เอกสารวิชาการ
การตรวจสอบเทคโนโลยีสารสนเทศ
ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

กลุ่มตรวจสอบภายใน
กรมพัฒนาที่ดิน
กระทรวงเกษตรและสหกรณ์

ประจำปีงบประมาณ พ.ศ. 2566

กรกฎาคม 2566

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศมีบทบาทในการดำเนินงานขององค์กรทั้งภาครัฐและภาคเอกชน ซึ่งกรมพัฒนาที่ดินก็เป็นองค์กรหนึ่งที่โดดเด่นในการนำระบบเทคโนโลยีสารสนเทศเข้ามาเป็นเครื่องมือในการขับเคลื่อนองค์กรทุกมิติ เป็นการตอบรับกับนโยบายภาครัฐ (ระบบ Thailand 4.0) ข้อมูลสารสนเทศและระบบเทคโนโลยี ซึ่งมีความจำเป็นอย่างมากที่ใช้เป็นเครื่องมือในการเพิ่มประสิทธิภาพการดำเนินงานให้บรรลุเป้าหมายด้วยความสะดวก รวดเร็ว ติดตามข้อมูลได้ตลอดเวลา องค์กรต่าง ๆ จึงต้องให้ความสำคัญกับความมั่นคงและการรักษาความปลอดภัยของสารสนเทศและระบบเทคโนโลยี เพื่อมิให้ก่อให้เกิดผลเสียต่อองค์กร

การตรวจสอบภายในเป็นเครื่องมือสำคัญของผู้บริหารที่สามารถสร้างความเชื่อมั่นและให้คำปรึกษาต่อการขับเคลื่อนองค์กรให้อยู่ภายใต้กฎระเบียบของภาครัฐ โดยมีระบบการควบคุมภายใน การบริหารความเสี่ยง การกำกับดูแล อย่างเพียงพอและเหมาะสม ซึ่งตรวจสอบการดำเนินงานด้านงานเทคโนโลยีสารสนเทศจำเป็นต้องให้ผู้ตรวจสอบภายในมีความรู้ และทักษะ ความเชี่ยวชาญ ชำนาญ เกี่ยวกับการปฏิบัติงานและการตรวจสอบด้านเทคโนโลยีสารสนเทศ แต่ปัญหาอุปสรรค คือ ยังไม่มีแนวทางการตรวจสอบที่ชัดเจน มีการใช้ดุลยพินิจของผู้ตรวจสอบภายในแต่ละคน ซึ่งจะไม่เป็นแนวทางเดียวกัน ดังนั้น กลุ่มตรวจสอบภายในกรมพัฒนาที่ดิน จึงจัดทำเอกสารวิชาการ เรื่อง การตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อให้ผู้ตรวจสอบภายในทุกคนมีแนวทางปฏิบัติงานที่เป็นมาตรฐานเดียวกัน ลดการใช้ดุลยพินิจในการปฏิบัติงาน

กลุมตรวจสอบภายใน คาดหวังเป็นอย่างยิ่งว่าเอกสารวิชาการฉบับนี้จะเป็นประโยชนแก่ผู้ตรวจสอบภายในของหน่วยงาน และผู้ที่สนใจในการใช้เป็นตำราในการศึกษา และค้นคว้าทำความเข้าใจในการปฏิบัติงานการตรวจสอบภายใน ด้านงานเทคโนโลยีสารสนเทศต่อไป

คณะทำงานวิชาการ

3 กรกฎาคม 2566

สารบัญ

สารบัญ (ต่อ)

สารบัญภาพ

สารบัญตาราง

บทสรุปผู้บริหาร

การจัดทำเอกสารวิชาการ “เรื่อง การตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ” ของกลุ่มตรวจสอบภายใน กรมพัฒนาที่ดิน มีความจำเป็นต่อการปฏิบัติงานของผู้ตรวจสอบภายในอย่างยิ่ง เพื่อเป็นกรอบยึดถือในการปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศให้เป็นไปในแนวทางเดียวกันตามมาตฐานการตรวจสอบภายในของภาครัฐ และเป็นการส่งเสริมสนับสนุนผู้บริหารกรมพัฒนาที่ดินในการขับเคลื่อนองค์กรภายใต้ กฎ ระเบียบ ของทางราชการที่เกี่ยวข้อง

การตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เป็นหนึ่งในประเภทงานตรวจสอบภายในที่กรมบัญชีกลางกำหนดให้หน่วยงานตรวจสอบภายในของภาครัฐ จัดทำแผนการตรวจสอบ ซึ่งเอกสารวิชาการฉบับนี้ครอบคลุมเนื้อหาการตรวจสอบเทคโนโลยีสารสนเทศ ประกอบด้วย แนวคิดการตรวจสอบ หลักการวิเคราะห์ประเด็นตรวจสอบ ความรู้พื้นฐานสำหรับการตรวจสอบ กฎ ระเบียบแนวปฏิบัติที่เกี่ยวข้องและวิธีการ ขั้นตอนการปฏิบัติงานตรวจสอบตามมาตรฐานการตรวจสอบภาครัฐ โดยนำเสนอข้อมูล ความรู้ข้อเท็จจริง แนวคิด ทฤษฎี การวิเคราะห์ ประเมินผล สรุปผล บนพื้นฐานข้อมูลตามข้อเท็จจริง สมเหตุสมผลและน่าเชื่อถือ รวมถึงการจัดทำกรณีศึกษาการตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยเริ่มต้นตั้งแต่การประเมินความเสี่ยงเบื้องต้น เพื่อกำหนดประเด็นการตรวจสอบ วัตถุประสงค์การตรวจสอบ ขอบเขตการตรวจสอบ การจัดทำแผนการปฏิบัติงานตรวจสอบ (Engagement Plan) เพื่อให้ทีมงานตรวจสอบใช้เป็นกรอบในการปฏิบัติงานตรวจสอบ

การปฏิบัติงานตรวจสอบ ณ สำนักงานหน่วยรับตรวจ ซึ่งหัวหน้าทีมตรวจสอบภายในจะแจ้งรายละเอียดการตรวจสอบ อันประกอบด้วย ประเด็นการตรวจสอบ วัตถุประสงค์การตรวจสอบขอบเขตการตรวจสอบ ระยะเวลาการตรวจสอบ และการปฏิบัติตามแผนการปฏิบัติงานตรวจสอบ (Engagement Plan) ด้วยเทคนิค เครื่องมือ และวิธีการตรวจสอบที่เหมาะสมและเพียงพอ โดยมีการตรวจสอบ ดังนี้

1. การประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ เพื่อให้ทราบถึงความเพียงพอ เหมาะสมของการควบคุม กำกับดูแล และการบริหารความเสี่ยง รวมถึงปัญหาและอุปสรรคในการปฏิบัติงานของหน่วยรับตรวจ
2. การสอบทานเอกสารหลักฐานการจัดทำและการปฏิบัติตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตาม พรบ. กฎ ระเบียบ ประกาศ ที่เกี่ยวข้อง
3. การสังเกตการณ์สภาพสิ่งแวดล้อมพื้นที่ปฏิบัติการด้านสารสนเทศว่ามีความปลอดภัยต่อการปฏิบัติงานของหน่วยรับตรวจ

4. การทดสอบระบบงาน IT เพื่อประเมินความเหมาะสมการควบคุมภายใน การจัดการความเสี่ยงด้าน IT

5. การตรวจสอบเครื่องมืออุปกรณ์ด้านสารสนเทศ เป็นการพิสูจน์จำนวนและสภาพของสิ่งที่ตรวจนับว่ามีอยู่ครบถ้วน ชำรุด หรือไม่

เมื่อการตรวจสอบเสร็จสิ้น ได้มีการรวบรวมข้อมูล วิเคราะห์ และประเมินผลจากการตรวจสอบเพื่อให้ได้มาซึ่งผลการตรวจสอบพร้อมข้อเสนอแนะ เสนอผู้บริหารส่วนราชการพิจารณาสั่งการให้หน่วยรับตรวจดำเนินการต่อไป

บทที่ 1

การตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

1. หลักการและความเป็นมา

ปัจจุบัน เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการสนับสนุนกระบวนการดำเนินงานขององค์กร ทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผลระบบงานสำคัญต่าง ๆ เช่น ระบบการเงิน ระบบการรับส่งข้อมูล ระบบสินทรัพย์ ระบบบริหารงานบุคคล โดยเฉพาะอย่างยิ่ง ระบบที่เกี่ยวข้องกับการให้บริการประชาชน ซึ่งนอกจากการนำเทคโนโลยีสารสนเทศต่าง ๆ ที่หน่วยงานนำมาใช้ให้การดำเนินงานขององค์กรมีความสะดวกรวดเร็วมีประสิทธิภาพแล้ว ยังเป็นการยกระดับการปฏิบัติราชการก้าวสู่ 4.0 ตามแผนยุทธศาสตร์ภาครัฐ อย่างไรก็ดี การใช้เทคโนโลยีสารสนเทศมีความเสี่ยงหลายประการที่ต้องเฝ้าระวังเพื่อมิให้การดำเนินงานของหน่วยงานเกิดความเสียหายหรือหยุดชะงัก เช่น ลักษณะการใช้งานในระบบงานที่มีความซับซ้อน ระบบมีความผิดพลาดหรือมีฟังก์ชันความผิดพลาดที่มีค่าความเสียหายสูง การรักษาความลับ การถูกบุกรุกระบบโดยบุคคลภายนอก การใช้งานไม่ครบถ้วน บุคคลภายนอกหรือบุคลากรภายในละเมิดสิทธิในการใช้งาน หรือเหตุการณ์ต่าง ๆ ที่มิอาจคาดหมายจากเหตุฉุกเฉิน ได้แก่ ไฟดับ อัคคีภัย เหตุภัยทางธรรมชาติ เป็นต้น ซึ่งอาจจะส่งผลกระทบและความเสียหายต่อระบบสารสนเทศ จึงจำเป็นต้องมีการควบคุมและตรวจสอบระบบสารสนเทศอย่างเพียงพอและเหมาะสม ให้ระบบมีสภาพพร้อมใช้งานตลอดเวลา

ตาม หนังสือกรมบัญชีกลาง ที่ กค 0409.2/ว 614 ลว. 23 ธ.ค. 2563 เรื่อง การกำหนดประเภทของงานตรวจสอบภายใน กำหนดให้มีการตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ เป็นส่วนหนึ่งของประเภทงานตรวจสอบภายใน เพื่อประเมินความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศของหน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยของสารสนเทศของหน่วยงานนั้น แต่การตรวจสอบ ด้านระบบสารสนเทศจำเป็นต้องใช้ผู้ตรวจสอบภายในที่มีความรู้ทักษะ ความเชี่ยวชาญเกี่ยวกับการตรวจสอบเทคโนโลยีสารสนเทศ เพื่อให้การปฏิบัติงานตรวจสอบเป็นไปอย่างมีประสิทธิภาพ ประสิทธิผล แต่ที่ผ่านมา พบปัญหาจากการตรวจสอบงานเทคโนโลยีสารสนเทศ ไม่มีแนวทางการตรวจสอบที่ชัดเจน ทำให้ผู้ตรวจสอบภายในปฏิบัติงานได้ไม่เป็นแนวทางเดียวกัน และยุ่งยากในการประเมินความเสี่ยงและระบบควบคุมภายใน ดังนั้น กลุ่มตรวจสอบภายใน กรมพัฒนาที่ดิน จึงจัดทำเอกสารวิชาการ เรื่อง การตรวจสอบเทคโนโลยีสารสนเทศด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อเป็นแนวทางการปฏิบัติงานตรวจสอบให้กับผู้ตรวจสอบภายในของกรมให้เป็นไปตามแนวทางมาตรฐานเดียวกัน ลดการใช้ดุลยพินิจในการปฏิบัติงาน และสอดคล้องกับกฎหมายระเบียบปฏิบัติที่เกี่ยวข้องตามนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน

2. วัตถุประสงค์

2.1 เพื่อให้ผู้ตรวจสอบภายใน กรมพัฒนาที่ดิน มีแนวทางการปฏิบัติงานตรวจสอบเทคโนโลยีสารสนเทศด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกรมพัฒนาที่ดิน เป็นลายลักษณ์อักษร

2.2 เพื่อใช้เป็นเครื่องมือในการถ่ายทอด การสอนงาน (Coaching) และสื่อสารวิธีการปฏิบัติงานให้แก่ผู้ตรวจสอบภายในให้เกิดความรู้ ความเข้าใจสามารถปฏิบัติงานทดแทนกันได้อย่างเป็นระบบ และมีมาตรฐานเดียวกันตามมาตรฐานงานตรวจสอบภายในของส่วนราชการ

2.3 เพื่อเผยแพร่ให้กับบุคคลภายนอกหรือหน่วยงานในสังกัดกรมได้รับรู้และเข้าใจกระบวนการปฏิบัติงาน

3. ขอบเขตและวิธีการศึกษา

3.1 ขอบเขตเนื้อหา

3.1.1 ขั้นตอน วิธีการตรวจสอบ ภายใต้หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติงานตรวจสอบภายในสำหรับ หน่วยงานของรัฐ

3.1.2 วิธีการตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกรมพัฒนาที่ดิน เกี่ยวกับการควบคุมตามมาตรการควบคุมภายในของการรักษาความปลอดภัยด้านสารสนเทศภายใต้กรอบระเบียบ ดังนี้

(1) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ฉบับที่ 2) พ.ศ. 2560

(2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

(3) พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

3.1.3 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

3.1.4 กระบวนงานการให้บริการและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศประกอบด้วย

(1) กำหนดนโยบายและแผนงาน

(2) การกำหนดโครงสร้างและผู้รับผิดชอบ

(3) ทำทะเบียนสินทรัพย์/จัดหมวดหมู่

(4) สรรหา อบรม ควบคุม คืนถอดถอนสิทธิของบุคคล

(5) ควบคุมด้านกายภาพ สิ่งแวดล้อม

(6) ป้องกัน/ควบคุมระบบเครือข่าย และการแลกเปลี่ยนข้อมูล

(7) ควบคุมการเข้าถึงข้อมูล

(8) ควบคุมการจัดหา พัฒนา บำรุงรักษาระบบ

(9) บริหารเหตุการณ์ การแก้ไข ทบทวนปรับปรุงอย่างต่อเนื่อง

3.2 วิธีการศึกษา

3.2.1 ศึกษาวิธีการจัดทำคู่มือ/แนวทางการปฏิบัติงาน/เอกสารทางวิชาการ

3.2.2 ศึกษาแนวคิดและหลักการตรวจสอบตามมาตรฐานงานตรวจสอบภายในของส่วนราชการและการควบคุมภายใน การบริหารความเสี่ยง

3.2.3 ศึกษาแนวคิด ทฤษฎีและวรรณกรรมที่เกี่ยวกับหลักการตรวจสอบระบบเทคโนโลยีสารสนเทศ องค์ประกอบการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ระเบียบ กฎหมายที่เกี่ยวข้อง ด้านเทคโนโลยีสารสนเทศ

3.2.4 ศึกษานโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมพัฒนาที่ดิน และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

3.2.5 รวบรวมและวิเคราะห์ข้อมูลกรณีศึกษาที่เกี่ยวข้องกับการจัดทำเอกสารวิชาการตรวจสอบภายใน เรื่อง การตรวจสอบเทคโนโลยีสารสนเทศ : ความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ

3.2.6 จัดทำเอกสารวิชาการตรวจสอบภายใน เรื่อง ตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกรมพัฒนาที่ดิน

3.2.7 เผยแพร่เอกสารวิชาการตรวจสอบภายใน เรื่อง ตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกรมพัฒนาที่ดิน เพื่อให้ผู้ตรวจสอบภายในถือปฏิบัติเป็นมาตรฐานเดียวกัน และสำหรับผู้ที่สนใจทั่วไปได้รับทราบกระบวนการ วิธีการขั้นตอนการปฏิบัติงานของกลุ่มตรวจสอบภายใน

4. คำจำกัดความ

4.1 การตรวจสอบภายใน หมายถึง กิจกรรมให้ความเชื่อมั่นและการให้คำปรึกษา อย่างเที่ยงธรรมและเป็นอิสระ ซึ่งจัดให้มีขึ้นเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานของหน่วยงานของรัฐให้ดีขึ้น และจะช่วยให้หน่วยงานของรัฐบรรลุถึงเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ด้วยการประเมิน และปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบ

4.2 การตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Auditing) หมายถึง การค้นหาหลักฐานสำหรับสิ่งผิดปกติที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ (IT) โดยมีวัตถุประสงค์เพื่อประเมินความเพียงพอของการควบคุมภายในด้าน IT และการจัดการความเสี่ยงด้าน IT ความถูกต้อง น่าเชื่อถือ และความมั่นคงปลอดภัยของข้อมูลในระบบเทคโนโลยีสารสนเทศ มีการปกป้องทรัพย์สิน ซึ่งจะช่วยให้ผู้ใช้งานสามารถใช้ระบบได้อย่างมีประสิทธิภาพ และตอบสนองวัตถุประสงค์และบรรลุเป้าหมายขององค์กรได้อย่างมีประสิทธิภาพ

4.3 ระบบเทคโนโลยีสารสนเทศ (IT) หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

4.4 ข้อมูลสารสนเทศ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

4.5 ระบบสารสนเทศ หมายถึง ระบบของการจัดเก็บ ประมวลผลข้อมูล โดยอาศัยบุคคลและเทคโนโลยีสารสนเทศในการดำเนินการ เพื่อให้ได้สารสนเทศที่เหมาะสมกับงาน หรือภารกิจแต่ละอย่าง หรือหมายถึงระบบที่ใช้ในการจัดเก็บ บันทึก ประมวลผล และจัดทำรายงานสารสนเทศให้ผู้บริหารและผู้ปฏิบัติใช้งาน

4.6 ส่วนราชการ หมายถึง กรมพัฒนาที่ดิน

4.7 อธิบดี หมายถึง อธิบดีกรมพัฒนาที่ดิน

4.8 หน่วยรับตรวจ หมายถึง หน่วยงานที่รับผิดชอบในการปฏิบัติงานของกรมพัฒนาที่ดิน

4.9 ผู้อำนวยการหน่วยรับตรวจ หมายถึง ผู้อำนวยการสำนัก/กอง/สพข./สพด./ศูนย์ฯ

4.10 กลุ่มตรวจสอบภายใน หมายถึง กลุ่มตรวจสอบภายในของกรมพัฒนาที่ดินตามกฎกระทรวงแบ่งส่วนราชการกรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์ พ.ศ. 2554

4.11 ผู้อำนวยการกลุ่มตรวจสอบภายใน หมายถึง ตำแหน่งสูงสุดในกลุ่มตรวจสอบภายใน ซึ่งทำหน้าที่ในการกำกับดูแลการบริหารงานของกลุ่มตรวจสอบภายใน

4.12 ผู้ตรวจสอบภายใน หมายถึง ผู้ที่ได้รับการแต่งตั้งจากอธิบดีกรมพัฒนาที่ดินให้ปฏิบัติงานตรวจสอบภายในของกรมพัฒนาที่ดิน

4.13 กระดาษทำการ หมายถึง เอกสารแบบฟอร์มที่ผู้ตรวจสอบภายในจัดทำขึ้นในระหว่างการตรวจสอบเพื่อบันทึกรายละเอียดการทำงานซึ่งประกอบด้วยข้อมูลต่าง ๆ ที่ใช้ในการตรวจสอบ ขอบเขตการตรวจสอบ วิธีการตรวจสอบ ข้อมูลจากการประเมินและวิเคราะห์ ผลสรุปของการตรวจสอบและติดตามผลการแก้ไขตามข้อเสนอแนะเพื่อใช้เป็นแนวทางในการรายงานผลการปฏิบัติงานและรายงานการติดตามผลการดำเนินการตามข้อเสนอแนะ

4.14 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ หมายถึง ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

4.15 ผู้ใช้งาน หมายถึง ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

4.16 สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

4.17 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตนั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

4.18 ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

4.19 Chief Security Officer (CSO) หมายถึง ผู้บริหารระดับสูงที่มีส่วนเกี่ยวข้องกับ Security ภายในองค์กร ซึ่งมีหน้าที่ที่ต้องรับผิดชอบดูแลในส่วนของความปลอดภัยของทั้งองค์กร โดยกำหนดเป้าหมายนโยบายด้านการรักษาความปลอดภัยข้อมูล โดยกำหนดให้ไปในทิศทางเดียวกันกับแผนยุทธศาสตร์ขององค์กร

จัดการพัฒนานโยบายด้านการรักษาความปลอดภัยข้อมูล จัดการบริหารเฝ้าระวังการโจมตีระบบและภัยต่าง ๆ ที่อาจเกิดขึ้นกับระบบมีการบริหารความเสี่ยง (Risk Management) และการวิเคราะห์ความเสี่ยง (Risk Analysis)

5. หน้าที่ความรับผิดชอบ

5.1 อธิบดี มีหน้าที่ พิจารณาสั่งการและลงนามในรายงานผลการตรวจสอบ และรายงานผลการดำเนินการตามข้อเสนอแนะ

5.2 ผู้อำนวยการหน่วยรับตรวจ (สำนัก/กอง/สพข./สพด./ศูนย์ฯ) มีหน้าที่

5.2.1 กำกับ ควบคุม เจ้าหน้าที่ในหน่วยงาน ให้ความร่วมมือและอำนวยความสะดวกในการปฏิบัติงานของกลุ่มตรวจสอบภายในให้บรรลุวัตถุประสงค์การตรวจสอบ

5.2.2 พิจารณาสั่งการให้ผู้รับผิดชอบในการปฏิบัติงานแต่ละด้านดำเนินการตามข้อสั่งการของอธิบดีในรายงานผลการตรวจสอบ

5.2.3 ลงนามในรายงานการติดตามผลการดำเนินการตามข้อเสนอแนะมายังกลุ่มตรวจสอบภายใน

5.3 ผู้อำนวยการกลุ่มตรวจสอบภายใน มีหน้าที่

5.3.1 ควบคุม กำกับ สอบทานการปฏิบัติงานของผู้ตรวจสอบภายในให้เป็นไปตามแผนการปฏิบัติงาน

5.3.2 สอบทานรายงานผลการตรวจสอบ

5.3.3 ลงนามในรายงานผลการตรวจสอบเสนอผู้บริหารกรมพัฒนาที่ดิน

5.3.4 พิจารณาแผนการติดตามผลการตรวจสอบและแบบติดตามผลการดำเนินการตามข้อเสนอแนะ

5.3.5 ลงนามในรายงานการติดตามผลการดำเนินการตามข้อเสนอแนะเสนอผู้บริหารกรมพัฒนาที่ดินเพื่อทราบหรือพิจารณาสั่งการ

5.4 ผู้ตรวจสอบภายใน มีหน้าที่

5.4.1 วางแผนปฏิบัติงานตรวจสอบในเรื่องที่ได้รับมอบหมายจากผู้อำนวยการกลุ่มตรวจสอบภายใน

5.4.2 ปฏิบัติงานตรวจสอบตามแผนการปฏิบัติงาน และบันทึกข้อมูลลงในกระดาษทำการ

5.4.3 รวบรวมกระดาษทำการเพื่อสรุปผลการตรวจสอบ พร้อมทั้งผลกระทบ และข้อเสนอแนะ

5.4.4 จัดทำ (ร่าง) รายงานผลการตรวจสอบเสนอผู้อำนวยการกลุ่มตรวจสอบภายในพิจารณาและหารือกับหน่วยรับตรวจ

5.4.5 จัดทำรายงานผลการตรวจสอบเสนอผู้อำนวยการกลุ่มตรวจสอบภายในพิจารณา

5.4.6 จัดส่งรายงานผลการตรวจสอบที่อธิบดีสั่งการให้กับหน่วยรับตรวจปฏิบัติตามข้อสั่งการ

5.4.7 กำหนดขั้นตอนการติดตามและจัดทำแผนแบบติดตามผลการดำเนินการตามข้อเสนอแนะเสนอผู้อำนวยการกลุ่มตรวจสอบภายในสอบทานและพิจารณา และให้หน่วยรับตรวจแสดงความคิดเห็นต่อแผนการติดตาม

