รายงานการเข้าร่วมโครงการเอพีโอ

11-IN-08-GE-TRC-B

Training Course on the Information Security Management System ISO 27000 Series

17-21 ตุลาคม 2554

ณ เบกาซี จาการ์ต้า ประเทศอินโดนีเซีย

จัดทำโดย นางสาวน้ำเพชร พรหมณา

วิทยากรที่ปรึกษา ส่วนพัฒนาหลักสูตรฝึกอบรม ฝ่ายฝึกอบรม สถาบันเพิ่มผลผลิตแห่งชาติ

22 พฤศจิกายน 2554

การใช้ชีวิตในปัจจุบันที่เต็มไปด้วยข้อมูลข่าวสารรอบตัว ทำให้ทุกคนยากที่จะหลีกเลี่ยงในการรับข้อมูลจากภายนอกทั้งที่เกี่ยวข้องและไม่เกี่ยวกับตัวเราในการดำรงชีวิตทั้งในด้านส่วนตัวและในด้านการทำงานไปได้เลย การจัดการกับข้อมูลเพื่อให้ได้มาซึ่งข้อมูลที่เป็นประโยชน์ ถูกต้องและเหมาะสมกับการใช้จึงเป็นสิ่งที่ทวีความสำคัญมากขึ้นเรื่อย ๆ โดยเฉพาะอย่างยิ่งในการแข่งขันทางธุรกิจที่ต้องอาศัยข้อมูลเป็นหลักในการพิจารณาตัดสินใจดำเนินงาน จึงถือได้ว่าข้อมูลเป็นหัวใจของการดำเนินงานที่บริษัทหรือองค์กรต่างๆ ต่างให้ความสำคัญในการดำเนินการเพื่อให้ได้มา ใช้และป้องกันดูแลซึ่งข้อมูลที่สำคัญของตนเองเป็นอย่างดี จนมีคำเปรียบเปรยว่า *"ผู้ใดมีข้อมูลข่าวสารในมือผู้นั้นครองโลก"* ซึ่งเป็นคำกล่าวที่แสดงให้เห็นถึงความสำคัญของข้อมูลและสารสนเทศได้ตรงประเด็นเป็นที่สุด ทั้งนี้เป็นเพราะข้อมูลเป็นสิ่งมีค่ามีราคา การโจรกรรมข้อมูลโดยใช้เทคโนโลยีใหม่ ๆ จึงกลายเป็นปัญหาสำคัญที่เกิดขึ้นในโลกปัจจุบันที่สามารถพบเห็นได้บ่อย ๆ ดังที่ปรากฏเป็นข่าวทั้งในประเทศและต่างประเทศอย่างสม่ำเสมอ

ดังนั้นเมื่อความปลอดภัยของข้อมูลและสารสนเทศได้กลายเป็นประเด็นที่องค์กรต้องหันมาให้ความสำคัญกับเรื่องนี้กันอย่างจริงจัง หลาย ๆ องค์กรจึงได้มองหาวิธีการในการจัดการเพื่อให้ข้อมูลและสารสนเทศที่สำคัญของตนเองมีความปลอดภัย หนึ่งในวิธีการที่ได้กลายมาเป็นจุดสนใจในการจัดการความปลอดภัยของข้อมูลและสารสนเทศก็คือ ISO/IEC 27001:2005 (Information Security Management System: ISMS) ซึ่งเป็นมาตรฐารการจัดการข้อมูลที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรที่กำหนดขึ้นโดยองค์กรที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศ คือ ISO (The International Organization for Standardization) และ IEC (The International Electrotechnical Commission) ทั้งนี้การประยุกต์ใช้ ISMS ในองค์กรจะช่วยให้กิจกรรมทางธุรกิจสามารถดำเนินการได้อย่างต่อเนื่องไม่สะดุดเนื่องจากช่วยป้องกันกระบวนการทางธุรกิจจากความเสี่ยงต่างที่จะส่งผลต่อความเสียหายของข้อมูลและสารสนเทศ

