รผก. (ภายใน)
เลขที่ 1461
วันที่ 1/7/59
เวลา 15.01

เลขที่ 1011
DCS —
วันที่ 1 ก.ค. 59
เวลา 16:51

กผส.
เลขที่ 475
วันที่ 29 มิ.ย. 2559
เวลา 10.12 น.

ฝกท 12/20
29 มิ.ย. 2559

รายงานสรุปการฝึกอบรม/สัมมนาภายนอก ประจำปี 2559

เรียน รผบ. ผ่าน ผชก.(นายสุชินฯ) รผก.(CTO) ผอ.ฝกท. ผอ.กผส. 30 มิ.ย. 59

ฝทท.
เลขที่ 117
วันที่ 30 มิ.ย. 2559
เวลา 11.08 น.

1152
06 ก.ค. 2559
15.05 น.

1. ข้าพเจ้า (~~นาย/นาง~~/นางสาว) [illegible] โอฬารผล
ตำแหน่ง หน.มผ. แผนก มผ. กอง กผส.
ฝ่าย ฝกท. และ (~~นาย/นาง~~/นางสาว) สิริพร [illegible]
ตำแหน่ง หน.ศค. รก.ผอ.กศค. แผนก ศค. กอง กศค.
ฝ่าย ฝกท. ได้รับอนุมัติให้ไปเข้าร่วมการฝึกอบรม/สัมมนาหลักสูตร/เรื่อง Become An IS Audit Professional จัดโดย บ.เอซิส โปรเฟสชั่นแนล จำกัด
ระหว่างวันที่ 13-15 มิถุนายน 2559 สถานที่จัด บ.เอซิส โปรเฟสชั่นแนล จำกัด
ค่าลงทะเบียนอบรม/สัมมนา ☑ เสียค่าใช้จ่าย 38,000 บาท ☐ ไม่เสียค่าใช้จ่าย

1803
1/07/59
14.44 น.

2. ข้าพเจ้าขอรายงานสรุปการฝึกอบรม/สัมมนา ดังนี้

2.1 สรุปรายละเอียดเนื้อหาของหลักสูตร (ไม่เขียนเฉพาะหัวข้อ ควรมีการบรรยายสรุป เพื่อถ่ายทอดองค์ความรู้ต่อไป)

รายละเอียดตามเอกสารแนบ

2.2 ข้อเสนอแนะในการนำความรู้ตามหลักสูตร/เรื่องจากการฝึกอบรม/สัมมนาครั้งนี้ มาประยุกต์ใช้กับ องค์การ

- นำมาใช้ในการปรับปรุงกระบวนการทำงาน เพื่อให้มีความพร้อมในการรองรับการตรวจสอบจากภายนอก และเพื่อให้กระบวนการทำงานมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น
- นำมาปรับปรุงกระบวนการด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

2.3 ความคิดเห็นเกี่ยวกับการฝึกอบรม/สัมมนา

(1) หลักสูตรที่ฝึกอบรม/สัมมนาครั้งนี้ช่วยเพิ่มพูนความรู้ของท่าน
☑ มาก ☐ ปานกลาง ☐ น้อย

เลขที่ 3525
วันที่ 06 ก.ค. 2559
เวลา 09.12

(2) ท่านคิดว่าการฝึกอบรม/สัมมนาครั้งนี้มีประโยชน์กับตัวท่านและองค์การเพียงใด

☑ มาก ☐ ปานกลาง ☐ น้อย

ระบุเหตุผล (ตอบได้มากกว่า 1 ข้อ)

☑ เนื้อหาเกี่ยวข้องโดยตรงและสามารถนำไปใช้กับการปฏิบัติงานได้อย่างดี
☐ เนื้อหาไม่เกี่ยวข้องกับการปฏิบัติงาน
☑ เป็นความรู้เสริม และมีประโยชน์ในการปฏิบัติงาน
☑ ได้แลกเปลี่ยนประสบการณ์กับบุคคลนอกองค์การ
☑ วิทยากรมีความรู้ ความสามารถ และประสบการณ์ ในการบรรยายเป็นอย่างดี
☐ เนื้อหาการอบรมไม่ตรงกับหัวข้อการบรรยาย
☐ อื่น ๆ .....