5.4.8 จัดส่งแผนการติดตามผลการตรวจสอบของกลุ่มตรวจสอบภายในให้หน่วยรับตรวจรับทราบ

5.4.9 ติดตามการแก้ไขตามข้อเสนอแนะพร้อมหลักฐานกับหน่วยรับตรวจภายในระยะเวลากำหนด

5.4.10 ประมวลผลวิเคราะห์และสรุปผลการติดตามการแก้ไขตามข้อเสนอแนะ

5.4.11 จัดทำ (ร่าง) รายงานการติดตามผลการดำเนินการตามข้อเสนอแนะเสนอผู้อำนวยการกลุ่มตรวจสอบภายในพิจารณา สอบทาน

5.4.12 จัดทำรายงานการติดตามผลการดำเนินการตามข้อเสนอแนะเสนอผู้อำนวยการกลุ่มตรวจสอบภายใน เพื่อเสนอผู้บริหารกรมพัฒนาที่ดิน

5.4.13 จัดส่งรายงานการติดตามผลการดำเนินการตามข้อเสนอแนะให้กับหน่วยรับตรวจทราบหรือปฏิบัติตามข้อสั่งการของผู้บริหารกรมพัฒนาที่ดิน (เฉพาะหน่วยรับตรวจที่รายงานไม่ครบทุกประเด็นหรือมิได้รายงานผลการแก้ไขตามข้อเสนอแนะ)

5.4.14 สำเนารายงานการติดตามผลการดำเนินการตามข้อเสนอแนะเข้าแฟ้มถาวร

5.5 หน่วยรับตรวจ มีหน้าที่

5.5.1 อำนวยความสะดวกและให้ความร่วมมือแก่ผู้ตรวจสอบภายใน

5.5.2 จัดเตรียมเอกสารหลักฐานที่เกี่ยวกับการดำเนินงาน รวมถึงข้อมูลที่เกี่ยวข้องให้ครบถ้วน สมบูรณ์พร้อมที่จะตรวจสอบได้

5.5.3 จัดทำบัญชีและจัดเก็บเอกสารประกอบรายการบัญชีพร้อมที่จะให้ผู้ตรวจสอบภายในตรวจสอบได้

5.5.4 จัดให้มีระบบการเก็บเอกสารในการปฏิบัติงานที่เหมาะสมและครบถ้วน

5.5.5 ชี้แจงและตอบข้อซักถามต่าง ๆ พร้อมทั้งหาข้อมูลเพิ่มเติมให้แก่ผู้ตรวจสอบภายใน

5.5.6 ปฏิบัติตามข้อทักท้วง และข้อเสนอแนะของผู้ตรวจสอบภายในในเรื่องต่าง ๆ ที่หัวหน้าหน่วยงานของรัฐสั่งให้ปฏิบัติ

5.5.7 รายงานผลการปฏิบัติตามข้อเสนอแนะของกลุ่มตรวจสอบภายใน พร้อมหลักฐานจัดส่งให้กลุ่มตรวจสอบภายใน ภายในระยะเวลาที่กำหนดตามแผนการติดตามผลการตรวจสอบของกลุ่มตรวจสอบภายใน

บทที่ 2

แนวคิดและหลักการตรวจสอบ

เอกสารวิชาการ การตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกรมพัฒนาที่ดิน ได้มีการศึกษาแนวคิดและหลักการที่เกี่ยวข้องเพื่อปรับใช้ในการตรวจสอบ ดังนี้

1. แนวคิดการตรวจสอบเทคโนโลยีสารสนเทศ “ความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ” ได้แก่

1.1 ความหมายของการตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Auditing)

1.2 วัตถุประสงค์ของการตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Auditing)

1.3 แนวคิดการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

2. หลักการวิเคราะห์ประเด็นตรวจสอบเทคโนโลยีสารสนเทศ “ความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ”

3. ความรู้พื้นฐานสำหรับการตรวจสอบเทคโนโลยีสารสนเทศและแนวคิดระบบการควบคุมภายใน (Internal Control System)

4. กฎหมาย ระเบียบ แนวปฏิบัติ ที่เกี่ยวของกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

4.1 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

4.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ฉบับที่ 2) พ.ศ. 2560

4.3 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

5. วิธีการ ขั้นตอนการปฏิบัติงานตรวจสอบตามมาตรฐานการตรวจสอบภาครัฐ

1. แนวคิดการตรวจสอบเทคโนโลยีสารสนเทศ “ความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ”

1.1 ความหมายของการตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Auditing)

การตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Auditing) หมายถึง การค้นหาหลักฐานสำหรับสิ่งผิดปกติที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ (แนวทางตรวจสอบระบบเทคโนโลยีสารสนเทศ ฝ่ายตรวจสอบระบบเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์, 2560)

1.2 วัตถุประสงค์ของการตรวจสอบเทคโนโลยีสารสนเทศ (Information Technology Auditing)

เพื่อประเมินความเพียงพอของการควบคุมภายในด้าน IT และการจัดการความเสี่ยงด้าน IT ความถูกต้องน่าเชื่อถือ และความมั่นคงปลอดภัยของข้อมูลในระบบเทคโนโลยีสารสนเทศ มีการปกป้องทรัพย์สิน ซึ่งจะช่วยให้ผู้ใช้งานสามารถใช้ระบบได้อย่างมีประสิทธิภาพ และตอบสนองวัตถุประสงค์และบรรลุเป้าหมายขององค์กรได้อย่างมีประสิทธิภาพ (แนวทางตรวจสอบระบบเทคโนโลยีสารสนเทศ ฝ่ายตรวจสอบระบบเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์, 2560)

1.3 แนวคิดการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

(กรมบัญชีกลาง, 2560) การควบคุมภายในด้านเทคโนโลยีสารสนเทศ ประกอบด้วย การควบคุมทั่วไป (General Control) และการควบคุมเฉพาะระบบงาน (Application Control)

1.3.1 การควบคุมทั่วไป (General Control) หมายถึง การควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุม นโยบายและวิธีการในการควบคุมระบบสารสนเทศ การควบคุมความปลอดภัย การควบคุมการพัฒนาและปรับปรุง และการป้องกัน/ลดความเสียหาย ของระบบ เป็นการควบคุมภายในสำหรับองค์กรในภาพรวม โดยมีองค์ประกอบการพิจารณา ดังนี้

(1) การกำหนดนโยบายในการใช้สารสนเทศ

(1.1) มีนโยบายการรักษาความปลอดภัย ด้านระบบเทคโนโลยีสารสนเทศ ที่ชัดเจนว่าใครต้องการเข้าถึง ข้อมูลอะไร เมื่อไหร่ ในระบบงานใด

(1.2) การให้สิทธิในการเข้าถึงข้อมูลเฉพาะบุคคลที่มีสิทธิในการเข้าถึงข้อมูลนั้น

(2) การแบ่งแยกหน้าที่งานในระบบสารสนเทศ

มีการแบ่งแยกหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานในระบบงานคอมพิวเตอร์ให้ชัดเจน เช่น แยกหน้าที่ การพัฒนาระบบออกจากหน้าที่ผู้ปฏิบัติการคอมพิวเตอร์ ผู้บริหารฐานข้อมูล (Database Administrator) ต้องไม่ทำหน้าที่อื่น ผู้พัฒนาระบบออกจากผู้ดูแลบำรุงรักษาระบบ

(3) การควบคุมโครงการพัฒนาระบบสารสนเทศ

โดยกำหนดแผนระยะยาว แผนงานพัฒนาระบบ กำหนดการประมวลผลข้อมูล มอบหมายหน้าที่ และความรับผิดชอบ การประเมินผลงานระหว่างการดำเนินโครงการ การสอบทานภายหลังการติดตั้งระบบ และนำระบบมาใช้งาน การวัดผลการดำเนินงานของระบบ

(4) การควบคุมการเปลี่ยนแปลงแก้ไขระบบ

โดยการกำหนดระเบียบวิธีปฏิบัติในการแก้ไขระบบที่เป็นลายลักษณ์อักษรมีการศึกษาถึงผลกระทบต่าง ๆ มีการทดสอบระบบที่แก้ไขแล้วก่อนนำไปใช้ จัดทำเอกสารคู่มือประกอบการแก้ไข และประเมินผลและสอบทานระบบงานภายหลังเริ่มใช้

(5) การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์

การประมวลผลข้อมูลของระบบงานต่าง ๆ มีความถูกต้อง ครบถ้วน การกู้คืนระบบและการสำรองข้อมูล การทดสอบ และการจัดการกับปัญหาของระบบ จัดทำแผนสำรอง

(6) การควบคุมเข้าถึงอุปกรณ์คอมพิวเตอร์

มีสถานที่จัดเก็บอุปกรณ์คอมพิวเตอร์มิดชิด ไม่มีอากาศร้อน ชื้น และมีการรักษาความปลอดภัยหนาแน่น กำหนดการเข้าออกได้เฉพาะผู้เกี่ยวข้อง กำหนดนโยบายรักษาความปลอดภัยที่ชัดเจน ติดระบบเตือนภัย กรณีมีผู้บุกรุก จำกัดให้ใช้โทรศัพท์เฉพาะเรื่องที่เกี่ยวกับงาน ติดอุปกรณ์ป้องกันเครื่องคอมพิวเตอร์

(7) การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ การกำหนดผู้ใช้ (User Views or Subschema) ตารางแสดงสิทธิในการเข้าถึงฐานข้อมูล (Database Authorization Table) และการเข้ารหัสข้อมูล (Data Encryption)

(8) การควบคุมการเข้าถึงระบบงาน ดังนี้

(8.1) การพิสูจน์ตัวจริง (Authentication) โดยกาหนดรหัสผ่าน (Password)

(8.2) การระบุตัวตนด้วยสิ่งที่มีทางกายภาพ (Physical Possession Identification)

(8.3) การกำหนดสิทธิ (Authorization)

(8.4) การบันทึกกิจกรรมต่าง ๆ ในระบบเพื่อการตรวจสอบ (Audit Logging)

1.3.2 การควบคุมเฉพาะระบบงาน (Application Control)

การควบคุมรายการข้อมูลในแต่ละระบบงานให้มีความถูกต้องและครบถ้วน โดยอาศัยทางเดินของข้อมูลเป็นแนวทางในการกำหนดขอบเขตการควบคุม เช่น ระบบ GFMIS โดยมีองค์ประกอบ ดังนี้

(1) การควบคุมการนำเข้าข้อมูล การควบคุมเกี่ยวกับงานจัดทำข้อมูลก่อนป้อนเข้าสู่ระบบคอมพิวเตอร์ การเตรียมข้อมูลนำเข้า การป้องกันข้อผิดพลาด การค้นหาข้อผิดพลาด และการแก้ไขข้อผิดพลาด เช่น การตรวจสอบตัวเลขตรวจสอบ (Check digit) ว่าเป็นตัวเลขที่ถูกหรือไม่ โดยเลขประจำตัว หรือรหัสสินค้า หรือเลขที่บัญชี

(2) การควบคุมการทำรายการป้อนเข้าสู่ระบบงาน โดยข้อมูลที่ป้อนเข้าสู่ระบบจะต้องถูกหลักเกณฑ์ ในการทำรายการ นอกจากนี้ยังรวมถึงเรื่องที่เกี่ยวกับการกระทบยอดข้อมูลนำเข้า เพื่อพิสูจน์ความถูกต้อง

(3) การควบคุมการสื่อสารข้อมูลให้มีความถูกต้องและครบถ้วน ซึ่งจะต้องคำนึงถึง Hardware และ Software ที่ใช้ในการสื่อสารข้อมูลการมอบอำนาจ

(4) การควบคุมการประมวลผลด้วยคอมพิวเตอร์ ให้มีความแม่นยำ ถูกต้อง และครบถ้วน เป็นไปตามหลักเกณฑ์การใช้แฟ้มข้อมูล การชี้แนะให้เห็นข้อผิดพลาด และการรายงาน

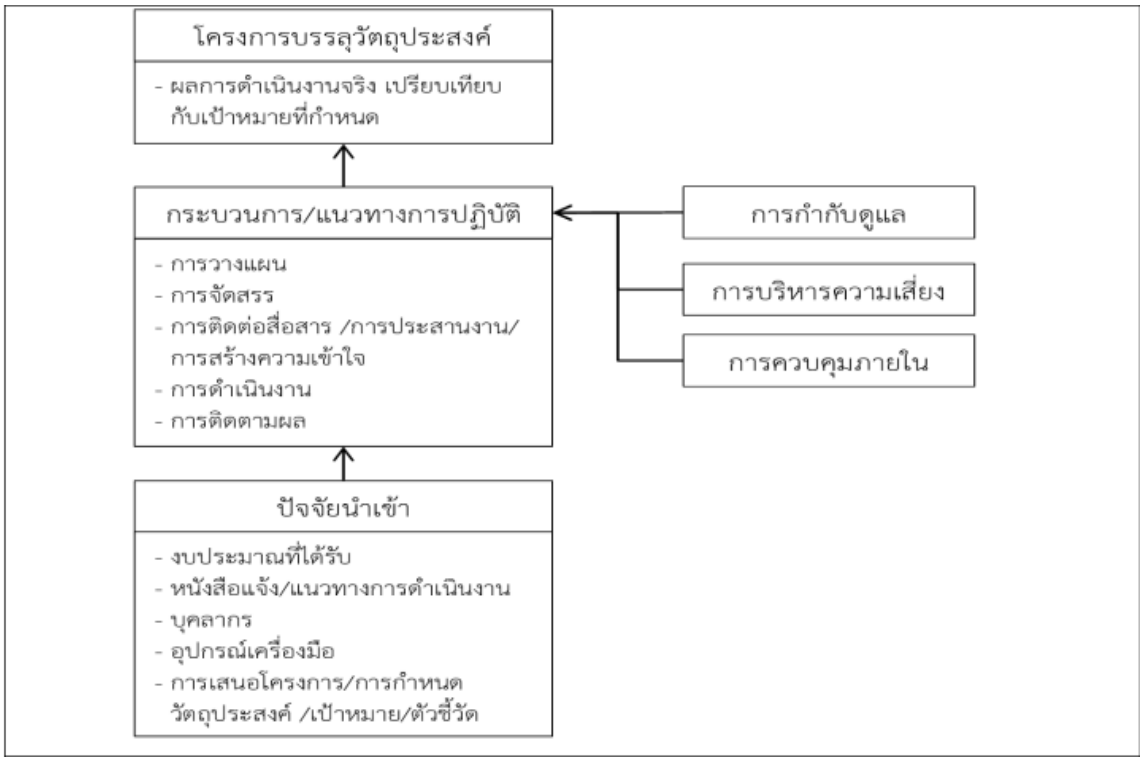
(5) การควบคุมการจัดเก็บข้อมูลไว้ในระบบ การกำหนดสิทธิการใช้ข้อมูล การรักษาความปลอดภัย การแก้ไขข้อผิดพลาด การสำรองข้อมูล และการกำหนดอายุการจัดเก็บแฟ้มข้อมูล

(6) การควบคุมผลลัพธ์ การกระทบยอดข้อมูลนำเข้าและผลลัพธ์ เพื่อพิสูจน์ความถูกต้องด้วยระบบ Manual ซึ่งเป็นหน้าที่โดยตรงของหน่วยงานควบคุมคุณภาพข้อมูล

2. หลักการวิเคราะห์ประเด็นตรวจสอบเทคโนโลยีสารสนเทศ “ความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ”

(กรมบัญชีกลาง, 2546) การกำหนดประเด็นที่จะตรวจสอบ ซึ่งได้จากการสำรวจข้อมูลเบื้องต้น เป็นการระบุจุดที่ต้องการหรือประเด็นเบื้องต้น หรืออีกนัยหนึ่งคือ ปัญหาสำคัญที่ควรตรวจสอบ (Matter Of Potential Significant : MOPS) ทั้งนี้ เนื่องจากการตรวจสอบเพื่อให้บรรลุวัตถุประสงค์ตามที่กำหนดอาจมีประเด็นที่ต้องพิจารณาจำนวนมาก ซึ่งหลักการ ค้นหาจุดที่สำคัญพิจารณาได้หลายทาง เช่น ผลการตรวจสอบครั้งก่อน (ถ้ามี) ผลการประเมินการควบคุมภายใน เป็นต้น

ภาพ ที่ 1 แสดงประเด็นที่ควรทำการสำรวจข้อมูลเบื้องต้นของโครงการ (Matter Of Potential Significant : MOPS)



เมื่อสำรวจข้อมูลแล้วเสร็จ ผู้ตรวจสอบจะสามารถระบุประเด็นปัญหาสำคัญได้ (Matter Of Significant : MOS) ให้นำประเด็นปัญหาสำคัญนั้นมากำหนดเป็นประเด็นการตรวจสอบ และแม้การกำหนดประเด็นการตรวจสอบจะมาจากปัญหาที่สำคัญ แต่วิธีการเขียนประเด็นการตรวจสอบไม่ควรเขียนในเชิงลบ (Negative)

ตัวอย่าง การกำหนดประเด็นตามกระบวนการ เช่น กรณีตรวจสอบการปฏิบัติตามระเบียบถ้ากำหนดวัตถุประสงค์ว่า เพื่อให้มั่นใจว่าการดำเนินการจัดทำนโยบายด้านสารสนเทศของหน่วยงานและการปฏิบัติงานเป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ซึ่งหากผู้ตรวจสอบภายในมิได้ระบุประเด็นการตรวจสอบ หมายความว่า ผู้ตรวจสอบภายในต้องตรวจสอบการดำเนินการทั้งหมด ซึ่งมีกฎหมายระเบียบหลายฉบับที่เกี่ยวข้อง ดังนั้นเพื่อให้ผู้ตรวจสอบภายในทุกคนในทีมเข้าใจตรงกัน และง่ายต่อการปฏิบัติงานจึงต้องกำหนดประเด็นในการตรวจสอบตามกระบวนการ/ขั้นตอนที่ได้จากการสำรวจข้อมูล พร้อมทั้งระบุวัตถุประสงค์ของการตรวจสอบในแต่ละประเด็น

3. ความรู้พื้นฐานสำหรับการตรวจสอบเทคโนโลยีสารสนเทศและแนวคิดระบบการควบคุมภายใน (Internal Control System)

ผู้ตรวจสอบภายในที่ได้รับมอบหมายให้ตรวจสอบระบบสารสนเทศ ตามมาตรฐานการตรวจสอบภายในด้านคุณสมบัติรหัสมาตรฐาน 1220 ความระมัดระวังรอบคอบเยี่ยงผู้ประกอบวิชาชีพจำเป็นต้องมีความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศ ความเสี่ยงและการควบคุมภายใน ความเชี่ยวชาญเกี่ยวกับระบบเทคโนโลยีสารสนเทศ เช่น ตรวจสอบระบบ GFMIS ต้องมีความรู้ ความเข้าใจในระบบ SAP และความเสี่ยง

การควบคุมภายในของระบบเทคโนโลยีสารสนเทศ โดยพิจารณาจาก Flowchart การทดสอบความเชื่อมโยงของระบบ (กระทรวงศึกษาธิการ, ๒๕๕๕)

3.1 โครงสร้างพื้นฐานด้านสารสนเทศ ประกอบด้วย

3.1.1 อุปกรณ์ : Hardware

3.1.2 โปรแกรม : Software

3.1.3 ฐานข้อมูล : Data & Storage Technology

3.1.4 เครือข่าย : Networks

3.1.5 บุคลากร : People ware

ภาพที่ 2 แสดงความเชื่อมโยงโครงสร้างพื้นฐานด้านสารสนเทศและการควบคุมความปลอดภัย

3.2 การควบคุมความปลอดภัย แบ่งเป็น 3 ด้าน คือ

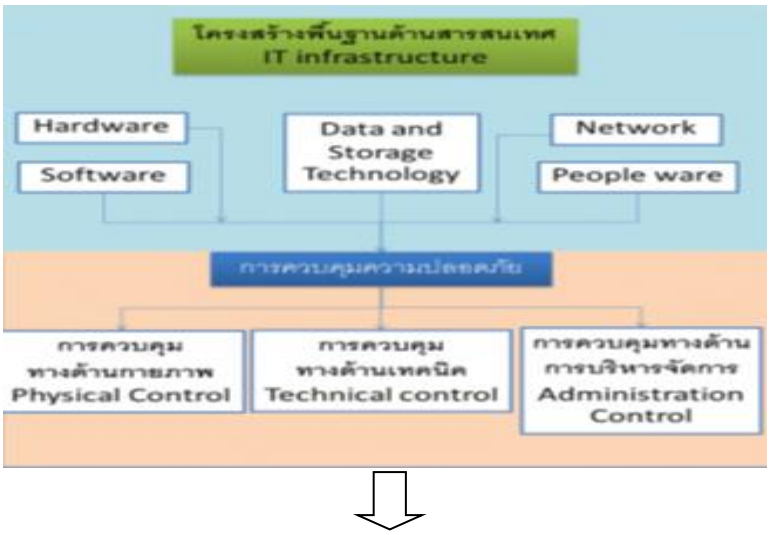
3.2.1 ด้านกายภาพ (Physical Control)

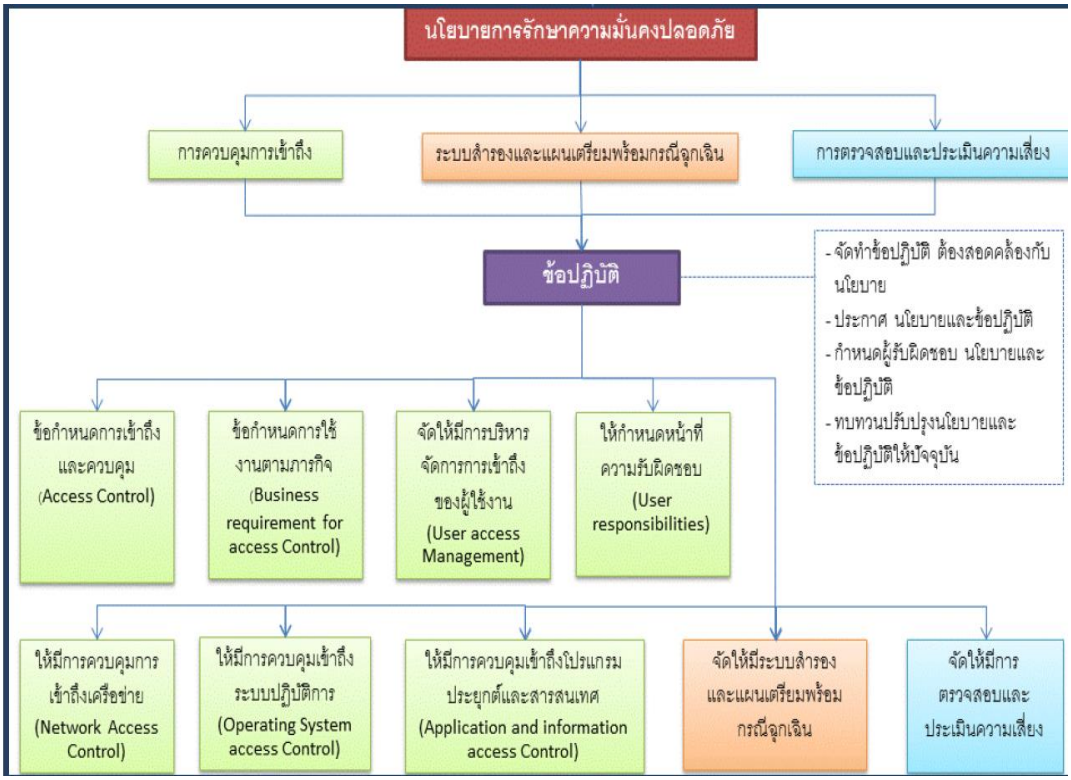
3.2.2 ด้านเทคนิค (Technical Control)

3.2.3 ด้านการบริหารจัดการ (Administrative Control)

3.3 การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนด

ภาพที่ 3 แสดงความเชื่อมโยงการควบคุมความปลอดภัยกับนโยบายและข้อปฏิบัติ ตามประกาศของหน่วยงาน





3.4 ความรู้พื้นฐานสำหรับการตรวจสอบเทคโนโลยีสารสนเทศ

3.4.1 การตรวจสอบการควบคุมทั่วไป

โดยตรวจสอบในเรื่อง การวางแผนระยะยาวและแผนระยะสั้น การจัดโครงสร้างงานสารสนเทศมีความเหมาะสมชัดเจน (การแบ่งแยกหน้าที่เหมาะสม) การพัฒนาและการเปลี่ยนแปลงแก้ไขระบบงาน การรักษาความปลอดภัยระบบสารสนเทศ การปฏิบัติการคอมพิวเตอร์ (การปิด-เปิดระบบ การบำรุงรักษา การจัดเก็บ) การจัดทำแผนกู้ระบบสารสนเทศ