ผู้เขียนได้รับโอกาสจาก APO ในการเข้าร่วมในโครงการ Training Course on Information Management System Based on ISO 27000 Series ที่จัดขึ้น ณ ประเทศอินโดนีเซีย เมืองเบกาซี ในช่วงวันที่ 17-21 ตุลาคม 2554 โดยมีผู้เข้าร่วมจากประเทศสมาชิกต่าง ๆ ของ APO จำนวนทั้งหมด 14 ประเทศ ได้แก่ บังคลาเทศ กัมพูชา ฟิจิ อินโดนีเซีย เกาหลีใต้ มองโกเลีย ลาว มาเลเซีย เนปาล ปากีสถาน อิหร่าน ฟิลิปินส์ ศรีลังกา ไทย และเวียดนาม รวมจำนวนทั้งสิ้น 22 คน ทั้งนี้โดยการประสานงานทั้งจากส่วนวิเทศสัมพันธ์ของสถาบันเพิ่มผลผลิตแห่งชาติ Program officer จาก APO ญี่ปุ่นที่ดูแลโครงการนี้คือ Ms. Hiroko Kosaka และจาก NPO Indonesia ที่ได้ดูแลผู้เข้าร่วมจากประเทศสมาชิกต่าง ๆ เป็นอย่างดี ตั้งแต่การเตรียมตัวก่อนการเข้าร่วมโครงการและการเดินทางไปยังประเทศอินโดนีเซีย การจัดเจ้าหน้าที่รับผู้เข้าร่วมโครงการที่สนามบินซูการ์โนฮอตตา จาการ์ต้า ไปยัง

โรงแรม Horison ที่เบกาซี การดูแลในระหว่างการฝึกอบรมและการดูงาน ณ บริษัท PT Panasonic Gobel Energy Indonesia การพาเที่ยวในบ่ายวันเสาร์ที่ 21 ตุลาคม 2554 และการส่งผู้เข้าร่วมกลับมายังสนามบินซูการ์โนฮอตตา เพื่อเดินทางกลับประเทศโดยสวัสดิภาพอย่างดีเยี่ยม

รูปที่ 1 ภาพถ่ายรวมในช่วงเริ่มต้นหลังพิธีเปิดอย่างเป็นทางการ

Resource person ที่ได้ให้ความรู้ในโครงการนี้ประกอบด้วย Mr Duggirala Sathya Prakash และ Mr Syed T. Zaidi จาก Det Norske Veritas ประเทศอินเดีย เป็นผู้บรรยายถึงรายละเอียดเกี่ยวกับข้อกำหนดและการประยุกต์ใช้ รวมถึงการตรวจประเมินมาตรฐาน ISO 27001 และ Mrs. Eka Dyan Lestari จาก PT Panasonic Gobel Energy Indonesia ผู้เป็น ISM Secretariat ของบริษัท ที่นำเสนอถึงรายละเอียดของ ISO 27001 ที่ทางบริษัทได้นำมาประยุกต์ใช้จนได้การรับรองระบบมาตรฐาน ISO 27001 เป็นที่เรียบร้อย โดยการอบรมในแต่ละวันที่กำหนดขึ้นเพื่อพัฒนาความรู้และมุมมองผู้เข้าร่วมต่อการประยุกต์ใช้มาตรฐาน ISO 27001 มีดังนี้

วันที่ 1 (17 ตุลาคม 2554) : Overview of ISMS

ในวันแรกหลังจากพิธีเปิดโครงการที่ดำเนินการอย่างเป็นทางการโดย APO Liaison คนใหม่ของ NPO Indonesia ที่เพิ่งเข้ารับตำแหน่งในวันแรกก็เริ่มทำงานได้อย่างเต็มที่และแข็งขันแล้ว หัวข้อที่ดำเนินการประกอบด้วย 3 การบรรยายหลัก ๆ คือ

