องค์การตลาดเพื่อเกษตรกร
WWW.ORTORKOR.COM

การตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ องค์การตลาดเพื่อเกษตรกร

พ.ศ. 2569 - 2570

องค์การตลาดเพื่อเกษตรกร
กองเทคโนโลยีและสารสนเทศ

คำนำ

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหนวยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ กำหนดให้หน่วยงานของรัฐจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยผู้ตรวจสอบภายในภาครัฐ (Internal Audit) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยของสารสนเทศของหน่วยงาน ประกอบกับมาตรฐานการตรวจสอบภายในและแนวทางการประกันคุณภาพงานตรวจสอบภายในภาครัฐ กำหนดมาตรฐานด้านคุณสมบัติ รหัส ๑๒๑๐.A ๓ ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านเทคโนโลยีสารสนเทศ ได้แก่ การควบคุมที่สนับสนุนการบริหารจัดการและการกำกับดูแล โดยจัดให้มีระบบควบคุมในส่วนโครงสร้างพื้นฐานด้านสารสนเทศ เช่น ระบบงานข้อมูล ระบบเครือข่าย และระบบบุคลากร ซึ่งประกอบด้วย การควบคุมทั่วไปและแบบเฉพาะทาง รวมถึงเทคนิควิธีการตรวจสอบด้านเทคโนโลยีสารสนเทศและประเด็นที่ใช้พิจารณา : การวางแผนการตรวจสอบ การเสนอ และการอนุมัติแผนการตรวจสอบ กำหนดให้การวางแผนการตรวจสอบครอบคลุมประเภทงานให้ความเชื่อมั่น ควรครอบคลุมการตรวจสอบด้านสารสนเทศ

ดังนั้น เพื่อให้การตรวจสอบภายในเป็นไปตามมาตรฐานการตรวจสอบภายใน และตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศ จึงได้จัดทำคู่มือการตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ผู้ตรวจสอบภายในขององค์การตลาดเพื่อเกษตรกร นำไปใช้ในการปฏิบัติงาน และรายงานผลตรวจสอบเป็นไปในแนวทางเดียวกันต่อไป

ผู้จัดทำ

กองเทคโนโลยีและสารสนเทศ

สารบัญ

คำนำ

- แผนการปฏิบัติงานตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศ ๑
- วัตถุประสงค์ของการตรวจสอบ ๒
- ขอบเขตและวิธีการตรวจสอบ ๒
- ขั้นตอนการดำเนินงาน ๒
- ข้อมูลพื้นฐานเพื่อประกอบการตรวจสอบ ๒
- กรอบประเด็นการตรวจสอบ ๖
- นิยามศัพท์ ๖
- กระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ๗
- แผนผังขั้นตอนการตรวจสอบ ๘
- แนวทางการคัดเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินความมั่นคงปลอดภัยสารสนเทศที่มีความเป็นกลางและเป็นธรรม ๑๐
- แนวทางการปฏิบัติงานการตรวจสอบระบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๑๓
- ผู้มีส่วนได้ส่วนเสียหลักที่สำคัญที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ๒๗
- แนวทางถ่ายทอดแนวปฏิบัติการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ๒๙
- การกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (Outcome) ๓๒

ภาคผนวก

- กระดาษทำการตรวจสอบแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ IT.A1.1 ๓๔
- กระดาษทำการตรวจสอบข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ IT.A1.2 ๓๕
- กระดาษทำการตรวจสอบแนวนโยบายการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่กระทบ พ.ร.บ.คอมพิวเตอร์ IT.A2 ๓๖
- กระดาษทำการตรวจสอบการควบคุมการเข้าถึงและควบคุมใช้งาน IT.A3.1 ๔๐
- กระดาษทำการตรวจสอบการใช้งานตามภารกิจ IT.A3.2 ๔๑
- กระดาษทำการตรวจสอบการบริหารจัดการการเข้าถึงผู้ใช้งาน IT.A3.3 ๔๒
- กระดาษทำการตรวจสอบการกำหนดหน้าที่ความรับผิดชอบ IT.A3.4 ๔๓
- กระดาษทำการตรวจสอบการเข้าถึงระบบเครือข่าย IT.A3.5 ๔๔
- กระดาษทำการตรวจสอบการเข้าถึงระบบปฏิบัติการ IT.A3.6 ๔๖
- กระดาษทำการตรวจสอบการเข้าถึงโปรแกรมประยุกต์ หรือ Application และสารสนเทศ IT.A3.7 ๔๗
- กระดาษทำการตรวจสอบการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน IT.A3.8 ๔๘
- กระดาษทำการสอบทานการจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ IT.A3.9 ๔๙

แผนการปฏิบัติงานตรวจสอบ
ระบบความมั่นคงปลอดภัยด้านสารสนเทศ

ปัจจุบันเทคโนโลยีสารสนเทศเพื่อการสื่อสาร มีความก้าวหน้าอย่างรวดเร็ว การทำธุรกรรมในระบบอิเล็กทรอนิกส์ขยายตัวเพิ่มมากขึ้น หน่วยงานภาครัฐจึงได้รับการสนับสนุนให้มีการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว ซึ่งจะเป็นการเพิ่มประสิทธิภาพและประสิทธิผลในการให้บริการ และเพื่อให้หน่วยงานภาครัฐสามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภายใต้มาตรฐานเดียวกัน และเพื่อเป็นการสร้างความเชื่อมั่นต่อประชาชน จึงได้มีการตราพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ ขึ้นตามลำดับ แต่อย่างไรก็ตาม สิ่งที่พัฒนาพร้อมกับความก้าวหน้าทางด้านเทคโนโลยี คือ ปัญหาด้านความปลอดภัยของระบบสารสนเทศที่มีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ และมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทั้งในส่วนของผู้ประกอบการ องค์กร ภาครัฐ และภาคเอกชนที่มีการดำเนินงานในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ทำให้หน่วยงานเหล่านั้นขาดความเชื่อมั่นต่อการทำธุรกิจในทุกรูปแบบ และเพื่อเป็นการป้องกันและแก้ไขปัญหาดังกล่าว จึงได้มีการกำหนดกฎหมายและประกาศเพิ่มเติม ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ ตามประกาศคณะกรรมการธุรกรรมฯ ในข้อ ๑๓ (๒) กำหนดให้หน่วยงานของรัฐจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัย (External Auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับ ความเสี่ยง และระดับความมั่นคงปลอดภัยของสารสนเทศขององค์การตลาดเพื่อเกษตรกรกับมาตรฐานการตรวจสอบภายใน และแนวทางการประกันคุณภาพงานตรวจสอบภายในภาครัฐ กำหนดมาตรฐานด้านคุณสมบัติรหัส ๑๒๑๐.A๓ ว่าผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านเทคโนโลยีสารสนเทศ ซึ่งได้แก่ การควบคุมที่สนับสนุนการบริหารจัดการและการกำกับดูแล โดยจัดให้มีระบบการควบคุมในส่วนโครงสร้างพื้นฐานด้านสารสนเทศ เช่น ระบบงานข้อมูล ระบบเครือข่าย และบุคลากร ซึ่งประกอบด้วย การควบคุมทั่วไป (General Controls) และแบบเฉพาะทาง (Technical Controls) รวมถึงเทคนิควิธีการตรวจสอบด้านเทคโนโลยีสารสนเทศ และประเด็นที่ใช้พิจารณา : การวางแผนตรวจสอบ การเสนอ และอนุมัติแผนการตรวจสอบ กำหนดให้ การวางแผนการตรวจสอบครอบคลุมประเภทงานให้ความเชื่อมั่นควรครอบคลุมการตรวจสอบด้านสารสนเทศ ด้วย

วัตถุประสงค์การตรวจสอบ

๑. เพื่อให้มั่นใจว่า หน่วยงานจัดให้มีการควบคุมด้านการรักษาความปลอดภัยระบบสารสนเทศตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ

๒. เพื่อให้มั่นใจว่า หน่วยงานปฏิบัติงานด้านการรักษาความปลอดภัยระบบสารสนเทศตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ

๓. เพื่อให้ทราบปัญหา และอุปสรรคในการปฏิบัติงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ และประกาศคณะกรรมการธุรกรรมทางอีเล็กทรอนิกส์ฯ และให้ข้อเสนอแนะเพื่อการพัฒนางาน