3. วิทยากรที่ให้ความรู้ในหลักสูตรนี้ ได้แก่

ชื่อ-สกุล	จากสถาบัน/หน่วยงาน	ระดับความสามารถของวิทยากร		
3.1 [illegible]	บ.เอชิโน ไมโครฟิน จำกัด	☑ ดีมาก	☐ ดี	☐ พอใช้
3.2	.....	☐ ดีมาก	☐ ดี	☐ พอใช้
3.3	.....	☐ ดีมาก	☐ ดี	☐ พอใช้

4. ข้อเสนอแนะในการส่งพนักงานเข้ารับการฝึกอบรม/สัมมนาตามหลักสูตร/เรื่องนี้สำหรับครั้งต่อไป

.....

.....

จึงเรียนมาเพื่อโปรดทราบ

[illegible] 5/7/59
[illegible] รองผู้ว่าการ [illegible]
[illegible] 5/7/59
รผบ.

ลงชื่อ .....
(นายสกลสิริพร ภัทรเลิศวิกุล)
ตำแหน่ง หน.สกล. จก.ผอ.กสก.
วันที่ 6 กรกฎาคม 2559

ลงชื่อ .....
(นายธวัชชัย โอฬารินคุณ)
ตำแหน่ง หน.มพ.
วันที่ 6 กรกฎาคม 2559

หมายเหตุ [illegible]

1. การส่งรายงานสรุปผลการฝึกอบรม/สัมมนา ควรสรุปรายละเอียดเนื้อหาหลักสูตรผ่านผู้บังคับบัญชาในสังกัดของตนเอง และนำเสนอเรียนถึง รผบ. (พร้อมแนบเอกสารประกอบการอบรมด้วย) 6-7-59

2. กรณีมีเอกสารการฝึกอบรมหรือใบประกาศนียบัตร ใบรับรอง กรุณาถ่ายสำเนาเอกสารดังกล่าว เพื่อ ฝทบ. จะได้บันทึกประวัติการฝึกอบรม

3. เมื่อ รผบ. พิจารณาเรื่องรายงานการฝึกอบรมภายนอกเรียบร้อยแล้ว กรุณาส่งเรื่องดังกล่าวไปที่ พบ.กพร.ฝทบ. เพื่อ ฝทบ.จะได้ดำเนินการลงประวัติฝึกอบรมต่อไป

4. สามารถดาวน์โหลดแบบฟอร์มได้ที่ หัวข้อข่าวทรัพยากรบุคคล หน้าแรกระบบงานสารสนเทศ รฟม. (INTRANET)

5. สอบถามข้อมูลเพิ่มเติมได้ที่ แผนกพัฒนาทรัพยากรบุคคล กองพัฒนาบุคลากรและระบบงาน ฝ่ายทรัพยากรบุคคล คุณรัชกร โทร 1224 คุณอัจฉรา โทร 1213 คุณมณฑิชา โทร 1275 และคุณจิตปภา โทร 1214

[illegible] 7/7/59

รายงานการฝึกอบรม

หลักสูตร Become An IS Audit Professional (ISAU)

1. <u>หน่วยงานที่ให้ใบรับรองและให้ความรู้เกี่ยวกับหลักการตรวจสอบและควบคุมระบบสารสนเทศ</u> คือ ISACA (Information Systems Audit and Control Association) www.isaca.org

2. **มาตรฐานที่เกี่ยวข้องกับการตรวจสอบและควบคุมระบบสารสนเทศของ ISACA** แบ่งเป็นหมวดได้ดังนี้

    2.1 หมวด General Standards ประกอบด้วย

        1001 Audit Charter

        1002 Organisational Independence

        1003 Professional Independence

        1004 Reasonable Expectation

        1005 Due Professional Care

        1006 Proficiency

        1007 Assertions

        1008 Criteria

    2.2 หมวด Performance Standards

        1201 Engagement Planning

        1202 Risk Assessment in Planning

        1203 Performance and Supervision

        1204 Materiality

        1205 Evidence

        1206 Using the Work of Other Experts

        1207 Irregularity and Illegal Acts

    2.3 หมวด Reporting Standards

        1401 Reporting

        1402 Follow-up Activities

3. **แนวปฏิบัติ (Guideline) ที่เกี่ยวข้องกับการตรวจสอบและควบคุมระบบสารสนเทศของ ISACA** แบ่งเป็นหมวดได้ดังนี้