- *The ISMS Standard :* เริ่มต้นจากการทำให้ผู้เข้าร่วมทุกคนเข้าใจถึงคำว่า “Information Security Management System” ว่ามีความหมายว่าอย่างไร จากนั้น Resource person ได้โยงให้เห็นถึงเหตุการณ์ต่าง ๆ ที่ทำให้ข้อมูลและสารสนเทศที่มีใช้อยู่เกิดความเสี่ยง ไม่ว่าจะเป็นภัยธรรมชาติ เช่น สึนามิ แผ่นดินไหว เป็นต้น การโจรกรรมข้อมูลด้วยวิธีการต่าง ๆ การไม่มีระบบการควบคุมภายในที่ทำให้ข้อมูลสูญหาย การก่อวินาศภัย และอื่น ๆ ซึ่งทำให้เห็นถึงความท้าทายที่ทำให้องค์กรที่มีการใช้ข้อมูล/สารสนเทศมาก ๆ อย่างเช่น ธนาคาร โรงพยาบาล บริษัทผลิตสินค้า บริษัทประกัน หน่วยงานราชการ และอื่นๆ ควรที่จะต้องหันมาให้ความสนใจในการหาวิธีการในการปกป้องและป้องกันข้อมูลสารสนเทศและระบบสารสนเทศในองค์กรอย่างเป็นระบบ
- Requirements of ISMS : กล่าวถึงรายละเอียดอย่างย่อของข้อกำหนดในมาตรฐาน ISO 27001 : 2005 ที่มีการวาง Framework แบบวงจร PDCA ภายใต้ข้อกำหนดตั้งแต่ข้อ 4.2.1 การจัดทำระบบ ISMS ถึงข้อกำหนด 4.2.4 การธำรงรักษาและการปรับปรุง ISMS โดยยกตัวอย่างการประยุกต์ใช้มาตรฐาน ISO/IEC 27001 ที่เริ่มต้นจาก

- การกำหนดนโยบาย ISMS เพื่อเป็นหลักของทิศทางในการดำเนินการรักษาความมั่นคงปลอดภัยของข้อมูลและสารสนเทศที่มีการใช้ในองค์กร
- การกำหนดขอบเขต (Scope) ของการจัดทำระบบ ISO 27001 ที่ชัดเจน เพื่อที่จะได้ทราบขอบเขตของการดำเนินงาน การวางและจัดทำระบบ รวมถึงการปฏิบัติใช้เพื่อให้เกิดการธำรงรักษาและการปรับปรุงระบบการบริหารความมั่นคงปลอดภัยของข้อมูลและสารสนเทศในองค์กรได้อย่างชัดเจน
- การกำหนดวิธีการในการประเมินความเสี่ยง (Risk Assessment Methodology)
- การกำหนดเอกสารที่จำเป็นเพื่อใช้สื่อในการปฏิบัติงาน ตัวอย่างเช่น ขั้นตอนการดำเนินการงาน (Procedure) , Statement of Applicability (SoA) เป็นต้น ทั้งที่เป็นขั้นตอนการดำเนินงานที่บังคับต้องมีตามที่มาตรฐานระบุไว้ (มีทั้งหมด 6 Procedure) และเอกสาร/ขั้นตอนการดำเนินงานที่มีความจำเป็นที่องค์กรเห็นสมควรว่าต้องมี ตัวอย่างเช่น Business Continuity Procedure/Policy, Back-up Procedure/policy เป็นต้น

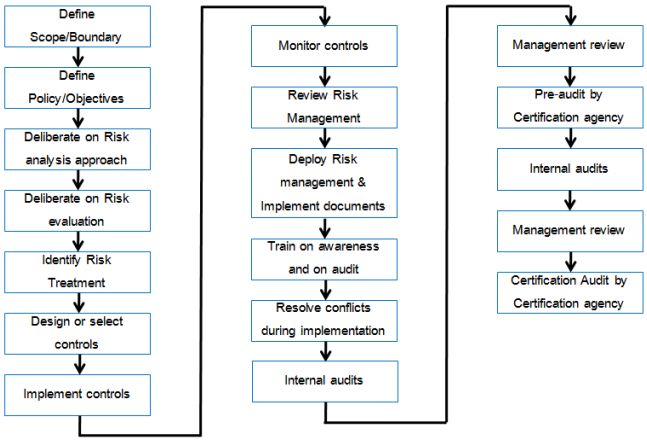
- ***Country Status Report :*** เป็นการนำเสนอของผู้เข้าร่วมโครงการในแต่ละประเทศที่มาจากองค์กรที่มีการดำเนินงานที่แตกต่างกัน ถึงการบริหารจัดการดูแลความปลอดภัยของข้อมูลและสารสนเทศในองค์กร โดยจะมีทั้งองค์กรที่ได้ทำระบบ ISO 27001 แล้ว และองค์กรที่ยังไม่ได้ทำระบบ ISO 27001 ที่สรุปในภาพรวมว่าส่วนใหญ่ก็มีการกำหนดวิธีการในการดูแล ป้องกันข้อมูลและสารสนเทศตาม ISO 27001 แต่อาจจะไม่ได้ทำครบทุกข้อกำหนดและ Control ที่ได้ระบุไว้ในมาตรฐาน

