com

โมเดล ISMF version2 นั้นประกอบไปด้วย 4 งานหลัก (Plan, Do, Check, Act ในภาพ 2.3) และแต่ละงานหลักมี 4 งานย่อย (รูปทรงกราฟวงกลมที่อยู่ถัดจากชื่องานหลัก) รวมทั้งหมด 16 งานย่อย โดยแต่ละงานหลักนั้นจะมีลูกศรสีแดงชี้ออกมาซึ่งหมายถึงผลลัพธ์สุดท้ายของแต่ละงานหลัก และองค์ประกอบสุดท้ายคือวงแหวนรอบนอกซึ่งแสดงถึงงานซึ่งจะต้องทำอย่างต่อเนื่องสม่ำเสมอตลอดโครงการไม่จำกัดว่าจะต้องทำในช่วงงานหลักใด สำหรับความหมายและหน้าที่ขององค์ประกอบต่างๆในโมเดล ISMF version 2 นั้นมีรายละเอียดดังนี้

Plan (การวางแผนด้านการรักษาความปลอดภัยของข้อมูล)

มีคำกล่าวที่ว่า “หากต้องการดำเนินการใดๆ อย่างราบรื่น แล้วการวางแผนอย่างรัดกุมนั้นเป็นสิ่งสำคัญที่ขาดไม่ได้" ซึ่งในมุมมองด้านการรักษาความปลอดภัยของข้อมูลก็เช่นกัน การวางแผนที่ดีนั้นจะทำให้ท่านทราบกิจกรรมที่จะต้องทำตลอดทั้งโครงการ โดยมีการคำนึงถึง Risk Management เป็นหลัก ซึ่งจะทำให้ความเข้มของการรักษาความปลอดภัยของข้อมูลนั้นไม่ตึงหรือหย่อนจนเกินไป อยู่ในระดับที่พอเหมาะกับ Risk Tolerance ในขั้นตอนวางแผนนี้ประกอบด้วยงานย่อยทั้งหมด 4 งาน ดังนี้

งานที่ 1 : Information Security Executive Briefing เป็นการเล่าถึง ขั้นตอน ขอบเขต ความต้องการ และข้อจำกัด ของโครงการให้กับผู้บริหารระดับสูงขององค์กร ทั้งนี้เพื่อเป็นการปรับความเข้าใจ ความคาดหวัง เตรียมความพร้อมเพื่อเริ่มโครงการ และเป็นการเก็บข้อมูลด้านธุรกิจขององค์กร เพื่อให้คำแนะนำเกี่ยวกับการตั้งโจทย์หรือเป้าหมายด้านการรักษาความปลอดภัยของข้อมูลขององค์กร ซึ่งอาจจะยึดมาตรฐานต่างๆ เช่น ISO/IEC 17799 (ISO/IEC27001) หรือมาตรฐานที่องค์กรประยุกต์ขึ้นเองก็ได้

งานที่ 2 : Gap Analysis เป็นการตรวจสอบองค์กรโดยการเปรียบเทียบกับมาตรฐานสากล เช่น ISO/IEC 17799 (ISO/IEC27001) ซึ่งจะช่วยให้การวางแผนเพื่อพัฒนาและปรับปรุงความปลอดภัยข้อมูลขององค์กรมีทิศทางที่ชัดเจนยิ่งขึ้น

งานที่ 3 : Information Security People, Process, and Technology Vulnerability Assessment เป็นการตรวจสอบหาช่องโหว่ด้านความปลอดภัยขององค์กรโดยมุ่งเน้นในด้านบุคลากร กระบวนการ และเทคโนโลยี ซึ่งจะช่วยให้ผู้วางแผนได้ทราบข้อมูลจุดอ่อนขององค์กรในเชิงลึก ทำให้สามารถวางแผนได้ตรงความเป็นจริงมากขึ้น

งานที่ 4 : Penetration Testing คือการตรวจสอบด้านการรักษาความปลอดภัยของข้อมูลระดับลึกที่สุด โดยมีการแสดงผลและขั้นตอนในการนำเอาช่องโหว่ที่พบในขั้นตอน Vulnerability Assessment มาใช้ในการเจาะระบบจริง (Ethical Hacking) ซึ่งจะช่วยลด fault positive และเพิ่ม Awareness ให้กับผู้บริหารและผู้ร่วมโครงการได้เป็นอย่างดี

ภายหลังจากดำเนินงานทั้ง 4 งานย่อยข้างต้นแล้ว ผู้ตรวจสอบและผู้ร่วมโครงการจึงสามารถร่วมกันพัฒนาแผนงานด้านการรักษาความปลอดภัยของข้อมูลให้แก่องค์กรได้ ซึ่งแผนดังกล่าวนั้นเรียกว่า "Information Security Master Plan"

DO (การนำแผนที่วางไว้มาปฏิบัติ)

ถึงแม้ว่าจะมีการวางแผนอย่างดีเพียงได้แต่หากปราศจากการดำเนินการอย่างเหมาะสมแล้ว โครงการคงไม่สามารถประสบความสำเร็จได้ ดังนั้นในขั้นตอนนี้จึงมีการนำผลลัพธ์จากขั้นตอนที่ผ่านมาเพื่อใช้เป็นแนวทางปฏิบัติ โดยแบ่งเป็นการทำงานในเชิงเทคนิค และเชิงนโยบาย รวมทั้งสิ้น 4 งานย่อยดังนี้

งานที่ 1 : Hardening เป็นการลดช่องโหว่ของระบบซึ่งเน้นในระดับ Host (Windows/UNIX) และ Network Device (Router, Switching) เป็นหลัก โดยแก้ไขเพื่อลดช่องโหว่ของเครื่องแม่ข่ายในระบบสำคัญๆ

งานที่ 2 : Defense in Depth เป็นการสร้างความปลอดภัยให้แก่ระบบในทุกระดับของระบบ ไม่ว่าจะเป็น DMZ, Network Gateway รวมไปถึง Host และ Application โดยเน้นการเขียนข้อกำหนดและ แนวทางเป็นหลัก

งานที่ 3 : Information Security Policy Development หมายถึงการพัฒนานโยบายด้านการรักษาความปลอดภัยของข้อมูล ซึ่งจะเป็นเส้นทางในการถ่ายทอด requirement ด้านการรักษาความปลอดภัยของข้อมูลขององค์กรมากสู่แนวทางและวิธีการปฏิบัติให้แก่พนักงานทุกคนในองค์กร

งานที่ 4 : Incident Response and BCP/DRP Plan การสร้างแผนจัดการกับเหตุการณ์ที่ไม่คาดฝัน และแผนสำรองฉุกเฉิน เพื่อรับมือกับภัยต่างๆที่อาจจะเกิดขึ้น เพื่อจำกัดความเสียหายให้เหลือน้อยที่สุด

ขั้นตอนที่ 2 นี้จะช่วยให้แผนที่วางไว้สามารถเกิดขึ้นจริงได้ในทางปฏิบัติ ซึ่งผลลัพธ์ของขั้นตอนนี้นั้นจะเป็นเอกสารต่างๆที่เกี่ยวข้องกับการดำเนินงานได้แก่ นโยบายรักษาความปลอดภัย แผนสำรองฉุกเฉิน และเอกสารมาตรฐานด้านความปลอดภัยสำหรับการพัฒนาระบบและเครื่องแม่ข่าย

Check (การตรวจสอบและเฝ้าระวัง)

หลังจากการการวางแผนและการปฏิบัติที่ดี การตรวจสอบและเฝ้าระวังนั้นก็เป็นสิ่งสำคัญที่จะต้องทำในลำดับต่อมา ทั้งนี้เพื่อเป็นการตรวจสอบถึงความสำเร็จของงาน ความยอมรับของพนักงานในองค์กร ช่องโหว่และภัยใหม่ๆที่พบในระบบ เพื่อนำมาใช้ปรับปรุงและแก้ไขนโยบายและนำมาใช้ในการทำงานขั้นตอนต่อไป

งานที่ 1 : Centralized Log Management คือการจัดการ จัดเก็บและรวบรวม Log จากอุปกรณ์ต่างๆไว้ที่ส่วนกลาง เพื่อความสะดวกในการวิเคราะห์ และการเก็บ Log ของระบบตามที่กฎหมายกำหนด

งานที่ 2 : Vulnerability Management เป็นการสร้างระบบบริหารจัดการช่องโหว่ของระบบ ซึ่งจะดำเนินการสแกนระบบและทำรายงานแบบ real-time โดยมีการปรับแต่งให้สร้าง traffic รบกวนระบบน้อยที่สุด นอกจากนั้นยังมีระบบ assign ช่องโหว่ที่พบให้กับบุคลากรต่างๆในองค์กร ซึ่งจะสามารถช่วยให้เกิดการติดตามงานและยังช่วยวัดประสิทธิผลการทำงานของพนักงานแต่ละบุคคลได้ในระดับหนึ่งอีกด้วย

งานที่ 3 : Compliance Management เป็นการจัดการเพื่อให้ผลักให้สิ่งที่เขียนอยู่ในนโยบายรักษาความปลอดภัยสามารถเป็นจริงได้ในทางปฏิบัติ โดยการใช้เครื่องมือในการควบคุมการทำงานและการใช้งานระบบสารสนเทศ นอกจากนั้นยังมีประโยชน์ในการเฝ้าติดตามพฤติกรรมการใช้งานระบบของผู้ใช้งานได้อีกด้วย

งานที่ 4 : Real-time Threat Monitoring and Intrusion Analysis นำผลที่ได้จาก "Centralized Log Management " มาเป็นวัตถุดิบในการวิเคราะห์การใช้งานและภัยที่เกิดขึ้นกับระบบ มีวัตถุประสงค์ในการลด Fault Positive ที่แฝงอยู่ใน Report และ Log จากอุปกรณ์ด้าน Information Security อุปกรณ์ host และ network ต่างๆ

ผลลัพธ์ขั้นตอนนี้เรียกว่า "Information Security Recommendation" เป็นผลสรุปและวิเคราะห์จากงานย่อยต่างๆ และผลลัพธ์นี้เองซึ่งจะนำมาใช้ในเป็นแนวทางในการปรับปรุงโครงการในขั้นตอนต่อไป

Act (การนำข้อข้อเสนอแนะมาใช้ในการปรับปรุงระบบ)

เป็นการนำ "Information Security Recommendation" จากขั้นตอนที่แล้ว มาใช้เพื่อเป็นแนวทางในการปรับแต่งนโยบาย วิธีการปฏิบัติ รวมไปถึงมาตรการต่างๆที่จะออกมาเพื่อให้พนักงานมีความเข้าใจและปฏิบัติตามนโยบาย รวมไปถึงการสร้างเกณฑ์วัดความสำเร็จของของโครงการ

งานที่ 1 : Incident Response and BCP/DRP Update เป็นการนำผลการวิเคราะห์และข้อแนะนำซึ่งเป็น outcome มาจากเฟสที่แล้ว มาใช้ในการปรับปรุงแก้ใช้สร้างแผนจัดการกับเหตุการณ์ที่ไม่คาดฝัน และแผนสำรองฉุกเฉินให้เหมาะสมกับองค์กรมากยิ่งขึ้น

งานที่ 2 : Information Security Policy Update เป็นการปรับปรุงนโยบายรักษาความปลอดภัยขององค์กรให้ทันสมัยและตอบรับกับปัจจัยภายในและภายนอกที่เปลี่ยนแปลงไป

งานที่ 3 : Patch Management เป็นบริหารจัดการ Patch ย่างเป็นขั้นตอน โดยมีการทดสอบความถูกต้องของไฟล์ patch มีการโหลด patch และดำเนินการติดตั้งโดยใช้ bandwidth น้อยที่สุด รวมไปถึงการ rollback อย่างมีประสิทธิผล

งานที่ 4 : Information Security Metrics หมายถึงการวิเคราะห์หาเกณฑ์วัดผลสำเร็จของการทำงานด้านการรักษาความปลอดภัยของข้อมูล

ผลลัพธ์สำคัญที่สุดของขั้นตอนนี้นั้นเรียกว่า "KPI and Information Security Scorecard" ซึ่งเป็นการนำเกณฑ์ตรวจวัดมาใช้ในการการวัดผลออกมาเป็น KPI ขององค์กร เพื่อใช้เป็นแนวทางในการตั้งเป้าหมายในการจัดทำโครงการรักษาความปลอดภัยของข้อข้อมูลในโครงการรอบต่อไป

สิ่งที่ต้องทำอย่างสม่ำเสมอตลอดโครงการ

งานในส่วนนี้จะอยู่ในวงแหวนรอบนอกของโมเดล ISMF version 2 ซึ่งเป็นงานจำเป็นที่จะต้องทำอย่างต่อเนื่องตลอดทั้งโครงการ ประกอบด้วยงานทั้งหมด 3 หัวข้อย่อยได้แก่

งานที่ 1 : Information Security Awareness Training and Education เป็นการจัดฝึกอบรบเพื่อเพิ่มความรู้และความตระหนักถึงความสำคัญของการรักษาความปลอดภัยให้แก่บุคลากรทุกระดับในองค์กร ซึ่งจะช่วยให้การบริหารจัดการด้าน "Information Security" ในองค์กรนั้นเป็นไปได้อย่างสะดวกมากขึ้น

งานที่ 2 : Incident Response and Forensics เป็นการเตรียมความพร้อมรับสิ่งที่ไม่คาดฝันอยู่เสมอ และ วิเคราะห์ต้นเหตุของปัญหา (Root-cause Analysis) จากวิธี Digital Forensics

งานที่ 3 : Managed Security Services หมายถึง การ Outsource เฝ้าระวังโดยการวิเคราะห์ Log ด้วยบุคลากรผู้เชี่ยวชาญจากภายนอก การเฝ้าระวังโดยการวิเคราะห์ Log ด้วยบุคลากรภายในองค์กรของเราเองนั้น นอกจากจะใช้เวลาค่อนข้างมากแล้วยังต้องการผู้เชี่ยวชาญที่แยกแยะระหว่าง Fault Alarm กับ Real Attack Alarm ซึ่งผู้เชี่ยวชาญต้องมีความชำนาญเป็นพิเศษด้านการวิเคราะห์การบุกรุกระบบ (Intrusion Analyst) ตลอดจนในปัจจุบันค่าตัวของบุคลากรที่มีความเชี่ยวชาญดังกล่าวก็ค่อนข้างสูงอยู่พอสมควร

จากปัญหาดังกล่าวจึงเกิดแนวคิดในการ "Outsource" ด้านการจัดการระบบรักษาความปลอดภัยซึ่งเรียกว่า "Managed Security Services" หรือ "MSS" การจัดจ้าง Outsource ด้าน Security โดยเฉพาะ เป็นแนวคิดที่ต้องการให้ Outsource มาช่วยในการจัดการบริหารความเสี่ยง และ ช่วยลดความเสี่ยงให้กับระบบโดยรวม (Risk Management and Risk Mitigation)

โมเดล ISFM Version 2 แสดงถึงการทำงานอย่างต่อเนื่อง และมีการทำแบบวนเป็นรอบซึ่งจะช่วยให้งานด้านการรักษาความปลอดภัยของข้อมูลนั้นสามารถพัฒนาอย่างต่อเนื่องบนพื้นฐานของ Risk Management และสำหรับบทความในตอนต่อไปนั้นจะเป็นการอธิบายลงรายละเอียดในแต่ละขั้นตอน ซึ่งจะช่วยให้คุณสามารถเข้าในวิธีการทำงานด้านการรักษาความปลอดภัยของข้อมูลได้อย่างถูกต้องมากยิ่งขึ้น

3. มาตรฐาน ISO/IEC 27001

เป็นมาตรฐานที่เกี่ยวกับการจัดการในเรื่องความปลอดภัยของข้อมูล ได้รับการพัฒนามาจาก Information Security Management Standard BS7799 ออกโดย British Standard Institute (BSI) ซึ่งมาตรฐานนี้เป็นส่วนหนึ่งของมาตรฐาน ISO (International Standard Organization) ที่ถูกกำหนดเพื่อเป็นแนวทางการจัดการด้านความปลอดภัยของข้อมูลภายในองค์กร โดยมีการกำหนดแนวทางสำหรับองค์กรในด้านการปฏิบัติงาน การจัดการเพื่อให้เกิดประสิทธิภาพ การพัฒนามาตรฐานความปลอดภัย เพื่อการสร้างความมั่นใจในการเชื่อมโยงระหว่างองค์กร เนื่องจากข้อมูลขององค์กรถือว่าเป็นสินทรัพย์ที่มีความสำคัญ ดังนั้น การรักษาความปลอดภัยของข้อมูล , การวิเคราะห์และการบริหารความเสี่ยงที่อาจเกิดขึ้นจึงถือเป็นสิ่งที่สำคัญในการบริหารงานองค์กรให้มีประสิทธิภาพ

มาตรฐาน ISO/IEC 27001 จะประกอบไปด้วย 11 หมวด ดังต่อไปนี้

หมวดที่ 1 : นโยบายความมั่นคงปลอดภัย (Security policy)

1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy)

มีจุดประสงค์เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

1.1.1 เอกสารนโยบายความมั่นคงปลอดภัยที่เป็นลายลักษณ์อักษร (Information security policy document)

(ผู้บริหารองค์กร) ต้องจัดทำนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรอย่างเป็นลายลักษณ์อักษร เอกสารนโยบายต้องได้รับการอนุมัติจากผู้บริหารขององค์กรก่อนนำไปใช้งาน และต้องเผยแพร่ให้พนักงานและหน่วยงานภายนอกทั้งหมดที่เกี่ยวข้องได้รับทราบ

1.1.2 การทบทวนนโยบายความมั่นคงปลอดภัย (Review of the information security policy)

(ผู้บริหารองค์กร) ต้องดำเนินการทบทวนนโยบายความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อองค์กร

หมวดที่ 2 : โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร (Internal organization) มีจุดประสงค์เพื่อบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

2.1.1 การให้ความสำคัญของผู้บริหารและการกำหนดให้มีการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management commitment to information security)

(ผู้บริหารองค์กร) ต้องให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัย โดยมีการกำหนดทิศทางที่ชัดเจน การกำหนดคำมั่นสัญญาที่ชัดเจนและการปฏิบัติที่สอดคล้อง การมอบหมายงานที่เหมาะสมต่อบุคลากร และการเล็งเห็นถึงความสำคัญของหน้าที่และความรับผิดชอบในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศ

2.1.2 การประสานงานความมั่นคงปลอดภัยภายในองค์กร (Information security coordination)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีตัวแทนพนักงานจากหน่วยงานต่างๆ ภายในองค์กรเพื่อประสานงานหรือร่วมมือกันในการสร้างความมั่นคงปลอดภัยให้กับสารสนเทศขององค์กร โดยที่ตัวแทนเหล่านั้นจะมีบทบาทและลักษณะงานที่รับผิดชอบที่แตกต่างกัน

2.1.3 การกำหนดหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัย (Allocation of information security responsibilities)

(ผู้บริหารสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบของพนักงานในการดำเนินงานทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กรไว้อย่างชัดเจน