    3.1 หมวด General Guidelines

        2001 Audit Charter

2002 Organisational Independence

2003 Professional Independence

2004 Reasonable Expectation

2005 Due Professional Care

2006 Proficiency

2007 Assertions

2008 Criteria

3.2 หมวด Performance Guidelines

2201 Engagement Planning

2202 Risk Assessment in Audit Planning

2203 Performance and Supervision

2204 Materiality

2205 Evidence

2206 Using the Work of Other Experts

2207 Irregularity and Illegal Acts

2208 Sampling

3.3 หมวด Reporting Guidelines

2401 Reporting

2402 Follow-up Activities

4. นิยามศัพท์ด้านการควบคุมและตรวจสอบระบบสารสนเทศ

4.1 Assertion คือ สิทธิของผู้ปฏิบัติ (Owner) หรือสิ่งที่ผู้ปฏิบัติยืนยันว่าได้ดำเนินการนั้นถูกต้อง (Completeness) ครบถ้วน

4.2 Audit Charter คือ บทบาท หน้าที่ของผู้ควบคุมหรือตรวจสอบระบบสารสนเทศหรือกฎบัตรซึ่งผู้ตรวจสอบจะสามารถตรวจสอบได้ตามหน้าที่เท่านั้น

4.3 Competence คือ ความรู้ความสามารถหรือทักษะของผู้ควบคุมหรือตรวจสอบระบบสารสนเทศซึ่งได้มาจากการเรียน (Education) การอบรม (Training) ประสบการณ์หรือทักษะต่าง ๆ (Experience and Skill) ที่ได้มาจากการปฏิบัติงาน

4.4 Criteria คือ หลักเกณฑ์การตรวจสอบ ตัวอย่างได้แก่ มาตรฐานสากล หรือ Framework ต่าง ๆ ได้แก่ Cobit หรือ ITIL เป็นต้น

4.5 Engagement คือ การที่ผู้ตรวจและผู้รับตรวจร่วมหารือและลงความเห็นตรงกัน (1 Job = 1 Engagement)

4.6 Independence คือ ผู้ตรวจต้องเป็นอิสระเชิงโครงสร้างไม่ขึ้นตรงกับตำแหน่งใด

4.7 Impairment คือ การที่ผู้ตรวจไม่สามารถดำเนินการตรวจสอบได้อย่างเต็มที่ เช่น การมีผลประโยชน์ทับซ้อน หรือการเกรงใจผู้รับตรวจ เป็นต้น

4.8 Materiality คือ การมีนัยสำคัญ เช่น รายการตรวจสอบแล้วพบว่ามีความเสี่ยงสูง เป็นต้น

4.9 Objectivity คือ การตรวจสอบอย่างตรงไปตรงมาโดยเปรียบเทียบกับ Criteria

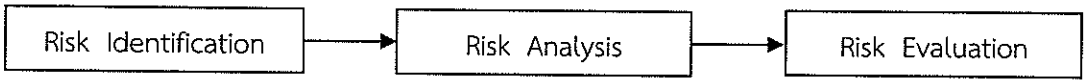
4.10 Opinion คือ การแสดงความเห็นในรายงาน (Report)

4.11 Professional Skepticism คือ ทักษะด้านความขี้สงสัย ความไม่เชื่อ ความระแวง ซึ่งผู้ตรวจสอบต้องนำไปใช้เมื่อผู้รับตรวจได้รายงานผลการปฏิบัติงานมา

