รายงานการเข้าร่วมโครงการเอพีโอ

12-IN-08-GE-TRC-B

Training Course on the Information Security Management System: ISO 27000 for SMEs

ระหว่างวันที่ 15 – 18 **พฤษภาคม** 2555

ณ กรุงโซล ประเทศ เกาหลีใต้

จัดทำโดย นายธารา ธีรวงศ์วศิน

ผู้จัดการส่วนเทคโนโลยีสารสนเทศ สำนักผู้อำนวยการ

วันที่ 1 มิถุนายน 2555

ส่วนที่ 1 ข้อมูลทั่วไปของโครงการ

1.1 รหัสและชื่อโครงการ :

12-IN-08-GE-TRC-B **Training Course on the Information Security Management System: ISO 27000 for SMEs**

1.2 ระยะเวลา : 4 วัน ตั้งแต่วันที่ 15 ถึงวันที่ 18 พฤษภาคม 2555

1.3 สถานที่จัด (เมือง ประเทศ) : กรุงโซล ประเทศเกาหลีใต้

1.4 ชื่อเจ้าหน้าที่เอพีโอประจำโครงการ

Ms. Yumiko Yamashita	(Program Officer, APO)
Mr. Jun Ho Kim	(Director, International Cooperation Department, APO Liaison Officer for the Republic of Korea, Korea Productivity Center (KPC))
Mr. Taiho Kang	(Project Manager, International Cooperation Department, Korea Productivity Center (KPC))

1.5 จำนวนวิทยากรบรรยาย : 2 ท่าน

APO International Expert (India)

1.5.1 Mr. Duggirala Sathya Prakash
Manager, Business Development
Det Norske Veritas AS
#202/203, Babukhan Millennium Centre, Opp. Rajbhavan Road
Somajiguda, Hyderabad – 500 082 India

1.5.2 Mr. Syed Taqi Ali Zaidi
Lead Auditor-ACT
Det Norske Veritas AS
#202/203, Babukhan Millennium Centre, Opp. Rajbhavan Road
Somajiguda, Hyderabad – 500 082 India

1.6 จำนวนผู้เข้าร่วมโครงการและประเทศที่เข้าร่วมโครงการ : ทั้งหมด 18 ท่าน จาก 13 ประเทศ

ส่วนที่ 2 เนื้อหา/องค์ความรู้จากการเข้าร่วมโครงการ

วัตถุประสงค์ของโครงการ :

1. เพื่อให้ผู้เข้าร่วมอบรมได้ทราบและเข้าใจถึง ความสำคัญของ การมีมาตรฐานในการจัดการด้านความปลอดภัยข้อมูลสารสนเทศทางธุรกิจและ ทรัพย์สินอื่น ๆ (Information Asset) ที่เกี่ยวข้อง ซึ่งมีความสำคัญต่อความต่อเนื่องในการดำเนินธุรกิจ

2. เพื่อให้ผู้เข้าร่วมอบรมได้เข้าใจถึงขั้นตอนหรือแนวทางการจัดการด้านความปลอดภัยตามแนวทางของระบบมาตรฐาน ISO 27000 โดยพิจารณาจากโครงสร้าง และข้อกำหนดของระบบมาตรฐานดังกล่าว

3. เพื่อให้ผู้เข้าร่วมอบรมได้ทำความเข้าใจกับขั้นตอนหลัก ๆ ที่สำคัญในการดำเนินการ Implement ระบบบริหารจัดการด้านความปลอดภัยให้เกิดขึ้นในองค์กร ตลอดจนวงจรของระบบที่ทำให้เกิดความต่อเนื่องในการบริหารจัดการด้านความปลอดภัยข้อมูลสารสนเทศทางธุรกิจและ ทรัพย์สินอื่น ๆ (Information Asset) ที่สำคัญ

(ต้องมีความยาวเพียงพอกับเนื้อหาสาระองค์ความรู้และประสบการณ์ที่ได้รับ ทั้งนี้ เพื่อประโยชน์ในการเผยแพร่องค์ความรู้และประสบการณ์ให้กับผู้สนใจ โดยจะนำเสนอผ่านการจัดพิมพ์ในวารสาร APO Digest และ/หรือเว็บไซต์ของสถาบัน)

2.1 ที่มาหรือวัตถุประสงค์ของโครงการโดยย่อ

a) เพื่อให้สามารถนำความรู้ไปใช้ในการจัดการด้านความปลอดภัยอย่างเพียงพอเพื่อปกป้อง Information Assets ที่สำคัญขององค์กร
b) เพื่อให้สามารถนำ Framework : PDCA (Deming Cycle) ไปใช้ในการปรับปรุงการดำเนินการด้าน ISMS อย่างต่อเนื่อง
c) เพื่อให้เข้าใจวิธีการจัดการความเสี่ยง และสามารถจัดการได้อย่างเป็นระบบ

2.2 เนื้อหา/องค์ความรู้ที่ได้จากการฟังบรรยาย (จำแนกตามหัวข้อและระบุชื่อวิทยากรบรรยาย)

1. ความสำคัญของการบริหารจัดการความปลอดภัยข้อมูลสารสนเทศและ ทรัพย์สินอื่น ๆ (Information Asset)

เริ่มต้นวันแรกของการอบรม ด้วยการให้ผู้เข้าร่วมอบรมแต่ละประเทศได้นำเสนอ Country Presentation ซึ่งมีเนื้อหาแนะนำตนเอง หน่วยงานหรือองค์กรที่ปฏิบัติงานอยู่ และตามด้วยเนื้อหาที่เกี่ยวข้องกับหัวข้ออบรม โดยให้แนะนำถึงสภาพหรือลักษณะทั่วไปของ SMEs ในประเทศ และกฎหมายที่เกี่ยวข้องกับระบบคอมพิวเตอร์และการสื่อสารข้อมูลสารสนเทศ การจัดการความปลอดภัยของข้อมูลสารสนเทศของประเทศ รวมไปถึงตัวอย่างภัยคุกคาม การกระทำผิด การละเมิด ภัยธรรมชาติ ผลกระทบที่เกิดขึ้น และความยากลำบากในการดำเนินการผลักดันให้เกิดการบริหารจัดการด้านความปลอดภัยข้อมูลสารสนเทศในกลุ่มธุรกิจขนาดกลางและขนาดย่อม (SMEs) ซึ่งไม่ว่าจะเป็นประเทศใด ล้วนมีข้อจำกัดในการดำเนินการที่คล้ายคลึงกัน

กล่าวคือ SME โดยส่วนใหญ่ขาดความรู้ ความเข้าใจถึง ความสำคัญ ของ ISMS อย่างลึกซึ้ง ขาดบุคลากรที่มีความสามารถ (บุคลากรดังกล่าวมีต้นทุนสูง) ประกอบกับ SMEs ส่วนใหญ่ให้ความสำคัญกับความอยู่รอด การหารายได้ การสร้างกำไร มากกว่าที่จะดำเนินการด้านความปลอดภัยข้อมูลสารสนเทศให้ได้ตามมาตรฐานสากล ดังนั้น การจัดการด้านความปลอดภัยของข้อมูล ในภาคของ SME โดยส่วนใหญ่ จึงเป็นการจัดการทั่วไปตามปกติ เช่น การจัดการด้านการสำเนาข้อมูลทางธุรกิจ การสำเนาข้อมูลตามที่กฎหมายกำหนด เพียงเพื่อให้สามารถรองรับสถานการณ์เมื่อเกิดเหตุจำเป็นเท่านั้น โดยไม่มีกระบวนการจัดการตามมาตรฐานที่จะช่วยให้ธุรกิจสามารถบริหารจัดการด้านความปลอดภัยได้อย่างครบวงจร

