บทที่ 2

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

ปัจจุบัน ความเสี่ยงหรือภัยคุกคามต่างๆที่สามารถสร้างความเสียหายต่อองค์กรนั้นได้เพิ่มจำนวนขึ้นเป็นอย่างมาก ไม่ว่าจะเป็นในเรื่องของการขโมยข้อมูลสารสนเทศที่เป็นความลับขององค์กรไปใช้ในทางที่มิชอบ การสร้างความปั่นป่วนให้กับระบบเครือข่ายขององค์กรตลอดจนการทำลายระบบคอมพิวเตอร์ขององค์กรจนไม่สามารถให้บริการได้ เป็นต้น ซึ่งองค์กรต่างๆที่มีระบบเทคโนโลยีสารสนเทศไว้สำหรับใช้ดำเนินกิจการภายในขององค์กรหรือไว้สำหรับให้บริการลูกค้านั้น ควรจะได้มีความตระหนักถึงภัยคุกคามเหล่านี้ และควรมีการจัดหามาตรการที่เหมาะสมต่างๆเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้ในอนาคต

ในส่วนของธนาคารพาณิชย์เองก็คงไม่สามารถหลีกเลี่ยงความจำเป็นในการจัดหามาตรการต่างๆเพื่อเฝ้าระวังและป้องกันภัยคุกคามที่อาจเกิดขึ้นกับบริการทางการเงินผ่านอินเทอร์เน็ตของตนเช่นเดียวกัน เนื่องจากในปัจจุบันบริการทางการเงินผ่านอินเทอร์เน็ตนั้นถือเป็นช่องทางในการทำธุรกรรมทางการเงินที่สะดวก รวดเร็ว และมีประสิทธิภาพ แต่ในขณะเดียวกันก็อาจเป็นช่องทางให้ผู้ไม่ประสงค์ดีเข้ามาเจาะระบบเพื่อนำข้อมูลสำคัญต่างๆของลูกค้าออกไปได้ ซึ่งความเสียหายที่เกิดขึ้นนั้นย่อมตกอยู่กับลูกค้าและธนาคารเป็นสำคัญ ไม่ว่าจะเป็นเรื่องของการเจาะระบบเพื่อขโมยรหัสประจำตัวและรหัสผ่านเข้าสู่ระบบ การลักลอบดูรายการทางการเงินในบัญชีของลูกค้า หรือการลักลอบเพิ่มบัญชีบุคคลที่สามและโอนเงินของลูกค้าออกไปยังบัญชีนั้นโดยที่ลูกค้าไม่รู้ตัว เป็นต้น ซึ่งความเสียหายที่อาจเกิดขึ้นกับธนาคารนั้นนอกจากจะอยู่ในรูปตัวเงินแล้วยังหมายรวมถึงภาพลักษณ์ที่ดีของธนาคาร ซึ่งไม่สามารถประเมินมูลค่าได้เลยอีกด้วย

จากความจำเป็นและความสำคัญดังกล่าว ทำให้องค์กรต่างๆรวมถึงธนาคารพาณิชย์จำเป็นต้องทบทวนและปรับปรุงนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศของตน โดยอาจจะอ้างอิงมาจากมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลสารสนเทศในปัจจุบันซึ่งมีหลายมาตรฐานและเป็นที่ยอมรับว่าเป็นมาตรฐานที่มีความน่าเชื่อถือ เช่น มาตรฐาน ISO/IEC 17799:2005 และมาตรฐาน ISO/IEC 27001:2005 เป็นต้น