3.4.2 การตรวจสอบการควบคุมเฉพาะระบบงาน

โดยการตรวจสอบในเรื่อง การกำหนดสิทธิในการใช้งานมีความเหมาะสมกับหน้าที่ความรับผิดชอบหรือไม่ การแบ่งแยกหน้าที่ในระบบงานสารสนเทศ การนำเข้าข้อมูลและรายการ การรับ-ส่งข้อมูลระหว่างระบบงาน การประมวลผลในระบบงาน การนำผลลัพธ์ไปใช้งานครบถ้วน ถูกต้องหรือไม่ มีการจัดเก็บเหมาะสมหรือไม่

4. กฎหมาย ระเบียบ แนวปฏิบัติ ที่เกี่ยวของกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

4.1 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ประกาศ ณ วันที่ 31 พ.ค. 2553 ประกอบด้วยสาระสำคัญ ดังนี้

4.1.1 การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

4.1.2 จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศที่อยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

4.1.3 การตรวจสอบและการประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

4.1.4 จัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ประกอบด้วย

(1) จัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(2) ประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(3) กำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน

(4) ทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

4.1.5 ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาครอบคลุม ดังนี้

(1) การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

(2) การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

(3) ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(4) กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

(5) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(6) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(7) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access control)

(8) ระบบสารสนเทศต้องจัดทำระบบสำรอง

(9) จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(10) กำหนดความรับผิดชอบที่ชัดเจน

(11) สามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่า ข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่า หรือเทียบเท่า

4.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ฉบับที่ 2) พ.ศ. 2560

ปัจจุบันระบบคอมพิวเตอร์เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือ ใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือ ใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ยอมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจสังคมและความมั่นคง ของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน จึงต้องมีการกำหนดบทลงโทษตามมาตรการ เพื่อป้องกันและปราบปรามการกระทำเกี่ยวกับความผิดคอมพิวเตอร์ ได้แก่

4.2.1 การควบคุมระบบคอมพิวเตอร์ของหน่วยงานตาม มาตรา 15 เพื่อป้องกันผู้ใช้บริการที่เข้าไปกระทำความผิดตามพระราชบัญญัติ

4.2.2 การเก็บข้อมูลจราจร ซึ่งหมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ และอื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ตามมาตรา 26 กำหนดให้หน่วยงานต้องจัดเก็บข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า 90 วันนับตั้งแต่การใช้บริการสิ้นสุดลง

4.3 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ปัจจุบันการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมากขึ้น สมควรสนับสนุนให้หน่วยงานของรัฐมีระบบการบริการของตน โดยการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว อันเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ พร้อมกับให้หน่วยงานของรัฐสามารถพัฒนา การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน และสร้างความเชื่อมั่น ของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ ประกอบกับมาตรา 35 วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์พ.ศ. 2544 บัญญัติว่า คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาแล้ว ให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด

ดังนั้น ตามมาตรา 5 หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังตอไปนี้

(1) การเข้าถึงหรือควบคุมการใชงานสารสนเทศ

(2) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใชงานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

กรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพรข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคลไม่ว่าโดยตรงหรือโดยอ้อมให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลสวนบุคคลด้วย โดยแนวนโยบายและแนวปฏิบัติให้หน่วยงานของรัฐ จัดทำเป็นประกาศและต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลบังคับใช้ได้หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

5. วิธีการ ขั้นตอนการปฏิบัติงานตรวจสอบตามมาตรฐานการตรวจสอบภาครัฐ

กระบวนการตรวจสอบระบบสารสนเทศมีกระบวนการเช่นเดียวกับตรวจสอบภายในประเภทอื่น ๆ โดยคู่มือฉบับนี้กล่าวถึงขั้นตอนการปฏิบัติงานตรวจสอบ เริ่มตั้งแต่ผู้ตรวจสอบภายในศึกษาทำความเข้าใจระบบงานสารสนเทศ (การควบคุมและความเสี่ยง) ประเมินความเสี่ยงเพื่อวางแผนการตรวจสอบ จัดทำแผนการปฏิบัติงานตามผลประเมินความเสี่ยง จัดทำกระดาษทำการ สรุปข้อเท็จจริง รายงานผลการตรวจสอบและการติดตามผลการตรวจสอบ ซึ่งเป็นไปตามมาตรฐานงานตรวจสอบภายใน (คู่มือการตรวจสอบภายในกรมพัฒนาที่ดิน, 2560) ดังนี้

5.1 การวางแผนการปฏิบัติงาน (Planning)

การวางแผนการปฏิบัติงานเป็นขั้นตอนที่ผู้ตรวจสอบภายในต้องจัดทำ โดยอาศัยข้อมูลจากการสำรวจข้อมูลเบื้องต้น ศึกษาทำความเข้าใจระบบงานสารสนเทศ (การควบคุมและความเสี่ยง) ประเมินผลความเสี่ยง ให้คลอบคลุมประเด็นการตรวจสอบที่มีความสำคัญรวมถึงออกแบบกระดาษทำการ (Working Paper) เพื่อเป็นหลักฐานการปฏิบัติงานตรวจสอบ โดยการผลลัพธ์ของการวางแผนการปฏิบัติงานอยู่ในรูปแบบแผนการปฏิบัติงาน (Engagement Plan) ซึ่งต้องผ่านการเห็นชอบจากผู้อำนวยการกลุ่มตรวจสอบภายใน โดยมีขั้นตอนดำเนินการ ดังนี้

5.1.1 การกำหนดประเด็นการตรวจสอบ ผู้ตรวจสอบภายในควรทำการสำรวจข้อมูลในด้านต่าง ๆ เช่น รวบรวมข้อมูลเกี่ยวกับกิจกรรม ประชุมหารือกับผู้บริหารของหน่วยรับตรวจ สัมภาษณ์บุคคลทั้งภายในและภายนอก ที่มีส่วนเกี่ยวข้องกับกิจกรรมที่จะตรวจสอบ วิเคราะห์เปรียบเทียบข้อมูลที่สำรวจได้ เป็นต้น

เพื่อหาข้อมูลหลักฐานเพิ่มเติมที่จะกำหนดประเด็นของการตรวจสอบว่าประเด็นใดควรตรวจสอบในรายละเอียดเพื่อจะได้กำหนดวัตถุประสงค์ ขอบเขต และแนวทางการปฏิบัติตรวจสอบในรายละเอียดต่อไป

5.1.2 การกำหนดวัตถุประสงค์ในการปฏิบัติงาน เมื่อได้ประเด็นการตรวจสอบแล้ว ผู้ตรวจสอบภายในควรกำหนดวัตถุประสงค์ให้ครอบคลุมประเด็นการตรวจสอบที่กำหนด โดยควรดำเนินเรื่องการประเมินความเสี่ยง การควบคุม กระบวนการกำกับดูแล

5.1.3 การกำหนดขอบเขตการปฏิบัติงาน ควรกำหนดให้เพียงพอที่จะบรรลุวัตถุประสงค์ที่กำหนดไว้ให้ครอบคลุมถึงระบบการทำงานต่าง ๆ เอกสารหลักฐาน รายงาน บุคลากร และทรัพย์สินที่เกี่ยวข้อง รวมถึงควรคำนึงถึงทรัพยากรด้านการตรวจสอบภายในที่จะใช้ในการตรวจสอบด้วย

5.1.4 การกำหนดแนวทางการปฏิบัติงาน เป็นการกำหนดวิธีปฏิบัติงานในรายละเอียดที่ผู้ตรวจสอบภายในต้องทำเป็นลายลักษณ์อักษร ซึ่งเป็นส่วนหนึ่งของการปฏิบัติงาน เพื่อใช้เป็นแนวทางในการปฏิบัติงานในรายละเอียดว่าในการตรวจสอบแต่ละเรื่องจะต้องตรวจสอบอะไรบ้าง ด้วยวัตถุประสงค์อะไร ที่หน่วยรับตรวจใด ณ เวลาใด และใช้วิธีการและเทคนิคการตรวจสอบใด ซึ่งจะช่วยในการรวบรวมหลักฐานในรายละเอียดเป็นไปอย่างมีประสิทธิภาพ โดยรายละเอียดขั้นตอนหรือวิธีการปฏิบัติงานตรวจสอบ ประกอบด้วย

(1) เรื่องและหน่วยรับตรวจควรกำหนดว่าเป็นแผนการปฏิบัติงานตรวจสอบในเรื่องใด ณ หน่วยรับตรวจใดบ้าง

(2) วัตถุประสงค์ในการปฏิบัติงาน กำหนดให้ทราบว่าผู้ตรวจสอบภายในจะทราบประเด็นข้อตรวจพบอย่างไรบ้าง เมื่อเสร็จสิ้นการตรวจสอบ

(3) ขอบเขตการปฏิบัติงาน ควรกำหนดขอบเขตประเด็นและปริมาณงานเพื่อแสดงให้เห็นถึงผลสำเร็จตามวัตถุประสงค์ในการปฏิบัติงานที่กำหนดไว้

(4) แนวทางการปฏิบัติงาน กำหนดขั้นตอนหรือวิธีการปฏิบัติงานตรวจสอบในแต่ละเรื่องให้ชัดเจนและเพียงพอ ระบุวิธีการในการคัดเลือกข้อมูล การวิเคราะห์ การประเมินผล และการบันทึกข้อมูลที่ได้รับระหว่างการบริหารงานตรวจสอบ รวมทั้งการกำหนดเทคนิคการตรวจสอบที่เหมาะสมจะช่วยให้การตรวจสอบได้หลักฐานครบถ้วนและเพียงพอที่จะบรรลุวัตถุประสงค์ที่กำหนดไว้

(5) ชื่อผู้ตรวจสอบภายในและระยะเวลาที่ตรวจสอบ เพื่อให้ทราบว่าใครเป็นผู้รับผิดชอบตรวจสอบเรื่องใด และตรวจสอบเมื่อใด

(6) สรุปผลการตรวจสอบ เพื่อใช้บันทึกผลการตรวจสอบโดยสรุปเฉพาะประเด็นการตรวจสอบที่สำคัญพร้อมระบุรหัสกระดาษทำการที่ใช้บันทึกผลการตรวจสอบ เพื่อสะดวกในการอ้างอิงและการค้นหากระดาษทำการ นอกจากนี้ ควรลงลายมือชื่อผู้ตรวจสอบและผู้สอบทานพร้อมทั้งวันที่ตรวจสอบหรือสอบทานไว้ด้วย เพื่อแสดงให้เห็นว่าใครเป็นผู้ตรวจสอบและผู้สอบทาน

5.2 การปฏิบัติงานตรวจสอบ (Examination)

การปฏิบัติงานตรวจสอบ (รหัสมาตรฐาน 2300) สำหรับการตรวจสอบระบบสารสนเทศต้องใช้ความรู้ ทักษะ ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ และหลักการประเมินควบคุมภายใน เพื่อให้การปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพ โดยมีขั้นตอน ดังนี้

5.2.1 ศึกษาข้อมูลพื้นฐานประกอบการตรวจสอบ ระเบียบกฎหมายเกี่ยวข้องกับระบบสารสนเทศ แนวทางการปฏิบัติงานตรวจสอบ และกระดาษทำการ

5.2.2 หัวหน้าทีมงานชี้แจงกับทีมงานเพื่อทำความเข้าใจเนื้อหา ขอบเขต วัตถุประสงค์เป้าหมายของการตรวจสอบ แนวทางการปฏิบัติงานตรวจสอบ วิธีการจัดเก็บข้อมูลในแบบกระดาษทำการต่าง ๆ ตามที่ปรากฏในแผนการปฏิบัติงาน (Engagement Plan) การเข้าถึงแหล่งข้อมูลเพื่อเก็บข้อมูลประกอบการตรวจสอบ

5.2.3 จัดทำหนังสือแจ้งการเข้าตรวจสอบต่อหน่วยรับตรวจ

5.2.4 ประชุมเปิดตรวจเพื่อชี้แจงวัตถุประสงค์ ขอบเขต แนวทางและวิธีการตรวจสอบ และขอความร่วมมือในการให้ข้อมูลประกอบการตรวจสอบ

5.2.5 ดำเนินการสอบทานเอกสารหลักฐานที่เกี่ยวข้องกับการจัดให้มีการควบคุมและการปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ฉบับที่ 2) พ.ศ. 2560 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ที่หน่วยงานใช้อยู่ในปัจจุบัน

5.2.6 ดำเนินการสอบทานการปฏิบัติตามนโยบายและข้อปฏิบัติของหน่วยงานตามจำนวนตัวอย่างที่สุ่มคัดเลือกไว้

5.2.7 สังเกตการณ์ปฏิบัติงานจริงตามระบบควบคุมที่กำหนดตามนโยบายและข้อปฏิบัติ

5.2.8 สอบถามและสัมภาษณ์ ผู้บริหารและผู้ปฏิบัติงาน

5.2.9 ดำเนินการตรวจนับเครื่องมือ อุปกรณ์ด้านระบบเทคโนโลยี และสังเกตสภาพกายภาพและการใช้งานของเครื่องมืออุปกรณ์ดังกล่าว

5.2.10 บันทึกข้อมูลจากการสอบทาน สังเกตการณ์ การตรวจนับ การสัมภาษณ์ การสอบถามในกระดาษทำการที่เกี่ยวข้อง

5.2.11 รวบรวมข้อมูลจากกระดาษทำการทั้งหมด เพื่อสรุปผลการตรวจสอบ ผลกระทบและข้อเสนอแนะ

5.2.12 ประชุมปิดตรวจ เพื่อสรุปผลการตรวจสอบทำความเข้าใจ ชี้แจง และขอความเห็นเพิ่มเติมในบางประเด็นที่ยังเป็นที่สงสัย พร้อมขอบคุณผู้ที่มีส่วนเกี่ยวข้องในการให้ข้อมูลการตรวจสอบ

5.3 การรายงานผลงานการปฏิบัติงาน (Reporting)

การรายงานผลการตรวจสอบ ซึ่งเป็นการรายงานผลการปฏิบัติงานให้ผู้บริหารส่วนราชการรับทราบถึงวัตถุประสงค์ ขอบเขต วิธีการปฏิบัติงานและผลการตรวจสอบ โดยการสรุปข้อตรวจพบ ประเด็นความเสี่ยงที่ควรควบคุมรวมถึงเรื่องอื่น ๆ ที่ผู้บริหารควรรับทราบ พร้อมข้อเสนอแนะในการปรับปรุงเพื่อเสนอให้ผู้บริหารพิจารณาสั่งการต่อไป โดยการจัดทำรายงานผลการตรวจสอบต้องคำนึงถึงความถูกต้อง ความชัดเจน กะทัดรัด ทันกาล สร้างสรรค์ และจูงใจให้ผู้อ่านจับประเด็นได้ตั้งแต่ต้นจนจบ ซึ่งรายละเอียดขั้นตอนวิธีการ ดังนี้

5.3.1 จัดทำ (ร่าง) รายงานผลการตรวจสอบพร้อมทั้งแจ้งให้หน่วยรับตรวจทราบผลเพื่อพิจารณาให้ความเห็น เสนอหัวหน้าหน่วยงานตรวจสอบภายใน

5.3.2 แล้วจัดทำรายงานผลการตรวจสอบพร้อมข้อเสนอแนะ เสนอหัวหน้าส่วนราชการเพื่อพิจารณาสั่งการ

5.3.3 สำเนารายงานผลการตรวจสอบแจ้งหน่วยรับตรวจให้รับทราบและถือปฏิบัติตามข้อสั่งการของหัวหน้าส่วนราชการ พร้อมรายงานผลการดำเนินการตามข้อสั่งการพร้อมเอกสารหลักฐานผ่านระบบสารสนเทศด้านการตรวจสอบภายใน มายังหน่วยงานตรวจสอบภายใน

5.4 การติดตามผล (Follow Up)

หลังจากที่หน่วยรับตรวจได้มีการแจ้งผลการดำเนินงานกลับมา ซึ่งได้มีการติดตามผลการตรวจสอบว่าหน่วยรับตรวจได้มีการรายงานผลการดำเนินงานตามข้อเสนอแนะตามระยะเวลาที่ได้กำหนด หากยังไม่ได้ดำเนินการหน่วยรับตรวจได้รายงานสาเหตุที่ไม่สามารถดำเนินการตามข้อเสนอแนะ หรือไม่ โดยมีขั้นตอนการปฏิบัติงานดังนี้

5.4.1 สอบทานรายงานผลการดำเนินการตามข้อสั่งการพร้อมเอกสารหลักฐานของหน่วยรับตรวจในระบบสารสนเทศด้านการตรวจสอบภายใน

5.4.2 สรุปผลการสอบทาน จัดทำ (ร่าง) รายงานผลการติดตามการดำเนินการตามข้อเสนอแนะเสนอหัวหน้าหน่วยงานตรวจสอบภายใน

5.4.3 จัดทำรายงานผลการติดตามการดำเนินการตามข้อเสนอแนะ เสนอหัวหน้าส่วนราชการเพื่อทราบและพิจารณา

บทที่ 3

การตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

1. ข้อมูลพื้นฐานเพื่อประกอบการตรวจสอบ

แบ่งออกเป็น 2 หัวข้อ คือ การตรวจสอบการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ IT General Control (ITGC) และการตรวจสอบการควบคุมเฉพาะระบบงาน โดยการตรวจสอบการควบคุมทั่วไป เพื่อที่จะประเมินว่าระบบมีการรักษาความลับ มีความสม่ำเสมอของข้อมูล ความพร้อมใช้ของข้อมูล ส่วนการตรวจสอบการควบคุมเฉพาะระบบงาน จะเป็นส่วนการจำกัดการเข้าถึงข้อมูลและสินทรัพย์ และการจัดให้มีการควบคุมและการปฏิบัติตามการควบคุมที่สอดคล้องกับกฎระเบียบที่เกี่ยวกับการรักษาความมั่งคงปลอดภัยระบบสารสนเทศ ซึ่งมีรายละเอียดดังนี้

1.1 การตรวจสอบการควบคุมทั่วไป IT General Control (ITGC)

1.1.1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ เป็นการกำกับดูแลด้านเทคโนโลยีสารสนเทศของผู้บริหารระดับสูงว่าได้มีการกำกับดูแลเทคโนโลยีสารสนเทศ มีการกำหนดทิศทาง โครงสร้างหน่วยงาน แผนการดำเนินงาน การลงทุนด้านการพัฒนา จัดหาบุคลากรด้าน IT และการจัดซื้ออุปกรณ์คอมพิวเตอร์ที่เหมาะสมกับหน่วยงาน การกำหนดนโยบาย มาตรฐานต่าง ๆ และวิธีการปฏิบัติงาน การประเมินความเสี่ยงของการปฏิบัติงานด้าน IT และมีการควบคุมในการปฏิบัติงานให้เป็นไปตามหลักเกณฑ์ของกฎหมาย กฎระเบียบต่าง ๆ ได้อย่างถูกต้อง

1.1.2 การควบคุมการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ ให้ความสำคัญในเรื่องของการบริหารจัดการ และการจัดลำดับความต้องการด้านเทคโนโลยีสารสนเทศของผู้ใช้งานว่าตรงกับความต้องการภายในหน่วยงานหรือไม่ ฉะนั้นต้องมีการจัดลำดับความสำคัญของงานที่มีความต้องการที่มีความเสี่ยงสูง เพื่อที่หน่วยงานจะนำความต้องการมาเรียงลำดับความเสี่ยง เพื่อพัฒนาระบบสารสนเทศเข้ามาใช้ในหน่วยงานตามความต้องการก่อนหลัง โดยผู้ตรวจสอบจะดูว่าหน่วยรับตรวจมีกระบวนการอย่างไร ในการจัดลำดับความเสี่ยงความต้องการด้านเทคโนโลยีสารสนเทศที่มีความต้องการไม่เท่ากันของแต่ละหน่วยงาน ส่วนวิธีการจัดหาการพัฒนา และบำรุงรักษาระบบสารสนเทศ ว่าหน่วยงานมีวิธีการควบคุมการออกแบบระบบได้ครบถ้วนและเป็นไปตามที่ผู้ใช้งานต้องการหรือไม่ และในระหว่างมีการพัฒนา มีกระบวนการทดสอบระบบก่อน มีการนำระบบขึ้นใช้งานจริง มีการบำรุงรักษาระบบให้มีประสิทธิภาพ ประสิทธิผลอย่างไร ปฏิบัติเป็นไปตามแนวทางที่หน่วยงานได้วางไว้หรือไม่ ดังนั้นผู้ตรวจสอบต้องเข้าไปดูการควบคุมด้านนโยบายและแนวปฏิบัติว่าได้มีการกำหนดแนววิธีปฏิบัติให้กับหน่วยงานหรือพนักงานที่จะนำระบบไปใช้งานที่เป็นลายลักษณ์อักษรและมีการเผยแพร่ไปยังผู้ปฏิบัติงาน และได้รับการอนุมัติจากผู้ที่มีอำนาจ และต้องมีการทบทวนวิธีปฏิบัติให้สอดคล้องกับสภาพแวดล้อมที่เปลี่ยนแปลงไปของหน่วยงานให้สามารถปฏิบัติงานในสภาพแวดล้อมที่เปลี่ยนแปลงไปได้ในปัจจุบัน

1.1.3 การควบคุมการบริหารการเปลี่ยนแปลงแก้ไขระบบสารสนเทศ หลังจากมีการใช้งานระบบไปในระยะหนึ่ง ระบบย่อมมีความต้องการใช้งานที่เพิ่มขึ้นที่เปลี่ยนแปลงไปหรือระบบอาจมีปัญหาเกิดขึ้น เพราะฉะนั้นกระบวนการแก้ไขระบบสารสนเทศจะต้องมีการออกแบบการควบคุม เพื่อให้ผู้ปฏิบัติได้มี

แนวทางการปฏิบัติงานตามที่ได้มีการออกแบบไว้ และในส่วนของการที่มีการเปลี่ยนแปลงแก้ไขระบบสารสนเทศไม่ว่าจะเป็นนโยบายและแนวปฏิบัติจะต้องมีการจัดทำขึ้นมา และในส่วนการขอเปลี่ยนแปลงแก้ไขต้องมีการทำเป็นลายลักษณ์อักษรขึ้นมา มีการอนุมัติโดยผู้มีอำนาจเผยแพร่และเพื่อให้เกิดการควบคุมที่ดีควรมีการทบทวนเป็นระยะ

1.1.4 การควบคุมการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

(1) นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) ผู้บริหารของหน่วยงานต้องให้ความสำคัญและมีการออกแบบการควบคุมในส่วนของนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy) และการปฏิบัตินี้ให้กับเจ้าหน้าที่ที่เกี่ยวข้องสามารถนำไปปฏิบัติงานได้จริงมีความมั่นคงปลอดภัย

(2) การควบคุมการเข้าถึงระบบ (Logical Access Control) เป็นการควบคุมว่าการให้สิทธิการเข้าถึงระบบเป็นไปตามอำนาจหน้าที่หรือไม่ และสิทธิที่ได้ยังคงเหมาะสม และมีการใช้งานอยู่หรือไม่ ซึ่งผู้บริหารต้องมีการทบทวนสิ่งที่หน่วยงานกำหนดออกมาว่าเจ้าหน้าที่ได้ปฏิบัติตามขั้นตอนหรือไม่

(3) การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control) หน่วยงานได้มีการแบ่ง Zoning ภายใน และภายนอกว่ามีการแบ่งอย่างชัดเจนหรือไม่ มีการทบทวนหรือไม่ว่า Zone ที่กำหนดไว้ยังคงเหมาะสมสามารถควบคุมการเข้าถึงข้อมูลของผู้ใช้งานได้จริง ๆ มีอุปกรณ์ป้องกันการเข้าถึงข้อมูลครบถ้วนหรือไม่ และหน่วยงานมีการควบคุมให้ผู้ปฏิบัติงานมีการปฏิบัติงานตามคู่มือความมั่นคงปลอดภัยที่กำหนดไว้ในอุปกรณ์ต่าง ๆ ว่ายังคงสามารถใช้งานได้อยู่หรือไม่ หากมีการเข้าถึงข้อมูลจากภายนอกระบบจะต้องมีการกำหนดว่าจะต้องมีการขอและมีการอนุมัติจากใครหรือไม่ภายใต้ข้อกำหนดความมั่นคงปลอดภัย