2.1.4 กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ (Authorization process for information processing facilities)

(ผู้บริหารสารสนเทศ) ต้องกำหนดกระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศใหม่และบังคับให้มีการใช้งานกระบวนการนี้

2.1.5 การลงนามมิให้เปิดเผยความลับขององค์กร (Confidentiality agreements)

(หัวหน้างานบุคคล) ต้องจัดให้มีการลงนามในข้อตกลงระหว่างพนักงานกับองค์กรว่าจะไม่เปิดเผยความลับขององค์กร (โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างพนักงานนั้น) รวมทั้งเงื่อนไขหรือข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับจะต้องได้รับการปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับความต้องการขององค์กร

2.1.6 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with authorities)

(ผู้บริหารสารสนเทศ) ต้องมีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่นๆ เช่น สำนักงานตำรวจแห่งชาติ สภาความมั่นคงแห่งชาติ บมจ. ทศท คอร์ปอเรชั่น บมจ. กสท โทรคมนาคม ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

2.1.7 การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)

(ผู้บริหารองค์กรและหัวหน้างานสารสนเทศ) ต้องมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่างๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่ความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ หรือสมาคมต่างๆ ในอุตสาหกรรมที่องค์กรมีส่วนร่วม

2.1.8 การทบทวนด้านความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระ (Independent review of information security)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศโดยผู้ตรวจสอบอิสระตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่มีความสำคัญมากต่อองค์กร

2.2 โครงสร้างทางด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับลูกค้าหรือหน่วยงานภายนอก (External parties)

มีจุดประสงค์เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กรที่ถูกเข้าถึง ถูกประมวลผล หรือถูกใช้ในการติดต่อสื่อสารกับลูกค้าหรือหน่วยงานภายนอก

2.2.1 การประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก (Identification of risks related to external parties)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการประเมินความเสี่ยงอันเกิดจากการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลสารสนเทศโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.2.2 การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคง

ปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security when dealing with customers)

(หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร เมื่อมีความจำเป็นต้องให้ลูกค้าหรือผู้ใช้บริการเข้าถึงสารสนเทศหรือทรัพย์สินสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

2.2.3 การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร (Addressing security in third party agreements)

(หัวหน้างานสารสนเทศ) ต้องระบุและจัดทำข้อกำหนดหรือข้อตกลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศระหว่างองค์กรและหน่วยงานภายนอก เมื่อมีความจำเป็นต้องให้หน่วยงานนั้นเข้าถึงสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศขององค์กร ก่อนที่จะอนุญาตให้สามารถเข้าถึงได้

หมวดที่ 3 การบริหารจัดการทรัพย์สินขององค์กร (Asset management)

3.1 หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร (Responsibility for assets)

มีจุดประสงค์เพื่อป้องกันทรัพย์สินขององค์กรจากความเสียหายที่อาจเกิดขึ้นได้

3.1.1 การจัดทำบัญชีทรัพย์สิน (Inventory of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) ต้องจัดทำและปรับปรุงแก้ไขบัญชีทรัพย์สินที่มีความสำคัญต่อองค์กรให้ถูกต้องอยู่เสมอ

3.1.2 การระบุผู้เป็นเจ้าของทรัพย์สิน (Ownership of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) ต้องจัดให้มีการระบุผู้เป็นเจ้าของสารสนเทศ (แต่ละชนิด) และทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ ตามที่กำหนดไว้ในบัญชีทรัพย์สิน

3.1.3 การใช้งานทรัพย์สินที่เหมาะสม (Acceptable use of assets)

(หัวหน้างานพัสดุและหัวหน้างานสารสนเทศ) จะต้องจัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศอย่างเหมาะสม เพื่อป้องกันความเสียหายต่อทรัพย์สินเหล่านั้น เช่น อันเกิดจากการขาดความระมัดระวัง การขาดการดูแลและเอาใจใส่ เป็นต้น

3.2 การจัดหมวดหมู่สารสนเทศ (Information classification)

มีจุดประสงค์เพื่อกำหนดระดับของการป้องกันสารสนเทศขององค์กรอย่างเหมาะสม

3.2.1 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification guidelines)

(หัวหน้างานสารสนเทศ) จะต้องจัดให้มีกระบวนการในการจัดหมวดหมู่ของทรัพย์สินสารสนเทศตามระดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย และระดับความสำคัญที่มีต่อองค์กร ทั้งนี้เพื่อจะได้หาวิธีการในการป้องกันได้อย่างเหมาะสม

3.2.2 การจัดทำป้ายชื่อ และการจัดการทรัพย์สินสารสนเทศ (Information labeling and handling)

(หัวหน้างานสารสนเทศ) จะต้องจัดให้มีขั้นตอนปฏิบัติในการจัดทำป้ายชื่อและการจัดการทรัพย์สินสารสนเทศตามที่ได้จัดหมวดหมู่ไว้แล้ว

หมวดที่ 4 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

4.1 การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง (เช่น เพื่อการบำรุงรักษาอุปกรณ์ต่างๆ ขององค์กร) และหน่วยงานภายนอก เข้าใจถึงบทบาท และหน้าที่ความรับผิดชอบของตน และเพื่อลดความเสี่ยงอันเกิดจากการขโมย การฉ้อโกง และการใช้อุปกรณ์ผิดวัตถุประสงค์

4.1.1 การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย (Roles and responsibilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่และความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศอย่างเป็นลายลักษณ์อักษรสำหรับพนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และ/หรือหน่วยงานภายนอกที่องค์กรต้องการว่าจ้างมาปฏิบัติงานให้องค์กร และจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

4.1.2 การตรวจสอบคุณสมบัติของผู้สมัคร (Screening)

(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องทำการตรวจสอบคุณสมบัติของผู้สมัคร (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) โดยละเอียด เช่น ตรวจสอบจากจดหมายรับรอง ประวัติการทำงาน วุฒิการศึกษา บุคคลหรือบริษัทที่สามารถอ้างอิงได้ การผ่านการอบรม เป็นต้น และจะต้องพิจารณากฎหมาย ระเบียบ จริยธรรม ชั้นความลับของทรัพย์สินสารสนเทศ และระดับความเสี่ยงในการเข้าถึง ประกอบการคัดเลือกด้วย

4.1.3 การกำหนดเงื่อนไขการจ้างงาน (Terms and conditions of employment)

(หัวหน้างานบุคคลและหน่วยงานภายในที่ต้องการว่าจ้าง) ต้องกำหนดเงื่อนไขการจ้างงาน (ทั้งกรณีการจ้างงานเป็นพนักงาน การว่าจ้างในลักษณะของสัญญา และการว่าจ้างหน่วยงานภายนอก) ซึ่งรวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ และบุคลากรที่จะได้รับการว่าจ้างดังกล่าวจะต้องเห็นชอบและลงนามในเงื่อนไขการจ้างงานนั้นด้วย

4.2 การสร้างความมั่นคงปลอดภัยในระหว่างการจ้างงาน (During employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ตระหนักถึงภัยคุกคามและปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัย หน้าที่ความรับผิดชอบซึ่งรวมถึงหน้าที่ความรับผิดชอบที่ผูกพันทางกฎหมาย และได้เรียนรู้และทำความเข้าใจเกี่ยวกับนโยบายความมั่นคงปลอดภัยขององค์กร รวมทั้งเพื่อลดความเสี่ยงอันเกิดจากความผิดพลาดในการปฏิบัติหน้าที่

4.2.1 หน้าที่ในการบริหารจัดการทางด้านความมั่นคงปลอดภัย (Management responsibilities)

(ผู้บริหารองค์กร) ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกปฏิบัติตามมาตรการการรักษาความมั่นคงปลอดภัย ตามนโยบายและขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

4.2.2 การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน (Information security awareness, education, and training)

(หัวหน้างานบุคคลและหัวหน้างานที่เกี่ยวข้อง) ต้องกำหนดให้พนักงานที่ได้รับการว่าจ้างตามสัญญาการจ้างงาน และผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอก ได้รับการอบรมเพื่อสร้างความตระหนักและเสริมสร้างความรู้ทางด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ การอบรมควรครอบคลุมถึงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์กรตามลักษณะงานที่พนักงานต้องรับผิดชอบด้วย

4.2.3 กระบวนการทางวินัยเพื่อลงโทษ (Disciplinary process)

(ผู้บริหารองค์กร) ต้องจัดให้มีกระบวนการทางวินัยเพื่อลงโทษพนักงานที่ฝ่าฝืนหรือละเมิดนโยบายหรือระเบียบปฏิบัติทางด้านความมั่นคงปลอดภัยขององค์กร

4.3 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or change of employment)

มีจุดประสงค์เพื่อให้พนักงาน ผู้ที่องค์กรทำสัญญาว่าจ้าง และหน่วยงานภายนอกได้ทราบถึงหน้าที่ความรับผิดชอบและบทบาทของตน เมื่อสิ้นสุดการจ้างงานหรือมีการเปลี่ยนการจ้างงาน

4.3.1 การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination responsibilities)

(หัวหน้างานบุคคล) ต้องกำหนดหน้าที่ความรับผิดชอบสำหรับผู้ที่องค์กรเลิกการจ้างงานหรือองค์กรเปลี่ยนลักษณะการจ้างงาน และกำหนดให้ปฏิบัติตามหน้าที่ดังกล่าว

4.3.2 การคืนทรัพย์สินขององค์กร (Return of assets)

(หัวหน้างานบุคคลและหัวหน้างานพัสดุ) ต้องกำหนดให้ผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงานคืนทรัพย์สินขององค์กรที่อยู่ในความครอบครองของตน

4.3.3 การถอดถอนสิทธิในการเข้าถึง (Removal of access rights)

(หัวหน้างานสารสนเทศและหัวหน้างานอาคาร) ต้องทำการถอดถอนสิทธิในการเข้าถึงสารสนเทศและทรัพย์สินสารสนเทศของผู้ที่องค์กรสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน

หมวดที่ 5 การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย และการก่อกวนหรือแทรกแซงต่อทรัพย์สินสารสนเทศขององค์กร

5.1.1 การจัดทำบริเวณล้อมรอบ (Physical security perimeter)

(หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องมีการจัดสรรพื้นที่ กั้นบริเวณ จัดทำผนังหรือกำแพงล้อมรอบ จัดทำประตูทางเข้า-ออกที่มีการควบคุม ตั้งโต๊ะทำการของ รปภ. บริเวณทางเข้า-ออกของสำนักงาน เป็นต้น เพื่อป้องกันการเข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศขององค์กร

5.1.2 การควบคุมการเข้า-ออก (Physical entry controls)

(หัวหน้างานสารสนเทศ และหัวหน้างานอาคาร) ต้องจัดให้มีการควบคุมการเข้า-ออก ในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

5.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงาน และทรัพย์สินอื่นๆ (Securing offices, rooms and facilities)

(หัวหน้างานอาคาร) ต้องจัดให้มีการสร้างความมั่นคงปลอดภัยทางกายภาพต่อสำนักงานห้องทำงานและทรัพย์สินอื่นๆ

5.1.4 การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม (Protecting against external and environmental threats)

(หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันต่อภัยคุกคามต่างๆ ได้แก่ ไฟไหม้ น้ำท่วม แผ่นดินไหว การระเบิด ความไม่สงบของบ้านเมือง หรือหายนะอื่นๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ

5.1.5 การปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)

(หัวหน้างานอาคาร) ต้องจัดให้มีการป้องกันทางกายภาพและแนวทางสำหรับการปฏิบัติงานในพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

5.1.6 การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, delivery, and loading areas)

(หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศขององค์กรโดยไม่ได้รับอนุญาต และถ้าเป็นไปได้ ควรจัดเป็นบริเวณแยกออกมาต่างหาก

5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security)

มีจุดประสงค์เพื่อป้องกันการสูญหาย การเกิดความเสียหาย การถูกขโมย หรือการถูกเปิดเผยโดยไม่ได้รับอนุญาตของทรัพย์สินขององค์กร และการทำให้กิจกรรมการดำเนินงานต่างๆ ขององค์กรเกิดการติดขัดหรือหยุดชะงัก

5.2.1 การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)

(พนักงาน) ต้องจัดวางและป้องกันอุปกรณ์ของสำนักงานเพื่อลดความเสี่ยงจากภัยคุกคามทางด้านสิ่งแวดล้อมและอันตรายต่างๆ รวมทั้งความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต

5.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่างๆ ได้แก่ ระบบกระแสไฟฟ้า ระบบน้ำประปา ระบบควบคุมอุณหภูมิ ระบบระบายอากาศ ระบบปรับอากาศ ระบบกระแสไฟฟ้าสำรอง ระบบสายสื่อสารสำรอง เป็นต้น

5.2.3 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling security)

(หัวหน้างานอาคาร และหัวหน้างานสารสนเทศ) ต้องกำหนดให้เดินสายไฟฟ้า สายสื่อสาร และสายเคเบิ้ลอื่นๆ ได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การทำให้เกิดอุปสรรคต่อสายสัญญาณ หรือการทำให้สายสัญญาณเหล่านั้นเสียหาย

5.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

5.2.5 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of equipment off-premises)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันอุปกรณ์ต่างๆ ที่ใช้งานอยู่นอกสำนักงานเพื่อไม่ให้เกิดความเสียหายต่ออุปกรณ์เหล่านั้น การป้องกันให้พิจารณาจากความเสี่ยงต่างๆ ที่มีต่ออุปกรณ์เหล่านั้น

5.2.6 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure disposal or re-use of equipment)

(พนักงาน) ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้ง หรือถูกบันทึกทับก่อนที่จะทิ้งอุปกรณ์ดังกล่าวไป ทั้งนี้เพื่อเป็นการป้องกันข้อมูลดังกล่าวหากมีการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

5.2.7 การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of property)

(หัวหน้างานอาคาร) ต้องไม่อนุญาตการนำทรัพย์สินขององค์กร ได้แก่ อุปกรณ์สารสนเทศ หรือซอฟต์แวร์ ออกนอกองค์กร เว้นเสียแต่จะได้รับอนุญาตแล้วเท่านั้น

หมวดที่ 6 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)

6.1 การกำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational procedures and responsibilities)

มีจุดประสงค์เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย

6.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Documented operating procedures)

(หัวหน้างานสารสนเทศ) ต้องจัดทำคู่มือขั้นตอนการปฏิบัติงาน ปรับปรุงตามระยะเวลาอันสมควร และแจกจ่ายให้กับผู้ที่เกี่ยวข้อง

6.1.2 การควบคุมการเปลี่ยนแปลง ปรับปรุง หรือแก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ (Change management)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการควบคุมการเปลี่ยนแปลง ปรับปรุง หรือ แก้ไขระบบหรืออุปกรณ์ประมวลผลสารสนเทศ

6.1.3 การแบ่งหน้าที่ความรับผิดชอบ (Segregation of duties)

(ผู้ที่เป็นเจ้าของกระบวนการทางธุรกิจ) ต้องกำหนดให้มีการแบ่งหน้าที่ความรับผิดชอบเพื่อลดโอกาสในการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต หรือใช้ผิดวัตถุประสงค์ต่อทรัพย์สินสารสนเทศขององค์กร

6.1.4 การแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน (Separation of development, test, and operational facilities)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการแยกระบบสำหรับการพัฒนา การทดสอบ และการให้บริการจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับการให้บริการจริงโดยไม่ได้รับอนุญาต

6.2 การบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third party service delivery management)

มีจุดประสงค์เพื่อจัดทำและรักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่โดยหน่วยงานภายนอกให้เป็นไปตามข้อตกลงที่จัดทำไว้ระหว่างองค์กรกับหน่วยงานภายนอก

6.2.1 การให้บริการโดยหน่วยงานภายนอก (Service delivery)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ผู้ให้บริการจากภายนอกปฏิบัติตามข้อกำหนดหรือข้อตกลงที่จัดทำขึ้นระหว่างองค์กรและผู้ให้บริการ ข้อตกลงควรกล่าวถึงมาตรการการรักษาความมั่นคงปลอดภัย ลักษณะของการให้บริการ และระดับของการให้บริการ

6.2.2 การตรวจสอบการให้บริการโดยหน่วยงานภายนอก (Monitoring and review of third party services)

(หัวหน้างานสารสนเทศ) ต้องตรวจสอบการให้บริการโดยหน่วยงานภายนอกอย่างสม่ำเสมอ เช่น การดูจากการให้บริการ การศึกษาจากรายงานและข้อมูลต่างๆ ที่กำหนดให้บันทึกไว้ เป็นต้น

6.2.3 การบริหารจัดการการเปลี่ยนแปลงในการให้บริการ (Managing changes to third party services)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้ทำการปรับปรุงเงื่อนไขการให้บริการของหน่วยงานภายนอกเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อระบบหรือกระบวนการที่เกี่ยวข้องกับงานให้บริการของหน่วยงานภายนอก เช่น การปรับปรุงระบบสารสนเทศใหม่ การพัฒนาระบบสารสนเทศใหม่ การปรับปรุงนโยบายและขั้นตอนปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัย การเปลี่ยนเทคโนโลยีใหม่ การใช้ผลิตภัณฑ์ใหม่ เป็นต้น ซึ่งมีผลกระทบต่อการดำเนินงานของผู้ให้บริการจากภายนอก

6.3 การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System planning and acceptance)

มีจุดประสงค์เพื่อลดความเสี่ยงจากความล้มเหลวของระบบ

6.3.1 การวางแผนความต้องการทรัพยากรสารสนเทศ (Capacity management)

(หัวหน้างานสารสนเทศ) ต้องมีการวางแผนเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคตเพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน

6.3.2 การตรวจรับระบบ (System acceptance)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีเกณฑ์ในการตรวจรับระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือที่เป็นรุ่นใหม่ รวมทั้งต้องดำเนินการทดสอบก่อนที่จะรับระบบนั้นมาใช้งาน

6.4 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Protection against malicious and mobile code)

มีจุดประสงค์เพื่อรักษาซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลายโดยซอฟต์แวร์ที่ไม่ประสงค์ดี

6.4.1 การป้องกันโปรแกรมที่ไม่ประสงค์ดี (Controls against malicious code)

(ผู้ดูแลระบบ) ต้องมีมาตรการสำหรับการตรวจจับ การป้องกัน และการกู้กลับคืนเพื่อป้องกันทรัพย์สินสารสนเทศจากโปรแกรมที่ไม่ประสงค์ดี รวมทั้งต้องมีการสร้างความตระหนักที่เกี่ยวข้องให้กับผู้ใช้งานด้วย

6.4.2 การป้องกันโปรแกรมชนิดเคลื่อนที่ (Controls against mobile code)

(ผู้ดูแลระบบ) ต้องมีมาตรการเพื่อควบคุมการใช้งานโปรแกรมชนิดเคลื่อนที่ (โปรแกรมที่เคลื่อนที่จากหน่วยความจำของเครื่องคอมพิวเตอร์หนึ่งเพื่อไปทำงานในหน่วยความจำของอีกเครื่องคอมพิวเตอร์หนึ่ง) ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยขององค์กร และต้องป้องกันไม่ให้โปรแกรมชนิดเคลื่อนที่อื่นๆ สามารถทำงานหรือใช้งานได้