SMEs โดยส่วนใหญ่ จะดำเนินการจัดการด้านความปลอดภัยในระบบสารสนเทศเท่าที่จำเป็น หรือเท่าที่มีประสบการณ์จากการได้รับผลกระทบจากภัยคุกคามเท่านั้น ซึ่งสาเหตุส่วนหนึ่งเกิดจากข้อจำกัดของธุรกิจ SMEs ซึ่งไม่มีกำลังเหมือนธุรกิจขนาดใหญ่ สัดส่วนของมูลค่าทางเศรษฐกิจของประเทศในกลุ่มของธุรกิจ SMEs นั้นถือว่า มีมูลค่าไม่น้อย ดังนั้น หากเกิดภัยที่ส่งผลกระทบและสร้างความเสียหายต่อการดำเนินธุรกิจในกลุ่ม SMEs แล้ว ย่อมส่งผลกระทบต่อเศรษฐกิจของประเทศไม่น้อยเช่นกัน การดำเนินการของภาครัฐ ในการส่งเสริม ผลักดัน และให้ความช่วยเหลือ ทั้งด้านการให้ความรู้ความเข้าใจ งบประมาณส่งเสริมสนับสนุน และการผลักดันด้านกฎหมายที่เกี่ยวข้อง ล้วนเป็นเรื่องสำคัญที่จะปกป้องมูลค่าทางเศรษฐกิจของประเทศ ให้รอดพ้น หรือลดทอนผลกระทบ ที่มาจากภัยคุกคามที่จะเกิดขึ้น

การเริ่มต้นด้วยการนำเสนอ Country Presentation ของแต่ละประเทศนั้น ผู้เชี่ยวชาญมีเจตนาให้ผู้เข้าร่วมอบรมได้ทำความเข้าใจกับ ลักษณะของแต่ละประเทศภายใต้เนื้อหาของเรื่องเดียวกันซึ่งสอดคล้องกับหัวข้ออบรมที่ว่าด้วยเรื่อง “Information Security Management System: ISO 27000 for SMEs” ตามที่ได้กล่าวไว้ข้างต้นนั้น เป็นการแสดงให้เห็นถึงความสำคัญของการบริหารจัดการความปลอดภัยข้อมูลสารสนเทศ (ISMS)

หลังจากการนำเสนอ Country Presentation ของแต่ละประเทศเสร็จเรียบร้อยแล้ว Mr. Duggirala Sathya Prakash ได้กล่าวนำเข้าสู่หลักสูตร และสรุปให้เห็นถึงความสำคัญของ Information Security Management Systems (ISMS)

จากนั้น Mr. Syed Taqi Ali Zaidi (APO International Expert) ได้นำเข้าสู่เนื้อหาในส่วนแรก เกี่ยวกับการนำ ISMS ไปใช้ในองค์กร กระบวนการเตรียมการเพื่อขึ้นระบบ ISMS ในองค์กร ซึ่งถือเป็นขั้นตอนวางแผนเพื่อ Establish ISMS เนื้อหาของการอบรม ประกอบไปด้วย

1. แนะนำมาตรฐาน ISO 27001 (The Requirements)
2. Control objective implementation (ที่ระบุไว้ใน ISO 27001 Annex A.)
3. Information และ Elements of information security
4. การกำหนด Scope and Boundary for ISMS
5. การประเมินความเสี่ยง (Risk Assessment)

6. การจัดการความเสี่ยง (Risk Management)
7. ทำความเข้าใจเกี่ยวกับ Document และ Records
8. เอกสารที่ต้องมีตาม Requirement ของระบบมาตรฐาน ISO 27001
9. Implementation & Operating

ในเอกสาร ISO 27001 Annex A ว่าด้วยเรื่อง Control objectives และ Controls
Control Objective คือ ข้อกำหนดที่กำหนดขึ้นเพื่อให้ได้ผลลัพธ์ที่ต้องการ เพื่อให้บรรลุตามวัตถุประสงค์ตามโยบายควบคุม ในการดำเนินงานของทีมงาน IT

Control โดยหลักแล้วกำหนดขึ้นเพื่อการบริหารจัดการความเสี่ยง ซึ่งรวมอยู่ใน Policy, Procedures, Guidelines, Practices, etc.

Control objectives ใน ISO 27001 Annex A. ประกอบด้วย

A.5 Security Policy (Information Security Policy)
เป็นการกำหนดนโยบายด้านความปลอดภัยของข้อมูล เพื่อ ให้ทิศทางการจัดการ การสนับสนุนสำหรับการรักษาความปลอดภัยข้อมูล เป็นไปอย่างสอดคล้องกับความต้องการทางธุรกิจ (Business Requirements) กฎหมายและกฎระเบียบที่เกี่ยวข้อง

A.6 Organization of information security
เป็นการจัดการด้านความปลอดภัยของข้อมูลในองค์กร โดยจะต้องกำหนดผู้รับผิดชอบดูแลจัดการด้านความปลอดภัยของข้อมูล

A.7 Asset management
เป็นการจัดการด้าน Assets ขององค์กร (Information Asset) โดยจะต้องมีการจำแนกประเภทของ Assets (Asset classification : Physical asset, Paper asset) โดยกำหนดชื่อของ Asset จุดอ่อน/ช่องโหว่ของ Asset นั้น และภัยคุกคามที่อาจจะเกิดกับ Asset นั้น ทั้งนี้เพื่อให้สามารถจัดการด้านการป้องกัน Asset ต่าง ๆ ได้อย่างเหมาะสม

A.8 Human resources security
เป็นการจัดการความปลอดภัยด้านทรัพยากรบุคคล ลดความเสี่ยงอันมาจากบุคลากร เพื่อให้แน่ใจว่าอยู่ในความปลอดภัย และไม่ได้รับผลกระทบจากบุคลากร

A.9 Physical and environmental security
เป็นการจัดการด้านลักษณะ และสภาพแวดล้อมทางกายภาพ ให้อยู่ในความปลอดภัย เพื่อไม่ให้เกิดการเข้าถึงโดยไม่ได้รับอนุญาต และป้องกันภัยคุกคามที่อาจเกิดขึ้นได้

A.10 Communications and operations management
เป็นการดำเนินการเพื่อให้แน่ใจว่า Facilities ต่าง ๆ ที่ใช้ในการประมวลผลข้อมูล อยู่ในความพร้อมใช้ สามารถทำงานได้อย่างถูกต้อง และปลอดภัย ดังนั้นจึงต้องมีการกำหนดขั้นตอนการดำเนินงาน ความรับผิดชอบ เพื่อให้เกิดความชัดเจน แน่นอนในการปฏิบัติการ เพื่อจัดการกับ Facilities ต่าง ๆ

ที่ใช้ในการประมวลผลข้อมูล (Operation Procedure & Responsibility, System Planning, Software, Backup, Network, Media handling etc.)

A.11 Access Control

เป็นการควบคุมการเข้าถึงข้อมูล พิจารณาจาก Business Requirement ว่ามีความต้องการอย่างไรในการควบคุมการเข้าถึงข้อมูล (User access control, Network access control, Application & information access control etc.)