ขอบเขตและวิธีการตรวจสอบ

๑. ดำเนินการสอบทานเอกสารหลักฐานที่เกี่ยวข้องกับการจัดให้มีการควบคุมและการปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ ที่หน่วยงานใช้อยู่ในปัจจุบัน

๒. ดำเนินการสุ่มสอบทานการปฏิบัติตามนโยบายและข้อปฏิบัติของหน่วยงาน

๓. สังเกตการปฏิบัติงานจริงตามระบบควบคุมที่กำหนดตามนโยบายและข้อปฏิบัติ

๔. สอบถามและสัมภาษณ์ ผู้บริหารและผู้ปฏิบัติงาน

ขั้นตอนการดำเนินงาน

๑. ศึกษาข้อมูลพื้นฐานประกอบการตรวจสอบ แนวทางการปฏิบัติงานตรวจสอบ และกระดาษทำการ

๒. ดำเนินการตรวจสอบโดย

๒.๑ แจ้งหน่วยรับตรวจ (หน่วยงานที่ดูแลระบบสารสนเทศขององค์กร) ถึงวันที่จะดำเนินการเปิดตรวจ

๒.๒ ประชุมเปิดตรวจเพื่อชี้แจงวัตถุประสงค์ ขอบเขต แนวทางและวิธีการตรวจสอบ พร้อมทั้งขอความร่วมมือในการให้ข้อมูล

๒.๓ ดำเนินการตรวจสอบตามแนวทางการปฏิบัติงานตรวจสอบ และบันทึกข้อมูลการตรวจสอบในกระดาษทำการ

๒.๔ เมื่อดำเนินการตรวจสอบแล้วเสร็จ ให้สรุปผลจากกระดาษทำการเก็บข้อมูลลงในกระดาษทำการสรุปผล

๒.๕ ประชุมปิดตรวจ เพื่อสรุปผลการตรวจสอบ ทำความเข้าใจ ชี้แจง และขอความเห็นเพิ่มเติมในบางประเด็นที่ยังเป็นที่สงสัย

๓. ร่างรายงานผลการตรวจสอบ พร้อมทั้งแจ้งให้หน่วยรับตรวจทราบผลเพื่อพิจารณาให้ความเห็นแล้วจัดทำรายงานผลการตรวจสอบพร้อมแนบความเห็นของหน่วยรับตรวจ เสนอผู้บริหารเพื่อพิจารณาสั่งการ

ข้อมูลพื้นฐานเพื่อประกอบการตรวจสอบ

๑. การตรวจสอบด้านสารสนเทศ ตามมาตรฐานการตรวจสอบภายในของกรมบัญชีกลางที่กำหนดในมาตรฐานการตรวจสอบภายในรหัส ๑๒๑๐.A๓ กำหนดให้ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านสารสนเทศ

๒. โครงสร้างพื้นฐานด้านสารสนเทศ ประกอบด้วย

๒.๑ อุปกรณ์ : Hardware

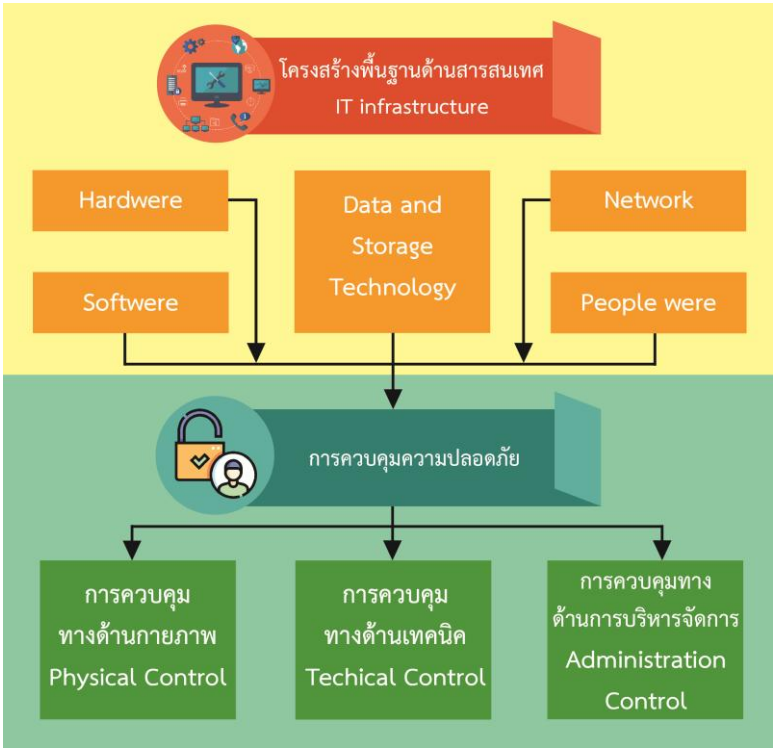
๒.๒ โปรแกรม : Software

๒.๓ ฐานข้อมูล : Data & Storage Technology

๒.๔ เครือข่าย : Networks

๒.๕ บุคลากร : People ware

ผังแสดงความเชื่อมโยงโครงสร้างพื้นฐานด้านสารสนเทศและการควบคุมความปลอดภัย



๓. การควบคุมความปลอดภัย แบ่งเป็น ๓ ด้าน คือ

๓.๑ มุมมองทางด้านกายภาพ (Physical Control)

๓.๒ มุมมองทางด้านเทคนิค (Technical Control)

๓.๓ มุมมองทางด้านการบริหารจัดการ (Administrative Control)

การจำแนกงานตรวจสอบตามมุมมองการควบคุม จากมุมมองทางด้านการควบคุม ทำให้งานตรวจสอบทางด้าน IT แบ่งเป็น ๓ ด้าน ได้แก่

๓.๑ ด้านกายภาพ

การตรวจสอบด้านกายภาพ (Physical Control) ได้แก่ ระบบควบคุมการเข้า-ออกห้องเซิฟเวอร์, Hardware ระบบ Backup/Restore และ ระบบไฟสำรอง เช่น มี UPS เพียงพอหรือไม่ และอุปกรณ์เฝ้าระวัง เช่น กล้องวงจรปด (CCTV) เป็นต้น

๓.๒ ด้านเทคนิค (Technical Control)

๑) การตรวจสอบระบบปฏิบัติการ (NOS Audit) เช่น การตรวจสอบระบบ Server ที่ใช้ MS Windows เช่น Windows NT, Window ๒๐๐๐ Server ตลอดจน Workstation ที่ใช้ Windows XP เป็นต้น การตรวจสอบควรจะครอบคลุมถึงระบบปฏิบัติการอื่นด้วย เช่น การตรวจสอบระบบปฏิบัติการ Unix เช่น Sun Solaris, HP/UX, IBM AIX และ ระบบปฏิบัติการ Linux ที่ได้รับความนิยมเพิ่มขึ้นเรื่อยๆ

๒) การตรวจสอบอุปกรณ์เครือข่าย (Network Devices Audit) เช่น การตรวจสอบRouter, การตรวจสอบ Switching และ การตรวจสอบ Remote Access Server ตลอดจน การตรวจสอบโครงสร้างของเครือข่าย (Network Infrastructure Audit) และ ประสิทธิภาพของเครือข่าย (Network Performance Audit) โดยใช้โปรแกรมตรวจสอบประเภท Packet Sniffer หรือ RMON Probe เป็นต้น

๓) การตรวจสอบอุปกรณ์รักษาความปลอดภัย (Security Devices Audit) เช่น การตรวจสอบ Firewall, การตรวจสอบ Intrusion Detection System (IDS), การตรวจสอบ Intrusion Prevention System (IPS), การตรวจสอบโปรแกรม Enterprise Anti-Virus, การตรวจสอบ VPN Server เป็นต้น การตรวจสอบอุปกรณ์รักษาความปลอดภัยนั้นเป็นสิ่งที่มีความจำเป็นอย่างสูง เพราะถ้าอุปกรณ์รักษาความปลอดภัยมีปัญหาเสียเอง หรือโดน Hacker เจาะเข้ามา compromised ก็จะทำให้เกิดปัญหากับความปลอดภัยของระบบโดยรวม ผู้ตรวจสอบควรเป็นผู้ชำนาญงานด้านการใช้งาน Firewall หรือ IDS/IPS มาก่อนด้วยจะช่วยได้มาก

