INTERNAL AUDIT

HIGHLAND RESEARCH AND DEVELOPMENT INSTITUTE (PUBLIC ORGANIZATION)

TRAINING MANUAL

Information Technology Audit

PREPARED BY
PEERAYA TECHARUNG

ONBOARDING 2026

คำนำ

เทคโนโลยีดิจิทัลได้เข้ามามีบทบาทสำคัญต่อการดำเนินงานของหน่วยงานภาครัฐในทุกมิติ ทั้งการบริหารจัดการองค์กร การให้บริการประชาชน การบริหารข้อมูล การเชื่อมโยงข้อมูลระหว่างหน่วยงาน ตลอดจนการสนับสนุนการตัดสินใจของผู้บริหาร การนำเทคโนโลยีสารสนเทศมาใช้จึงต้องดำเนินการภายใต้หลักธรรมาภิบาลที่ดี มีการบริหารจัดการความเสี่ยงอย่างเหมาะสม มีระบบการควบคุมภายในที่มีประสิทธิผล และสอดคล้องกับกฎหมาย มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 รวมทั้งมาตรฐานรัฐบาลดิจิทัลและมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ สำหรับสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) (สวพส.) เทคโนโลยีสารสนเทศเป็นกลไกสำคัญในการสนับสนุนพันธกิจขององค์กร ทั้งด้านการวิจัยและพัฒนาพื้นที่สูง การส่งเสริมอาชีพและพัฒนาคุณภาพชีวิตของเกษตรกรบนพื้นที่สูง การบริหารจัดการฐานข้อมูล การบริหารโครงการ การบริหารทรัพยากรองค์กร ตลอดจนการให้บริการข้อมูลและบริการดิจิทัลแก่ประชาชนและหน่วยงานภาครัฐ ดังนั้น การกำกับดูแลด้านเทคโนโลยีสารสนเทศ การรักษาความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล และการบริหารความต่อเนื่องของระบบสารสนเทศ จึงเป็นองค์ประกอบสำคัญที่ส่งผลต่อความสำเร็จในการดำเนินภารกิจขององค์กร

จากการดำเนินการตรวจสอบด้านเทคโนโลยีสารสนเทศของ สวพส. อย่างต่อเนื่อง พบว่ามีองค์ความรู้ เทคนิค วิธีการตรวจสอบ และแนวปฏิบัติที่มีประสิทธิผล ซึ่งสามารถรวบรวมและพัฒนาให้เป็นแนวทางสำหรับผู้ตรวจสอบภายใน ทั้งในด้านการวางแผนการตรวจสอบ การประเมินความเสี่ยง การจัดทำ Audit Program การรวบรวมและประเมินหลักฐาน การสรุปผลการตรวจสอบ การจัดทำข้อเสนอแนะ การติดตามผลการตรวจสอบ และการจัดการองค์ความรู้ เพื่อให้การปฏิบัติงานมีมาตรฐานเดียวกัน มีความครบถ้วน โปร่งใส สามารถสอบทานได้ และสร้างคุณค่าเพิ่มให้แก่องค์กร “แนวปฏิบัติการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit Guideline)” ฉบับนี้จัดทำขึ้นจากการศึกษาและประยุกต์ใช้หลักการตามมาตรฐานสากลด้านการตรวจสอบภายในและการกำกับดูแลเทคโนโลยีสารสนเทศ ประกอบกับบทเรียนจากการปฏิบัติงานตรวจสอบจริงของหน่วยตรวจสอบภายใน สวพส.

หน่วยตรวจสอบภายในคาดหวังว่าแนวปฏิบัติฉบับนี้จะเป็นเครื่องมือสำคัญในการพัฒนาศักยภาพของผู้ตรวจสอบภายในให้สามารถปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศได้อย่างมีมาตรฐาน เป็นระบบ และสอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยีและความเสี่ยงในยุคดิจิทัล อีกทั้งยังเป็นเครื่องมือสนับสนุนให้ผู้บริหารและหน่วยรับตรวจนำผลการตรวจสอบไปใช้ในการยกระดับการกำกับดูแล การบริหารความเสี่ยง การควบคุมภายใน และการพัฒนาระบบเทคโนโลยีสารสนเทศขององค์กรให้มีประสิทธิภาพ มั่นคงปลอดภัย โปร่งใส และสามารถสนับสนุนการบรรลุพันธกิจของ สวพส.

พีรญา เตชะรัง
เจ้าหน้าที่ตรวจสอบภายใน
30 กรกฎาคม 2569

สารบัญ

ส่วนที่ 1
บทนำ

- **ความเป็นมาของการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)**

ปัจจุบันเทคโนโลยีสารสนเทศ (Information Technology: IT) มีบทบาทสำคัญต่อการบริหารจัดการองค์กรภาครัฐในทุกมิติ ทั้งการบริหารงาน การให้บริการประชาชน การบริหารทรัพยากร การจัดเก็บและวิเคราะห์ข้อมูล การสื่อสารภายในองค์กร ตลอดจนการสนับสนุนการตัดสินใจของผู้บริหาร โดยเฉพาะภายใต้นโยบายการพัฒนารัฐบาลดิจิทัล (Digital Government) ที่มุ่งเน้นให้หน่วยงานของรัฐนำเทคโนโลยีดิจิทัลมาปรับเปลี่ยนรูปแบบการดำเนินงาน เพิ่มประสิทธิภาพการให้บริการ และสร้างความโปร่งใสในการบริหารราชการแผ่นดิน

สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) หรือ สวพส. เป็นหน่วยงานที่มีภารกิจในการวิจัย พัฒนา และถ่ายทอดองค์ความรู้เพื่อยกระดับคุณภาพชีวิตของประชาชนบนพื้นที่สูง โดยมีการนำระบบเทคโนโลยีสารสนเทศมาใช้สนับสนุนภารกิจในหลายด้าน เช่น ระบบสารสนเทศเพื่อการบริหารองค์กร (ERP) ระบบฐานข้อมูลเกษตรกร ระบบสารสนเทศภูมิศาสตร์ (GIS) เว็บไซต์และบริการอิเล็กทรอนิกส์ ระบบเครือข่ายคอมพิวเตอร์ ระบบศูนย์ข้อมูล (Data Center) ระบบสำรองข้อมูล (Backup System) รวมถึงการให้บริการข้อมูลแก่ประชาชนและหน่วยงานภายนอกผ่านช่องทางดิจิทัล การพึ่งพาระบบสารสนเทศเพิ่มขึ้นอย่างต่อเนื่อง ทำให้ความเสี่ยงด้านเทคโนโลยีสารสนเทศมีความซับซ้อนและส่งผลกระทบต่อการดำเนินงานขององค์กรมากขึ้น ไม่ว่าจะเป็นภัยคุกคามทางไซเบอร์ (Cyber Threats) การรั่วไหลของข้อมูลส่วนบุคคล การโจมตีด้วยมัลแวร์หรือแรนซัมแวร์ ความผิดพลาดของระบบ การหยุดชะงักของบริการ การบริหารจัดการสิทธิผู้ใช้งานที่ไม่เหมาะสม ตลอดจนความเสี่ยงจากผู้ให้บริการภายนอก (Third Party Risk) หากไม่มีการกำกับดูแล การบริหารความเสี่ยงและการควบคุมภายในที่เพียงพอ อาจส่งผลกระทบต่อการดำเนินภารกิจความเชื่อมั่นของผู้รับบริการ และภาพลักษณ์ขององค์กร

นอกจากนี้ หน่วยงานภาครัฐยังต้องปฏิบัติตามกฎหมายและมาตรฐานด้านดิจิทัลที่เกี่ยวข้อง เช่น พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ รวมถึงมาตรฐานรัฐบาลดิจิทัลและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งล้วนกำหนดให้หน่วยงานของรัฐต้องมีระบบการกำกับดูแล การควบคุม และการบริหารจัดการเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ ด้วยเหตุนี้การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit : IT Audit) จึงเป็นภารกิจสำคัญของหน่วยตรวจสอบภายในในการให้ความเชื่อมั่นว่าระบบการกำกับดูแล (Governance) การบริหารความเสี่ยง (Risk Management) และการควบคุมภายใน (Internal Control) ด้านเทคโนโลยีสารสนเทศขององค์กรมีความเพียงพอ เหมาะสม และสามารถสนับสนุนการบรรลุวัตถุประสงค์ขององค์กรได้อย่างมีประสิทธิภาพ

- **ความสำคัญของการตรวจสอบด้านเทคโนโลยีสารสนเทศ**

การตรวจสอบด้านเทคโนโลยีสารสนเทศ ไม่ได้มุ่งเน้นเพียงการตรวจสอบระบบคอมพิวเตอร์หรืออุปกรณ์สารสนเทศเท่านั้น แต่เป็นการประเมินความเพียงพอของระบบการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายในที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศทั้งองค์กร เพื่อให้มั่นใจว่าการใช้เทคโนโลยีสามารถสนับสนุนการดำเนินงานได้อย่างมั่นคง ปลอดภัย มีประสิทธิภาพ และเป็นไปตามกฎหมาย สำหรับ สวพส. การตรวจสอบด้านเทคโนโลยีสารสนเทศมีความสำคัญในประเด็นหลัก ดังนี้

1) สนับสนุนการบรรลุพันธกิจขององค์กร ระบบสารสนเทศเป็นกลไกสำคัญในการสนับสนุนการวิจัย การพัฒนาพื้นที่สูง การถ่ายทอดองค์ความรู้ และการให้บริการข้อมูลแก่เกษตรกร หน่วยงานภาครัฐ ภาคเอกชน และประชาชน การตรวจสอบ IT ช่วยประเมินว่าระบบเหล่านี้มีความพร้อมและสามารถสนับสนุนภารกิจขององค์กรได้อย่างต่อเนื่อง
2) เสริมสร้างธรรมาภิบาลด้านดิจิทัล (Digital Governance) การตรวจสอบช่วยประเมินโครงสร้างการกำกับดูแลด้านเทคโนโลยีสารสนเทศ ความชัดเจนของบทบาทหน้าที่ การกำหนดนโยบาย การติดตามผลการดำเนินงาน และการรายงานต่อผู้บริหาร ซึ่งเป็นองค์ประกอบสำคัญของการบริหารองค์กรดิจิทัล
3) ลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ การตรวจสอบช่วยระบุและประเมินความเสี่ยงที่อาจส่งผลกระทบต่อการดำเนินงาน เช่น ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การสูญหายของข้อมูล ความเสี่ยงจากผู้ให้บริการภายนอก ความเสี่ยงจากการเปลี่ยนแปลงระบบ หรือความเสี่ยงจากการกำหนดสิทธิผู้ใช้งานที่ไม่เหมาะสม พร้อมเสนอแนวทางควบคุมที่เหมาะสมกับบริบทของ สวพส.
4) เพิ่มความมั่นใจในการปฏิบัติตามกฎหมายและมาตรฐาน การตรวจสอบช่วยประเมินว่าการดำเนินงานของ สวพส. สอดคล้องกับกฎหมายที่เกี่ยวข้อง อาทิ PDPA กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ และมาตรฐานรัฐบาลดิจิทัล รวมทั้งแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ
5) ส่งเสริมการใช้ทรัพยากรด้านเทคโนโลยีอย่างคุ้มค่า การตรวจสอบครอบคลุมการบริหารโครงการด้านเทคโนโลยี การจัดซื้อจัดจ้างระบบสารสนเทศ การบริหารผู้ให้บริการภายนอก และการบริหารสินทรัพย์ด้านเทคโนโลยี เพื่อให้การใช้ทรัพยากรเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และเกิดความคุ้มค่าสูงสุด
6) เพิ่มความพร้อมในการรับมือเหตุการณ์ฉุกเฉิน การตรวจสอบประเมินความเหมาะสมของแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (IT Business Continuity Plan: IT BCP) แผนตอบสนองต่อเหตุการณ์ด้านไซเบอร์ (Cyber Incident Response Plan: CIRP) การกำหนดค่า RTO และ RPO ตลอดจนการซักซ้อมแผน เพื่อให้องค์กรสามารถดำเนินภารกิจได้อย่างต่อเนื่องเมื่อเกิดเหตุการณ์ไม่คาดคิด
7) สนับสนุนการตัดสินใจของผู้บริหาร รายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศให้ข้อมูลเชิงวิเคราะห์เกี่ยวกับความเสี่ยง จุดอ่อนของการควบคุมภายใน และผลกระทบที่อาจเกิดขึ้นต่อภารกิจขององค์กร ทำให้ผู้บริหารและคณะกรรมการตรวจสอบสามารถใช้ข้อมูลดังกล่าวประกอบการกำหนดนโยบาย การจัดสรรทรัพยากร และการบริหารความเสี่ยงเชิงกลยุทธ์ได้อย่างมีประสิทธิภาพ

- **บทบาทของหน่วยตรวจสอบภายในด้าน IT Audit**

หน่วยตรวจสอบภายในมีบทบาทในการให้ความเชื่อมั่นและให้ข้อเสนอแนะเชิงสร้างสรรค์ เพื่อพัฒนาระบบการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายในด้านเทคโนโลยีสารสนเทศ โดยมีบทบาทสำคัญ ได้แก่

1) ประเมินความเพียงพอของการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Governance)
2) ประเมินประสิทธิผลของการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)
3) ประเมินความเพียงพอของการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls)
4) ประเมินการปฏิบัติตามกฎหมาย มาตรฐาน และนโยบายที่เกี่ยวข้อง
5) ให้ข้อเสนอแนะที่สามารถลดความเสี่ยง เพิ่มประสิทธิภาพ และยกระดับการบริหารจัดการด้านดิจิทัลของ สวพส.
6) ติดตามผลการดำเนินการตามข้อเสนอแนะ เพื่อให้เกิดการปรับปรุงอย่างต่อเนื่องและสร้างผลกระทบเชิงระบบต่อองค์กร

- **บริบทของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) และความจำเป็นของการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit)**

สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) (สวพส.) จัดตั้งขึ้นเพื่อสืบสานพระราชปณิธานในการพัฒนาพื้นที่สูงตามแนวพระราชดำริ และเป็นหน่วยงานหลักในการดำเนินงานด้านการวิจัย การพัฒนาและการถ่ายทอดองค์ความรู้เพื่อยกระดับคุณภาพชีวิตของประชาชนบนพื้นที่สูง ควบคู่กับการอนุรักษ์ทรัพยากรธรรมชาติและสิ่งแวดล้อม ตลอดจนการสร้างความมั่นคงทางเศรษฐกิจ สังคม และสิ่งแวดล้อมอย่างยั่งยืน การดำเนินงานของ สวพส. มีลักษณะเป็นการบูรณาการองค์ความรู้ด้านการวิจัย การพัฒนาเกษตร การพัฒนาชุมชน การบริหารจัดการทรัพยากรธรรมชาติ และการให้บริการวิชาการ โดยเชื่อมโยงการดำเนินงานร่วมกับหน่วยงานภาครัฐ ภาคเอกชน สถาบันการศึกษา องค์กรปกครองส่วนท้องถิ่น ตลอดจนเครือข่ายเกษตรกรและชุมชนบนพื้นที่สูงในหลายจังหวัดของประเทศ

ภายใต้บริบทดังกล่าว เทคโนโลยีสารสนเทศจึงเป็นกลไกสำคัญในการสนับสนุนการดำเนินงานของ สวพส. ในทุกระดับ ตั้งแต่การบริหารจัดการภายในองค์กร การบริหารงบประมาณและทรัพยากร การจัดเก็บและวิเคราะห์ข้อมูล การติดตามผลโครงการ การให้บริการประชาชน ไปจนถึงการสนับสนุนการตัดสินใจเชิงนโยบายของผู้บริหาร ซึ่งการขับเคลื่อนองค์กรด้วยเทคโนโลยีดิจิทัล สวพส. มีการนำเทคโนโลยีดิจิทัลมาใช้สนับสนุนการดำเนินงานในหลายด้าน ได้แก่

1. ระบบสารสนเทศเพื่อการบริหารองค์กร ใช้สนับสนุนการบริหารงานภายในองค์กร เช่น
   - ระบบ ERP
   - ระบบบัญชีและการเงิน
   - ระบบงบประมาณ
   - ระบบพัสดุ
   - ระบบทรัพยากรบุคคล
   - ระบบสารบรรณอิเล็กทรอนิกส์
   - ระบบบริหารโครงการ

   ระบบดังกล่าวเป็นข้อมูลสำคัญขององค์กร หากเกิดความผิดพลาดหรือหยุดชะงักจะส่งผลกระทบต่อการบริหารงานโดยตรง

2. ระบบสารสนเทศเพื่อการวิจัยและพัฒนาพื้นที่สูง ประกอบด้วย
   - ฐานข้อมูลเกษตรกร
   - ฐานข้อมูลพื้นที่สูง
   - ระบบสารสนเทศภูมิศาสตร์ (GIS)
   - ฐานข้อมูลงานวิจัย
   - ฐานข้อมูลการผลิต และการตลาด

   ข้อมูลเหล่านี้เป็นฐานข้อมูลเชิงยุทธศาสตร์ขององค์กร ซึ่งจำเป็นต้องมีมาตรการรักษาความถูกต้อง ความครบถ้วน และความมั่นคงปลอดภัยของข้อมูล
3. ระบบบริการดิจิทัล (Digital Services) เช่น
   - เว็บไซต์องค์กร
   - ระบบรับเรื่องร้องเรียน
   - ระบบเผยแพร่องค์ความรู้

   ระบบดังกล่าวเป็นช่องทางการให้บริการแก่ประชาชนและผู้มีส่วนได้ส่วนเสีย จึงต้องมีความพร้อมในการให้บริการ มีความปลอดภัย และเป็นไปตามมาตรฐานรัฐบาลดิจิทัล
4. โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ประกอบด้วย
   - Data Center
   - Server
   - Cloud Services
   - Network
   - Internet
   - Firewall
   - Wireless Network
   - End Point Device