A.12 Information systems acquisition, development and maintenance

เป็นการดำเนินการเพื่อให้เกิดความมั่นใจ ในความปลอดภัยของระบบสารสนเทศที่มีอยู่ ตั้งแต่ในกระบวนการได้มาซึ่งระบบ กระบวนการพัฒนา และการบำรุงรักษา

A.13 Information security incident management

เพื่อให้มั่นใจว่ามีการจัดการด้านการตอบสนองต่อเหตุการณ์ที่เกิดขึ้นที่เกี่ยวกับความปลอดภัยของข้อมูล การกำหนดบทบาทหน้าที่ความรับผิดชอบ การติดต่อสื่อสาร วิธีการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น การรายงานผล เพื่อแก้ไขปรับปรุงจุดอ่อน หรือช่องโหว่ที่เกิดขึ้น เพื่อนำไปสู่การแก้ไขปรับปรุง

A.14 Business continuity management

เพื่อให้มั่นใจว่า องค์กรมีการจัดการด้านความปลอดภัยโดยครอบคลุมถึงผลกระทบด้านความต่อเนื่องในการดำเนินธุรกิจ เพื่อป้องกันไม่ให้กระบวนการทางธุรกิจที่สำคัญต้องหยุดชะงัก หรือล้มเหลว

A.15 Compliance

เพื่อให้มั่นใจว่า องค์กรมีการปฏิบัติตามข้อกำหนดของกฎหมาย กฎระเบียบ หรือข้อผูกพันธ์ทางสัญญาต่าง ๆ

Information และ Elements of information security

องค์ประกอบสำคัญของ Information Security มีอยู่ด้วยกัน 3 องค์ประกอบด้วยกัน คือ (CIA)

Confidentiality : คือ คุณสมบัติด้าน การไม่เปิดเผยข้อมูลสำคัญให้กับคน หน่วยงาน หรือกระบวนการที่ไม่ได้รับอนุญาต

Integrity : คือ คุณสมบัติด้านความถูกต้อง สมบูรณ์ของข้อมูล

Availability : คือ คุณสมบัติด้าน ความสามารถในการเข้าถึง และความพร้อมใช้ ซึ่งเป็นไปตามสิทธิ์ที่ได้รับ

การกำหนด Scope and Boundary for ISMS

Scope นั้น Focus ที่ (1) ขอบเขตของการ implementation ระบบ ISMS และ (2) ขอบเขตของการนำระบบ ISMS ขององค์กรเข้ารับการขอ Certify

Boundary นั้น เป็นการพิจารณาจากสถานที่ตั้ง หรือ หน่วยงาน ซึ่งเป็นได้ทั้ง Physical และ Logical

การประเมินความเสี่ยง (Risk Assessment)

เพื่อประเมินความเสี่ยงที่มีผลกระทบต่อความปลอดภัยของ Information Asset สำคัญขององค์กร โดยการหาว่ามีภัยคุกคาม มีจุดอ่อน หรือมีช่องโหว่ใดบ้างที่มีผลต่อ Information Assets สำคัญขององค์กร เริ่มต้นด้วยการจำแนก Assets ต่าง ๆ (Software, Hardware, People, Paper, Physical Asset, Intangible Asset etc.) แล้วประเมินหาช่องโหว่/จุดอ่อน ประเมินหาภัยคุกคามที่มีต่อช่องโหว่/จุดอ่อนนั้น ๆ จากนั้นประเมินผลกระทบที่มีต่อ Information Assets นั้น (จำแนกตามองค์ประกอบสำคัญ CIA คือ ผลกระทบที่มีต่อ Confidentiality, Integrity, Availability) และจัดลำดับความเสี่ยงที่ประเมินได้ (Risk classification) โดยพิจารณาจากโอกาสที่จะเกิด และผลกระทบที่ได้รับ

การจัดการความเสี่ยง (Risk Management)

ภายหลังจากการประเมินความเสี่ยงแล้ว จะนำผลที่ประเมินได้ มาทำการคัดเลือก และกำหนดแนวทางการจัดการ ซึ่งประกอบด้วย 4 แนวทางด้วยดังนี้

Risk treatment options

1. Risk Reduction คือ การดำเนินการเพื่อลดความเสี่ยง
2. Risk Acceptance คือ ระดับความเสี่ยงที่ยอมรับได้
3. Risk Avoidance คือ การหลีกเลี่ยงความเสี่ยงนั้น
4. Risk Transfer คือ การถ่ายโอนความเสี่ยงนั้น ให้ผู้อื่นรับไปดำเนินการแทน

โดยส่วนมากแล้วจะต้องมีการดำเนินการเพื่อลดความเสี่ยง (Risk Reduction) สิ่งที่จะต้องดำเนินการต่อไปเพื่อ Controls คือ การกำหนดกฎระเบียบ วิธีปฏิบัติ และเอกสารที่เกี่ยวข้อง (Rules and Documents)

Risk Management Plan (กำหนดแผนบริหารจัดการความเสี่ยง)

โดยในแผนจะต้องมีข้อมูลกิจกรรมที่จำเป็นสำหรับการดำเนินการลดความเสี่ยงทั้งหมด กำหนดผู้รับผิดชอบ จัดลำดับความสำคัญ และรายละเอียดอื่นที่จำเป็น

Implementation controls

โดยองค์กรจะต้องทำการ Implement แผนจัดการความเสี่ยง และคอยติดตาม กำกับดูแล (Monitor) เพื่อให้มั่นใจว่าสภาพแวดล้อมที่เกี่ยวข้องกับ Information Asset ได้มีการดำเนินการตามแผนจัดการเพื่อความเสี่ยงที่ได้กำหนดไว้

ทำความเข้าใจเกี่ยวกับ Document และ Records

การจัดทำ Documents ที่ดีจะต้องมีองค์ประกอบของการจัดทำและควบคุมเอกสารดังรายละเอียดต่อไปนี้

- Document No.#
- Title of Document
- Date & Version
- Purpose
- Contents/Photograph
- Records/Attachment
- Distribution/Recipient

Author

Status: Reviewed/Approved Sign

Change History

Type of document (Confidential/Private/Public)

Page Number/Page Amount

เอกสารที่ต้องมีตาม Requirement ของระบบมาตรฐาน ISO 27001

ในการจัดทำเอกสาร ใช้มาตรฐานข้างต้นในการจัดทำ เพื่อประโยชน์ในการนำไปใช้งาน การควบคุม การติดตาม โดยเอกสารตาม Requirement ของระบบ ISO 27001 นั้นประกอบด้วย

1. ISMS Scope
2. ISMS Policy & Objective
3. Risk Assessment methodology
4. ISMS Manual (which has references to all the clauses of ISO 27001 standard)
5. Risk assessment reports
6. Risk treatment methodology (Reduce, Avoid, Transfer, Accept)
7. Risk treatment plans
8. Procedures & Controls (in support of ISMS)
9. Statement of Applicability

   เป็นเอกสารที่องค์กรต้องจัดทำขึ้นเพื่อแสดงให้เห็นถึงการนำ Control ต่าง ๆ ตามมาตรฐานที่กำหนดไปประยุกต์ใช้ให้เหมาะสมกับความต้องการและสภาพแวดล้อมขององค์กร โดยเนื้อหาในเอกสารนี้ระบุถึง..

   a. Control Number
   b. Control Description
   c. Applicable (ระบุ Yes/No)
   d. Reason for Applicability / Non Applicability
   e. Remark
10. Mandated procedures
    a. Document Control
    b. Control of Records
    c. Internal Audit Procedure
    d. Corrective Action / Preventive Action
    e. Procedure for Risk Assessment