๔) การตรวจสอบโปรแกรมฐานข้อมูล (RDBMS Audit) เช่น การตรวจสอบ Oracle, IBM DB๒, Microsoft SQL Server, Informix, SYBASE หรือ MySQL RDBMS การตรวจสอบโปรแกรมฐานข้อมูลควรกระทำ ควบคู่ไปกับการตรวจสอบระบบปฏิบัติการที่โปรแกรมฐานข้อมูลทำงานอยู่ เช่น Oracle ทำงานบน Unix เป็นต้น เพื่อที่จะเจาะลึกลงไปในด้านความปลอดภัยของตัวโปรแกรมฐานข้อมูลเองว่ามีช่องโหว่หรือไม่ ผู้ตรวจสอบควรเป็นผู้เชี่ยวชาญการใช้งานโปรแกรมฐานข้อมูลนั้นๆมาก่อน เพราะการตรวจสอบต้องใช้ความรู้เชิงลึกทางด้าน RDBMS ด้วย

๕) การตรวจสอบโปรแกรมประยุกต&และโปรแกรมที่ให้บริการในลักษณะ Server (Application Specific Audit) เช่น การตรวจสอบ Web Server IIS บน Microsoft Windows Platform และ การตรวจสอบ Web Server Apache บน Unix/Linux Platform ซึ่งทั้ง ๒ เป็นโปรแกรม Web Server ยอดนิยมอยู่ใน ขณะนี้ นอกจากการตรวจสอบ Web Server แล้ว IT Auditor ควรตรวจสอบ Mail Server, FTP Server, LDAP Server, RADIUS Server ตลอดจน DNS Server ซึ่งถือเป็นหัวใจหลักของระบบ หาก DNS Server มีปัญหาจะทำหัระบบไม่สามารถอ้างอิง Hostname ได้ ซึ่งจะก่อให้เกิดปัญหาใหญ่กับระบบ โดยรวม

๓.๓ ด้านการบริหารจัดการ (Administrative Control)

การตรวจสอบกระบวนการบริหารจัดการควบคุมด้านสารสนเทศ (Administrative Control) ได้แก่ การตรวจสอบ Policy, Standard, Guideline และ Procedure ที่องค์กรมีอยู่ว่าครอบคลุม และ มีการปฏิบัติตามหรือไม่ ในขั้นตอนนี้รวมถึงการตรวจสอบว่าองค์กรมีการจัด ฝึกอบรมด้านการรักษาความปลอดภัย (Security Awareness Training) หรือไม่ ซึ่งตามปกติควรจะมีเป็นประจำทุกปี การตรวจสอบการบริหารจัดการนั้นต้องพิจารณาจากโครงสร้างหน่วยงาน, การแบ่งแยกหน้าที่ต่างๆในหน่วยงาน, การจัดทำแผนสำรองฉุกเฉิน และแผนรับเหตุการณ& (Business Continuity Planning ,Disaster Recovery Planning and Incident Response Procedure) ตลอดจนการควบคุมการเปลี่ยนแปลงระบบงาน (Change Control Management)

สำหรับการตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศตามที่กำหนดนี้จะเป็นการตรวจสอบทางด้านกายภาพ และการตรวจสอบทางด้านการบริหารจัดการ

๔. การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ กำหนดในเรื่องต่อไปนี้

๔.๑ การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ได้แก่

๑) การควบคุมระบบคอมพิวเตอร์ของหน่วยงานตาม มาตรา ๑๕ เพื่อป้องกันผู้ใช้บริการที่เข้าไปกระทำความผิดตามพระราชบัญญัติคอมพิวเตอร์ เช่น นำเข้าข้อมูลอันเป็นเท็จทำให้เกิดความเสียหายต่อความมั่นคง สร้างความตื่นตระหนกต่อประชาชน หรือเผยแพร่ภาพลามกอนาจาร เป็นต้น

๒) การเก็บข้อมูลจราจร ซึ่งหมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ และอื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ตามมาตรา ๒๖ กำหนดให้หน่วยงานต้องจัดเก็บข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วันนับตั้งแต่การใช้บริการสิ้นสุดลง

การควบคุมทั้ง ๒ เรื่องที่กล่าวมาข้างต้น หน่วยงานดำเนินการ ด้วยวิธีการ ดังนี้คือ

๑) การควบคุมการเข้าสู่ระบบ (Access Control) ด้วยการกำหนด Username และ Password ให้กับผู้ใช้งาน

๒) การเก็บ Log file ข้อมูลจราจรทางคอมพิวเตอร์ของหน่วยงาน

โดยปกติ Log file เป็นไฟล์ที่ถูกสร้างขึ้นอัตโนมัติ โดยโปรแกรม (ซึ่งผู้เขียนโปรแกรมต้องเขียนเรื่องนี้ไว้) เพื่อใช้ในการเก็บข้อมูลสถานะต่างๆ โดยจะบันทึกข้อมูลทั้งหมดที่เกิดขึ้นตั้งแต่ผู้ใช้บริการเข้าสู่ระบบ (Log - In) จนกระทั่งผู้ใช้บริการออกนอกระบบ (Log - Out) หรือปดการใช้งาน และในบางโปรแกรม เช่น โปรแกรม GFMIS จะมีการเก็บ Log file ไว้เพื่อการตรวจสอบ และบางโปรแกรม Log file สามารถใช้เพื่อสั่งให้ระบบย้อนกลับไปปฏิบัติงานได้ในกรณีที่เกิดปัญหาได้

๔.๒ การควบคุมประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ กำหนดดังนี้

๑) ให้จัดทำนโยบายและข้อปฏิบัติให้ครอบคลุมเนื้อหาตามที่ประกาศกำหนด

๒) ให้ประกาศเผยแพร่นโยบายและข้อปฏิบัติ พร้อมทั้งทบทวนให้เป็นปัจจุบัน

๓) ให้ปฏิบัติตามนโยบายและข้อปฏิบัติที่กำหนดและประกาศไว้

๔) กรณีที่เกิดความเสียหายหรืออันตรายต่อองค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติ ผู้บริหารระดับสูงต้องรับผิดชอบต่อความเสียหายดังกล่าว

๕) หน่วยงานสามารถเลือกใช้ข้อปฏิบัติที่ต่างจากประกาศได้ หากมีความเหมาะสมกว่าหรือเทียบเท่า

กรอบประเด็นการตรวจสอบ

ประเด็นที่ ๑ นโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ

๑.๑ การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติ คลอบคลุมข้อกำหนดตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ

๑.๒ การเผยแพร่นโยบายและข้อปฏิบัติ ให้ผู้ที่เกี่ยวข้องทราบสามารถเข้าถึงเข้าใจและปฏิบัติตามได้

๑.๓ กำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติที่ชัดเจน

๑.๔ ทบทวนนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ประเด็นที่ ๒ การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ

ประเด็นที่ ๓ การควบคุมตามประกาศคณะกรรมการธุรกรรมฯ

๓.๑ การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

๓.๑.๑ การกำหนดการเข้าถึงสารสนเทศ

๑). การควบคุมการเข้าถึงระบบสารสนเทศ

๒). การควบคุมการเข้าถึงระบบเครือข่าย

๓). การควบคุมการเข้าถึงระบบปฏิบัติการ

๔). การควบคุมการเข้าถึงโปรแกรมประยุกต์ (Applications) และสารสนเทศ

๓.๑.๒ การกำหนดการใช้งานตามภารกิจ

๓.๑.๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน

๓.๑.๔ การกำหนดหน้าที่ความรับผิดชอบ

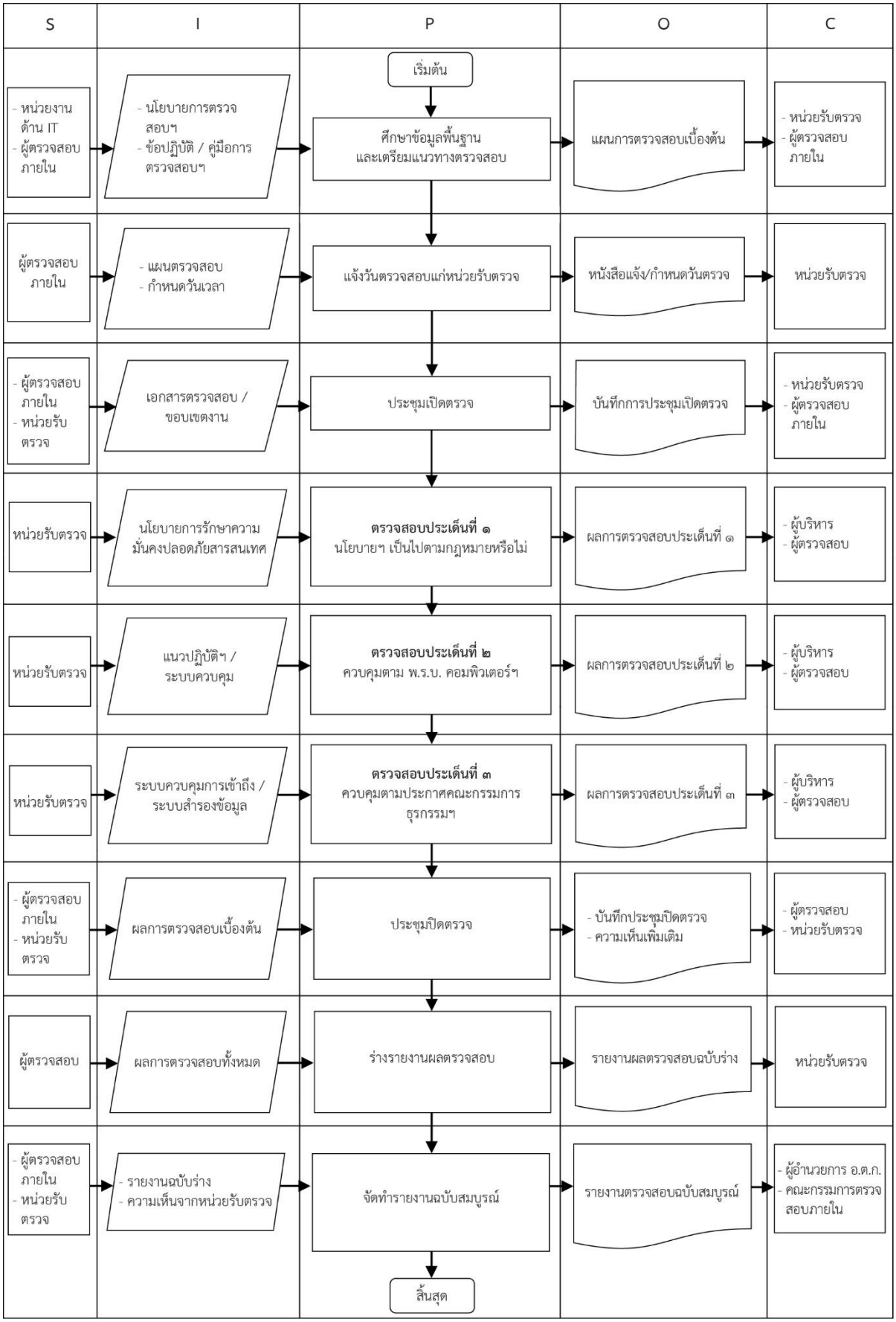
๓.๒ การจัดให้มีระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

๓.๓ การจัดให้มีการตรวจสอบและประเมินความเสี่ยง

นิยามศัพท์ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

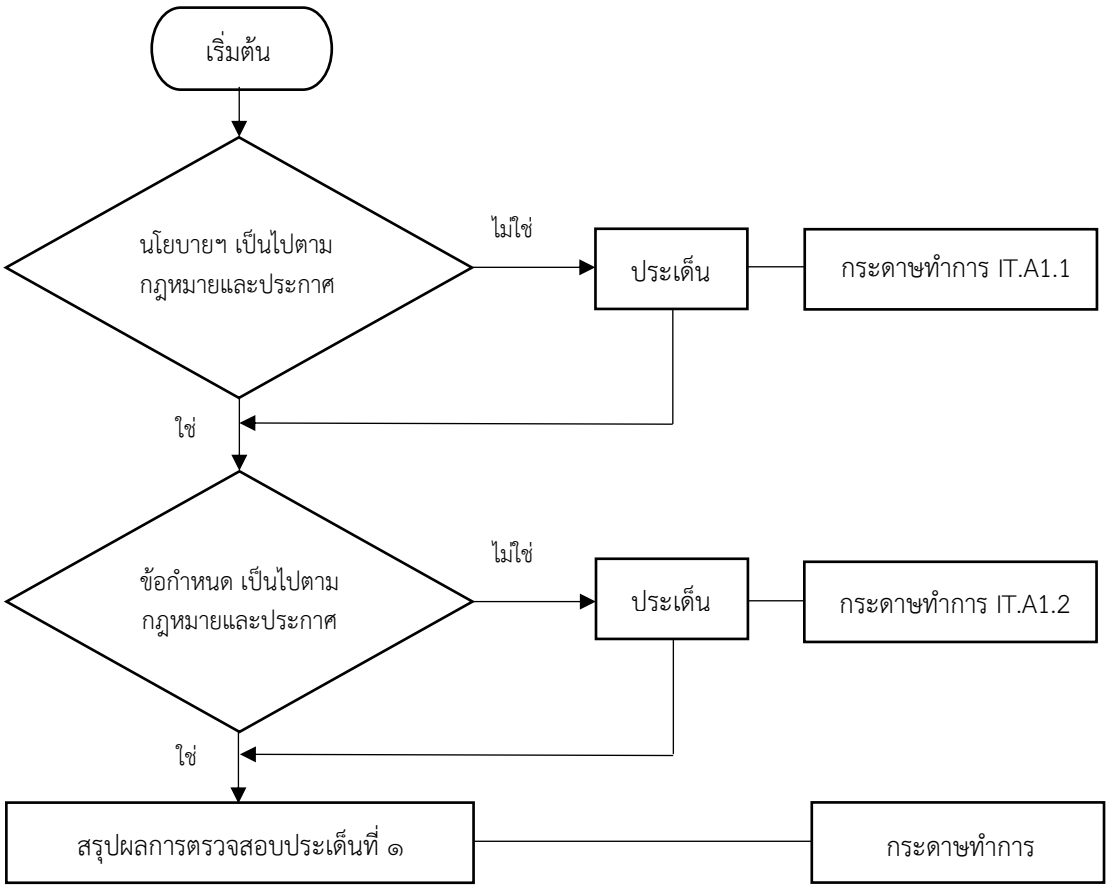
รายการ	ความหมาย
ผู้ใช้งาน	ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป
สิทธิของผู้ใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพรวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
ความมั่นคงปลอดภัยด้านสารสนเทศ	การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

กระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

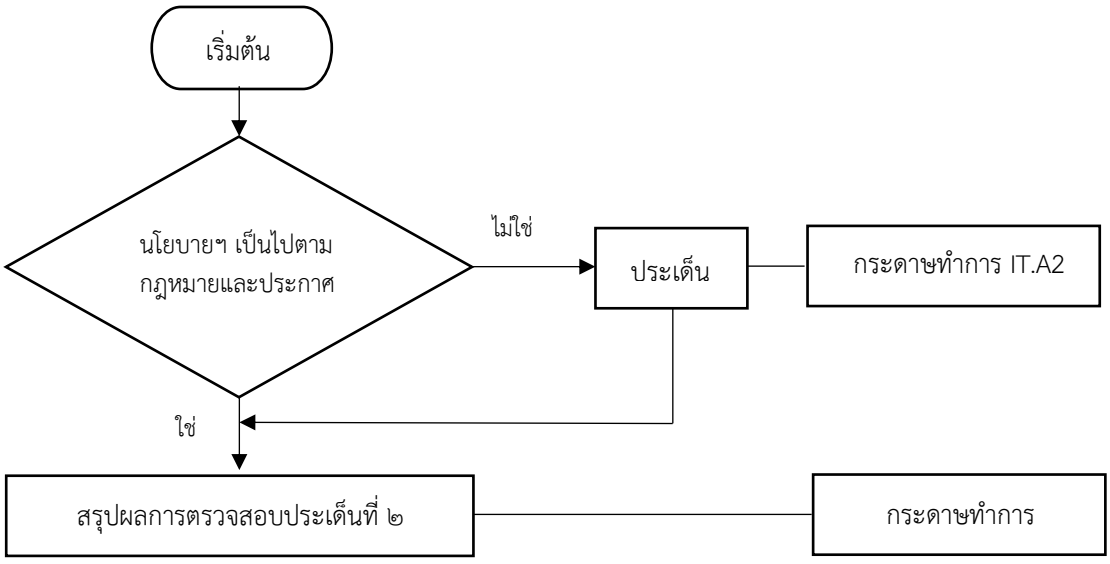


แผนผังขั้นตอนการตรวจสอบ

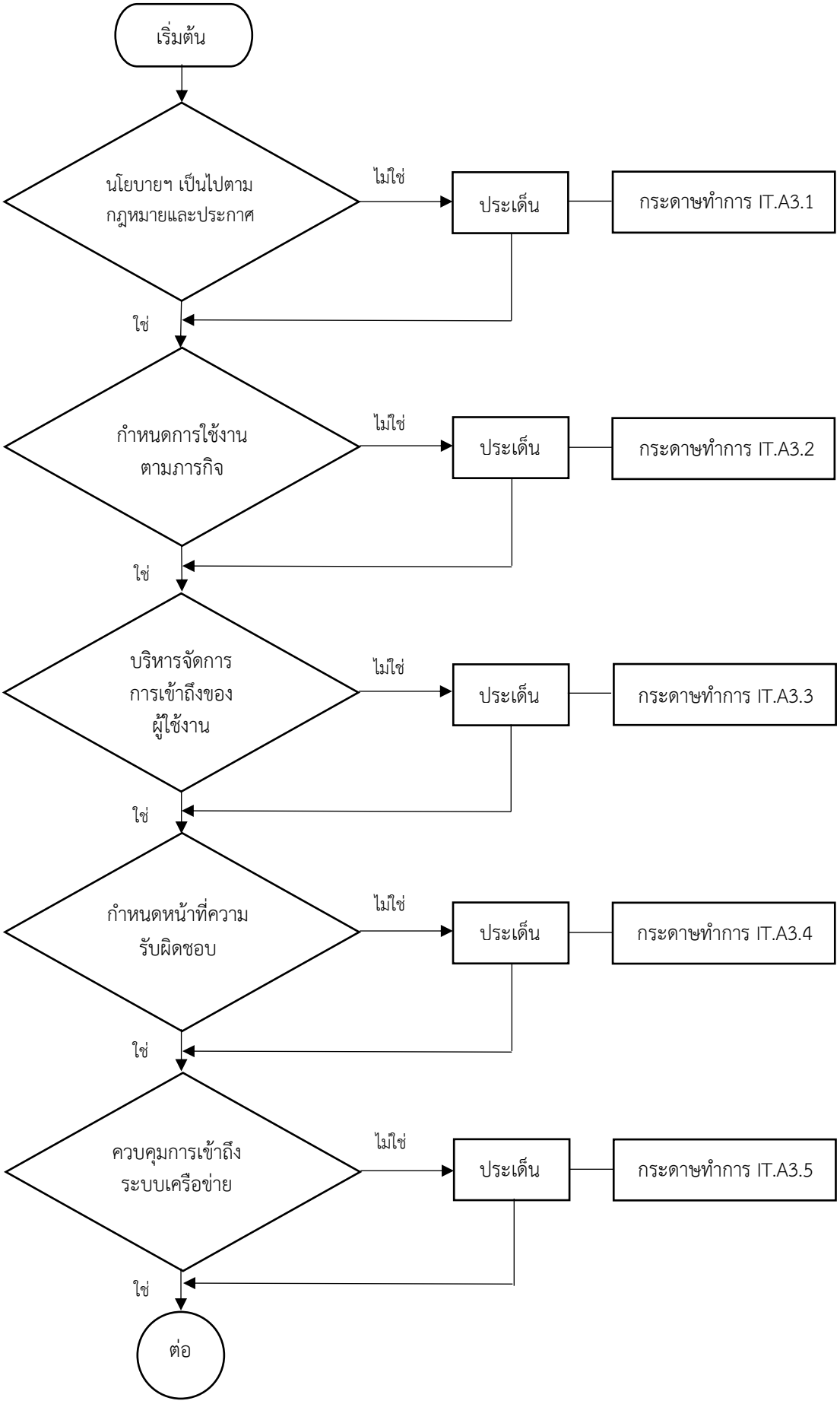
<u>ประเด็นที่ ๑ นโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศ</u>

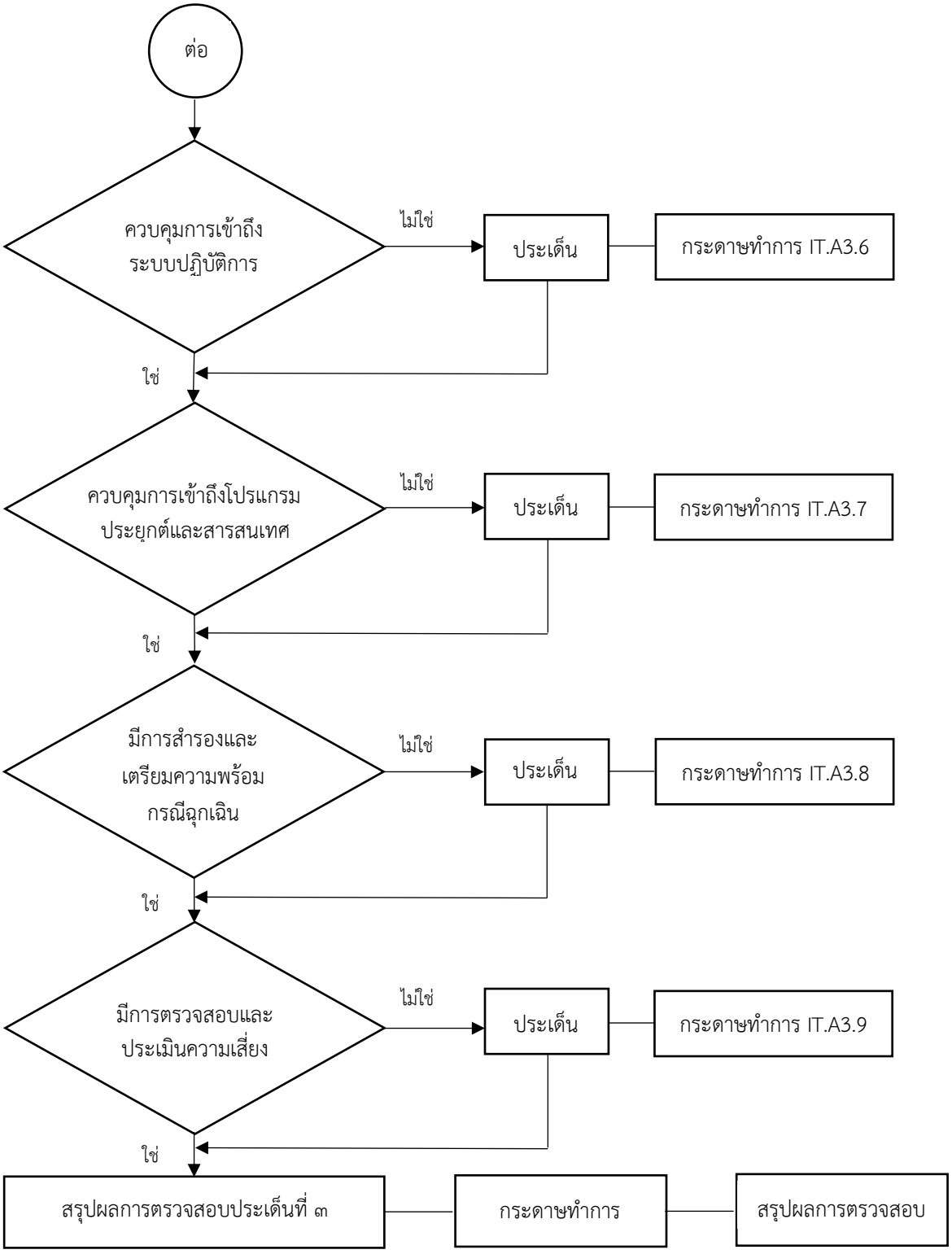


<u>ประเด็นที่ ๒ การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ</u>



ประเด็นที่ ๓ การควบคุมตามประกาศคณะกรรมการธุรกรรมฯ




ต่อ
ควบคุมการเข้าถึง
ระบบปฏิบัติการ
ไม่ใช่
ประเด็น
กระดาษทำการ IT.A3.6
ใช่
ควบคุมการเข้าถึงโปรแกรม
ประยุกต์และสารสนเทศ
ไม่ใช่
ประเด็น
กระดาษทำการ IT.A3.7
ใช่
มีการสำรองและ
เตรียมความพร้อม
กรณีฉุกเฉิน
ไม่ใช่
ประเด็น
กระดาษทำการ IT.A3.8
ใช่
มีการตรวจสอบและ
ประเมินความเสี่ยง
ไม่ใช่
ประเด็น
กระดาษทำการ IT.A3.9
ใช่
สรุปผลการตรวจสอบประเด็นที่ ๓
กระดาษทำการ
สรุปผลการตรวจสอบ

แนวทางการคัดเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินความมั่นคงปลอดภัยสารสนเทศที่มีความเป็นกลางและเป็นธรรม

เพื่อให้การตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของ อ.ต.ก. เป็นไปอย่างมีประสิทธิภาพ ได้รับความน่าเชื่อถือ และก่อให้เกิดประโยชน์สูงสุดในการพัฒนาปรับปรุงระบบ จึงจำเป็นต้องมีแนวทางที่ชัดเจนในการคัดเลือกผู้ตรวจประเมินและกระบวนการตรวจประเมินที่รับประกันความเป็นกลางและความเป็นธรรม

๑. ความเป็นอิสระ (Independence) ผู้ตรวจประเมินต้องปราศจากความขัดแย้งทางผลประโยชน์ (Conflict of Interest) และสามารถแสดงความคิดเห็นหรือข้อเสนอแนะได้อย่างอิสระ ไม่ถูกจำกัดโดยความสัมพันธ์ส่วนตัวหรือภาระผูกพันอื่นใดกับหน่วยงานหรือบุคลากรที่ถูกตรวจสอบ

๒. ความสามารถและความเชี่ยวชาญ (Competence and Expertise) ผู้ตรวจประเมินต้องมีความรู้ ความเข้าใจ และประสบการณ์ที่เพียงพอในด้านความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการความเสี่ยง และมาตรฐานที่เกี่ยวข้อง

๓. ความโปร่งใส (Transparency) กระบวนการคัดเลือกและดำเนินการตรวจประเมินควรมีความชัดเจน สามารถตรวจสอบได้ และสื่อสารให้ผู้ที่เกี่ยวข้องทราบอย่างเหมาะสม

๔. ความเป็นธรรม (Fairness) การปฏิบัติต่อผู้ถูกตรวจสอบควรเป็นไปอย่างเท่าเทียมกัน ไม่มีการเลือกปฏิบัติ และให้โอกาสในการชี้แจงหรือแสดงข้อมูลประกอบอย่างครบถ้วน

แนวทางการคัดเลือกผู้ตรวจประเมิน

อ.ต.ก. พิจารณาผู้ตรวจประเมินได้จาก ๒ แหล่งหลัก คือ ผู้ตรวจสอบภายใน (Internal Audit) และผู้ประเมินภายนอก (External Assessor/Auditor) โดยมีแนวทางดังนี้

๑. การใช้ผู้ตรวจสอบภายใน (Internal Audit)

<u>คุณสมบัติ</u>

- ความรู้ด้าน IT Security

ผู้ตรวจสอบภายในที่ได้รับมอบหมายต้องมีความรู้ความเข้าใจเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านเทคโนโลยีสารสนเทศตามที่มาตรฐานการตรวจสอบภายในกำหนด (เช่น มาตรฐานรหัส ๑๒๑๐.A๓) และควรได้รับการอบรมหรือมีประสบการณ์ที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยสารสนเทศโดยเฉพาะ

- การพัฒนาทักษะอย่างต่อเนื่อง

ควรมีการจัดฝึกอบรม หรือส่งเสริมให้ผู้ตรวจสอบภายในได้รับการรับรองในสาขาที่เกี่ยวข้อง (เช่น CISA, ISO ๒๗๐๐๑ Lead Auditor) เพื่อให้มีความรู้ที่ทันสมัยและครอบคลุม

- ความเป็นอิสระ

• การจัดโครงสร้าง หน่วยงานตรวจสอบภายในควรรายงานตรงต่อผู้บริหารสูงสุดของ อ.ต.ก. (เช่น ผู้อำนวยการ อ.ต.ก. หรือคณะกรรมการตรวจสอบ) เพื่อให้มั่นใจในความเป็นอิสระในการปฏิบัติงาน

• การหมุนเวียนงาน (Rotation) ควรมีการหมุนเวียนผู้ตรวจสอบภายในที่รับผิดชอบงานด้าน IT Security เพื่อป้องกันการผูกขาดหรือความคุ้นเคยที่อาจส่งผลกระทบต่อความเป็นกลาง

• การแยกหน้าที่ ผู้ตรวจสอบภายในที่ดำเนินการตรวจสอบ ไม่ควรมีส่วนเกี่ยวข้องโดยตรงในการออกแบบ พัฒนา หรือดำเนินการระบบที่กำลังถูกตรวจสอบมาก่อน

<u>กระบวนการคัดเลือก</u>

- มอบหมายโดยหัวหน้าหน่วยงานตรวจสอบภายใน โดยพิจารณาจากคุณสมบัติ ความเชี่ยวชาญ และความพร้อม

- แจ้งให้หน่วยงานที่เกี่ยวข้องทราบถึงผู้ที่จะเข้ามาทำการตรวจสอบ

๒. การใช้ผู้ประเมินภายนอก (External Assessor/Auditor)

<u>คุณสมบัติของหน่วยงาน/บุคคลภายนอก</u>

- ความเชี่ยวชาญเฉพาะด้าน

• มีประสบการณ์และผลงานที่น่าเชื่อถือในการให้บริการประเมินความมั่นคงปลอดภัยสารสนเทศ (เช่น การประเมิน ISO ๒๗๐๐๑, การทดสอบเจาะระบบ)

• การรับรอง (Certifications) ควรมีบุคลากรที่มีใบรับรองระดับสากลที่เกี่ยวข้อง (เช่น ISO 27001 Lead Auditor, CISSP, CISA, CEH)

• ความเป็นกลางและไม่มีส่วนได้ส่วนเสีย

ตรวจสอบความขัดแย้งทางผลประโยชน์ ผู้เสนอราคาหรือหน่วยงานภายนอกต้องยืนยันว่าไม่มีความสัมพันธ์ทางธุรกิจ หรือส่วนได้ส่วนเสียอื่นใดกับ อ.ต.ก. ที่อาจส่งผลกระทบต่อความเป็นกลางของการประเมิน

อ้างอิงและผลงาน ขอ Reference หรือ Case Study จากหน่วยงานอื่นที่เคยใช้บริการ เพื่อประกอบการพิจารณาถึงความน่าเชื่อถือและความเป็นกลาง

ชื่อเสียงและประสบการณ์: พิจารณาจากชื่อเสียงของบริษัท/บุคลากรที่ผ่านมาในการให้บริการที่คล้ายคลึงกัน

<u>กระบวนการคัดเลือก (จัดซื้อจัดจ้าง)</u>

- กำหนดขอบเขตและ TOR ที่ชัดเจน

ระบุคุณสมบัติ ประสบการณ์ และใบรับรองที่ต้องการอย่างละเอียดในเอกสารขอบเขตงาน (Terms of Reference - TOR)

- ประกวดราคา/คัดเลือก

ดำเนินการตามระเบียบการจัดซื้อจัดจ้างของ อ.ต.ก. โดยมีการพิจารณาจาก:

- ข้อเสนอทางเทคนิค (Technical Proposal)

เน้นความเข้าใจในงาน, แผนการดำเนินงาน, ระเบียบวิธี (Methodology), คุณสมบัติของทีมงาน

- ข้อเสนอด้านราคา (Commercial Proposal)

ต้องสมเหตุสมผลและคุ้มค่า

- คณะกรรมการพิจารณา

ควรประกอบด้วยบุคลากรจากหลายส่วนงาน (เช่น IT, กฎหมาย, จัดซื้อ, บริหาร) เพื่อให้การพิจารณามีมุมมองที่หลากหลายและโปร่งใส

- การเซ็นสัญญา

ระบุเงื่อนไขเรื่องความเป็นกลาง, การรักษาความลับ, และการรายงานผลให้ชัดเจนในสัญญา

แนวทางการดำเนินการตรวจประเมินที่มีความเป็นกลางและเป็นธรรม

๑. การวางแผนการตรวจสอบ (Planning Phase)

- กำหนดขอบเขตและวัตถุประสงค์ที่ชัดเจน

ผู้ตรวจประเมินและหน่วยงานที่ถูกตรวจสอบควรตกลงร่วมกันในขอบเขตการตรวจสอบ, วัตถุประสงค์, และระยะเวลาที่แน่นอน เพื่อให้ทั้งสองฝ่ายมีความเข้าใจตรงกัน