1.1.5 การควบคุมทางกายภาพและสภาพแวดล้อม

(1) การบริหารจัดการสิทธิการเข้าถึงทางกายภาพ เกี่ยวข้องกับศูนย์คอมพิวเตอร์หลัก DC (Data Center) และศูนย์คอมพิวเตอร์สำรอง DR (Disaster Recovery) ของหน่วยงานที่ Application เหล่านั้นตั้งอยู่ โดย DC (Data Center) และ DR (Disaster Recovery) ถือว่าเป็นพื้นที่ที่มีความสำคัญและมีความเสี่ยงสูง เพราะฉะนั้นการเข้าถึงข้อมูลในศูนย์คอมพิวเตอร์หลัก DC (Data Center) ที่เก็บข้อมูลจะต้องได้รับอนุมัติและเป็นผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้น เพราะฉะนั้นจะต้องมีการทบทวน มีการออกแบบการควบคุมในการจะเข้าถึง DC (Data Center) และ DR (Disaster Recovery) ต้องดำเนินการขอใคร และใครที่ทำหน้าที่อนุมัติและจะต้องมีเอกสารอะไรบ้าง และจะต้องระบุด้วยว่าเข้าไปทำอะไร

(2) การบริหารจัดการและการบำรุงรักษาทรัพย์สินด้าน IT ห้อง DC (Data Center) และ DR (Disaster recovery) ซึ่งเป็นพื้นที่ที่สำคัญที่เก็บอุปกรณ์ต่าง ๆ ซึ่งต้องได้รับการบำรุงรักษาตามระยะเวลาที่กำหนดไว้ และต้องมีการทดสอบตามแผนที่หน่วยงานกำหนดไว้ รวมถึงอุณหภูมิความเย็นของห้องเป็นไปตามที่หน่วยงานกำหนดไว้ เพื่อที่จะให้ในส่วนของ DC (Data Center) และ DR (Disaster Recovery) สามารถทำงานได้อย่างเต็มประสิทธิภาพ ส่วนกล้องต้องมีการเฝ้าสังเกตป้องกันการบุกรุกของ DC (Data Center) และ

DR (Disaster Recovery) ตลอด 24 ชั่วโมงหรือไม่ ซึ่งเหล่านี้เป็นสิ่งที่หน่วยงานต้องมีการพิจารณาว่าเป็นความเสี่ยงประเภทไหนตามที่มีการออกแบบการควบคุมไว้

1.1.6 การควบคุมการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ การให้บริการและการส่งมอบงานด้าน IT ต้องมีการทำข้อตกลงการปฏิบัติงานว่าผู้ปฏิบัติงานได้มีการส่งมอบงานอะไรบ้าง และส่วนของการควบคุมประสิทธิภาพระบบคอมฯ และเครือข่าย หน่วยงานจะต้องมีการออกแบบและการควบคุม เฝ้าสังเกตว่าระบบคอมพิวเตอร์สามารถประมวลผลในอัตราที่หน่วยงานกำหนดไว้หรือไม่ ระบบเครือข่ายมี Down Time หรือไม่ มีการเข้าถึงข้อมูลที่แออัดในช่วงไหนบ้าง ต้องมีการเฝ้าสังเกตและมีการบริหารจัดการเครือข่าย เพื่อให้ระบบสารสนเทศสามารถใช้งานและสามารถดำเนินงานตอบสนองกับการดำเนินงานได้เป็นปกติกับการดำเนินงานหน่วยงานได้ ระบบสารสนเทศต้องมีการสำรองข้อมูลเมื่อเกิดข้อมูลเสียหายเกิดขึ้นหน่วยงานสามารถที่จะมีชุดข้อมูลเดิมที่จะสามารถนำมาใช้แทนชุดข้อมูลเดิมที่มีปัญหาขึ้น และสามารถใช้งานได้ตามปกติ โดยการสำรองหน่วยงานต้องมีการแบ่งว่าข้อมูลที่สำรองนั้นเป็นข้อมูลแบบไหน สำรองแบบทั้งหมด สำรองเฉพาะที่ต่างหรือเฉพาะที่เพิ่มขึ้น ซึ่งหน่วยงานต้องมีการกำหนดว่าจะสำรองแบบไหน และหลังจากมีการสำรองข้อมูลเสร็จเรียบร้อยแล้วอุปกรณ์ที่สำรองหน่วยงานจะต้องมีการจัดเก็บไว้ที่ไหน เก็บในศูนย์คอมพิวเตอร์หลัก DC (Data Center) และศูนย์คอมพิวเตอร์สำรอง DR (Disaster Recovery) กี่ชุดและหลังการจัดเก็บข้อมูลหน่วยงานต้องมีการทดสอบการนำชุดคำสั่งนำมาทดลองการใช้งานว่าสามารถนำกลับมาใช้งานได้อีกหรือไม่

1.1.7 การบริหารความต่อเนื่องทางธุรกิจและแผนฟื้นฟูระบบสารสนเทศ หน่วยงานต้องมีการประเมินว่าในหน่วยงานมีความเสี่ยงทางด้านไหน มีการกำหนดวางแผน BCP (Business Continuity Plan) และ DRP (Disaster Recovery Plan) อย่างไร ถ้าหากระบบเกิดล่ม (Down Time) ขึ้นมาหน่วยงานจะต้องมีการกำหนดระยะเวลาฟื้นฟูระบบกลับมาให้ใช้งานภายในกี่นาที กี่ชั่วโมง โดยหน่วยงานต้องมีการพิจารณาตามเกณฑ์ความเสี่ยงของหน่วยงาน และมีการทดสอบตามแผนว่าสามารถบรรลุวัตถุประสงค์หรือเป็นไปตามที่หน่วยงานได้กำหนดไว้หรือไม่

1.1.8 การควบคุมการใช้บริการ ผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ การควบคุมผู้ให้บริการภายนอก (Outsourcing) ที่หน่วยงานจ้างเข้ามาดำเนินการแทนเจ้าหน้าที่ของหน่วยงานหรือแทนบางส่วนของงานในหน่วยงานว่ามีการกำหนดในส่วนของนโยบายและแนวปฏิบัติหรือไม่ และในสัญญาจ้างต้องมีการกำหนดการรักษาความลับข้อมูลของทางราชการเป็นสัญญาการรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement : NDA) บทลงโทษหากไม่ปฏิบัติตามสัญญา และในส่วนของการกำกับดูแลต้องดูว่าผู้บริการภายนอกทำงานตามสัญญาจ้างอย่างไร การส่งมอบงานเป็นไปตามที่กำหนดในสัญญาหรือไม่ ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศที่จัดทำไว้ได้ครบถ้วนหรือไม่ และสัญญาการรักษาข้อมูลที่เป็นความลับเกี่ยวกับสัญญาจ้างได้มีการจัดทำไว้อย่างครบถ้วนหรือไม่ มีการจัดเก็บอย่างไร มีผู้รับผิดชอบดูแลหรือไม่ ซึ่งเหล่านี้เป็นเรื่องของ IT Outsourcing ที่หน่วยงานจะต้องมีการควบคุม

1.2 การตรวจสอบการควบคุมเฉพาะระบบงาน

การควบคุมการนำเข้าข้อมูล (Input) การควบคุมการประมวลผล (Processing) และการควบคุมการนำข้อมูลออก (Output) ซึ่งทั้ง 3 กระบวนงานนี้ขึ้นอยู่กับการบริหารจัดการสิทธิในการเข้าถึงว่าในทุกขั้นตอนต้องมีการบริหารจัดการสิทธิในการเข้าใช้งานอีกว่าจะให้เข้าถึงแบบจำกัดเฉพาะผู้ที่มีหน้าที่ที่เกี่ยวข้องเท่านั้น

1.2.1 การควบคุมการนำเข้าข้อมูล (Input) โดยการควบคุมการนำเข้าข้อมูล (Input) จะนำเข้าข้อมูลในระบบต้องมีการแจ้งเตือนหรือไม่ ถ้าไม่เป็นไปตามเงื่อนไขที่เราออกแบบไว้ระบบสามารถแจ้ง Error ได้ว่าไม่ถูกต้องตามรูปแบบที่กำหนดไว้หรือไม่ ซึ่งระบบที่ดีต้องมีการแจ้งเตือนได้ด้วยว่าไม่สามารถดำเนินการได้เพราะอะไร และมีส่วนที่เกิดข้อผิดพลาดเกิดจากตรงไหน เพื่อแจ้งให้ผู้ใช้งานได้เข้าใจได้

1.2.2 การควบคุมการประมวลผล (Processing) จะเกี่ยวข้องกับการเข้าถึงการประมวลผลหรือหน้าที่ของผู้ที่จะเข้าถึงมาดำเนินการมาเข้าถึงข้อมูลว่าประมวลผลข้อมูล เมื่อมีข้อผิดพลาดหรือประมวลผลไม่สำเร็จ หน่วยงานมีการดำเนินการอย่างไร มีการบริหารการจัดการอย่างไร และมีการควบคุมอย่างไร สิทธิต่าง ๆ มีการทบทวนหรือไม่ มีการกำหนดสิทธิได้เหมาะสมหรือไม่ เพื่อที่จะให้ความเชื่อมั่นว่าข้อมูลที่เข้ามานั้นได้มีการจัดการกับข้อมูลและข้อมูลมีการประมวลผลได้อย่างถูกต้อง

1.2.3 การควบคุมการแสดงผล (Output) จะเกี่ยวกับการรายงาน (Report) หรือเป็นข้อมูลที่อยู่ในระบบที่เราสามารถทำการค้นหาข้อมูล (Query) มาแสดงผลได้ ซึ่งข้อมูลเหล่านี้ต้องมีการจัดประเภทของข้อมูลอีกว่าข้อมูลส่วนไหนเป็นข้อมูลลับหรือไม่ ข้อมูลไหนเป็นข้อมูลเฉพาะภายในสามารถที่จะเข้าถึงโดยเฉพาะบุคคลภายในเท่านั้น หน่วยงานต้องมีการจัดประเภทรายการอีกว่าข้อมูลไหนลับ ไม่ลับ ข้อมูลไหนสามารถเข้าถึงได้บ้าง และเอกสารที่พิมพ์ออกมา (Print Out) สามารถที่จะพิมพ์ซ้ำได้หรือไม่ ต้องพิจารณาในส่วนของตัว Output และข้อมูลการค้นหาข้อมูล (Query) ถ้าข้อมูลไหนเป็นความลับหน่วยงานจะต้องมีการจำกัดสิทธิในการเข้าถึงข้อมูลด้วย ซึ่งสิ่งเหล่านี้เป็นเรื่องของการบริหารจัดการ Output

2. เทคนิคและเครื่องมือที่ใช้ในการตรวจสอบ

วิธีการรวบรวมหลักฐานและข้อเท็จจริงต่าง ๆ ในการปฏิบัติงานตรวจสอบ โดยผู้ตรวจสอบภายในจะเลือกใช้เทคนิคการตรวจสอบให้เหมาะสมกับเรื่องที่จะตรวจสอบ เพื่อให้ได้มาซึ่งหลักฐานที่เพียงพอ ที่ผู้ตรวจสอบภายในจะเสนอความเห็นและข้อเสนอแนะไว้ในรายงานผลการตรวจสอบ ซึ่งการตรวจสอบเทคโนโลยีสารสนเทศด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ จะใช้เทคนิคและเครื่องมือในการตรวจสอบ ดังนี้

2.1 การสุ่มตัวอย่างตามวิธี Stratified Sampling เป็นการเลือกตัวอย่างของข้อมูลที่มีลักษณะแตกต่างกันที่ได้แบ่งข้อมูลออกเป็นกลุ่ม โดยมี 2 ขั้นตอน ได้แก่

2.1.1 แบ่งข้อมูลออกเป็นกลุ่มโดยการรวมข้อมูลที่มีลักษณะเหมือนกันไว้ในกลุมเดียวกัน

2.1.2 สุมเลือกตัวอย่างจากแต่ละกลุ่มเหล่านั้นอีกครั้งหนึ่ง โดยวิธีการสุ่มตัวอย่างอาจแตกต่างกันไปในแต่ละกลุม

2.2 การตรวจนับ เป็นการพิสูจน์จำนวนและสภาพของสิ่งที่ตรวจนับว่ามีอยู่ครบถ้วนตามที่บันทึกไว้หรือไม่ สภาพของสิ่งของนั้นเป็นอย่างไร อยู่ในสภาพชำรุดเสียหายหรือไม่ อย่างไร

2.3 การวิเคราะห์เปรียบเทียบ เป็นการศึกษาและเปรียบเทียบความสัมพันธ์ และความเปลี่ยนแปลงของข้อมูลต่าง ๆ ว่าเป็นไปตามที่คาดหมาย หรือเป็นไปตามควร หรือไม่

2.4 การสอบถาม เป็นการสอบถามผู้ที่เกี่ยวข้อง เพื่อให้ได้ข้อเท็จจริงต่าง ๆ ทั้งทำเป็นลายลักษณ์อักษรหรือด้วยวาจา

2.5 การสังเกตการณ์ เป็นการสังเกตให้เห็นด้วยตาในสิ่งที่ต้องการทราบอย่างระมัดระวัง แล้วบันทึกเหตุการณ์ต่าง ๆ ไว้

2.6 การประเมินผล เป็นการเปรียบเทียบมาตรฐานหรือหลักเกณฑ์ที่กำหนดไว้กับผลการปฏิบัติงานจริงว่าเกิดผลต่างหรือไม่

3. วิธีการตรวจสอบ

การตรวจสอบตามมาตรฐานความมั่นคงปลอดภัยของแต่ละเรื่อง ดังนี้

3.1 นโยบายความมั่นคงปลอดภัยในหน่วยงาน เป็นการสอบทานการนำนโยบายสู่การปฏิบัติที่เกิดประสิทธิภาพ ประสิทธิผล เป็นไปตามเจตนารมณ์ของนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ตามตารางที่ 1 ดังนี้

ตารางที่ 1 : แสดงวิธีการตรวจสอบนโยบายความมั่นคงปลอดภัยในหน่วยงาน

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
ความชัดเจนในนโยบาย	การสื่อสารในหลายช่องทางเกี่ยวกับการชี้แจงทำความเข้าใจในนโยบาย	- สอบทานวิธีการสื่อสารทำความเข้าใจ เช่น รายงานการประชุม/บทความ/การประชาสัมพันธ์ เว็บไซต์, บอร์ดการประชาสัมพันธ์ ฯลฯ
ความชัดเจนในแนวทางปฏิบัติงาน	- การปฏิบัติงานที่สอดคล้องกับเป้าหมายของนโยบาย - กำหนดผู้รับผิดชอบในแผนงานไว้อย่างชัดเจน และมีการแต่งตั้งผู้รับผิดชอบการขับเคลื่อนนโยบาย	- ตรวจสอบความเหมาะสมของขั้นตอนการปฏิบัติงานที่หน่วยงานกำหนดไว้ แผนงานสอดคล้องกับเป้าหมายของนโยบาย - สัมภาษณ์/สอบถาม/สังเกตการณ์การนำขั้นตอนไปปฏิบัติเกิดผลตามที่คาดหวัง เพียงใด - ตรวจสอบคำสั่งแต่งตั้ง/การมอบหมายหน้าที่ผู้รับผิดชอบ

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
การมอบหมายอำนาจหน้าที่อย่างเหมาะสมในการขับเคลื่อนนโยบาย	- กำหนดขอบเขตการรักษาความมั่นคงปลอดภัย ครอบคลุมทั้ง 3 ระดับ ได้แก่ ผู้บริหาร ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ และผู้ปฏิบัติงานทั่วไปในองค์กร - กำหนดความรับผิดชอบของผู้ที่เกี่ยวข้องในการบริหารจัดการความมั่นคงปลอดภัย	- ตรวจสอบคำสั่งแต่งตั้ง/การมอบหมาย ผู้ที่เกี่ยวข้อง/หน้าที่ขอบเขตการรักษาความมั่นคงปลอดภัย
การจัดระบบการควบคุมกำกับติดตาม ประเมินผลการนำนโยบายสู่การปฏิบัติและการทบทวนแนวทางปฏิบัติ/นโยบาย	ติดตามอย่างสม่ำเสมอ และผลการประเมินตรงกับความเป็นจริง	-ตรวจสอบเอกสารหลักฐานการติดตามประเมินผลการนำนโยบายสู่การปฏิบัติ - สอบทานและสัมภาษณ์เกี่ยวกับกระบวนการติดตามประเมินผลการนำนโยบายสู่การปฏิบัติ

3.2 โครงสร้างความมั่นคงปลอดภัยสารสนเทศ สอบทานถึงประสิทธิภาพ ประสิทธิผลการขับเคลื่อนให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ตามตารางที่ 2 ดังนี้

ตารางที่ 2 : แสดงวิธีการตรวจสอบโครงสร้างความมั่นคงปลอดภัยสารสนเทศ

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
การแต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ CSO ในหน่วยงาน	- การแต่งตั้งคณะกรรมการ CSO - การมอบหมายอำนาจหน้าที่ของคณะกรรมการ CSO ที่ ครอบคลุม 4 กระบวนการ ได้แก่ การกำหนดแนวปฏิบัติ การสื่อสาร การติดตามการประเมินการนำนโยบาย/แนวปฏิบัติ/มาตรการสู่การปฏิบัติ	-ตรวจสอบคำสั่งแต่งตั้งคณะกรรมการ CSO
การขับเคลื่อนระบบการรักษาความมั่นคงปลอดภัยสารสนเทศโดยคณะกรรมการ CSO	การประชุมคณะกรรมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ CSO	- ตรวจสอบหลักฐานการขับเคลื่อน เช่น รายงานการประชุมคณะกรรมการ CSO
การกำหนดบทบาทหน้าที่ของหัวหน้างาน IT ผู้ปฏิบัติงาน IT	- มีการกำหนดบทบาทหน้าที่ของหัวหน้างาน IT ผู้ปฏิบัติงาน IT	- สอบทานบทบาทหน้าที่ของหัวหน้างาน IT ผู้ปฏิบัติงาน IT

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
	- มีแผนผังโครงสร้างการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน	- สอบทานแผนผังโครงสร้างการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงาน - สัมภาษณ์/สอบทานและสังเกตการณ์การปฏิบัติงานของผู้ปฏิบัติงาน IT และหัวหน้างาน IT ว่ามีการปฏิบัติตามโครงสร้างที่กำหนด หรือไม่

3.3 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร สอบทานเกี่ยวกับความเสี่ยงอันเกิดจากการกระทำของบุคลากร จากการใช้อุปกรณ์ผิดวัตถุประสงค์ หรือผู้ไม่มีสิทธิใช้ ตามตารางที่ 3 ดังนี้

ตารางที่ 3 : แสดงวิธีการตรวจสอบความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
การสรรหาบุคลากร	การกำหนดบทบาทหน้าที่ความรับผิดชอบของบุคลากร และบุคลากรภายนอกให้สอดคล้องและปฏิบัติตามกฎ ระเบียบเกี่ยวกับความมั่นคงปลอดภัย ของหน่วยงาน	- ตรวจสอบเอกสารการสรรหาบุคลากรว่ามีการกำหนดบทบาทและหน้าที่ความรับผิดชอบที่ชัดเจนและสอดคล้องและปฏิบัติตามกฎ ระเบียบ เกี่ยวกับความมั่นคงปลอดภัยของหน่วยงาน
ระหว่างการปฏิบัติงาน	- มีการฝึกอบรม และประเมินผลการอบรม อย่างน้อยปีละครั้ง - มีการกำหนดบทลงโทษในการละเมิดแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยระบบสารสนเทศที่หน่วยงานกำหนด	- สอบทานเอกสารการจัดการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศหน่วยงานและการประเมินผล - สอบทานการกำหนดบทลงโทษในการละเมิด
สิ้นสุดการจ้างหรือย้ายหรือลาออก	- กำหนดขอบเขตความรับผิดชอบสำหรับการดำเนินการเลิกจ้างงาน - กำหนดการคืนสินทรัพย์ของหน่วยงานทั้งหมดที่อยู่ในครอบครอง	- สอบทานการกำหนดขอบเขตความรับผิดชอบและแนวทางปฏิบัติสำหรับการเลิกจ้างงาน - สอบทานการคืนทรัพย์สินของหน่วยงาน

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
	- การถอดถอนสิทธิในการเข้าถึงข้อมูลของหน่วยงาน	- สอบทานการถอดถอนสิทธิในการเข้าถึงข้อมูลของหน่วยงาน

3.4 การบริหารทรัพย์สินด้านเทคโนโลยีสารสนเทศ เป็นการสอบทานการควบคุม ดูแล รักษา อุปกรณ์เครื่องมือ ให้มีการใช้งานอย่างคุ้มค่า และป้องกันการสูญหาย ตามตารางที่ 4 ดังนี้

ตารางที่ 4 : แสดงวิธีการตรวจสอบการบริหารทรัพย์สินด้านเทคโนโลยีสารสนเทศ

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
การบริหารจัดการบัญชีทรัพย์สิน	จัดทำทะเบียนบัญชีทรัพย์สิน (อุปกรณ์คอมพิวเตอร์เครือข่าย และ software)	- สอบทานและพิสูจน์ความครบถ้วนและถูกต้องของทะเบียนหรือบัญชีทรัพย์สิน
ผู้ถือครองทรัพย์สิน	- การจัดทำหลักเกณฑ์การจัดสรรอุปกรณ์คอมพิวเตอร์ให้เหมาะสมกับภารกิจบุคลากร และการประกาศใช้ - จัดทำคู่มือการใช้งาน อุปกรณ์เครื่องมือ รวมทั้งการดูแลรักษาและการประกาศใช้ -จัดให้มีการตรวจสอบ บำรุงรักษาอุปกรณ์เครื่องมือให้มีสภาพพร้อมใช้งานตลอดเวลา	-สอบทานหลักเกณฑ์ คู่มือการใช้งานที่หน่วยงานจัดทำขึ้น - สังเกตการณ์ทางกายภาพของทรัพย์สินอยู่ในสภาพพร้อมใช้งาน - สอบทานแผน-ผล การดูแลบำรุงรักษาอุปกรณ์เครื่องมือ
การคืนหลักทรัพย์สิน	การกำหนดนโยบายการคืนทรัพย์สินให้หน่วยงานเมื่อเลิกจ้าง	- สอบทานนโยบายและผลจากการปฏิบัติตามนโยบาย
จัดชั้นความลับของสารสนเทศ	- การจัดหมวดหมู่ทรัพย์สินสารสนเทศ แบ่งเป็น ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้ - กำหนดชั้นความลับ สารสนเทศแบ่งเป็นปกติ ลับ ลับมาก ลับที่สุด - การกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ	- สอบทานทะเบียนคุมทรัพย์สิน -สอบทานการกำหนดชั้นความลับ
กำหนดมาตรการป้องกันอุปกรณ์สารสนเทศที่ใช้งานนอกหน่วยงาน	กำหนดมาตรการป้องกัน อุปกรณ์สารสนเทศที่ใช้งานนอกหน่วยงาน	- สอบทานแนวทางปฏิบัติ/มาตรการ

3.5 การควบคุมการเข้าถึง เป็นการสอบทานการควบคุมการเข้าถึงระบบสารสนเทศ/ข้อมูลและอุปกรณ์ที่สำคัญของหน่วยงาน รวมทั้งประเมินการปฏิบัติของหน่วยงานให้เป็นไปตามนโยบายที่กำหนดตามตารางที่ 5 ดังนี้