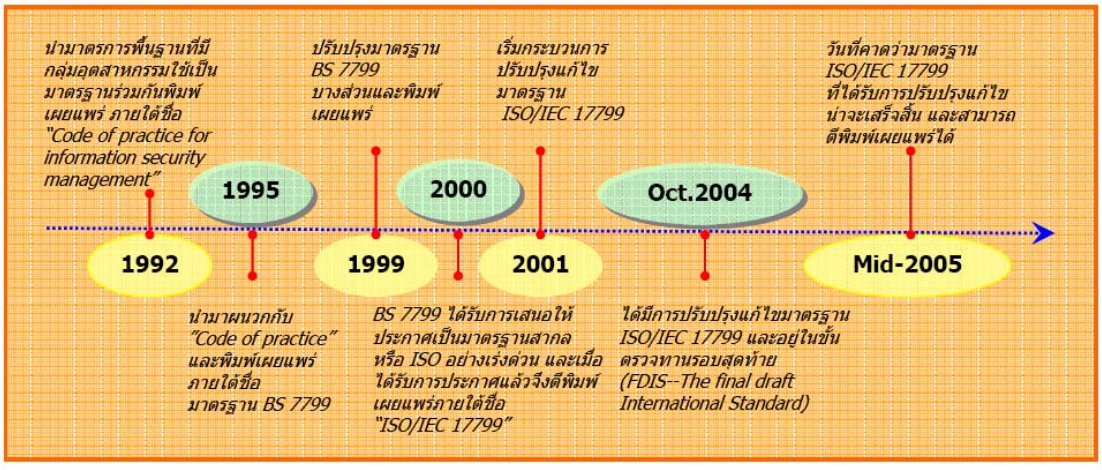
อย่างไรก็ตาม องค์กรต่างๆอาจไม่จำเป็นต้องดำเนินการตามมาตรฐานใดมาตรฐานหนึ่งเพียงมาตรฐานเดียว แต่ควรต้องทำความเข้าใจแนวคิดและข้อปฏิบัติของมาตรฐานต่างๆอย่างละเอียดและนำมาพัฒนาเป็นนโยบายทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่เหมาะสมกับลักษณะการดำเนินกิจการของตน เพื่อเป็นการป้องกันความเสียหายหรือลดความเสี่ยงที่อาจเกิดขึ้นให้อยู่ในระดับที่องค์กรสามารถยอมรับได้

มาตรฐาน ISO/IEC 17799:2005

มาตรฐาน ISO/IEC 17799:2005 เป็นมาตรฐานการจัดการด้านความปลอดภัยของข้อมูล ที่เน้นที่ระบบการบริหารจัดการภายในองค์กรเพื่อรักษาความปลอดภัยของข้อมูล โดยมีข้อกำหนดต่างๆตั้งแต่กระบวนการนำข้อมูลมาใช้และการจัดเก็บข้อมูล ตลอดจนการมีแผนรับมือเมื่อเกิดเหตุฉุกเฉินขึ้นกับข้อมูล เพื่อให้องค์กรสามารถปฏิบัติตัวได้อย่างถูกต้อง และสามารถกู้ข้อมูลกลับขึ้นมาเพื่อทำให้องค์กรสามารถดำเนินกิจกรรมของตนต่อไปตามปกติได้อย่างรวดเร็วที่สุด

ภาพที่ 2.1

พัฒนาการของมาตรฐาน ISO/IEC 17799:2005



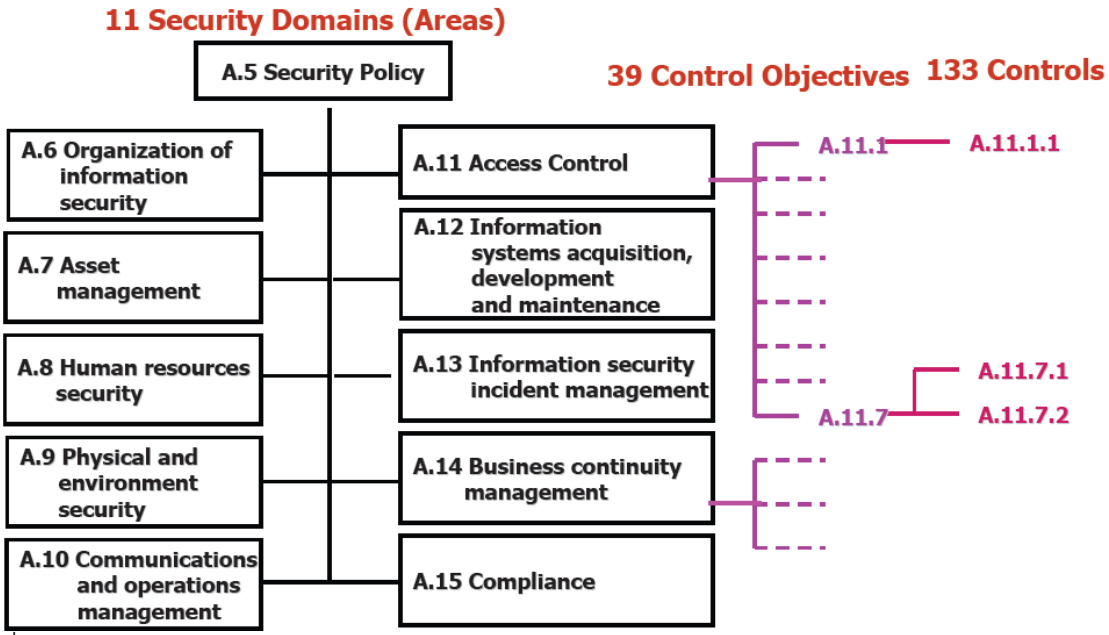
ที่มา: ดวงกมล ทรัพย์พิทยากร. “ISO 17799 อดีต ปัจจุบัน และอนาคต” ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, 5 กรกฎาคม 2548 < http://www.thaicert.org>