- แจ้งแผนการตรวจสอบล่วงหน้า

ควรแจ้งกำหนดการ, รายชื่อผู้ตรวจสอบ, และเอกสารที่ต้องการล่วงหน้า เพื่อให้หน่วยงานที่ถูกตรวจสอบมีเวลาเตรียมตัว

- ประชุมเปิด (Opening Meeting)

จัดประชุมร่วมกันระหว่างผู้ตรวจประเมินและผู้บริหารของหน่วยงานที่ถูกตรวจสอบ เพื่อชี้แจงวัตถุประสงค์ ขอบเขต แผนการทำงาน และตอบข้อซักถาม

๒. การดำเนินการตรวจสอบ (Execution Phase)

- เก็บข้อมูลด้วยหลายวิธี

ใช้หลากหลายวิธีในการเก็บข้อมูล เช่น การสัมภาษณ์บุคลากร, การตรวจสอบเอกสาร, การสังเกตการณ์กระบวนการทำงาน, การทดสอบระบบ (ถ้ามีการตกลงกัน)

- บันทึกข้อมูลและหลักฐาน

ผู้ตรวจประเมินต้องบันทึกข้อมูลและหลักฐานที่พบอย่างเป็นระบบและสามารถอ้างอิงได้ เพื่อสนับสนุนข้อค้นพบ

- เปิดโอกาสให้ชี้แจง

หากพบข้อบกพร่องหรือประเด็นที่น่าสงสัย ผู้ตรวจประเมินควรเปิดโอกาสให้บุคลากรที่เกี่ยวข้องชี้แจงให้ข้อมูลเพิ่มเติม, หรือแสดงหลักฐานโต้แย้งได้อย่างเต็มที่

- รักษาความเป็นส่วนตัวและข้อมูลที่เป็นความลับ: ผู้ตรวจประเมินต้องรักษาความลับของข้อมูลที่ได้รับ และไม่นำข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับไปเปิดเผยโดยไม่ได้รับอนุญาต

๓. การรายงานผล (Reporting Phase)

- ความเป็นจริงและหลักฐาน

รายงานผลการตรวจสอบต้องอยู่บนพื้นฐานของข้อเท็จจริงและหลักฐานที่รวบรวมได้ ไม่ใช้ความรู้สึกส่วนตัว

- ความชัดเจนและกระชับ

รายงานควรเขียนให้เข้าใจง่าย ชัดเจน และตรงประเด็น โดยเน้นข้อค้นพบที่สำคัญ, ความเสี่ยงที่เกี่ยวข้อง, และข้อเสนอแนะที่ปฏิบัติได้จริง

- ให้โอกาสทบทวนและโต้แย้ง (Management Response)

• ก่อนออกรายงานฉบับสมบูรณ์ ควรให้หน่วยงานที่ถูกตรวจสอบมีโอกาสทบทวนร่างรายงานและให้ข้อคิดเห็น หรือชี้แจงข้อเท็จจริงที่แตกต่างไปจากที่ระบุในรายงาน

• ในรายงานฉบับสมบูรณ์ ควรมีส่วนที่ให้ผู้บริหารของหน่วยงานที่ถูกตรวจสอบระบุแผนการตอบสนองต่อข้อเสนอแนะ (Management Response) เช่น การยอมรับ, การวางแผนปรับปรุง, หรือการให้เหตุผลที่ไม่เห็นด้วย (พร้อมหลักฐานประกอบ)

- ประชุมปิด (Closing Meeting)

จัดประชุมสรุปผลการตรวจสอบกับผู้บริหารของหน่วยงานที่ถูกตรวจสอบ เพื่อนำเสนอข้อค้นพบและข้อเสนอแนะ และตอบข้อซักถามต่างๆ

๔. การติดตามผล (Follow-up Phase)

- กำหนดแผนการปรับปรุง

อ.ต.ก. และหน่วยงานที่ถูกตรวจสอบควรมีการกำหนดแผนการปรับปรุงแก้ไขที่ชัดเจน โดยมีผู้รับผิดชอบและกรอบเวลาที่แน่นอน

- ติดตามความคืบหน้า

ผู้ตรวจประเมิน (หรือหน่วยงานที่รับผิดชอบ) ควรมีการติดตามความคืบหน้าของการดำเนินการตามแผนปรับปรุง เพื่อให้มั่นใจว่ามีการแก้ไขและพัฒนาอย่างต่อเนื่อง

แนวทางการปฏิบัติงานการตรวจสอบระบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ประเด็นการตรวจสอบที่ ๑ นโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

วัตถุประสงค์
๑. เพื่อให้มั่นใจว่า หน่วยงานกำหนดนโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
๒. เพื่อทราบปัญหาอุปสรรคในการดำเนินการ

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
๑. การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ **<u>วัตถุประสงค์</u>** เพื่อให้มั่นใจว่า การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเป็นไปตามที่กำหนดในกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	๑. หน่วยงานมีการจัดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร ๒. นโยบายมีเนื้อหาครอบคลุมเรื่องต่อไปนี้ ๒.๑ การเข้าถึงหรือการควบคุมการใช้สารสนเทศ ๒.๒ จัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน ๒.๓ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ ๓. หน่วยงานประกาศนโยบายให้ผู้ที่เกี่ยวข้องทราบ ๔. หน่วยงานกำหนดผู้รับผิดชอบตามนโยบายที่ชัดเจน ๕. หน่วยงานมีการทบทวนนโยบายให้เป็นปัจจุบัน	๑. ตรวจสอบเอกสารหลักฐานว่าหน่วยงานได้กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษรหรือ ไม่ กรณีที่ไม่ได้ดำเนินการให้สอบถามสาเหตุจากผู้ที่เกี่ยวข้อง ๒. กรณีที่จัดทำให้ตรวจสอบเนื้อหาในนโยบายว่าครอบคลุมประเด็นที่กำหนดตามเกณฑ์ และมีหลักฐานเชื่อได้ว่ามีการทบทวนเป็นปัจจุบัน ๓. ตรวจสอบว่า มีการออกคำสั่งหรือมอบหมายสั่งการให้รับผิดชอบ ตามนโยบายที่กำหนดหรือไม่ ๔. ตรวจสอบ/สังเกต การประกาศนโยบายให้ผู้ที่เกี่ยวข้องทราบ ๕. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ พร้อมถ่ายเอกสารนโยบายที่จัดทำ (ถ้ามี) แนบกระดาษทำการเป็นหลักฐาน	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A1.1 **<u>หลักฐาน</u>** ๑. เอกสารนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๒. หลักฐานแสดงการประกาศเผยแพร่ ๓. คำสั่งหรือหนังสือมอบหมายสั่งการ **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศภาพรวมขององค์กร ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
๒. การจัดทำข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ **<u>วัตถุประสงค์</u>** เพื่อให้มั่นใจว่า การจัดทำข้อปฏิบัติในการรักษาความมั่นคงปลอดภัย เป็นไปตามที่กำหนดในกฎหมายและประกาศคณะกรรมการธุรกรรมฯ	๑. ข้อปฏิบัติสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัย ๒. ข้อปฏิบัติมีเนื้อหาอย่างน้อยต่อไปนี้ ๒.๑ มีข้อกำหนดการควบคุมการเข้าถึง ๒.๒ มีข้อกำหนดการใช้งานตามภารกิจ ๒.๓ มีการจัดการการเข้าถึงของผู้ใช้งาน ๒.๔ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน ๒.๕ มีการควบคุมการเข้าถึงเครือข่าย ๒.๖ มีการควบคุมการเข้าถึงระบบปฏิบัติการ ๒.๗ มีการควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ ๒.๘ จัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน ๒.๙ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ ๓. หน่วยงานประกาศข้อปฏิบัติให้ผู้ที่เกี่ยวข้องทราบ ๔. หน่วยงานกำหนดผู้รับ-ผิดชอบตามข้อปฏิบัติที่ชัดเจน ๕. หน่วยงานมีการทบทวนข้อปฏิบัติเป็นปัจจุบัน	๑. ตรวจสอบเอกสารหลักฐานว่าหน่วยงานได้กำหนดข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสอดคล้องกับนโยบายที่กำหนดทุกข้อหรือไม่ ๒. ตรวจสอบข้อปฏิบัติที่กำหนดครอบคลุมทุกประเด็นตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์และมีหลักฐานเชื่อได้ว่ามีการทบทวนเป็นปัจจุบัน ๓. ตรวจสอบว่า มีการออกคำสั่งหรือมอบหมายสั่งการให้รับผิดชอบ ตามข้อปฏิบัติที่กำหนดหรือไม่ ๔. ตรวจสอบ/สังเกตการประกาศข้อปฏิบัติฯ ให้ผู้ที่เกี่ยวข้องทราบ ๕. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ พร้อมถ่ายเอกสารข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยแนบกระดาษทำการเป็นหลักฐาน	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A1.2 **<u>หลักฐาน</u>** ๑. เอกสารนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ๒. หลักฐานแสดงการประกาศเผยแพร่ ๓. คำสั่งหรือหนังสือมอบหมายสั่งการ **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศภาพรวมขององค์กร ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ประเด็นการตรวจสอบที่ ๒ หน่วยงานดำเนินการควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ. ๒๕๕๐ และ(ฉบับที่ ๒) พ.ศ. ๒๕๖๐