ตารางที่ 5 : แสดงวิธีการตรวจสอบการควบคุมการเข้าถึง

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
นโยบายควบคุมการเข้าถึง	กำหนดนโยบาย/แนวทางปฏิบัติการควบคุมการเข้าถึงระบบ	- สอบทานนโยบาย/แนวทางปฏิบัติเกี่ยวกับการควบคุม และการทบทวนเป็นปัจจุบัน
การบริหารจัดการการเข้าถึงของผู้ใช้งาน	- การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน - การจัดการสิทธิการเข้าถึงของผู้ใช้งาน - การบริหารจัดการสิทธิการเข้าถึงตามระดับสิทธิ - การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน - การถอดถอนหรือปรับปรุงสิทธิการเข้าถึง - กำหนดให้เจ้าหน้าที่ที่มีอุปกรณ์คอมพิวเตอร์กำหนดรหัสผ่านในการเข้าใช้งานอุปกรณ์นั้น ๆ	- ทดสอบการลงทะเบียนและการถอดถอนสิทธิผู้ใช้งานในระบบสารสนเทศของหน่วยงาน - ตรวจสอบการกำหนดสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศหน่วยงานและการเข้าถึงอุปกรณ์ที่ใช้งานหรือระบบเครือข่าย - ตรวจสอบการกำหนดระบบการเข้าถึงสารสนเทศตามระดับชั้นความลับสารสนเทศ - ตรวจสอบขั้นตอนการบริหารจัดการข้อมูลรหัสผ่านของผู้ใช้งานและทดสอบการออกรหัสผู้ใช้งานจากระบบ - สอบทานขั้นตอนการถอดถอนสิทธิและทดสอบการถอดถอนสิทธิของเจ้าหน้าที่ที่หมดการจ้าง - สอบทานและทดสอบการกำหนดขั้นตอนการปฏิบัติงานในการกำหนดรหัสผ่านในการเข้าใช้งานทุกอุปกรณ์
การควบคุมการเข้าถึงระบบ	- การออกมาตรการการเข้าถึงระบบเครือข่าย โดยใช้ไอพีแอดเดรส - มีการจัดทำคู่มือขั้นตอนการใช้งาน	- สอบทานมาตรการและทดสอบการเข้าถึงระบบเครือข่ายโดยใช้ไอพีแอดเดรส - สอบทานคู่มือการใช้งานเครือข่าย

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
	- มีการแยกประเภทของ ผู้ใช้งาน และกำหนดการเข้าถึงข้อมูล ในระดับชั้นต่าง ๆ เช่น ผู้บริหาร, ผู้ปฏิบัติงาน ฯลฯ - ขั้นตอนการปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย	- สอบทานรหัสผ่านว่ามีการแยกประเภท ผู้ใช้งานและกำหนดระดับการเข้าถึงข้อมูล หรือไม่ - ตรวจสอบขั้นตอนการปฏิบัติและการทดสอบการล็อกอินเข้าใช้งานระบบ

3.6 การเข้ารหัสข้อมูล เป็นตรวจสอบการเข้ารหัสข้อมูลที่สำคัญของหน่วยงาน เพื่อป้องกันการเปลี่ยนแปลงแก้ไขหรือรั่วไหลของข้อมูล ตามตารางที่ 6 ดังนี้

ตารางที่ 6 : แสดงวิธีการตรวจสอบการเข้ารหัสข้อมูล

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
นโยบายการใช้มาตรการเข้ารหัสข้อมูล	- มีการประกาศนโยบายในการใช้มาตรการเข้ารหัสข้อมูล - ผู้ปฏิบัติงาน IT มีความเข้าใจในนโยบายการเข้าใช้รหัสข้อมูลตามที่หน่วยงานกำหนดไว้	- สอบทานนโยบายการเข้ารหัสข้อมูล - ให้ผู้ปฏิบัติงานเข้ารหัสข้อมูลตามที่หน่วยงานกำหนด

3.7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากความไม่ปลอดภัยทางกายภาพต่อระบบสารสนเทศของหน่วยงาน ตามตารางที่ 7 ดังนี้

ตารางที่ 7 : แสดงวิธีการตรวจสอบความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย	- ขอบเขตหรือบริเวณโดยรอบทางกายภาพในการรักษาความมั่นคงปลอดภัย โดยการประเมินความเสี่ยงเพื่อนำไปจัดลำดับความเสี่ยงในการเข้า-ออก - ควบคุมการเข้า-ออก ทางกายภาพ - การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและอุปกรณ์	- ตรวจสอบการกำหนดขอบเขตหรือบริเวณพื้นในการรักษาความมั่นคงปลอดภัย - ตรวจเยี่ยมชมสถานที่ที่เป็นพื้นที่ที่กำหนดไว้รักษาความปลอดภัยและระบบการควบคุมเข้า-ออกสถานที่

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
	- การป้องกันภัยคุกคามจากภายนอกและสภาพแวดล้อม	
อุปกรณ์	- การกำหนดพื้นที่ที่ใช้ในการติดตั้งอุปกรณ์ที่มีความสำคัญให้เข้าถึงยาก - มีการจัดวางอุปกรณ์ที่มีความสำคัญไม่ให้เสี่ยงต่อภัยคุกคามด้านสิ่งแวดล้อมและอันตรายและโอกาสสำหรับการเข้าถึง ไม่ได้รับอนุญาต - ความมั่นคงปลอดภัยของการเดินสายสัญญาณและ สายสื่อสาร - อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล	- ตรวจเยี่ยมสถานที่

3.8 ความมั่นคงปลอดภัยสำหรับการสื่อสาร ข้อมูล เป็นการตรวจสอบการโอนถ่ายข้อมูลและการสื่อสาร รับ-ส่งข้อมูลผ่านระบบเครือข่าย เพื่อป้องกันการเปลี่ยนแปลงแก้ไขหรือรั่วไหลของข้อมูลหน่วยงาน ตามตารางที่ 8 ดังนี้

ตารางที่ 8 : แสดงวิธีการตรวจสอบความมั่นคงปลอดภัยสำหรับการสื่อสาร ข้อมูล

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย	- การบริหารจัดการและควบคุมโดยมีการกำหนดขั้นตอน/มาตรการในการบริหารจัดการและควบคุมระบบเครือข่าย - การกำหนดขั้นตอนการให้บริการเครือข่าย - ต้องมีการจัดแบ่งเครือข่ายตามกลุ่มที่กำหนด	- ตรวจสอบมาตรการเครือข่ายของหน่วยงาน - ตรวจสอบการกำหนดความมั่นคงปลอดภัยสำหรับบริการเครือข่ายของหน่วยงานและข้อตกลงการให้บริการเครือข่ายและการบริหารจัดการข้อตกลง - ตรวจสอบความเหมาะสมในแผนผังการแบ่งเครือข่ายกับการรักษาความมั่นคงปลอดภัยหรือไม่ และการกำหนดผู้ดูและระบบเครือข่าย การกำหนดสิทธิ

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
		และการให้สิทธิแก่ผู้ใช้งานระบบเครือข่ายเหมาะสม หรือไม่ - การแยกประเภทของผู้ใช้งานและกำหนดการเข้าถึงข้อมูลในระดับชั้นต่าง ๆ
การถ่ายโอนสารสนเทศ	- นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ - ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ - การส่งข้อความทางอิเล็กทรอนิกส์ - ข้อตกลงการรักษาความลับ	- สอบทานนโยบายและขั้นตอนปฏิบัติ - สอบทานข้อตกลง - สัมภาษณ์เจ้าหน้าที่ที่เกี่ยวข้อง

3.9 การจัดหา การพัฒนา และการบำรุงรักษาระบบ เป็นการตรวจสอบ เพื่อควบคุม กำกับ ดูแล การพัฒนาระบบสารสนเทศให้เป็นไปตามนโยบายและมาตรฐานความมั่นคงปลอดภัย ตามตารางที่ 9 ดังนี้

ตารางที่ 9 : แสดงวิธีการตรวจสอบการจัดหา การพัฒนา และการบำรุงรักษาระบบ

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
ความต้องการด้านความมั่นคงปลอดภัยของระบบ	- การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ	- สัมภาษณ์การวิเคราะห์ และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ - ตรวจสอบเอกสารประกอบการวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศในการพัฒนาและออกแบบระบบสารสนเทศ
ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน	นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัยโดยหน่วยงานต้องกำหนดเกณฑ์สำหรับการพัฒนาซอฟต์แวร์และระบบ	ตรวจสอบและสัมภาษณ์นโยบายและแนวทางปฏิบัติในการพัฒนาระบบสารสนเทศหรือซอฟต์แวร์ของหน่วยงาน

3.10 ความสัมพันธ์กับผู้ให้บริการภายนอก เป็นการตรวจสอบการตกลงในการดำเนินการจ้างผู้รับจ้างภายนอกหน่วยงานมาดำเนินการให้เป็นไปอย่างถูกต้อง สามารถควบคุมกำกับ ตรวจสอบและประเมินผลการจ้างได้ ตามตารางที่ 10 ดังนี้

ตารางที่ 10 : แสดงวิธีการตรวจสอบความสัมพันธ์กับผู้ให้บริการภายนอก

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการ	การกำหนดนโยบายเพื่อความปลอดภัยในการจ้างผู้รับจ้างจากภายนอก	สอบทานนโยบาย
การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก	การกำหนดเงื่อนไข/ข้อตกลงการให้บริการในการจ้างงาน	สอบทานข้อตกลงการจ้าง

3.11 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ เป็นการตรวจสอบกระบวนการแก้ไขปัญหาหรือเหตุการณ์ความไม่ปลอดภัยระบบสารสนเทศ เพื่อให้การปฏิบัติงานกระบวนการแก้ไขปัญหาหรือแก้ไขเหตุการณ์ความไม่ปลอดภัยระบบสารสนเทศของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ ประสิทธิผล ตามตารางที่ 11 ดังนี้

ตารางที่ 11 : แสดงวิธีการตรวจสอบการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	กำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติ	- สัมภาษณ์และทดสอบกระบวนการบริหารจัดการแก้ไขปัญหา/แก้ไขเหตุการณ์ที่ไม่มั่นคงปลอดภัย
การรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ	มีการรายงานผ่านทางช่องทางการบริหารจัดการที่เหมาะสมและรายงานอย่างรวดเร็วที่สุดเท่าที่จะทำได้	- สุ่มตรวจสอบช่องทางการแจ้งเตือนปัญหาที่เกิดขึ้นและจับระยะเวลาในการรายงานว่ามีความรวดเร็วเหมาะสมอย่างไร
การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	การจัดทำขั้นตอนการปฏิบัติในการแก้ไขปัญหาความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน	ตรวจสอบและสัมภาษณ์ขั้นตอนการปฏิบัติในการแก้ไขปัญหาความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานกำหนด
การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ	มีการแจ้งเวียนให้ทราบกันอย่างทั่วถึง	สอบทานหลักฐานการแจ้งเวียน

3.12 การบริหารความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ ตามตารางที่ 12 ดังนี้

ตารางที่ 12 : แสดงวิธีการตรวจสอบการบริหารความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ	การกำหนดรายการข้อมูลที่สำคัญที่ต้องสำรองข้อมูล	สัมภาษณ์และตรวจสอบกระบวนการกำหนดรายงานข้อมูลที่สำคัญที่ต้องสำรองข้อมูล
การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ	การทดสอบข้อมูลที่สำรองไว้	สัมภาษณ์และตรวจสอบเกี่ยวกับสถานที่และการจัดเก็บสื่อบันทึกข้อมูลที่สำรองและสำเนาขั้นตอนหรือวิธีการปฏิบัติต่าง ๆ
การเตรียมการอุปกรณ์ประมวลผลสำรอง	การจัดลำดับความสำคัญของระบบงาน/กระบวนงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้คืนของแต่ละระบบงานด้วยการประเมินความเสี่ยง	ตรวจสอบและสัมภาษณ์การประเมินความเสี่ยงและการ ประเมินผลกระทบของกระบวนงานหลัก โดยการจัดลำดับความสำคัญของระบบงาน/กระบวนงาน ความสัมพันธ์ของแต่ละระบบงาน และระยะเวลาในการกู้คืนของแต่ละระบบงาน

3.13 การปฏิบัติงานที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ ตามตารางที่ 13 ดังนี้

ตารางที่ 13 : แสดงวิธีการตรวจสอบการปฏิบัติงานที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง	การปฏิบัติตามข้อกำหนดทางกฎหมายเทคโนโลยีสารสนเทศ	สัมภาษณ์และตรวจสอบการวิเคราะห์กระบวนการปฏิบัติงานที่เสี่ยงต่อการละเมิดกฎหมาย
สิทธิในทรัพย์สินทางปัญญา	ขั้นตอนการปฏิบัติงานที่เหมาะสมไม่ละเมิดกฎหมาย ระเบียบข้อบังคับ รวมทั้งสัญญาจ้าง ที่ว่าด้วยเรื่องสิทธิในทรัพย์สินทางปัญญาและการใช้ผลิตภัณฑ์ซอฟต์แวร์ที่มีกรรมสิทธิ์	ตรวจสอบและสัมภาษณ์การกำหนดขั้นตอนการปฏิบัติงานและสัญญาจ้างว่าไม่มีจุดเสี่ยงต่อการละเมิดกฎหมาย ระเบียบข้อบังคับ
การป้องกันข้อมูล	การกำหนดแนวทางการจัดทำสัญญาจ้างกับเอกชนของหน่วยงาน	ตรวจสอบแนวทางการจัดทำสัญญาจ้างกับเอกชนของหน่วยงาน

หัวข้อย่อย	ขั้นตอน	เครื่องมือที่ใช้
ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล	การกำหนดให้ข้อมูลส่วนตัวต้องมีการเข้ารหัสหรือขออนุญาตจากเจ้าของเรื่องให้เป็นไปตามข้อบังคับ	ตรวจสอบและสัมภาษณ์ข้อมูลส่วนตัวว่ามีการเข้ารหัส หรือไม่ โดยให้ผู้ปฏิบัติงานเปิดฐานข้อมูลที่มีข้อมูลส่วนบุคคลจัดเก็บไว้ว่ามีการเข้ารหัสไว้ หรือไม่
ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย	การกำหนดขั้นตอน/แนวทางปฏิบัติในการทบทวนระบบให้สอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร	ตรวจสอบขั้นตอนการปฏิบัติตามนโยบาย และมาตรฐานความมั่นคงปลอดภัยที่หน่วยงานต้องกำหนดขึ้นใช้ในการปฏิบัติงานว่ามีครอบคลุมตามที่นโยบาย/มาตรฐานความมั่นคงปลอดภัย หรือไม่ และการกำหนดดังกล่าวเหมาะสมและครอบคลุมความเสี่ยง หรือไม่

บทที่ 4

กรณีศึกษา การตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

สำหรับกรณีศึกษาการตรวจสอบเทคโนโลยีสารสนเทศ ซึ่งเป็นหนึ่งในประเภทของงานตรวจสอบภายในที่กรมบัญชีกลางได้กำหนดให้มีการตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศโดยการประเมินความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ (หนังสือกรมบัญชีกลาง ที่ กค 0409.2/ ว 614 ลว. 23 ธ.ค. 2563 การกำหนดประเภทของงานตรวจสอบภายใน) ดังนั้น เพื่อให้ผู้ตรวจสอบภายในเกิดความเข้าใจในกระบวนการตรวจสอบการควบคุมด้านเทคโนโลยีสารสนเทศ จึงนำการดำเนินการตรวจสอบเทคโนโลยีสารสนเทศของกรม A เป็นกรณีศึกษา โดยมีรายละเอียด ดังนี้

1. การกำหนดประเด็นการตรวจสอบ

การกำหนดประเด็นการตรวจสอบเป็นโดยใช้ข้อมูลจากการสำรวจข้อมูลเบื้องต้น ศึกษาทำความเข้าใจระบบงานสารสนเทศ (การควบคุมและความเสี่ยง) ประเมินผลความเสี่ยง โดยมีเกณฑ์การประเมินความเสี่ยงเบื้องต้น ดังนี้

เกณฑ์สำหรับใช้ในการประเมินความเสี่ยงของกระบวนงานกิจกรรม/โครงการ พิจารณาจาก 2 ปัจจัย คือ ด้านโอกาส และด้านผลกระทบ และการให้คะแนนทั้ง 2 ปัจจัย ดังนี้

- โอกาสที่จะเกิด (Likelihood) พิจารณาความเป็นไปได้ที่จะเกิดเหตุการณ์ความเสี่ยงในช่วงเวลาหนึ่งในรูปแบบความถี่ หรือความน่าจะเป็นที่จะเกิดเหตุการณ์นั้น ๆ

- ผลกระทบ (Impact) การวัดระดับของความเสียหายที่จะเกิดขึ้นจากความเสี่ยงนั้น โดยสามารถแบ่งเป็นผลกระทบทางด้านการเงินและผลกระทบที่ไม่ใช่การเงิน

1. เกณฑ์โอกาสเกิดความเสี่ยง (Likelihood)

โอกาสเกิดการทุจริต (Likelihood)	
3	เหตุการณ์ที่อาจเกิดได้สูง
2	เหตุการณ์ที่อาจเกิดขึ้นได้ไม่สูงมาก
1	เหตุการณ์ไม่น่ามีโอกาสเกิดขึ้น

2. เกณฑ์ผลกระทบ (Impact)

ระดับของผลกระทบ (Impact)	
3	มีผลกระทบต่อหน่วยงาน AA /กรม A ในระดับสูง
2	มีผลกระทบต่อหน่วยงาน AA /กรม A ในระดับปานกลาง
1	มีผลกระทบต่อกระบวนการภายใน/การเรียนรู้/องค์ความรู้

3. เกณฑ์การวัดระดับของความเสี่ยง (Risk Score)

โอกาสเกิด (L)	ผลกระทบ (I)		
	1	2	3
3	ต่ำ	ปานกลาง	สูง
2	ต่ำ	ต่ำ	ปานกลาง
1	ต่ำ	ต่ำ	ต่ำ

การประเมินความเสี่ยงเบื้องต้นที่เกี่ยวข้องกับกิจกรรมที่ตรวจพบ

กิจกรรม : การตรวจสอบเทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

ลำดับที่	ขั้นตอน/กระบวนงาน	ปัจจัยเสี่ยง	การประเมินความเสี่ยง		ระดับความเสี่ยง	
			โอกาส	ผลกระทบ		
1.	การประเมินความเสี่ยงและการควบคุมภายในด้านเทคโนโลยีสารสนเทศของกรม A	ประเมินความเสี่ยงให้ครอบคลุมทุกด้าน	3	2	6	ปานกลาง
2.	การแต่งตั้งคณะกรรมการด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรม A	-	-	-	-	-
3.	การแต่งตั้งคณะกรรมการการบริหารความเสี่ยงและการควบคุมภายในด้านสารสนเทศของกรม A	มิได้แต่งตั้งเฉพาะภารกิจดังกล่าว	2	2	4	ต่ำ
4.	การขับเคลื่อนของคณะกรรมการด้านเทคโนโลยีสารสนเทศและการสื่อสาร และคณะกรรมการบริหารความเสี่ยงและการควบคุมภายใน	มิได้ขับเคลื่อนอย่างต่อเนื่อง	3	2	6	ปานกลาง
5.	นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกรม A ตามประกาศ	- สาระไม่ครอบคลุมตามประกาศคณะกรรมการธุรกรรมทาง	3	3	9	สูง

ลำดับที่	ขั้นตอน/กระบวนงาน	ปัจจัยเสี่ยง	การประเมินความเสี่ยง		ระดับความเสี่ยง	
			โอกาส	ผลกระทบ		
	คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 และกฎระเบียบที่เกี่ยวข้องรวมถึงทบทวนเป็นปัจจุบัน	อิเล็กทรอนิกส์ พ.ศ. 2553 -ไม่ได้ผ่านความเห็นชอบของผู้บริหารระดับสูง				
6.	การเผยแพร่นโยบายและแนวปฏิบัติตามกฎระเบียบที่เกี่ยวข้องของกรม A	เผยแพร่ผ่านช่องทางที่ครอบคลุมไม่ทั่วถึง	2	2	4	ต่ำ
7.	การปฏิบัติ การควบคุม การติดตาม และการประเมินผลการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและกฎระเบียบที่เกี่ยวข้องของกรม A	ควบคุมติดตามการปฏิบัติตามนโยบายและแนวปฏิบัติไม่ต่อเนื่องและรัดกุม	3	3	9	สูง
8.	การจัดทำแผนรองรับสถานการณ์แผนฉุกเฉินจากภัยพิบัติอันมีผลกระทบต่อระบบสารสนเทศและแผนรองรับภัยพิบัติและการบริหารจัดการรักษาความมั่นคงปลอดภัยไซเบอร์	แผนฯ มิได้ผ่านความเห็นชอบของผู้บริหารระดับสูงของกรม A	3	2	6	ปานกลาง
9.	การเผยแพร่แผนรองรับสถานการณ์ฉุกเฉินและแผนรองรับภัยพิบัติ	เผยแพร่ไม่ทั่วถึง	2	2	4	ต่ำ
10.	การปฏิบัติการควบคุมติดตามและประเมินผล แผนรองรับสถานการณ์ฉุกเฉินฯ และแผนรองรับภัยพิบัติ	ควบคุมติดตามการปฏิบัติตามแผนไม่ต่อเนื่อง	2	3	6	ปานกลาง

ลำดับที่	ขั้นตอน/กระบวนงาน	ปัจจัยเสี่ยง	การประเมินความเสี่ยง		ระดับความเสี่ยง	
			โอกาส	ผลกระทบ		
11.	การจัดทำแผนพร้อมความเสี่ยงด้านเทคโนโลยีสารสนเทศและมีการทบทวนเป็นประจำทุกปี	- มิได้มาจากบุคลากรทุกระดับขององค์กร - ไม่ครอบคลุมทุกด้าน	2	3	6	ปานกลาง
12.	การเผยแพร่แผนบริหารความเสี่ยงให้เจ้าหน้าที่ของกรมทราบอย่างทั่วถึง รวมถึงการติดตามและประเมินผลการปฏิบัติตามแผนบริหารความเสี่ยง	- เผยแพร่ไม่ทั่วถึง - การติดตามและประเมินผลอาจไม่เพียงพอ				
13.	สภาพแวดล้องห้องเครื่องคอมพิวเตอร์แม่ข่ายการเข้าถึงและการใช้งาน (ระบบเครือข่าย ระบบปฏิบัติการ Application)	ผู้เข้าถึงและผู้ใช้งานในระบบมิใช่ผู้รับผิดชอบหรือตรงตามภารกิจกรม	3	3	9	สูง
14.	การตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระจากภายนอก	มิได้จัดให้มีการตรวจสอบและประเมินจากผู้ตรวจสอบภายในหรือภายนอกเป็นประจำทุกปี	3	2	6	ปานกลาง
15.	การควบคุม ดูแลเครื่องมืออุปกรณ์ ด้านสารสนเทศเป็นไปตามระเบียบ และพร้อมจะใช้งาน	ควบคุมเครื่องมืออุปกรณ์ในฐานข้อมูลทรัพย์สินของหน่วยงาน AA ไม่ครบทุกรายการ และอยู่ในสภาพไม่พร้อมใช้งาน	2	3	6	ปานกลาง

ลงชื่อ.....ก.....ผู้ประเมินความเสี่ยง
(.....นางสาว..ก.....)
ตำแหน่ง....หัวหน้าทีมตรวจสอบภายใน...
วันที่.....xx...เดือน..xx..พ.ศ..25xx.....

ลงชื่อ.....B.....ผู้สอบทาน
(.....นางสาว..B.....)
ตำแหน่ง...หัวหน้าหน่วยงานตรวจสอบภายใน...
วันที่.....xx...เดือน..xx..พ.ศ..25xx.....

จากการประเมินความเสี่ยงเบื้องต้นของการรักษาความปลอดภัยสารสนเทศของกรม A ได้นำขั้นตอนงานที่มีความเสี่ยง**ระดับสูง**มากำหนดประเด็นการตรวจสอบ ได้แก่

1. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกรม A ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 และกฎระเบียบที่เกี่ยวข้อง รวมถึงทบทวนเป็นปัจจุบัน

2. การปฏิบัติ การควบคุม การติดตาม และการประเมินผลการปฏิบัติตามนโยบาย และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

3. สภาพแวดล้องห้องเครื่องคอมพิวเตอร์แม่ข่าย การเข้าถึงและการใช้งาน (ระบบเครือข่าย ระบบปฏิบัติการ Application) กฎระเบียบที่เกี่ยวข้องของกรม A

ความเสี่ยงเบื้องต้นดังกล่าว ผู้ตรวจสอบภายในได้กำหนด **ประเด็นการตรวจสอบ** คือ การควบคุมและการปฏิบัติตามการควบคุมของการรักษาความปลอดภัยด้านสารสนเทศ ไม่เพียงพอ ไม่เหมาะสม

2. แผนการปฏิบัติงาน (Engagement Plan)

ผู้ตรวจสอบภายในจะมีการจัดทำแผนการปฏิบัติงาน (Engagement Plan) ตรวจสอบในกิจกรรมที่/โครงการได้รับมอบหมายจากหัวหน้าหน่วยงานตรวจสอบภายใน เพื่อเป็นกรอบในการปฏิบัติงานตรวจสอบของทีมงานตรวจสอบ ซึ่งแผนการปฏิบัติต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานตรวจสอบภายในก่อนนำไปใช้ในการปฏิบัติงาน โดยรายละเอียดการจัดทำแผน มีดังนี้

แผนการปฏิบัติงาน (Engagement Plan)
ตามแผนการตรวจสอบประจำปีงบประมาณ พ.ศ. 25xx

.....