6.5 การสำรองข้อมูล (Back-up/Housekeeping)

มีจุดประสงค์เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

6.5.1 การสำรองข้อมูล (Information back-up)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอและให้เป็นไปตามนโยบายการสำรองข้อมูลขององค์กร

6.6 การบริหารจัดการทางด้านความมั่นคงปลอดภัยสำหรับเครือข่ายขององค์กร (Network security management)

มีจุดประสงค์เพื่อป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย

6.6.1 มาตรการทางเครือข่าย (Network controls)

(ผู้ดูแลระบบ) ต้องบริหารและจัดการเครือข่าย กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่างๆ ทางเครือข่าย และดูแลรักษาความมั่นคงปลอดภัยสำหรับระบบและแอพพลิเคชั่นที่ใช้งานเครือข่าย รวมทั้งสารสนเทศต่างๆ ที่ส่งผ่านทางเครือข่าย

6.6.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)

(หัวหน้างานสารสนเทศ) ต้องกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดในการบริหารจัดการสำหรับบริการเครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่าย โดยที่บริการเครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก

6.7 การจัดการสื่อที่ใช้ในการบันทึกข้อมูล (Media handling and security)

มีจุดประสงค์เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต และการติดขัดหรือหยุดชะงักทางธุรกิจ

6.7.1 การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of removable media)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

6.7.2 การกำจัดสื่อบันทึกข้อมูล (Disposal of media)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการทำลายสื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไปแล้ว การทำลายต้องเป็นไปอย่างมั่นคงและปลอดภัย

6.7.3 ขั้นตอนปฏิบัติสำหรับการจัดการสารสนเทศ (Information handling procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการจัดการและการจัดเก็บสารสนเทศเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตหรือการใช้งานผิดวัตถุประสงค์

6.7.4 การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ (Security of system documentation)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการป้องกันเอกสารระบบจากการเข้าถึงโดยไม่ได้รับอนุญาต

6.8 การแลกเปลี่ยนสารสนเทศ (Exchange of information)

มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศและซอฟต์แวร์ที่มีการแลกเปลี่ยนกันภายในองค์กร และที่มีการแลกเปลี่ยนกับหน่วยงานภายนอก

6.8.1 นโยบายและขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนสารสนเทศ (Information exchange policies and procedures)

(ผู้บริหารองค์กร) ต้องกำหนดนโยบาย ขั้นตอนปฏิบัติ และมาตรการรองรับ เพื่อป้องกันปัญหาของการแลกเปลี่ยนสารสนเทศระหว่างองค์กร (เช่น องค์กรและหน่วยงานภายนอก) โดยผ่านทางช่องทางการสื่อสารทุกชนิด

6.8.2 ข้อตกลงในการแลกเปลี่ยนสารสนเทศ (Exchange agreements)

(หัวหน้างานสารสนเทศ) ต้องจัดทำข้อตกลงในการแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ระหว่างองค์กร อย่างเป็นลายลักษณ์อักษร

6.8.3 การส่งสื่อบันทึกข้อมูลออกไปนอกองค์กร (Physical media in transit)

(หัวหน้างานสารสนเทศและหัวหน้างานธุรการ) ต้องป้องกันสื่อบันทึกข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตการใช้งานผิดวัตถุประสงค์ และการทำให้ข้อมูลเกิดความเสียหายในระหว่างที่ส่งข้อมูลนั้นออกไปนอกองค์กร

6.8.4 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการในการป้องกันสารสนเทศที่มีการส่งผ่านทางข้อความอิเล็กทรอนิกส์

6.8.5 ระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (Business information systems)

(ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายและขั้นตอนปฏิบัติเพื่อป้องกันสารสนเทศที่เกี่ยวข้องกับระบบสารสนเทศทางธุรกิจที่เชื่อมโยงกัน

6.9 การสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce services)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับบริการพาณิชย์อิเล็กทรอนิกส์และในการใช้งาน

6.9.1 การพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศของระบบพาณิชย์อิเล็กทรอนิกส์ที่มีการส่งผ่านทางเครือข่ายสาธารณะจากการฉ้อโกง การปฏิเสธ การเปิดเผย และการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

6.9.2 การทำธุรกรรมออนไลน์ (On-line transactions)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการสำหรับการป้องกันสารสนเทศที่รับ-ส่งที่เกี่ยวข้องกับการทำธุรกรรมออนไลน์ ทั้งนี้เพื่อป้องกันไม่ให้เกิดความไม่สมบูรณ์ของสารสนเทศที่รับ-ส่ง สารสนเทศถูกส่งไปผิดเส้นทางบนเครือข่าย การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผยสารสนเทศโดยไม่ได้รับอนุญาต หรือการทำสำเนาสารสนเทศโดยไม่ได้รับอนุญาต

6.9.3 สารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ (Publicly available information)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีการป้องกันความถูกต้องและความสมบูรณ์ของสารสนเทศที่มีการเผยแพร่ออกสู่สาธารณะ

6.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)

มีจุดประสงค์เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต

6.10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย อย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

6.10.2 การตรวจสอบการใช้งานระบบ (Monitoring system use)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่

6.10.3 การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือการแก้ไขโดยไม่ได้รับอนุญาต

6.10.4 บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and operator logs)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ

6.10.5 การบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร

6.10.6 การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)

(ผู้ดูแลระบบ) ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุก

หมวด 7 การควบคุมการเข้าถึง (Access control)

7.1 ข้อกำหนดทางธุรกิจสำหรับการควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control)

มีจุดประสงค์เพื่อควบคุมการเข้าถึงสารสนเทศ

7.1.1 นโยบายการควบคุมการเข้าถึงระบบ (Access control policy)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการจัดทำนโยบายควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงตามระยะเวลาที่กำหนดไว้ การจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางธุรกิจและทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ

7.2 การบริหารจัดการการเข้าถึงของผู้ใช้ (User access management)

มีจุดประสงค์เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

7.2.1 การลงทะเบียนพนักงาน (User registration)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนพนักงานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น เมื่อลาออกไป หรือเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

7.2.2 การบริหารจัดการสิทธิการใช้งานระบบ (Privilege management)

(ผู้ดูแลระบบ) ต้องจัดให้มีการควบคุมและจำกัดสิทธิการใช้งานระบบตามความจำเป็นในการใช้งาน

7.2.3 การบริหารจัดการรหัสผ่านผู้ใช้งาน (User password management)

(ผู้ดูแลระบบ) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างเป็นทางการ เพื่อควบคุมการจัดสรรรหัสผ่านให้แก่ผู้ใช้งานอย่างมีความมั่นคงปลอดภัย

7.2.4 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบอย่างเป็นทางการตามระยะเวลาที่กำหนดไว้

7.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ

7.3.1 การใช้งานรหัสผ่าน (Password use)

(ผู้ดูแลระบบ) ต้องกำหนดวิธีปฏิบัติที่ดีสำหรับผู้ใช้งานในการเลือกและใช้งานรหัสผ่าน

7.3.2 การป้องกันอุปกรณ์ที่ไม่มีพนักงานดูแล (Unattended user equipment)

(พนักงาน) ต้องมีวิธีเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์สำนักงานที่ไม่มีพนักงานดูแล

7.3.3 นโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)

(ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายเพื่อควบคุมไม่ให้มีการปล่อยให้ทรัพย์สินสารสนเทศที่สำคัญ เช่น เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ อยู่ในบริเวณที่เป็นที่สาธารณะหรือพบเห็นได้ง่าย เป็นต้น

7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

7.4.1 นโยบายการใช้งานบริการเครือข่าย (Policy on use of network services)

(ผู้บริหารสารสนเทศ) ต้องจัดทำนโยบายการใช้งานเครือข่ายซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้ได้ บริการได้ไม่สามารถใช้งานได้

7.4.2 การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User authentication for external connections)

(ผู้ดูแลระบบ) ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

7.4.3 การพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks)

(ผู้ดูแลระบบ) ต้องกำหนดให้อุปกรณ์บนเครือข่ายสามารถระบุและพิสูจน์ตัวตนเพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว

7.4.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection)

(ผู้ดูแลระบบ) ต้องมีมาตรการป้องกันการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ มาตรการต้องครอบคลุมทั้งการป้องกันทางกายภาพและการป้องกันการเข้าถึงโดยผ่านทางเครือข่าย

7.4.5 การแบ่งแยกเครือข่าย (Segregation in networks)

(ผู้ดูแลระบบ) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ

7.4.6 การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

(ผู้ดูแลระบบ) ต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางธุรกิจได้ระบุไว้

7.4.7 การควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

(ผู้ดูแลระบบ) ต้องกำหนดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง

7.5 การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

7.5.1 ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

(ผู้ดูแลระบบ) ต้องจัดให้มีขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยสำหรับการเข้าถึงหรือการเข้าใช้งานระบบปฏิบัติการ

7.5.2 การระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)

(ผู้ดูแลระบบ) ต้องจัดให้ผู้ใช้งานมีข้อมูลสำหรับระบุตัวตนในการเข้าใช้งานระบบที่ไม่ซ้ำซ้อนกัน และต้องจัดให้มีกระบวนการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบตามข้อมูลระบุตัวตนที่ได้รับ

7.5.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)

(ผู้ดูแลระบบ) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่มีการควบคุมการกำหนดรหัสผ่านที่มีคุณภาพ

7.5.4 การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)

(ผู้ดูแลระบบ) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือมีอยู่แล้ว

7.5.5 การหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

(ผู้ดูแลระบบ) ต้องกำหนดให้ระบบตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบมาเป็นระยะเวลาหนึ่งตามที่กำหนดไว้

7.5.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

(ผู้ดูแลระบบ) ต้องจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูง

7.6 การควบคุมการเข้าถึงแอพพลิเคชันและสารสนเทศ (Application and information access control)

มีจุดประสงค์เพื่อป้องกันการเข้าถึงสารสนเทศของแอพพลิเคชันโดยไม่ได้รับอนุญาต

7.6.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

(ผู้ดูแลระบบ) ต้องจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอพพลิเคชันตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ การเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

7.6.2 การแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)

(หัวหน้างานสารสนเทศ) ต้องแยกระบบสารสนเทศที่มีความสำคัญสูงไว้ในบริเวณที่แยกต่างหากออกมาสำหรับระบบนี้โดยเฉพาะ

7.7 การควบคุมอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร (Mobile computing and teleworking)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกองค์กร

7.7.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)

(ผู้บริหารสารสนเทศ) ต้องกำหนดนโยบายเพื่อควบคุมหรือป้องกันอุปกรณ์สื่อสารชนิดพกพา (เช่น notebook, palm, และ laptop เป็นต้น) และต้องกำหนดมาตรการป้องกันโดยพิจารณาจากความเสี่ยงที่มีต่ออุปกรณ์เหล่านี้

7.7.2 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

(ผู้บริหารสนเทศ) ต้องกำหนดนโยบาย แผนงาน และขั้นตอนปฏิบัติสำหรับบุคลากรที่จำเป็นต้องปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

หมวดที่ 8 การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of information systems)

มีจุดประสงค์เพื่อให้การจัดหาและการพัฒนาระบบสารสนเทศได้พิจารณาถึงประเด็นทางด้านความมั่นคงปลอดภัยเป็นองค์ประกอบพื้นฐานที่สำคัญ

8.1.1 การวิเคราะห์และการระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security requirements analysis and specification)

(ผู้พัฒนา และผู้เป็นเจ้าของระบบ) ต้องวิเคราะห์และระบุข้อกำหนดทางด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศใหม่ หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว

8.2 การประมวลผลสารสนเทศในแอพพลิเคชัน (Correct processing in applications)

มีจุดประสงค์เพื่อป้องกันความผิดพลาดในสารสนเทศ การสูญหายของสารสนเทศ การเปลี่ยนแปลงสารสนเทศโดยไม่ได้รับอนุญาต หรือการใช้งานสารสนเทศผิดวัตถุประสงค์

8.2.1 การตรวจสอบข้อมูลนำเข้า (Input data validation)

(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับตรวจสอบข้อมูลนำเข้าของแอพพลิเคชันว่าข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนที่จะนำไปประมวลผลต่อไป

8.2.2 การตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล (Control of internal processing)

(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับการตรวจสอบว่าข้อมูลที่อยู่ในระหว่างการประมวลผลเกิดความผิดพลาดขึ้นหรือไม่ เช่น อาจมีสาเหตุจากความผิดพลาดในการประมวลผล การกระทำโดยเจตนาของผู้ที่เกี่ยวข้อง เป็นต้น

8.2.3 การตรวจสอบความถูกต้องของข้อความ (Message integrity)

(ผู้พัฒนาระบบ) ต้องระบุข้อกำหนดสำหรับการตรวจสอบความถูกต้องของข้อความสำหรับแอพพลิเคชัน (เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง) รวมทั้งกำหนดมาตรการรองรับเพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความนั้นโดยไม่ได้รับอนุญาต

8.2.4 การตรวจสอบข้อมูลนำออก (Output data validation)

(ผู้พัฒนาระบบ) ต้องกำหนดกลไกสำหรับการตรวจสอบข้อมูลนำออกจากแอพพลิเคชันเพื่อเป็นการทบทวนว่าการประมวลผลของสารสนเทศที่เกี่ยวข้องเป็นไปอย่างถูกต้องและเหมาะสม

8.3 มาตรการการเข้ารหัสข้อมูล (Cryptographic controls)

มีจุดประสงค์เพื่อรักษาความลับของข้อมูล ยืนยันตัวตนของผู้ส่งข้อมูล หรือรักษาความถูกต้องสมบูรณ์ของข้อมูลโดยใช้วิธีการการเข้ารหัสข้อมูล

8.3.1 นโยบายการใช้งานการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีนโยบายควบคุมการใช้งานการเข้ารหัสข้อมูล และให้มีผลบังคับใช้งานภายในองค์กร

8.3.2 การบริหารจัดการกุญแจเข้ารหัสข้อมูล (Key management)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบริหารจัดการสำหรับกุญแจที่ใช้ในการเข้าหรือถอดรหัสข้อมูล โดยกุญแจเหล่านี้จะใช้งานร่วมกับเทคนิคการเข้ารหัสข้อมูลที่กำหนดเป็นมาตรฐานขององค์กร

8.4 การสร้างความมั่นคงปลอดภัยให้กับไฟล์ของระบบที่ให้บริการ (Security of system files)

มีจุดประสงค์เพื่อสร้างความมั่นคงปลอดภัยให้กับไฟล์ต่างๆ ของระบบที่ให้บริการ

8.4.1 การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบที่ให้บริการ (Control of operational software)

(หัวหน้างานสารสนเทศ) ต้องจัดให้มีขั้นตอนปฏิบัติเพื่อควบคุมการติดตั้งซอฟต์แวร์ต่างๆ ลงไปยังระบบที่ให้บริการ ทั้งนี้ เพื่อลดความเสี่ยงที่จะทำให้ระบบให้บริการนั้นเกิดความเสียหายทำงานผิดปกติ หรือไม่สามารถใช้งานได้

8.4.2 การป้องกันข้อมูลที่ใช้สำหรับการทดสอบ (Protection of system test data)

(ผู้พัฒนาระบบ) ต้องหลีกเลี่ยงการใช้ข้อมูลจริงที่ใช้งานอยู่บนระบบให้บริการสำหรับทำการทดสอบระบบ หากมีความจำเป็นต้องใช้ ต้องกำหนดให้มีการป้องกันและควบคุมการใช้งาน เช่น ควรลบทิ้งบางส่วนของข้อมูลที่เป็นความลับ ข้อมูลส่วนตัว หรือข้อมูลสำคัญ

8.4.3 การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access control to program source code)

(หัวหน้างานสารสนเทศ) ต้องจำกัดการเข้าถึงซอร์สโค้ดสำหรับระบบที่ให้บริการ ทั้งนี้เพื่อป้องกันการเปลี่ยนแปลงที่อาจเกิดขึ้นโดยไม่ได้รับอนุญาต หรือโดยไม่ได้เจตนา

8.5 การสร้างความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบและกระบวนการสนับสนุน (Security in development and support processes)

มีจุดประสงค์เพื่อรักษาความมั่นคงปลอดภัยสำหรับซอฟต์แวร์และสารสนเทศของระบบ

8.5.1 ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบ (Change

control procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบเกิดความเสียหาย ทำงานผิดปกติ หรือไม่สามารถใช้งานได้

8.5.2 การตรวจสอบการทำงานของแอพพลิเคชันภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical review of applications after operating system changes)

(ผู้ดูแลระบบ) ต้องทำการตรวจสอบทางเทคนิคภายหลังจากที่ทำการเปลี่ยนแปลงระบบปฏิบัติการเพื่อดูว่าแอพพลิเคชันที่ทำงานอยู่บนระบบปฏิบัติการนั้น ทำงานผิดปกติ ไม่สามารถใช้งานได้ หรือมีปัญหาทางด้านความมั่นคงปลอดภัยเกิดขึ้นหรือไม่

8.5.3 การจำกัดการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต (Restrictions on changes to software packages)

(หัวหน้างานสารสนเทศ) ต้องหลีกเลี่ยงการเปลี่ยนแปลงแก้ไขต่อซอฟต์แวร์ที่มาจากผู้ผลิต หากจำเป็นต้องแก้ไข ต้องแก้ไขตามความจำเป็นเท่านั้น และต้องมีการควบคุมการแก้ไขนั้นอย่างเข้มงวดด้วย

8.5.4 การป้องกันการรั่วไหลของสารสนเทศ (Information leakage)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการเพื่อป้องกันการรั่วไหลของสารสนเทศขององค์กร หรือลดโอกาสที่จะทำให้สารสนเทศเกิดการรั่วไหลออกไป

8.5.5 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(หัวหน้างานสารสนเทศ) ต้องกำหนดมาตรการเพื่อควบคุมและตรวจสอบการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

8.6 การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์ (Technical Vulnerability Management)

มีจุดประสงค์เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่างๆ

8.6.1 มาตรการควบคุมช่องโหว่ทางเทคนิค (Control of technical vulnerabilities)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่างๆ ที่ใช้งาน ประเมินความเสี่ยงของช่องโหว่เหล่านั้น รวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

หมวดที่ 9 การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

9.1 การรายงานเหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events and weaknesses)

มีจุดประสงค์เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กรได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

9.1.1 การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting information security events)

(พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร โดยผ่านช่องทางการรายงานที่กำหนดไว้ และจะต้องดำเนินการอย่างรวดเร็วที่สุดเท่าที่จะทำได้

9.1.2 การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Reporting security weaknesses)

(พนักงาน หรือผู้ที่องค์กรว่าจ้างตามสัญญาการจ้างงาน หรือพนักงานของหน่วยงานภายนอกที่ปฏิบัติงานอยู่ภายในองค์กร) ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กรที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