Implementation & Operating

ในการ implement ระบบ ISO 27001 นั้นใช้วงจร PDCA นำ ในทุก ๆ กิจกรรม โดยมี Frame work ของกิจกรรมหลักที่ต้องดำเนินการดังนี้

1. Management commitment
2. Scope & Policy
3. Setup Risk Assessment team
4. Start of Risk Assessment team
5. Complete Risk Assessment
6. Start Documents
7. Audit Training
8. Finish Document
9. Becoming to Audit stage

หลังจากที่ได้ implement ระบบ ISO 27001 แล้ว กลไกการ Improvement จะประยุกต์ใช้ ISMS Management Framework ในการปรับปรุง โดยให้ความสำคัญกับการบริหารจัดการความเสี่ยง (Risk Management) ซึ่งต้องมีการบริหารจัดการอย่างเป็นระบบและครบวงจร เพื่อให้ ISMS ขององค์กรมีการพัฒนาปรับปรุงอย่างต่อเนื่อง

ความเห็นเพิ่มเติมจากการเข้าร่วมการอบรมในหลักสูตร

จากการตั้งข้อสังเกตตลอดหลักสูตรอบรม พบว่า ชื่อของหลักสูตรนั้น ทำให้ผู้เข้าร่วมอบรมส่วนใหญ่จะเข้าใจว่าเนื้อหาของหลักสูตรน่าจะเป็นการ Customize เนื้อหาสำหรับ SMEs โดยเฉพาะ หรือถ้าเป็น Frame work ที่จะนำไปใช้ในการ Implement ระบบ ISMS ตามมาตรฐาน ISO 27001 นั้น น่าจะเป็น Framework ที่มีความเหมาะสมกับ SMEs ที่สามารถนำไปปฏิบัติได้ แต่จากการอบรมที่ผ่านมานั้น มีเพียงวันแรกที่มีการนำเสนอ Country Presentation ในหัวข้อเดียวกัน เกี่ยวกับ ISMS สำหรับ SMEs ในแต่ละประเทศ เพื่อเริ่มต้นและชักนำเข้าสู่หลักสูตร และมีตัวอย่างที่ใช้ในการทำ Workshop ที่ใช้ SMEs Bank เป็นตัวอย่าง โดยเนื้อหาในส่วนอื่นจากการฟังการบรรยายนั้น ไม่มีการกล่าวถึง SMEs อีกเลย

จากความเข้าใจตลอดหลักสูตรและการตั้งข้อสังเกตข้างต้นนั้น ทำให้เข้าใจว่า การบริหารจัดการด้านความปลอดภัยระบบสารสนเทศ (ISMS) ตามมาตรฐาน ISO 27001 นั้น เมื่อพิจารณาในเนื้อหา Guide Line ในการ implementation และ Requirement ตามที่ระบุไว้ใน ISO 27001 ประกอบกับเนื้อหาที่รับการอบรม จะเห็นได้ว่าหลักสูตร มุ่งเน้นที่ (ให้ผู้เข้าอบรมสามารถนำไปปฏิบัติได้)

1. ความเข้าใจในระบบมาตรฐานที่เกี่ยวข้อง
2. การพิจารณาเนื้อหาตามเอกสาร ISO 27001 (ISMS Requirement)
3. กระบวนการในการ Implement ISMS
4. การวิเคราะห์ความเสี่ยง
5. การประเมินความเสี่ยง
6. แนวทางการจัดการความเสี่ยง
7. การจัดทำเอกสารต่าง ๆ และการจัดการเอกสาร
8. การ Apply : PDCA กับ การบริหารจัดการความปลอดภัยระบบสารสนเทศ (ISMS)

การที่เนื้อหาในหลักสูตรไม่ได้ระบุถึง การประยุกต์สำหรับ SMEs ตรง ๆ นั้น เนื่องจาก Business Environment & Requirements ของแต่ละองค์กรมีความแตกต่างกัน ดังนั้น การนำระบบ ISMS ตามมาตรฐาน ISO 27001 ไป implement ในองค์กร ก็จะต้องดำเนินขั้นตอนตาม Framework หลักของการ Implement รวมถึงการพิจารณาเอกสาร Guideline / Requirement ต่าง ๆ ซึ่งไม่สามารถลดทอนได้ตามขนาดขององค์กร หากแต่การพิจารณา Control ต่าง ๆ ที่กำหนดไว้ใน ISO 27001 นั้น สามารถนำไปพิจารณาปรับใช้ตามขอบเขตความต้องการ และความเหมาะสมตามสภาพแวดล้อมขององค์กรที่จะนำ ISMS ไปใช้ได้ ซึ่งจุดมุ่งหมายของการทำ ISMS ตามมาตรฐาน ISO 27001 ก็เพื่อให้องค์กรนั้นเกิดการบริหารจัดการด้านความปลอดภัยอย่างเป็นระบบและครบวงจร สามารถพัฒนาปรับปรุงได้อย่างต่อเนื่องตามสภาพแวดล้อมและปัจจัยการดำเนินธุรกิจที่เปลี่ยนแปลงไป

2.3 เนื้อหา/องค์ความรู้ที่ได้จากการศึกษาดูงานแต่ละแห่ง (ถ้ามี) พร้อมแนบภาพประกอบ

a) ข้อมูลเกี่ยวกับสถานที่ศึกษาดูงาน

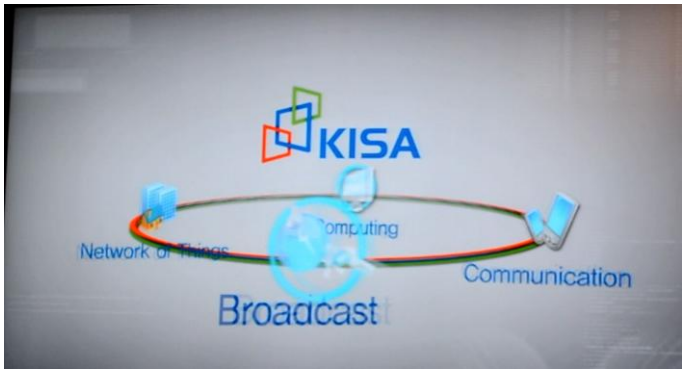
Korea Internet Security Agency (KISA) ได้เริ่มจัดตั้งขึ้นเมื่อ July 23rd 2009 โดยการรวมตัวกันจัดตั้งของ 3 องค์กร คือ Korea Information Security Agency(KISA), Korea IT International Cooperation Agency(KICA), National Internet Development Agency(NIDA) ทำหน้าที่หลักในการให้บริการสนับสนุนด้านความปลอดภัยของเทคโนโลยีเครือข่ายอินเตอร์เน็ต แห่งชาติเกาหลี มีความเพรียบพร้อมด้วยเครื่องมือในการติดตามตรวจสอบที่ทันสมัย ภายใต้การดำเนินการผ่านกิจกรรมสนับสนุนส่งเสริมในรูปแบบต่าง ๆ