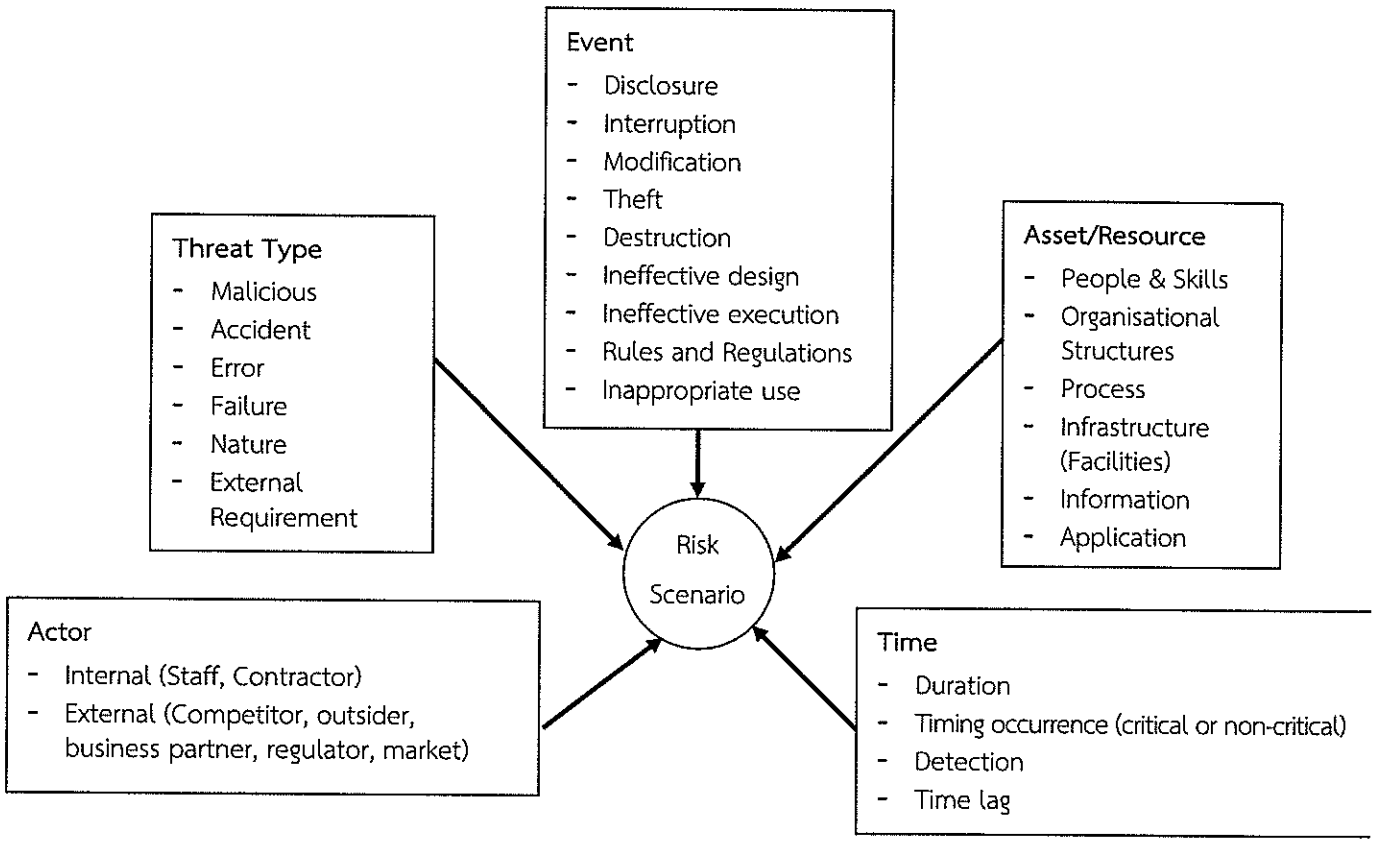
4.12 Proficiency คือ ความชำนาญ ความสามารถในการปฏิบัติหน้าที่

5. **การประเมินความเสี่ยง (Risk Assessment)** เพื่อประเมินความเสี่ยงและจัดลำดับความเสี่ยง และนำรายการที่มีความเสี่ยงสูงมาบรรจุใน Audit Program เพื่อตรวจสอบและหาแนวทางในการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

กระบวนการประเมินความเสี่ยง



การประเมินความเสี่ยงของระบบสารสนเทศต้องครอบคลุม ดังนี้



6. แนวทางเพื่อหาหลักฐาน (Evidences) จากหน่วยรับตรวจ

6.1 สอบถาม/สัมภาษณ์ ผู้ตรวจสอบต้องจัดเตรียมรายการคำถามให้ชัดเจน

6.2 สังเกตการณ์ ผู้ตรวจสอบต้องจัดทำรายการล่วงหน้าว่าต้องการสังเกตการณ์การดำเนินการใดบ้าง หรืออาจมีบางรายการที่ไม่ต้องแจ้งให้ทราบล่วงหน้า

