สรุปการประชุม/สัมมนา
เรื่อง "มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ : ความจำเป็น และความพร้อมขององค์กร"

จากที่ได้รับคำสั่งให้ นายสุรชาติ วรกุลรังสรรค์ และนายอนิรุท สว่างมั่น ให้เข้าร่วมสัมมนาการเผยแพร่ความรู้เกี่ยวกับมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ : ความจำเป็น และความพร้อมขององค์กร" ในวันพฤหัสบดีที่ 4 มีนาคม 2553 เวลา 08.00 – 16.30 น. ณ ห้อง แกรนด์ C ชั้น 4 โรงแรม มิราเคิล แกรนด์ คอนเวนชั่น โดยมีรายละเอียดโดยสรุปดังนี้

วัตถุประสงค์

1. เพื่อเผยแพร่ความรู้ความเข้าใจ เกี่ยวกับมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์
2. เพื่อสร้างความรู้ความเข้าใจให้กับหน่วยงานภาครัฐเกี่ยวกับ "แนวทางปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ตามมาตรฐาน ISO/IEC 27001"
3. เพื่อให้หน่วยงานภาครัฐได้รับทราบถึงผลกระทบของการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องตามกฎหมาย

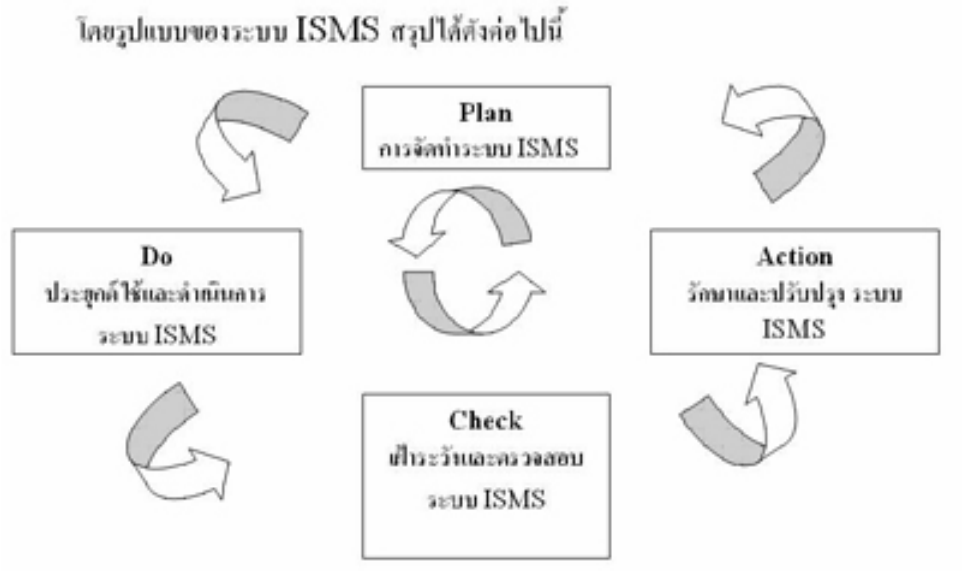
ด้วย พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 (แก้ไขเพิ่มเติม พ.ศ.2551) มาตรา 25 กำหนดว่า ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้ ทางกระทรวงเทคโนโลยีสารสนเทศ จึงจัดทำเอกสาร "มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์" โดยแต่งตั้งคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เพื่อจัดทำเอกสารมาตรฐานด้านความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ขึ้น จำนวน 3 เวอร์ชั่น (ปัจจุบันเป็นเวอร์ชั่น 2.5)

ปัจจุบัน ได้มีการพยายามผลักดันให้เกิดการใช้ประโยชน์จากมาตรฐานการรักษาความมั่นคงปลอดภัยที่ได้จัดทำขึ้น โดยการนำมาประยุกต์ใช้ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเป้าหมายสำคัญของการดำเนินงานในส่วนที่เกี่ยวกับมาตรฐานดังกล่าวคือ การผลักดันประกาศมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ให้เป็นมาตรฐานของประเทศไทย นอกจากนี้ ทางกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารยังได้มีส่วนร่วมในการจัดทำ "(ร่าง) แนวทางปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001" ซึ่งเอกสารดังกล่าว เป็นการอธิบายถึงรายละเอียดแนวทางปฏิบัติที่เป็นมาตรฐานสำหรับการจัดการความปลอดภัยของข้อมูล (Information Security Management) ซึ่งสอดคล้องกับมาตรฐานสากล (ISO)