   โครงสร้างพื้นฐานเหล่านี้ถือเป็นทรัพยากรสำคัญขององค์กร หากขาดการบริหารจัดการที่เหมาะสม อาจส่งผลกระทบต่อการดำเนินงานทั้งองค์กร

- **ประโยชน์และคุณค่าของการตรวจสอบด้านเทคโนโลยีสารสนเทศต่อ สวพส.**

ในปัจจุบันเทคโนโลยีสารสนเทศเป็นกลไกสำคัญในการขับเคลื่อนพันธกิจของ สวพส. ทั้งในด้านการวิจัย การพัฒนา การส่งเสริมอาชีพ การบริหารโครงการ การให้บริการประชาชน การจัดการฐานข้อมูลเกษตรกร การบริหารทรัพยากรองค์กร และการเชื่อมโยงข้อมูลกับหน่วยงานภาครัฐอื่น หากระบบสารสนเทศขาดการกำกับดูแลที่ดี ขาดมาตรการควบคุมภายในที่เหมาะสม หรือไม่สามารถบริหารจัดการความเสี่ยงด้านเทคโนโลยีได้อย่างมีประสิทธิภาพ ย่อมส่งผลกระทบต่อการดำเนินงานขององค์กรในหลายมิติ ทั้งด้านประสิทธิภาพ ความน่าเชื่อถือ ความมั่นคงปลอดภัยของข้อมูล และความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย

การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit : IT Audit) จึงเป็นกลไกสำคัญในการให้ความเชื่อมั่นต่อผู้บริหารและคณะกรรมการตรวจสอบว่า ระบบการกำกับดูแล (Governance) การบริหารความเสี่ยง (Risk Management) และการควบคุมภายใน (Internal Control) ด้านเทคโนโลยีสารสนเทศของ สวพส. มีความเพียงพอ เหมาะสม และสามารถสนับสนุนการบรรลุพันธกิจ

ขององค์กรได้อย่างมีประสิทธิผล ที่สำคัญ IT Audit ในปัจจุบันมิได้มีบทบาทเพียงการค้นหาข้อบกพร่องหรือการตรวจสอบการปฏิบัติตามระเบียบ (Compliance Audit) เท่านั้น แต่ได้พัฒนาไปสู่การเป็นเครื่องมือในการสร้างคุณค่า (Value Creation) และยกระดับการบริหารจัดการองค์กรในภาพรวม โดยมุ่งเน้นการให้ข้อเสนอแนะเชิงระบบที่สามารถลดความเสี่ยง เพิ่มประสิทธิภาพ และสนับสนุนการตัดสินใจของผู้บริหารในระยะยาว

1. ยกระดับการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (Digital Governance)

การตรวจสอบช่วยประเมินว่าการกำกับดูแลด้านเทคโนโลยีสารสนเทศของ สวพส. มีโครงสร้าง บทบาท หน้าที่ และกลไกการกำกับติดตามที่ชัดเจนหรือไม่ รวมถึงประเมินว่าผู้บริหารได้รับข้อมูลสารสนเทศที่เพียงพอสำหรับการตัดสินใจ ผลจากการตรวจสอบทำให้ผู้บริหารสามารถกำหนดนโยบายด้านดิจิทัล ติดตามความก้าวหน้าของโครงการ และบริหารความเสี่ยงด้านเทคโนโลยีได้อย่างเป็นระบบ ส่งผลให้การลงทุนด้านเทคโนโลยีสารสนเทศเกิดความคุ้มค่าและสอดคล้องกับยุทธศาสตร์ขององค์กร

2. สนับสนุนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

IT Audit ช่วยระบุ วิเคราะห์ และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจส่งผลกระทบต่อการดำเนินงานของ สวพส. เช่น

- ความเสี่ยงจากการโจมตีทางไซเบอร์
- ความเสี่ยงจากการรั่วไหลของข้อมูลส่วนบุคคล
- ความเสี่ยงจากการหยุดชะงักของระบบสารสนเทศ
- ความเสี่ยงจากผู้ให้บริการภายนอก
- ความเสี่ยงจากการกำหนดสิทธิ์การเข้าถึงระบบไม่เหมาะสม

การตรวจสอบทำให้องค์กรสามารถกำหนดมาตรการควบคุมที่เหมาะสม ลดโอกาสเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อพันธกิจและบริการขององค์กร

3. เสริมสร้างความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

การตรวจสอบช่วยประเมินความพร้อมขององค์กรในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากภัยคุกคามทางไซเบอร์ ได้แก่

- การควบคุมสิทธิ์ผู้ใช้งาน
- การบริหารจัดการรหัสผ่าน
- การติดตาม Security Logs
- การบริหารจัดการช่องโหว่
- การสำรองข้อมูล
- การตอบสนองต่อเหตุการณ์ด้านไซเบอร์
- การซักซ้อมแผนรับมือเหตุการณ์

ผลจากการตรวจสอบช่วยลดความเสี่ยงของการหยุดชะงักของระบบ การสูญหายของข้อมูล และความเสียหายต่อภาพลักษณ์ขององค์กร

4. ส่งเสริมการปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้อง

การตรวจสอบช่วยประเมินการปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ช่วยลดความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย ลดโอกาสเกิดบทลงโทษ และเพิ่มความน่าเชื่อถือขององค์กร เช่น

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- มาตรฐานรัฐบาลดิจิทัล (DGA)

5. เพิ่มประสิทธิภาพของระบบสารสนเทศและการให้บริการ

การตรวจสอบช่วยประเมินประสิทธิภาพของระบบสารสนเทศที่ใช้สนับสนุนภารกิจของ สวพส. เช่น ระบบ ERP ระบบฐานข้อมูลเกษตรกร ระบบสารสนเทศเพื่อการวิจัย และระบบบริการประชาชน ข้อเสนอแนะจากการตรวจสอบช่วยให้หน่วยงานปรับปรุงกระบวนการทำงาน ลดขั้นตอนที่ซ้ำซ้อน พัฒนาระบบให้มีความเสถียร และเพิ่มคุณภาพการให้บริการแก่ผู้รับบริการและผู้มีส่วนได้ส่วนเสีย

- **ผลลัพธ์ที่คาดหวังจากการตรวจสอบด้านเทคโนโลยีสารสนเทศ**

การดำเนินการตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางในคู่มือนี้ คาดว่าจะก่อให้เกิดผลลัพธ์สำคัญ ได้แก่

1) ระบบการกำกับดูแลด้านเทคโนโลยีสารสนเทศของ สวพส. มีความชัดเจนและสอดคล้องกับหลักธรรมาภิบาล
2) ความเสี่ยงด้านเทคโนโลยีสารสนเทศได้รับการบริหารจัดการอย่างเป็นระบบและเหมาะสม
3) ระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศมีประสิทธิผลและสามารถป้องกันหรือลดผลกระทบจากความเสี่ยงที่สำคัญ
4) การดำเนินงานเป็นไปตามกฎหมาย มาตรฐาน และนโยบายที่เกี่ยวข้อง
5) ผู้บริหารสามารถใช้ผลการตรวจสอบเป็นข้อมูลประกอบการตัดสินใจเชิงบริหารและเชิงกลยุทธ์
6) หน่วยรับตรวจนำข้อเสนอแนะไปปรับปรุงการดำเนินงานอย่างต่อเนื่อง ส่งผลให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศของ สวพส. มีประสิทธิภาพ โปร่งใส และสามารถรองรับการพัฒนาองค์กรสู่รัฐบาลดิจิทัลได้อย่างยั่งยืน

จากผลการตรวจสอบด้านเทคโนโลยีสารสนเทศของ สวพส. ข้อเสนอแนะของผู้ตรวจสอบภายในมิได้มุ่งเน้นเพียงการแก้ไขข้อบกพร่องเฉพาะประเด็น แต่สามารถขยายผลสู่การปรับปรุงเชิงระบบ เช่น การเสนอให้จัดทำรายงาน Digital Governance ต่อผู้บริหารอย่างสม่ำเสมอ การพัฒนาแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA) การจัดทำกระบวนการรองรับการใช้สิทธิของเจ้าของข้อมูล การพัฒนาระบบติดตามการจัดการข้อมูลตลอดวงจรชีวิต การซักซ้อมแผนตอบสนองเหตุข้อมูลรั่วไหล การทบทวนค่า RTO/RPO จากผลการวิเคราะห์ผลกระทบทางธุรกิจ การกำหนดบทบาทผู้รับผิดชอบในแผนตอบสนองเหตุการณ์ให้ชัดเจน ตลอดจนการยกระดับการบริหารความเสี่ยงของผู้ให้บริการภายนอกและการกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศใน TOR ของโครงการด้าน IT ข้อเสนอแนะเหล่านี้ส่งผลให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศของ สวพส. เปลี่ยนจากการแก้ไขปัญหาเฉพาะหน้าไปสู่การพัฒนาระบบการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายในอย่างเป็นรูปธรรม ซึ่งช่วยเพิ่มความพร้อมขององค์กรในการรองรับภัยคุกคามทางไซเบอร์ การปฏิบัติตามกฎหมาย การรักษาความมั่นคงปลอดภัยของข้อมูล และการดำเนินภารกิจอย่างต่อเนื่อง

ส่วนที่ 2
กรอบแนวคิด กฎหมาย และมาตรฐานที่ใช้ในการตรวจสอบด้านเทคโนโลยีสารสนเทศ

การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit : IT Audit) มีวัตถุประสงค์เพื่อให้ความเชื่อมั่นว่าการกำกับดูแล (Governance) การบริหารความเสี่ยง (Risk Management) และการควบคุมภายใน (Internal Control) ด้านเทคโนโลยีสารสนเทศขององค์กร มีความเพียงพอ เหมาะสม และสามารถสนับสนุนการบรรลุวัตถุประสงค์ขององค์กรได้อย่างมีประสิทธิผล ผู้ตรวจสอบภายในจึงต้องอาศัยมาตรฐานวิชาชีพ กฎหมาย ระเบียบ และกรอบการกำกับดูแลที่ได้รับการยอมรับทั้งในระดับสากลและระดับประเทศเป็นเกณฑ์ในการตรวจสอบ (Audit Criteria) เพื่อให้ผลการตรวจสอบมีความถูกต้อง เชื่อถือได้ และสามารถสะท้อนถึงความเพียงพอของระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน

สำหรับการตรวจสอบด้านเทคโนโลยีสารสนเทศของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) แนวปฏิบัติการตรวจสอบฉบับนี้กำหนดให้ใช้กรอบแนวคิดและมาตรฐานหลัก ได้แก่

1) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

เป็นกฎหมายหลักที่กำหนดหลักเกณฑ์ในการเก็บรวบรวม ใช้ เปิดเผย และโอนข้อมูลส่วนบุคคล เพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล และกำหนดหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) ให้ดำเนินการตามหลักความโปร่งใส ความจำกัดของวัตถุประสงค์ ความมั่นคงปลอดภัยของข้อมูล และความรับผิดชอบต่อข้อมูล (Accountability) ในการตรวจสอบด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบภายในใช้กฎหมายฉบับนี้เป็นเกณฑ์ในการประเมินการกำกับดูแลข้อมูลส่วนบุคคลของ สวพส. ครอบคลุมการจัดทำ Privacy Notice การขอความยินยอม (Consent) การจัดทำบันทึกรายการประมวลผลข้อมูล (ROPA) การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) การบริหารจัดการเหตุละเมิดข้อมูลส่วนบุคคล (Personal Data Breach Management) การใช้สิทธิของเจ้าของข้อมูล (Data Subject Rights) ตลอดจนมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อให้มั่นใจว่าการบริหารจัดการข้อมูลของ สวพส. เป็นไปตามกฎหมาย ลดความเสี่ยงจากการละเมิดข้อมูล และสร้างความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสีย

2) พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม

เป็นกฎหมายที่กำหนดฐานความผิดเกี่ยวกับการเข้าถึงระบบหรือข้อมูลคอมพิวเตอร์โดยมิชอบ การทำลายหรือแก้ไขข้อมูล การเผยแพร่ข้อมูลอันเป็นเท็จ การรบกวนการทำงานของระบบคอมพิวเตอร์ รวมถึงกำหนดหน้าที่ของผู้ให้บริการในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Computer Traffic Data) เพื่อสนับสนุนการสืบสวนเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย ในการตรวจสอบด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบภายในใช้กฎหมายฉบับนี้เป็นเกณฑ์ในการประเมินมาตรการควบคุมการเข้าถึงระบบ การจัดเก็บและการสอบทาน Security Log การบริหารจัดการบัญชีผู้ใช้งาน การตรวจสอบเหตุการณ์ผิดปกติ (Incident Monitoring) และการกำหนดมาตรการป้องกันการกระทำ

ความผิดทางคอมพิวเตอร์ เพื่อให้ระบบสารสนเทศของ สวพส. มีความมั่นคงปลอดภัย สามารถตรวจสอบย้อนหลังได้ และรองรับการดำเนินการตามกฎหมายเมื่อเกิดเหตุการณ์ผิดปกติ

3) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

เพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยกำหนดให้หน่วยงานมีการบริหารจัดการความเสี่ยงด้านไซเบอร์ การเฝ้าระวังภัยคุกคาม การป้องกัน การตรวจจับ การตอบสนอง และการฟื้นฟูระบบเมื่อเกิดเหตุการณ์ด้านไซเบอร์ แม้ สวพส. จะไม่ได้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) แต่หลักการตามกฎหมายดังกล่าวสามารถนำมาประยุกต์ใช้เพื่อยกระดับการบริหารจัดการความมั่นคงปลอดภัยขององค์กรได้ ในการตรวจสอบผู้ตรวจสอบภายในจะประเมินนโยบายและมาตรการด้าน Cybersecurity การประเมินความเสี่ยงด้านไซเบอร์ การบริหารจัดการเหตุการณ์ผิดปกติ (Cyber Incident Management) การจัดทำและทดสอบแผนตอบสนองเหตุการณ์ด้านไซเบอร์ (Cyber Incident Response Plan: CIRP) การบริหารช่องโหว่ (Vulnerability Management) และการสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้มั่นใจว่าระบบสารสนเทศของ สวพส. มีความพร้อมในการป้องกันและตอบสนองต่อภัยคุกคามที่อาจส่งผลกระทบต่อภารกิจขององค์กร

4) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

กำหนดให้ข้อมูลอิเล็กทรอนิกส์ เอกสารอิเล็กทรอนิกส์ และลายมือชื่ออิเล็กทรอนิกส์ มีผลทางกฎหมายเช่นเดียวกับเอกสารกระดาษ หากดำเนินการตามหลักเกณฑ์ที่กฎหมายกำหนด ส่งผลให้หน่วยงานของรัฐสามารถให้บริการและดำเนินกระบวนการทางอิเล็กทรอนิกส์ได้อย่างถูกต้องตามกฎหมาย ในการตรวจสอบด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบภายในใช้กฎหมายฉบับนี้เป็นเกณฑ์ในการประเมินความน่าเชื่อถือของระบบงานอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ การจัดเก็บเอกสารอิเล็กทรอนิกส์ ความถูกต้องครบถ้วนของข้อมูล และการรักษาความมั่นคงปลอดภัยของระบบที่รองรับการให้บริการดิจิทัล เพื่อให้มั่นใจว่ากระบวนการให้บริการและการดำเนินงานของ สวพส. ผ่านระบบอิเล็กทรอนิกส์มีผลสมบูรณ์ตามกฎหมายและสามารถตรวจสอบได้

5) มาตรฐานรัฐบาลดิจิทัล (Digital Government)

มาตรฐานรัฐบาลดิจิทัลเป็นกรอบแนวทางที่กำหนดโดยหน่วยงานภาครัฐเพื่อยกระดับการบริหารงานและการให้บริการภาครัฐด้วยเทคโนโลยีดิจิทัล โดยมุ่งเน้นการพัฒนากระบวนการทำงาน การเชื่อมโยงข้อมูลภาครัฐ การให้บริการประชาชนผ่านช่องทางดิจิทัล การใช้ Digital ID การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน การบริหารจัดการข้อมูลภาครัฐ และการกำกับดูแลด้านดิจิทัล (Digital Governance) ในการตรวจสอบด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบภายในใช้มาตรฐานดังกล่าวในการประเมินความพร้อมขององค์กรด้านรัฐบาลดิจิทัล การกำกับดูแลโครงการดิจิทัล การบริหารจัดการข้อมูลภาครัฐ การพัฒนาบริการดิจิทัล และการดำเนินงานให้สอดคล้องกับนโยบายรัฐบาลดิจิทัล เพื่อสนับสนุนให้ สวพส. พัฒนาระบบสารสนเทศที่มีประสิทธิภาพ โปร่งใส เชื่อมโยงข้อมูลได้อย่างปลอดภัย และตอบสนองต่อความต้องการของผู้รับบริการได้อย่างมีประสิทธิผล

6) COBIT 2019 และ NIST Cybersecurity Framework (CSF)

เป็นกรอบมาตรฐานสากลที่ได้รับการยอมรับอย่างแพร่หลายในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ โดย **COBIT 2019** มุ่งเน้นการสร้างระบบการกำกับดูแลเทคโนโลยีสารสนเทศ (IT Governance) ที่เชื่อมโยงเป้าหมายด้านธุรกิจกับการบริหารจัดการ IT ผ่านกระบวนการที่ครอบคลุมด้านการวางแผน การดำเนินงาน การติดตาม และการปรับปรุงอย่างต่อเนื่อง ส่วน **NIST Cybersecurity Framework (CSF)** มุ่งเน้นการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ผ่าน 6 ฟังก์ชันหลัก ได้แก่ Govern, Identify, Protect, Detect, Respond และ Recover ซึ่งครอบคลุมวงจรการบริหารความมั่นคงปลอดภัยทั้งหมด ในการตรวจสอบด้านเทคโนโลยีสารสนเทศของ สวพส. ผู้ตรวจสอบภายในใช้ COBIT 2019 เป็นกรอบในการประเมินการกำกับดูแล การบริหารความเสี่ยง และการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls) ขณะที่ใช้ NIST CSF เป็นเกณฑ์ในการประเมินความพร้อมด้าน Cybersecurity การบริหารเหตุการณ์ผิดปกติ การบริหารช่องโหว่ การป้องกันภัยคุกคาม และการฟื้นฟูระบบหลังเกิดเหตุการณ์ เพื่อให้ข้อเสนอแนะที่สอดคล้องกับมาตรฐานสากลและสามารถยกระดับการบริหารจัดการเทคโนโลยีสารสนเทศของ สวพส. ได้อย่างเป็นรูปธรรมและยั่งยืน