6.3 ขอดูเอกสาร (Documentation Review) ผู้ตรวจสอบต้องจัดเตรียมรายการเอกสารที่ต้องการตรวจสอบ (Request For Information: RFI) ให้พร้อม

6.4 Re-performance คือการทดสอบในสภาวะแวดล้อมที่เหมือนจริง (Integrated Test Facilities: ITF)

6.5 Analytics คือการขอข้อมูลจากผู้รับตรวจไปทำการวิเคราะห์ เช่น การวิเคราะห์หาการฉ้อโกง (Fraud) หรือหาสาเหตุของการเกิดปัญหา เป็นต้น

7. การสุ่มตัวอย่าง (Sampling)

7.1 วัตถุประสงค์ของการสุ่มตัวอย่าง เพื่อตรวจสอบเนื้อหาและตรวจสอบการปฏิบัติว่าได้ดำเนินการตาม Compliance ที่กำหนดไว้หรือไม่ โดยการสุ่มตัวอย่างนั้นสามารถทำได้ทั้งแบบใช้สถิติและไม่ใช้สถิติ

7.1.1 การสุ่มแบบใช้สถิติ (Statistical sampling method) ได้แก่

7.1.1.1 การสุ่มอย่างง่าย (Simple random sampling) เช่น การจับสลาก หรือการใช้ตารางเลขสุ่ม เป็นต้น

7.1.1.2 การสุ่มอย่างเป็นระบบ (Systematic random sampling) คือการเลือกตัวอย่างหรือตัวแทนจำนวน n หน่วยจากประชากรขนาด N หน่วย โดยที่แต่ละหน่วยมีโอกาสหรือความน่าจะเป็นที่จะถูกเลือกมาเป็นตัวอย่างเท่ากัน

7.1.1.3 การเลือกตัวอย่างแบบแบ่งชั้น (Stratified Sampling) การเลือกตัวอย่างวิธีนี้ ตัวอย่างจะถูกแบ่งออกเป็นกลุ่มตามลักษณะอย่างใดอย่างหนึ่งโดยไม่ให้มีหน่วยซ้ำกัน เช่น แบ่งตามเพศ หรืออายุ เป็นต้น

7.1.2 การสุ่มแบบไม่ใช้สถิติ (Non-statistical sampling methods) ได้แก่

7.1.2.1 การสุ่มแบบบังเอิญ (Haphazard Sampling) การคัดเลือกตัวอย่างโดยไม่มีการใช้กระบวนการสุ่มหรือไม่มีหลักการในการสุ่ม

7.1.2.2 การเลือกตัวอย่างแบบตัดสินใจเอง (Judgmental Sampling)

7.2 ขนาดของตัวอย่างต้องมีความเพียงพอและมีประสิทธิผล

8. **วัตถุประสงค์ของการควบคุมสารสนเทศ (Control Objective)**

8.1 How เพื่อให้ทราบว่าทำอย่างไร

8.2 Who เพื่อให้ทราบว่าใครเป็นคนดำเนินการ

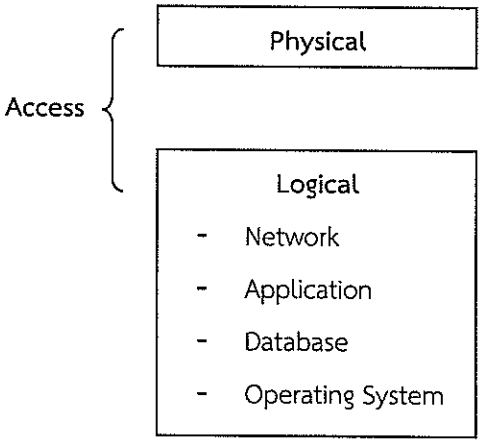
8.3 When เพื่อให้ทราบว่าดำเนินการเมื่อไหร่ เช่น เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เป็นต้น