วันที่ 2 (18 ตุลาคม 2554) : Implementing ISMS in an Organization

ในวันที่ 2 จะเน้นประเด็นไปที่การประยุกต์ใช้ ISO 27001 ในองค์กร เพื่อให้ผู้เข้าร่วมได้เห็นถึงแนวทาง/ขั้นตอนในการนำไปประยุกต์ใช้ในองค์กรของตนเองเมื่อสิ้นสุดการเข้าร่วมโครงการ โดยแบ่งหัวข้อออกเป็น 3 หัวข้อ เช่นเดียวกับวันที่ 1 ดังนี้

- ***ISMS Risk Management :*** การบริหารความเสี่ยง (Risk management) เป็นสิ่งสำคัญสำหรับระบบ ISO 27001 ดังนั้นในการบรรยายจึงเริ่มต้นตั้งแต่
  - การปูพื้นฐานถึงคำนิยามของคำต่าง ๆ ที่ควรต้องรู้ในการบริหารความเสี่ยง เช่น Risk, Risk analysis, Risk evaluation, Risk assessment, Risk treatment, Risk acceptance เป็นต้น เพื่อนำไปใช้ในการบริหารความเสี่ยงได้อย่างถูกต้องตามขั้นตอน
  - ความสัมพันธ์ของภัยคุกคาม (Threat) จุดอ่อน (Vulnerability) ความเสี่ยง (Risk) ทรัพย์สิน (Asset) มูลค่าของทรัพย์สิน (Asset value) การควบคุม (Control) และข้อกำหนด (Requirement) ที่ภายใน Risk life cycle
  - วิธีการประเมินความเสี่ยง ตั้งแต่การชี้บ่งความเสี่ยง การประเมินที่มองถึงโอกาสและความรุนแรงที่เกิดขึ้น และการกำหนดวิธีการในการจัดการกับความเสี่ยงที่อาจพิจารณาได้จาก ทางเลือก 4 ทางเลือก คือ การยอมรับความเสี่ยงที่เกิดขึ้น การถ่ายโอนความเสี่ยงไปยังหน่วยงานอื่น การกำหนดมาตรการควบคุมที่เหมาะสม การหลีกเลี่ยงความเสี่ยง เพื่อให้ระดับของความเสี่ยงอยู่ในระดับที่ยอมรับได้

- *Implementation of ISMS :* สิ่งที่เน้นในการประยุกต์ใช้ ISO 27001 คือ Critical Success factor ที่ประกอบไปด้วย 1) การมีนโยบาย ISMS (Information security policy) 2) วัฒนธรรมขององค์กร (Organizational culture) 3) ความมุ่งมั่นของผู้บริหารที่ต่อมีการแสดงให้เห็นถึงการสนับสนุนอย่างชัดเจน (Management commitment/visible support) 4) การบริหารความเสี่ยง (Risk management) 5) การตลาดที่มีประสิทธิผล (Effective marketing) 6) ข้อแนะนำ (Guidance) 7) การสนับสนุนด้านการเงิน (Financial support) 8) ความตระหนัก การฝึกอบรม และการศึกษา (Awareness, training and education) 9) การจัดการกับอุบัติการณ์ (Incident management) ทั้งนี้ Resource person ยังได้แสดงให้เห็นถึงขั้นตอนการประยุกต์ใช้ระบบจนถึงขั้นตอนการขอการรับรองระบบ (ตามที่แสดงในรูปภาพที่ 2)