ส่วนที่ 3
ความเสี่ยงที่สำคัญ และการควบคุม

ผู้ตรวจสอบภายใน ประเมินว่าความเสี่ยงที่สำคัญได้รับการระบุ ประเมิน และควบคุมอย่างเหมาะสม โดยพิจารณาครอบคลุมมิติ Governance – Risk Management – Internal Control (GRC) รวมถึงกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศมีวัตถุประสงค์เพื่อ ระบุความเสี่ยงที่อาจส่งผลกระทบต่อภารกิจของ สวพส. ประเมินความเพียงพอของมาตรการควบคุมภายในด้าน IT สนับสนุนการวางแผนการตรวจสอบแบบอิงความเสี่ยง (Risk-Based IT Audit) กำหนดประเด็นการตรวจสอบที่มีความสำคัญ และเสนอแนวทางลดความเสี่ยงและเพิ่มประสิทธิภาพการดำเนินงาน จากการวิเคราะห์บริบทการดำเนินงานของ สวพส. ความเสี่ยงด้าน IT สามารถแบ่งได้ ดังนี้

1) ประเมินความเสี่ยงและการควบคุมด้านเทคโนโลยีสารสนเทศของ สวพส. เป็นไปตามกฎหมาย มาตรฐาน ประกาศ และแนวทางที่เกี่ยวข้อง ได้แก่ ด้านธรรมาภิบาลดิจิทัล (Digital Governance) ด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA)

ความเสี่ยง	ผลกระทบ	การควบคุมที่มี
ไม่มี Digital Governance ที่ชัดเจน	โครงการ IT ไม่สอดคล้องกับยุทธศาสตร์ขององค์กร	กรอบธรรมาภิบาล (Digital Governance Framework) เช่น นโยบาย โครงสร้าง
ผู้บริหารไม่ได้รับรายงานด้าน IT อย่างสม่ำเสมอ	ตัดสินใจไม่ทันต่อความเสี่ยง	รายงาน Digital Governance ต่อผู้บริหารปีละ 1 ครั้ง
ไม่มีการบริหารความเสี่ยงด้าน Digital	เกิดความเสี่ยงสะสมโดยไม่มีการจัดวางมาตรการควบคุม	คณะทำงานบริหารควบเสี่ยงและควบคุมภายในของ สวพส. โดยมีการทบทวนความเสี่ยงเป็นประจำทุกปี
ไม่มี Privacy Notice	ไม่ปฏิบัติตามกฎหมาย PDPA	จัดทำ Privacy Notice ทุกกระบวนการ
ไม่มี DPIA	ประเมินผลกระทบไม่ครบถ้วน	จัดทำ DPIA สำหรับกิจกรรมที่มีความเสี่ยงสูง
ไม่ได้จัดทำหรือปรับปรุงทะเบียนกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) ให้เป็นปัจจุบัน	เก็บข้อมูลเกินความจำเป็น	จัดทำ ROPA กำหนดระยะเวลาการจัดเก็บและทำลายข้อมูล
ไม่มีขั้นตอน/แนวทางปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูล หรือข้อมูลรั่วไหล	แจ้งเหตุไม่ทันตามกฎหมาย	จัดทำขั้นตอน/แนวทางปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูล หรือ ข้อมูลรั่วไหล

2) ประเมินความเสี่ยงและการควบคุมการรักษาความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลระบบสารสนเทศของ สวพส. ได้แก่ ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

ความเสี่ยง	ผลกระทบ	การควบคุมที่มี
ถูกโจมตีทางไซเบอร์	ระบบหยุดให้บริการ	Firewall, IDS, EDR
ไม่มีการติดตาม Log	ตรวจจับเหตุการณ์ไม่ได้	Security Log Monitoring
ไม่มีแผนตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ	รับมือเหตุการณ์ล่าช้า ไม่ทันกาล	จัดทำ Cyber Incident Response Plan
บุคลากรของ สวพส. ขาดความรู้ ความตระหนัก และทักษะด้านความมั่นคงปลอดภัยไซเบอร์	ไม่สามารถรับมือเมื่อเกิดเหตุการณ์	ให้ความรู้ จัดฝึกอบรม ให้แก่บุคลากรอย่างต่อเนื่อง
ไม่มีการซักซ้อม	บุคลากรไม่พร้อมรับเหตุ	ฝึกซ้อมแผนแบบ Table Top Exercise

3) ประเมินความเสี่ยงและการควบคุมของแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP) ได้แก่ การจัดทำและดำเนินการตามแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ

ความเสี่ยง	ผลกระทบ	การควบคุมที่มี
ไม่มี BIA หรือการวิเคราะห์ผลกระทบทางธุรกิจ	กำหนดลำดับความสำคัญไม่ได้	จัดทำ Business Impact Analysis ในระบบที่สำคัญ
RTO/RPO ไม่เหมาะสม	กู้คืนระบบไม่ได้ตามเป้าหมาย	ทบทวนค่า RTO/RPO ทุกปี
ไม่มี Disaster Recovery Plan	ระบบกลับมาใช้งานไม่ได้	จัดทำ DRP
ไม่มี Backup Policy	สูญเสียข้อมูล	กำหนด Daily Backup
ไม่มีการซ้อมแผน	แผนใช้ไม่ได้จริง	ซักซ้อม BCP/DRP อย่างน้อยปีละครั้ง

4) ประเมินความเสี่ยงและการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls) 15 ประเด็น

ประเด็นการประเมิน	ความเสี่ยง	การควบคุมที่มี
โครงสร้างและการกำกับดูแลด้านเทคโนโลยีสารสนเทศ	ไม่มีนโยบาย IT	กลยุทธ์หรือแผนงานด้าน IT
การบริหารจัดการผู้ให้บริการภายนอก	ผู้ให้บริการภายนอกมีระบบป้องกันที่ไม่รัดกุม ทำให้ข้อมูลรั่วไหล	NDA
การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ	ไม่ประเมินความเสี่ยง	ประเมินความเสี่ยงด้าน IT ขององค์กร
การบริหารจัดการการตั้งค่าระบบ และการควบคุมการตั้งค่ารหัสผ่าน	ตั้งค่าระบบไม่ปลอดภัยหรือไม่เป็นไปตามมาตรฐานด้านความมั่นคงปลอดภัยที่กำหนดไว้	

ประเด็นการประเมิน	ความเสี่ยง	การควบคุมที่มี
การบริหารจัดการบัญชีผู้ใช้งาน	User เกินความจำเป็น	กำหนดสิทธิ์ตามบทบาทหน้าที่ อนุมัติการใช้สิทธิ์
การจำกัดสิทธิการเข้าถึงผู้ใช้งานที่มีสิทธิสูง (HPID) และการควบคุมผู้ใช้งานระบบ	Admin ใช้งานโดยไม่มีการควบคุม	Log Monitoring
การสอบทาน Log ด้านความมั่นคงปลอดภัย	Log ถูกลบหรือแก้ไข	กำหนดนโยบายการจัดเก็บ Log การจัดเก็บ Log ครอบคลุมทุกระบบสำคัญ จำกัดสิทธิ์ผู้เข้าถึง
การตรวจสอบช่องโหว่และทดสอบเจาะระบบ	ระบบถูกโจมตีจากช่องโหว่	สแกนช่องโหว่ครอบคลุมระบบที่มีความสำคัญต่อภารกิจ อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงระบบที่มีนัยสำคัญ
การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา	รับมือเหตุการณ์ล่าช้า	กำหนดขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ไม่ปกติ
การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์	Malware Ransomware	Antivirus ฝึกอบรม/ให้ความรู้เพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์
การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม และความปลอดภัยของอุปกรณ์ปลายทาง	บุคคลภายนอกเข้าห้อง Server	CCTV Visitor Log ระบบ Access Control
การบริหารจัดการการเปลี่ยนแปลง	เปลี่ยนระบบโดยไม่ได้อนุมัติ	แบบฟอร์มคำขอเปลี่ยนแปลง การอนุมัติการเปลี่ยนแปลงระบบจากผู้มีอำนาจ
การสำรองข้อมูล (Data Backup) และการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ	กู้คืนข้อมูลไม่ได้	Backup Policy การทดสอบกู้คืนข้อมูลหรือระบบ
การบริหารขีดความสามารถของระบบ	Server เต็ม ระบบล่ม	ติดตามและตรวจสอบขีดความสามารถหรือปริมาณการใช้งาน
การจัดหาและการพัฒนาระบบ	พัฒนาระบบไม่ปลอดภัย	ทดสอบระบบขั้นสุดท้ายโดยผู้ใช้งานจริง

ความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สวพส. มีความเชื่อมโยงโดยตรงกับการบรรลุพันธกิจทั้งด้านการวิจัย การพัฒนาพื้นที่สูง การเผยแพร่องค์ความรู้ และการบริหารจัดการภายใน การประเมินความเสี่ยงควรครอบคลุมการกำกับดูแลดิจิทัล การคุ้มครองข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยไซเบอร์ ความต่อเนื่องทางธุรกิจ และการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบภายในควรใช้ Risk and Control ในการเชื่อมโยงระหว่างความเสี่ยง ผลกระทบ และมาตรการควบคุมที่ควรมี เพื่อวางแผนการตรวจสอบแบบอิงความเสี่ยง (Risk-Based IT Audit) และจัดทำข้อเสนอแนะที่สามารถลดความเสี่ยง ยกระดับการควบคุมภายใน และสร้างคุณค่าเชิงระบบให้แก่ สวพส. ได้อย่างเป็นรูปธรรมและยั่งยืน

ส่วนที่ 4
วิธีการตรวจสอบ

การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit: IT Audit) ของหน่วยตรวจสอบภายใน ดำเนินการตามแนวทางการตรวจสอบภายในแบบอิงความเสี่ยง (Risk-Based Internal Audit) โดยมุ่งประเมินความเพียงพอและประสิทธิผลของ การกำกับดูแล (Governance) การบริหารความเสี่ยง (Risk Management) และการควบคุมภายใน (Internal Control) ด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าระบบสารสนเทศสามารถสนับสนุนภารกิจของ สวพส. มีความปลอดภัย มีประสิทธิภาพ และเป็นไปตามกฎหมาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง การตรวจสอบครอบคลุมการประเมินทั้งด้านการปฏิบัติตามกฎหมาย (Compliance Audit) ความเพียงพอของระบบควบคุม (Control Assessment) และการวิเคราะห์ความเสี่ยง (Risk Assessment) พร้อมทั้งให้ข้อเสนอแนะเชิงระบบเพื่อยกระดับการบริหารจัดการด้านเทคโนโลยีสารสนเทศของ สวพส.

- **กระบวนการตรวจสอบ (IT Audit Process)**

การตรวจสอบใช้แนวทาง Risk-Based IT Audit โดยพิจารณาความเสี่ยงที่มีนัยสำคัญต่อภารกิจของ สวพส. และจัดลำดับความสำคัญของประเด็นตรวจสอบ ประกอบด้วย

1) จัดทำ Engagement plan กำหนดวัตถุประสงค์ ขอบเขต และวิธีการตรวจสอบ
2) ศึกษาภารกิจ ยุทธศาสตร์ และโครงสร้างการกำกับดูแลด้าน IT ของ สวพส.
3) ศึกษากฎหมาย ระเบียบ มาตรฐาน และแนวทางที่เกี่ยวข้อง
4) ประเมินความเสี่ยงของระบบสารสนเทศและกระบวนการที่เกี่ยวข้อง
5) จัดทำ Audit Program
6) ดำเนินการตรวจสอบ วิเคราะห์ผลการตรวจสอบและประเมินความเสี่ยงของข้อบกพร่อง
7) จัดทำกระดาษทำการและให้ข้อเสนอแนะเชิงระบบ
8) ประชุมปิดตรวจร่วมกับหน่วยรับตรวจ และผู้ที่เกี่ยวข้อง
9) รายงานผลต่อผู้บริหาร คณะกรรมการตรวจสอบ และคณะกรรมการสถาบัน
10) ติดตามผลการดำเนินการผ่านระบบ CMT

- **วิธีการตรวจสอบ (IT Audit Process)**

การตรวจสอบแบ่งออกเป็น 5 หมวด ดังนี้

แนวทางการตรวจสอบ	วิธีการตรวจสอบ
PDPA และกฎหมายที่เกี่ยวข้อง	ตรวจสอบความสอดคล้องของการดำเนินงานด้านเทคโนโลยีสารสนเทศกับกฎหมาย ระเบียบ มาตรฐานรัฐบาลดิจิทัล ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และนโยบายภายในของ สวพส. โดยเน้นการประเมินเชิง Compliance และการวิเคราะห์ช่องว่าง (Gap Analysis) รวบรวมกฎหมาย มาตรฐาน และประกาศที่เกี่ยวข้องทั้งหมด 1) ตรวจสอบการจัดทำนโยบาย และแผนพัฒนาดิจิทัล

แนวทางการตรวจสอบ	วิธีการตรวจสอบ
	2) ตรวจสอบการดำเนินงานด้าน PDPA ประเด็น Privacy Management, Data Management, Data Security, Third Party, Incident Management 3) สุ่มกระบวนงานที่ใช้ข้อมูลส่วนบุคคลอย่างน้อย 1 กระบวนงาน 4) สุ่มตรวจสอบหลักฐานการขอความยินยอมและการแจ้ง Privacy Notice 5) ตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศเป็นไปตามข้อกำหนดของมาตรฐานรัฐบาลดิจิทัล ประกาศแนวทางของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ 6) วิเคราะห์ช่องว่างการไม่ปฏิบัติตาม และจัดระดับความเสี่ยง 7) สัมภาษณ์ผู้รับผิดชอบด้าน IT และ PDPA 8) สรุปข้อค้นพบและข้อเสนอแนะเชิงระบบ
การรักษาความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลระบบสารสนเทศ	ประเมินความเพียงพอของมาตรการด้าน Cybersecurity และ IT Governance ครอบคลุมการป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคาม รวมถึงโครงสร้างการกำกับดูแลด้าน IT ตรวจสอบนโยบายความมั่นคงปลอดภัยว่าทันสมัยหรือไม่ 1) ตรวจสอบโครงสร้างการกำกับดูแลด้าน Cybersecurity 2) สุ่มเหตุการณ์ไซเบอร์ย้อนหลัง 6–12 เดือน 3) ตรวจสอบขั้นตอนการแจ้งเหตุและการตอบสนอง 4) วิเคราะห์ความเสี่ยงจากจุดอ่อนที่พบ 5) สรุปข้อค้นพบและข้อเสนอแนะเชิงป้องกันและแก้ไข
บริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP)	ประเมินความครบถ้วนและความพร้อมของแผน BCP การกำหนด RTO/RPO และผลการซักซ้อมแผนให้สามารถรองรับเหตุขัดข้องและภัยคุกคามที่สำคัญ 1) ตรวจสอบความครบถ้วนของแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ 2) เปรียบเทียบ BCP กับผล Impact Analysis 3) ตรวจสอบการกำหนด RTO/RPO 4) ตรวจสอบหลักฐานการซักซ้อมแผนย้อนหลัง 1 ปี 5) สัมภาษณ์ผู้รับผิดชอบแผน 6) ประเมินความพร้อมจริงเมื่อเกิดเหตุ 7) วิเคราะห์ช่องว่าง และเสนอแนะแนวทางปรับปรุงแผน 8) สรุปข้อค้นพบและข้อเสนอแนะ
การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls)	ประเมินความเพียงพอและประสิทธิผลของ IT General Controls 15 ประเด็น 1) โครงสร้างและการกำกับดูแลด้านเทคโนโลยีสารสนเทศ 2) การบริหารจัดการผู้ให้บริการภายนอก

แนวทางการตรวจสอบ	วิธีการตรวจสอบ
	3) การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ 4) การบริหารจัดการการตั้งค่าระบบ และการควบคุมการตั้งค่ารหัสผ่าน 5) การบริหารจัดการบัญชีผู้ใช้งาน 6) การจำกัดสิทธิการเข้าถึงผู้ใช้งานที่มีสิทธิสูง (HPID) และการควบคุมผู้ใช้งานระบบ 7) การสอบทาน Log ด้านความมั่นคงปลอดภัย 8) การตรวจสอบช่องโหว่และทดสอบเจาะระบบ 9) การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา 10) การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และแผนการรับมือภัยคุกคามทางไซเบอร์ 11) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมและความปลอดภัยของอุปกรณ์ปลายทาง 12) การบริหารจัดการการเปลี่ยนแปลง 13) การสำรองข้อมูล (Data Backup) และการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ 14) การบริหารขีดความสามารถของระบบ 15) การจัดหาและการพัฒนาระบบ