1. หน่วยรับตรวจ : หน่วยงาน AA

2. กิจกรรมที่ตรวจสอบ : เทคโนโลยีสารสนเทศ ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

3. ประเด็นการตรวจสอบ : การควบคุม และการปฏิบัติตามการควบคุมของการรักษาความปลอดภัยด้านสารสนเทศ ไม่เพียงพอ ไม่เหมาะสม

4. วัตถุประสงค์ : 1. เพื่อให้มั่นใจว่าหน่วยงาน AA มีการกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A เป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และ กฎหมายอื่นที่เกี่ยวข้อง

2. เพื่อให้มั่นใจว่าหน่วยงาน AA มีการควบคุมภายในด้านเทคโนโลยีสารสนเทศและการจัดการความเสี่ยงด้านการดำเนินงานระบบสารสนเทศที่เพียงพอเหมาะสม

5. ขอบเขตการตรวจสอบ : 1. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A
2. ติดตามผลการดำเนินการตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของกรม A

6. ระยะเวลาที่เข้าตรวจสอบ : ธันวาคม 25XX – มิถุนายน 25xx

7. การจัดสรรทรัพยากร

7.1 จำนวนบุคลากร : 3 คน ประกอบด้วย
1. นางสาว ก
2. นางสาว ข
3. นางสาว ค

7.2 งบประมาณ : .....-..... บาท

แนวทางการปฏิบัติงาน :

แนวทางการปฏิบัติงาน	ชื่อผู้ตรวจสอบ	รหัสกระดาษทำการ
1. ศึกษาแผนแม่บท พระราชบัญญัติ กฎหมาย ประกาศ เกี่ยวกับการควบคุมและการรักษาความปลอดภัยด้านสารสนเทศ	นางสาว ก นางสาว ข นางสาว ค	ตสน.สท. 1/2566 ตสน.สท. 2/2566 ตสน.สท. 3/2566 ตสน.สท. 4/2566
2. สอบทานรายงานประเมินความเสี่ยงและการจัดการความเสี่ยงด้านการควบคุมและรักษาความปลอดภัยด้านสารสนเทศ		
3. ประชุมเปิดตรวจกับหน่วยรับตรวจ AA พร้อมแจ้งรายละเอียดการตรวจสอบและซักถามข้อมูลกับเจ้าหน้าที่หน่วยรับตรวจ AA		
4. สอบทานการจัดทำนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ 4.1 การจัดทำนโยบายด้านสารสนเทศ และการสื่อสารของกรม A ครอบคลุมข้อกำหนดตามกฎหมายและประกาศคณะกรรมการที่เกี่ยวข้อง 4.2 การเผยแพร่นโยบายและข้อปฏิบัติให้ผู้ที่เกี่ยวข้องทราบ		

แนวทางการปฏิบัติงาน	ชื่อผู้ตรวจสอบ	รหัสกระดาษทำการ
4.3 การกำหนดชัดเจนเกี่ยวกับผู้รับผิดชอบตามนโยบายและข้อปฏิบัติ 4.4 ทบทวนนโยบายและข้อปฏิบัติเป็นปัจจุบันอยู่เสมอ 4.5. การกำหนดนโยบายครอบคลุมบทบาทหน้าที่ของบุคลากร 3 ระดับ ได้แก่ ผู้บริหาร ผู้ปฏิบัติงานด้านเทคโนโลยี และผู้ปฏิบัติงานทั่วไปในองค์กร 4.6 การแต่งตั้งคณะกรรมการรักษาความปลอดภัยด้านสารสนเทศของกรม A 4.6.1 บทบาทหน้าที่คณะกรรมการฯครอบคลุมการวางแผนและการกำหนดแนวปฏิบัติ/มาตรการ การสื่อสารประชาสัมพันธ์ การควบคุม-กำกับ การติดตาม การประเมินผล การนำไปสู่การปฏิบัติ 4.6.2 กระบวนการขับเคลื่อนระบบการรักษาความปลอดภัยสารสนเทศโดยคณะกรรมการ 4.6.3 มีการทบทวนหรือแก้ไขเพิ่มเติมคณะกรรมการอย่างน้อย 1 ครั้งต่อไป 4.7 บุคลากร 4.7.1 สอบทานแผนผังโครงสร้างการปฏิบัติงานในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศระบบสารสนเทศ บทบาทหน้าที่ของหัวหน้า IT และ ผู้ปฏิบัติงานด้าน IT 4.7.2 การคัดกรองบุคลากรปฏิบัติงานเกี่ยวกับการรักษา ความปลอดภัยของระบบสารสนเทศและการพัฒนาบุคลากรให้มีความพร้อมที่จะสนับสนุนนโยบายความปลอดภัย ขององค์กร		

แนวทางการปฏิบัติงาน	ชื่อผู้ตรวจสอบ	รหัสกระดาษทำการ
4.7.3 การจ้างผู้รับจ้างเหมา/บุคคลภายนอกครอบคลุมเพียงพอและสอดคล้องกับการปฏิบัติตามนโยบายการรักษาความปลอดภัยของระบบสารสนเทศ 4.7.4 ตรวจสอบมาตรการ/แนวการปฏิบัติในการถอดถอนสิทธิในการเข้าถึงข้อมูลขององค์กรและการคืนทรัพย์สินที่กรมถือครองเมื่อสิ้นสุดการจ้าง/พ้นจากตำแหน่ง 4.8 การติดตามและประเมินผลการนำนโยบายสู่การปฏิบัติและมีการทบทวนแนวทางปฏิบัติ/นโยบาย		
5. สอบทานการควบคุมตามพระราชบัญญัติและประกาศคณะกรรมการ 5.1 การเข้าถึงและการควบคุมการใช้งาน (1) การกำหนดการเข้าถึงระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ และโปรแกรมประยุกต์ (Application) และสารสนเทศ (2) การกำหนดการใช้งานตามภารกิจ (3) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (4) การกำหนดหน้าที่ความรับผิดชอบ 5.2 การจัดให้มีระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน 5.3 การจัดให้มีการบริหารความเสี่ยงด้านสารสนเทศ 5.4 การพัฒนาความรู้ด้านสารสนเทศแก่บุคลากรของกรม A		
6. การสอบทานการบริหารทรัพย์สินด้านเทคโนโลยีสารสนเทศ		ตสน.สท. 1/2566 ตสน.สท. 2/2566 ตสน.สท. 5/2566

แนวทางการปฏิบัติงาน	ชื่อผู้ตรวจสอบ	รหัสกระดาษทำการ
6.1 การจัดทำบัญชีทรัพย์สิน ทะเบียนบัญชีทรัพย์สินเป็นปัจจุบัน มีการจัดหมวดหมู่ (อุปกรณ์คอมพิวเตอร์ เครือข่าย และ software) ประกอบด้วย ชื่ออุปกรณ์ หมายเลข ปีที่ได้รับ สถานที่ใช้งาน ผู้รับผิดชอบ 6.2 ผู้ถือครองทรัพย์สิน มีการระบุชื่อผู้ใช้อุปกรณ์คอมพิวเตอร์ชัดเจนและปรับปรุงเป็นปัจจุบันทุกครั้งที่มีการเปลี่ยนแปลง 6.3 การใช้ทรัพย์สินอย่างเหมาะสม มีหลักเกณฑ์จัดสรรอุปกรณ์คอมพิวเตอร์ตรงตามภารกิจการใช้งาน มีการจัดทำคู่มือการใช้งานมีการประกาศใช้ให้ผู้ใช้งานทราบอย่างทั่วถึง และจัดให้มีการตรวจสอบบำรุงรักษาอุปกรณ์คอมพิวเตอร์ให้มีความพร้อมใช้งาน 6.4 ตรวจนับความมีอยู่จริงของทรัพย์สินถูกต้องตรงกับทะเบียนทรัพย์สิน 6.5 การกำหนดชั้นความลับของสารสนเทศและการเข้าถึงข้อมูลตามระดับชั้นความลับสารสนเทศ (ไม่ลับ ลับ ลับมาก ลับที่สุด) 6.6 กำหนดนโยบาย/มาตรการ/แนวปฏิบัติป้องกันอุปกรณ์สารสนเทศที่ใช้งานจากภายนอกของกรม A และเครื่องคอมพิวเตอร์แบบพกพา		
7. สอบทานข้อตกลงการให้บริการของผู้ให้บริการภายนอก โดยเงื่อนไขการจ้างครอบคลุมการระบุสิทธิหน้าที่ของคู่สัญญา การแบ่งชำระงวดเงิน การควบคุมกำกับ ติดตาม และประเมินผลโดยผู้รับจ้าง ความเป็นเจ้าของลิขสิทธิ์		ตสน.สท. 2/2566
8. การจัดการเหตุการณ์ความไม่มั่นคงปลอดภัยสารสนเทศ		

แนวทางการปฏิบัติงาน	ชื่อผู้ตรวจสอบ	รหัสกระดาษทำการ
8.1 สัมภาษณ์กระบวนการบริหารจัดการแก้ไขปัญหา/เหตุการณ์ความไม่มั่นคงปลอดภัย 8.2 สอบทานเอกสารหลักฐานการกำหนดผู้รับผิดชอบในการแก้ไขปัญหา ขั้นตอนงานการสื่อสารประชาสัมพันธ์ 8.3 สอบทานช่องทางการรายงานสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ 8.4 มีการแจ้งเวียนเหตุการณ์ความมั่นคงสารสนเทศที่จัดขึ้นให้เจ้าหน้าที่ภายในหน่วยงาน AA ทราบ 8.5 สอบทานการจัดเก็บหลักฐานสารสนเทศปลอดภัย ข้อกำหนดควบคุมนำมาใช้เพื่อไม่ให้เกิดการสูญหาย 8.6 สอบทานแผนการสำรองข้อมูล และรายงานผลการสำรองข้อมูลตามแผน 8.7 สอบทานนโยบายให้มีการทดสอบข้อมูลสำรอง การนำข้อมูลที่กู้คืนมาใช้ การกำหนดสถานที่ในการเก็บรักษาข้อมูลสำรอง		ตสน.สท. 1/2566 ตสน.สท. 2/2566
9. สอบทานมาตรการจัดการและควบคุมเครือข่ายเป็นลายลักษณ์อักษร การแบ่งแยกเครือข่ายในการดูแลรักษาความมั่นคงปลอดภัย	นางสาว ค	ตสน.สท. 2/2566 ตสน.สท. 5/2566
10. สอบทานนโยบายและขั้นตอนในการถ่ายโอนสารสนเทศ และการทำลายข้อมูลหรือสื่อที่บันทึกของหน่วยงาน AA	นางสาว ค	ตสน.สท. 2/2566
11. สอบทานการปฏิบัติงานและการรายงานผลเป็นตามคู่มือ/ขั้นตอนการปฏิบัติงาน	นางสาว ค	ตสน.สท. 2/2566 ตสน.สท. 5/2566
12. การทดสอบ/การสังเกตการณ์พื้นที่ปฏิบัติงานด้านสารสนเทศของกรม A บริเวณพื้นที่ที่กำหนดการรักษาความปลอดภัย การควบคุมการเข้า-ออก	นางสาว ก นางสาว ข นางสาว ค	ตสน.สท. 3/2566 ตสน.สท. 4/2566

แนวทางการปฏิบัติงาน	ชื่อผู้ตรวจสอบ	รหัสกระดาษทำการ
การเข้าระบบตามลำดับชั้นความลับ การเก็บรักษากุญแจ		
13. บันทึกข้อมูลที่ได้จากการตรวจสอบลงในกระดาษทำการของแต่ละหัวข้อเรื่อง	นางสาว ค	ตสน.สท. 2/2566 ตสน.สท. 3/2566
14. วิเคราะห์และประมวลผลข้อที่จัดเก็บเพื่อทราบถึงแนวโน้ม ปัญหา อุปสรรค ที่มีผลต่อการบรรลุวัตถุประสงค์ของการปฏิบัติงานการปฏิบัติงานของหน่วยรับตรวจ AA	นางสาว ก นางสาว ข นางสาว ค	ตสน.สท. 6/2566
15. สรุปผลการตรวจสอบ ปัญหา สาเหตุ ผลกระทบและแนวทางการปรับปรุง แก้ไข ปัญหาต่าง ๆ	นางสาว ก นางสาว ข นางสาว ค	
16. สรุปปิดตรวจกับหน่วยรับตรวจ AA ทำความเข้าใจในประเด็นต่าง ๆ แลกเปลี่ยนความคิดเห็นหาข้อยุติในประเด็นความเห็นที่ไม่ตรงกัน และขอบคุณผู้ที่เกี่ยวข้องในการให้ความร่วมมือ	นางสาว ก	
17. รวบรวมข้อเท็จจริงจากหลักฐานและกระดาษทำการทั้งหมด เพื่อสรุปข้อตรวจพบและจัดทำ (ร่าง) รายงานผลการตรวจสอบ	นางสาว ก นางสาว ข นางสาว ค	
18. จัดทำ (ร่าง) รายงานผลการตรวจสอบเสนอหัวหน้าหน่วยงานตรวจสอบภายในพิจารณา	นางสาว ก นางสาว ข	
19. จัดทำรายงานผลการตรวจสอบเสนอผู้อำนวยการกลุ่มตรวจสอบภายใน เพื่อเสนอหัวหน้าส่วนราชการของกรม A		
20. จัดเก็บข้อมูลที่มาจากการปฏิบัติงานตรวจสอบในรูปแบบอิเล็กทรอนิกส์และแฟ้มถาวร	นางสาว ค	
สรุปผลการตรวจสอบ		

3. การปฏิบัติงานตรวจสอบ

ผู้ตรวจสอบภายในได้รายละเอียดการตรวจสอบ ณ หน่วยรับตรวจ AA ประกอบด้วย ประเด็นการตรวจสอบ วัตถุประสงค์การตรวจสอบ ขอบเขตการตรวจสอบ ระยะเวลาการตรวจสอบ และปฏิบัติงานตามแผนการปฏิบัติงาน (Engagement Plan) ดังนี้

3.1 ประเด็นการตรวจสอบ

การควบคุม และการปฏิบัติตามการควบคุมของการรักษาความปลอดภัยด้านสารสนเทศไม่เพียงพอ ไม่เหมาะสม

3.2 วัตถุประสงค์การตรวจสอบ

3.2.1 เพื่อให้มั่นใจว่าหน่วยงาน AA มีการกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ ของกรม A เป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และกฎหมายอื่นที่เกี่ยวข้อง

3.2.2 เพื่อให้มั่นใจว่าหน่วยงาน AA มีการควบคุมภายในด้านเทคโนโลยีสารสนเทศและการจัดการความเสี่ยงด้านการดำเนินงานระบบสารสนเทศที่เพียงพอ เหมาะสม

3.3 ขอบเขตการตรวจสอบ

3.3.1 การควบคุม และการปฏิบัติตามมาตรการควบคุมภายในของการรักษาความปลอดภัยด้านสารสนเทศภายใต้กรอบระเบียบ ดังนี้

(1) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ฉบับที่ 2) พ.ศ. 2560

(2) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

(3) พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

3.3.2 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

3.4 ระยะเวลาการตรวจสอบ

ระหว่าง เดือน ธ.ค. – เม.ย. 25XX

3.5 ปฏิบัติงานตามแผนการปฏิบัติงาน (Engagement Plan)

สอบทานและรวบรวมข้อมูล เอกสารหลักฐานจากการปฏิบัติงานของหน่วยรับตรวจ AA และบันทึกผลจากการสอบทานในกระดาษทำการของผู้ตรวจสอบภายใน เพื่อวิเคราะห์และประมวลผล สรุปเป็นผลการตรวจสอบ ดังนี้

3.5.1 การประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ เพื่อทราบว่าหน่วยงาน AA มีการควบคุม กำกับดูแล และบริหารความเสี่ยง ที่เพียงพอ และเหมาะสม หรือไม่ โดยใช้เครื่องมือแบบประเมินการควบคุมภายใน (รหัสกระดาษทำการ : ตสน.สท. 1/2566)

ตสน.สท. 1/2566

แบบประเมินการควบคุมภายในด้านเทคโนโลยีสารสนเทศ
หน่วยรับตรวจ กรม A

วัตถุประสงค์ :

แบบประเมินนี้จัดทำขึ้นเพื่อเป็นแนวทางในการประเมินการควบคุมด้านเทคโนโลยีสารสนเทศ เพื่อให้ทราบว่าหน่วยงาน AA มีการกำกับดูแล บริหารความเสี่ยง และการควบคุมภายในด้านสารสนเทศที่เพียงพอ เหมาะสม เป็นไปตามระเบียบ กฎหมายกำหนด

การกรอกข้อมูลในแบบประเมินการควบคุมภายใน

1. กรณี มีการปฏิบัติตามรายการสอบทาน แสดงถึงการควบคุมภายในที่ดี ให้ทำเครื่องหมาย “√” ในช่อง”มี/ใช่”

2. กรณี ไม่มีการปฏิบัติตามรายการสอบทาน แสดงถึงจุดอ่อนของการควบคุมภายใน ให้ทำเครื่องหมาย “×” ในช่อง “ไม่มี/ไม่ใช่”

3. กรณี คำตอบว่า “มี/ใช่” ให้แนบเอกสารหลักฐานประกอบ (File PDF) หรือกรณีเผยแพร่ในระบบสารบรรณอิเล็กทรอนิกส์ของกรม ให้ระบุ Link ที่อยู่ของไฟล์เอกสาร

4. กรณี คำตอบว่า “ไม่มี/ไม่ใช่” ให้อธิบายเพิ่มเติมถึงสาเหตุที่มิได้ปฏิบัติตามรายการสอบทาน หรือระบุการควบคุมอื่นที่มีอยู่ทดแทนได้

5. ผู้ให้ข้อมูล คือ ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน AA ในการให้ข้อมูล

ลำดับที่	รายการสอบทาน	ผลการประเมิน		*เอกสารหลักฐานประกอบ
		มี/ใช่	ไม่มี/ไม่ใช่	
1	**การกำหนดและการปฏิบัติตามนโยบาย/แผน** 1.1 นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกรม A (1) นโยบายและแนวปฏิบัติได้รับความเห็นชอบให้ประกาศใช้จากผู้มีอำนาจ หรือไม่ ซึ่งรวมถึงการปรับปรุงในปีงบประมาณ พ.ศ. 2556 – 2560	✓		(1)หนังสือลงนามให้ความเห็นชอบ

ลำดับที่	รายการสอบทาน	ผลการประเมิน		*เอกสารหลักฐานประกอบ
		มี/ใช่	ไม่มี/ไม่ใช่	
	(2) หน่วยงาน AA มีการทบทวนปรับปรุงหลังจากปีงบประมาณ พ.ศ. 2560 และได้รับความเห็นชอบให้ประกาศใช้จากผู้มีอำนาจ หรือไม่		✓	(2)หนังสือลงนามให้ความเห็นชอบ
	(3) การเผยแพร่นโยบายและแนวปฏิบัติฯ บนเว็บไซต์ของหน่วยงาน AA ได้รับอนุมัติจากผู้มีอำนาจหรือไม่	✓		(3) หนังสืออนุมัติการเผยแพร่
	(4) นอกจากเผยแพร่ผ่านช่องทางเว็บไซต์ของหน่วยงาน AA แล้ว มีเผยแพร่ผ่านช่องทางอื่น หรือไม่		✓	(4) หนังสืออนุมัติการเผยแพร่
	(5) หน่วยงาน AA ได้ดำเนินการตรวจสอบและประเมินนโยบายนี้ตามระยะเวลา 1 ครั้งต่อปี หรือไม่		✓	(5) รายงานสรุปผลการตรวจสอบและประเมินผ่านการเสนอผู้มีอำนาจ (ปีงบประมาณล่าสุด)
	1.2 แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร			
	(1) แผนได้รับความเห็นชอบให้ประกาศใช้จากผู้มีอำนาจ หรือไม่	✓		(1)หนังสือลงนามให้ความเห็นชอบ
	(2) การเผยแพร่แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติบนเว็บไซต์ หน่วยงาน AA ได้รับอนุมัติจากผู้มีอำนาจ หรือไม่	✓		(2) หนังสืออนุมัติการเผยแพร่
	(3) นอกจากเผยแพร่ผ่านช่องทางเว็บไซต์ของหน่วยงาน AA แล้ว มีเผยแพร่ผ่านช่องทางอื่น หรือไม่		✓	(3) หลักฐานการเผยแพร่ช่องทางอื่น
	(4) หน่วยงาน AA ได้กำหนดเป็นนโยบายหรือแนวปฏิบัติให้มีการทบทวนและปรับปรุงแผนรองรับฯ เป็นประจำทุกปีหรือไม่	✓		(4) นโยบายหรือแนวปฏิบัติ
	(5) หน่วยงาน AA มีการทดสอบระบบตามแผนการทดสอบ ดังนี้			(5) รายงานผลการทดสอบระบบ
	(5.1) การทำงานของ Core Switch L-3	✓		
	(5.2) การกู้คืนข้อมูล	✓		
	(5.3) ระบบรักษาความปลอดภัยห้องควบคุมระบบเครือข่าย	✓		

ลำดับที่	รายการสอบทาน	ผลการประเมิน		*เอกสารหลักฐานประกอบ
		มี/ใช่	ไม่มี/ไม่ใช่	
	(6) หน่วยงาน AA มีการติดตามและรายงานผลให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน		✓	(6) รายงานผลการติดตามของเดือนปัจจุบันล่าสุด
	(7) บัญชีอุปกรณ์เครือข่าย/UPS ให้บริการ/เครื่องแม่ข่ายสำหรับให้บริการ ตามที่แนบท้ายในแผนข้อมูลเปลี่ยนแปลง หรือไม่	✓		(7) บัญชีทรัพย์สิน ณ ปัจจุบัน (หากเปลี่ยนแปลง)
	1.3 แผนรองรับภัยพิบัติและการบริหารจัดการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรม A			
	(1) ได้รับความเห็นชอบให้ประกาศใช้จากผู้มีอำนาจ หรือไม่	✓		(1) หนังสือลงนามเห็นชอบ
	(2) หน่วยงาน AA มีการทบทวนปรับปรุงหลังจากปีงบประมาณ พ.ศ. 2563 และได้รับความเห็นชอบให้ประกาศใช้จากผู้มีอำนาจ หรือไม่	✓		(2) รายงานผลการปรับปรุงที่ได้รับความเห็นชอบจากผู้มีอำนาจ
	(3) การเผยแพร่แผนรองรับภัยพิบัติฯ บนเว็บไซต์ของหน่วยงาน AA ได้รับอนุมัติจากผู้มีอำนาจ หรือไม่	✓		(3) หนังสืออนุมัติจากผู้มีอำนาจ
	(4) นอกจากเผยแพร่ผ่านช่องทางเว็บไซต์ของหน่วยงาน AA แล้ว มีเผยแพร่ผ่านช่องทางอื่นอีก หรือไม่		✓	(4) หลักฐานการเผยแพร่ช่องทางอื่น
	(5) หน่วยงาน AA ได้ทดสอบการปฏิบัติตามแผนอย่างน้อยปีละ 1 ครั้ง หรือไม่	✓		(5) รายงานผลการตรวจสอบและประเมินของปีงบประมาณล่าสุด
	1.4 การบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของกรม A			
	(1) แผนฯ ปีงบประมาณ พ.ศ. 2564 ได้รับความเห็นชอบให้ประกาศใช้จากผู้มีอำนาจ หรือไม่	✓		(1) หนังสือลงนามเห็นชอบ
	(2) หน่วยงาน AA ได้จัดให้มีการบริหารความเสี่ยงในปีงบประมาณ พ.ศ. 2565 และได้รับความเห็นชอบให้ประกาศใช้จากผู้มีอำนาจ หรือไม่	✓		(2) รายงานผลการปรับปรุงที่ได้รับความเห็นชอบจากผู้มีอำนาจ
	(3) การเผยแพร่ข้อมูลการบริหารความเสี่ยงบนเว็บไซต์ของหน่วยงาน AA ได้รับอนุมัติจากผู้มีอำนาจ หรือไม่	✓		(3) หนังสืออนุมัติจากผู้มีอำนาจ