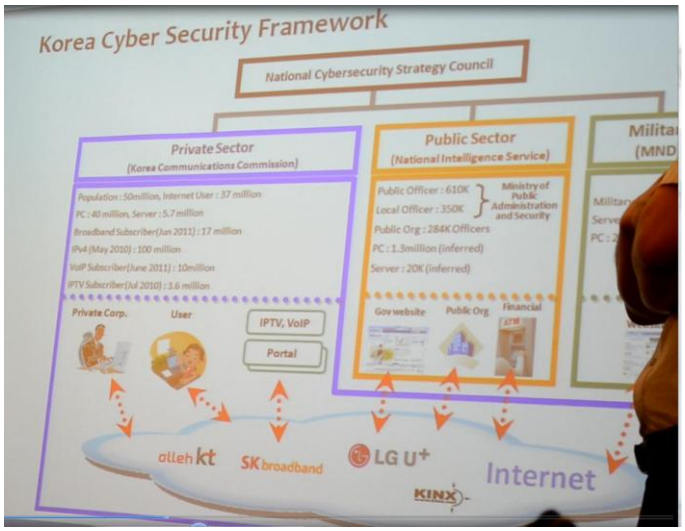
1) ทาง KISA มีการ Promote การใช้งาน Internet ในเกาหลี ผ่านกิจกรรมที่ได้จัดทำขึ้นในรูปแบบต่าง ๆ อาทิเช่น การสร้างวัฒนธรรมการใช้งานอินเตอร์เน็ตที่ดี ผ่านโครงการสนับสนุนทางการศึกษาแก่เด็กและเยาวชนในการเสริมสร้างจรรยาบรรณที่ดีในการใช้งานอินเตอร์เน็ต (Internet Ethics Education) รวมถึงการถ่ายทอดความรู้ให้กับครูอาจารย์ มีการจัดตั้งโครงการวัฒนธรรมอินเตอร์เน็ตชั้นสูง (Advanced Internet Culture) มีการจัดตั้งโครงการ Korea Internet Dream Star for Next Generation เพื่อส่งเสริมการใช้งานอินเตอร์เน็ตในภาคประชาชน
2) ทาง KISA มี Call Center กลางเพื่อให้บริการ Consult เกี่ยวกับการใช้งานอินเตอร์เน็ต ให้คำแนะนำในการใช้งาน รับแจ้งปัญหาที่พบในการใช้งาน และครอบคลุมเรื่องอื่น ๆ ที่เกี่ยวข้อง
3) มีระบบ Monitoring การใช้งานรายบุคคล โดยผ่าน i-Pin (Internet Personal Identification Number)

KISA มีกลยุทธ์สนับสนุน Global Market ประกอบด้วยบริการ 5 ด้านอันได้แก่ Broadband, IPTV, Digital Multimedia Broadcasting, Wireless Broadband Internet, Broadcasting Contents

ในการบริหารจัดการด้านความปลอดภัยเครือข่ายอินเตอร์เน็ตของประเทศเกาหลี แบ่งเป็น 3 ด้านหลัก ๆ (พิจารณาจาก Korea Cyber Security Framework) คือ Private Sector,

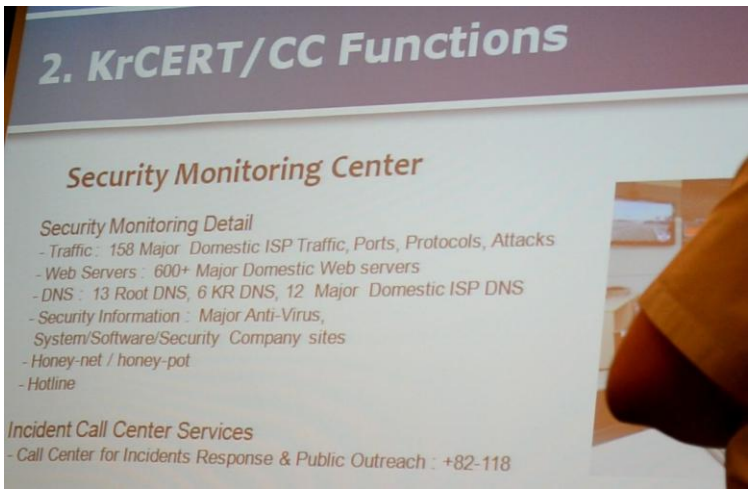
Public Sector และ Military Sector มีการกำหนด โครงสร้างความรับผิดชอบ การสื่อสาร เพื่อรองรับต่อกรณีการเกิด Crisis โดยมี KISA กำกับดูแล ในการกำกับดูแลด้านความปลอดภัยนั้น มีหน่วยงาน (Korea Internet Security Center - KISC) และ ทีมงานที่ทำหน้าที่ในการ Monitor การใช้งาน ปัญหา ภัยคุกคามที่เกิดขึ้นในการใช้งาน มีการแบ่งระดับความร้ายแรงของปัญหา และกำหนดขั้นตอนในการจัดการกับปัญหา มีการประยุกต์ทางโครงสร้าง (Network infrastructure) เรียกว่า HoneyNet เพื่อใช้ประโยชน์ในการจัดการกับปัญหาและเรียนรู้ภัยคุกคามในเครือข่าย เพื่อใช้ประโยชน์ในการจัดการแก้ไข และการป้องกัน

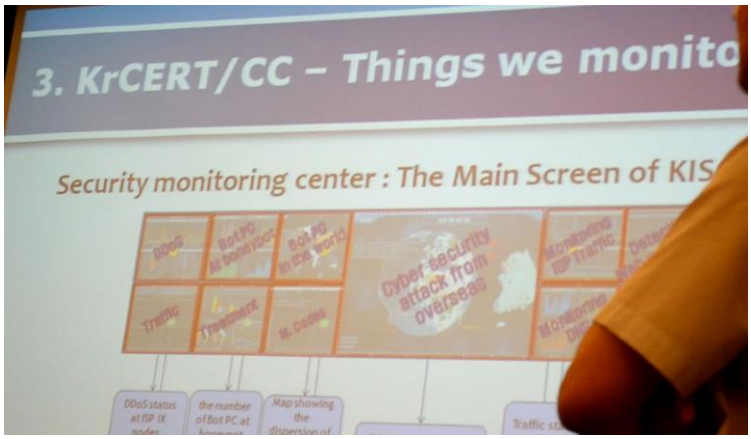


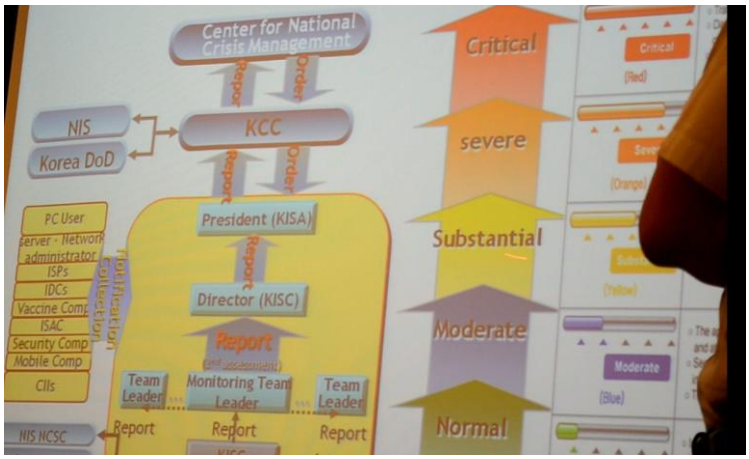

Korea Cyber Security Framework
National Cybersecurity Strategy Council
Private Sector
(Korea Communications Commission)
Public Sector
(National Intelligence Service)
Public Officer : 610K
Local Officer : 350K
Ministry of Public Administration and Security
Public Org : 284K Officers
PC : 1.3million (inferred)
Server : 20K (inferred)
Gov website
Public Org
Financial
Private Corp.
User
IPTV, VoIP
Portal
olleh kt
SK broadband
LG U+
KINX
Internet