- **เครื่องมือที่ใช้ในการตรวจสอบ (Audit Tools)**

การตรวจสอบใช้เครื่องมือมาตรฐาน ได้แก่

1. Audit Checklist: ลักษณะเป็นชุดคำถามที่มีโครงสร้างชัดเจน ซึ่งผู้ตรวจสอบ (Auditor) ใช้เป็นแนวทางในการตรวจประเมินการทำงาน ระบบงาน หรือเอกสารที่เกี่ยวข้อง เพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามมาตรฐาน กฎหมาย ระเบียบ หรือหลักเกณฑ์ที่กำหนดไว้ได้อย่างครบถ้วน
2. Risk Assessment Matrix: เป็นเครื่องมือที่ใช้ประเมินและจัดลำดับความสำคัญของความเสี่ยง โดยนำตัวแปรสำคัญ 2 ค่า ได้แก่ โอกาสที่จะเกิด (Likelihood) และความรุนแรงของผลกระทบ (Impact) เพื่อหาค่าระดับความเสี่ยง
3. Engagement plan: แผนการปฏิบัติงานตรวจสอบ โดยรายละเอียดที่จัดทำขึ้นล่วงหน้าเพื่อกำหนดวัตถุประสงค์ ขอบเขต ประเด็นการตรวจสอบ เอกสารประกอบการตรวจสอบ ความรู้/ทักษะที่ใช้ในการตรวจสอบ และทรัพยากรที่ต้องใช้
4. Audit Program: แนวทางการปฏิบัติงานตรวจสอบ เป็นรายละเอียดที่ผู้ตรวจสอบ (Auditor) จัดทำขึ้นล่วงหน้า เพื่อกำหนดขั้นตอน วิธีการ ขอบเขต และวัตถุประสงค์ในการตรวจสอบเรื่องใดเรื่องหนึ่งอย่างเป็นระบบ ช่วยควบคุมการทำงานให้บรรลุเป้าหมายและมีหลักฐาน
5. Working Paper: เอกสาร บันทึก หรือหลักฐานที่ผู้ตรวจสอบภายใน จัดทำขึ้นในระหว่างการปฏิบัติงาน เพื่อแสดงรายละเอียดของวิธีการตรวจสอบ ขอบเขตงาน หลักฐานที่ได้รับ และข้อสรุปจากการตรวจสอบ

6. Sampling: กระบวนการคัดเลือกกลุ่มประชากร หรือข้อมูลส่วนหนึ่งจากประชากรทั้งหมด เพื่อนำมาศึกษา วิเคราะห์ หรือตรวจสอบ แล้วใช้ผลลัพธ์นั้นอ้างอิงกลับไปยังประชากรทั้งหมดโดยไม่ต้องเก็บข้อมูลจากทุกคน
7. Audit Finding: สิ่งที่ตรวจพบจากการตรวจสอบ คือ สิ่งที่เป็นอยู่ (Condition) สาเหตุ (Cause) ผลกระทบ (Effect) ข้อสังเกตและข้อเสนอแนะ (Recommendation) หรือผลสรุปที่ได้จากการรวบรวมและประเมินหลักฐานของผู้ตรวจสอบ โดยนำไปเทียบกับเกณฑ์มาตรฐาน (Criteria) หรือวัตถุประสงค์ที่กำหนดไว้ ซึ่งแสดงให้เห็นถึงจุดอ่อน ความไม่สอดคล้อง หรือโอกาสในการปรับปรุงขององค์กร
8. Evidence Register: ระบบหรือเอกสารที่ใช้รวบรวม จัดเก็บ บันทึก และเชื่อมโยงรายการพยานหลักฐาน (Evidence) ต่าง ๆ ที่สนับสนุนข้อค้นพบ การดำเนินงาน หรือการปฏิบัติตามมาตรฐาน โดยมักใช้ในงานตรวจสอบภายใน การประเมินความสอดคล้องตามกฎหมายและข้อกำหนด
9. Follow-up Tracking (CMT): ระบบ กระบวนการติดตามงาน ตรวจสอบสถานะความคืบหน้า หรือบันทึกข้อมูลย้อนหลัง เพื่อให้รู้ว่ามีเรื่องใดต้องติดตามผล ติดต่อใคร และต้องดำเนินการต่อในช่วงเวลาใด ช่วยลดความผิดพลาดและเพิ่มประสิทธิภาพในการติดตามการปฏิบัติงานตามข้อเสนอแนะแนะ

- **หลักฐานการตรวจสอบ (Audit Evidence)**

  หลักฐานที่ใช้ในการตรวจสอบ ประกอบด้วย

  1. นโยบายและระเบียบด้านเทคโนโลยีสารสนเทศ
  2. นโยบายความมั่นคงปลอดภัยสารสนเทศ
  3. นโยบายและมาตรการ PDPA
  4. รายงานรัฐบาลดิจิทัล
  5. รายงานการประเมินความเสี่ยง
  6. รายงานการทดสอบระบบ
  7. Security Log
  8. Incident Report
  9. รายงานการสำรองข้อมูล
  10. แผน BCP/DRP
  11. รายงานการซักซ้อมแผน
  12. สัญญาและ TOR งานด้าน IT
  13. รายงานการประชุมคณะกรรมการที่เกี่ยวข้อง
  14. หลักฐานจากการสัมภาษณ์ และการสังเกตการณ์

ส่วนที่ 5
เทคนิคการตรวจสอบ

การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit: IT Audit) เป็นการตรวจสอบที่ต้องอาศัยทั้งความรู้ด้านการตรวจสอบภายในและความรู้ด้านเทคโนโลยีสารสนเทศ ผู้ตรวจสอบภายในจำเป็นต้องเลือกใช้เทคนิคการตรวจสอบ (Audit Techniques) ให้เหมาะสมกับลักษณะของระบบสารสนเทศ ความเสี่ยงของกระบวนการ และวัตถุประสงค์ของการตรวจสอบ เพื่อให้ได้หลักฐานการตรวจสอบ (Audit Evidence) ที่เพียงพอ เหมาะสม และเชื่อถือได้

สำหรับการตรวจสอบของ สวพส. ผู้ตรวจสอบควรใช้เทคนิคการตรวจสอบแบบผสมผสาน โดยบูรณาการการตรวจสอบเอกสาร การสัมภาษณ์ การสังเกตการณ์ การทดสอบระบบ การวิเคราะห์ข้อมูล และการใช้เครื่องมือดิจิทัล เพื่อให้สามารถประเมินการกำกับดูแล การบริหารความเสี่ยง และการควบคุมภายในด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน

1. การศึกษาข้อมูลและเอกสาร (Document Review)

เพื่อประเมินว่าหน่วยงานมีการกำหนดนโยบาย ระเบียบ ขั้นตอนการปฏิบัติงาน และเอกสารที่เกี่ยวข้องอย่างครบถ้วน ตัวอย่างเอกสาร เช่น IT Policy, Cybersecurity Policy, PDPA Policy, Information Security Policy, Digital Governance Framework, BCP / DRP, Change Management Procedure, รายงานการประชุม, รายงานผลการดำเนินงานด้านดิจิทัล

2. การสัมภาษณ์ (Interview)

เพื่อยืนยันความเข้าใจในการปฏิบัติงานและเปรียบเทียบกับเอกสารที่กำหนด ซึ่งผู้ที่สามารถให้ข้อมูลประกอบด้วย ผู้บริหาร CIO ผู้ดูแลระบบ DPO เจ้าของข้อมูล เจ้าของระบบ ผู้ใช้งานระบบ ผู้รับจ้างภายนอก ทั้งนี้ เทคนิคการสัมภาษณ์การตั้งคำถามและการพูดคุยเพื่อเก็บข้อมูล โดยอาจเป็นคำถามปลายเปิดให้ผู้ตอบอิสระ (Open-ended Questions) ซึ่งจะไม่มีตัวเลือกตายตัว และช่วยให้ได้ความคิดเห็นและเหตุผลเชิงลึก การตั้งคำถามแบบติดตามหรือต่อยอด หรือคำถามเจาะลึกต่อยอดจากคำตอบเดิม (Follow-up Questions) เป็นคำถามที่ถามต่อเนื่องจากคำตอบที่เพิ่งได้รับช่วยขยายความ หรือเจาะลึกในจุดที่น่าสนใจทำให้เข้าใจเรื่องราวกว้างขึ้น ไม่หลุดประเด็น และการตั้งคำถามแบบพาทำทีละขั้นตอน (Walk-through Questions) เป็นคำถามที่ชวนผู้ตอบจำลองหรือทำตามขั้นตอนจริงทีละสเต็ปช่วยให้เห็นปัญหาหน้างานจริงแบบละเอียด

3. การสังเกตการณ์ (Observation)

เพื่อยืนยันว่าการปฏิบัติงานจริงเป็นไปตามระเบียบ หรือหลักเกณฑ์ที่กำหนด เช่น การเข้าออกห้อง Server การควบคุมผู้มาติดต่อ การจัดเก็บเอกสาร Hard Copy การสำรองข้อมูล การอนุมัติ Change Request

4. Walkthrough

กระบวนการตรวจสอบ แนะนำ หรือจำลองการทำงานทีละขั้นตอน ตั้งแต่จุดเริ่มต้นจนถึงเป้าหมายสุดท้าย เพื่อให้เข้าใจระบบการทำงาน ค้นหาข้อผิดพลาด หรือศึกษาเส้นทาง เช่น การขอ User Account การอนุมัติสิทธิ การเปลี่ยนแปลงระบบ การแจ้ง Incident การใช้สิทธิ PDPA

5. การสอบทานระบบ (System Review)

เพื่อดูว่ามีความเหมาะสม มีประสิทธิภาพ และเป็นไปตามกฎระเบียบหรือหลักเกณฑ์ที่กำหนดไว้หรือไม่ เช่น การสอบทาน Configuration, User Account, Password Policy, Security Settings

6. การทดสอบการควบคุม (Test of Controls)

กระบวนการตรวจสอบและประเมินประสิทธิภาพการทำงานของระบบการควบคุมภายในด้านเทคโนโลยีสารสนเทศ เพื่อดูว่ามาตรการหรือนโยบายที่องค์กรกำหนดขึ้น สามารถป้องกันความเสี่ยง รักษาความปลอดภัยของข้อมูล และทำให้ระบบงานมีความถูกต้องเชื่อถือได้จริงหรือไม่

7. การตรวจสอบรายการตัวอย่าง (Sampling)

การตรวจสอบรายการตัวอย่าง (Audit Sampling) ในการตรวจสอบเทคโนโลยีสารสนเทศ (IT Audit) คือ การเลือกชุดข้อมูล บันทึกรายการ หรือกิจกรรมไอทีส่วนหนึ่งจากประชากรทั้งหมดมาตรวจสอบ แทนการตรวจทุกรายการ เพื่อประเมินว่าระบบควบคุมภายในด้าน IT ทำงานอย่างมีประสิทธิภาพและถูกต้องตามเกณฑ์ โดยสามารถแบ่งเป็นประเภทได้ดังนี้

- Random Sampling
- Judgment Sampling
- Risk-Based Sampling

8. การวิเคราะห์ข้อมูล (Data Analytics)

ตรวจสอบความปลอดภัยและช่องโหว่ของระบบวิเคราะห์พฤติกรรมการใช้งานที่ผิดปกติหรือมีความเสี่ยงประเมินประสิทธิภาพการทำงานของระบบไอทีสนับสนุนการตัดสินใจและให้ข้อเสนอแนะในการปรับปรุงการควบคุมภายในกระบวนการนำเข้า รวบรวม และตรวจวิเคราะห์ข้อมูลดิจิทัล เช่น Log ไฟล์ระบบฐานข้อมูล หรือพฤติกรรมการใช้งาน เพื่อประเมินความเสี่ยง ตรวจสอบความถูกต้อง ป้องกันการทุจริต และหาข้อผิดพลาดในระบบ IT ขององค์กร โดยสามารถใช้เครื่องมือ Excel หรือ Power BI ในการวิเคราะห์ เช่น

- User ไม่ได้ Login เกิน 90 วัน
- Admin Login นอกเวลาทำงาน
- รหัสผ่าน (Password) ไม่มีวันหมดอายุ (Password Never Expire)

9. การตรวจสอบ Log

เป็นการรวบรวม ตรวจสอบ และวิเคราะห์ไฟล์บันทึกประวัติกิจกรรม (Log File) ที่ระบบคอมพิวเตอร์, เครือข่าย, หรือแอปพลิเคชัน สร้างขึ้นอัตโนมัติ เพื่อดูว่าเกิดเหตุการณ์อะไรขึ้นบ้าง ใครเป็นผู้ใช้งาน และระบบทำงานปกติหรือไม่ตรวจสอบ เช่น Login Logout Failed Login เพื่อวิเคราะห์ความผิดปกติ การโจมตี

10. การตรวจสอบการปฏิบัติตามกฎหมาย (Compliance Testing)

เป็นกระบวนการตรวจสอบระบบงานและข้อมูลขององค์กรให้สอดคล้องกับกฎหมาย ระเบียบ หรือหลักเกณฑ์ที่กำหนด ได้แก่

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์
- การบริหารงานภาครัฐแบบดิจิทัล / ธรรมาภิบาลข้อมูล
- พระราชบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์

11. เทคนิคการใช้ AI และ Data Analytics สนับสนุนการตรวจสอบ

เพื่อยกระดับการตรวจสอบให้สอดคล้องกับแนวโน้มการตรวจสอบสมัยใหม่ ผู้ตรวจสอบภายในของ สวพส. ควรประยุกต์ใช้เทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (AI) ในขั้นตอนต่าง ๆ ของการตรวจสอบ โดยยังคงใช้ดุลยพินิจของผู้ตรวจสอบเป็นหลัก

ตัวอย่างการประยุกต์ใช้

- วิเคราะห์ความครบถ้วนของนโยบายหรือเอกสารด้วย AI
- ช่วยจัดกลุ่มและวิเคราะห์ Log หรือ Incident จำนวนมาก
- วิเคราะห์ข้อมูลผู้ใช้งานเพื่อค้นหารายการผิดปกติ (Anomaly Detection)
- วิเคราะห์แนวโน้มความเสี่ยงจากข้อมูลการตรวจสอบย้อนหลัง

ทั้งนี้ ผลลัพธ์จาก AI ควรได้รับการตรวจสอบความถูกต้องและยืนยันด้วยหลักฐานการตรวจสอบที่เชื่อถือได้ก่อนนำไปใช้เป็นข้อสรุปหรือข้อเสนอแนะ

12. ข้อควรระวังในการใช้เทคนิคการตรวจสอบ

ผู้ตรวจสอบควรคำนึงถึงประเด็นต่อไปนี้

- เลือกเทคนิคให้เหมาะสมกับวัตถุประสงค์และระดับความเสี่ยงของงานตรวจสอบ
- ใช้หลักฐานจากหลายแหล่งเพื่อเพิ่มความน่าเชื่อถือของข้อสรุป
- รักษาความลับของข้อมูลและปฏิบัติตามข้อกำหนดของ PDPA ตลอดกระบวนการตรวจสอบ
- บันทึกขั้นตอน วิธีการ และผลการทดสอบไว้อย่างครบถ้วนใน Working Papers เพื่อให้สามารถสอบทานย้อนหลังได้

ส่วนที่ 6
Lessons Learned

การถอดบทเรียน (Lessons Learned) เป็นกระบวนการสำคัญในการบริหารองค์ความรู้ (Knowledge Management : KM) ของหน่วยตรวจสอบภายใน ซึ่งมุ่งรวบรวมประสบการณ์ ข้อค้นพบ ปัจจัยความสำเร็จ อุปสรรค และแนวทางแก้ไขที่เกิดขึ้นจากการปฏิบัติงานตรวจสอบ เพื่อนำไปพัฒนาวิธีการตรวจสอบให้มีประสิทธิภาพมากยิ่งขึ้น และลดการเกิดข้อผิดพลาดในอนาคต

สำหรับการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit) ของ สวพส. การถอดบทเรียนมีความสำคัญเป็นพิเศษ เนื่องจากเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงอย่างรวดเร็ว มีความซับซ้อน และเกี่ยวข้องกับกฎหมาย มาตรฐาน และภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงอยู่ตลอดเวลา ดังนั้น ผู้ตรวจสอบภายในจึงต้องนำผลการตรวจสอบที่ผ่านมา มาวิเคราะห์หาแนวโน้มของความเสี่ยง จุดอ่อนของระบบควบคุม และปัจจัยแห่งความสำเร็จ เพื่อยกระดับการตรวจสอบให้เป็นเชิงรุก (Proactive Audit) และสร้างคุณค่าเพิ่มให้กับองค์กร

วัตถุประสงค์ของการถอดบทเรียน

1. เพื่อรวบรวมองค์ความรู้จากการตรวจสอบด้าน IT อย่างเป็นระบบ
2. เพื่อสรุปปัจจัยที่ส่งผลต่อความสำเร็จและอุปสรรคของการตรวจสอบ
3. เพื่อพัฒนาแนวทางการตรวจสอบให้มีมาตรฐานเดียวกัน
4. เพื่อใช้เป็นฐานข้อมูล (Knowledge Base) สำหรับผู้ตรวจสอบภายในรุ่นต่อไป
5. เพื่อยกระดับการตรวจสอบจากการตรวจสอบเชิงปฏิบัติการ (Operational Audit) ไปสู่การตรวจสอบเชิงกลยุทธ์ (Strategic Audit)

Lesson 1 การกำกับดูแลด้านดิจิทัล (Digital Governance) ต้องรายงานผู้บริหารอย่างเป็นระบบ

สิ่งที่พบ:	แม้ สวพส. จะมีการดำเนินงานรายงานผลการดำเนินงานด้านดิจิทัล ทั้งนี้ยังไม่มีแนวทางการรายงานผลการดำเนินงานด้านธรรมาภิบาลและการกำกับดูแลด้านดิจิทัล (Digital Governance) ส่งผลให้ผู้บริหารไม่สามารถเห็นภาพรวมของความเสี่ยง ความก้าวหน้า และประเด็นสำคัญด้านดิจิทัลได้อย่างครบถ้วน
บทเรียนที่ได้รับ:	ผู้บริหารควรได้รับรายงานผลการดำเนินงานด้านธรรมาภิบาลและการกำกับดูแลด้านดิจิทัล (Digital Governance) หรือรายงานด้านเทคโนโลยีสารสนเทศในภาพรวมเป็นประจำ เพื่อใช้ในการตัดสินใจเชิงนโยบายและการบริหารความเสี่ยง
แนวทางพัฒนา:	• จัดทำรายงานผลการดำเนินงานด้านธรรมาภิบาลและการกำกับดูแลด้านดิจิทัล (Digital Governance) เสนอผู้บริหารที่ได้รับมอบหมายให้ดูแลเรื่องดังกล่าวอย่างสม่ำเสมอ เช่น 1 ครั้ง/ไตรมาส หรือ 1 ครั้ง/ปี • รายงานสถานะโครงการดิจิทัล ความเสี่ยงไซเบอร์ และตัวชี้วัดรัฐบาลดิจิทัลต่อผู้บริหาร