9.2 การบริหารจัดการและการปรับปรุงแก้ไขต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Management of information security incidents and improvements)

มีจุดประสงค์เพื่อให้มีวิธีการที่สอดคล้องและได้ผลในการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

9.2.1 หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and procedures)

(หัวหน้างานสารสนเทศ) ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติเพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร และขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

9.2.2 การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from security incidents)

(ผู้ดูแลระบบ) ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ ปริมาณที่เกิดขึ้น และค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้ว และเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

9.2.3 การเก็บรวบรวมหลักฐาน (Collection of evidence)

(หัวหน้างานนิติการและหัวหน้างานสารสนเทศ) ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

หมวดที่ 10 การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

10.1 หัวข้อพื้นฐานสำหรับการบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Information security aspects of business continuity management)

มีจุดประสงค์เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจ เพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาอันเหมาะสม

10.1.1 กระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ (Including information security in the business continuity management process)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ การบริหารจัดการและการปรับปรุงกระบวนการดังกล่าวอย่างสม่ำเสมอ กระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับธุรกิจ

10.1.2 การประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity and risk assessment)

(หัวหน้างานสารสนเทศ) ต้องระบุเหตุการณ์ที่สามารถทำให้ธุรกิจขององค์กรเกิดการติดขัดหรือหยุดชะงัก โอกาสที่จะเกิดขึ้น ผลกระทบที่เป็นไปได้ รวมทั้งผลที่เกิดขึ้นต่อความมั่นคงปลอดภัยสำหรับสารสนเทศขององค์กร

10.1.3 การจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ (Developing and implementing continuity plans including information security)

(ผู้บริหารสารสนเทศ) ต้องจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจและการดำเนินงานต่างๆ ให้สามารถดำเนินต่อไปได้ในระดับและช่วงเวลาที่กำหนดไว้ ภายหลังจากที่มีเหตุการณ์ที่ทำให้ธุรกิจเกิดการติดขัด หยุดชะงัก หรือล้มเหลว

10.1.4 การกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ (Business continuity planning framework)

(ผู้บริหารสารสนเทศ) ต้องกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ เพื่อให้แผนงานที่เกี่ยวข้องทั้งหมดมีความสอดคล้องกัน ครอบคลุมข้อกำหนดทางด้านความมั่นคงปลอดภัยที่กำหนดไว้ และจัดลำดับความสำคัญของงานต่างๆ ที่ต้องดำเนินการ

10.1.5 การทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ (Testing, maintaining and re-assessing business continuity plans)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้มีการทดสอบและปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ เพื่อให้แผนมีความทันสมัยและได้ผลเป็นอย่างดี

หมวดที่ 11 การปฏิบัติตามข้อกำหนด (Compliance)

11.1 การปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with legal requirements)

มีจุดประสงค์เพื่อหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติ ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่นๆ

11.1.1 การระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย (Identification of applicable legislation)

(หัวหน้างานนิติการ) ต้องระบุข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) ที่เกี่ยวข้องกับการดำเนินงานหรือธุรกิจขององค์กร ต้องบันทึกข้อกำหนดดังกล่าวไว้เป็นลายลักษณ์อักษร และ

ปรับปรุงข้อกำหนดเหล่านั้นให้ทันสมัยอยู่เสมอ รวมทั้งกำหนดแนวทางการปฏิบัติเพื่อให้สอดคล้องกับข้อกำหนดดังกล่าว

11.1.2 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights (IRP))

(หัวหน้างานนิติการ) ต้องกำหนดขั้นตอนปฏิบัติเพื่อป้องกันการละเมิดสิทธิหรือทรัพย์สินทางปัญญา ขั้นตอนปฏิบัติดังกล่าวต้องกำหนดหรือควบคุมให้ปฏิบัติตามข้อกำหนดทางด้านกฎหมาย ทางด้านระเบียบปฏิบัติ และที่ปรากฏในสัญญา (ระหว่างองค์กร และบุคคลหรือหน่วยงานภายนอกอื่น) รวมทั้งข้อกำหนดในการใช้งานผลิตภัณฑ์ซอฟต์แวร์จากผู้ขายด้วย

11.1.3 การป้องกันข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร (Protection of organizational records)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันข้อมูลที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและระเบียบปฏิบัติ ข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ จากการสูญหาย การถูกทำลายให้เสียหาย และการปลอมแปลง

11.1.4 การป้องกันข้อมูลส่วนตัว (Data protection and privacy of personal information)

(หัวหน้างานนิติการ และหัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการป้องกันข้อมูลส่วนตัวตามที่ระบุหรือกำหนดไว้ในกฎหมาย ระเบียบปฏิบัติ และข้อสัญญาที่เกี่ยวข้อง

11.1.5 การป้องกันการใช้งานอุปกรณ์ประมวลผลสารสนเทศผิดวัตถุประสงค์ (Prevention of misuse of information processing facilities)

(หัวหน้างานสารสนเทศ) ต้องป้องกันไม่ให้ผู้ใช้งานใช้อุปกรณ์ประมวลผลสารสนเทศขององค์กรผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต

11.1.6 การใช้งานมาตรการการเข้ารหัสข้อมูลตามข้อกำหนด (Regulation of cryptographic controls)

(หัวหน้างานนิติการและหัวหน้างานสารสนเทศ) ต้องกำหนดให้ใช้มาตรการการเข้ารหัสข้อมูลโดยให้ยึดถือตาม หรือต้องสอดคล้องกับข้อตกลง กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

11.2 การปฏิบัติตามนโยบาย มาตรฐานความมั่นคงปลอดภัยและข้อกำหนดทางเทคนิค (Compliance with security policies and standards, and technical compliance)

มีจุดประสงค์เพื่อให้ระบบเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

11.2.1 การปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัย (Compliance with security policies and standards)

(ผู้บริหารสารสนเทศ) ต้องกำหนดให้ผู้บังคับบัญชาคอยกำกับ ดูแล และควบคุมการปฏิบัติงานของผู้ที่อยู่ใต้การบังคับบัญชาของตน ให้ปฏิบัติตามขั้นตอนปฏิบัติทางด้านความมั่นคงปลอดภัยตามหน้าที่ความรับผิดชอบของตน ทั้งนี้เพื่อให้การปฏิบัติเป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัยขององค์กร

11.2.2 การตรวจสอบการปฏิบัติตามมาตรฐานทางเทคนิคขององค์กร (Technical compliance checking)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการตรวจสอบระบบสารสนเทศอย่างสม่ำเสมอ เพื่อควบคุมให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยทางเทคนิคขององค์กร

11.3 การตรวจประเมินระบบสารสนเทศ (Information systems audit considerations)

มีจุดประสงค์เพื่อให้การตรวจประเมินระบบสารสนเทศได้ประสิทธิภาพสูงสุดและมีการแทรกแซงหรือทำให้หยุดชะงักต่อกระบวนการทางธุรกิจน้อยที่สุด

11.3.1 มาตรการการตรวจประเมินระบบสารสนเทศ (Information systems audit controls)

(หัวหน้างานสารสนเทศ) ต้องระบุข้อกำหนดและกิจกรรมที่เกี่ยวข้องกับการตรวจประเมินระบบสารสนเทศขององค์กร เพื่อให้มีผลกระทบน้อยที่สุดต่อกระบวนการทางธุรกิจ เช่น การหยุดชะงักของกระบวนการทางธุรกิจในระหว่างที่ทำการตรวจประเมิน

11.3.2 การป้องกันเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (Protection of information systems audit tools)

(หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการจำกัดการเข้าถึงเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ (เช่น ซอฟต์แวร์ที่ใช้ในการตรวจประเมิน) เพื่อป้องกันการใช้งานผิดวัตถุประสงค์ หรือการเปิดเผยข้อมูลการตรวจประเมินโดยไม่ได้รับอนุญาต

4. การบริหารความเสี่ยง (Risk Management)

โดยทั่วไป การบริหารความเสี่ยงคือกระบวนการในการวัด หรือการประเมินความเสี่ยงและพัฒนากลยุทธ์ในการบริหารจัดการ กลยุทธ์ประกอบด้วย การให้ผู้อื่นเป็นผู้รับความเสี่ยง การหลีกเลี่ยงต่อความเสี่ยง การลดผลกระทบจากความเสี่ยง และ การยอมรับบางส่วนหรือทั้งหมดของผลกระทบ การบริหารความเสี่ยงในยุคก่อนเน้นไปความเสี่ยงที่มาจากสาเหตุทางกายภาพหรือทางด้านการกระทำผิดกฎหมาย (เช่น ภัยธรรมชาติ ไฟไหม้ อุบัติเหตุ การตาย และอื่นๆ) การบริหารความเสี่ยงทางด้านการเงิน หรือ ทางด้านอื่นๆ เน้นไปที่การบริหารโดยใช้เครื่องมือทางด้านการเงิน

การบริหารความเสี่ยงในอุดมคตินั้นเป็นกระบวนการซึ่งมีการจัดลำดับความสำคัญโดยความเสี่ยงที่ก่อความเสียหายที่รุนแรงและมีโอกาสในการเกิดมากจะถูกดำเนินการก่อนและความเสี่ยงที่ก่อให้เกิดความเสียหายต่ำกว่าและโอกาสในการเกิดต่ำจะถูกดำเนินการในลำดับถัดมา ในทางปฏิบัติกระบวนการมีความแตกต่างกันไปอย่างมาก การชั่งน้ำหนักระหว่างความเสี่ยงที่โอกาสในการเกิดสูงแต่ผลกระทบไม่ความรุนแรงและความเสี่ยงที่ผลกระทบรุนแรงแต่โอกาสในการเกิดต่ำมักจะมีการตัดสินใจผิดอยู่บ่อยครั้ง

การบริหารความเสี่ยงของสิ่งที่จับต้องมิได้ระบุถึงนิยามใหม่ของความเสี่ยง โดยระบุว่าความเสี่ยงมีโอกาสเกิดได้ตลอดเวลา แต่มันถูกละเลยจากองค์กรซึ่งมีความล้าหลังต่อการบริหารความเสี่ยง ตัวอย่างเช่น ความเสี่ยงในการขาดความรู้จะเกิดขึ้นเมื่อต้องการนำความรู้นั้นมาประยุกต์ใช้ ความเสี่ยงจากการขาดการประสานงานเกิดขึ้นมือความร่วมมือกันไม่มีประสิทธิภาพเท่าที่ควร ความเสี่ยงจะมีผลโดยตรงต่อการลดผลิตผลของพนักงาน ลดการควบคุมค่าใช้จ่าย รายได้ การบริการ คุณภาพ และอื่นๆ

กระบวนการในการบริหารความเสี่ยงมีขั้นตอนดังนี้

1. การจัดทำเนื้อหาและขอบเขตของการประเมินความเสี่ยง (Establish the context) เป็นขั้นตอนที่นำแผนงานที่มีอยู่เดิมและตรวจดูความสัมพันธ์กับขอบเขตในการโจมตีวัตถุประสงค์ของผู้มีส่วนได้เสีย กรอบในการประเมินความเสี่ยง และประเด็นในการประเมินและการวิเคราะห์สำหรับกระบวนเหล่านี้

2. การระบุความเสี่ยง (Identification) หลังจากขั้นตอนแรก ขั้นตอนต่อไปนี้จะเป็นการระบุถึงความเสี่ยง การระบุถึงความเสี่ยงจะเริ่มจากแหล่งที่มาของปัญหาหรือตัวปัญหาเอง การเลือกวิธีในการระบุความเสี่ยงนั้นขึ้นอยู่กับแต่วัฒนธรรม การปฏิบัติของแต่ละอุตสาหกรรม และ

การปฏิบัติตามกฎระเบียบ วิธีระบุความเสี่ยงถูกจัดทำให้เป็นต้นแบบหรือพัฒนาเป็นต้นแบบ ซึ่งมีหลายวิธีเช่น

- Objectives-based Risk Identification
- Scenario-based Risk Identification
- Taxomony-base Risk Identification
- Common-risk Checking

3. การประเมินความเสี่ยง (Assessment) หลังจากมีการระบุความเสี่ยงแล้วจะมีการประเมินถึงผลกระทบและโอกาสในการเกิดเหตุการณ์ มีการวัดระดับของความเสี่ยงในเชิงปริมาณ เช่นในกรณีของความเสียหายของอาคาร ในหลักการแล้ว มีความเสี่ยงแตกต่างในการระบุอัตราในการเกิดเหตุการณ์ และในการประเมินความเสียหายจากผลกระทบต่อทรัพย์สินต่างๆก็เป็นเรื่องที่ยาก การประเมินทรัพย์สินเป็นสิ่งที่จำเป็นต้องระบุไว้ ในปัจจุบันมีหลายทฤษฎีในการวัดปริมาณความเสี่ยง ซึ่งก็มีสูตรในการคำนวณแตกต่างกันมาก แต่ในทางความหมายอย่างสูตรความเสี่ยงสามารถวัดในรูปของ อัตราการเกิด **x** ผลกระผลกระทบต่อเหตุการณ์ = ความเสี่ยง

4. การบรรเทาความเสี่ยง (Potential Risk Treatments) เมื่อได้ประเมินความเสี่ยงแล้ว ก็มีหลายเทคนิคเช่นกันได้แก่

- การหลีกเลี่ยงต่อความเสี่ยง(Risk avoidance) เป็นการเลือกที่จะไม่ปฏิบัติในบางกิจกรรมโดยการหลีกเลี่ยงอาจจะทำให้ชะลอความเสียหายที่อาจจะเกิด แต่ในบางครั้งก็อาจจะลดโอกาสในการทำกำไรได้ในขณะเดียวกัน

- การลดความเสี่ยง(Risk reduction) เป็นการนำเครื่องมือเพื่อช่วยลดผลกระทบหากเหตุการณ์นั้นได้เกิดขึ้น

- การยอมรับต่อความเสี่ยง(Risk retention) เป็นการตัดสินใจที่ยอมรับความเสี่ยงมีระบบควบคุมที่มีประสิทธิภาพ หรือมีเงินทุนเพียงพอที่จะรองรับผลกระทบที่อาจจะเกิดขึ้น

- การถ่ายโอนความเสี่ยง(Risk transfer) เป็นการถ่ายโอนความเสี่ยงให้กับผู้อื่น เช่น การทำสัญญากับบริษัทประกันภัย เป็นต้น

5. การจัดทำแผนงาน (Create the plan) หลังจากได้ตัดสินใจในการเลือกวิธีการในการบรรเทาแต่ละความเสี่ยงแล้วนั้น ผู้บริหารจะต้องตัดสินใจและให้ความเห็นชอบในการจัดทำแผนงานโดยกำหนดตารางในการดำเนินงานและกำหนดผู้รับผิดชอบในแต่ละข้อปฏิบัติ

6. การลงมือปฏิบัติ (Implementation) หลังจากที่ได้มีการวางแผนงานเป็นที่เรียบร้อยแล้ว ก็จะเป็นการดำเนินตามกลยุทธ์ในการบรรเทาความเสี่ยงซึ่งสอดคล้องกับข้อปฏิบัตินั้น เช่น การซื้อความคุ้มครองต่อทรัพย์สิน เป็นต้น

7. การทบทวนและตรวจสอบแผนงาน (Review and evaluation of the plan) ในการวางแผนงานนั้นมักมีการเปลี่ยนแปลง การสูญเสีย หรือ การดำเนินที่ไม่เป็นไปตามแผนงาน ดังนั้นจึงต้องการปรับปรุงแผนงาน ตามช่วงระยะเวลาที่เหมาะสม โดยมีวัตถุประสงค์หลัก ดังนี้

- เพื่อประเมินแผนงานที่ได้วางไว้ว่ายังคงสามารถใช้งานได้อย่างประสิทธิภาพหรือไม่
- เพื่อประเมินถึงระดับของความเสี่ยงต่อสภาพแวดล้อมของธุรกิจที่เปลี่ยนแปลงไป

5. NIST SP 800-30

NIST (National Institute of Standards and Technology) เป็นหน่วยงานภายใต้กำกับดูแลของกระทรวงพาณิชย์ ประเทศสหรัฐอเมริกา ได้มอบหมายให้ แผนกความปลอดภัยทางด้านคอมพิวเตอร์(Computer security division) ได้จัดทำแนวปฏิบัติทางด้านความปลอดภัย (Security Guideline 800 series) ขึ้นภายใต้กฎหมายความปลอดภัยทางด้านคอมพิวเตอร์ปี 1987 (the Computer Security Act of 1987) และกฎหมายปฏิรูปการจัดการเทคโนโลยีสารสนเทศปี 1996 (the Information Technology Management Reform Act of 1996) เพื่อเป็นแนวทางให้กับหน่วยงานภาครัฐและองค์กรที่สนใจได้นำไปปฏิบัติ และในจำนวนนั้นมีแนวปฏิบัติที่น่าสนใจคือ NIST SP (special Publication) 800-30 : Risk management guide for information technology systems ซึ่งมีจุดมุ่งหมายในการบริหารความเสี่ยง โดยพิจารณาจากโอกาสในการเกิดและผลกระทบที่จะเกิดขึ้น เพื่อที่จะสร้างกระบวนการในการบริหารความเสี่ยงได้อย่างมีประสิทธิภาพและลดความเสี่ยงในระดับที่ยอมรับได้ต่อไป

กระบวนการในการบริหารความเสี่ยงตามรูปแบบของ NIST SP 800-30 นั้นได้แบ่งกระบวนการออกเป็น 2 ขั้นตอนหลักๆด้วยกันได้แก่

1. การประเมินความเสี่ยง (Risk Assessment)
2. การบรรเทาความเสี่ยง (Risk Mitigation)

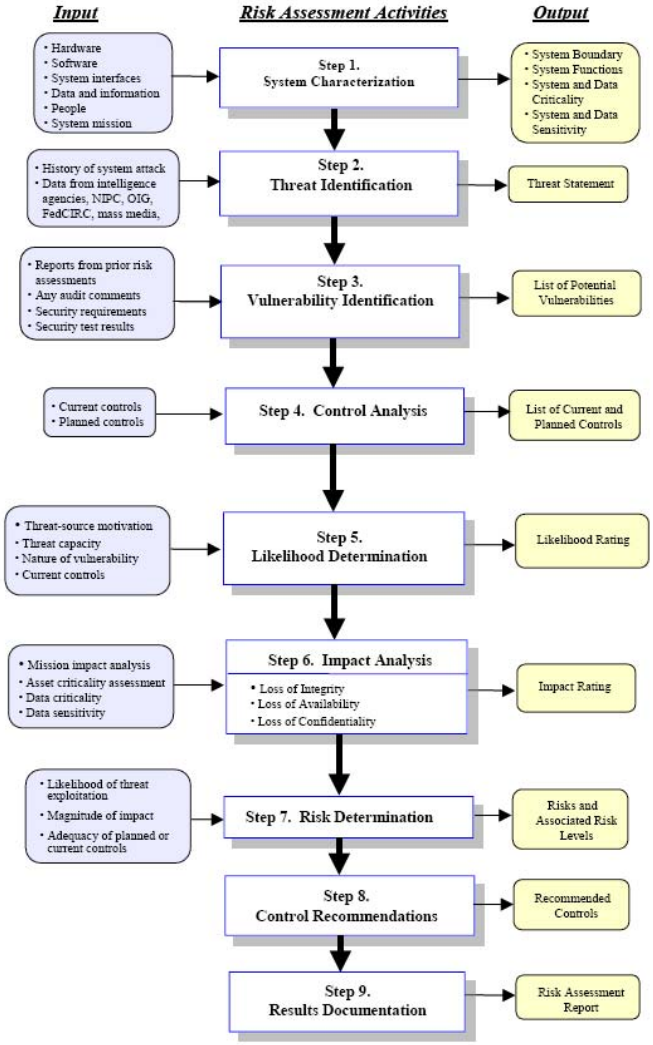
จากรูปแบบของ NIST SP 800-30 โดยพิจารณาการประเมินความเสี่ยงซึ่งสอดคล้องกับงานวิจัยฉบับนี้เป็นหลัก