8.4 Evidences หลักฐานที่ดำเนินการคืออะไรโดยเปรียบเทียบกับ Audit Criteria เพื่อจะได้ผลลัพธ์คือสิ่งที่ตรวจพบ (Findings)

9. **การควบคุมสารสนเทศ** แบ่งเป็น 2 ด้าน ดังนี้

9.1 General Control คือ การควบคุมทั่วไปเป็นการควบคุมที่อาศัยนโยบาย และระเบียบปฏิบัติงาน เป็นต้น

9.2 Application Control คือ การควบคุมภายในเฉพาะงานที่สร้างไว้ภายในระบบงานคอมพิวเตอร์ เช่น การควบคุมการให้สิทธิในการเข้าใช้งานระบบ หรือการควบคุมการป้อนข้อมูลลงในระบบ เป็นต้น



10. **ISACA ได้แบ่งการตรวจสอบและควบคุมสารสนเทศไว้ 4 ระดับ** ดังนี้

10.1 <u>ระดับ Network</u> แบ่งการตรวจสอบออกเป็น 2 ด้าน ดังนี้

10.1.1 Network Security Design คือดูการออกแบบด้านการรักษาความมั่นคงปลอดภัย ประกอบด้วย

10.1.1.1 การประเมินความเสี่ยงของระบบการรักษาความมั่นคงปลอดภัย

10.1.1.2 การกำหนดนโยบาย (Policy)

10.1.1.3 การกำหนด Trust Zone

10.1.1.4 การ Hardened System เช่น สิ่งที่ Default มากับเครื่องคอมพิวเตอร์หรือระบบให้ดำเนินการปรับเปลี่ยนทั้งหมด เช่น User หรือ Password เป็นต้น

10.1.2 Security Component ประกอบด้วย

10.1.2.1 Router

10.1.2.2 Switch

10.1.2.3 Firewall

10.1.2.4 Remote Access (VPN)

10.1.2.5 Remote Access (Dial Up)

10.1.2.6 Wireless Networking

10.1.2.7 IPS, IDS

10.1.2.8 Network Security Assessment สามารถดำเนินการได้ ดังนี้

10.1.2.8.1 ทดสอบโดยบุคคลภายในองค์กร

10.1.2.8.2 ทดสอบโดยบุคคลภายนอกองค์กร

10.2 ระดับ Application แบ่งการตรวจสอบออกเป็น 6 ด้าน ดังนี้

10.2.1 Source document design คือ การจัดเตรียมเอกสารที่เกี่ยวข้องกับการออกแบบเพื่อให้สามารถเก็บข้อมูลได้อย่างถูกต้อง เช่น แบบฟอร์มการกรอกข้อมูลต่าง ๆ ต้องออกแบบมาเป็นลิสต์หรือเป็นรายการให้ผู้ใช้เลือกโดยที่ผู้ใช้งานกรอกข้อมูลเองน้อยที่สุด เป็นต้น เพื่อป้องกันการกรอกข้อมูลที่ผิดพลาดหรือลดความผิดพลาดให้น้อยลง

10.2.2 Source data procedures การตรวจสอบคู่มือหรือขั้นตอนปฏิบัติว่าการใช้งานระบบเป็นไปตามที่ได้กำหนดไว้ตามคู่มือหรือไม่ (อาจใช้วิธีสังเกตการณ์)

10.2.3 Data entry authorization คือตรวจสอบรายการสิทธิว่าใครมีสิทธิในการเข้าใจระบบหรือมีสิทธิในการอนุมัติบ้าง เช่น ธนาคารจะมีตัวอย่างลายมือชื่อของลูกค้าเก็บไว้เพื่อเทียบกับลายมือชื่อของลูกค้า

10.2.4 Transaction identifier คือการกำหนดให้หมายเลขเอกสารหรือหมายเลข Transaction ไม่ซ้ำกันเพื่อป้องกันความผิดพลาด

10.2.5 Data editing การกำหนดสิทธิการเข้าถึงข้อมูลว่าใครสามารถดำเนินการอะไรกับข้อมูลได้บ้าง เช่น การป้อนข้อมูล การแก้ไขข้อมูล การอนุมัติหรือยกเลิกรายการข้อมูล เป็นต้น

10.2.6 Processing Integrity คือ การตรวจสอบความถูกต้องของข้อมูล เช่น จำนวน Transactions ของระบบ หรือจำนวนเงินตามช่วงเวลา เป็นต้น