Lesson 2 PDPA ต้องเปลี่ยนจาก "การมีเอกสาร" ไปสู่ "การปฏิบัติจริง"

สิ่งที่พบ:	สวพส. มีการแต่งตั้ง DPO และคณะทำงานด้าน PDPA รวมถึงจัดทำเอกสารที่เกี่ยวข้องหลายรายการ แต่ยังขาดแนวปฏิบัติที่ชัดเจนสำหรับการจัดการเหตุละเมิดข้อมูล (Data Breach) การประเมินผลกระทบ (DPIA) และการรองรับการใช้สิทธิของเจ้าของข้อมูล
บทเรียนที่ได้รับ:	การปฏิบัติตาม PDPA ไม่ควรจำกัดอยู่เพียงการจัดทำเอกสาร แต่ต้องมีขั้นตอนการดำเนินงานที่สามารถนำไปใช้ได้จริง และมีการทดสอบความพร้อมเป็นระยะ
แนวทางพัฒนา:	• จัดทำแนวปฏิบัติกรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล และแนวปฏิบัติกรณีเจ้าของข้อมูลขอใช้สิทธิตามกฎหมาย • ประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล • ฝึกซ้อมการตอบสนองเหตุข้อมูลรั่วไหล

Lesson 3 การคุ้มครองข้อมูลต้องครอบคลุมทั้งข้อมูลอิเล็กทรอนิกส์และเอกสารกระดาษ

สิ่งที่พบ:	มาตรการด้าน PDPA ส่วนใหญ่มุ่งเน้นการควบคุมข้อมูลในระบบสารสนเทศ ขณะที่การจัดเก็บ การใช้ การโอนย้าย และการทำลายข้อมูลในรูปแบบเอกสาร (Hard Copy) ยังไม่มีระบบติดตามและสอบทานที่เป็นมาตรฐาน
บทเรียนที่ได้รับ:	การคุ้มครองข้อมูลส่วนบุคคลต้องครอบคลุมทุกสื่อ ไม่ใช่เฉพาะข้อมูลอิเล็กทรอนิกส์
แนวทางพัฒนา:	• สอบทานการปฏิบัติตามมาตรการเป็นประจำ

Lesson 4 Cyber Incident Response ต้องผ่านการซักซ้อม

สิ่งที่พบ:	หน่วยงานมีแผนตอบสนองต่อเหตุการณ์ผิดปกติ แต่ยังไม่เคยมีการซักซ้อมแผนในสถานการณ์จำลอง
บทเรียนที่ได้รับ:	แผนที่ไม่ได้รับการทดสอบ อาจไม่สามารถนำไปใช้ได้จริงเมื่อเกิดเหตุการณ์
แนวทางพัฒนา:	• จัด Tabletop Exercise หรือจัด Cyber Drill • ประเมินผลหลังการซักซ้อม (After Action Review)

Lesson 5 BCP ที่ดีต้องเริ่มจาก Business Impact Analysis (BIA)

สิ่งที่พบ:	การกำหนดค่า RTO และ RPO ยังไม่มีการวิเคราะห์ผลกระทบของแต่ละระบบต่อภารกิจหลักขององค์กรอย่างเป็นระบบ
บทเรียนที่ได้รับ:	การกำหนด RTO/RPO ต้องอ้างอิงผลการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) เพื่อให้สอดคล้องกับความสำคัญของระบบสารสนเทศแต่ละประเภท
แนวทางพัฒนา:	• จัดทำ BIA ครอบคลุมระบบสำคัญ • ทบทวน RTO/RPO เป็นประจำทุกปี

Lesson 6 แผนที่ดีต้องมีผู้รับผิดชอบและทรัพยากรที่ชัดเจน

สิ่งที่พบ:	แผนบางส่วนระบุเพียงหน่วยงานที่รับผิดชอบ แต่ไม่ได้กำหนดผู้รับผิดชอบหลักหรือทรัพยากรที่ต้องใช้ในแต่ละขั้นตอน
บทเรียนที่ได้รับ:	เมื่อเกิดเหตุฉุกเฉิน ความไม่ชัดเจนของบทบาทหน้าที่จะทำให้การตอบสนองล่าช้า
แนวทางพัฒนา:	• กำหนด Incident Owner • ระบุชื่อผู้ประสานงาน • จัดทำ Contact List

Lesson 7 ความเสี่ยงของผู้ให้บริการภายนอกเป็นความเสี่ยงขององค์กร

สิ่งที่พบ:	การประเมินผู้ให้บริการด้าน IT ยังมุ่งเน้นด้านการจัดซื้อจัดจ้างมากกว่าความมั่นคงปลอดภัยของข้อมูล
บทเรียนที่ได้รับ:	Third Party Risk Management เป็นองค์ประกอบสำคัญของ IT Governance โดยเฉพาะในยุคที่องค์กรใช้บริการ Cloud และ Outsourcing มากขึ้น
แนวทางพัฒนา:	• ประเมิน Vendor Risk • จัดทำ Security Assessment • ประเมินการปฏิบัติตาม PDPA ของผู้รับจ้าง

Lesson 8 TOR ควรสะท้อนข้อกำหนดด้าน Cybersecurity

สิ่งที่พบ:	TOR งานด้าน IT บางโครงการยังไม่ได้กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน
บทเรียนที่ได้รับ:	การควบคุมความมั่นคงปลอดภัยควรเริ่มตั้งแต่กระบวนการจัดซื้อจัดจ้าง ไม่ใช่หลังจากเริ่มใช้งานระบบแล้ว
แนวทางพัฒนา:	กำหนดความมั่นคงปลอดภัยสารสนเทศใน และการปฏิบัติตามกฎหมายใน TOR

Lesson 9 การตรวจสอบ IT ต้องเชื่อมโยงกับภารกิจขององค์กร

ความเสี่ยงด้าน IT ไม่ได้ส่งผลกระทบเฉพาะต่อระบบสารสนเทศ แต่ส่งผลโดยตรงต่อพันธกิจของ สวพส. เช่น การให้บริการข้อมูลวิชาการ การบริหารโครงการ การสนับสนุนเกษตรกรบนพื้นที่สูง และการบริหารงบประมาณ ดังนั้น การกำหนดประเด็นการตรวจสอบควรเชื่อมโยงกับความเสี่ยงของภารกิจหลัก เพื่อให้ข้อเสนอแนะสามารถสร้างคุณค่าในระดับองค์กรได้อย่างแท้จริง

Lesson 10 การตรวจสอบเชิงระบบสร้างคุณค่ามากกว่าการตรวจสอบเชิงปฏิบัติ

ข้อเสนอแนะที่มุ่งปรับปรุงโครงสร้างการกำกับดูแล กระบวนการบริหารความเสี่ยง และมาตรฐานการดำเนินงาน มีผลกระทบเชิงบวกต่อองค์กรในระยะยาวมากกว่าการแก้ไขปัญหาเฉพาะจุด เช่น การจัดทำรายงานด้าน Digital Governance การกำหนดกระบวนการ PDPA และการบูรณาการข้อกำหนดด้าน Cybersecurity ใน TOR ซึ่งช่วยยกระดับการบริหารจัดการด้านเทคโนโลยีสารสนเทศทั้งระบบ

ปัจจัยแห่งความสำเร็จ (Critical Success Factors)

1. ผู้บริหารให้การสนับสนุนการตรวจสอบและติดตามผลอย่างจริงจัง
2. หน่วยรับตรวจเปิดเผยข้อมูลและให้ความร่วมมือ
3. ผู้ตรวจสอบมีความรู้ทั้งด้าน IT และการตรวจสอบภายใน
4. ใช้แนวทาง Risk-Based IT Audit
5. มีการติดตามผลผ่านระบบ CMT อย่างต่อเนื่อง
6. มีการจัดเก็บองค์ความรู้ (Knowledge Base) จากผลการตรวจสอบ
7. มีการทบทวนและปรับปรุงแนวทางการตรวจสอบทุกปี

การนำบทเรียนไปพัฒนาแนวทางการตรวจสอบ

บทเรียนที่ได้รับจากการตรวจสอบ IT Audit ของ สวพส. ควรถูกนำไปใช้ในการปรับปรุงคู่มือและวิธีปฏิบัติงานของหน่วยตรวจสอบภายในอย่างต่อเนื่อง โดยเฉพาะการพัฒนา *Risk Assessment, Audit Program, Working Papers, Checklist และแนวทางการให้ข้อเสนอแนะ* ให้สอดคล้องกับความเสี่ยงที่เปลี่ยนแปลง รวมทั้งกฎหมายด้านดิจิทัลที่เกี่ยวข้อง

ภาคผนวก

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

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 Evidence

7 การสรุปผลการตรวจสอบ

1. **Condition** (สภาพที่พบ)
2. **Criteria** (เกณฑ์อ้างอิง)
3. **Cause** (สาเหตุ)
4. **Effect** (ผลกระทบ)
5. **Recommendation** (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

11 การติดตามผล (Follow-up)

CMT

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 Objective Paper ในการปฏิบัติงาน
4. อ้างอิงกฎหมายและมาตรฐานสากลในการประเมิน
5. CMT ติดตามผลระบบ CMT จนกว่าประเด็นจะได้รับการแก้ไข
6. จัดทำ AAR และพัฒนาองค์ความรู้หลังทุกภารกิจ
7. ทบทวนและปรับปรุงคู่มือทุกปี ให้สอดคล้องกับกฎหมาย เทคโนโลยี และความเสี่ยง

หน่วยตรวจสอบภายใน - สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)
ประเมินความเสี่ยง การตรวจสอบเทคโนโลยีสารสนเทศ (IT Audit)
ปีงบประมาณ พ.ศ. 2569

- **วัตถุประสงค์**
  1) ระบุความเสี่ยงสำคัญด้านเทคโนโลยีสารสนเทศของ สวพส.
  2) จัดลำดับความสำคัญของประเด็นที่จะตรวจสอบ
  3) กำหนดขอบเขตและความลึกของการตรวจสอบ (Audit Scope & Depth)
  4) สนับสนุนแนวทางการตรวจสอบเชิงความเสี่ยง (Risk-based Audit)

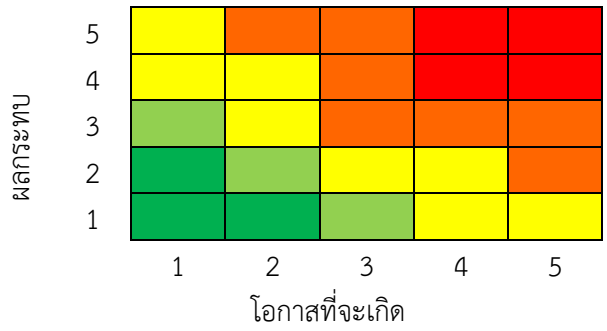
- **ระบุความเสี่ยงของการดำเนินงานโครงการ**

กิจกรรม	เหตุการณ์/ปัจจัยความเสี่ยง	ระดับความเสี่ยง		
		โอกาส	ผลกระทบ	ระดับ
1. การดำเนินการด้านเทคโนโลยีสารสนเทศของ สวพส. เป็นไปตามกฎหมาย มาตรฐาน ประกาศ และแนวทางที่เกี่ยวข้อง	1. นโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศไม่สอดคล้องกับกฎหมาย มาตรฐาน หรือประกาศที่มีการปรับปรุงล่าสุด	1	4	4 (ต่ำ)
	2. ไม่มีนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ที่เป็นทางการและเป็นปัจจุบัน	1	5	5 (ต่ำ)
	3. ไม่ได้แต่งตั้งหรือกำหนดบทบาทหน้าที่ของผู้ควบคุมข้อมูล /ผู้ประมวลผลข้อมูล /DPO อย่างชัดเจน	1	5	5 (ต่ำ)
	4. ไม่ได้จัดทำหรือปรับปรุงทะเบียนกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) ให้เป็นปัจจุบัน	2	4	8 (ต่ำ)
	5. ไม่มีมาตรการทำลายข้อมูลเมื่อพ้นระยะเวลาที่กำหนด	2	5	10 (ปานกลาง)
2. การรักษาความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลระบบสารสนเทศของ สวพส.	1. ระบบสารสนเทศของ สวพส. ถูกโจมตีจากมัลแวร์ แรนซัมแวร์ หรือภัยคุกคามไซเบอร์รูปแบบอื่น	5	2	10 (ปานกลาง)
	2. เกิดการรั่วไหลหรือถูกเข้าถึงข้อมูลโดยมิชอบจากการโจมตีทางไซเบอร์	5	2	10 (ปานกลาง)
	3. ไม่มีโครงสร้างการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Governance) ที่ชัดเจนและเป็นทางการ	1	5	5 (ต่ำ)

กิจกรรม	เหตุการณ์/ปัจจัยความเสี่ยง	ระดับความเสี่ยง		
		โอกาส	ผลกระทบ	ระดับ
	4. ไม่มีนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) ที่เป็นปัจจุบัน	1	5	5 (ต่ำ)
	5. ไม่มีการจัดให้มีการสอบทาน Log ด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ	1	5	5 (ต่ำ)
	6. ไม่มีแผนตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ	1	5	5 (ต่ำ)
	7. การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างล่าช้า หรือไม่เป็นไปตามขั้นตอนที่กำหนด	2	5	10 (ปานกลาง)
	8. บุคลากรของ สวพส. ขาดความรู้ ความตระหนักและทักษะด้านความมั่นคงปลอดภัยไซเบอร์	2	5	10 (ปานกลาง)
3. แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP)	1. ไม่มีการจัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศอย่างเป็นทางการ	1	5	5 (ต่ำ)
	2. แผน BCP ไม่ครอบคลุมระบบสารสนเทศหรือกระบวนงานที่มีความสำคัญต่อภารกิจหลัก	2	5	10 (ปานกลาง)
	3. การกำหนดค่า RTO และ RPO ไม่เหมาะสมกับระดับผลกระทบของแต่ละระบบ	2	4	8 (ต่ำ)
	4. ไม่มีการซักซ้อมแผน BCP ตามรอบระยะเวลาที่กำหนด	1	5	5 (ต่ำ)
	5. ไม่สามารถกู้คืนข้อมูลหรือระบบงานจากข้อมูลสำรองได้เมื่อเกิดเหตุขัดข้อง	1	5	5 (ต่ำ)
	6. บุคลากรที่เกี่ยวข้องไม่ทราบบทบาทหน้าที่และขั้นตอนการปฏิบัติตามแผน BCP	3	5	15 (สูง)
	7. แผน BCP ไม่ได้รับการทบทวนและปรับปรุงให้สอดคล้องกับสภาพแวดล้อมที่เปลี่ยนแปลงไป	1	5	5 (ต่ำ)
4. การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls)	1. ผู้ใช้งานระบบได้รับสิทธิในการเข้าถึงข้อมูลหรือระบบงานเกินกว่าความจำเป็นตามหน้าที่รับผิดชอบ	2	5	10 (ปานกลาง)
	2. ไม่ได้เพิกถอนสิทธิการเข้าถึงระบบของบุคลากรที่พ้นสภาพจากการปฏิบัติงานแล้ว	1	5	5 (ต่ำ)
	3. บัญชีผู้ใช้งานที่มีสิทธิสูง (High Privileged ID) *ไม่ได้รับการควบคุม*และกำกับดูแลอย่างเหมาะสม	1	5	5 (ต่ำ)
	4. มีการเปลี่ยนแปลงระบบงานหรือโปรแกรมโดยไม่ได้รับการอนุมัติล่วงหน้าตามขั้นตอนที่กำหนด	3	5	15 (สูง)

กิจกรรม	เหตุการณ์/ปัจจัยความเสี่ยง	ระดับความเสี่ยง		
		โอกาส	ผลกระทบ	ระดับ
	5. การตั้งค่าระบบสารสนเทศไม่เป็นไปตามมาตรฐานด้านความมั่นคงปลอดภัยที่กำหนดไว้	1	5	5 (ต่ำ)
	6. ไม่มีการสำรองข้อมูลตามรอบระยะเวลาที่กำหนด	1	5	5 (ต่ำ)
	7. ไม่สามารถกู้คืนข้อมูลจากระบบสำรองได้เนื่องจากไม่ได้ทดสอบการกู้คืนข้อมูลเป็นประจำ	2	5	10 (ปานกลาง)
	8. ไม่มีการจัดเก็บหรือบริหารจัดการ Log ระบบสารสนเทศอย่างเหมาะสม	1	5	5 (ต่ำ)
	9. มาตรการควบคุมการเข้าถึงห้องแม่ข่าย (Server Room) ไม่เพียงพอ	1	5	5 (ต่ำ)
	10. ระบบสารสนเทศใหม่ไม่ได้ผ่านกระบวนการทดสอบการใช้งาน (UAT) ก่อนนำไปใช้งานจริง	1	5	5 (ต่ำ)
	11. การใช้บริการจากผู้ให้บริการภายนอกโดยไม่มีข้อตกลงระดับการให้บริการ (SLA) ที่ชัดเจน	3	5	15 (สูง)

- **การกำหนดเกณฑ์การประเมินความเสี่ยง**



20-25	ระดับสูงมาก	ตรวจสอบเชิงลึก ประเด็นเร่งด่วน กำหนดมาตรการควบคุมเพิ่มเติม
15-19	ระดับสูง	กำหนดเป็นประเด็นสำคัญในการตรวจสอบ จัดทำแผนปรับปรุงและติดตามผลใกล้ชิด
9-14	ระดับปานกลาง	ตรวจสอบตามตัวอย่าง และติดตามความคืบหน้าในการปรับปรุง
4-8	ระดับต่ำ	ตรวจสอบในภาพรวม และเฝ้าระวัง
1-3	ระดับต่ำมาก	เฝ้าระวังตามปกติ

1) โอกาสที่จะเกิด (Likelihood)

ระดับคะแนน		รายละเอียด
5	สูงมาก	โอกาสเกิดขึ้นเป็นประจำ หรือเคยเกิดขึ้นอย่างน้อย 5 ครั้ง ในช่วง 1ปีที่ผ่านมา
4	สูง	มีโอกาสเกิดขึ้นสูง หรือเคยเกิดขึ้นอย่างน้อย 3 ครั้ง ในช่วง 1 ปีที่ผ่านมา
3	ปานกลาง	มีโอกาสเกิดขึ้นบางครั้งขึ้นอยู่กับสภาพแวดล้อม หรือเคยเกิดขึ้นอย่างน้อย 1 ครั้ง ในช่วง 1 ปีที่ผ่านมา
2	ต่ำ	มีโอกาสเกิดขึ้นต่ำ หรือเคยเกิดขึ้นอย่างน้อย 1 ครั้ง ในช่วง 2 ปีที่ผ่านมา
1	ต่ำมาก	มีโอกาสเกิดขึ้น 0 ครั้ง เนื่องจากมีมาตรการควบคุมที่เข้มแข็งและเหมาะสม

2) ผลกระทบ (Impact)

ระดับคะแนน		รายละเอียด
5	สูงมาก	ส่งผลกระทบต่อภารกิจหลักของ สวพส. อย่างมีนัยสำคัญ ระบบหลักหยุดชะงักทั้งองค์กร เกิดการรั่วไหลของข้อมูลร้ายแรง หรือเป็นการฝ่าฝืนกฎหมายอย่างมีสาระสำคัญ เสื่อมเสียชื่อเสียงองค์กร
4	สูง	ระบบหยุดชะงักเป็นระยะเวลานาน ส่งผลกระทบต่อการให้บริการ เสื่อมเสียชื่อเสียงองค์กร
3	ปานกลาง	ส่งผลกระทบต่อการให้บริการบางส่วน ระบบทำงานล่าช้า หรือจำเป็นต้องใช้ทรัพยากรจำนวนมากในการแก้ไข
2	ต่ำ	ส่งผลกระทบในระดับเล็กน้อย สามารถแก้ไขได้ภายในหน่วยงาน โดยไม่กระทบต่อภาพรวมขององค์กร
1	ต่ำมาก	ไม่ส่งผลกระทบต่อการดำเนินงานหรือการให้บริการของ สวพส.