6. การประเมินความเสี่ยง (Risk Assessment)

เป็นกระบวนการแรกในการบริหารจัดการความเสี่ยง องค์กรจะใช้ขั้นตอนนี้เพื่อทำการระบุภัยคุกคามที่จะส่งผลต่อระบบสารสนเทศขององค์กร ผลลัพธ์ที่ได้จากขั้นตอนนี้จะช่วยให้สามารถกำหนดแนวทางในการควบคุมที่เหมาะสมสำหรับการบรรเทาหรือการขจัดความเสี่ยงในขั้นตอนต่อไป โดยความทั่วไป ความเสี่ยงเป็นรูปแบบของโอกาสในการเกิดซึ่งมาจากภัยคุกคามต่างๆที่โจมตีไปยังจุดอ่อนของระบบ และผลลัพธ์ของผลกระทบที่จะเกิดขึ้นต่อเหตุการณ์นั้นๆ

การประเมินความเสี่ยงได้รวบรวมขั้นตอนหลักๆที่สำคัญไว้ทั้งสิ้น 9 ขั้นตอนดังต่อไปนี้

ภาพที่ 2.4 ขั้นตอนของวิธีการประเมินความเสี่ยง



ที่มา: National Institute of Standards and Technology (NIST), Risk Management Guide for Information Technology Systems, 2002

- ขั้นตอนที่ 1 การระบุคุณสมบัติของระบบ (System Characterization) เป็นการระบุขอบเขตของระบบสารสนเทศ ทรัพยากร และองค์ประกอบอื่นๆในระบบ การกระทำดังกล่าวเพื่อระบุขอบเขตในการประเมินความเสี่ยง วิเคราะห์ผู้ปฏิบัติงานที่ได้รับอนุญาต และจัดหาข้อมูลที่ใช้ในการระบุความเสี่ยง

- ขั้นตอนที่ 2 การระบุเกี่ยวกับภัยคุกคาม (Threat Identification) ขั้นตอนนี้เป็นการระบุแหล่งที่มาของภัยคุกคาม รวมถึงการระบุแรงจูงใจและการกระทำหรือวิธีการอันก่อให้เกิดภัยคุกคามขึ้น เพื่อทำการรวบรวมและนำไปประเมินผลต่อในขั้นตอนต่อไป

- ขั้นตอนที่ 3 การระบุเกี่ยวกับจุดอ่อนของระบบ (Vulnerability Identification) เป็นการระบุถึงจุดอ่อนของระบบโดยทำการรวบรวมข้อมูล ซึ่งประกอบไปด้วย จุดอ่อนที่เกิดขึ้น , แหล่งที่มาของภัยคุกคาม และการกระทำอันก่อให้เกิดภัยคุกคาม จากนั้นจึงทำการทดสอบระบบโดยใช้ข้อมูลข้างต้น และพัฒนาสิ่งที่จำเป็นต่อการรักษาความปลอดภัยของระบบ

- ขั้นตอนที่ 4 การวิเคราะห์มาตรการควบคุม (Control Analysis) ขั้นตอนนี้จะมีการวิเคราะห์มาตรการควบคุมหรือแผนที่จะถูกนำมาใช้สำหรับองค์กรเพื่อบรรเทาหรือขจัดโอกาสในการเกิดความเสี่ยง โดยจะมีการจัดทำข้อมูลของโอกาสที่จะเกิดภัยคุกคามขึ้นในขั้นตอนที่ 5 ต่อไป

- ขั้นตอนที่ 5 การกำหนดเกณฑ์ของโอกาส (Likelihood Determination) ในขั้นตอนนี้เป็นการจัดทำเกณฑ์ของโอกาสที่จะเกิดขึ้นซึ่งส่งผลไปยังจุดอ่อนของระบบโดยอยู่ในภาวะแวดล้อมของภัยคุกคาม องค์ประกอบที่ควรพิจารณาได้แก่

  - แรงจูงใจและความสามารถของแหล่งที่มาของภัยคุกคาม
  - ลักษณะของจุดอ่อนที่พบ
  - กฎเกณฑ์ที่ใช้และความมีประสิทธิภาพของมาตรการควบคุมในปัจจุบัน

โอกาสซึ่งจะมีผลต่อจุดอ่อนของระบบนั้น สามารถอธิบายได้ใน 3 ระดับคือ สูง กลาง และ ต่ำ ซึ่งจะแสดงนิยามของแต่ละระดับดังตาราง

ตารางที่ 2.1 ระดับของโอกาสในการเกิด

ระดับของโอกาส	นิยามของโอกาส
สูง (High)	แหล่งของภัยคุกคามมีแรงจูงใจสูง , มีความสามารถมาก และขาดมาตรการควบคุมสำหรับป้องกันจุดอ่อนจากการโจมตีที่มีประสิทธิภาพ
กลาง (Medium)	แหล่งของภัยคุกคามมีแรงจูงใจและมีความสามารถ แต่มาตรการควบคุมอยู่ในตำแหน่งที่อาจจะสามารถยับยั้งการโจมตีได้
ต่ำ (Low)	แหล่งของภัยคุกคามขาดแรงจูงใจ และมาตรการควบคุมอยู่ในตำแหน่งที่อาจจะสามารถยับยั้งการโจมตีได้

ที่มา: National Institute of Standards and Technology (NIST), Risk Management Guide for Information Technology Systems, 2002

- ขั้นตอนที่ 6 การวิเคราะห์ผลกระทบ (Impact Analysis) เป็นการวัดระดับความเสี่ยงโดยประเมินจากผลกระทบที่มีผลมาจากการโจมตีของภัยคุกคามได้เป็นผลสำเร็จ โดยก่อนที่จะมีการประเมินนั้นจะต้องมีการเก็บรวบรวมข้อมูลที่จำเป็นซึ่งประกอบด้วย

  - วัตถุประสงค์การใช้งานของระบบ
  - มูลค่าหรือความสำคัญของข้อมูลในระบบ
  - ความอ่อนไหวของข้อมูลในระบบ

ด้วยเหตุนี้ ผลกระทบที่เกิดขึ้นกับระบบจะสามารถอธิบายได้ในรูปแบบของความสูญเสีย , การลดทอนของสิ่งใดสิ่งหนึ่งหรือองค์ประกอบต่างๆของสิ่งนั้น ซึ่งเป็นไปตามเป้าหมายของความปลอดภัยอันได้แก่ ความสูญเสียด้านความลับของข้อมูล (Loss of Confidentiality) , ความสูญเสียด้านบูรณภาพของข้อมูล (Loss of Integrity) และความสูญเสียด้านการให้บริการข้อมูล (Loss of Availability) ดังนั้นตามแนวปฏิบัตินี้ได้กำหนดระดับของผลกระทบในเชิงปริมาณประกอบด้วยระดับ สูง กลาง และ ต่ำ ดังตาราง

ตารางที่ 2.2 ระดับของผลกระทบที่เกิดขึ้น

ความสำคัญของผลกระทบ	นิยามของผลกระทบ (Impact Definition)
สูง (High)	- การโจมตีจุดอ่อนจะมีผลให้เกิดค่าใช้จ่ายอย่างสูงต่อทรัพย์สินที่มีความสำคัญที่จับต้องได้หรือทรัพยากรอื่นๆ - อาจจะทำลาย ทำความเสียหาย หรือขัดขวางภารกิจ ชื่อเสียง หรือ ผลประโยชน์ ขององค์กร อย่างมีนัยสำคัญ - อาจจะมีผลต่อการเสียชีวิตของผู้คนหรือการได้รับบาดเจ็บสาหัส
กลาง (Medium)	- การโจมตีจุดอ่อนจะมีผลให้เกิดค่าใช้จ่ายต่อทรัพย์สินที่จับต้องได้หรือทรัพยากรอื่นๆ - อาจจะทำลาย ทำความเสียหาย หรือขัดขวางภารกิจ ชื่อเสียง หรือ ผลประโยชน์ ขององค์กร - อาจจะมีผลต่อผู้คนทำให้ได้รับบาดเจ็บ
ต่ำ (Low)	- การโจมตีจุดอ่อนจะมีผลให้เกิดค่าใช้จ่ายต่อทรัพย์สินบางส่วนที่จับต้องได้หรือทรัพยากรอื่นๆ - อาจจะส่งผลกระทบที่เห็นได้ชัดต่อภารกิจ ชื่อเสียง หรือ ผลประโยชน์ ขององค์กร

ที่มา: National Institute of Standards and Technology (NIST), Risk Management Guide for Information Technology Systems, 2002

- ขั้นตอนที่ 7 การระบุนิยามของความเสี่ยง (Risk Determination) ในขั้นตอนนี้จะมีการประเมินความเสี่ยงที่มีผลต่อระบบสารสนเทศในรูปแบบของ

  - โอกาสของแหล่งที่มาของภัยคุกคามที่เข้าโจมตีจุดอ่อนของระบบ
  - ความสำคัญของผลกระทบที่เกิดจากแหล่งที่มาของภัยคุกคามซึ่งโจมตีจุดอ่อนของระบบเป็นผลสำเร็จ
  - ความสามารถที่เพียงพอของแผนหรือมาตรการควบคุมที่จะบรรเทาหรือขจัดความเสี่ยง

การระบุตารางความเสี่ยงเกิดจากโอกาสในการเกิดความเสี่ยงคูณกับผลกระทบที่เกิดจากความเสี่ยงนั้นๆ โดยระบุค่าความน่าจะเป็นของโอกาสในการเกิดความเสี่ยง เช่น สูง (1.0), กลาง (0.5) และ ต่ำ (0.1) และระบุค่าของผลกระทบที่เกิดจากความเสี่ยง เช่น สูง (100) , กลาง (50) และ ต่ำ (10)

ตารางที่ 2.3 ค่าความเสี่ยง

โอกาสเกิดภัยคุกคาม	**ผลกระทบ**		
	สูง (10)	**กลาง** (50)	**ต่ำ** (100)
สูง(1.0)	**ต่ำ** 10 x 1.0 = 10	**กลาง** 50 x 1.0 = 50	**สูง** 100 x 1.0 = 100
กลาง (0.5)	**ต่ำ** 10 x 0.5 = 5	**กลาง** 50 x 0.5 = 25	**กลาง** 100 x 0.5 = 50
ต่ำ (0.1)	**ต่ำ** 10 x 0.1 = 1	**ต่ำ** 50 x 0.1 = 5	**ต่ำ** 100 x 0.1 = 10

เมื่อได้ออกแบบตารางความเสี่ยงเรียบร้อยแล้ว จึงกำหนดระดับความเสี่ยงตามช่วงของคะแนนดังตาราง

ตารางที่ 2.4 คะแนนตามระดับความเสี่ยง

ระดับความเสี่ยง	**คะแนน**
สูง (High)	> 50 ถึง 100
กลาง (Medium)	> 10 ถึง 50
ต่ำ (Low)	1 ถึง 10
เล็กน้อยหรือไม่มีนัยสำคัญ (Negligible)	< 1

เมื่อได้กำหนดตารางความเสี่ยงขึ้นแล้วจะทำให้ผู้บริหารที่เกี่ยวข้องได้รับทราบถึงแผนงานแล้วระบุผู้รับผิดชอบ ดังตารางข้างล่างนี้

ตารางที่ 2.5 ระดับของผลกระทบที่เกิดขึ้น

ระดับความเสี่ยง	คำอธิบายความเสี่ยงและแผนงานที่จำเป็น
สูง (High)	ถ้าผลจากการสังเกตการณ์หรือการค้นพบประเมินได้ว่ามีความเสี่ยงสูง จะต้องมีความจำเป็นอย่างยิ่งที่จะหามาตรการแก้ไข ระบบที่มีอยู่เดิมอาจจะดำเนินการต่อไปได้ แต่แผนปฏิบัติงานจะต้องถูกกำหนดขึ้นอย่างเร็วที่สุด
กลาง (Medium)	ถ้าผลจากการสังเกตการณ์หรือการค้นพบประเมินได้ว่ามีความเสี่ยงปานกลาง แผนการแก้ไขจะมีความจำเป็นและแผนงานจะถูกพัฒนาขึ้นเพื่อรวมเข้ากับแผนปฏิบัติงานหลักในเวลาที่สมเหตุสมผล
ต่ำ (Low)	ถ้าผลจากการสังเกตการณ์หรือการค้นพบประเมินได้ว่ามีความเสี่ยงต่ำ ผู้ดูแลรับผิดชอบจะต้องระบุแผนแก้ไขที่จำเป็นหรือตัดสินใจที่จะยอมรับความเสี่ยงนั้น

- ขั้นตอนที่ 8 การให้คำแนะนำถึงมาตรการควบคุมที่จะนำมาใช้ (Control Recommendations) เป็นขั้นตอนในการลดหรือขจัดความเสี่ยงโดยมีมาตรการที่เหมาะสม โดยทำให้ความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้ ซึ่งเป็นการนำผลจากการประเมินความเสี่ยงมาประกอบการพิจารณา

- ขั้นตอนที่ 9 การสรุปรายงาน (Results Documentation) เป็นการสรุปผลจากการประมินความเสี่ยงในรูปของรายงานอย่างเป็นทางการ สำหรับรายงานนี้จะทำให้ผู้บริหารได้นำมาไปตัดสินใจ , วางนโยบาย และกำหนดงบประมาณในการดำเนินงาน รวมถึงการเปลี่ยนแปลงอื่นๆที่จะมีผลในอนาคตต่อไป

<u>การวิเคราะห์มาตรฐานในการประเมินความเสี่ยง</u>

ข้อดีของมาตรฐาน NIST SP 800-30

- NIST SP 800-30 เน้นการประเมินความเสี่ยงในด้านสารสนเทศ และเป็นมาตรฐานที่ใช้กันอย่างแพร่หลายในอเมริกาและอีกหลายประเทศ และไม่มีค่าใช้จ่ายใดๆ

- มีการแบ่งระดับความเสี่ยงแบบตาราง 3x3 ซึ่งแบ่งเป็นระดับ สูง กลาง และต่ำ จึงทำให้ง่ายต่อการทำความเข้าใจ

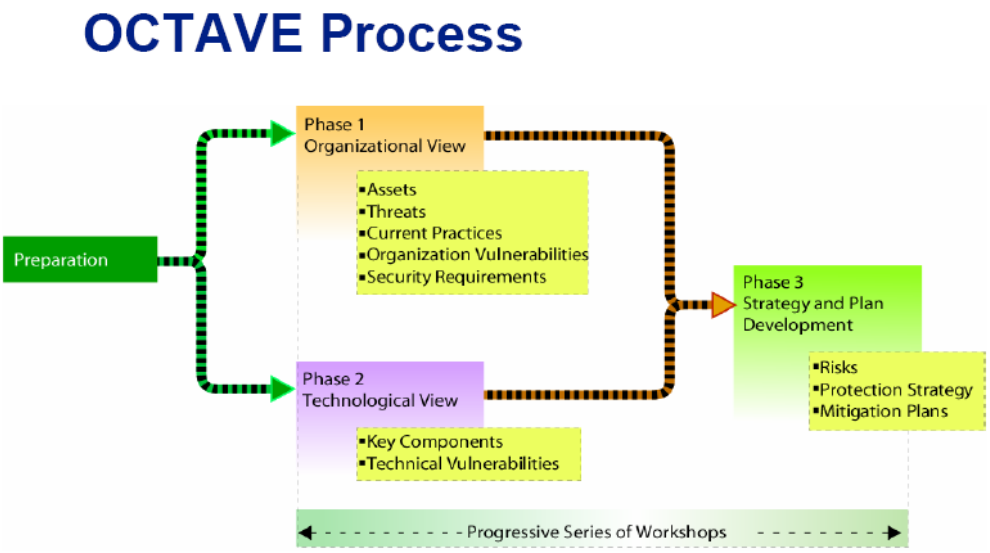
ข้อจำกัดของมาตรฐาน NIST SP 800-30

- เนื่องจากระดับของโอกาส ไม่ได้ระบุให้ชัดเจนว่า มีความถี่ในการเกิดภัยคุกคามมากเพียงใดจึงทำให้แต่ละหน่วยงานที่นำไปปฏิบัติต้องตีความ ซึ่งอาจจะแตกต่างกันไป

7. OCTAVE

OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability Evaluation) เป็นวิธีในการประเมินความเสี่ยงซึ่งริเริ่มโดยสถาบันวิศวกรรมซอฟต์แวร์แห่งมหาวิทยาลัย Carnegie Mellon โดยความร่วมมือของหน่วยงาน CERT (Computer Emergency Response Team) โดย OCTAVE มุ่งเน้นในการประเมินความเสี่ยงขององค์กร มิใช่ความเสี่ยงทางด้านเทคโนโลยี แบ่งเป็น 2 เวอร์ชั่น ซึ่งได้แก่ OCTAVE (Full Version) สำหรับหน่วยงานขนาดใหญ่ที่มีพนักงาน 300 คนขึ้นไป และ OCTAVE-S สำหรับหน่วยงานขนาดเล็กประมาณ 100 คนหรือน้อยกว่า

ภาพที่ 2.5 ขั้นตอนในการการทำงานของ OCTAVE



ที่มา: Carnegie Mellon University, OCTAVE Process, 2003

OCTAVE แบ่งขั้นตอนในการดำเนินงาน ซึ่งเรียกว่า OCTAVE Method ออกเป็น 3 ช่วง ดังนี้

ช่วงที่ 1 การสร้างข้อมูลของภัยคุมคามที่มีต่อทรัพย์สิน (Build Asset-Based Threat Profiles) เป็นการประเมินภาพรวมขององค์กร สมาชิกในองค์กรจะเป็นผู้ประเมินว่าทรัพย์สินใดมีความสำคัญต่อองค์กร และขณะนี้มีการปกป้องทรัพย์สินเหล่านั้นอย่างไร ทีมวิเคราะห์จะเลือกทรัพย์สินที่มีความสำคัญที่สุด (Critical asset) , ระบุความต้องการความปลอดภัยและระบุภัยคุกคามต่อทรัพย์สินเหล่านั้น รวมทั้งกำหนดวิธีหรือแนวทางที่จะก่อให้เกิดภัยคุกคาม ซึ่งประกอบด้วยขั้นตอนต่างๆดังนี้