ทั้งนี้ มาตรฐาน ISO/IEC 17799:2005 มีจุดเริ่มต้นมาจากมาตรฐาน BS7799 Part 1 ซึ่งถูกพัฒนาขึ้นครั้งแรกในปี ค.ศ. 1995 โดย British Standard Institute (BSI) ของประเทศ

อังกฤษ มาตรฐานดังกล่าวเกิดจากการรวบรวมมาตรการพื้นฐาน (Baseline) ทางอุตสาหกรรมที่หลายๆองค์กรยึดถือร่วมกันและถูกนำไปใช้อย่างแพร่หลายทั่วโลก แม้แต่องค์กรที่ไม่ได้อยู่ในภาคอุตสาหกรรม และได้ถูกแก้ไขปรับปรุงหลายครั้ง จนกระทั่งได้รับการพิจารณาจาก International Organizational for Standard (ISO) และ International Electrotechnical Commission (IEC) ประกาศให้เป็นมาตรฐานสากล ISO/IEC 17799:2000 – Code of Practice for Information Security Management ซึ่งในฉบับล่าสุดที่เปลี่ยนชื่อเป็น ISO/IEC 17799:2005 – Security Technique – Code of Practice for Information Security Management นั้นจะประกอบไปด้วยหัวข้อ (Domain) และวัตถุประสงค์ (Control Objectives) ที่ใช้ในการควบคุมทางด้านการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่ปรับปรุงใหม่แล้วทั้งหมด 11 หัวข้อ ใน 39 วัตถุประสงค์ รวมเป็นมาตรการ (Controls) ทั้งสิ้น 133 มาตรการ ดังต่อไปนี้

ภาพที่ 2.2

โครงสร้างของมาตรฐาน ISO/IEC 17799:2005



ที่มา: บรรจง หะรังษี. “ISO/IEC 27001/17799 Information Security Management Standard.” ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, 5 มิถุนายน 2550 <http://www.thaicert.org>

A.5 Security Policy

กล่าวถึงการจัดทำนโยบายการจัดการด้านความปลอดภัยของข้อมูลสารสนเทศภายในองค์กร การเห็นความสำคัญของนโยบายและการให้การสนับสนุนจากผู้บริหารระดับสูงเพื่อให้มีการนำนโยบายดังกล่าวไปใช้อย่างมีประสิทธิภาพ และการทบทวนนโยบายอย่างสม่ำเสมอ

A.6 Organization of Information Security

กล่าวถึงการจัดตั้งหน่วยงานเพื่อทำหน้าที่ประสานงานและดำเนินการด้านการดูแลรักษาความปลอดภัยของข้อมูลสารสนเทศภายในองค์กร

A.7 Asset Management

กล่าวถึงการจำแนกประเภทของข้อมูลสารสนเทศภายในองค์กรตามระดับความสำคัญ และการควบคุมการเข้าถึงข้อมูลสารสนเทศและทรัพย์สินต่างๆที่เกี่ยวกับงานด้านเทคโนโลยีสารสนเทศ รวมทั้งการกำหนดหน้าที่และความรับผิดชอบในการดูแลข้อมูลสารสนเทศและทรัพย์สินต่างๆขององค์กร

A.8 Human Resources Security

กล่าวถึงการให้ความรู้แก่พนักงานขององค์กรในเรื่องของภัยคุกคามต่างๆ ข้อแนะนำในการปฏิบัติงานที่ถูกต้องเหมาะสมและปลอดภัย การปฏิบัติตนเมื่อพบความผิดปกติขึ้นกับระบบงาน รวมทั้งการระบุระเบียบวิธีปฏิบัติเมื่อมีการจ้างพนักงานใหม่เข้ามาหรือเมื่อมีพนักงานเก่าลาออกไป