แผนการปฏิบัติงานการตรวจสอบ (Engagement Audit Plan)
เทคโนโลยีสารสนเทศ (IT Audit)
หน่วยตรวจสอบภายใน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

หน่วยรับตรวจ : ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
ชื่อแผนงาน/โครงการ : เทคโนโลยีสารสนเทศ (IT Audit)

วัตถุประสงค์ในการตรวจสอบ :

1. เพื่อให้มั่นใจว่าการดำเนินการด้านเทคโนโลยีสารสนเทศของ สวพส. เป็นไปตามกฎหมาย มาตรฐาน ประกาศ และแนวทางที่เกี่ยวข้อง
2. เพื่อให้มั่นใจว่าการรักษาความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลระบบสารสนเทศของ สวพส. อยู่ในระดับที่เหมาะสม
3. เพื่อให้มั่นใจว่าแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ สามารถรองรับเหตุขัดข้องและภัยคุกคามที่สำคัญ
4. เพื่อให้มั่นใจว่าการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls) มีประสิทธิผลเพียงพอ และเหมาะสม
5. เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุ/ข้อจำกัด ในการปฏิบัติงาน รวมทั้งให้ข้อเสนอแนะ/ข้อสังเกตในการแก้ไขปรับปรุงเพื่อการปฏิบัติงานให้มีประสิทธิภาพ

ประเด็นการตรวจสอบ :

1. การดำเนินงานด้านเทคโนโลยีสารสนเทศของ สวพส. เป็นไปตามกฎหมาย ระเบียบ มาตรฐานและแนวปฏิบัติที่เกี่ยวข้อง
2. ความครบถ้วนของนโยบาย และแนวปฏิบัติด้านเทคโนโลยีสารสนเทศของ สวพส. ว่ามีความสอดคล้องกับกฎหมาย ข้อบังคับ และกฎระเบียบที่เกี่ยวข้อง
3. แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ
4. ความมีประสิทธิผล ความเพียงพอและเหมาะสม ของการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (ITGC)

ขอบเขตการตรวจสอบ :

1. สอบทานการดำเนินงานด้านเทคโนโลยีสารสนเทศของ สวพส. เป็นไปตามกฎหมาย ระเบียบ มาตรฐานและแนวปฏิบัติที่เกี่ยวข้อง
2. สอบทานความครบถ้วนของนโยบาย และแนวปฏิบัติด้านเทคโนโลยีสารสนเทศของ สวพส. ว่ามีความสอดคล้องกับกฎหมาย ข้อบังคับ และกฎระเบียบที่เกี่ยวข้อง
3. สอบทานการควบคุมปลอดภัยทางกายภาพ (Physical Security)
4. สอบทานแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ และผลการซักซ้อมตามแผน
5. ประเมินความมีประสิทธิผล ความเพียงพอและเหมาะสมของการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ
6. สัมภาษณ์เจ้าหน้าที่ที่เกี่ยวข้อง

เอกสารประกอบการตรวจสอบ :

1. นโยบายและแนวปฏิบัติในการดำเนินงานด้านเทคโนโลยีสารสนเทศของ สวพส.
2. แผนการบริหารความต่อเนื่องด้าน IT (BCP) และรายงานการซักซ้อมแผน BCP
3. รายงานเหตุการณ์ด้านความปลอดภัยสารสนเทศ
4. รายงานรัฐบาลดิจิทัล (DG) ปีงบประมาณ พ.ศ. 2568
5. โครงสร้างและการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Governance)
6. แผนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)
7. สัญญาและข้อตกลงการให้บริการของผู้ให้บริการภายนอก ปีงบประมาณ พ.ศ. 2568
8. ทะเบียนบัญชีสิทธิผู้ใช้งานที่มีสิทธิสูง (High Privileged ID Restriction)
9. แบบฟอร์มการร้องขอเปลี่ยนแปลงที่ได้รับการอนุมัติ ปีงบประมาณ พ.ศ. 2568
10. รายงานการทดสอบการกู้คืนข้อมูล ปีงบประมาณ พ.ศ. 2568
11. เอกสารอื่น ๆ ที่เกี่ยวข้อง

ความรู้/ทักษะที่ใช้ในการตรวจสอบ :

ความรู้ที่ใช้ในการตรวจสอบ	ทักษะที่ใช้ในการตรวจสอบ
1. กฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง	1. การวิเคราะห์เปรียบเทียบ
2. IT GOVERNANCE	2. การสื่อสาร
3. CYBERSECURITY	3. การแก้ไขปัญหา
4. การควบคุมภายใน และการบริหารความเสี่ยง	4. การทำงานเป็นทีม
	5. การบริหารเวลา
	6. การใช้งานคอมพิวเตอร์
	7. จริยธรรมและธรรมาภิบาล

กฎระเบียบที่เกี่ยวข้อง :

1. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
2. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม
3. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
4. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม
5. พระราชกฤษฎีการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549
6. มาตรฐานรัฐบาลดิจิทัล
7. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่งคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และที่แก้ไขเพิ่มเติม
8. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555
9. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) ปีงบประมาณ พ.ศ. 2565
10. ประกาศสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

11. ประกาศสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

ระยะเวลาในการตรวจสอบ : ตั้งแต่วันที่ 16 ธันวาคม 2568 – 15 มกราคม 2569 (20 วันทำการ)

ผู้รับผิดชอบในการตรวจสอบ :

1. นางสาวรินทิพย์ ต่อปัญญาเรือง หัวหน้าหน่วยตรวจสอบภายใน
2. นางพีรญา เตชะรัง เจ้าหน้าที่ตรวจสอบภายใน 5
3. นายกิตติกร ชมภูแก้ว เจ้าหน้าที่ปฏิบัติงานตรวจสอบภายใน

แนวทางการตรวจสอบ (Audit Program)
เทคโนโลยีสารสนเทศ (IT Audit)
หน่วยตรวจสอบภายใน
สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

ช่วงวันที่เข้าตรวจสอบ : ตั้งแต่วันที่ 16 ธันวาคม 2568 – 15 มกราคม 2569 (20 วันทำการ)

วัตถุประสงค์ :

1. เพื่อให้มั่นใจว่าการดำเนินการด้านเทคโนโลยีสารสนเทศของ สวพส. เป็นไปตามกฎหมาย มาตรฐาน ประกาศ และแนวทางที่เกี่ยวข้อง
2. เพื่อให้มั่นใจว่าการรักษาความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลระบบสารสนเทศของ สวพส. อยู่ในระดับที่เหมาะสม
3. เพื่อให้มั่นใจว่าแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ สามารถรองรับเหตุขัดข้อง และภัยคุกคามที่สำคัญ
4. เพื่อให้มั่นใจว่าการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls) มีประสิทธิผล เพียงพอ และเหมาะสม
5. เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุ/ข้อจำกัด ในการปฏิบัติงาน รวมทั้งให้ข้อเสนอแนะ/ข้อสังเกตในการแก้ไขปรับปรุงเพื่อการปฏิบัติงานให้มีประสิทธิภาพ

ลำดับ	แนวทางการตรวจสอบ	ขอบเขตการสุ่มตัวอย่าง	วิธีการตรวจสอบ	ผู้ตรวจสอบ	เวลาที่ใช้ (วัน)		เอกสารอ้างอิง
					ประมาณ	จริง	กระดาษทำการ
1	การดำเนินการด้านเทคโนโลยีสารสนเทศของ สวพส. เป็นไปตามกฎหมาย มาตรฐาน ประกาศ และแนวทางที่เกี่ยวข้อง	**Audit Tools:** - Checklist **Audit Technique:** - สัมภาษณ์ - ตรวจสอบเอกสารหลักฐานที่เกี่ยวข้อง - Walkthrough **Audit Evidence:** - นโยบายและแนวปฏิบัติด้าน IT - นโยบายและมาตรการคุ้มครองข้อมูลส่วนบุคคล - รายงานรัฐบาลดิจิทัล (DG)	ตรวจสอบความสอดคล้องของการดำเนินงานด้านเทคโนโลยีสารสนเทศกับกฎหมาย ระเบียบ มาตรฐานรัฐบาลดิจิทัล ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ และนโยบายภายในของ สวพส. โดยเน้นการประเมินเชิง Compliance และการวิเคราะห์ช่องว่าง (Gap Analysis) รวบรวมกฎหมาย มาตรฐาน และประกาศที่เกี่ยวข้องทั้งหมด 1) ตรวจสอบการจัดทำนโยบาย และแผนพัฒนาดิจิทัล 2) ตรวจสอบการดำเนินงานด้าน PDPA ประเด็น Privacy Management, Data Management,	รินทิพย์ (PDPA) พีรญา (รัฐบาลดิจิทัล)			CA-69-01-01-1(PDPA) CA-69-01-01-2(DGA)

ลำดับ	แนวทางการตรวจสอบ	ขอบเขตการสุ่มตัวอย่าง	วิธีการตรวจสอบ	ผู้ตรวจสอบ	เวลาที่ใช้ (วัน)		เอกสารอ้างอิง
					ประมาณ	จริง	กระดาษทำการ
		- รายงานเหตุการณ์ละเมิดข้อมูล	Data Security, Third Party, Incident Management 3) สุ่มกระบวนงานที่ใช้ข้อมูลส่วนบุคคลอย่างน้อย 1 กระบวนงาน 4) สุ่มตรวจสอบหลักฐานการขอความยินยอมและการแจ้ง Privacy Notice 5) ตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศของ สวพส. เป็นไปตามข้อกำหนดของมาตรฐานรัฐบาลดิจิทัล ประกาศ/แนวทางของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ 6) วิเคราะห์ช่องว่างการไม่ปฏิบัติตาม และจัดระดับความเสี่ยง 7) สัมภาษณ์ผู้รับผิดชอบด้าน IT และ PDPA 8) สรุปข้อค้นพบและข้อเสนอแนะเชิงระบบ				
2	การรักษาความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลระบบสารสนเทศของ สวพส.	**Audit Tools:** - Checklist **Audit Technique:** **-** สัมภาษณ์ - ตรวจสอบเอกสารหลักฐาน - Walkthrough **Audit Evidence:** - นโยบายความมั่นคงปลอดภัยสารสนเทศ - โครงสร้าง IT Governance - รายงานเหตุการณ์ไซเบอร์ - รายงานทดสอบเจาะระบบ (ถ้ามี)	ประเมินความเพียงพอของมาตรการด้าน Cybersecurity และ IT Governance ครอบคลุมการป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคาม รวมถึงโครงสร้างการกำกับดูแลด้าน IT ตรวจสอบนโยบายความมั่นคงปลอดภัยว่าทันสมัยหรือไม่ 1) ตรวจสอบโครงสร้างการกำกับดูแลด้าน Cybersecurity 2) สุ่มเหตุการณ์ไซเบอร์ย้อนหลัง 6–12 เดือน 3) ตรวจสอบขั้นตอนการแจ้งเหตุและการตอบสนอง 4) วิเคราะห์ความเสี่ยงจากจุดอ่อนที่พบ	กิตติกร			CA-69-01-02

ลำดับ	แนวทางการตรวจสอบ	ขอบเขตการสุ่มตัวอย่าง	วิธีการตรวจสอบ	ผู้ตรวจสอบ	เวลาที่ใช้ (วัน)		เอกสารอ้างอิง
					ประมาณ	จริง	กระดาษทำการ
		- แผนตอบสนองเหตุการณ์	5) สรุปข้อค้นพบและข้อเสนอแนะเชิงป้องกันและแก้ไข				
3	แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP)	**Audit Tools:** - Checklist **Audit Technique:** - สัมภาษณ์ - Document Review - Walkthrough **Audit Evidence:** - แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (BCP) - รายงานการซักซ้อมแผน - รายงานการทดสอบกู้คืนข้อมูล - บันทึกการปรับปรุงแผน	ประเมินความครบถ้วนและความพร้อมของแผน BCP การกำหนด RTO/RPO และผลการซักซ้อมแผนให้สามารถรองรับเหตุขัดข้องและภัยคุกคามที่สำคัญ 1) ตรวจสอบความครบถ้วนของแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ 2) เปรียบเทียบ BCP กับผล Impact Analysis 3) ตรวจสอบการกำหนด RTO/RPO 4) ตรวจสอบหลักฐานการซักซ้อมแผนย้อนหลัง 1 ปี 5) สัมภาษณ์ผู้รับผิดชอบแผน 6) ประเมินความพร้อมจริงเมื่อเกิดเหตุ 7) วิเคราะห์ช่องว่าง และเสนอแนะแนวทางปรับปรุงแผน 8) สรุปข้อค้นพบและข้อเสนอแนะ	พีรญา			CA-69-01-03
4	การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls)	**Audit Tools:** - Checklist **Audit Technique:** - สัมภาษณ์ - Observation **Audit Evidence:**	ประเมินความเพียงพอและประสิทธิผลของ IT General Controls 15 ประเด็น 1) โครงสร้างและการกำกับดูแลด้านเทคโนโลยีสารสนเทศ 2) การบริหารจัดการผู้ให้บริการภายนอก 3) การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ 4) การบริหารจัดการการตั้งค่าระบบ และการควบคุมการตั้งค่ารหัสผ่าน 5) การบริหารจัดการบัญชีผู้ใช้งาน	รินทิพย์ รินทิพย์ พีรญา รินทิพย์ รินทิพย์			CA-69-01-04

ลำดับ	แนวทางการตรวจสอบ	ขอบเขตการสุ่มตัวอย่าง	วิธีการตรวจสอบ	ผู้ตรวจสอบ	เวลาที่ใช้ (วัน)		เอกสารอ้างอิง
					ประมาณ	จริง	กระดาษทำการ
			6) การจำกัดสิทธิการเข้าถึงผู้ใช้งานที่มีสิทธิสูง (HPID) และการควบคุมผู้ใช้งานระบบ	รินทิพย์			
			7) การสอบทาน Log ด้านความมั่นคงปลอดภัย	กิตติกร			
			8) การตรวจสอบช่องโหว่และทดสอบเจาะระบบ	พีรญา			
			9) การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา	กิตติกร			
			10) การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์	กิตติกร			
			11) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม และความปลอดภัยของอุปกรณ์ปลายทาง	กิตติกร			
			12) การบริหารจัดการการเปลี่ยนแปลง	พีรญา			
			13) การสำรองข้อมูล (Data Backup) และการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ	กิตติกร			
			14) การบริหารขีดความสามารถของระบบ	พีรญา			
			15) การจัดหาและการพัฒนาระบบ	พีรญา			
5	จัดทำรายงานผลการตรวจสอบ	-	1) สรุปและร่างรายงานผลการตรวจสอบ โดยข้อเสนอแนะมีความเหมาะสมกับบริบทของ สวพส. และลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT) หรือเพิ่มประสิทธิภาพการดำเนินงาน รวมถึงมีผลต่อการเปลี่ยนแปลงเชิงโครงสร้างหรือแนวทางการดำเนินงานด้านเทคโนโลยีสารสนเทศ (IT) เสนอหัวหน้าหน่วยตรวจสอบภายใน	พีรญา			
			2) ประชุมปิดตรวจร่วมกับหน่วยรับตรวจ				
			3) เสนอรายงานผลการตรวจสอบต่อ ผอ. สวพส.				

ลำดับ	แนวทางการตรวจสอบ	ขอบเขตการสุ่มตัวอย่าง	วิธีการตรวจสอบ	ผู้ตรวจสอบ	เวลาที่ใช้ (วัน)		เอกสารอ้างอิง
					ประมาณ	จริง	กระดาษทำการ
			4) รายงานผลการตรวจสอบต่อคณะกรรมการตรวจสอบ 5) ติดตามการดำเนินตามข้อเสนอแนะของหน่วยรับตรวจผ่านระบบ CMT และรายงานความก้าวหน้า 6) จัดทำแนวทางการปฏิบัติงานตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT) สามารถใช้เป็นต้นแบบ (Best Practice) ของหน่วยตรวจสอบภายใน สวพส.				