รูปที่ 2 Road Map to Certification

- *Case Study : PT Panasonic Gobel Energy Indonesia (PECGI)* ในส่วนนี้ได้บรรยายถึงรายละเอียดของระบบ ISO 27001 ที่บริษัทได้มีการประยุกต์ใช้ภายใต้ Scope คือ Provision of the Information Security Management activities in relation to the manufacture of Manganese Dry Batteries, Torchlight and Lithium Coin Batteries in accordance with the Statement of Applicability, Version: 1 บริษัทได้ดำเนินการทำระบบตามแนวทางที่บริษัทแม่ในประเทศญี่ปุ่นกำหนด โดยแบ่งมาตรการในการควบคุม (Control) ออกเป็น 4 กลุ่ม คือ
    - กลุ่มที่ 1 : Information Management Controls ที่มีการแบ่งประเภทของข้อมูลออกเป็น 3 ระดับคือ 1) Strictly Confidential (“SC”) 2) Confidential (“C”) และ 3) Internal Use Only (“IUO”) และการทำ Non-Disclosure Agreement (NDA) กับ ผู้ส่งมอบ
    - กลุ่มที่ 2 : Personnel Security Controls ประกอบไปด้วยการสร้างความตระหนักการศึกษาและการฝึกอบรมที่มีการกำหนดรายละเอียดการฝึกอบรมให้กับพนักงานใหม่และการทำ ISM Test ทุกปี รวมถึงการทำ ISM Socialization การให้พนักงานทุกคนลงนามในข้อตกลงในการทำงาน (Contract agreement) การปฏิบัติตาม PKB Book ของพนักงาน และสุดท้ายเป็นข้อกำหนด ISMS สำหรับพนักงานและผู้เยี่ยมชม
    - กลุ่มที่ 3 : Physical Security Controls มีการแบ่งแยกระดับของความปลอดภัยในแต่ละพื้นที่ออกเป็น 3 ระดับ คือ Zone A (เข้มงวดสูงสุด) Zone B (เข้มงวดปานกลาง) และ

Zone C (ทั่วไปที่ต้องมี ID) โดยในแต่ละ Zone จะมีวิธีการควบคุมในการเข้า-ออก มีกล้อง CCTV และการจัดแยกพื้นที่จอดรถให้อยู่ภายนอกบริษัท พร้อมกับการกำหนดมาตรการในการควบคุมความปลอดภัยและการนำทรัพย์สินเข้า-ออกบริษัท

- กลุ่มที่ 4 : IT Security Controls กำหนดมาตรการในการจัดการกับ Malicious การ back-up การปรับเปลี่ยนข้อมูลและซอฟท์แวร์ การจัดการสื่อสารผ่านโทรศัพท์ แฟกซ์ การใช้ ID และ Password ในระบบสารสนเทศและอื่น ๆ

ทั้งนี้ไปทราบถึงแผนและขั้นตอนในการดำเนินงานสำหรับ ปี 2554 ที่ทางบริษัทได้กำหนดไว้

วันที่ 3 (19 ตุลาคม 2554) : Sessions on Internal Auditing

สำหรับในวันที่ 3 หลังจากที่ทราบถึงข้อกำหนดและแนวทางวิธีการประยุกต์ใช้มาตรฐาน ISO 27001 แล้ว สิ่งสำคัญถัดมาคือ การประเมินถึงประสิทธิผลของระบบ ISO 27001 ด้วยวิธีการที่เป็นที่รู้จักกันดีสำหรับการทำระบบมาตรฐานนั้นก็คือ การตรวจประเมินภายใน ซึ่งในวันนี้แบ่งเป็นกิจกรรมออกเป็น 2 กิจกรรม คือ

- กิจกรรมที่ 1 : การฟังการบรรยายและการเตรียมก่อนไปเยี่ยมชมบริษัทที่ได้รับการรับรองระบบ ISO 27001 โดยเริ่มจากวิธีการพิจารณาถึงทรัพย์สิน (Asset) ภัยคุกคาม (Treat) และจุดอ่อน (Vulnerability) เพื่อเป็นพื้นฐานในการตรวจประเมินต่อไป ทั้งนี้ในระบบ ISO 27001 จะเน้นความปลอดภัยของข้อมูล/สารสนเทศในด้านการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้ของทรัพย์สิน (CIA : Confidentiality, Integrity and Availability) ทั้งนี้ทรัพย์สินยังแบ่งออกได้เป็น 7 ประเภท คือ 1) Physical assets 2) Paper assets 3) Software assets 4) People asset 5) Information assets 6) Intangible assets 7) Service assets โดยได้มีการยกตัวอย่างของทรัพย์สินในแต่ละประเภทอย่างชัดเจน รวมถึงภัยคุกคามที่เข้ามากระทบต่อทรัพย์สินทำให้เกิดความสูญเสียความสามารถในการทำงานได้ของทรัพย์สินนั้น

  จากนั้นก็ได้บรรยายถึงหลักเกณฑ์และวิธีการในการตรวจประเมินภายในระบบ ISO 27001 ตามรูปที่ 3

รูปที่ 3 กระบวนการตรวจประเมิน (Audit process)