1. Korea Cyber Security
Cyber Crisis Response Framework
President
National Center for Crisis Management
Ministry of National Defense
Defense Security Command
Military Area/each unit
National Intelligence Service
KNCERT/CC
Critical Infrastructures in Government/public sector
Korea Communications Commission
KrCERT/CC
Critical Infrastructures in private sector
The framework covers the public

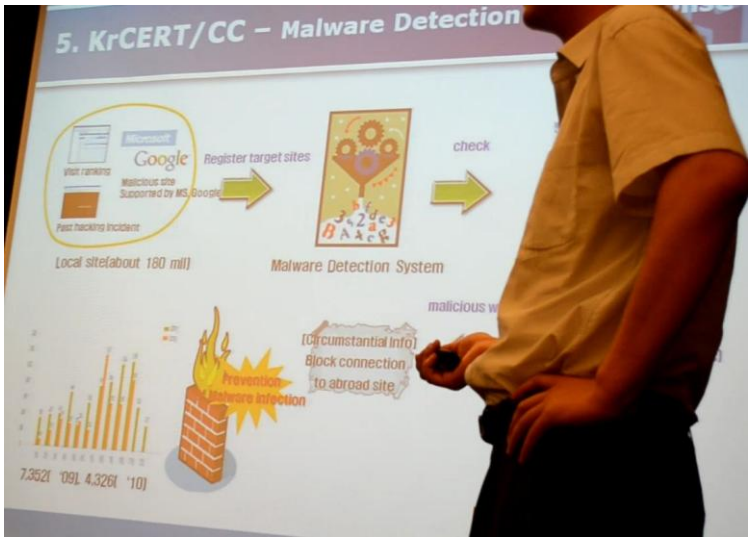
.

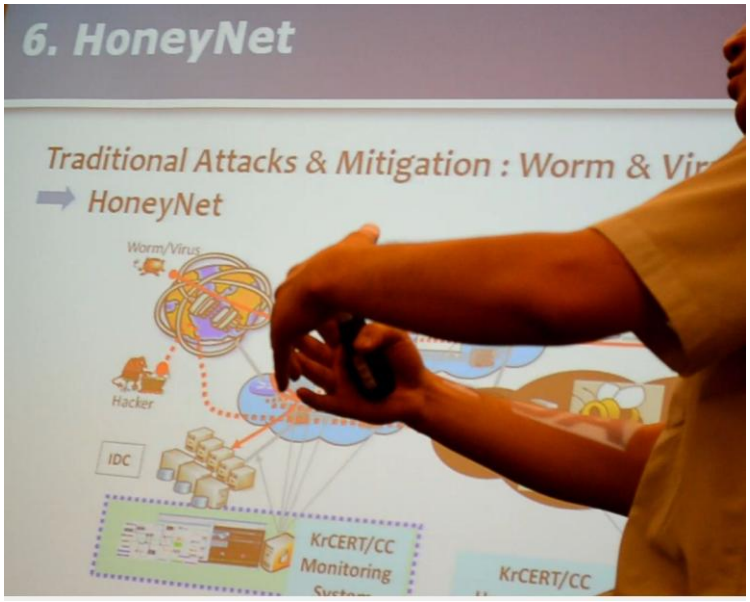

2. KrCERT/CC Functions
Security Monitoring Center
Security Monitoring Detail
- Traffic : 158 Major Domestic ISP Traffic, Ports, Protocols, Attacks
- Web Servers : 600+ Major Domestic Web servers
- DNS : 13 Root DNS, 6 KR DNS, 12 Major Domestic ISP DNS
- Security Information : Major Anti-Virus, System/Software/Security Company sites
- Honey-net / honey-pot
- Hotline
Incident Call Center Services
- Call Center for Incidents Response & Public Outreach : +82-118

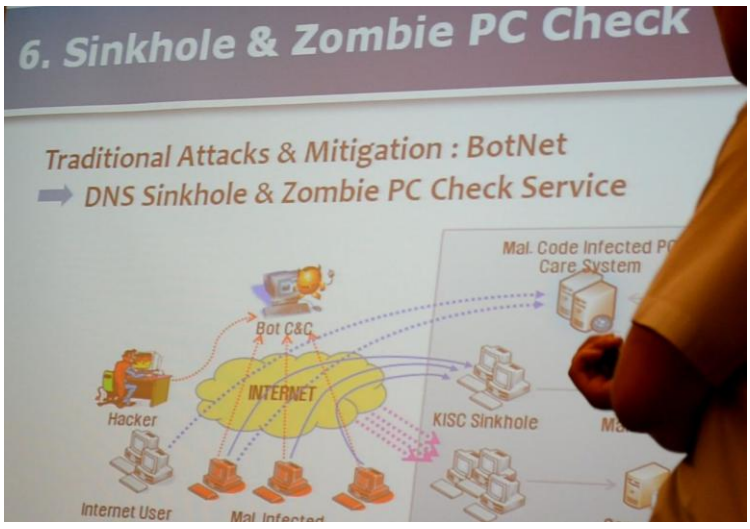

3. KrCERT/CC – Things we monito
Security monitoring center : The Main Screen of KIS
DDoS
Traffic
Cyber security attack from overseas
DDoS status at ISP IX
the number of Bot PC at
Map showing the

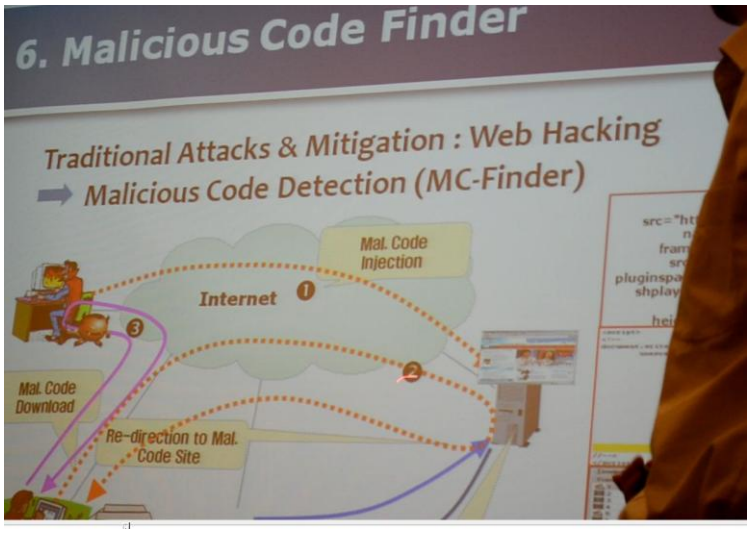

Center for National Crisis Management
NIS
Korea DoD
KCC
President (KISA)
Director (KISC)
Report
Team Leader
Monitoring Team Leader
Team Leader
Report
Report
Report
PC User
Server · Network administrator
ISPs
IDCs
Vaccine Comp
ISAC
Security Comp
Mobile Comp
CIIs
Notification
Collection
NIS NCSC
Critical
severe
Substantial
Moderate
Normal