กระดาษทำการ	การตรวจสอบการปฏิบัติตามกฎระเบียบ (Compliance Audit)
หน่วยตรวจสอบภายใน สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)	การตรวจสอบเทคโนโลยีสารสนเทศ (IT Audit)
วันที่จัดทำ: วันที่..... มกราคม 2569	**เรื่อง** การดำเนินการด้านเทคโนโลยีสารสนเทศของ สวพส. เป็นไปตามกฎหมาย มาตรฐาน ประกาศและแนวทางที่เกี่ยวข้อง
หน่วยรับตรวจ: ศูนย์ข้อมูล สำนักยุทธศาสตร์และแผน	**รหัส** CA-69-01-01

วัตถุประสงค์การตรวจสอบ

1. เพื่อให้มั่นใจว่าการดำเนินงานด้านเทคโนโลยีสารสนเทศของ สวพส.เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ ประกาศ และแนวทางปฏิบัติที่เกี่ยวข้อง
2. เพื่อให้มั่นใจว่านโยบาย ระเบียบ และแนวปฏิบัติด้านเทคโนโลยีสารสนเทศของ สวพส. มีการจัดทำอย่างเป็นทางการ ได้รับการอนุมัติจากผู้มีอำนาจและมีการทบทวนปรับปรุงให้เป็นปัจจุบัน สอดคล้องกับการเปลี่ยนแปลงของกฎหมายและเทคโนโลยี
3. เพื่อให้ข้อเสนอแนะเชิงปรับปรุงในการยกระดับการกำกับดูแล การควบคุมภายใน และการบริหารจัดการด้านเทคโนโลยีสารสนเทศของ สวพส. ให้สอดคล้องกับกรอบธรรมาภิบาลดิจิทัลและแนวปฏิบัติที่ดี

ลำดับ	ประเด็นการตรวจสอบ	ผลการตรวจสอบ		เอกสารหลักฐานที่เกี่ยวข้อง	หมายเหตุ
		มี	ไม่มี		
1	**ธรรมาภิบาลและการกำกับดูแลด้านดิจิทัล (Digital Governance)**				
	1.1 มีการกำหนดโครงสร้างการกำกับดูแลด้านรัฐบาลดิจิทัลอย่างเป็นทางการ				
	1.2 มีคำสั่งแต่งตั้งคณะทำงาน/ผู้รับผิดชอบด้านดิจิทัล				
	1.3 มีการกำหนดบทบาทหน้าที่ผู้บริหารด้านดิจิทัลชัดเจน				
	1.4 มีการกำหนดนโยบายด้านรัฐบาลดิจิทัล				
	1.5 มีการรายงานผลการดำเนินงานด้านดิจิทัลต่อผู้บริหารระดับสูง				
2	**กลยุทธ์และแผนพัฒนา**				
	2.1 มีการจัดทำแผนพัฒนาดิจิทัลและได้รับการอนุมัติ				
	2.2 แผนดิจิทัลมีความเชื่อมโยงกับยุทธศาสตร์และภารกิจหลักของ สวพส.				
	2.3 มีการกำหนดเป้าหมายและตัวชี้วัดด้านดิจิทัลอย่างชัดเจน				
	2.4 มีการทบทวนและปรับปรุงแผนอย่างน้อยปีละ 1 ครั้ง				
	2.5 มีการติดตามและรายงานผลการดำเนินงานตามแผน				
3	**การบริหารจัดการข้อมูลภาครัฐ**				
	3.1 มีนโยบายและแนวปฏิบัติด้านธรรมาภิบาลข้อมูล				
	3.2 กำหนด Data Owner / Data Steward ครบถ้วน				
	3.3 มีการจัดชั้นข้อมูล (Data Classification)				
	3.4 มีมาตรฐานคุณภาพข้อมูล (Data Quality)				
	3.5 ข้อมูลสามารถนำไปใช้ประโยชน์และเชื่อมโยงระหว่างหน่วยงาน				

4	**การคุ้มครองข้อมูลส่วนบุคคลและความโปร่งใส**				
	4.1 มีการแต่งตั้ง DPO และกำหนดบทบาทหน้าที่ชัดเจน				
	4.2 มี Privacy Notice ครบถ้วนตาม PDPA				
	4.3 มีทะเบียนกิจกรรมประมวลผลข้อมูล (ROPA)				
	4.4 มีมาตรการรองรับสิทธิของเจ้าของข้อมูล				
	4.5 มีการกำหนดแผนและขั้นตอนการจัดการเหตุละเมิดข้อมูลส่วนบุคคล				
5	**ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)**				
	5.1 มีนโยบายความมั่นคงปลอดภัยไซเบอร์				
	5.2 มีการประเมินความเสี่ยงด้าน Cybersecurity				
	5.3 มีมาตรการควบคุม/ป้องกันด้านเทคนิคและการเข้าถึงระบบ				
	5.4 มีการจัดทำแผนรับมือเหตุการณ์ฉุกเฉิน (Incident Response Plan)				
	5.5 มีการทดสอบ/ซักซ้อมแผนรับมือภัยไซเบอร์				
6	**เทคโนโยลีและการควบคุมทั่วไปด้าน IT (ITGC)**				
	6.1 มีการควบคุมการเข้าถึงระบบตามบทบาทหน้าที่				
	6.2 มีการบริหารจัดการการเปลี่ยนแปลงระบบ				
	6.3 มีระบบสำรองข้อมูลและการกู้คืน				
	6.4 มีแผน BCP ด้านเทคโนโลยีสารสนเทศ				
	6.5 มีการทดสอบแผน BCP				
7	**การให้บริการดิจิทัลภาครัฐ**				
	7.1 มีบริการดิจิทัลที่ตอบสนองภารกิจหลัก				
	7.2 การออกแบบบริการยึดประชาชน/ผู้ใช้เป็นศูนย์กลาง				
	7.3 มีการกำหนดตัวชี้วัดด้านการให้บริการดิจิทัล				
	7.4 มีการวัดและประเมินความพึงพอใจผู้ใช้งาน				
8	**การพัฒนาศักยภาพบุคลากรดิจิทัล**				
	8.1 มีการจัดทำแผนพัฒนาทักษะดิจิทัลบุคลากร				
	8.2 บุคลากร สวพส. ได้รับการอบรมด้าน IT และ Cybersecurity				
	8.3 มีการส่งเสริมวัฒนธรรมการทำงานแบบดิจิทัล				

กระดาษทำการ

หน่วยตรวจสอบภายใน สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

วันที่จัดทำ: วันที่... เดือน กุมภาพันธ์ 2569

หน่วยรับตรวจ: ศูนย์ข้อมูล สำนักยุทธศาสตร์และแผน

การตรวจสอบการปฏิบัติตามกฎระเบียบ (Compliance Audit)	
การตรวจสอบเทคโนโลยีสารสนเทศ (IT Audit)	
เรื่อง	การดำเนินการด้านเทคโนโลยีสารสนเทศของ สวพส. เป็นไปตามกฎหมาย มาตรฐาน ประกาศ และแนวทางที่เกี่ยวข้อง
รหัส	CA-69-01-01

วัตถุประสงค์การตรวจสอบ

1. เพื่อให้มั่นใจว่าการดำเนินงานด้านเทคโนโลยีสารสนเทศของ สวพส.เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ ประกาศ และแนวทางปฏิบัติที่เกี่ยวข้อง
2. เพื่อให้มั่นใจว่านโยบาย ระเบียบ และแนวปฏิบัติด้านเทคโนโลยีสารสนเทศของ สวพส. มีการจัดทำอย่างเป็นทางการ ได้รับการอนุมัติจากผู้มีอำนาจและมีการทบทวน ปรับปรุงให้เป็นปัจจุบัน สอดคล้องกับการเปลี่ยนแปลงของกฎหมายและเทคโนโลยี
3. เพื่อให้ข้อเสนอแนะเชิงปรับปรุงในการยกระดับการกำกับดูแล การควบคุมภายใน และการบริหารจัดการด้านเทคโนโลยีสารสนเทศของ สวพส. ให้สอดคล้องกับกรอบธรรมาภิบาลดิจิทัลและแนวปฏิบัติที่ดี

ลำดับ	ประเด็นการตรวจสอบ	ผลการตรวจสอบ		เอกสารหลักฐานที่เกี่ยวข้อง	หมายเหตุ
		มี	ไม่มี		
1	PRIVACY MANAGEMENT				
	การกำกับดูแล				
	1 เอกสารกำหนดหน้าที่ความรับผิดชอบของคณะกรรมการที่รับผิดชอบในการคุ้มครองข้อมูลส่วนบุคคล				
	DPO				
	2 มีการแต่งตั้ง DPO ที่มีความรู้ความสามารถ และเป็นอิสระ				
	3 DPO ได้รับอำนาจและงบประมาณในการปฏิบัติงาน				
	นโยบายคุ้มครองข้อมูลส่วนบุคคล				
	4 มีการจัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล อนุมัติ และสื่อสารอย่างเหมาะสม				
	PRIVACY NOTICE				
	5 มีการจัดทำ PRIVACY NOTICE สื่อสารไปยังเจ้าของข้อมูลส่วนบุคคล				
	การอบรมและการตระหนักรู้				
	6 มีการอบรมเพื่อสร้างความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคล				
2	DATA MANAGEMENT				
	การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล				
	1 มีการจัดทำนโยบายการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล				
	2 มีการจัดทำเอกสารการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล				
	บันทึกรายการประมวลผลข้อมูล				
	3 มีการจัดทำ ROPA				
	การจัดการคำร้องขอของเจ้าของข้อมูล				
	4 มีแนวปฏิบัติการจัดการคำร้องขอของเจ้าของข้อมูล				
	นโยบายของระยะเวลาการเก็บรักษาและลบข้อมูลส่วนบุคคล				
	5 มีการจัดทำนโยบายของระยะเวลาการเก็บและลบข้อมูลส่วนบุคคล				
	การสอบทานการลบข้อมูล				

	6 มีแผนและแนวทางในการลบข้อมูลเป็นประจำ				
	ระบบติดตามระยะเวลาการเก็บรักษา				
	7 มีกระบวนการ/ระบบในการติดตามระยะเวลาการเก็บรักษา				
3	DATA SECURITY				
	นโยบายการรักษาความปลอดภัยข้อมูลส่วนบุคคล				
	1 มีการจัดทำนโยบายการรักษาความปลอดภัยข้อมูลส่วนบุคคล				
	การตั้งค่าความปลอดภัย				
	2 มีการตั้งค่าความปลอดภัยให้สอดคล้องกับนโยบายเพื่อปกป้องการเข้าถึงข้อมูลส่วนบุคคล				
	การกำหนดสิทธิการเข้าถึงข้อมูล				
	3 มีการจัดทำ User Authorization Matrix และสอบทานเป็นประจำ				
	การร้องขอการเข้าถึงข้อมูล				
	4 การอนุมัติการสร้างผู้ใช้งาน				
	5 การให้สิทธิผู้ใช้งานเป็นไปตามนโยบายการกำหนดสิทธิการเข้าถึงข้อมูล				
	การระงับสิทธิการเข้าถึงข้อมูล				
	6 มีกระบวนการระงับสิทธิผู้ใช้งานอย่างทันท่วงที				
	การสอบทานสิทธิผู้ใช้งาน				
	7 มีการสอบทานสิทธิการเข้าถึงของผู้ใช้งานเป็นประจำอย่างน้อยปีละครั้ง				
	การเข้ารหัสข้อมูล				
	8 มีการจัดทำนโยบายการเข้ารหัสข้อมูล				
	9 ข้อมูลที่สำคัญควรได้รับการเข้ารหัสในการจัดเก็บและโอนย้าย				
	DLP				
	10 มีกระบวนการหรือระบบงานในการปกป้องข้อมูลรั่วไหล				
	11 มีการจัดทำนโยบายเพื่อปกป้องข้อมูลรั่วไหล				
	การควบคุมความปลอดภัยทางกายภาพ Physical Security				
	12 นโยบายควรครอบคลุมการปกป้องความปลอดภัยทางกายภาพ				
	13 มีการแนวทางการจัดเก็บ โอนย้าย และใช้งานข้อมูลประเภทเอกสาร (Hard copies) อย่างปลอดภัย				
	การสอบทาน Security and Activities log				
	14 มีการนำระบบงาน SIEM มาใช้				
	15 มีแนวทางการตั้งค่าการปกป้องคุ้มครองข้อมูลส่วนบุคคล				
	16 เจ้าหน้าที่ Security Officer สอบทาน Log เป็นประจำและแจ้งเหตุการณ์ผิดปกติอย่างทันท่วงที				
4	THIRD PARTY				
	การจัดทำสัญญาการเป็น Data Processor				
	1 มีการจัดทำสัญญาการเป็น Data Processor ที่ครอบคลุมทุกหัวข้อทางกฎหมาย				
5	INCIDENT MANGEMENT				
	แผนการตอบสนองต่อเหตุการณ์ผิดปกติ / ข้อมูลรั่วไหล				
	1 มีการจัดทำแผนการตอบสนองต่อเหตุการณ์ผิดปกติ				
	2 มีการซักซ้อมแผนการตอบสนองต่อเหตุการณ์ผิดปกติ				

กระดาษทำการ

หน่วยตรวจสอบภายใน สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

วันที่จัดทำ: วันที่..... มกราคม 2569

หน่วยรับตรวจ: ศูนย์ข้อมูล สำนักยุทธศาสตร์และแผน

การตรวจสอบการปฏิบัติตามกฎระเบียบ (Compliance Audit)	
การตรวจสอบเทคโนโลยีสารสนเทศ (IT Audit)	
เรื่อง	การรักษาความมั่นคงปลอดภัยไซเบอร์และการกำกับดูแลระบบสารสนเทศของ สวพส.
รหัส	CA-69-01-02

วัตถุประสงค์การตรวจสอบ

1) เพื่อให้มั่นใจว่า การกำกับดูแล และมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สวพส. ว่ามีการออกแบบและนำไปปฏิบัติอย่างเหมาะสม สอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง
2) เพื่อประเมินความสอดคล้องระหว่างนโยบายด้านความมั่นคงปลอดภัยไซเบอร์กับการปฏิบัติงานจริงของหน่วยงานและบุคลากรที่เกี่ยวข้อง รวมถึงระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากร
3) เพื่อให้ข้อเสนอแนะเชิงปรับปรุงในการยกระดับการควบคุมภายใน การกำกับดูแล และการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของ สวพส. ให้มีความเหมาะสม และสอดคล้องกับแนวปฏิบัติที่ดี

ลำดับ	ประเด็นการตรวจสอบ	ผลการตรวจสอบ		เอกสารหลักฐานที่เกี่ยวข้อง	หมายเหตุ
		มี	ไม่มี		
1	**โครงสร้างและการกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์**				
	1.1 มีการจัดทำประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นลายลักษณ์อักษร หรือไม่				
	1.2 มีการกำหนดโครงสร้างการกำกับดูแล และมีการระบุหน้าที่ความรับผิดชอบของบุคลากรหรือไม่				
	1.3 มีการแจ้งรายชื่อเจ้าหน้าที่ทั้งระดับบริหารและดับปฏิบัติการเพื่อทำหน้าที่ประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยัง สกมช. หรือไม่				
2	**การสุ่มตรวจเหตุการณ์ไซเบอร์ย้อนหลัง**				
	2.1 มีการบันทึกเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ในรอบ 6-12 เดือนที่ผ่านมาและจัดทำรายงานสรุปเสนอผู้บังคับบัญชาอย่างครบถ้วนหรือไม่				
3	**การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์**				
	3.1 มีการจัดทำโครงสร้างการรายงานเหตุการณ์ ที่ระบุหน้าที่ตาม พรบ. และกฎหมายที่เกี่ยวข้อง หรือไม่				
	3.2 มีการกำหนดเกณฑ์และเงื่อนไขเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ต้องแจ้งผู้รับผิดชอบและดำเนินการตามแผนรองรับ				

	3.3 มีการระบุรายชื่อและช่องทางการติดต่อ ในกรณีเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์ ไว้อย่างชัดเจนหรือไม่				
	3.4 มีการกำหนดแบบฟอร์มบันทึกเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดข้อมูลที่ครบถ้วน				
	3.5 มีการรายงานเมื่อตรวจสอบว่ามีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวงแนวทางปฏิบัติและกรอบมาตราฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานและมีการแจ้งไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับกับดูแลของตนโดยเร็ว				
	3.6 มีการรายงานสรุปผลการดำเนินการฉบับสมบูรณ์ ต่อหน่วยงานกำกับเมื่อภัยคุกคามสิ้นสุดลง เพื่อปิดเหตุการณ์หรือไม่				
4	**ตรวจสอบขั้นตอนแจ้งเหตุ และแผนรับการรับมือเหตุภัยคุกคามทางไซเบอร์**				
	4.1 มีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ที่เป็นลายลักอักษรหรือไม่				
	4.2 มีการกำหนดโครงสร้างหน้าที่ความรับผิดชอบแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างชัดเจนและเป็นลายลักษณ์อักษร หรือไม่				
	4.3 มีการซักซ้อมแผนรับมือภัยคุกคามไซเบอร์ เพื่อให้มั่นใจว่าบุคลากรสามารถปฏิบัติได้จริง อย่างน้อยปีละ 1 ครั้งหรือไม่				
	4.4 มีการจัดฝึกอบรมหรือกิจกรรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากรทุกระดับอย่างน้อยปีละ 1 ครั้ง หรือไม่				