- ขั้นตอนที่ 1 การเก็บข้อมูลจากผู้บริหารระดับสูง (Identify Senior Management Knowledge) เป็นขั้นตอนที่ให้ทีมวิเคราะห์ได้พูดคุยกับ ผู้บริหารระดับสูง (Senior Manager) เพื่อเก็บข้อมูลต่างๆ
- ขั้นตอนที่ 2 การเก็บข้อมูลจากผู้บริหารในแต่ละหน่วยงาน (Identify Operational Area Management Knowledge) เป็นการให้ทีมวิเคราะห์ได้พูดคุยกับผู้จัดการในแต่ละหน่วยงาน (Operational Area Manager) เพื่อเก็บข้อมูลต่างๆ
- ขั้นตอนที่ 3 การเก็บข้อมูลจากผู้ปฏิบัติงาน (Identify Staff Knowledge) เป็นการให้ทีมวิเคราะห์ได้พูดคุยกับ ผู้ปฏิบัติงาน เพื่อเก็บข้อมูลต่างๆ
- ขั้นตอนที่ 4 การกำหนดข้อมูลภัยคุกคาม (Create Threat Profiles) เป็นการที่ทีมวิเคราะห์ได้นำข้อมูลที่รวบรวมจากผู้ปฏิบัติงานในระดับงานต่างๆมาจัดกลุ่ม ทำการเลือกทรัพย์สินที่มีความสำคัญที่สุด (Critical asset) และกำหนดวิธีหรือแนวทางที่จะก่อให้เกิดภัยคุกคามต่อทรัพย์สินนั้นๆ

ช่วงที่ 2 การระบุเกี่ยวกับจุดอ่อนของระบบโครงสร้างพื้นฐาน (Identify Infrastructure Vulnerabilities) เป็นการประเมินโครงสร้างข้อมูล ทีมวิเคราะห์จะทำการระบุระบบข้อมูลที่มีความสำคัญและองค์ประกอบอื่นๆที่เกี่ยวข้องกับทรัพย์สินที่มีความสำคัญที่สุด (Critical asset) ทีมวิเคราะห์จะทำการทดสอบหาจุดอ่อนของระบบ (Technology Vulnerabilities) ซึ่งจะนำไปสู่การกระทำใดๆที่ไม่ได้รับอนุญาตซึ่งมีผลโดยตรงต่อทรัพย์สินนั้นๆ ประกอบด้วยขั้นตอนต่างๆดังนี้

- ขั้นตอนที่ 5 การระบุองค์ประกอบที่สำคัญของระบบ (Identify Key Components) ทีมวิเคราะห์และพนักงานทางด้าน IT ที่ได้คัดเลือกมา จะนำข้อมูลทางด้านโครงสร้างพื้นฐานของคอมพิวเตอร์ในหน่วยงาน แผนผังของระบบเครือข่าย และข้อมูลอื่นๆที่จำเป็นเพื่อประเมินระบบข้อมูลที่ได้คัดเลือกมา โดยทำการระบุระบบที่จะทำการศึกษา

องค์ประกอบต่างๆทางด้านเครือข่ายในการสู่ระบบ และองค์ประกอบที่ถูกเลือกเพื่อใช้ในการทดสอบจุดอ่อนของระบบ

- ขั้นตอนที่ 6 การประเมินองค์ประกอบที่ได้คัดเลือกไว้แล้ว (Evaluate Selected) ทีมวิเคราะห์และพนักงานทางด้าน IT ที่ได้คัดเลือกมา ทำการทดสอบองค์ประกอบที่ถูกเลือกในขั้นตอนที่ 5 โดยอาศัยซอฟต์แวร์ จากนั้นจึงนำผลการทดสอบมาสรุป เพื่อเตรียมนำเข้าสู่ขั้นตอนในการสร้างแผนป้องกันความเสี่ยงต่อไป

ช่วงที่ 3 การพัฒนากลยุทธ์และแผนในการรักษาความปลอดภัย (Develop Security Strategy and Plans) ในระหว่างการประเมิน ทีมวิเคราะห์จะทำการระบุความเสี่ยงต่างๆที่จะเกิดกับทรัพย์สินที่มีความสำคัญที่สุด (Critical asset) และตัดสินใจว่าจะทำอย่างไรกับความเสี่ยงเหล่านั้น ทีมจะสร้างกลยุทธ์ในการป้องกันสำหรับองค์กรและแผนการลดความเสี่ยงซึ่งจะระบุถึงความเสี่ยงที่จะมีผลต่อทรัพย์สินที่มีความสำคัญที่สุด (Critical asset) โดยพิจารณาบนพื้นฐานของการวิเคราะห์ข้อมูลที่ได้รวบรวมมา ประกอบด้วยขั้นตอนต่างๆดังนี้

- ขั้นตอนที่ 7 การดำเนินการตามผลวิเคราะห์ความเสี่ยง (Conduct Risk Analysis) ทีมวิเคราะห์จะทำการระบุผลกระทบจากภัยคุกคามมีต่อทรัพย์สินที่มีความสำคัญที่สุด (Critical asset) และทำการกำหนดเกณฑ์ในการประเมินความเสี่ยงในเชิงปริมาณ เช่น สูง กลาง และ ต่ำ จากนั้นจึงทำการประเมินผลกระทบจากภัยคุกคามที่มีต่อทรัพย์สินที่มีความสำคัญที่สุด (Critical asset) โดยใช้เกณฑ์ที่ได้กำหนดไว้ข้างต้น
- ขั้นตอนที่ 8 การพัฒนากลยุทธ์ในการป้องกัน (Develop Protection Strategy) ในขั้นตอนนี้จะมีการสร้างกลไกในการป้องกันความเสี่ยงสำหรับองค์กร แผนการลดความเสี่ยงที่จะมีต่อทรัพย์สินที่มีความสำคัญที่สุด (Critical asset)

จากขั้นตอนต่างๆที่ได้กล่าวข้างต้น โดยพิจารณาในขั้นตอนของการประเมินความเสี่ยง พบว่ามีหลักเกณฑ์ที่ถูกนำมาพิจาณาดังตัวอย่างต่อไปนี้

- ชื่อเสียง / ความเชื่อมั่นของลูกค้า
- ชีวิต / สุขภาพของลูกค้า
- ผลผลิต
- การเงิน
- อื่นๆ

ตัวอย่างของหลักเกณฑ์ในการประเมินความเสี่ยงดังตัวอย่างต่อไปนี้

ตารางที่ 2.6 หลักการในการประเมินความเสี่ยง

หลักเกณฑ์ในการประเมินผลกระทบของความเสี่ยง			
ขอบเขตผลกระทบ	**สูง**	**กลาง**	**ต่ำ**
ชื่อเสียง / ความเชื่อมั่นของลูกค้า	• ชื่อเสียงถูกทำลายหรือเสียหาย • สูญเสียความนิยมหรือการยอมรับ • ความเชื่อมั่นของลูกค้าลดลงมากกว่า 30 %	• ชื่อเสียงถูกทำลาย , ต้องใช้ความพยายามหรือค่าใช้จ่ายในการกู้ชื่อเสียง • ถูกลดความนิยมหรือการยอมรับลงโดยองค์กรที่มีหน้าที่ตรวจสอบ • ความเชื่อมั่นของลูกค้าลดลง 10% - 30%	• ชื่อเสียงถูกกระทบพียงเล็กน้อย , ใช้ความพยายามหรือค่าใช้จ่ายเพียงเล็กน้อยในการกู้ชื่อเสียง • ไม่มีการเปลี่ยนแปลงความนิยมหรือการยอมรับลงโดยองค์กรที่มีหน้าที่ตรวจสอบ • ความเชื่อมั่นของลูกค้าลดลงน้อยกว่า 10 %
ชีวิต / สุขภาพของลูกค้า	• ลูกค้าสูญเสียชีวิต • ทำให้เกิดการพิการส่วนใดส่วนหนึ่งของร่างกายอย่างถาวร	• ลูกค้าได้รับการคุกคามต่อชีวิตแต่แก้ไขด้วยการรักษาเยียวยา • ทำให้เกิดการพิการส่วนใดส่วนหนึ่งของร่างกายชั่วคราวหรือสามารถรักษาได้	• ไม่มีการสูญเสียหรือการคุกคามต่อชีวิต • ทำให้เกิดการลดสมรรถภาพต่อร่างกายลงเล็กน้อยแต่สามารถเป็นปรกติได้ใน 4 วัน

ตารางที่ 2.6 (ต่อ) หลักการในการประเมินความเสี่ยง

หลักเกณฑ์ในการประเมินผลกระทบของความเสี่ยง			
ขอบเขตผลกระทบ	**สูง**	**กลาง**	**ต่ำ**
ผลผลิต	• มีการใช้เวลางานเพิ่มขึ้นอย่างน้อย 40 % และเพิ่มคนงานขึ้นอย่างน้อย 10 % ใช้เวลามากกว่า 2 วัน • ข้อมูลลูกค้าสูญหายหรือได้รับความเสียหาย	• พนักงานทำงานเพิ่มขึ้น 10-40% ต่อวัน • การทำงานไม่ต่อเนื่อง ข้อมูลได้รับล่าช้า	• พนักงานไม่ได้รับความสะดวกสบายน้อยกว่า 1 วันแต่ไม่มีการเพิ่มคนงานหรือชั่วโมงงาน
ค่าปรับ / บทลงโทษ	• เสียค่าปรับมากกว่า 100,000 เหรียญ	• เสียค่าปรับ 10,000 ถึง 100,000 เหรียญ	• ไม่เสียค่าปรับหรือเสียน้อยกว่า 10,000 เหรียญ
การเงิน	• ค่าใช้จ่ายในการดำเนินงานต่อปีเพิ่มขึ้น 15 % • สูญเสียรายได้ต่อปี 20 % • สูญเสียทางการเงินต่อครั้งมากกว่า 1,000,000 เหรียญ	• ค่าใช้จ่ายในการดำเนินงานต่อปีเพิ่มขึ้น 2-15% • สูญเสียรายได้ต่อปี 5-20% • สูญเสียทางการเงินต่อครั้ง 250,000 ถึง 1,000,000 เหรียญ	• ค่าใช้จ่ายในการดำเนินงานต่อปีเพิ่มขึ้นน้อยกว่า 2% • สูญเสียรายได้ต่อปีน้อยกว่า 5% • สูญเสียทางการเงินต่อครั้งน้อยกว่า 250,000 เหรียญ

ตารางที่ 2.6 (ต่อ) หลักการในการประเมินความเสี่ยง

หลักเกณฑ์ในการประเมินผลกระทบของความเสี่ยง			
ขอบเขตผลกระทบ	**สูง**	**กลาง**	**ต่ำ**
อื่นๆ	• สูญเสียสิ่งอำนวยความสะดวกหรืออาคารจากเพลิงไหม้	• สิ่งอำนวยความสะดวกหรืออาคารได้รับความเสียหายชั่วคราว	• เครื่องปรับอากาศไม่สามารถทำงานได้ภายใน 2 สัปดาห์

ที่มา : Carnegie Mellon University, OCTAVE Process, 2003

อย่างไรก็ตาม OCTAVE มีข้อจำกัดอยู่ในหลายประเด็น ได้แก่

<u>การวิเคราะห์มาตรฐานในการประเมินความเสี่ยง</u>

ข้อดีของมาตรฐาน OCTAVE

- OCTAVE เน้นการประเมินความเสี่ยงซึ่งพิจารณาผลกระทบจากหลายๆด้านซึ่งจะมีผลต่อการดำเนินงานขององค์กร จึงทำให้สามารถเห็นภาพรวมทั้งหมด โดยมิได้พิจารณาในด้านเทคโนโลยีสารสนเทศแต่เพียงอย่างเดียว
- เป็นมาตรฐานที่มีให้เลือกทั้งองค์กร ขนาดใหญ่และขนาดเล็ก จึงทำให้สามารถนำไปเลือกใช้ได้อย่างเหมาะสม
- มีการวัดผลกระทบในเชิงปริมาณที่ชัดเจนทำให้สามารถตรวจสอบถึงระดับของผลกระทบของแต่ละองค์กรได้อย่างดี

ข้อจำกัดของมาตรฐาน OCTAVE

- OCTAVE ไม่เหมือนกับมาตรฐานอื่นๆเช่น AS/NZS 4360:2004 ที่ไม่มีการกำหนดโอกาสในการเกิดภัยคุกคามเพราะได้ตั้งสมมติฐานว่าภัยคุกคามนั้นสามารถเกิดขึ้นได้ตลอดเวลา และไม่เหมาะสมที่จะนำมาใช้ในหลายๆองค์กร
- OCTAVE เป็นมาตรฐานที่ประกอบด้วย 18 บท ซึ่งถือว่ากฎเกณฑ์ที่ค่อนข้างมากและมีความซับซ้อนเกินไป

OCTAVE ยังเป็นมาตรฐานที่ไม่แพร่หลายเท่ากับมาตรฐานอื่นๆเช่น NIST SP 800-30 และ ISO 17799 จึงทำให้การพัฒนามาตรฐานนี้ในภาพรวมเป็นไปได้ช้า

กฎหมายที่เกี่ยวข้อง

1. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2551

1.1 ที่มาของ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ในปัจจุบันการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ หรือ ระบบอิเล็กทรอนิกส์ได้เข้ามามีบทบาท และ ทวีความสำคัญเพิ่มขึ้นตามลำดับต่อระบบเศรษฐกิจและคุณภาพชีวิตของประชาชนในประเทศไทย แต่ในขณะเดียวกันการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ก็มีแนวโน้มขยายวงกว้างและทวีความรุนแรงเพิ่มมากขึ้นด้วย ดังนั้น ข้อมูลจราจรทางคอมพิวเตอร์นับเป็นพยานหลักฐานสำคัญในการดำเนินคดี อันเป็นประโยชน์อย่างยิ่งต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ ใน พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงสมควรกำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ดังกล่าว

จากการประกาศใช้ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มีผลบังคับใช้แล้ว ตั้งแต่ วันพุธที่ 18 กรกฎาคม 2550 ทำให้หลายองค์กรทั้งภาครัฐและภาคเอกชนต้องมีการปรับตัวครั้งใหญ่ เนื่องจากมาตรา 26 ใน พรบ. ได้กล่าวไว้ว่า “ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท” ทำให้หลายคนเกิดความสงสัยว่าองค์กรของตนถือเป็น “ผู้ให้บริการ” หรือไม่ และการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ดังกล่าวนั้นหมายถึงข้อมูลอะไรบ้าง ควรมีการจัดเก็บแบบใดถึงจะถูกต้องตามวัตถุประสงค์ของ พรบ. โดยที่องค์กรแต่ละองค์กรมีลักษณะการใช้ระบบสารสนเทศที่แตกต่างกัน ดังนั้นจึงควรมีการแนวทาง หรือ”Guideline” ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ให้ถูกต้องและเหมาะสมกับลักษณะการใช้ระบบสารสนเทศหรือระบบอินเทอร์เน็ตของแต่ละองค์กรที่มีความแตกต่างกันค่อนข้างมาก รวมทั้งร้านอินเทอร์เน็ตคาเฟ่ที่มีอยู่มากมายในประเทศไทย ควรจัดเก็บข้อมูลอย่างไรเป็นต้น ตลอดจน หลายองค์กรยังไม่มีความพร้อมในการ

จัดเก็บข้อมูลจราจรคอมพิวเตอร์ ทำให้ผู้บริหารระบบสารสนเทศขององค์กรต้องการทราบระยะเวลาในการผ่อนผันว่าทางการจะผ่อนผันได้นานกี่วันนับจากวันที่กฎหมายประกาศใช้ ก่อนที่จะมีการตรวจสอบหรือการขอข้อมูลโดยพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งโดยรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ดังนั้นทางกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้ออกประกาศกระทรวงฯ สำหรับหลักเกณฑ์ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ดังกล่าว เพื่อให้เกิดความเหมาะสมในทางปฏิบัติและเพื่อให้หลายองค์กรได้มีแนวทางที่ชัดเจนในการปฏิบัติ ว่าข้อมูลจราจรอะไรบ้างที่ควรจัดเก็บ ข้อมูลอะไรที่ไม่ต้องจัดเก็บ ตลอดจนวิธีการจัดเก็บอย่างถูกต้อง ตรงตามลักษณะการใช้ระบบสารสนเทศหรือระบบอินเทอร์เน็ตของแต่ละองค์กร เช่น การจัดเก็บในลักษณะ “Centralized Log”เป็นต้น

1.2 บทวิเคราะห์ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ บทวิเคราะห์มาตรา 5 ถึง มาตรา 17

มาตรา 5 ถึง มาตรา 10 เป็นการนำหลักการ CIA (Confidentially, Integrity และ Availability) มาประยุกต์ใช้กับการโจมตีของผู้ไม่หวังดีในแบบต่างๆ เช่น การเจาะระบบเข้าไปแอบขโมยสำเนาข้อมูล, การแอบดูชื่อและรหัสผ่านโดยใช้โปรแกรมประเภท Sniffer หรือการโจมตีเปลี่ยนหน้าเว็บไซต์ (Web Defacement, see www.zone-h.org) ตลอดจนการโจมตีให้เว็บไซต์ล่ม (Denial of Services) ล้วนแต่เข้าข้อกฎหมายในมาตรา 5 ถึง มาตรา 10 ทั้งสิ้น ซึ่งมีโทษทั้งจำทั้งปรับมาตรา 11 นั้น เกี่ยวข้องโดยตรงกับผู้ที่ชอบส่ง “SPAM Mail” โดยไม่ระบุชื่อผู้ส่ง ซึ่งมีโทษปรับไม่เกินหนึ่งแสนบาท มาตรา 12 เป็นการกระทำผิดที่มีโทษในกรณีที่มีผลกระทบต่อความมั่นคงทางเศรษฐกิจของประเทศหรือ บริการสาธารณะ โทษสูงสุดถึงจำคุก 15 ปี และปรับถึง 3 แสนบาท แต่ถ้าหากทำให้ผู้อื่นถึงแก่ความตาย โทษจะสูงสุดถึงจำคุก 20 ปีเลยทีเดียว มาตรา 14 ถึง 16 นั้น ผู้ใช้คอมพิวเตอร์ ตลอดจนผู้ให้บริการตามข้อกำหนดของกฎหมาย ต้องระมัดระวังไม่ให้ข้อมูลอัน “ไม่เหมาะสม” ปรากฏอยู่บนอินเทอร์เน็ตในลักษณะการปรากฏของตัวข้อมูลเอง เช่น รูปภาพ หรือ ข้อความ ที่ถูก Upload ขึ้นไป รวมถึง Link ที่พาไปยังข้อมูลดังกล่าวด้วย เพราะฉะนั้นท่านที่ชอบ Forward Mail โดยไม่ระวัง อาจเข้าข้อกฎหมายในมาตราที่ 14 ข้อ 5 ซึ่งมีโทษจำคุกไม่เกิน 5 ปี หรือ ปรับไม่เกิน 1 แสนบาท หรือ ทั้งจำทั้งปรับ เราได้วิเคราะห์ถึงหมวด 1 “ความผิดเกี่ยวกับคอมพิวเตอร์” ตั้งแต่มาตรา 5 ถึง มาตรา 17 โดยที่มาตรา 5, 6, 7, 8, 9, 10 และ มาตรา 12 กล่าวถึง ความผิดที่กระทำต่อคอมพิวเตอร์ และ มาตรา 11 และ มาตรา 13 ถึง มาตรา 16