โดยสามารถสรุปในภาพรวมของกระบวนการตรวจประเมินได้เป็น 4 ส่วน ดังนี้

- การวางแผนการตรวจประเมิน (Plan) ณ ขั้นตอนนี้ผู้ตรวจประเมินจะเริ่มต้นจากการพิจารณาถึงขอบเขต เกณฑ์ วัตถุประสงค์ของการตรวจประเมินในครั้งนั้น ๆ เพื่อกำหนดแผนการตรวจประเมินที่เหมาะสมเพื่อใช้ในการสื่อสารกับผู้ที่เกี่ยวข้อง เช่น ผู้ตรวจประเมินในทีม ผู้รับการตรวจประเมินในหน่วยงานต่าง ๆ เป็นต้น จากนั้นทีมผู้ตรวจประเมินจะร่วมกันดำเนินการศึกษาข้อมูลที่เกี่ยวข้องกับหัวข้อที่รับผิดชอบในการตรวจประเมินเพื่อเตรียมหัวข้อหรือประเด็นที่จะใช้ในการตรวจประเมินไว้ในเอกสารรายการการตรวจประเมิน (Audit Checklist) และแบ่งบทบาทหน้าที่ในการตรวจประเมิน
- การดำเนินการตรวจประเมิน (Conduct) ทีมผู้ตรวจประเมินจะเริ่มต้นการตรวจประเมินตามกำหนดเวลาที่ระบุไว้ในแผนการตรวจประเมิน โดยเริ่มต้นจากการประชุมเปิดเพื่ออธิบายถึงขอบเขต วัตถุประสงค์ของการตรวจประเมิน แผนและวิธีการตรวจประเมิน พร้อมกับยืนยันรายละเอียดขั้นตอนการตรวจประเมินกับผู้รับการตรวจประเมินก่อนที่จะเริ่มการตรวจประเมิน ทั้งนี้ในระหว่างที่ดำเนินการตรวจประเมินอยู่นั้นผู้ตรวจประเมินสามารถปรับใช้รูปแบบวิธีการตรวจประเมิน (Audit Track) ให้เหมาะสม ซึ่งรวมถึงวิธีการสุ่มดูหลักฐาน เพื่อให้ได้มาซึ่งข้อมูลถึงการปฏิบัติงาน (ที่อาจมาจากสัมภาษณ์ผู้ปฏิบัติงาน การปฏิบัติที่เกิดขึ้นที่หน้างาน หรือหลักฐานที่เป็นเอกสาร/บันทึกงาน) ในประเด็นที่เกี่ยวข้องตามที่ข้อกำหนดของมาตรฐาน ISO 27001 ระบุไว้กับงานนั้น ๆ พร้อมจดบันทึกไว้ในช่วงระหว่างการตรวจประเมิน
- การรายงานผลการตรวจประเมิน (Report) ทีมผู้ตรวจประเมินจะสรุปข้อมูลที่ได้ในระหว่างการตรวจประเมินเพื่อสรุปผลการตรวจประเมิน ซึ่งผลการตรวจประเมินแบ่งได้เป็น 3 กลุ่ม ดังนี้ 1. การดำเนินงานที่ดี (noteworthy efforts) 2. การดำเนินงานที่ยังมีข้อบกพร่อง (NC : Non-conformity) 3. การดำเนินการที่เป็นข้อสังเกตุ (OBS : Observation) ทั้งนี้หัวใจหลักขององค์ประกอบในการเขียนข้อสรุปของการดำเนินงานที่เป็นข้อบกพร่องนั้นจะต้องประกอบด้วยรายละเอียดของสิ่งที่เป็นข้อบกพร่อง หลักฐานที่ระบุ และข้อกำหนดในมาตรฐาน ISO 27001 จากนั้นทีมผู้ตรวจประเมินจะทำการรายงานผลการตรวจประเมินให้ตัวแทนผู้รับการตรวจประเมินรับทราบเพื่อนำข้อมูลไปดำเนินการปรับปรุง แก้ไข หรือป้องกันการดำเนินงานภายใต้ระบบ ISO 27001 ตามช่วงระยะเวลาที่เหมาะสมต่อไป
- การติดตามผลการดำเนินการหลังการตรวจประเมิน (Follow up) การติดตามผลการดำเนินการถือเป็นอีกหนึ่งหัวใจสำคัญในการดำเนินงานในระบบ ISO 27001 ที่ต้องตามถึงการดำเนินการว่าได้ดำเนินการแก้ไขที่สาเหตุและมีการขยายผลการแก้ไขได้อย่างครอบคลุม ครบถ้วนและสมบูรณ์ เพื่อไม่ให้ปัญหาหรือข้อบกพร่องนั้นย้อนกลับมาเกิดขึ้นซ้ำอันจะทำให้ประสิทธิผลของระบบ ISO 27001 ได้ไม่ตรงตามวัตถุประสงค์ที่บริษัทต้องการ