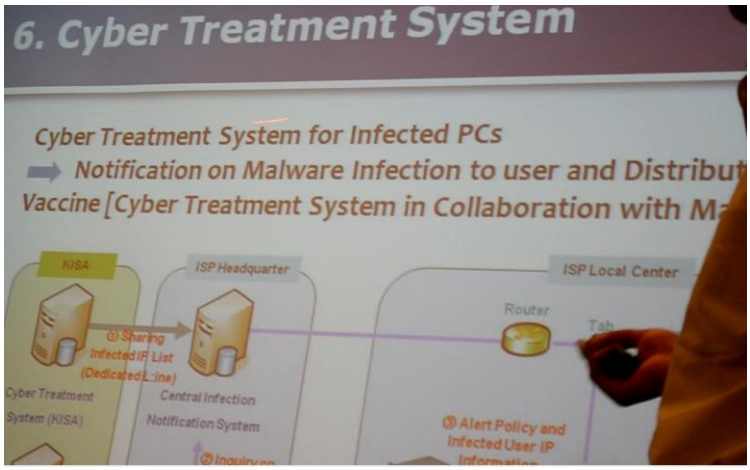

5. KrCERT/CC - Incident handling
Security monitoring center : KrCERT/CC's Tasks & Job
Detection
Analysis
Dissemination
kt
LG U+
ISP/ESM
Remote Ag
IDS/Firewi
Notice Mail
S/W,H/W
Worm Detection
Vuls.
Foreign Info.
KrCERT/CC
Mail
Web.
INCERT
FIRST
APCERT
Microsoft


5. KrCERT/CC – Malware Detection
Google
Register target sites
check
Local site(about 180 mil)
Malware Detection System
[Circumstantial Info]
Block connection
to abroad site
Prevention
Malware infection


6. HoneyNet
Traditional Attacks & Mitigation : Worm & Vir
HoneyNet
Worm/Virus
Hacker
IDC
KrCERT/CC
Monitoring
KrCERT/CC


6. Sinkhole & Zombie PC Check
Traditional Attacks & Mitigation : BotNet
DNS Sinkhole & Zombie PC Check Service
Bot C&C
INTERNET
Hacker
KISC Sinkhole
Internet User


6. Malicious Code Finder
Traditional Attacks & Mitigation : Web Hacking
Malicious Code Detection (MC-Finder)
Mal. Code Injection
Internet
Mal. Code Download
Re-direction to Mal. Code Site


6. Cyber Treatment System
Cyber Treatment System for Infected PCs
Notification on Malware Infection to user and Distribut
Vaccine [Cyber Treatment System in Collaboration with Ma
KISA
ISP Headquarter
ISP Local Center
Router
Cyber Treatment System (KISA)
Central Infection Notification System
Alert Policy and Infected User IP


6. DDoS Shelter
DDoS Shelter
to minimize damage for small and medium enterprise
not capable of handling DDoS attacks
Broadband
DNS Server
Request : Origin WWW
Response : 10.10.10.1
Response : DDoS Shelter IP
Botnet
Internet User
Alter Web Server Domain IP to DDoS Shelter IP for the attack period
Normal
Attack Traffic
DDoS Shelter

b) เนื้อหาความรู้ที่ได้รับจากการดูงาน

จากการศึกษาดูงานที่ KISA นี้ทำให้เห็นถึงวิสัยทัศน์ กลยุทธ์ ตลอดจนกระบวนการ การบริหารจัดการที่สอดรับและสนับสนุนเพื่อให้ได้มาซึ่ง ประสิทธิภาพของการให้บริการเทคโนโลยีเครือข่ายอินเตอร์เน็ต ของประเทศเกาหลี ซึ่งถูกแสดงให้เห็นตั้งแต่ระดับภาพรวมตลอดไปจนถึงกลไกการปฏิบัติการ มีการวางแผนอย่างเป็นขั้นตอน และดำเนินแผนงานสำคัญที่มีความเกี่ยวข้องกับภาระกิจหน้าที่ของ KISA ได้อย่างรอบด้าน กล่าวคือ

1) มีการจัดตั้งหน่วยงานกลาง หรือ องค์กรกลางขึ้นมา เพื่อทำหน้าที่ในการดูแลด้านความปลอดภัยของเครือข่ายอินเตอร์เน็ตของประเทศเกาหลี (Korea Information Security Agency – KISA)

2) มีการส่งเสริมภาคประชาชน ให้รู้และเข้าใจถึงการใช้งานอินเตอร์เน็ตอย่างปลอดภัย และมีจรรยาบรรณ โดยการมีโครงการร่วมกับสถาบันการศึกษาส่งเสริมด้านความรู้ทั้งระดับอาจารย์ นักเรียน และเยาวชนทั่วไป (เป็นการดำเนินการโดย KISA)

3) มีการจัดตั้ง KISA Academy เพื่อสร้างและพัฒนาบุคลากรให้มีความรู้ทางด้านเทคโนโลยีด้านเครือข่ายอินเตอร์เน็ต
4) มีการจัดตั้ง Call Center เพื่อรับเรื่องจากผู้ใช้บริการ และคอยให้บริการในทุก ๆ เรื่องที่เกี่ยวข้อง (รับแจ้งปัญหาที่พบในการใช้งาน ร้องเรียน ตลอดจนการขอรับคำแนะนำในการใช้งาน)
5) มีการวางโครงสร้างการประสานงาน การติดต่อสื่อสาร เพื่อรองรับ Crisis
6) มีการพัฒนาระบบบริหารจัดการ สนับสนุนการแก้ไขปัญหา การตรวจ ติดตาม การแจ้งเตือน รวมถึงการจัดระดับความร้ายแรงของปัญหา หรือภัยคุกคาม
7) มีการประยุกต์ใช้เทคโนโลยีเพื่อสนับสนุนด้านการจัดการกับปัญหา ทั้งเชิงรุก และเชิงรับ (เพิ่มเติมจากโครงสร้างเทคโนโลยีโดยพื้นฐาน)

จะเห็นได้ว่า การพัฒนาเพื่อสนับสนุนประสิทธิภาพในด้านการจัดการ ดูแลความปลอดภัยให้กับเครือข่ายอินเตอร์เน็ตของประเทศเกาหลี นอกจากจะดำเนินการพัฒนาด้านเทคโนโลยีที่เกี่ยวข้องแล้ว ยังพัฒนาด้านคนควบคู่ไปด้วย ทั้งด้านการให้ความรู้แก่ภาคประชาชน การสร้างจิตสำนึกและจรรยาบรรณที่ดีในการใช้งาน รวมถึงการพัฒนาบุคลากรให้มีความสามารถด้านเทคโนโลยีที่เกี่ยวข้อง ซึ่งจะเป็นปัจจัยสำคัญที่เกื้อหนุนให้ระบบเทคโนโลยีเครือข่ายอินเตอร์เน็ตของประเทศ มีความปลอดภัย สร้างความน่าเชื่อถือ ซึ่งจะเป็นประโยชน์ต่อผู้ใช้บริการ และนักลงทุน สะท้อนภาพลักษณ์ถึงความพร้อมของระบบเทคโนโลยีของประเทศ ที่จะให้บริการในการประกอบกิจกรรมต่าง ๆ ได้อย่างมั่นคง ปลอดภัย และมีประสิทธิภาพสูง