ระบบมาตรฐานด้านความปลอดภัยของข้อมูล ISO 27001

ISO/IEC 27001:2005 (Information Security Management System: ISMS) เป็นมาตรฐานการจัดการข้อมูลที่มีความสำคัญเพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่อง ซึ่งข้อกำหนดต่างๆกำหนดขึ้นโดยองค์กรที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศ คือ ISO (The International Organization for Standardization) และ IEC (The International Electrotechnical Commission) การประยุกต์ใช้ ISMS จะช่วยให้กิจกรรมทางธุรกิจต่อเนื่องไม่สะดุด, ช่วยป้องกันกระวนการทางธุรกิจจากภัยร้ายแรงต่างๆเช่น แผ่นดินไหว, วาตภัย, อุทกภัย ฯลฯ

หลักการของการออกแบบโครงสร้างระบบ ISO/IEC27001:2005 จะใช้ อ้างอิง รูปแบบ PDCA Model (Plan Do Check Action) ซึ่งเป็นโครงสร้างเดียวกับ ระบบ การบริหารที่เป็นสากลที่ใช้กันทั่วโลก เช่น ระบบการจัดการคุณภาพ (ISO 9001:2000), ระบบการจัดการสิ่งแวดล้อม (ISO14001:2004), ระบบการจัดการคุณภาพสำหรับอุตสาหกรรมรถยนต์ (ISO/TS 16949), ระบบการจัดการจัดการคุณภาพสำหรับอุตสาหกรรมอาหาร (ISO 21001) ฯลฯ ซึ่งองค์ที่มีการประยุกต์ระบบการจัดการต่างๆนี้แล้ว จะสามารถต่อยอดระบบ ISO/IEC27001:2005 ได้เร็วและง่ายขึ้น แต่สำหรับ องค์กรที่ยังไม่มีระบบการจัดการใดๆ ก็ใช่ว่าจะประยุกต์ใช้ยากเพราะ ระบบ มีการเขียนที่เข้าใจง่ายและแบ่งหมวดให้ง่ายต่อความเข้าใจตาม PDCA อยู่แล้วเพียงแต่ต้องทำความเข้าใจกับระบบให้มากขึ้น



ระบบ ISMS เป็นระบบ Dynamic system ที่ใช้โครงสร้าง PDCA ระบบจะมีการหมุนเพื่อปรับปรุงอย่างต่อเนื่องอยู่ตลอดเวลาไม่ที่สิ้นสุด โดยโครงสร้างของข้อกำหนด จะถูกแบ่งตาม PDCA ดังนี้

Plan การจัดทำระบบ ISMS	4.2.1 Establish ISMS a) กำหนด scope และ ขอบเขตการจัดทำระบบ ISMS b) กำหนด ISMS Policy c) กำหนด รูปแบบการประเมินความเสี่ยง d) กำหนดความเสี่ยง e) วิเคราะห์ และ ประเมินความเสี่ยง f) กำหนดและประเมิน วิธีการเพื่อลดความเสี่ยง g) เลือกการควบคุม เพื่อลดความเสี่ยง h) เห็นชอบความเสี่ยงที่เหลืออยู่โดย management I) เห็นชอบและประยุกต์ใช้ ระบบ โดย management J) จัดทำ Statement of Applicable(SOA)
Do ประยุกต์ใช้และ ดำเนินการ ระบบ ISMS	4.2.2 Implement and Operate the ISMS a) กำหนดแผนการลดความเสี่ยง b) ดำเนินการตามแผนลดความเสี่ยง c) ดำเนินการ ตามการควบคุมที่เลือกตาม 4.2.1g d) กำหนดการวัดประสิทธิภาพของระบบการควบคุม e) จัดทำรายการฝึกอบรม f) จัดการการประยุกต์ใช้ระบบ g) ประยุกต์ใช้ ระเบียบปฏิบัติงาน
Check เฝ้าระวังและตรวจสอบ ระบบ ISMS	4.2.3 Monitor and review ISMS a) จัดทำ ระเบียบปฏิบัติการ เฝ้าระวังและตรวจสอบระบบ ISMS b) ทบทวนประสิทธิภาพของ ระบบอย่างสม่ำเสมอ c) วัดประสิทธิภาพการควบคุมในการปฏิบัติตามข้อกำหนด d) ทบทวน การประเมินความเสี่ยงตามแผน ความเสี่ยงที่เหลือ ระบบการประเมินความเสี่ยง และการเปลี่ยนแปลงต่างๆ ตามรอบเวลาที่กำหนด e) ดำเนินการ ตรวจติดตามภายในระบบISMS f) ดำเนินการ จัดทำ management review g) ปรับปรุง security plan ให้ทันสมัย h) บนทึกการการทำงานและหลักฐานที่มีผลต่อประสิทธิภาพและประสิทธิผลของระบบ
Action รักษาและปรับปรุง ระบบ ISMS	4.2.4 Maintain and improve the ISMS a) ปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัย b) ดำเนินการ corrective action และ preventive action c) สื่อสาร วิธีการและการปรับปรุงต่างๆ ให้กับผู้ที่เกี่ยวข้องต่างๆ d) แน่ใจว่า วิธีการที่ปรับปรุงขึ้น บรรลุจุดประสงค์ที่วางไว้