ทั้งนี้เพื่อให้ผู้เข้าร่วมโครงการสามารถนำความรู้ในเรื่องของกระบวนการตรวจประเมินไปประยุกต์ใช้ได้จริง ทางโครงการอบรมนี้จึงได้ทำการแบ่งกลุ่มผู้เข้าร่วมออกเป็น 4 กลุ่มเพื่อจัดทำแผนการตรวจ

ประเมินและกำหนดประเด็นคำถามเพื่อใช้ประเมินระบบ ISO 27001 ในระหว่างการเข้าไปเยี่ยมชมที่บริษัท PT Panasonic Gobel Energy Indonesia (PECGI)

- กิจกรรมที่ 2 : การเยี่ยมชมบริษัท PT Panasonic Gobel Energy Indonesia (PECGI) ในช่วงบ่ายได้เดินทางไปยัง PECGI และได้เข้าเยี่ยมชมระบบ ISO 27001 ที่บริษัทได้มีการประยุกต์ใช้จริงโดยจุดที่ทางบริษัทได้นำเสนอมีทั้งการบรรยายสรุป การพาไปเยี่ยมชมจุดที่เกี่ยวกับ ISO 27001 และการตอบข้อซักถามของผู้เข้าร่วม ซึ่งส่วนใหญ่จะเป็นลักษณะของการดูการควบคุมทางกายภาพ เช่น การดูพื้นที่ที่บริษัทกำหนดให้จอดรถภายนอกโรงงาน การกำหนดประตูทางเข้าของพนักงานและผู้มาติดต่อบริษัทแยกจากกัน การตรวจสอบทรัพย์สินทั้งก่อนเข้า-ออกของพนักงานและผู้ติดต่อ การจัดตู้ล็อคเก็บของส่วนบุคคลไว้ก่อนเข้าพื้นที่ทำงาน ระบบรักษาความปลอดภัย ระบบการแสดงตัวตน (ID Card) ในการเข้าในแต่ละพื้นที่ตามสิทธิที่กำหนด การทำ ISM Patrol เป็นต้น เป็นที่น่าเสียดายที่ไม่ได้มีโอกาสได้เห็นถึงเอกสารที่ทางบริษัทใช้ในการทำระบบ ไม่ว่าจะเป็น SoA วิธีการรายละเอียดของเกณฑ์ที่ใช้ในการประเมินความเสี่ยงและรายละเอียดการควบคุมอื่น ๆ ที่ได้กำหนดไว้เป็นเอกสารเพื่อสื่อให้กับพนักงานและบุคคลที่เกี่ยวข้องกับงานของบริษัทได้ปฏิบัติตาม แต่สิ่งสำคัญที่เห็นในการที่เข้าเยี่ยมชมบริษัทนี้ความมุ่งมั่นของผู้บริหาร ความเข้มแข็งของทีมงานทำและดูแลระบบรวมถึงการให้ความร่วมมือในการปฏิบัติตามอย่างจริงจังของบุคลากรทุกคนที่ได้ฝังรากจนกลายเป็นวัฒนธรรมของบริษัทที่มีการประพฤติปฏิบัติเป็นปกติ

รูปที่ 4 การเข้าเยี่ยมชม ณ บริษัท PT Panasonic Gobel Energy Indonesia (PECGI)