กล่าวถึงการใช้คอมพิวเตอร์ในการกระทำความผิด ตลอดจนมาตรา 17 กล่าวถึงการกระทำความผิดนอกราชอาณาจักรต้องรับโทษในราชอาณาจักร สรุปสาระสำคัญของมาตรา 5 ถึงมาตรา 17 ได้ดังนี้

ตารางที่ 2.7

หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์

ฐานความผิดและบทลงโทษสำหรับการกระทำโดยมิชอบ	
มาตรา 5	การเข้าถึงระบบคอมพิวเตอร์
มาตรา 6	การล่วงรู้มาตรการการป้องกันการเข้าถึง
มาตรา 7	การเข้าถึงข้อมูลคอมพิวเตอร์
มาตรา 8	การดักข้อมูลคอมพิวเตอร์โดยมิชอบ
มาตรา 9	การรบกวนข้อมูลคอมพิวเตอร์
มาตรา 10	การรบกวนระบบคอมพิวเตอร์
ฐานความผิดและบทลงโทษสำหรับการกระทำโดยมิชอบ	
มาตรา 11	สแปมเมล์ (Spam Mail)
มาตรา 12	การกระทำผิดต่อความมั่นคง
มาตรา 13	การจำหน่าย / เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด
มาตรา 14	การปลอมแปลงข้อมูลคอมพิวเตอร์ / เผยแพร่เนื้อหาอันไม่เหมาะสม
มาตรา 15	ความรับผิดของผู้ให้บริการ
มาตรา 16	การเผยแพร่ภาพจากการตัดต่อ / ดัดแปลง
มาตรา 17	การกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักร

ตารางที่ 2.8

บทกำหนดโทษ

ฐานความผิด	โทษจำคุก	โทษปรับ
มาตรา 5 การเข้าถึงคอมพิวเตอร์โดยมิชอบ	ไม่เกิน 6 เดือน	ไม่เกิน 30,000 บาท
มาตรา 6 ล่วงรู้มาตรการป้องกัน	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
มาตรา 7 การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	ไม่เกิน 2 ปี	ไม่เกิน 40,000 บาท
มาตรา 8 การดักข้อมูลคอมพิวเตอร์	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท
มาตรา 9 การรบกวนข้อมูลคอมพิวเตอร์	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 10 การรบกวนระบบคอมพิวเตอร์ มาตรา 11 สแปมเมล์	ไม่เกิน 5 ปี ไม่มี	ไม่เกิน 100,000 บาท ไม่เกิน 100,000 บาท
มาตรา 12 การกระทำต่อความมั่นคง (1) ก่อความเสียหายแก่ข้อมูลคอมพิวเตอร์ (2) กระทบต่อความมั่นคงปลอดภัยของประเทศ/ เศรษฐกิจวรรคท้าย เป็นเหตุให้ผู้อื่นถึงแก่ชีวิต	 ไม่เกิน 30 ปี 3 ปี ถึง 15 ปี 10 ปี ถึง 20 ปี	 +ไม่เกิน 200,000 บาท 60,000-300,000 บาท ไม่มี
มาตรา 13 การจำหน่าย/เผยแพร่ชุดคำสั่ง	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
มาตรา 14 การเผยแพร่เนื้อหาอันไม่เหมาะสม	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 15 ความรับผิดชอบ ISP	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 16 การตัดต่อภาพผู้อื่น ถ้าสุจริต ไม่มีความผิด	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท

สำหรับมาตรา 18 ถึง มาตรา 30 อยู่ใน *หมวด 2 "พนักงานเจ้าหน้าที่"* ซึ่งรวมถึง ข้อปฏิบัติของผู้ให้บริการที่ต้องให้ความร่วมมือกับพนักงานเจ้าหน้าที่ด้วย

<u>บทวิเคราะห์มาตรา 18 ถึง มาตรา 30</u>

มาตรา 18 ให้อำนาจพนักงานเจ้าหน้าที่ซึ่งผ่านหลักสูตรการฝึกอบรมเรื่อง Computer and Network Forensic และมีคุณสมบัติตามที่กฎกระทรวงกำหนด เช่น ผ่านการสอบ Local Security Certification ที่ทางกระทรวงได้กำหนดขึ้น หรือ ผ่านการสอบ International Security Certification สากลเช่น CompTIA Security+, SSCP หรือ CISSP มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้เพื่อมาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้และสั่งให้ผู้ให้

บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่ เพื่อใช้ข้อมูลดังกล่าวเป็นหลักฐานในการสืบสวนสอบสวนและประกอบการพิจารณาคดี โดยมาตราที่ 18 วรรค 4 ถึง 8 นั้น พนักงานเจ้าหน้าที่ ต้องยื่นคำร้องต่อศาลและขอหมายศาลก่อนถึงจะมีอำนาจสำเนาข้อมูล ส่งให้ส่งมอบ, ตรวจสอบเข้าถึง, ถอดรหัส สลักข้อมูล รวมทั้งการยึดและอายัดระบบ ทั้งนี้ในมาตรา 19 บัญญัติไว้ว่าพนักงานเจ้าหน้าที่ต้องส่งสำเนาบันทึกรายละเอียดให้แก่ศาลภายใน 48 ชม. และจะยึด/อายัดห้ามเกิน 30 วันขยายได้เต็มที่อีกไม่เกิน 60 วัน สำหรับมาตรา 20 ได้บัญญัติถึงเรื่องการระงับการทำให้แพร่หลายของข้อมูลที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรหรือข้อมูลที่มีลักษณะต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน ยกตัวอย่าง เช่น พนักงานเจ้าหน้าที่มีอำนาจในการ Block เว็บไซต์ที่ไม่เหมาะสม เป็นต้น และในมาตรา 21 พนักงานเจ้าหน้าที่สามารถร้องขอให้ศาลมีคำสั่งห้ามจำหน่ายหรือเผยแพร่หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้งานและทำลายข้อมูลนั้นได้ โดยที่ชุดคำสั่งไม่พึงประสงค์ หมายถึง มัลแวร์ (MalWare) ต่างๆ เช่น ไวรัส, หนอนคอมพิวเตอร์ (worm), ม้าโทรจัน, สปายแวร์ ตลอดจน โปรแกรม Hacking Tool ต่าง ๆ พนักงานเจ้าหน้าที่ก็มีความรับผิดชอบในการเก็บรักษาข้อมูลที่ได้มาเช่นกัน ดังที่บัญญัติไว้ในมาตราที่ 22 ถึงมาตรา 24 ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลที่ได้มาตามมาตรา 18 แก่บุคคลใด หากฝ่าฝืน พนักงานเจ้าหน้าที่ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือ ปรับไม่เกิน 6 หมื่นบาท หรือ ทั้งจำทั้งปรับ โดยในมาตรา 23 หากพนักงานเจ้าหน้าที่ประมาทเลินเล่อ ทำให้ผู้ล่วงรู้ข้อมูลดังกล่าวต้องระวางโทษทั้งจำคุกและปรับและ มาตรา 24 ได้บัญญัติผู้อื่นที่ล่วงรู้ข้อมูลที่ได้ว่าจากพนักงานเจ้าหน้าที่ก็มีโทษจำคุกและปรับ เช่นเดียวกันกับพนักงานเจ้าหน้าที่ ที่ปฏิบัติตนไม่ชอบ

ผลสำรวจทางสถิติ

1. ผลการสำรวจการจัดอันดับภัยอินเทอร์เน็ต 10 อันดับ ในปี ค.ศ. 2008[1] มีดังต่อไปนี้

อันดับที่ 1 ภัยจากการถูกขโมยชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานระบบออนไลน์ผ่านทางอินเทอร์เน็ต (Username/Password and Identity Theft)

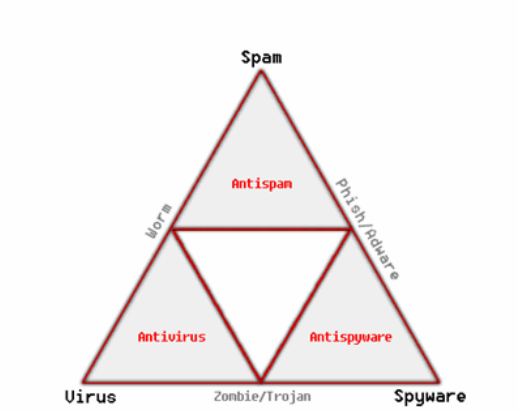
อันดับที่ 2 ภัยจากการโจมตี Web Server และ Web Application

อันดับที่ 3 ภัยข้ามระบบ (Cross-platform/Multi-platform Attack)

อันดับที่ 4 ภัยจากการถูกขโมยข้อมูล หรือ ข้อมูลความลับรั่วไหลออกจากองค์กร (Data Loss/Leakage and Theft)

อันดับที่ 5 ภัยจากมัลแวร์และสามเหลี่ยมแห่งความชั่วร้าย (SPAM , VIRUS and SPYWARE)

ภาพที่ 2.6 แสดงสามเหลี่ยมแห่งความชั่วร้าย



อันดับที่ 6 ภัยจากการใช้โปรแกรมประเภท Peer-to-Peer (P2P) และ Instant Messaging (IM)

อันดับที่ 7 ภัยจากแฮกเกอร์มืออาชีพข้ามชาติ (Professional International Blackhat Attack)

อันดับที่ 8 ภัยไร้สายจากการใช้งานอุปกรณ์ Mobile และ Wireless (Mobile/Wireless Attack)

---

[1] แหล่งที่มา : หนังสือ eLeader Thailand ประจำเดือน เดือนกุมภาพันธ์ 2551

อันดับที่ 9 ภัยจากการโจมตีด้วยเทคนิค DoS (Denial of Services) หรือ DDoS (Distributed Denial of Services) Attack

อันดับที่ 10 ภัยที่เกิดขึ้นจากตัวของเราเอง (Negligence Information Security)

2. ผลการสำรวจการจัดอันดับภัยอินเทอร์เน็ต 10 อันดับ ในปี ค.ศ. 2008[2] (Top 10 Cyber Security Issues for 2008) มีดังต่อไปนี้

อันดับที่ 1 Preparation for Cyber Warfare

อันดับที่ 2 Protecting Our Critical Infrastructure

อันดับที่ 3 Data Vulnerability and Protection

อันดับที่ 4 Software Bugs are a National Security Issue

อันดับที่ 5 Economic Costs of Software Bugs

อันดับที่ 6 Software Bugs Can Cost Lives

อันดับที่ 7 Alternative Devices

อันดับที่ 8 Foreign Software Influence

อันดับที่ 9 Protecting Our Financial Infrastructure

อันดับที่ 10 Identity Theft – A Terrorist Tool

3. ผลสรุปสาเหตุที่เหยื่อถูกโจมตีไว้ 10 สาเหตุหลัก[3] มีรายละเอียดดังนี้

สาเหตุที่ 1 ความไม่เข้าใจในเรื่องความปลอดภัยข้อมูลอย่างเพียงพอ (No or Not Enough Information Security Awareness)

สาเหตุที่ 2 ความไม่ตระหนัก และ ไม่เข้าใจเรื่องการบริหารความเสี่ยงและการประเมินความเสี่ยง (No Risk Management Awareness)

สาเหตุที่ 3 ความไม่เข้าใจในหลัก "GRC" (Governance Risk and Compliance) (No GRC Awareness)

---

[2] แหล่งที่มา Spy-Ops , Author by Kevin G. Coleman

[3] แหล่งที่มา : หนังสือ eLeader Thailand ประจำเดือน เดือนกุมภาพันธ์ 2551

สาเหตุที่ 4 การไม่มีแนวนโยบายและแนวทางปฏิบัติที่เกี่ยวกับความปลอดภัยข้อมูลในองค์กร (No Information Security Policy and Guideline)

สาเหตุที่ 5 ความไม่ใส่ใจปฏิบัติตามแนวนโยบายและแนวทางปฏิบัติที่เกี่ยวกับความปลอดภัยข้อมูล เนื่องจากองค์กรไม่มีการฝึกอบรม "Security Awareness Training" และไม่มีเอกสาร "Acceptable Use Policy" (No Policy Enforcement)

สาเหตุที่ 6 ผู้บริหารระดับสูงขององค์กรไม่ให้ความสำคัญเรื่องความปลอดภัยข้อมูลอย่างเพียงพอ หรือไม่จริงจังในการผลักดันเรื่องความปลอดภัยข้อมูล (Top Management Security Awareness Ignorance)

สาเหตุที่ 7 ไม่มีการนำ "Best Practices" ต่างๆ เช่น CobiT หรือ ITIL มาประยุกต์ใช้ในองค์กร ในการปรับปรุง Process ภายใน (No Best Practices Implementation)

สาเหตุที่ 8 การไม่ปฏิบัติตามมาตรฐานด้านความปลอดภัยข้อมูล เช่น ISO/IEC 27001 เป็นต้น (No Information Security Standard)

สาเหตุที่ 9 ความไม่เข้าใจในเรื่องการควบคุมภายใน (Internal Control) และการตรวจสอบระบบสารสนเทศ (IT Audit) (No IT audit and control awareness)

สาเหตุที่ 10 การที่เราไม่มีความรู้มากเพียงพอเท่าทันกับการโจมตีแบบใหม่ๆของแฮกเกอร์ (No new/update Information Security Knowledge) เนื่องจากไม่ได้ Update ข้อมูลใหม่ๆ จากการอ่าน Magazine หรือ การเข้าฟังงานสัมมนา ตลอดจนขาดการฝึกอบรมความรู้เรื่องความปลอดภัยข้อมูลอย่างสม่ำเสมอ

4. ผลสำรวจความตื่นตัวของภาคธุรกิจ ในการจัดทำ Privacy Policy[4] (พฤศจิกายน 2006) สำรวจจาก websites จำนวนทั้งสิ้น 730 websites :

ตารางที่ 2.9

ผลสำรวจความตื่นตัวของภาคธุรกิจ ในการจัดทำ Privacy Policy

ประเภทอุตสาหกรรม	จำนวนเว็บไซต์	เปอร์เซ็นต์
บริษัทในตลาดหลักทรัพย์	187	25.62
หน่วยงานของรัฐและรัฐวิสาหกิจ	155	21.23
สถาบันการศึกษา	105	14.38
อุตสาหกรรมท่องเที่ยว	100	13.70
สถาบันการเงิน	68	9.32
กลุ่มธุรกิจการให้บริการความปลอดภัย	52	7.12
ผู้ให้บริการบนเว็บไซต์	39	5.34
ผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต	24	3.29

งานวิจัยที่เกี่ยวข้อง

1. งานวิจัยเรื่อง "นโยบายการรักษาความปลอดภัยสารสนเทศ กรณีศึกษาบริษัท XYZ จำกัด"

โดย รังสิต งามพรประเสริฐ ปี พ.ศ. 2547 เป็นงานวิจัยเพื่อศึกษาแนวทางการสร้างนโยบายการรักษาความปลอดภัยของข้อมูลที่มีการนำเทคโนโลยีสารสนเทศต่างๆ มาใช้ และศึกษาวิธีการวิเคราะห์ความเสี่ยงของสารสนเทศของบริษัท XYZ โดยใช้มาตรฐาน ISO17799 เป็นเครื่องมือในการ สร้างนโยบายดังกล่าว ผลที่ได้จากงานวิจัยทำให้สามารถสรุปความเสี่ยงหลักขององค์กรได้จากการประเมินความเสี่ยง ได้แก่ การโจมตีจากไวรัสผ่านทางอินเทอร์เน็ต , การให้ข้อมูลแก่ลูกค้าและคู่ค้า และมีการจัดเก็บข้อมูลสำคัญและอีเมล์ไว้ที่เครื่องลูกข่าย เป็นต้น ซึ่งได้มีการนำประเด็นที่มีความเสี่ยงสูงมาพิจารณาแก้ไขและปรับปรุง เพื่อลดหรือป้องการความเสี่ยงนั้นๆ และ

[4] แหล่งที่มา : ผลการสำรวจของ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

จากการเก็บรวบรวมข้อมูลและศึกษาพบว่าแนวทางการจัดการความปลอดภัยสารสนเทศควรครอบคลุมทั้งประเด็นด้านเทคนิคและการบริหารจัดการ ซึ่งแนวทางที่ได้รับความนิยมและได้รับการพิสูจน์แล้วคือ มาตรฐาน ISO 17799 จึงสามารถสรุปการจัดทำนโยบายด้านความปลอดภัยข้อมูลออกเป็น 2 ส่วนคือ แนวทางการบริหารจัดการและแนวทางการจัดการทางเทคนิค

งานวิจัยนี้ได้มีการศึกษาแนวคิดและทฤษฎีต่างๆ เพื่อใช้ในการสร้างนโยบายการรักษาความปลอดภัยของข้อมูล ได้แก่ Information Security , ISMF , BS ISO/IEC 17799:2000 , กระบวนการพัฒนาความปลอดภัยอย่างต่อเนื่อง (Model PDCA) และการวิเคราะห์ความเสี่ยง ซึ่งในการทำงานวิจัยเรื่อง “การศึกษาและจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544” ไดนำในส่วนของการประเมินความเสี่ยงซึ่งเป็นส่วนหนึ่งในทฤษฎีการวิเคราะห์ความเสี่ยง ที่มีการใช้แบบจำลองที่มีการกำหนดระดับความรุนแรงและโอกาสในการเกิดความเสี่ยงเพื่อนำมากำหนดระดับความเสี่ยงมาใช้เป็นแนวทางในการทำวิจัย แต่ในส่วนของโอกาสในการเกิดความเสี่ยงที่ใช้ข้อมูลจากแหล่งข้อมูลจากการสำรวจหรือจากความเห็นของผู้ดูแลระบบ และระดับความรุนแรงที่เกิดขึ้นซึ่งเก็บรวบรวมจากผู้ดูแลระบบนั้นไม่มีสถิติหรือมาตรฐานใดๆมารองรับ ทำให้ขาดความน่าเชื่อถือและอาจเกิดความผิดพลาดในการประเมินความเสี่ยงขึ้นได้

2. งานวิจัยเรื่อง “ความคุ้มค่าในการนำมาตรฐาน BS 7799 มาใช้ในองค์กร”

