แนวทางการปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศ

ต้นแบบ (Best Practice) ของหน่วยตรวจสอบภายใน สวพส.

1 วัตถุประสงค์

เพื่อให้การตรวจสอบด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีระบบ โปร่งใส และประเมินความเพียงพอของการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายในของ สวพส. ให้สอดคล้องกับกฎหมาย มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้อง

2 หลักการตรวจสอบ

Risk-Based IT Audit

- ความสำคัญของระบบ (Critical System)
- ความเสี่ยงของข้อมูล
- Cyber Risk
- ผลกระทบต่อพันธกิจ
- Compliance Risk
- Digital Government

3 กระบวนการตรวจสอบ (IT Audit Process)

1. Annual Risk Assessment
2. Engagement Planning
3. Understand IT Environment
4. IT Risk Assessment
5. Audit Program
6. Fieldwork
7. Data Analysis
8. Working Paper
9. Draft Report
10. Exit Meeting
11. Follow-up ผ่าน CMT

4 แนวทางการตรวจสอบ (Audit Methodology)

4.1 Document Review
ตรวจสอบเอกสารสำคัญ เช่น นโยบาย, ขั้นตอนการปฏิบัติงาน, คู่มือ, TOR, สัญญา, DRP, BCP, Risk Register, Minutes

4.2 Walkthrough
ให้ผู้ดูแลระบบอธิบาย Workflow ของกระบวนการสำคัญ เช่น Backup, Restore, User Creation, Incident

4.3 Interview
สัมภาษณ์ผู้เกี่ยวข้อง เช่น CIO, IT Manager, System Admin, DPO, เจ้าของระบบ (System Owner)

4.4 Observation
สังเกตสภาพแวดล้อมจริง เช่น Server Room, Network Room, CCTV, Backup Device

4.5 Configuration Review
ตรวจสอบการตั้งค่าระบบ เช่น Password Policy, Firewall, MFA, Antivirus, EDR

4.6 Sampling
สุ่มตรวจข้อมูล เช่น User Account, Admin Account, Change Request, Incident, Backup

5 การจัดทำ Audit Program

- Objective
- Scope
- Audit Procedure
- Sample
- Audit time (days)
- Working Paper
- Rules and Regulations

6 การรวบรวมหลักฐาน

รวบรวมหลักฐานจากหลายแหล่งอย่างเหมาะสมและเพียงพอ

- Document
- Interview
- Observation
- System Exidence

7 การสรุปผลการตรวจสอบ

ใช้รูปแบบ 5C

1. **Condition** (สภาพที่พบ)
2. **Criteria** (เกณฑ์อ้างอิง)
3. **Cause** (สาเหตุ)
4. **Consequence** (ผลกระทบ)
5. **Corrective Action** (ข้อเสนอแนะ)

กำหนด Risk Rating

High Medium Low OFI

8 การจัดลำดับความเสี่ยงตามผลการตรวจสอบ (Issue Risk Rating)

ความเสี่ยง	ระยะเวลาการปรับปรุง
ความเสี่ยงสูง (Relatively High Risk)	ภายใน 15 วัน
ความเสี่ยงปานกลาง (Medium Risk)	ภายใน 30 วัน (1 เดือน)
ความเสี่ยงต่ำ (Low Risk)	ภายใน 45 วัน
ความเห็นเพิ่มเติม (OFI : Opportunity for Improvement)	ดุลยพินิจของผู้บริหาร

9 Checklist

- PDPA
- Cybersecurity
- Digital Government
- IT General Controls (ITGC)
- Disaster Recovery Plan (DRP)
- Business Continuity Plan (BCP)

10 Knowledge Base

จัดเก็บและพัฒนาองค์ความรู้อย่างต่อเนื่อง

- Audit Program
- Checklist
- Best Finding
- Evidence
- Objective

เป็น IT Audit Repository ของหน่วยตรวจสอบภายใน

11 การติดตามผล (Follow-up)

ติดตามการดำเนินการผ่านระบบ CMT

- Responsible Person
- Due Date
- Status
- Progress
- Risk

จนกว่าประเด็นจะได้รับการแก้ไข

12 การประเมินคุณภาพ (Quality Assurance)

ทุกภารกิจต้องมีการ Review โดย Senior Auditor ก่อนออกรายงาน

- Risk
- Objective
- Finding
- Recommendation

13 การพัฒนาองค์ความรู้ (AAR)

หลังเสร็จสิ้นภารกิจทุกครั้ง จัดทำ After Action Review (AAR)

- สิ่งที่ทำได้ดี
- ปัญหาและอุปสรรค
- บทเรียนที่ได้รับ
- แนวทางปรับปรุง

บันทึกเข้าสู่คลังองค์ความรู้

14 ปัจจัยแห่งความสำเร็จ (Critical Success Factors)

1. ใช้การตรวจสอบแบบอิงความเสี่ยง (Risk-Based Audit)
2. ใช้มาตรฐานและเครื่องมือเดียวกันทั้งหน่วยตรวจสอบ
3. ใช้ Checklist และ Working Paper มาตรฐาน
4. อ้างอิงกฎหมายและมาตรฐานสากลในการประเมิน
5. ติดตามผลผ่านระบบ CMT จนกว่าประเด็นจะได้รับการแก้ไข
6. จัดทำ AAR และพัฒนาองค์ความรู้หลังทุกภารกิจ
7. ทบทวนและปรับปรุงคู่มือทุกปี ให้สอดคล้องกับกฎหมาย เทคโนโลยี และความเสี่ยงที่เปลี่ยนแปลง

ยกระดับการตรวจสอบด้านเทคโนโลยีสารสนเทศ สร้างคุณค่า เพิ่มความมั่นใจ ให้กับ สวพส. อย่างยั่งยืน