A.9 Physical and Environment Security

กล่าวถึงการรักษาความปลอดภัยของสถานที่ทำงาน การควบคุมการเข้าออก และการนำสิ่งของเข้าออก เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาตและเพื่อป้องกันความเสียหายและความสูญหายของทรัพย์สินขององค์กร

A.10 Communications and Operations Management

กล่าวถึงการรักษาความปลอดภัยให้แก่เครื่องคอมพิวเตอร์ ระบบเครือข่ายและการประมวลผลข้อมูลสารสนเทศ การสำรองข้อมูลสารสนเทศ รวมทั้งการจัดเก็บและทำลายสื่อที่ใช้ในการบันทึกข้อมูลสารสนเทศอย่างเหมาะสม

A.11 Access Control

กล่าวถึงการควบคุมการเข้าถึงข้อมูลสารสนเทศและการป้องกันการเข้าถึงข้อมูลสารสนเทศโดยผู้ไม่ได้รับอนุญาต ไม่ว่าจะเป็นจากการเข้าใช้งานเครื่องคอมพิวเตอร์ภายในองค์กร การเข้าใช้งานผ่านระบบเครือข่าย หรือการเข้าถึงระบบจากระยะไกล

A.12 Information Systems Acquisition, Development and Maintenance

กล่าวถึงการควบคุมการพัฒนาระบบคอมพิวเตอร์ ระบบเครือข่าย ซอฟท์แวร์ และฮาร์ดแวร์ เริ่มตั้งแต่การจัดซื้อจัดจ้าง การติดตั้งระบบ การใช้งานจริง ไปจนถึงการบำรุงรักษาอย่างสม่ำเสมอ รวมทั้งการควบคุมการเข้ารหัสข้อมูลสารสนเทศอย่างเหมาะสม

A.13 Information Security Incident Management

กล่าวถึงการจัดทำรายงานเหตุการณ์ผิดปกติต่างๆที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลสารสนเทศและการบริหารจัดการเหตุละเมิดความมั่นคงของข้อมูลสารสนเทศ เพื่อประโยชน์ในการแก้ไขและป้องกันไม่ให้เหตุการณ์ดังกล่าวเกิดขึ้นซ้ำอีกในอนาคต

A.14 Business Continuity Management

กล่าวถึงการจัดทำแผนการจัดการให้ธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง (Business Continuity Plan: BCP) ซึ่งก็คือวิธีปฏิบัติในการรับมือกรณีที่เกิดความผิดพลาด หรือภัยธรรมชาติซึ่งสร้างความเสียหายให้แก่ระบบ เพื่อให้องค์กรสามารถกลับมาดำเนินงานตามปกติได้เร็วที่สุด

A.15 Compliance

กล่าวถึงการปฏิบัติงานที่ถูกต้องตามกฎหมายหรือข้อตกลงต่างๆที่องค์กรได้กระทำร่วมกับผู้อื่น ไม่ว่าจะเป็นในเรื่องของลิขสิทธิ์ซอฟท์แวร์หรือกฎระเบียบอื่นๆของภาครัฐ

ภาพที่ 2.3
มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์
เวอร์ชั่น 1 ประจำปี 2547 และเวอร์ชั่น 2 ประจำปี 2549

ที่มา: บรรจง หะรังษี. “ISO/IEC 27001/17799 Information Security Management Standard.” ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, 5 มิถุนายน 2550 <http://www.thaicert.org>