ลำดับที่	รายการสอบทาน	ผลการประเมิน		*เอกสารหลักฐานประกอบ
		มี/ใช่	ไม่มี/ไม่ใช่	
	(4) นอกจากเผยแพร่ผ่านเว็บไซต์ของหน่วยงาน AA แล้ว มีเผยแพร่ผ่านช่องทางอื่น หรือไม่	✓		(4) หลักฐานการเผยแพร่ช่องทางอื่น
	(5) หน่วยงาน AA ได้กำหนดเป็นนโยบายหรือแนวปฏิบัติให้มีการทบทวนและปรับปรุงการบริหารความเสี่ยงฯ เป็นประจำทุกปี หรือไม่	✓		(5) นโยบายและแนวปฏิบัติ
	1.5 โครงการพัฒนาระบบสารสนเทศของกรม A			
	1.5.1 แผนแม่บท IT			
	(1) แผนแม่บท IT พ.ศ. 2557 – 2561 ได้รับความเห็นชอบจากผู้มีอำนาจและมีการประกาศใช้ หรือไม่	✓		(1) หนังสือให้ความเห็นชอบจากผู้มีอำนาจ
	(2) กรม A มีการจัดทำแผนแม่บท IT หลังรอบระยะเวลาแผนแม่บท IT พ.ศ. 2557 – 2561 หรือไม่	✓		(2) แผนแม่บท IT ฉบับปัจจุบัน
	1.5.2 แผนปฏิบัติการดิจิทัลของกรม A			
	(1) แผนปฏิบัติการดิจิทัลของกรม A พ.ศ. 2563 – 2565 ได้รับความเห็นชอบประกาศใช้จากผู้มีอำนาจ หรือไม่	✓		(1) หนังสือให้ความเห็นชอบจากผู้มีอำนาจ
	(2) มีการติดตามและประเมินผลการปฏิบัติตามแผนปฏิบัติการดิจิทัล หรือไม่	✓		(2) รายงานผลการติดตามและประเมินผล และหนังสือเสนอผู้มีอำนาจทราบ
	(3) แผนปฏิบัติการดิจิทัลของกรม A พ.ศ. 2566 – 2570 อยู่ระหว่างดำเนินการประกาศใช้ใช่หรือไม่	✓		(3) รายงานการประชุมของคณะกรรมการจัดทำแผนฯ
	1.6 หน่วยงาน AA มีการติดตามและประเมินผลการนำนโยบายต่าง ๆ สู่การปฏิบัติ หรือไม่	✓		1.6 รายงานติดตามและประเมินผลฉบับล่าสุด
2	**การแต่งตั้งคณะกรรมการ** 2.1 คณะกรรมการด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรม A			
	2.1.1 หน่วยงาน AA มีการทบทวนความเหมาะสมของคำสั่งแต่งตั้งคณะกรรมการพร้อมอำนาจหน้าที่เป็นประจำทุกปี หรือไม่	✓		2.1.1 เลขที่คำสั่งแต่งตั้งปัจจุบัน 2.1.2 รายงานการประชุม

ลำดับที่	รายการสอบทาน	ผลการประเมิน		*เอกสารหลักฐานประกอบ
		มี/ใช่	ไม่มี/ไม่ใช่	
	2.1.2 มีการขับเคลื่อนตามอำนาจหน้าที่ของคณะกรรมการ อย่างต่อเนื่อง หรือไม่	✓		
	2.2 คณะกรรมการรักษาความปลอดภัยของระบบสารสนเทศของกรม A			2.2.1 เลขที่คำสั่งแต่งตั้งปัจจุบัน
	2.2.1 หน่วยงาน AA มีการแต่งตั้งคณะกรรมการฯ เพื่อบริหารจัดการรักษาความปลอดภัยของระบบสารสนเทศของกรม A หรือไม่		✓	2.2.2 รายงานการประชุม
	2.2.2 มีการขับเคลื่อนตามอำนาจหน้าที่ของคณะกรรมการ อย่างต่อเนื่อง หรือไม่		✓	
	2.3 คณะกรรมการบริหารความเสี่ยงด้านสารสนเทศของกรม A			23.1 เลขที่คำสั่งแต่งตั้งปัจจุบัน
	2.3.1 หน่วยงาน AA มีการแต่งตั้งคณะกรรมการฯ เพื่อบริหารจัดการความเสี่ยงด้านสารสนเทศ ของกรม A หรือไม่	✓		2.3.2 รายงานการประชุม
	2.3.2 มีการขับเคลื่อนตามอำนาจหน้าที่ของคณะกรรมการอย่างต่อเนื่องหรือไม่	✓		
3	**การเข้าถึง และการใช้งาน (ระบบเครือข่าย ระบบปฏิบัติการ Application)**			
	3.1 กำหนดสิทธิในการเข้าถึงการใช้งานทุกระบบเป็นลายลักษณ์อักษรที่ชัดเจน	✓		3.1 คำสั่งแต่งตั้ง/มอบหมาย
	3.2 มีแผนและระบบการตรวจสอบบำรุงรักษาสายไฟฟ้าภายในห้องปฏิบัติการ สายเคเบิล และอุปกรณ์คอมพิวเตอร์ Hardware ของหน่วยงาน AA อยู่สม่ำเสมอ	✓		3.2 แผนการซ่อมบำรุงรักษาของปีงบประมาณล่าสุด
	3.3 หน่วยงาน AA จัดทำคู่มือ/แนวการปฏิบัติงานของทุกระบบซึ่งได้รับความเห็นชอบจากผู้มีอำนาจให้กับผู้ใช้งาน (User)	✓		3.3 คู่มือ/แนวการปฏิบัติงานพร้อมหนังสือลงนามให้ความเห็นชอบ
	3.4 มีข้อกำหนดในการลงทะเบียนการใช้งานที่ชัดเจน	✓		3.4 ทะเบียนลงชื่อการใช้งาน
	3.5 หน่วยงาน AA มีการจ้างผู้รับจ้างหรือผู้ให้บริการภายนอกด้านสารสนเทศ หรือไม่	✓		3.5 สัญญาจ้างหรือข้อตกลง

ลำดับที่	รายการสอบทาน	ผลการประเมิน		*เอกสารหลักฐานประกอบ
		มี/ใช่	ไม่มี/ไม่ใช่	
	3.6 ระบบงาน IT ในลักษณะ Web Application Mobile Application ของหน่วยงาน AA ได้มีการติดตามและจัดเก็บข้อมูลสถิติการใช้งานของแต่ละระบบงาน หรือไม่	✓		3.6 รายงานการติดตามและสถิติการใช้งานของแต่ละระบบงาน
4	**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ฉบับที่ 2) พ.ศ. 2560** 4.1 กรม A มีการเฝ้าระวัง ป้องกัน และดำเนินการเกี่ยวกับพระราชบัญญัติดังกล่าว หรือไม่ 4.2 กรม A มีมาตรการลงโทษเจ้าหน้าที่ของหน่วยงาน AA เนื่องจากการกระทำความผิดตามพระราชบัญญัติดังกล่าว หรือไม่	✓ ✓		4.1 หลักฐานดำเนินการ 4.2 มาตรการ
5	**ปัญหา อุปสรรค การปฏิบัติงานด้านสารสนเทศ**			

หมายเหตุ : ***ช่อง “เอกสารหลักฐานประกอบ” หากหน่วยงาน AA มีเอกสารหลักฐานอื่นใดนอกเหนือจากที่ระบุไว้ ซึ่งจะเป็นประโยชน์ต่อการตรวจสอบ สามารถระบุเพิ่มเติมได้

ผู้ให้ข้อมูล.....ชื่อผู้ให้ข้อมูล..หน่วยงาน...AA.....
(.....ชื่อผู้ให้ข้อมูล..หน่วยงาน...AA.....)
ตำแหน่ง.....ผู้ให้ข้อมูล..หน่วยงาน...AA.....
วันที่.....xx...เดือน..xx..พ.ศ..25xx.....

ผู้สอบถาม.....ก.....
(.....นางสาว..ก.....)
ตำแหน่ง.....หัวหน้าทีมตรวจสอบภายใน.....
วันที่..... xx...เดือน..xx..พ.ศ..25xx.....

3.5.2 สอบทานนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A กับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 ว่ามีความสอดคล้อง ครอบคลุมตามประกาศ หรือไม่ โดยมีเครื่องมือเป็นกระดาษทำการ (รหัส ตสน. สท. 2/2566)

ตสน.สท. 2/2566

กระดาษทำการ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หน่วยรับตรวจ กรม A

วันที่ .....

วัตถุประสงค์ : เพื่อให้ทราบว่านโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A สอดคล้องกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 หรือไม่

ลำดับ	ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553	นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A	
	รายการ	ผลการสอบทาน	
		มี	ไม่มี
1	นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A ครอบคลุมเนื้อหา 1.1 การเข้าถึงหรือควบคุมการใช้งาน 1.2 จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ 1.3 แผนเตรียมความพร้อมกรณีฉุกเฉิน 1.4 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ	✓	
2	หน่วยงาน AA มีประกาศนโยบายและข้อปฏิบัติให้ผู้เกี่ยวข้องทั้งหมดทราบและถือปฏิบัติ	✓	
3	หน่วยงาน AA กำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติอย่างชัดเจน	✓	
4	หน่วยงาน AA มีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติเป็นปัจจุบันเสมอ	✓	

ลำดับ	ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553	นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A	
	รายการ	ผลการสอบทาน	
		มี	ไม่มี
5	ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ครอบคลุมเนื้อหา 5.1 การเข้าถึงและควบคุมการใช้งานสารสนเทศ 5.2 ข้อกำหนดการใช้งานตามภารกิจ 5.3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน 5.4 กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน 5.5 การควบคุมการเข้าถึงเครือข่าย 5.6 การควบคุมการเข้าถึงระบบปฏิบัติการ 5.7 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น 5.8 การจัดทำระบบสำรอง 5.9 การจัดให้มีการให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ 5.10 กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย	✓	
6	การเข้าถึงและควบคุมการใช้งานสารสนเทศ ครอบคลุมเนื้อหา 6.1 การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผล 6.2 การอนุญาต การกำหนดสิทธิ การมอบอำนาจ 6.3 ประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับ ระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง	✓	
7	ข้อกำหนดการใช้งานตามภารกิจ 7.1 การควบคุมการเข้าถึงสารสนเทศ 7.2 การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย	✓	
8	การบริหารจัดการการเข้าถึงของผู้ใช้งาน เฉพาะผู้ที่ได้รับอนุญาตแล้วและผ่านการฝึกอบรม หลักสูตรความมั่นคงปลอดภัยสารสนเทศ 8.1 สร้างความรู้ความเข้าใจเกี่ยวกับการใช้งาน และมาตรการป้องกัน	✓	

ลำดับ	ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553	นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A	
	รายการ	ผลการสอบทาน	
		มี	ไม่มี
	8.2 การลงทะเบียนผู้ใช้งานและการตัดออกจากทะเบียนผู้ใช้งาน 8.3 การบริหารจัดการสิทธิของผู้ใช้งาน 8.4 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน 8.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน		
9	กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน 9.1 การใช้งานรหัสผ่าน 9.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ 9.3 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ 9.4 ข้อมูลความลับให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544	✓	
10	การควบคุมการเข้าถึงเครือข่าย 10.1 การใช้งานบริการเครือข่าย 10.2 การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร 10.3 การระบุอุปกรณ์บนเครือข่าย 10.4 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ 10.5 การแบ่งแยกเครือข่าย 10.6 การควบคุมการเชื่อมต่อทางเครือข่าย 10.7 การควบคุมการจัดเส้นทางบนเครือข่าย	✓	
11	การควบคุมการเข้าถึงระบบปฏิบัติการ 11.1 การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย 11.2 การระบุและยืนยันตัวตนของผู้ใช้งาน 11.3 การบริหารจัดการรหัสผ่าน 11.4 การใช้งานโปรแกรมอรรถประโยชน์ 11.5 การว่างเว้นใช้งานให้ยุติการใช้งานระบบสารสนเทศ 11.6 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ	✓	

ลำดับ	ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.2553	นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A	
	รายการ	ผลการสอบทาน	
		มี	ไม่มี
12	การควบคุมการเข้าถึงโปรแกรมประยุกต์ มีการควบคุม ดังนี้ 12.1 การจำกัดการเข้าถึงสารสนเทศ 12.2 ระบบซึ่งไวต่อการรบกวน 12.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ 12.4 การปฏิบัติงานจากภายนอกสำนักงาน	✓	
13	ระบบสำรอง ตามแนวทาง ดังนี้ 13.1 พิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสม 13.2 แผนเตรียมความพร้อมกรณีฉุกเฉิน 13.3 กำหนดหน้าที่ความรับผิดชอบของบุคลากรดูแลระบบสารสนเทศ ระบบสำรอง และแผนฉุกเฉิน 13.4 การทดสอบระบบสารสนเทศ ระบบสำรอง และแผนฉุกเฉินให้มีสภาพพร้อมใช้งาน 13.5 ความถี่ในการปฏิบัติ	✓	
14	การตรวจสอบและประเมินความเสี่ยง 14.1 จัดให้มีอย่างน้อยปีละ 1 ครั้ง 14.2 จัดให้มีการประเมินโดยผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก	✓	

สรุปผลการสอบทาน

.....

.....

.....

ผู้สอบถาม.....ก.....

(.....นางสาว..ก.....)

ตำแหน่ง.....หัวหน้าทีมตรวจสอบภายใน.....

วันที่..... xx...เดือน..xx..พ.ศ..25xx.....

3.5.3 สังเกตการณ์สภาพสิ่งแวดล้อมพื้นที่ปฏิบัติการด้านสารสนเทศ เพื่อให้มั่นใจมีความปลอดภัย และสอดรับกับนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของหน่วยงาน AA โดยมีเครื่องมือกระดาษทำการ (ตสน. สท. 3/2566)

ตสน.สท. 3/2566

กระดาษทำการ สังเกตการณ์ พื้นที่ปฏิบัติการด้านสารสนเทศ

หน่วยรับตรวจ กรม A

วันที่ .....

วัตถุประสงค์ : เพื่อให้ทราบว่ากรม A ได้ปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ หรือไม่

ลำดับ	เรื่อง	ผลการสังเกตการณ์		คำอธิบาย พร้อมหลักฐาน (ภาพถ่าย หรือ เอกสาร)
		มี/ใช่	ไม่มี/ไม่ใช่	
1	พื้นที่ปฏิบัติงานด้านสารสนเทศเป็นพื้นที่เฉพาะส่วนบุคคลที่ได้รับอนุญาตเท่านั้น	✓		ห้องควบคุมระบบ NETWORK - มีการกำหนดรายชื่อผู้รับผิดชอบแปะไว้ที่หน้าห้อง - มีการสแกนนิ้วก่อนเข้าห้อง
2	จัดให้มีการลงทะเบียนก่อนการเข้าในพื้นที่ปฏิบัติงาน	✓		- มีการกรอกแบบฟอร์มขอเข้าใช้งานเครื่องแม่ข่าย *ยกเว้นเจ้าหน้าที่ของบริษัทที่เข้ามาดูแลระบบที่สามารถเข้ามาได้ โดยที่ไม่ต้องกรอกแบบฟอร์ม เจ้าหน้าที่ของบริษัท 4-5 คน ที่ดูแลระบบสามารถเข้าได้ ตามรายชื่อในสัญญา
3	มีการติดตั้งกล้องวงจรปิดในพื้นที่ปฏิบัติงานด้านสารสนเทศ	✓		มีการติดตั้งกล้องวงจรปิด 2 ตัว ลักษณะการทำงานเป็นระบบ Online บันทึก Video ได้ 30 วัน แต่ไม่มีจอมอนิเตอร์กล้องวงจรปิดสำหรับผู้ควบคุมการปฏิบัติงานเป็นการเฉพาะ

ลำดับ	เรื่อง	ผลการสังเกตการณ์		คำอธิบาย พร้อมหลักฐาน (ภาพถ่าย หรือ เอกสาร)
		มี/ใช่	ไม่มี/ไม่ใช่	
4	สถานที่เก็บเครื่องมืออุปกรณ์ด้านสารสนเทศมีการล๊อคกุญแจเมื่อไม่มีการใช้งาน และสถานที่เก็บกุญแจมีความปลอดภัย	✓		ผู้รับผิดชอบควบคุมงานด้านสารสนเทศ คือ รายชื่อตามที่ประกาศด้านหน้าประตูทางเข้า ห้อง Server แต่ไม่มีผู้รับผิดชอบอุปกรณ์ด้านสารสนเทศเป็นการเฉพาะแต่ละตู้
5	มีการติดตั้งสัญญาณเตือนป้องกันกรณีฉุกเฉิน เช่น เกิดอัคคีภัย โจรกรรม อุทกภัย เป็นต้น	✓		- มีอุปกรณ์ตรวจจับความเคลื่อนไหว เซ็นเซอร์ - มีเครื่องดักจับควัน ทดสอบปีละ 2 ครั้ง
6	เครื่อง UPS (เครื่องสำรองไฟ) มีเพียงพออยู่ในสถานะพร้อมใช้งาน	✓		มี UPS รองรับ Server ทั้งหมดเพียงพอ
7	หน่วยงาน AA มีการควบคุมการเชื่อมต่อ Terminal กับระบบคอมพิวเตอร์หลักอย่างรัดกุม	✓		- ต้องมีการขออนุญาตก่อนไปใช้ในระบบและต้องผ่านความเห็นชอบจากผู้มีอำนาจ (ผอ.หน่วยงาน AA) - เบื้องต้น Firewall จะมีการควบคุมป้องกันตามนโยบายของ Firewall อยู่แล้ว - ต้องมีการระบุขอบเขตการใช้งานที่ชัดเจน เช่น ช่วงเวลา และ server ที่จะเข้าไปดำเนินการ - มีการกำหนด User และ Password ในการเข้าใช้งาน
8	หน่วยงาน AA มีจัดทำ/ติดข้อความ/สัญลักษณ์เกี่ยวกับกฎ ข้อบังคับของเจ้าหน้าที่ขณะปฏิบัติงาน ข้อปฏิบัติตนในการเข้าใช้งานในพื้นที่ปฏิบัติการด้านสารสนเทศ (ห้อง Server) ในที่เปิดเผยผู้ใช้งานสังเกตเห็นได้ชัดเจน		✓	ไม่มีข้อปฏิบัติในการเข้าใช้งานในพื้นที่ห้อง Server
9	หน่วยงาน AA มีการแจ้งเวียนให้ผู้รับผิดชอบตามนโยบายรับทราบเป็นหลักฐาน		✓	ไม่มีการมอบหมายเป็นลายลักษณ์อักษร

ลำดับ	เรื่อง	ผลการสังเกตการณ์		คำอธิบาย พร้อมหลักฐาน (ภาพถ่าย หรือ เอกสาร)
		มี/ใช่	ไม่มี/ไม่ใช่	
10	อุณหภูมิของห้องที่จัดเก็บเครื่องมืออุปกรณ์ หรือข้อมูลสารสนเทศ	✓		มีการกำหนดอุณภูมิห้อง 20 องศา
11	มีการแบ่งแยกเครือข่ายตามกลุ่มผู้ใช้งาน ได้แก่ กลุ่มบริการสารสนเทศ กลุ่มผู้ใช้งาน กลุ่มระบบสารสนเทศ	✓		มีอยู่ในแผนไซเบอร์ ไม่สามารถเผยแพร่เอกสารสู่ภายนอกได้

ข้อสังเกต

1. แนวปฏิบัติการใช้งานห้อง Server

2. เอกสารกำหนดสิทธิผู้รับผิดชอบ

ผู้ให้ข้อมูล.....ชื่อผู้ให้ข้อมูล..หน่วยงาน...AA.....
(.....ชื่อผู้ให้ข้อมูล..หน่วยงาน...AA.....)
ตำแหน่ง.....ผู้ให้ข้อมูล..หน่วยงาน...AA.....
วันที่.....xx...เดือน..xx..พ.ศ..25xx.....

ผู้สอบถาม.....ก.....
(.....นางสาว..ก.....)
ตำแหน่ง.....หัวหน้าทีมตรวจสอบภายใน.....
วันที่..... xx...เดือน..xx..พ.ศ..25xx.....

3.4.4 การทดสอบระบบงาน IT เป็นการค้นหาหลักฐานสำหรับสิ่งผิดปกติที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ (IT) โดยมีวัตถุประสงค์เพื่อประเมินความเพียงพอของการ ควบคุมภายในด้าน IT และการจัดการความเสี่ยงด้าน IT โดยมีเครื่องมือเป็นกระดาษทำการ (ตสน. สท. 4/2566)

ตสน.สท. 4/2566

กระดาษทำการ ทดสอบระบบงาน IT กรม A

หน่วยรับตรวจ กรม A

วันที่ .....

วัตถุประสงค์ : เพื่อให้ทราบว่ากรม A ได้ปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ หรือไม่

ลำดับ	เรื่อง	ผลการทดสอบ		คำอธิบาย พร้อมหลักฐาน (ภาพถ่าย หรือ เอกสาร)
		มี/ใช่	ไม่มี/ไม่ใช่	
1	การใช้งาน 1 คน ต่อ 1 User ไม่มีการใช้ร่วม และมีเอกสารกำหนดสิทธิชัดเจน รวมถึงการทบทวนสิทธิอย่างเหมาะสม	✓		- 1 User ใช้งานได้คนเดียว - มีการแจ้งผู้ใช้งาน Username Password เป็นหนังสือลับ - ใช้งานได้ตามสิทธิของตนเอง เช่น ระบบ e-Saraban ในส่วนของธุรการกับบทบาทส่วนบุคคล เป็นต้น - ต้องเป็น Username password เฉพาะงานที่รับผิดชอบ หรือไม่แจ้งเป็นหนังสือรับ - สิทธิบุคคลภายนอกเข้ามา
2	มีคู่มือการปฏิบัติงานของ User แต่ละระดับ	✓		- ระบบ e-Saraban จะมีคู่มือแบ่งระดับการทำงานของแต่ละระดับ - ถ้ากรณีที่มีการใช้งานภายในหน่วยงานจะไม่มีคู่มือ - จะมีคู่มือเกือบทุกระดับ หากเป็นส่วนที่ต้องใช้งานร่วมกันหลายหน่วยงาน

ลำดับ	เรื่อง	ผลการทดสอบ		คำอธิบาย พร้อมหลักฐาน (ภาพถ่าย หรือ เอกสาร)
		มี/ใช่	ไม่มี/ไม่ใช่	
3	การยืนยันตัวตนบุคคลก่อนอนุญาตให้ผู้ใช้งานเชื่อมต่อเข้าระบบสารสนเทศ/เครือข่ายของหน่วยงาน AA	✓		- ต้องมีการขออนุญาตขอใช้งานเป็นหนังสือ - มีการลงนามให้ความเห็นชอบอนุมัติสิทธิการใช้งาน - มีการระบุว่าจะดูที่ไหนได้บ้างเฉพาะงานนั้นๆ - มี Log เก็บข้อมูลการใช้งาน - มีแบบฟอร์สำหรับการขอใช้งานเพื่อเชื่อมต่อเข้าระบบสารสนเทศ
4	หน่วยงาน AA มีกำหนดรหัสผ่านที่สามารถทำงานอัตโนมัติได้	✓		- Internet - รับรองเงินเดือน - Hotspot
5	หน่วยงาน AA มีกำหนดเวลาในการเชื่อมต่อระบบสารสนเทศหรือโปรแกรมต่าง ๆ	✓		- Intranet (45 นาที) - ส่วนใหญ่จะให้ใช้เวลาในระบบ 15 นาที โปรแกรมเมอร์จะเข้าใจแบบนั้น - ถ้าระบบมีความสำคัญ อาจจะน้อยกว่า 15 นาที ขึ้นอยู่กับผู้เขียนโปรแกรม
6	ผู้ใช้งาน เข้าใช้งานในระบบตามสิทธิที่ได้รับเท่านั้น	✓		- ยกตัวอย่างระบบ e-Saraban มีชื่อตามสิทธิที่ได้เฉพาะบุคคลตามบทบาทที่ได้รับ - ยกตัวอย่างระบบจองห้องประชุมของ Admin กับคนอนุมัติห้องประชุม
7	การถอดถอนสิทธิ กรณีการเลิกจ้าง หรือพ้นจากตำแหน่งความรับผิดชอบ	✓		- ยกตัวอย่างข้าราชการลาออก - การระบุสถานะดูจากคำสั่งของกรม A - ถ้าเกษียณอายุราชการจะดูข้อมูลปีละครั้ง - ถ้าลาออกจะดูจากคำสั่งใน e-document ลาออกเลยแก้ไขเลย

ลำดับ	เรื่อง	ผลการทดสอบ		คำอธิบาย พร้อมหลักฐาน (ภาพถ่าย หรือ เอกสาร)
		มี/ใช่	ไม่มี/ไม่ใช่	
				- ทดสอบโดยนำชื่อที่ถอดถอนสิทธิไปแล้วเข้าใช้งานในระบบ
8	ระบบสารสนเทศ ระบบสำรองข้อมูล และการนำข้อมูลที่กู้คืนมาใช้งาน มีการทดสอบความพร้อมของระบบงานต่าง ๆ	✓		- มีการทดสอบการสำรองข้อมูล - กำหนดความถี่ในการสำรองข้อมูลจะมากกว่าทีกำหนดในเล่มนโยบาย -การสำรองข้อมูลทำงานร่วมกัน ระหว่างเจ้าหน้าที่ของกรม A และผู้รับจ้าง
9	การแจ้งปัญหาอุปสรรคการใช้ระบบเทคโนโลยีสารสนเทศจากผู้ใช้ระบบเทคโนโลยีสารสนเทศ - จำนวนครั้งต่อปี (ประมาณการ) - ประเภท/รายการ/เรื่องส่งแจ้ง (ส่วนใหญ่) - หน่วยงาน AA มีการจัดทำทะเบียนคุมการแจ้งหรือไม่	✓		- สามารถดูจากระบบได้ในการนับจำนวนคำร้องขอแจ้งเรื่องซ่อม - มีการรวบรวมข้อมูลตามหน่วยงาน - หน่วยงาน AA มีระบบแจ้งปัญหาอุปสรรคการใช้งานในระบบหน้า Intranet
10.	หน่วยงานมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ฉบับที่ 2) พ.ศ. 2560	✓		- หน่วยงานที่รับผิดชอบดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้จำนวนไม่น้อยกว่า 90 วัน ตามพระราชบัญญัติกำหนด

สรุปผลการสอบทาน

แนะนำเพิ่มเติมเรื่องเกณฑ์การในการวิเคราะห์ในการสำรองข้อมูล

ผู้ให้ข้อมูล.....ชื่อผู้ให้ข้อมูล..หน่วยงาน...AA.....
(.....ชื่อผู้ให้ข้อมูล..หน่วยงาน...AA.....)
ตำแหน่ง.....ผู้ให้ข้อมูล..หน่วยงาน...AA.....
วันที่.....xx...เดือน..xx..พ.ศ..25xx.....