10.3 ระดับ Database แบ่งการตรวจสอบเป็น 6 ด้าน ดังนี้

10.3.1 Access and Authorized

10.3.2 Security Process and Monitoring

10.3.3 Backup and Recovery

10.3.4 Encryption

10.3.5 Trust and Relationship

10.3.6 Network and Security

10.4 ระดับ Operating System แบ่งการตรวจสอบออกเป็น 5 ด้าน ดังนี้

10.4.1 การให้สิทธิใช้งาน System Folders, Program Folders และ Data Folders

10.4.2 HPID (High Privilege ID), ID คือ ผู้มีสิทธิสูงสุดในระบบปฏิบัติการหรือ ID ของ Administrator ซึ่งจะต้องมีการทบทวนสิทธิหรือตรวจสอบการใช้งาน (Review) ว่า HPID หรือ ID ได้มีการดำเนินการอะไรในระบบปฏิบัติการไปบ้าง

10.4.3 Log ต้องมีการทบทวน (Review)

10.4.4 General System Setting

10.4.5 Password Setting

11. บทสรุป

สิ่งที่นักตรวจสอบจะต้องเรียนรู้เพื่อให้สามารถตรวจสอบได้อย่างมีประสิทธิภาพและประสิทธิผล มีดังนี้

11.1 ต้องมีความรู้เกี่ยวกับ Information System Standards and Guidelines

11.2 Approach มี 2 แบบ คือ เกิดปัญหาแล้วค่อยตรวจสอบหาสาเหตุที่แท้จริง (Root cause) หรือ ตรวจสอบก่อนเพื่อป้องกันการเกิดปัญหา ทั้งนี้ การตรวจสอบนั้นจะต้องใช้ Compliance ต่าง ๆ มาประกอบการพิจารณา เช่น กฎกระทรวง กฎหมาย นโยบายฯ หรือมาตรฐานสากลต่าง ๆ พร้อมทั้งวิเคราะห์ความเสี่ยงเพื่อนำมาบริหารจัดการให้อยู่ในระดับที่ยอมรับได้

11.3 Professional Skepticism คือ การมีทักษะด้านการช่างสังเกต ช่างสงสัย

11.4 Audit Criteria ผู้ตรวจสอบต้องมีความรู้เกี่ยวกับเงื่อนไขที่นำมาใช้ในการตรวจสอบให้มากที่สุด เช่น Good practice ต่าง ๆ เป็นต้น

11.5 Practical Recommendation คือ มีความสามารถในการหาสาเหตุของปัญหา และหาแนวทางเพื่อปรับปรุงแก้ไข รวมทั้งสามารถโน้มน้าวให้หน่วยรับตรวจทำตามข้อแนะนำ

12. เอกสารที่ใช้ในการดำเนินการตรวจสอบ แสดงรายละเอียดตามภาคผนวก

ภาคผนวก

Audit Plan (Long-term)

#	Audit Area	Owner	Risk						Timeline												Team
									Y1				Y2				Y3				
			F1	F2	F3	F4	F5	Total	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
1	IT Strategic Management	IT Strategy	M	M	M	M	M	M		√												
2	IT Risk Management	Risk Management	H	H	H	H	H	H			√				√				√			
3	Systems Development and Project Management	PMO	M	L	L	H	M	M	√													
4	Change Management	IT Operation	H	H	M	M	H	H		√				√						√			Audit Team-A
5	Business Continuity Management	IT Strategy	M	M	L	L	H	M									√					
6	Generic Application Control	Head of Business	M	M	M	M	M	M								√						
7	UNIX/LINUX Operating System Security	IT Operation	H	H	M	L	L	M							√							
8	Windows Active Directory	IT Operation	H	H	M	L	L	M						√								
9	Microsoft SQL Server Database	IT Operation	H	H	M	L	L	M					√									
10	Oracle Database	IT Operation	H	H	M	L	L	M				√										
11	Network Perimeter Security	IT Infrastructure	H	H	M	L	L	M			√											
12	Cloud Computing Management	IT Operation	M	M	L	L	L	L							√							

Audit Plan (Short-term)

#	Audit Area	Owner	Risk						Timeline												Team	Audit Focus
									Y1													
			F1	F2	F3	F4	F5	Total	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12		
1	IT Strategic Management	IT Strategy	M	M	M	M	M	M				√										
2	IT Risk Management	Risk Management	H	H	H	H	H	H							√							
3	Systems Development and Project Management	PMO	M	L	L	H	M	M		√												
4	Change Management	IT Operation	H	H	M	M	H	H					√								Audit Team-A	Security purpose
5	Oracle Database	IT Operation	H	H	M	L	L	M											√			
6	Network Perimeter Security	IT Infrastructure	H	H	M	L	L	M								√						