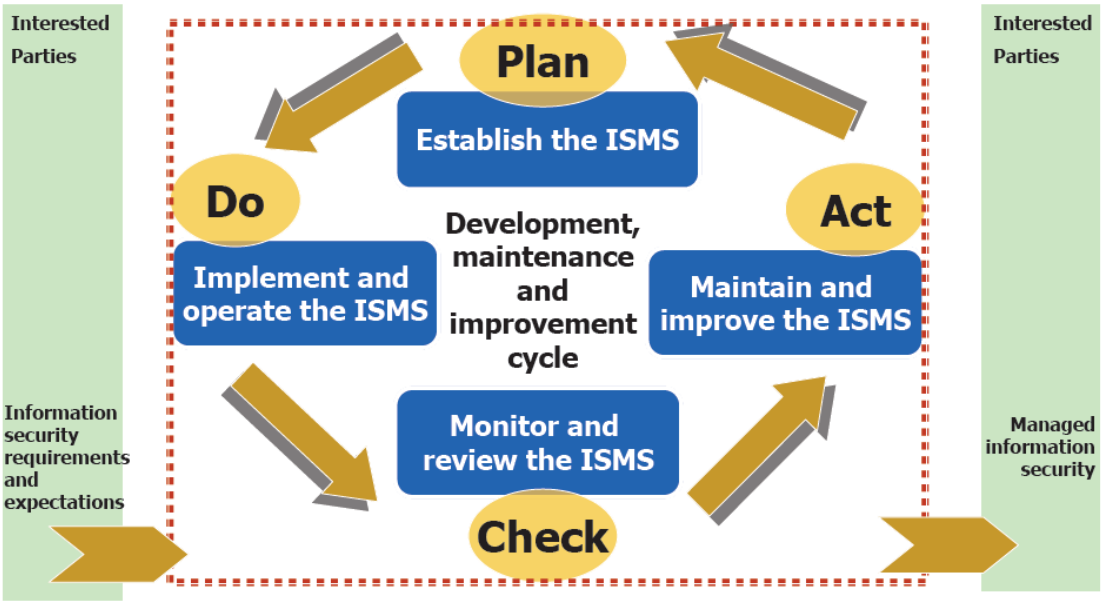
สำหรับประเทศไทยนั้น คณะอนุกรรมการด้านความมั่นคงภายใต้คณะอนุกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งถูกจัดตั้งขึ้นตามพระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ได้นำเอามาตรฐาน ISO/IEC 17799:2000 มาเป็นแนวทางในการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 1) ประจำปี พ.ศ.2547 และต่อมาได้นำเอามาตรฐาน ISO/IEC 17799:2005 มาเป็นแนวทางในการกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 2) ประจำปี พ.ศ.2549 โดยได้มีการปรับเปลี่ยนในสาระสำคัญสองประการ ประการแรกคือ มีการเพิ่มมาตรการที่เห็นว่ามีความเหมาะสมกับสภาพแวดล้อมและสถานการณ์ทางด้านเทคโนโลยีสารสนเทศในประเทศไทยรวมเป็นจำนวนทั้งสิ้น 144 มาตรการ ประการที่สองคือ มีการแบ่งระดับของมาตรการเป็นระดับ 1 – 3 เพื่อช่วยให้องค์กรค่อยๆนำมาตรการแต่ละระดับไปปรับใช้ด้วยวิธีค่อยเป็นค่อยไป ในกรณีที่องค์กรเห็นว่าการนำมาตรการทั้งหมดไปปฏิบัตินั้นเป็นเรื่องที่ทำได้ยาก

มาตรฐาน ISO/IEC 27001:2005

มาตรฐาน ISO/IEC 27001:2005 เป็นมาตรฐานเกี่ยวกับระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Information Security Management Systems: ISMS) ซึ่งจะกำหนดความต้องการ (Set of Requirements) ในการจัดทำระบบ ISMS เพื่อช่วยให้องค์กรสามารถสร้างระบบ ISMS ขึ้นมาได้อย่างมีประสิทธิภาพ ซึ่งระบบ ISMS นี้ถือเป็นส่วนหนึ่งของระบบบริหารจัดการขององค์กรที่มีพื้นฐานมาจากแนวทางการบริหารจัดการความเสี่ยงของธุรกิจ (Business Risk Approach) โดยมีวัตถุประสงค์เพื่อรักษาไว้ซึ่งความลับ (Confidentiality) บูรณภาพ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลสารสนเทศและทรัพย์สินอื่นๆขององค์กร เพื่อให้องค์กรสามารถรอดพ้นจากภัยคุกคามต่างๆได้