ผู้สอบถาม.....ก.....
(.....นางสาว..ก.....)
ตำแหน่ง.....หัวหน้าทีมตรวจสอบภายใน.....
วันที่..... xx...เดือน..xx..พ.ศ..25xx.....

3.4.5 การตรวจนับเครื่องมืออุปกรณ์ด้านสารสนเทศ เป็นการพิสูจน์จำนวนและสภาพของสิ่งที่ตรวจนับว่ามีอยู่ครบถ้วน ชำรุด หรือไม่ สุ่มตัวอย่างตรวจนับโดยวิธี Stratified Sampling ด้วยการแบ่งเครื่องมืออุปกรณ์เป็นหมวดหมู่/ประเภท และสุ่มจากแต่ละประเภท โดยมีเครื่องมือเป็นกระดาษทำการ (ตสน. สท. 5/2566)

ตสน.สท. 5/2566

กระดาษทำการ การตรวจนับเครื่องมืออุปกรณ์ ด้านสารสนเทศ

หน่วยรับตรวจ กรม A

วันที่ .....

วัตถุประสงค์ : เพื่อให้ทราบว่ากรม A มีการควบคุมเครื่องมืออุปกรณ์ตรงกับทะเบียนคุม/บัญชีอุปกรณ์ เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กฎหมาย ระเบียบ ข้อบังคับ หรือไม่

ลำดับ	รายการเครื่องมืออุปกรณ์ (ทะเบียนคุม)	สถานที่ตั้ง	ผลการตรวจนับ	
			ตรง/ไม่ตรง	ใช้ได้/ใช้ไม่ได้
1	N-AT02-อุปกรณ์กำหนดเครือข่าย ATM : Cisco Light Stream 1010 (2)	หน่วยงาน AA	✓	✓
2	N-PH01 อุปกรณ์ระบบ IP Phone (60 เครื่อง)	หน่วยงาน BB	ตรวจนับได้เพียง 1 เครื่อง สำหรับหน่วยงาน AA รหัสครุภัณฑ์ 5805-001-0147 หน่วยงาน AA#1 หน่วยงาน AA ดำเนินการส่งมอบอุปกรณ์ให้หน่วยงาน BB ใช้งาน และรับผิดชอบอุปกรณ์เองแล้ว	
3	N-WF01 ระบบ WIFI LDD Hotspot	หน่วยงาน CC	✓	✓
4	N-CM01 อุปกรณ์ Call Manager	หน่วยงาน DD	ใช้งานได้แต่ปัจจุบันไม่ได้ใช้งาน เนื่องจากสำรองไว้ใช้งานในกรณีเครือข่ายโทรศัพท์เกิดปัญหาขัดข้องเท่านั้น	
5	N-NS03 อุปกรณ์ระบบ Network Attach Storage	หน่วยงาน EE	✓	✓

หมายเหตุ : ทุกรายการที่สุ่มบรรจุอยู่ในแผนบำรุงรักษา

สรุปผลการตรวจนับ

- รายการเครื่องมืออุปกรณ์ (ทะเบียนคุม) เมื่อเปรียบเทียบของปี 2565 กับปีงบประมาณ 2566 ไม่มีรายการเปลี่ยนแปลงแต่ของปี 2566 จะเป็นการจัดประเภทหมวดอุปกรณ์ ซึ่งเมื่อมีการสอบทานข้อมูลหน่วยงานจะใช้ข้อมูลของปี 2565 และข้อมูลปี 2566 ประกอบการสอบทาน

- รายการเครื่องมืออุปกรณ์ของปี 2566 จะประกอบเฉพาะรายการที่หน่วยงาน AA ควบคุมที่ห้องปฏิบัติการ

- หน่วยงาน AA มีการนำ N-CM01 อุปกรณ์ Call Manager ระบบสื่อสารผ่าน IP Address แต่ยังมิได้จัดทำแผนเสนอคณะกรรมการ IT

ข้อเสนอแนะ

ควรมีการพิจารณาทบทวนเครื่องมืออุปกรณ์และระบบว่าปัจจุบันมีการใช้งานหรือไม่ หากต้องการใช้งานในอนาคตควรมีการจัดทำแผนการใช้งานที่ชัดเจน และเหมาะสมกับสภาพแวดล้อมของหน่วยงาน เพื่อให้ตอบสนองความต้องการต่อผู้ใช้งานได้อย่างแท้จริง

ผู้ให้ข้อมูล.....ชื่อผู้ให้ข้อมูล..หน่วยงาน...AA.....
(.....ชื่อผู้ให้ข้อมูล..หน่วยงาน...AA.....)
ตำแหน่ง.....ผู้ให้ข้อมูล..หน่วยงาน...AA.....
วันที่.....xx...เดือน..xx..พ.ศ..25xx.....

ผู้สอบถาม.....ก.....
(.....นางสาว..ก.....)
ตำแหน่ง.....หัวหน้าทีมตรวจสอบภายใน.....
วันที่..... xx...เดือน..xx..พ.ศ..25xx.....

บทที่ 5

สรุปผลการตรวจสอบกรณีศึกษา

การปฏิบัติงานตรวจสอบ โดยมีหน่วยรับตรวจ AA ของกรม A เมื่อเสร็จสิ้นงานตรวจสอบ ทีมตรวจสอบได้รวบรวมหลักฐาน โดยรวบรวมจากเอกสาร ข้อมูล ข้อเท็จจริง ที่ได้จากการตรวจสอบ วิเคราะห์ ประเมินผลจากการตรวจสอบ เพื่อให้ได้ข้อสรุปผลการตรวจสอบพร้อมข้อเสนอแนะ เสนอหัวหน้าหน่วยงานตรวจสอบต่อไป และหัวหน้าส่วนราชการ ตามลำดับ ดังนี้

รายการ	ผลการตรวจสอบ	ข้อเสนอแนะ/ความคิดเห็น
1. การกำหนดและการปฏิบัติตามนโยบายตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 โดยมีขอบเขต ดังนี้ 1.1 ประกาศนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A ประกาศ ณ วันที่ 1 ตุลาคม 25XX 1.2 แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร 1.3 แผนรองรับภัยพิบัติและการบริหารจัดการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรม A 1.4 การบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของกรม A 1.5 โครงการพัฒนาระบบสารสนเทศของกรม A (แผนแม่บท IT) 1.6 การติดตามและประเมินผล การนำนโยบายต่าง ๆ สู่การปฏิบัติ	จากการสอบทานเอกสารนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A ซึ่งมีรายละเอียด ดังนี้ ● วัตถุประสงค์ ● องค์ประกอบของนโยบายแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยได้แบ่งแนวปฏิบัติไว้เป็น 10 ส่วน (ส่วนที่1–10) ซึ่งประกอบด้วยวัตถุประสงค์และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของกรม A ● ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ **ผลการตรวจสอบ :** 1. จากการสอบทานระหว่างประกาศของกรม A เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A พ.ศ. 2555 (ฉบับที่ประกาศใช้ ณ วันที่ 1 ต.ค. 25XX) กับเอกสารนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A แนบท้ายประกาศ พบว่า	1. เห็นควรจัดทำประกาศของกรม A เรื่อง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A โดยนำนโยบายส่วนที่ 9 นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ และส่วนที่ 10 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศเป็นองค์ประกอบของนโยบาย เพื่อให้มีความครอบคลุม ครบถ้วน ตรงกันกับเอกสารนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A 2. กรม A ควรมีข้อกำหนดด้านการควบคุมความมั่นคงปลอดภัยของข้อมูลสารสนเทศเพิ่มเติมเพื่อลดความเสี่ยงในการใช้งานอุปกรณ์สารสนเทศ/การใช้/การเข้าถึงข้อมูลสารสนเทศ และควรสื่อสารไปยังผู้ใช้งานของทุกหน่วยงานสังกัดกรม A เพื่อให้ตระหนักรับรู้และปฏิบัติตามอย่างปลอดภัย ซึ่งจะทำให้กรม A มีมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย (ประกาศคณะกรรมการธุรกรรมทาง

รายการ	ผลการตรวจสอบ	ข้อเสนอแนะ/ความคิดเห็น
	องค์ประกอบของเอกสารนโยบายฯ ส่วนที่ 9 และส่วนที่ 10 ไม่ปรากฏในประกาศของกรม A 2. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีเนื้อหาไม่ครอบคลุมบางประเด็น ได้แก่ - การจัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์ โดยหน่วยงานภายนอก/ผู้ให้บริการภายนอก (ผู้รับจ้าง) - การระบุเงื่อนไขการปกปิดข้อมูลจากหน่วยงานภายนอก/ผู้ให้บริการภายนอก (ผู้รับจ้าง) กรณีที่มีการจัดจ้างให้เข้าดูแลระบบเครือข่าย/ดำเนินการอื่นใด ซึ่งอาจมีผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	อิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555) โดยข้อกำหนดควรครอบคลุมถึงประเด็นต่าง ๆ ดังนี้ 2.1 กำหนดการควบคุมบริษัทที่จัดจ้าง (outsource) ดูแลระบบเครือข่ายและคอมพิวเตอร์ ในกรณีมีการจ้างเหมาดำเนินงาน การดูแล พัฒนาและบำรุงรักษาระบบ รวมถึงการควบคุมก่อนและหลังการจ้าง เช่น ข้อกำหนดการรักษาข้อมูลความลับของทางราชการ เป็นต้น 2.2 การส่งคืนสินทรัพย์ กรณีเสื่อมสภาพ/ล้าสมัย หรือกรณียืมสินทรัพย์ระหว่างหน่วยงานควรมีข้อกำหนดในการดำเนินการที่ชัดเจน เช่น - กำหนดการล้างข้อมูล (Format Data) และการล้างการตั้งค่าทั้งหมดออกจากอุปกรณ์ก่อน/ให้ทำลายข้อมูลสำคัญในสินทรัพย์ก่อนที่จะกำจัดสินทรัพย์ดังกล่าวหรือส่งคืนสินทรัพย์/ตัดจำหน่ายครุภัณฑ์ออกจากทะเบียนคุมของหน่วยงาน - กำหนดวิธีการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในสินทรัพย์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำสินทรัพย์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ เป็นต้น **หมายเหตุ :** คำนิยามสินทรัพย์/ทรัพย์สิน ตามเอกสารนโยบายฯ เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ

รายการ	ผลการตรวจสอบ	ข้อเสนอแนะ/ความคิดเห็น
		และเครื่องคอมพิวเตอร์แบบพกพา อุปกรณ์ระบบเครือข่ายรวมถึงสื่อที่ใช้ในการบันทึกข้อมูล เป็นต้น
2. การสอบทานการดำเนินงานด้านนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A - การเข้าถึงและการใช้งาน (ระบบเครือข่าย ระบบปฏิบัติการ Application)	จากการสอบทานการจัดทำขั้นตอนการปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ พบว่า การดำเนินการส่วนใหญ่เป็นไปตามนโยบายและแนวปฏิบัติฯ 1. ผลการสอบทานการดำเนินงานสรุปได้ดังนี้ : - มีการจัดทำเอกสารขั้นตอนการปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศ โดยหน่วยงาน AA ได้มีการจัดทำคู่มือการสร้าง Bookmark ในเอกสารไฟล์ Word และนำขึ้นเผยแพร่ผ่านเว็บไซต์ของหน่วยงาน AA โดยผ่านความเห็นชอบจากคณะทำงานวิชาการของกรม A - มีการจัดทำคู่มือการใช้งานสำหรับระบบที่ใช้ร่วมกันหลายหน่วยงาน 2. ผลการสุ่มทดสอบการปฏิบัติงานด้านต่าง ๆ พบว่า เป็นไปตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม A ซึ่งมีรายละเอียดดังนี้ - ทดสอบระบบรักษาความปลอดภัยห้อง Server ภายใต้นโยบาย 2 ครั้ง/ปี และมีการรายงานผลการทดสอบเสนอต่อ ผอ.หน่วยงาน AA (ทดสอบครั้งที่ 1 วันที่ 15 มีนาคม 25XX โดยผู้ตรวจสอบภายในเข้าร่วมสังเกตการณ์)	-มีการปฏิบัติตามนโยบาย และแนวปฏิบัติฯ ที่กำหนด แต่เพื่อให้เกิดการควบคุมภายในที่ดีและลดความเสี่ยงจากกรณีผู้ที่ไม่มีสิทธิในการเข้าถึงการใช้งานในระบบเครือข่าย เห็นควรเพิ่มขั้นตอนและระยะเวลาการถอดถอนสิทธิผู้ใช้งานกรณีพนักงานจ้างเหมาเอกชนสิ้นสุดการจ้างงาน

รายการ	ผลการตรวจสอบ	ข้อเสนอแนะ/ความคิดเห็น
	- ทดสอบการใช้งานได้ตามสิทธิของตนเองจากระบบ e-Saraban แสดงผลบทบาทตำแหน่งธุรการและบทบาทส่วนบุคคล ตรงตามสิทธิของตนเอง - ทดสอบระบบจองห้องประชุม แสดงผลบทบาทผู้ดูแลระบบกับผู้อนุมัติ - ทดสอบการถอดถอนสิทธิจากรายชื่อและรหัสผ่านผู้ที่เกษียณอายุราชการในปีงบประมาณ พ.ศ. 2565 (ข้าราชการ/พนักงานราชการ)	
3. การตรวจนับเครื่องมืออุปกรณ์ด้านสารสนเทศ	การสุ่มสอบทานตรวจนับเครื่องมืออุปกรณ์ด้านสารสนเทศตามบัญชีอุปกรณ์เครือข่าย/ UPS ให้บริการ (ส่วนกลาง) จำนวน 5 รายการ ได้แก่ - รายการที่ 1 N-AT02 อุปกรณ์กำหนดเครือข่าย ATM : Cisco Light Stream 1010 (2) - รายการที่ 2 N-PH01 อุปกรณ์ระบบ IP Phone (60 เครื่อง) - รายการที่ 3 N-WF01 ระบบ WIFI LDD Hotspot - รายการที่ 4 N-CM01 อุปกรณ์ Call Manager ระบบสื่อสารผ่าน IP Address - รายการที่ 5 N-NS03 อุปกรณ์ระบบ Network Attach Storage ห้อง server **ผลการตรวจนับ :** 1. รายการที่ 2 N-PH01 อุปกรณ์ระบบ IP Phone (60 เครื่อง) มีจำนวน	3.1 ควรพิจารณาทบทวนปรับปรุงบัญชีอุปกรณ์เครือข่าย/UPS ที่ให้บริการให้เป็นปัจจุบัน และควรบรรจุอยู่ในแผนการบำรุงรักษาอย่างต่อเนื่อง 3.2 รายการ N-CM01 อุปกรณ์ Call Manager ระบบสื่อสารผ่าน IP Address ซึ่งปัจจุบันอุปกรณ์ที่ต้องใช้ร่วมกับอุปกรณ์ระบบ IP Phone คงเหลือปรากฏในระบบฐานข้อมูลครุภัณฑ์ online ของกรม A จำนวน 7 เครื่อง โดยบางเครื่องมิได้อยู่ในสภาพพร้อมใช้งาน จึงเห็นควรให้หน่วยงาน AA ที่รับผิดชอบเทคโนโลยีสารสนเทศประสานกับหน่วยงานผู้ครอบครองอุปกรณ์ระบบ IP Phone พิจารณาดำเนินการตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ส่วนที่ 3 การบำรุงรักษาการตรวจสอบ ส่วนที่ 4 การจำหน่ายพัสดุ

รายการ	ผลการตรวจสอบ	ข้อเสนอแนะ/ความคิดเห็น
	ไม่ตรงกับระบบฐานข้อมูลครุภัณฑ์ online ของกรม A โดยมีหน่วยงานผู้ถือครองจำนวน 6 แห่ง (7 เครื่อง) ได้แก่ หน่วยงาน AA หน่วยงาน BB หน่วยงาน CC หน่วยงาน DD หน่วยงาน EE และหน่วยงาน FF 2. รายการที่ 4 N-CM01 อุปกรณ์ Call Manager ระบบสื่อสารผ่าน IP Address เป็นระบบที่ต้องใช้ร่วมกับอุปกรณ์ระบบ IP Phone ซึ่งปัจจุบันคงเหลือปรากฏในระบบฐานข้อมูลครุภัณฑ์ online ของกรม A จำนวน 7 เครื่อง	
4. การสอบทานสภาพแวดล้อมทั่วไปห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server)	สภาพแวดล้อมโดยทั่วไปมีการจัดการและการควบคุมภายใน ซึ่งจากการสังเกตการณ์ภายในห้อง Server พบว่ามีการติดตั้งอุปกรณ์สำหรับป้องกันความเสียหายทางกายภาพ ได้แก่ - อุปกรณ์ตรวจจับควัน และอุปกรณ์ตรวจจับการเคลื่อนไหว - กล้องวงจรปิด 2 เครื่อง เพื่อเฝ้าระวังควบคุมผู้ที่ไม่ได้รับอนุญาตให้เข้า-ออกประตูทั้ง 2 ด้าน **ผลการตรวจสอบ :** หน่วยงาน AA ยังไม่มีการจัดทำป้ายชื่อ (Label) ผู้รับผิดชอบอุปกรณ์ด้านสารสนเทศเป็นการเฉพาะแต่ละตู้ที่จัดเก็บและไม่มีข้อกำหนด ในการเข้าใช้งานในพื้นที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server)	- ควรพิจารณาทบทวนและปรับปรุงรายชื่อผู้ดูแลสินทรัพย์แต่ละรายการ รวมถึงการจัดทำป้ายชื่อ (Label) ผู้รับผิดชอบอุปกรณ์บนตู้จัดเก็บ เพื่อให้มั่นใจว่าสินทรัพย์ทุกรายการมีผู้ดูแลรับผิดชอบอย่างเหมาะสม พร้อมทั้งจัดทำข้อกำหนดต่าง ๆ ในการเข้าใช้งานในพื้นที่ห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) และปิดประกาศข้อกำหนดไว้ด้านประตูทางเข้าเพื่อเป็นการควบคุมทางด้านกายภาพและเปิดเผยให้ผู้ที่เกี่ยวข้องและผู้ที่ไม่เกี่ยวข้องทราบและถือปฏิบัติโดยทั่วกัน - ควรจัดให้มีเจ้าหน้าที่ตรวจสอบประวัติการเข้า–ออกพื้นที่ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) เป็นประจำและควรมีการปรับปรุงข้อกำหนดรายการผู้มีสิทธิเข้า-ออกของเจ้าหน้าที่หน่วยงาน AA ที่รับผิดชอบด้านเทคโนโลยีสารสนเทศของกรม A

รายการ	ผลการตรวจสอบ	ข้อเสนอแนะ/ความคิดเห็น
		และผู้รับจ้างเป็นระยะ เพื่อเป็นการควบคุมสภาพแวดล้อมทางด้านกายภาพเชิงรุก และลดความเสี่ยงจากการเข้าถึงระบบโดยไม่ได้รับอนุญาต รวมถึงเป็นการป้องกันสินทรัพย์ของราชการให้มีความปลอดภัยมากยิ่งขึ้น

บรรณานุกรม

กรมสนับสนุนบริการสุขภาพ (กลุ่มตรวจสอบภายใน), คู่มือการตรวจสอบภายในด้านเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ ปีงบประมาณ พ.ศ. 2558 – 2560, 2558.

กรมบัญชีกลาง, “หนังสือ ที่ กค 0409.2/ว 614”, 23 ธันวาคม 2563.

กรมบัญชีกลาง, “หนังสือ ที่ กค 0416.2/ว 292”, 24 กันยายน 2546.

กรมบัญชีกลาง, “หนังสือ ที่ กค 0416.3/ว 380”, 8 ธันวาคม 2546.

กรมบัญชีกลาง (สำนักกำกับและพัฒนาการตรวจสอบภาครัฐ), การตรวจสอบด้านเทคโนโลยีสารสนเทศ, สืบค้นจาก www.cgd.go.th เมื่อ วันที่ 2 ธันวาคม 2565.

กระทรวงศึกษาธิการ (กลุ่มตรวจสอบภายในระดับกระทรวง), แนวทางตรวจสอบความมั่นคงปลอดภัยด้านสารสนเทศประจำปีงบประมาณ พ.ศ. 2556, 2555.

กระทรวงเกษตรและสหกรณ์ (กลุ่มตรวจสอบภายใน), คู่มือการตรวจสอบภายใน กรมพัฒนาที่ดิน, 2560.

กระทรวงศึกษาธิการ (กลุ่มตรวจสอบภายในระดับกระทรวง), คู่มือการจัดทำแนวทางการตรวจสอบแกระดาษทำการ, 2558

“พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549”, ราชกิจจานุเบกษา 124 (10 ม.ค. 2550) : 1 - 4

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550”, ราชกิจจานุเบกษา 124 (18 มิ.ย. 2550) : 4 – 13.

ธนาคารอาคารสงเคราะห์ (ฝ่ายตรวจสอบระบบเทคโนโลยีสารสนเทศ), แนวทางการตรวจสอบระบบเทคโนโลยีสารสนเทศ, 2560.

คณะผู้จัดทำ

นางสาวปภาดา	ฟูรังษีโรจน์	ผู้อำนวยการกลุ่มตรวจสอบภายใน	ที่ปรึกษา
นางสาวลภัสวีณ์	สังข์ประเสริฐ	นักวิชาการตรวจสอบภายในชำนาญการพิเศษ	
นายจักรพล	วงค์มูล	เจ้าหน้าที่คอมพิวเตอร์	
นางสาวพิมพ์ชนก	แก่นลออ	เจ้าหน้าที่ตรวจสอบภายใน	