2.4 เนื้อหา/องค์ความรู้ที่ได้จากการเข้าร่วมกิจกรรมกลุ่ม (Group Discussion)

a) หากองค์กรจะนำระบบมาตรฐาน ISO 27000 ไปใช้ จำเป็นต้องได้รับการสนับสนุนจากผู้บริหารระดับสูงอย่างจริงจัง
b) กระบวนการหรือขั้นตอนดำเนินการเพื่อให้เกิดระบบบริหารจัดการด้านความปลอดภัยเริ่มต้นที่การจัดตั้งคณะทำงาน การให้ความรู้ความเข้าใจเกี่ยวกับระบบบริหารจัดการตามมาตรฐาน การวางแผนการดำเนินงาน และการเตรียมการในขั้นตอนต่าง ๆ โดยมีแนวทางตาม Requirement ของระบบมาตรฐาน ISO 27001
c) Framework ของการดำเนินการตามมาตรฐาน ISO 27000 นั้นใช้ Framework PDCA (Deming Cycle) โดยเริ่มต้นตั้งแต่กระบวนการวางแผน การเตรียมการ ตลอดไปจนถึงการดำเนินการซึ่งกลายเป็นวงจรการดำเนินการตามระบบมาตรฐาน เพื่อให้เกิดการบริหารจัดการด้านความปลอดภัยที่มีความต่อเนื่องอย่างยั่งยืน
d) ขั้นการเตรียมการเพื่อจะ Implement ISMS ตามระบบมาตรฐาน ISO 27000
e) ได้มีโอกาสในการวิเคราะห์ความเสี่ยงจาก กรณีศึกษาของธุรกิจธนาคาร
f) ได้ทำการจำแนก Asset จากการพิจารณาเนื้อหาในกรณีศึกษา (Asset Categorization)
g) ได้ทำการประเมินความเสี่ยงจากกรณีศึกษา (Risk Assessment)
    1) การหาภัยคุกคามที่มีต่อ Information Asset (Threats)
    2) การหาจุดอ่อน หรือช่องโหว่ที่มีต่อ Information Asset (Vulnerability)
    3) การประเมินระดับความเสี่ยง / ความน่าจะเป็น (Probability)
    4) การประเมินระดับความร้ายแรงของผลกระทบที่จะเกิดโดยภาพรวม (Consequently)
    5) การประเมินระดับความร้ายแรงของผลกระทบจำแนกตาม Elements of Information Security (Confidential, Integrity, Availability)
    6) ทำการจัดลำดับความร้ายแรงของความเสี่ยง (Risk classification)
    7) ทำการกำหนดแนวทางรองรับความเสี่ยง (Risk treatment option ประกอบด้วย Reduce, Avoidance, Transfer และ Acceptance)
h) ได้ทำการเขียนโครงร่าง Policy

i) ได้ทำการเขียน Procedure โดยวิทยากรได้กำหนดให้แต่ละกลุ่มเขียน Procedure เพื่อการจัดการที่แตกต่างกัน (กลุ่มที่ร่วมทำกิจกรรมได้รับมอบหมายให้ทำ Backup Procedure)

ส่วนที่ 3 ประโยชน์ที่ได้รับจากการเข้าร่วมโครงการ

3.1 ประโยชน์ต่อตนเอง

3.1.1 ได้เข้าใจถึงความสำคัญของการมีระบบบริหารจัดการด้านความปลอดภัยข้อมูลสารสนเทศและทรัพย์สินที่เกี่ยวข้องที่มีความสำคัญต่อการดำเนินธุรกิจ

3.1.2 ได้เข้าใจถึง Requirement ตามมาตรฐาน ISO 27001

3.1.3 ได้เข้าใจถึงกระบวนการหรือขั้นตอนในการ implement และมีโอกาสได้ทำกิจกรรมกลุ่มในแต่ละขั้นตอน ทำให้เข้าใจถึงข้อสงสัย หรือประเด็นปัญหาที่เกิดขึ้น เมื่อต้องลงมือปฏิบัติจริง

3.1.4 สามารถนำความรู้ดังกล่าวมาใช้ประโยชน์ในการศึกษาเพิ่มเติม

3.2 ประโยชน์ต่อหน่วยงานต้นสังกัด

3.2.1 สามารถนำความรู้ที่ได้รับมา ถ่ายทอดให้ ทีมงานภายใน หรือหน่วยงานที่เกี่ยวข้องให้ทราบและเข้าใจถึงความสำคัญ การนำไปปรับใช้หรือปฏิบัติ

3.3 ประโยชน์ต่อสายงานหรือวงการในหัวข้อนั้นๆ

3.3.1 สามารถนำความรู้ที่ได้มาใช้ประโยชน์ในการวางแผน หรือกำหนดกรอบ Framework หรือ Roadmap ในการพัฒนาระบบเทคโนโลยีสารสนเทศขององค์กรเพิ่มเติม โดยทำให้เห็นว่านอกจากการพัฒนาระบบสารสนเทศที่มุ่งเน้นไปในด้านของการมีระบบเทคโนโลยีและสารสนเทศที่ดีมีประสิทธิภาพแล้ว ในมิติของการพัฒนาด้านการบริหารจัดการ ทั้งในแง่ของนโยบาย กระบวนการสนับสนุน และเครื่องมือสนับสนุนที่เกี่ยวข้องด้านความปลอดภัยข้อมูลสารสนเทศและทรัพย์สินที่เกี่ยวข้องอย่างมีนัยสำคัญนั้น ถือเป็นอีกมิติหนึ่งที่องค์กรควรให้ความสำคัญและส่งเสริมให้มีการพัฒนาควบคู่กันไป กับการพัฒนาระบบเทคโนโลยีสารสนเทศขององค์กร

3.4 กิจกรรมการขยายผลที่ได้ดำเนินการภายใน 1 เดือนหลังเข้าร่วมโครงการ

3.4.1 กิจกรรม เช่น การฝึกอบรมภายในหน่วยงาน การบรรยายในทีมงาน บทความที่ลง newsletter เป็นต้น

3.4.1.1 จัดประชุมทีมงานภายใน IT ที่เกี่ยวข้อง เพื่อสื่อสาร และ ถ่ายทอดประสบการณ์ เพื่อให้ทีมงานภายในเห็นความสำคัญ และทิศทางที่จะต้องมุ่งไป ตามแผนพัฒนา (Roadmap) ภายหลังนำความรู้ที่ได้รับมา พิจารณาทบทวนโครงสร้างของแผนพัฒนาเดิม (Roadmap เดิม) โดยปรับเพิ่มเติม แผนกิจกรรมหลักที่ต้องดำเนินการ จัดลำดับ และนำไปใช้เป็นแนวทางในการกำหนดแผนงานประจำปีที่เกี่ยวข้อง

3.4.2 สรุปรายละเอียดกิจกรรม พร้อมภาพถ่าย และใบลงชื่อผู้ร่วมกิจกรรม

3.5 กิจกรรมการขยายผลที่จะดำเนินการภายใน 6 เดือนหลังเข้าร่วมโครงการ

3.5.1 แผนงานกิจกรรมที่จะดำเนินการ

3.5.2 ส่งเอกสารสรุปกิจกรรมดังข้อ 3.4.2 เมื่อเสร็จสิ้นกิจกรรมให้ส่วนวิเทศสัมพันธ์

ส่วนที่ 4 เอกสารแนบ

4.1 กำหนดการฉบับล่าสุด (Program)

4.2 เอกสารประกอบการประชุม/สัมมนา (Training Materials)

4.3 ประวัติโดยสังเขปของวิทยากรบรรยาย (CV)

4.4 รายงานก่อนการเดินทาง (Country Paper-Thailand)

4.5 เอกสารนำเสนอผลงานหลังจากเข้าร่วมกิจกรรมกลุ่ม (Group Presentation)

หมายเหตุ 1. ตัวอักษรและขนาดของตัวอักษรที่ใช้ คือ Cordia New 14 pt.

2. รายงานการเข้าร่วมโครงการเอพีโอ ต้องจัดทำเป็นรายบุคคล และมีกำหนดจัดส่งภายในระยะเวลา 1 เดือน หลังจากเดินทางกลับจากการเข้าร่วมโครงการ