ภาพที่ 2.4

แนวทางการจัดตั้งระบบ ISMS ตามมาตรฐาน ISO/IEC 27001:2005

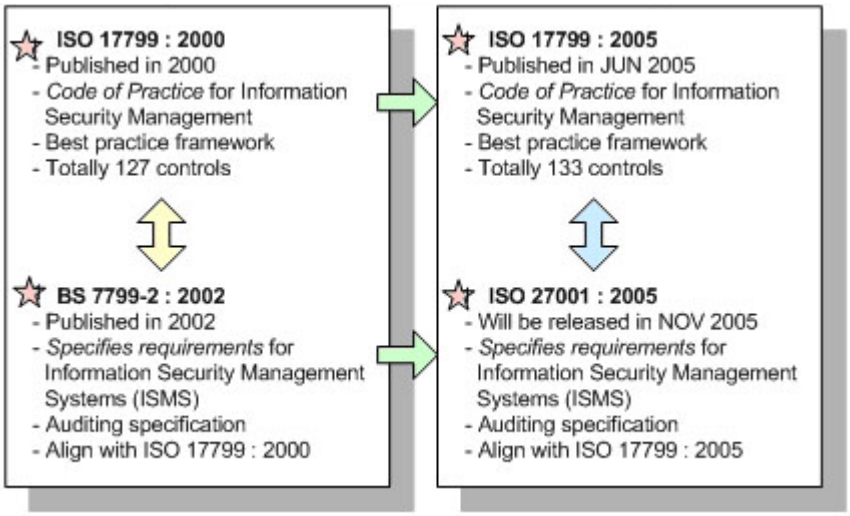


ที่มา: บรรจง หะรังษี. “ISO/IEC 27001/17799 Information Security Management Standard.” ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, 5 มิถุนายน 2550 <http://www.thaicert.org>

มาตรฐาน ISO/IEC 27001:2005 ประกอบไปด้วยข้อกำหนดและแนวทางในการจัดตั้งระบบ ISMS ขึ้นภายในองค์กรตั้งแต่การริเริ่มทำระบบ การนำระบบไปใช้ การดำเนินงานของระบบ การวัดผลและการทบทวนการดำเนินงานของระบบ การบำรุงรักษาระบบ และการปรับปรุงระบบอย่างสม่ำเสมอ รวมถึงแนวทางในการออกใบรับรอง (Certification) ให้กับระบบ โดยที่หัวใจสำคัญของระบบ ISMS นั้นอยู่ที่การทำการตรวจประเมินความเสี่ยงและการเลือกวิธีการควบคุมให้เหมาะสมกับการปฏิบัติงานและระดับความเสี่ยงที่ยอมรับได้ขององค์กร นอกจากนั้น มาตรฐานนี้ยังได้ถูกปรับปรุงเพื่อให้มีความเข้ากันได้กับมาตรฐาน ISO9001 และ ISO14001 ซึ่งจะช่วยให้องค์กรที่ได้รับมาตรฐานดังกล่าวแล้วมีความคุ้นเคยกับระบบเอกสาร การทบทวนโดยผู้บริหาร (Management Review) และการตรวจติดตามระบบภายใน (Internal Audit) ที่มีแนวปฏิบัติคล้ายคลึงกันอีกด้วย

ภาพที่ 2.5

พัฒนาการของมาตรฐาน ISO/IEC 27001:2005



ที่มา: สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ. “ISO17799 (BS7799) ความมั่นคงปลอดภัย จากภาครัฐสู่ภาครัฐ.” สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ <http://www.gits.net.th>

ทั้งนี้ มาตรฐาน ISO/IEC 27001:2005 มีจุดเริ่มต้นมาจากมาตรฐาน BS7799 Part 2 ซึ่งถูกประกาศใช้ครั้งแรกในปี ค.ศ. 1998 หลังจากนั้นได้ถูกปรับปรุงแก้ไขและประกาศเป็น BS7799-2:2002 Information Security Management Systems – Specification with Guidance for Use ซึ่งมีเนื้อหาว่าด้วยการจัดตั้งระบบการจัดการความปลอดภัยของข้อมูลขึ้นภายในองค์กร โดยประยุกต์เข้ากับหลักการของ Plan-Do-Check-Act (PDCA) เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบและมีการพัฒนาอย่างต่อเนื่อง (Continuous Improvement) และได้มีการอ้างอิงมาตรการของการควบคุมทางด้านการจัดการความปลอดภัยของข้อมูลทั้ง 133 มาตรการตามมาตรฐาน ISO/IEC 17799:2005 โดยระบุไว้ในส่วนของ Annex A ทั้งนี้ เนื้อหาของมาตรฐาน ISO/IEC 27001:2005 นั้นจะแบ่งออกเป็น 8 ส่วน ดังต่อไปนี้