กระดาษทำการ

หน่วยตรวจสอบภายใน สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

วันที่จัดทำ: วันที่..... มกราคม 2569

หน่วยรับตรวจ: ศูนย์ข้อมูล สำนักยุทธศาสตร์และแผน

การตรวจสอบการปฏิบัติตามกฎระเบียบ (Compliance Audit)
การตรวจสอบเทคโนโลยีสารสนเทศ (IT Audit)
เรื่อง แผนความต่อเนื่องทางธุรกิจด้านระบบเทคโนโลยีสารสนเทศ (BCP IT)
รหัส CA-69-01-03

วัตถุประสงค์การตรวจสอบ

1) เพื่อให้มั่นใจว่าการจัดทำแผนความต่อเนื่องทางธุรกิจด้านระบบเทคโนโลยีสารสนเทศ (BCP IT) ของ สวพส. สามารถนำไปปฏิบัติอย่างเหมาะสม สอดคล้องกับความเสี่ยงและความสำคัญของระบบสารสนเทศที่สนับสนุนภารกิจหลักขององค์กร
2) เพื่อให้ข้อเสนอแนะเชิงปรับปรุงในการยกระดับความพร้อมด้านความต่อเนื่องของระบบสารสนเทศและโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของ สวพส. เพื่อลดผลกระทบต่อภารกิจหลัก ภาพลักษณ์ และความเชื่อมั่นของผู้มีส่วนได้เสีย

ลำดับ	ประเด็นการตรวจสอบ	ผลการตรวจสอบ		เอกสารหลักฐานที่เกี่ยวข้อง	หมายเหตุ
		มี	ไม่มี		
1	**กรอบแผนความต่อเนื่องทางธุรกิจด้านระบบเทคโนโลยีสารสนเทศ (BCP IT)**				
	1.1 แผนความต่อเนื่องทางธุรกิจด้านระบบเทคโนโลยีสารสนเทศ (BCP IT) ได้รับอนุมัติจากผู้บริหาร				
	1.2 มีการกำหนดผู้รับผิดชอบชัดเจน				
	1.3 มีการสื่อสารนโยบายหรือแผนให้แก่ผู้ที่เกี่ยวข้องรับทราบ				
2	**การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis)**				
	2.1 มีการจัดทำ Business Impact Analysis (BIA) อย่างเป็นทางการ				
	2.2 Business Impact Analysis ครอบคลุมระบบที่สำคัญ				
	2.3 มีการจัดลำดับความสำคัญระบบ				
	2.4 มีการกำหนดค่า RTO และ RPO สำหรับระบบสำคัญตาม BIA (BIA - RTO/RPO - DR)				
	2.5 มีการทบทวน Business Impact Analysis (BIA) อย่างน้อยปีละครั้ง				
3	**การกู้คืนระบบเทคโนโลยีสารสนเทศ (แผนรับมือ)**				
	3.1 ครอบคลุมระบบสารสนเทศที่สำคัญ				
	3.2 มีการกำหนดขั้นตอนการดำเนินงานชัดเจน				
	3.3 มีการกำหนดผู้รับผิดชอบเป็นทางการ				
	3.4 ข้อมูลติดต่อฉุกเฉินเป็นปัจจุบัน				
	3.5 มีการทดสอบการกู้คืนระบบอย่างน้อยปีละ 1 ครั้ง				
4	**การสำรองข้อมูล (Backup)**				
	4.1 การสำรองข้อมูลครอบคลุมระบบสารสนเทศที่สำคัญ				
	4.2 รอบระยะเวลาการสำรองข้อมูลสอดคล้องกับ RPO				
	4.3 มีการเก็บข้อมูล (Backup) สำรองแยกนอกสถานที่				
	4.4 มีการทดสอบการสำรองข้อมูล				
5	**การทดสอบ/ซักซ้อมแผนความต่อเนื่องทางธุรกิจด้านระบบเทคโนโลยีสารสนเทศ (BCP IT)**				
	5.1 มีการทดสอบ/ซักซ้อมแผน BCP อย่างเป็นทางการ				
	5.2 การทดสอบ/ซักซ้อม BCP ครอบคลุมทุกส่วนงานที่เกี่ยวข้องและสำคัญ				

	5.3 มีการรายงานผลการทดสอบ/ซักซ้อมแผน BCP และเสนอผู้บริหาร				
	5.4 บุคลากรมีความเข้าใจบทบาทของตนเองในแผน BCP				
6	**การสื่อสารในภาวะฉุกเฉิน**				
	6.1 มีการระบุขั้นตอน ผู้รับผิดชอบ และช่องทางการแจ้งเหตุในภาวะฉุกเฉินอย่างเป็นทางการทั้งภายในและภายนอกองค์กร				
	6.2 มีการกำหนดช่องสำรองในการสื่อสาร กรณีช่องหลักไม่สามารถสื่อสารได้				
	6.3 บุคลากรรับทราบขั้นตอนการสื่อสารกรณีฉุกเฉิน				
7	**การติดตามและปรับปรุง**				
	7.1 มีการติดตามผลการดำเนินงานตามแผน BCP IT อย่างเป็นระบบ				
	7.2 มีการทบทวนและปรับปรุงแผนหลังการทดสอบ/ซักซ้อม				
	7.3 มีการจัดทำรายงานการทบทวนและปรับปรุงแผนเสนอผู้บริหาร				

กระดาษทำการ

หน่วยตรวจสอบภายใน สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

วันที่จัดทำ: วันที่..... มกราคม 2569

หน่วยรับตรวจ: ศูนย์ข้อมูล สำนักยุทธศาสตร์และแผน

การตรวจสอบการปฏิบัติตามกฎระเบียบ (Compliance Audit)
การตรวจสอบเทคโนโลยีสารสนเทศ (IT Audit)
เรื่อง: การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (IT General Controls)
รหัส: CA-69-01-04

วัตถุประสงค์การตรวจสอบ

1. เพื่อประเมินความเพียงพอและประสิทธิผลของการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศของ สวพส. ว่ามีการออกแบบและนำไปปฏิบัติอย่างเหมาะสมสอดคล้องกับกฎหมายมาตรฐานและแนวปฏิบัติที่เกี่ยวข้องเพื่อสนับสนุนการดำเนินภารกิจของ สวพส ให้เป็นไปอย่างมั่นคง ปลอดภัย และต่อเนื่อง
2. เพื่อประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจส่งผลกระทบต่อความถูกต้อง ครบถ้วน และความเชื่อถือได้ของ ข้อมูลสารสนเทศ รวมถึงความมั่นคงปลอดภัยไซเบอร์และเพื่อให้ข้อเสนอแนะเชิงปรับปรุงในการยกระดับระบบควบคุมภายในด้านเทคโนโลยีสารสนเทศของ สวพส
3. ให้ข้อเสนอแนะมีความเหมาะสมกับบริบทของ สวพส. และลดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT) หรือเพิ่มประสิทธิภาพการดำเนินงาน รวมถึงมีผลต่อการเปลี่ยนแปลงเชิงโครงสร้างหรือแนวทางการดำเนินงานด้านเทคโนโลยีสารสนเทศ (IT)

ลำดับ	ประเด็นการตรวจสอบ	ผลการตรวจสอบ		เอกสารหลักฐานที่เกี่ยวข้อง	หมายเหตุ
		มี	ไม่มี		
1	**โครงสร้างและการกำกับดูแลด้านเทคโนโลยีสารสนเทศ**				
	1.1 มีนโยบายด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและได้รับการอนุมัติจากผู้บริหารระดับสูง				
	1.2 มีแผนแม่บทด้านดิจิทัล/เทคโนโลยีสารสนเทศที่สอดคล้องกับยุทธศาสตร์หรือเป้าหมายขององค์กร				
	1.3 มีการกำหนดบทบาทหน้าที่และความรับผิดชอบด้าน IT อย่างชัดเจน				
	1.4 มีคณะกรรมการหรือกลไกกำกับดูแลด้าน IT อย่างเป็นทางการ				
	1.5 มีการรายงานผลการดำเนินงานและความเสี่ยงด้าน IT ต่อผู้บริหารอย่างต่อเนื่อง				
	1.6 มีการทบทวนและปรับปรุงนโยบายด้าน IT อย่างน้อยปีละ 1 ครั้ง				
2	**การบริหารจัดการผู้ให้บริการภายนอก**				
	2.1 มีหลักเกณฑ์การคัดเลือกผู้ให้บริการด้าน IT				
	2.2 มีการประเมินความเสี่ยงผู้ให้บริการก่อนทำสัญญา				
	2.3 มีการกำหนดข้อตกลงการรักษาความลับ				
	2.4 มีข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศในสัญญา				
	2.5 มีการติดตามและประเมินผลการปฏิบัติงานของผู้ให้บริการเป็นระยะ				
	2.6 มีแผนรองรับ หรือมีการเตรียมความพร้อม กรณีผู้ให้บริการไม่สามารถให้บริการได้ตามสัญญา				
3	**การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ**				
	3.1 มีการกำหนดนโยบายและโครงสร้างการบริหารความเสี่ยงด้าน IT				
	3.2 มีการประเมินโอกาสและผลกระทบของความเสี่ยงอย่างเป็นระบบ				
	3.3 มีแผนควบคุม และการบริหารจัดการความเสี่ยง				
	3.4 มีการติดตามและรายงานความเสี่ยงต่อผู้บริหาร และผู้กำกับดูแลอย่างต่อเนื่อง				
4	**การบริหารจัดการการตั้งค่าระบบ และการควบคุมการตั้งค่ารหัสผ่าน**				
	4.1 มีการจัดทำและอนุมัตินโยบายการตั้งค่าความปลอดภัยของระบบ				
	4.2 มีนโยบายการตั้งค่ารหัสผ่านเป็นลายลักษณ์อักษร				
	4.3 การตั้งค่ารหัสผ่าน มีการกำหนดความซับซ้อน ความยาว อายุ				
	4.4 มีการกำหนดจำนวนครั้งการล็อกอินผิดพลาดก่อนล็อกบัญชี				
	4.5 มีการปิดใช้งานบัญชีที่ไม่มีการใช้งานตามระยะเวลาที่กำหนด				
5	**การบริหารจัดการบัญชีผู้ใช้งาน**				
	5.1 มีกระบวนการสร้างบัญชีผู้ใช้งาน เช่น การอนุมัติ การยืนยันตัวตน				
	5.2 มีการกำหนดสิทธิตามบทบาทหน้าที่				
	5.3 มีการเพิกถอนบัญชีเมื่อพ้นสภาพหรือย้ายงาน				
	5.4 มีการบันทึกประวัติการเปลี่ยนแปลงสิทธิผู้ใช้งาน				
	5.5 มีการทบทวนสิทธิผู้ใช้งานเป็นระยะ				
	5.6 แยกหน้าที่ระหว่างผู้ขอ ผู้อนุมัติ และผู้ดำเนินการด้านระบบ				
6	**การจำกัดสิทธิการเข้าถึงผู้ใช้งานที่มีสิทธิสูง (HPID) และการควบคุมผู้ใช้งานระบบ**				
	6.1 มีการกำหนดสิทธิ์และการใช้งานบัญชีผู้มีสิทธิสูง (HPID) และบัญชีผู้ดูแลระบบ (Admin)				
	6.2 มีการกำหนดขั้นตอนการขอใช้ และการอนุมัติจากผู้มีอำนาจใช้งานบัญชีผู้มีสิทธิสูง (HPID)				
	6.3 มีบัญชีผู้มีสิทธิสูง (HPID) และบัญชีผู้ดูแลระบบ (Admin) แยกจากบัญชีผู้ใช้งานทั่วไป				
	6.4 จำกัดจำนวนบัญชีผู้มีสิทธิสูงให้อยู่ในระดับที่จำเป็น				
	6.5 มีการบันทึก Log การใช้งานบัญชี HPID				
	6.6 มีการทบทวนสิทธิ HPID เป็นระยะ				
	6.7 มีการเพิกถอนสิทธิ HPID เมื่อพ้นความจำเป็น				

7	**การสอบทาน Log ด้านความมั่นคงปลอดภัย**				
	7.1 มีการกำหนดประเภท Log ที่ต้องจัดเก็บ				
	7.2 มีการตั้งค่าระบบให้บันทึก Log อย่างครบถ้วน				
	7.3 ระบุแหล่งที่มาของ Log				
	7.4 กำหนดระยะเวลาการเก็บรักษา Log				
	7.5 มีการมอบหมายผู้รับผิดชอบ และความถี่ในการสอบทาน Log				
	7.6 มีการตั้งค่าแจ้งเตือนเมื่อพบเหตุการณ์ผิดปกติใน Log และเชื่อมโยงแผนตอบสนองเหตุการณ์				
	7.7 มีการป้องกันการแก้ไขหรือลบ Log โดยไม่ได้รับอนุญาติ				
8	**การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา**				
	8.1 มีคู่มือการจัดการเหตุการณ์ผิดปกติ หรือปัญหา				
	8.2 มีกระบวนการ/ขั้นตอนการรับแจ้งเหตุการณ์ผิดปกติ หรือปัญหา				
	8.3 มีการตอบสนองการแจ้งเตือน และการจัดลำดับความสำคัญ				
	8.4 มีการวิเคราะห์หาสาเหตุ				
	8.5 มีมาตรการป้องกันเหตุซ้ำ				
	8.6 มีการจัดทำ Lesson Learned และปรับปรุงกระบวนการทำงาน				
9	**การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์**				
	9.1 มีการกำหนดนโยบายและโครงสร้างการบริหารความเสี่ยงไซเบอร์				
	9.2 มีการระบุภัยคุกคามไวเบอร์และการประเมินผลระทบ				
	9.3 มีการกำหนดและนำมาตรการควบคุมมาใช้เพื่อลดความเสี่ยงไซเบอร์อย่างเหมาะสม				
	9.4 มีการจัดทำแผนครอบคลุมขั้นตอนการรับมือภัยคุกคามหรือตอบสนองเหตุการณ์ผิดปกติทางไซเบอร์อย่างเป็นทางการ				
	9.5 มีการรายงานผลการทดสอบแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์				
	9.6 มีการรายงานเหตุการณ์ภัยคุกคามไซเบอร์ต่อผู้บริหารอย่างต่อเนื่อง				
10	**การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม และความปลอดภัยของอุปกรณ์ปลายทาง**				
	10.1 มีการควบคุมการเข้าถึงห้องเวิร์ฟเวอร์				
	10.2 มีระบบควบคุมอุณหภูมิ ความชื้น UPS หรือ Generator				
	10.3 มีการจัดวางอุปกรณ์ IT ให้ปลอดภัยจากความเสียหายทางกายภาพ				
	10.4 มีการใช้งานกล้องวงจรปิด (CCTV) ระบบแจ้งเตือน และมีการบันทึกเหตุการณ์				
	10.5 มีการลบข้อมูลก่อนนำอุปกรณ์กลับมาใช้หรือทิ้ง				
	10.6 มีนโยบายการใช้อุปกรณ์ปลายทาง เช่น				
	- การลงทะเบียนขอเชื่อมต่อระบบสารสนเทศของ สวพส.				
	- มีการติดตั้งเครื่องมือในการป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี				
11	**การบริหารจัดการการเปลี่ยนแปลง**				
	11.1 มีการจัดทำนโยบาย หรือแนวปฏิบัติการบริหารจัดการการเปลี่ยนแปลงระบบ				
	11.2 มีแบบคำขอเปลี่ยนแปลงระบบ (Change Request) และได้รับอนุมัติจากผู้มีอำนาจ				
	11.3 มีการประเมินความเสี่ยงและผลกระทบก่อนดำเนินการเปลี่ยนแปลง				
	11.4 มีการจัดทำแผนเปลี่ยนแปลงระบบ และแผนย้อนกลับกรณีล้มเหลว				
	11.5 มีการทดสอบ และได้รับการอนุมัติจากผู้มีอำนาจก่อนนำขึ้นใช้งานจริง				
12	**การสำรองข้อมูล (Data Backup) และการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ**				
	12.1 มีการจัดทำแนวปฏิบัติการสำรองข้อมูล และได้รับอนุมัติจากผู้บริหาร				
	12.2 มีการอบรมให้ความรู้แก่บุคลากรอย่างสม่ำเสมอ				
	12.3 มีการจัดเก็บข้อมูลสำรอง และมาตรการรักษาความปลอดภัย				
	12.4 มีการทดสอบการกู้คืนข้อมูล และความสมบูรณ์ของไฟล์สำรองเป็นระยะ				
	12.5 มีการจัดทำแผนความต่อเนื่องทางธุรกิจด้านระบบเทคโนโลยีสารสนเทศ				
	12.6 มีการซักซ้อมแผนแผนความต่อเนื่องทางธุรกิจด้านระบบเทคโนโลยีสารสนเทศ				
	12.7 มีการกำหนดบทบาทหน้าที่ของทีม IT และผู้มีส่วนเกี่ยวข้อง				
13	**การบริหารขีดความสามารถของระบบ**				
	13.1 มีนโยบายหรือแนวทางด้าน Capacity Management และการอนุมัติจากผู้บริหาร				
	13.2 มีการวิเคราะห์แนวโน้มและการคาดการณ์ความต้องการในอนาคต				
	13.3 มีการติดตาม เฝ้าระวังการใช้งานทรัพยากรระบบ เช่น CPU, RAM, Network				
	13.4 มีการกำหนดค่าขีดจำกัด และการแจ้งเตือนเมื่อทรัพยากรใกล้เต็มขีดความสามารถ				
	13.5 มีการจัดทำรายงาน Capacity และการสื่อสารกับผู้มีส่วนได้เสีย				

14	**การจัดหาและการพัฒนาระบบ**				
	14.1 มีการกำหนดขั้นตอน SDLC อย่างชัดเจน				
	14.2 มีแบบฟอร์ม Requirement และได้รับอนุมัติจากผู้มีอำนาจ				
	14.3 มีการวิเคราะห์ความต้องการและวางแผนโครงการ				
	14.4 การออกแบบมีการกำหนด Functional ตาม Requirement และ				
	กำหนด Non Functional เช่น Security				
	14.5 มีการทดสอบ และได้รับการอนุมัติจากผู้มีอำนาจก่อนนำขึ้นใช้งานจริง				
	14.6 มีการประเมินผลหลังใช้งาน