สำหรับระบบ ISO/IEC 17799:2005 เป็นกรอบด้านการควบคุมระบบ ความปลอดภัยข้อมูล ซึ่งแบ่งออกเป็น 11 การควบคุมหลักดังนี้

1. นโยบายความมั่นคงปลอดภัย (Security policy)
2. โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization Information Security)
3. การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)
4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resource Security)
5. การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environment) security
6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management)
7. การควบคุมการเข้าถึง (Access control)
8. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)
9. การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Information security incident management)
10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)
11. การปฏิบัติตามข้อกำหนด (Compliance)

โดยระบบ ISO/IEC 27001:2005 มีการแนะนำให้ประยุกต์ ข้อกำหนดของ ISO/IEC17799:2005 มาใช้ในการควบคุมและจัดการเกี่ยวกับความเสี่ยงที่เกิดขึ้น (ตามข้อกำหนด 4.2.1g ของ ISO/IEC 27001:2005) และ หากองค์กรจะไม่เลือกประยุกต์และ/หรือใช้บางส่วน ข้อกำหนดของ ISO/IEC17799:2005 สามารถกระทำได้แต่ต้องมีการอธิบายสาเหตุของการไม่เลือกประยุกต์ใช้ให้ชัดเจนไว้ใน SOA (ตามข้อกำหนด 4.2.1j ของ ISO/IEC 27001:2005)

โดยสรุปแล้วระบบการจัดการความปลอดภัยข้อมูล ISO/IEC 27001:200หรือ ISMS เป็นระบบ dynamic systemที่มีการประยุกต์หลักการ PDCA Cycle ที่สามารถประยุกต์ใช้ได้กับทุกธุรกิจ เพื่อให้ระบบข้อมูลขององค์กร มี Confidentiality ให้แน่ใจว่าข้อมูลต่างๆ สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิที่จะเข้าเท่านั้น, มี Integrity ป้องกัน ให้ ข้อมูล มี ความถูกต้อง และความสมบูรณ์ และ Availability แน่ใจว่าผู้ที่มีสิทธิ ในการเข้าถึงข้อมูล สามารถเข้าถึงได้เมื่อมีความต้องการ โดยระบบ การจัดการ ISMS นั้น จะเป็นระบบการจัดการภายใต้ความสี่ยงที่ยอมรับได้ ไม่ใช่ให้ระบบไม่มีความเสี่ยงเลยหรือไม่เกิดปัญหาเลย ทำให้เกิดประสิทธิภาพในการใช้ ทรัพยากรในการลงทุนสำหรับการจัดการความปลอดภัยของข้อมูลอย่างมีประสิทธ์ภาพ โดยส่วนใหญ่จะมีการใช้ร่วมกับ ระบบ ISO/IEC 17799:2005 เพื่อเป็นให้เกิดประสิทธิภาพในการดำเนินงาน

ประเทศไทยมีบริษัทที่ได้รับประกาศนียบัตรรับรองมาตรฐาน ISO/IEC 27001:2005 จำนวนไม่น้อยกว่า 27 บริษัท (จากทั้งหมดมากกว่า 5600 บริษัท) เช่น

- AEON Thana Sinsap (Thailand) Public Company Limited
- Metropolitan Electricity Authority
- Metropolitan Water Authority
- National Science and Technology Development Agency
- PTTICT Solutions Co., Ltd.
- Thanachart Bank Public Co., Ltd.
- United Nation
- United Information Highway