Foreword

0 Introduction

1 Scope

2 Normative Reference

3 Terms and Definitions

4 Information Security Management System

5 Management Responsibility

6 Internal ISMS Audit

7 Management Review of The ISMS

8 ISMS Improvement

ในส่วนของการออกใบรับรอง (Certification) นั้นสามารถแบ่งได้เป็น 2 ประเภท คือ การออกใบรับรองให้กับองค์กร (Organization Certification) เพื่อเป็นการรับรองว่าองค์กรดังกล่าวมีระบบ ISMS ที่มีประสิทธิภาพ โดยที่สิ่งที่องค์กรจำเป็นต้องดำเนินการเพื่อให้ได้รับการรับรองจะถูกระบุอยู่ในเนื้อหาส่วนที่ 4 ถึงส่วนที่ 8 กับการออกใบรับรองให้กับบุคคล (Individual Certification) ที่ทำหน้าที่เป็นผู้ตรวจรับรองระบบว่าบุคคลนั้นเป็นผู้ที่มีความรู้ ความชำนาญในระบบ ISMS เป็นอย่างดี และมีคุณสมบัติเพียงพอที่จะทำหน้าที่ตรวจรับรองระบบ ISMS ได้ โดยองค์กรสากลที่ทำหน้าที่ควบคุมการออกใบรับรองให้กับผู้ตรวจรับรองระบบก็คือ International Register of Certificated Auditors (IRCA) ทั้งนี้ การยื่นขอใบรับรองสำหรับระบบ ISMS ขององค์กรใดๆก็ตามนั้นจะมีขั้นตอนการยื่นขอใบรับรองเหมือนกับการยื่นขอใบรับรองของมาตรฐาน ISO อื่นๆ นั่นคือ จะต้องเริ่มจากการเลือกบริษัทที่จะเข้ามาทำหน้าที่ตรวจรับรองระบบ ซึ่งจะต้องเป็นบริษัทที่ได้รับการขึ้นทะเบียนอย่างถูกต้อง (Accredited) ก่อน หลังจากนั้นจึงเป็นการวางแผนและกำหนดขอบเขตของระบบที่จะตรวจรับรอง และหลังจากที่องค์กรได้รับการรับรองระบบ ISMS เรียบร้อยแล้ว องค์กรจะต้องได้รับการตรวจประเมินระบบซ้ำ (Surveillance Audit) ทุก 6 เดือนหรือ 1 ปี และต้องทำการตรวจรับรองใหม่ทั้งระบบ (Re-Certification Audit) ทุก 3 ปี ส่วนบุคคลที่ต้องการยื่นขอใบรับรอง (Auditor Certification) จาก IRCA นั้นจะต้องเป็นผู้ที่มีวุฒิการศึกษาขั้นต่ำในระดับปริญญาหรืออนุปริญญา และมีประสบการณ์ในการทำงานอย่างน้อย 4 ปีขึ้นไป และที่สำคัญจะต้องผ่านการอบรมและการสอบในหลักสูตร ISO27001 and ISO27002 Information Security Management Systems Lead Auditor Training Course ที่ได้รับการรับรองจาก IRCA ซึ่งมีการจัดอบรมอยู่ในหลายประเทศทั่วโลก รวมทั้งประเทศไทยด้วยเช่นกัน

สำหรับประเทศไทยนั้น ทางภาครัฐได้เห็นความสำคัญของมาตรฐาน ISO/IEC 27001:2005 โดยการนำมาตรฐานดังกล่าวมาแปลเป็นภาษาไทย และได้แนะนำให้หน่วยงานของรัฐที่มีภารกิจเกี่ยวข้องกับการดูแลโครงสร้างพื้นฐานของประเทศให้มีการนำเอามาตรฐาน

ISO/IEC 27001:2005 มาปรับใช้ในหน่วยงานของตน และในส่วนของกระทรวงการคลังก็ได้กำหนดให้มีการตรวจประเมินรัฐวิสาหกิจหลักของประเทศในการจัดทำมาตรฐานดังกล่าว โดยมีกรอบระยะเวลาชัดเจนว่าจะต้องได้รับการรับรองให้แล้วเสร็จภายในปี พ.ศ. 2554 นอกจากนี้มาตรฐาน ISO/IEC 27001:2005 ยังถูกใช้เป็นรากฐานในการพัฒนากฎหมายธุรกรรมทางอิเล็กทรอนิกส์และกฎหมาย ICT ของประเทศหลายฉบับ เช่น พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชกฤษฎีกากำหนดวิธีการแบบมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น

กรณีศึกษา

สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ (สบทร.) ซึ่งเป็นหน่วยงานภายใต้สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) กระทรวงวิทยาศาสตร์และเทคโนโลยี ถือเป็นหน่วยงานภาครัฐหน่วยงานแรกของประเทศไทยที่ได้รับการรับรองมาตรฐาน ISO/IEC 27001:2005 จาก BSI เมื่อวันที่ 4 ธันวาคม พ.ศ. 2549