วันที่ 4 (20 ตุลาคม 2554) : Workshop and Examination

ในวันที่ 4 เป็นการทำงานกลุ่มเพื่อสรุปถึงประเด็นของสิ่งที่พบในระหว่างการเข้าเยี่ยมชมที่บริษัท PT Panasonic Gobel Energy Indonesia (PECGI) ว่าได้พบประเด็นที่ทางบริษัทมีการดำเนินงานที่สอดคล้อง/ไม่สอดคล้อง/ข้อสังเกตเมื่อเทียบกับข้อกำหนดในมาตรฐาน ISO 27001 ตามประเด็นที่แต่ละกลุ่มได้ถูกมอบหมายให้ประเมินในระหว่างการเยี่ยมชม โดยในระหว่างการทำงานกลุ่มจะเห็นได้ว่ารายละเอียดของข้อมูลที่แต่ละผู้เข้าร่วมแต่ละท่านที่ได้มามีมุมมองที่แตกต่างกัน ทำให้ต้องมีการพูดคุยอธิบายเหตุผลเพื่อที่จะได้ทำการสรุปออกมาเป็นความเห็นของกลุ่มได้ซึ่งก็ใช้เวลาพอสมควรในแต่ละประเด็น จากนั้นกลุ่มก็จัดทำเอกสารนำเสนอเพื่อเตรียมพร้อมสำหรับการนำเสนอในวันที่ 5 และภายหลังจากการรับประทานอาหารกลางวันแล้วในช่วงบ่ายเป็นการทำ

แบบทดสอบความเข้าใจเกี่ยวกับความรู้ในมาตรฐาน ISO 27001 ที่ได้รับในโครงการนี้ ซึ่งผลสุดท้ายพบว่าผู้เข้าร่วมทุกท่านผ่านหมด โดยมีเพื่อสมาชิกจากฟิลิปปินส์เป็นผู้ที่ได้คะแนนสูงสุด

วันที่ 5 (21 ตุลาคม 2554) : Group presentation and closing

สำหรับวันสุดท้ายแต่ละกลุ่มได้นำเสนอสิ่งที่ได้พบในการเข้าเยี่ยมชมที่บริษัท PT Panasonic Gobel Energy Indonesia (PECGI) ในฐานะเป็นผู้ตรวจประเมิน Resource person ทั้ง 2 ท่านก็ให้คำแนะนำที่เป็นประโยชน์เพิ่มเติมในภายหลังจากที่มีการนำเสนอของแต่ละกลุ่ม และสุดท้ายก็เป็นพิธีปิดอย่างเป็นทางการ

รูปที่ 5 การทำงานกลุ่ม และการนำเสนอผลงาน

จากการที่ได้เข้าร่วมโครงการในครั้งนี้ทำให้ได้เห็นถึงความสำคัญของการจัดการข้อมูลให้มีความปลอดภัย รวมวิธีการในการประยุกต์ใช้มาตรฐาน ISO 27001 ในองค์กร ซึ่งจากความรู้ที่ได้มานี้สามารถที่นำมาขยายผลต่อกับงานที่รับผิดชอบในปัจจุบันส่วนหนึ่งคือการให้คำปรึกษาแนะนำการจัดทำระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) ทั้งนี้เนื่องจากข้อมูลที่ในแต่ละองค์กรใช้นั้นล้วนแล้วแต่มีผลต่อการดำเนินงานขององค์กรทั้งสิ้น หากขาดซึ่งข้อมูลหรือข้อมูลมีความไม่สมบูรณ์ พร้อมใช้ก็สามารถทำให้เกิดผลกระทบต่อการดำเนินงานขององค์กรได้ แต่ก็เป็นที่น่าเสียดายที่หลังจากที่ได้กลับมาจากการเข้าร่วมโครงการนี้แล้วประเทศไทยก็เผชิญกับภัยธรรมชาติที่ไม่สามารถคาดคิด (น้ำท่วม) ซึ่งทำให้การที่จะนำความรู้ที่ได้จากโครงการไปใช้กับบริษัทลูกค้าในโครงการ TLC-มอก. 22301 (BCM) เกิดการหยุดชะงักไปเนื่องจากบริษัทลูกค้าได้รับผลกระทบจากภัยพิบัติดังกล่าว ซึ่งมีทั้งน้ำท่วม หรือได้รับผลกระทบทางอ้อมจากปัญหาการทำงานที่สะดุดเนื่องจากลูกค้าของลูกค้าถูกน้ำท่วม ทำให้ไม่สามารถนำความรู้ที่ได้จากโครงการนี้ไปใช้ได้ แต่หลังจากที่ภัยทางธรรมชาตินี้ได้ผ่านพ้นไปแล้วก็น่าที่จะได้นำไปใช้กับลูกค้าในโอกาสถัดไป