โดยนาย Frank-Arne Stamland ปี 2547 จากการศึกษาแนวทางการจัดการความมั่นคงปลอดภัยสารสนเทศพบว่ามาตรฐาน ISO 27001 นั้นได้รับความนิยม และให้การรองรับมาตรฐานระดับนานาชาติ ซึ่งเป็นแนวทางที่เน้นเชิงการจัดการมากกว่าทางเทคนิค ซึ่งเหมาะสมต่อการสร้างนโยบายให้เข้าใจได้ง่าย ซึ่งวิทยานิพนธ์นี้มีวัตถุประสงค์ในการศึกษาความสามารถในการป้องกันตรวจสอบ และการตอบสนองต่อเหตุการณ์ทางด้านการละเมิดความปลอดภัยของข้อมูลองค์กร ที่นำมาตรฐาน BD 7799 มาใช้ด้วยสมมติฐานว่าจะสามารถลดการละเมิดความปลอดภัยเหล่านั้นได้ นอกจากนี้ยังได้ศึกษาเปรียบเทียบกับองค์กรที่นำมาตรฐาน BS 7799 มาใช้เป็นแนวทาง แต่ไม่ได้ของการรับรอง และองค์กรที่ไม่ได้ใช้มาตรฐานใดๆ

ในวิทยานิพนธ์นี้ มีการเก็บข้อมูลจากแบบสอบถามที่ส่งให้ผู้จัดการฝ่ายความมั่นคงปลอดภัยสารสนเทศ และเจ้าหน้าที่ความมั่นคงปลอดภัยสารสนเทศขององค์กร ที่มีการนำระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System ISMS) มาใช้ในองค์กร

โดยในแบบสอบถามได้มีการจัดเก็บข้อมูลดังนี้

- ข้อมูลการจัดทำนโยบายการจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กรและเก็บ
- ส่วนของการจัดการความมั่นคงปลอดภัยสารสนเทศของ ที่มีการนำมาปฏิบัติใช้ และแนวทางปฏิบัติเป็นอย่างไร
- รวมถึงการเก็บรวบรวมข้อมูลที่เกี่ยวข้องในการวัดการเจริญเติบโต (Maturity) ของการจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งจะสะท้อนให้เห็นสถานะของความมั่นคงปลอดภัยสารสนเทศขององค์กร

เมื่อเก็บรวบรวมข้อมูลแล้ว ได้นำมาวิเคราะห์ระดับการเจริญเติบโต (Maturity) ของการจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งได้กำหนดระดับการเจริญเติบโตไว้ 6 ระดับดังนี้

ระดับ 0 ระดับที่ไม่มีความมั่นคงปลอดภัยสารสนเทศ

ไม่มีกระบวนการจัดการความมั่นคงปลอดภัยสารสนเทศ

ระดับ 1 ระดับเริ่มต้น

มีลักษณะของการจัดการเป็นแบบชั่วคราว และมีความยุ่งยากในบ้างครั้ง มีการระบุกระบวนการต่างๆ เพียงเล็กน้อย และความสำเร็จขึ้นอยู่กับความพยายาม และจริงจังในส่วนบุคคล

ระดับ 2 ระดับที่สามารถทบทวนได้

กระบวนการการจัดการโครงการขั้นพื้นฐานที่สามารถตรวจสอบงบประมาณ เวลาและงานที่ต้องการย้อนหลังได้ มีระเบียบวินัยในการปฏิบัติตามกระบวนการตามความจำเป็น โดยใช้ปัจจัยต่างๆ ต่อไปนี้ในการชี้วัด

- การจัดการด้านความต้องการ (Requirement Management)
- การวางแผนโครงการซอฟต์แวร์ต่างๆ (Software Project Planning)
- การตรวจสอบและพิจารณาความผิดพลาดโครงการซอฟต์แวร์ต่างๆ (Software Project Tracking and Oversight)
- การจัดการองค์กรที่ทำสัญญารับงานพัฒนาซอฟต์แวร์ (Software Subcontract Management)

- การรับประกันคุณภาพซอฟต์แวร์ (Software Quality Assurance)
- การจัดการการกำหนดค่าและการทำงานของซอฟต์แวร์ (Software Configuration Management)

ระดับที่ 3 ระดับที่สามารถกำหนดได้

มีการจัดทำเอกสารทางด้านการจัดการและทางเทคนิคซึ่งมีมาตรฐาน และสามารถนำมาใช้ร่วมกับซอฟต์แวร์ ด้านกระบวนการทำงานองค์กรทุกโครงการ ต้องได้รับการตรวจสอบโดยมีกระบวนการในการพัฒนา และดูแลรักษาซอฟต์แวร์มาตรฐานขององค์กร โดยใช้ปัจจัยต่างๆ ต่อไปนี้ในการชี้วัด

- มุ่งเน้นกระบวนการขององค์กร (Organization Process Focus)
- การกำหนดกระบวนการขององค์กร (Organization Process Definition)
- โปรแกรมการฝึกอบรม (Training Program)
- การจัดการการเชื่อมต่อซอฟต์แวร์ (Integrated Software Management)
- การวิจัยและพัฒนาผลิตภัณฑ์ซอฟต์แวร์ (Software Product Engineering)
- การประสานงานระหว่างฝ่าย (Intergroup Coordination)
- การตรวจสอบฝ่ายอื่นๆ (Peer Reviews)

ระดับ 4 ระดับที่ได้รับการจัดการ

มีการประเมินรายละเอียดของกระบวนการในซอฟต์แวร์และคุณภาพของสินค้า โดยมีความเข้าใจเชิงคุณภาพ และมีการควบคุมทั้งกระบวนการในซอฟต์แวร์ และตัวผลิตภัณฑ์ซอฟต์แวร์ โดยใช้ปัจจัยต่างๆ ต่อไปนี้ในการชี้วัด

- การจัดการกระบวนการเชิงคุณภาพ (Quantitative Process Management)
- การจัดการคุณภาพซอฟต์แวร์ (Software Quality Management)

ระดับ 5 ระดับที่มีการใช้อย่างคุ้มค่า

มีการพัฒนากระบวนการต่างๆ อย่างต่อเนื่องโดยข้อมูลผลตอบรับจากกระบวนการต่างๆ และจากการนำแนวคิดด้านนวัตกรรม และเทคโนโลยีมาปรับใช้ในองค์กร โดยใช้ปัจจัยต่างๆ ต่อไปนี้ในการชี้วัด

- การป้องกันการเกิดความเสียหาย (Defect Prevention)

- การจัดการการเปลี่ยนแปลงทางเทคโนโลยี (Technology Change Management)
- การจัดการการเปลี่ยนแปลงกระบวนการ (Process Change Management)

3. งานวิจัยเรื่อง "การวิเคราะห์ความเสี่ยงการรักษาความปลอดภัยของข้อมูลสำหรับองค์กรขนาดใหญ่และขนาดกลาง ในเขตกรุงเทพมหานคร"

โดย ทรงชล มหารมณ์ จากการศึกษาถึงภัยคุกคาม และปัจจัยที่ก่อให้เกิดความเสี่ยงที่เป็นพฤติกรรม และลักษณะการทำงานของบุคลากรในองค์กร ในการรักษาความปลอดภัยข้อมูลสารสนเทศขององค์กรขนาดกลาง และขนาดใหญ่ โดยการแยกประเภทของความเสี่ยงตามความปลอดภัยของข้อมูล ได้แก่ ความเชื่อถือ (Confidentiality) ความถูกต้องและสมบรูณ์ (Integrity) และความสามารถในการนำมาใช้ประโยชน์ได้เมื่อต้องการ (Availability) ความเสี่ยงที่เป็นไปได้ว่าจะเกิดขึ้นกับความปลอดภัยของข้อมูล

จากงานวิจัยพบว่าภัยคุกคามที่ก่อให้เกิดความเสี่ยงต่อการรักษาความปลอดภัยข้อมูล ที่มีความเสี่ยงในระดับสูง ซึ่งองค์กรขนาดกลาง และใหญ่ควรให้ความสนใจ และหาแนวทางการแก้ไข ซึ่งในที่นี่จะยกแนวทาง 8 ภัยคุกคาม เรียงลำดับตามความเสี่ยงจากสูงไปต่ำดังนี้

1. การใช้ชื่อ (User ID) ร่วมกันเพื่อเข้าใช้ข้อมูล
2. การรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด
3. การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้
4. การปกป้องรหัสผ่าน (Password) อย่างไม่เหมาะสม
5. การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม
6. พนักงานขาดการฝึกอบรมด้านเทคนิคอย่างเหมาะสม
7. ระบบรักษาความปลอดภัยข้อมูล และขั้นตอนการให้สิทธิการใช้งาน ไม่มีการเปลี่ยนแปลงให้ทันสมัย
8. การออกแบบระบบซับซ้อนเกินไป

ซึ่งภัยคุกคามดังกล่าวส่วนหนึ่งจะมาจาก การที่ภายในองค์กรมีการเชื่อมต่ออินเตอร์เน็ต ทำให้ผู้บุกรุกที่จะเข้ามาสร้างปัญหาให้กับองค์กร สามารถเข้ามาทางเครือข่ายอินเตอร์เน็ต หากระบบการรักษาความปลอดภัยขององค์กรไม่มีประสิทธิภาพมากเพียงพอ อย่างไรก็ตาม ความเสี่ยงสามารถเกิดขึ้นได้จากภายในองค์กรเองเช่นกัน เมื่อผู้บุกรุกเป็นพนักงานในองค์กร

แนวทางการป้องกันและแก้ปัญหาจากภัยคุกคามที่เกิดขึ้น ควรจะสอดคล้องกับการจัดการบริหารระบบความปลอดภัยที่มีประสิทธิภาพ ซึ่งโดยสรุปแล้วสามารถแบ่งได้เป็น การควบคุมความเสี่ยงในการรักษาความปลอดภัยข้อมูลขององค์กรเป็น 3 ส่วนหลักๆ ได้แก่

1. การควบคุมที่เกี่ยวข้องกับบุคลากรในองค์กร เช่นการจัดฝึกอบรมพนักงาน

2. การควบคุมที่เกี่ยวข้องกับกระบวนการทำงานและนโยบายองค์กร เช่น การควบคุมการเข้าใช้ข้อมูล (Access Control) ,การสำรองและกู้ข้อมูล (Back up and Recovery) เพื่อเป็นการป้องกันการสูญหายของข้อมูลที่ยังใช้งานอยู่

3. การควบคุมที่เกี่ยวข้องกับการใช้เทคโนโลยีภายในองค์กร เช่น การจัดทำกระบวนการและนโยบายที่เหมาะสมในการควบคุมใช้งานเทคโนโลยีต่างๆ

4. งานวิจัยเรื่อง "การศึกษาและจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544"

โดย นายนริทธ์ จินดาจามร, นางสาวขวัญตา วรรณโภคิน, นายอรรฆพล คุ้มเศรณี

งานวิจัยเรื่องนี้มีวัตถุประสงค์หลักเพื่อกำหนดแนวปฏิบัติที่เป็นรูปธรรมในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้กับองค์กรภาครัฐและภาคเอกชนที่เกี่ยวข้องกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์ อ้างอิงตามมาตรฐานความปลอดภัยสากล ISO/IEC17799:2005 ประกอบร่างพระราชกฤษฎีกา มาตรา 25, มาตรา 32 และมาตรา 35 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

ในการศึกษาวิจัยครั้งนี้จะเป็นการนำเอามาตรฐานความปลอดภัยสากล ISO/IEC17799 : 2005 และหลักการบริหารความเสี่ยง (Risk Management) มาใช้ เพื่อเป็นแนวทางให้กับกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ โดยใช้วิธีการเก็บรวบรวมข้อมูล ด้วยการส่งแบบสอบถาม ซึ่งจะแบ่งเป็น 2 ส่วนดังนี้

- ส่วนแรกจะเป็นการจัดระดับของมาตรการในการรักษาความปลอดภัย ISO/IEC 17799:2005 และการจับคู่ประเด็นความเสี่ยงทางด้านเทคโนโลยีสารสนเทศกับมาตรฐานความปลอดภัยสากล ISO/IEC 17799:2005 โดยคัดเลือกกลุ่มตัวอย่างจากบุคคลซึ่งเป็นผู้เชี่ยวชาญในด้านความมั่นคงปลอดภัยสารสนเทศ

- ส่วนที่สองจะเป็นการประเมินระดับความเสี่ยงหน่วยงานภาครัฐและภาคเอกชนที่อยู่ภายใต้กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ฉบับนี้ โดยการเก็บรวมรวบข้อมูลและทำการวัดค่า

ความจำเป็น (Scoring Model) ในด้านรักษาความปลอดภัยเพื่อป้องกันหรือลดความเสี่ยงที่อาจจะเกิดขึ้น เพื่อนำมาสู่การสร้างแนวปฏิบัติ (Practice Statement) ที่สอดคล้องกับมาตรฐานความปลอดภัยสากล ISO/IEC17799:2005

และเมื่อนำข้อมูลที่ได้จากแบบสอบถามมาเข้าสู่แบบจำลองที่ได้จัดทำขึ้น จะสามารถระบุข้อปฏิบัติที่แต่ละหน่วยงานนั้นๆ ต้องปฏิบัติตามมาตรฐานความปลอดภัยสากล ISO/IEC17799:2005 โดยผลของงานวิจัยฉบับนี้จะระบุข้อปฏิบัติให้กับหน่วยงานต่างๆ ที่เป็นกลุ่มตัวอย่าง ซึ่งมีรายละเอียดดังต่อไปนี้

- ข้อปฏิบัติที่จำเป็นจะต้องปฏิบัติตาม (Must to do) อย่างเข้มข้น
- ข้อปฏิบัติที่ปฏิบัติตามระดับความเสี่ยงด้านสารสนเทศที่ประเมินได้จากแบบสอบถาม ซึ่งแบ่งได้เป็น 3 ระดับ ดังนี้ Best Practice, Accredit และ Mandatory

จากงานวิจัยพบว่า การที่หน่วยงานภาครัฐและภาคเอกชน จะสามารถปฏิบัติตามกฎหมายฉบับนี้ โดยนำมาตรฐานความปลอดภัยสากล ISO/IEC17799:2005 มาใช้อ้างอิงได้นั้น จำเป็นจะต้องมีการประเมินระดับความเสี่ยงด้านสารสนเทศของหน่วยงานนั้นๆ ก่อน หลังจากนั้นจึงเข้าสู่แบบจำลองที่ได้จัดทำขึ้นในงานวิจัยฉบับนี้ เพื่อกำหนดแนวปฏิบัติที่เป็นรูปธรรมในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้กับหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องกับการประกอบธุรกรรมทางอิเล็กทรอนิกส์

5. งานวิจัยเรื่อง “การสร้างมาตรฐานการบริหารความปลอดภัยของข้อมูล โดยการประยุกต์ใช้ ISO 17799” กรณีศึกษา ของบริษัทให้บริการด้านการจัดซื้อออนไลน์

โดย เพ็ญประภา พิพัฒนาโฆษิต โดยงานวิจัยเรื่องนี้มีวัตถุประสงค์เพื่อทำการศึกษาแนวทางขั้นตอนการดำเนินงาน สำหรับการประยุกต์ใช้มาตรฐานสากล ISO 17799 ในการรักษาความปลอดภัยของข้อมูล ระบบคอมพิวเตอร์และระบบสารสนเทศในองค์กรที่ให้บริการด้านการจัดซื้อออนไลน์(e-Procurement) และเพื่อศึกษาปัจจัยที่มีผลต่อความเสี่ยงด้านความปลอดภัยของข้อมูลที่อาจเกิดขึ้นกรณีที่องค์กรขาดการป้องกัน และสรุปเป็นนโยบายนำเสนอแก่ผู้บริหารขององค์กร สำหรับนำไปจัดทำนโยบายเพิ่มเติมและปรับปรุงองค์กรเพื่อให้เหมาะสมกับการพัฒนาทางธุรกิจ

ในการศึกษาวิจัยครั้งนี้จะเป็นการนำเอามาตรฐานความปลอดภัยสากล ISO/IEC 17799:2005 และนำหลักการบริหารความเสี่ยง (Risk Management) มาใช้ โดยใช้สูตร

ระดับความเสี่ยง (R) = โอกาสเกิดภัยคุกคาม (L) x ความรุนแรงของผลกระทบ (I)

เมื่อหาค่าระดับความเสี่ยง ได้แล้วจะค่าไปเทียบในตาราง เมตริกซ์ 5 x 5 จะได้ระดับความเสี่ยงที่เกิดขึ้นในแต่ละเหตุการณ์

ซึ่งจากผลการศึกษาพบว่าองค์กรตัวอย่างได้ให้ความสำคัญต่อการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศเป็นอย่างมาก เนื่องจากรูปแบบธุรกิจที่ให้บริการมีความเกี่ยวข้องกับระบบสารสนเทศและการจัดเก็บข้อมูลที่เป็นความลับของลูกค้าอยู่เป็นจำนวนมาก โดยผลจากการวิเคราะห์พบว่าความเสี่ยงที่มีระดับสูงที่พบในองค์กรมีทั้งหมด 7 ภัยคุกคาม ได้แก่ การเก็บรวบรวมข้อมูลสำคัญไว้ที่เดียวกันหมด ,การสูญเสียลูกค้าเนื่องจากระบบไม่สามารถให้บริการได้ ,การใช้ชื่อ (User ID)ร่วมกันเพื่อเข้าใช้ข้อมูล ,การพิมพ์ข้อมูลสำคัญโดยปราศจากการควบคุม ,ผู้บุกรุกสามารถเข้าถึง (Access) เครื่องคอมพิวเตอร์ในองค์กรได้ ,Router / Firewall เสียทำให้ไม่สามารถใช้งานได้ และ ฐานข้อมูล(database)ถูกขัดจังหวะการทำงาน(corrupt)เนื่องจากฮาร์ดแวร์หรือซอฟแวร์อาจทำงานผิดพลาด

ซึ่งการวิเคราะห์ผลนั้นพบว่าทั้ง 7 คุกคาม องค์กรได้ให้ความตระหนักในการป้องกันอยู่ก่อนแล้ว เช่น มีมาตรการในการป้องกันและรักษาความปลอดภัย, จัดทำแผนสำรองกรณีฉุกเฉิน, จัดเตรียมสถานที่ที่เหมาะสม, จัดทำระบบสำรอง เป็นต้น แต่จากการประเมินที่ยังพบความเสี่ยงสูงอยู่ อาจเนื่องมากจากการขาดการประชามสัมพันธ์ให้แก่บุคลากรในองค์กรให้ทั่วถึง ทำให้การรับทราบเกิดเฉพาะในกลุ่มที่ทำงานหรือมีความเกี่ยวข้องกับระบบสารสนเทศโดยตรง

ดังนั้นทางผู้วิจัยจึงได้ทำการทดสอบสมมติฐาน โดยอิงมาตรฐาน ISO 17799 โดยทดสอบความสัมพันธ์ในแต่ละข้อของ ISO 17799 กับ ตัวแปรอิสระคือ หน่วยงานทางด้าน IT กับ Non-IT และจาก ช่วงอายุงานในการทำงานที่องค์กรปัจจุบัน ซึ่งผลส่วนใหญ่แตกต่างกันไปในแต่ละหัวข้อ เพื่อให้ผู้บริหารนำไปประกอบการพิจารณาจัดทำแผนในการพัฒนาหรือให้ความสำคัญตามแต่ละกลุ่มที่แตกต่างกันออกไป