ภาพที่ 2.6

ใบรับรองมาตรฐาน ISO/IEC 27001:2005 ของสำนักบริการเทคโนโลยีสารสนเทศภาครัฐ

ที่มา: สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ. “Certified ISO27001:2005.” สำนักบริการเทคโนโลยีสารสนเทศภาครัฐ <http://www.gits.net.th>

สบทร. ดำเนินงานโดยมีเป้าหมายในการเป็นองค์กรที่มีระบบการบริหารภายในและระบบบริหารความมั่นคงสารสนเทศในลักษณะเดียวกับองค์กรนานาชาติ ที่สามารถให้บริการแก่หน่วยงานภาครัฐได้อย่างมีประสิทธิภาพและมีคุณภาพเป็นที่ยอมรับในระดับสากล ทั้งนี้ สบทร. ได้ตั้งเป้าหมายในการได้รับการรับรองมาตรฐาน ISO/IEC 27001:2005 ไว้สองส่วน ได้แก่ บริการใบรับรองอิเล็กทรอนิกส์ (CA Service) เพื่อเพิ่มความน่าเชื่อถือทางด้านความมั่นคงปลอดภัยของบริการ และในส่วนของการดำเนินงานในภาพรวมของ สบทร. ที่จำเป็นต้องมีการจัดตั้งระบบ ISMS ซึ่งได้แก่ การบริหารจัดการความเสี่ยง เพื่อช่วยให้ สบทร. สามารถระบุปัญหาและวางแผนเพื่อลดความเสี่ยงทางด้านความมั่นคงปลอดภัยของข้อมูลสารสนเทศได้อย่างเป็นระบบ นอกจากนี้ยังช่วยให้หน่วยงานภาครัฐอื่นๆสามารถมั่นใจได้ว่าบริการต่างๆของ สบทร. มีคุณภาพและความปลอดภัยตามมาตรฐานสากล

จากเป้าหมายดังกล่าว สบทร. จึงได้มีมติให้ดำเนินการจัดตั้งระบบ ISMS ขึ้นเมื่อประมาณกลางปี พ.ศ. 2548 โดยมีการจัดตั้งทีมงานเพื่อดำเนินการตามขั้นตอนต่างๆตามหลักการของ PDCA ดังต่อไปนี้

Plan

- กำหนดขอบเขตและส่วนงานที่เกี่ยวข้อง
- จัดตั้งทีมงานและกำหนดหน้าที่ความรับผิดชอบ

Do

- กำหนดนโยบายความมั่นคงปลอดภัยของข้อมูลสารสนเทศขององค์กร
- บริหารจัดการความเสี่ยงด้วยการประเมินความเสี่ยง การวิเคราะห์ความเสี่ยง และการแก้ไขความเสี่ยง
- เลือกใช้มาตรการความมั่นคงปลอดภัยที่เหมาะสม
- ฝึกอบรมพนักงานในเรื่องของความมั่นคงปลอดภัยของข้อมูลสารสนเทศในทุกระดับ

Check

- ดำเนินการตรวจประเมินภายในของระบบ ISMS
- ทบทวนระบบ ISMS โดยผู้บริหาร

Act

- ปรับปรุงระบบ ISMS ตามสิ่งที่ได้ตรวจพบ
- วิเคราะห์หาสาเหตุของปัญหาที่แท้จริง
- ป้องกันไม่ให้เกิดปัญหาซ้ำอีก

เมื่อ สบทร. ได้จัดทำระบบ ISMS ตามแผนที่ได้กำหนดไว้เสร็จสิ้นแล้วและมีความพร้อมที่จะเข้ารับการตรวจประเมิน ทาง สบทร.จึงได้ดำเนินการคัดเลือกหน่วยงานที่จะทำหน้าที่ตรวจประเมินระบบ โดยในท้ายที่สุด สบทร.ได้เลือกให้ BSI Thailand Co., Ltd. เข้ามาทำหน้าที่นี้ในช่วงเดือนพฤศจิกายน พ.ศ. 2549 เนื่องจากหน่วยงานดังกล่าวเป็นหน่วยงานที่มีความน่าเชื่อถือ มีประสบการณ์ และมีความเกี่ยวข้องกับการกำหนดมาตรฐานต่างๆอยู่แล้ว ซึ่งทาง สบทร.ก็ได้ผ่านการประเมินและได้รับการรับรองระบบ ISMS ตามมาตรฐาน ISO/IEC 27001:2005 ในท้ายที่สุด