Detailed Audit Plan

Audit Area:	Change Management	Risk Level:	High	Audtee:	IT Operation
Audit Focus:	Security purpose of change management process (program change)				
Objective:	ตรวจสอบกระบวนการ Change management ของฝ่าย IT ว่ามีการควบคุมที่สำคัญ ได้แก่ Assess change, Authorize change และ Coordinate change				
Scope:	Change ประเภท Program change ที่เกิดขึ้นระหว่าง 1 ม.ค. 59 ถึง 30 เม.ย. 59				
Timeline:	1-15 พ.ค. 59	Team Lead:	นายใจดี มีเงิน	Team Member:	นางสาวกุหลาบ สวยดี นางสาวชอุ่ม สง่างาม

Audit Program

Reference:	AP001
Audit Area:	Change Management Process
Objective:	ตรวจสอบกระบวนการ Change management ของฝ่าย IT ว่ามีการควบคุมที่สำคัญ ได้แก่ Assess change, Authorize change และ Coordinate change
Scope:	Change ประเภท Program change ที่เกิดขึ้นระหว่าง 1 ม.ค. 59 ถึง 30 เม.ย. 59

Risk	Control	Test of Control Design	Test of Operational Effectiveness	Finding	Reference
เกิด Negative impact ต่อBusiness, process, program, ...	Assess change	ได้รับเอกสาร RFC: 10001 สอบทานแล้วพบว่า มีการบันทึกผลกระทบ...	อ้างอิงไปยัง WP001	จากการสุ่มตรวจสอบพบว่า RFC 1 จาก 6 รายการ ไม่มีการวิเคราะห์ผลกระทบ, อนุมัติและสื่อสาร Raised issue in report	SUP001
	Authorize change	ได้รับเอกสาร RFC: 10001 สอบทานแล้วพบว่า มีการอนุมัติ...	อ้างอิงไปยัง WP001	จากการสุ่มตรวจสอบพบว่า RFC 1 จาก 6 รายการ ไม่มีการวิเคราะห์ผลกระทบ, อนุมัติและสื่อสาร Raised issue in report	SUP001
	Coordinate	ได้รับเอกสาร RFC: 10001 สอบทานแล้วพบว่า มีการสื่อสาร...	อ้างอิงไปยัง WP001	จากการสุ่มตรวจสอบพบว่า RFC 1 จาก 6 รายการ ไม่มีการวิเคราะห์ผลกระทบ, อนุมัติและสื่อสาร Raised issue in report	SUP001

SUP001

แนบตัวอย่างเอกสาร RFC: 10001 ที่ไป TOD มา

Audit Work Paper

Reference:	WP001					
Objective:	TOE ของกระบวนการ change mangement					
Sampling Parameter:	Pop = 20, Sampling 30% = 6		Items Selected:		1, 2, 6, 9, 11, 13	
Test of Operational Effectiveness:						
A: Assess change B: Approve change C: Coordinate change	#	Item Selected	A	B	C	Comment
	1	RFC1	√	√	√	
	2	RFC2	√	√	√	
	3	RFC6	X	X	X	แนบเอกสาร RFC6 อ้างอิง SUP002 *(Raised issue in report)*
	4	RFC9	√	√	√	
	5	RFC11	√	√	√	
	6	RFC13	√	√	√	
Conclusion:	จากการสุ่มตรวจสอบ RFC จำนวน 6 จาก 20 รายการ ระหว่างเดือน ... ถึง ... พบว่า ... รายละเอียดการสุ่มตรวจสอบ อ้างอิงไปยัง TOE_CM.xlsx					

Windows RAT-STATS

Statistical Software

Random Number Generator

Date:	14/6/2016	Time:	14:28
Audit:	TOE_CM		
Order	Value	Seed Number	Frame Size
6	1	52083.69	20
5	2		
3	6		
1	9		
2	11		
4	13		

SUP002

แนบเอกสาร RFC6 ที่มีประเด็น