วัตถุประสงค์
๑. เพื่อให้มั่นใจว่า หน่วยงานดำเนินการควบคุมความปลอดภัย ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
๒. เพื่อทราบปัญหาอุปสรรคในการดำเนินการ

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
๑. การควบคุมป้องกันมิให้ผู้ใช้งานเข้าไปกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ **<u>วัตถุประสงค์</u>** เพื่อให้มั่นใจว่าหน่วยงานได้ดำเนินการเพื่อเป็นการป้องกันมิให้ผู้ใช้งานเข้าไปกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงาน	หน่วยงานได้มีการประกาศเผยแพร่การกระทำความผิดผ่านระบบคอมพิวเตอร์ของหน่วยงาน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ให้กับผู้ใช้งานทราบ	๑. ตรวจสอบเอกสารหลักฐานว่ามีการประกาศเผยแพร่ข้อมูลเกี่ยวกับการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ฯ ให้กับผู้ใช้งานทราบ ๒. สอบถามสัมภาษณ์ผู้บริหาร และผู้ปฏิบัติงานที่เกี่ยวข้อง ๓. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A2 **<u>หลักฐาน</u>** เอกสารหลักฐานแสดงการประกาศเผยแพร่ **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง
๒. การเก็บข้อมูลจราจรทางคอมพิวเตอร์ **<u>วัตถุประสงค์</u>** เพื่อให้มั่นใจว่าหน่วยงานมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ	หน่วยงานที่รับผิดชอบดำเนินการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้จำนวนไม่น้อยกว่า ๙๐ วัน	๑. สอบถามสัมภาษณ์ผู้บริหาร และผู้ปฏิบัติงานที่เกี่ยวข้องถึงกระบวนการและหลักฐานที่แสดงว่ามีการจัดเก็บ ๒. ตรวจสอบหลักฐานให้มั่นใจว่ามีการจัดเก็บครบตามวันเวลาที่กำหนดจริง ๓. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A2 **<u>หลักฐาน</u>** เอกสารหลักฐานแสดงจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ประเด็นการตรวจสอบที่ ๓ หน่วยงานดำเนินการควบคุมตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

วัตถุประสงค์

๑. เพื่อให้มั่นใจว่าดำเนินการควบคุมตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน-วยงานของรัฐ (ฉบับที่ ๑) พ.ศ. ๒๕๕๓ และ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

๒. เพื่อทราบปัญหาอุปสรรคในการดำเนินการ

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
๑. การควบคุมการเข้าถึงและการควบคุมการใช้งาน(Access Control) สารสนเทศ **<u>วัตถุประสงค์</u>** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑. มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลทางกายภาพ เช่น โดยบัตรผ่านหรือรหัสในการเข้าสู่ส่วนที่สำคัญ ล็อคประตูเมื่อไม่มีการเข้าใช้งาน มีระบบCCTV หรือยามรักษาความปลอดภัย ฯลฯ ๒. มีการกำหนดสิทธิในการเข้าถึง การอนุญาตและการมอบอำนาจ ๓. มีการกำหนดเกี่ยวกับ ๓.๑ ประเภทของข้อมูล ๓.๒ ชั้นความลับของข้อมูล ๓.๓ ระดับชั้นการเข้าถึง ๓.๔ เวลาที่เข้าถึง ๓.๕ ช่องทางที่เข้าถึง	๑. ตรวจสอบหลักฐานที่แสดงว่ามีการควบคุมการเข้าถึงข้อมูลอุปกรณ์ในการประมวลผลข้อมูลทางกายภาพของหน่วยงานหรือไม่อย่างไร ๒. สอบทานสิทธิการอนุญาต และการมอบอำนาจให้เป็นไปตามคำสั่งหรือการมอบหมายสั่งการของหัวหน้าส่วนงาน ๓. มีเอกสารแสดงการจัดประเภท และลำดับความสำคัญของข้อมูล เพื่อกำหนดการเข้าถึงและช่องทางที่เข้าถึง ๔. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A3.1 **<u>หลักฐาน</u>** เอกสารหลักฐานแสดงการควบคุม **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ๒. ศูนย์ควบคุมคอมพิวเตอร์ของหน่วยงาน ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
๒. การกำหนดการใช้งานตามภารกิจ (Business requirements for access control) **<u>วัตถุประสงค์</u>** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการใช้งานตามภารกิจเป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ	มีข้อปฏิบัติสำหรับการใช้งานสารสนเทศตามภารกิจโดยมีการควบคุมเป็น ๒ ส่วน คือ ๑. การควบคุมการเข้าถึงสารสนเทศ ๒. การปรับปรุงให้สอดคล้องกับข้อกำหนดในการปฏิบัติงานและข้อกำหนดด้านความปลอดภัย	๑. ตรวจสอบหน่วยงานได้จัดทำข้อปฏิบัติสำ หรับการใช้งานสารสนเทศตามภารกิจหรือไม่ ๒. ถ้ามีให้ตรวจสอบข้อกำหนดดังกล่าวว่าครอบคลุม การควบคุมการเข้าถึงและการควบคุมด้านความปลอดภัยหรือไม่ ๓. บันทึกข้อมูลจากการตรวจสอบลงในกระดาษทำการ	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A3.2 **<u>หลักฐาน</u>** เอกสารหลักฐานแสดงการควบคุม **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง
๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access Management) **<u>วัตถุประสงค์</u>** เพื่อให้ทราบว่าหน่วยงานบริหารจัดการการเข้าถึงของผู้ใช้งาน ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑. มีการให้ความรู้ ความเข้าใจให้แก่ผู้ใช้งานถึงภัยและผลกระทบจากการใช้งานระบบโดยไม่ระมัดระวังและรู้เท่าไม่ถึงการณ์ ๒. มีกำหนดให้ลงทะเบียนผู้ใช้งาน เพื่ออนุญาตและเพิกถอนสิทธิ ๓. มีการควบคุมและจำกัดสิทธิ โดยให้เป็นไปตามหลัก Need to know	๑. สอบทานว่าหน่วยงานได้จัดให้มีการให้ความรู้ ความเข้าใจแก่ผู้ใช้งาน เป็นประจำหรือไม่ ด้วยวิธีการใด ๒. สอบทานว่า ๒.๑ มีข้อกำหนดในการลงทะเบียนและผังขั้นตอนการปฏิบัติในการลงทะเบียน ๒.๒ มีข้อปฏิบัติหรือหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ ๒.๓ มีข้อปฏิบัติหรือหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ ๓. สอบทานเอกสารแสดงการกำหนดสิทธิใน(ตารางกำหนดสิทธิ) แต่ละระบบว่า มี User จำนวนกี่คน มีการสร้าง User ร่วมได้หรือไม่ สิทธิที่ให้ในแต่ละกลุ่ม	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A3.3 **<u>หลักฐาน</u>** เอกสารหลักฐานแสดงการควบคุม **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
		เป็นอย่างไร เหมาะสมหรือไม่ ทั้งนี้อาจดำเนินการตรวจสอบทุกระบบหรือสุ่มตรวจเฉพาะระบบสำคัญๆ โดยให้พิจารณาตามความจำเป็นและเหมาะสม	
	๔. การให้รหัสผ่านและการเพิกถอนรหัสให้กับผู้ใช้งาน มีการดำเนินการผ่านกระบวนการด้านการบริหาร	๔. สอบทานกระบวนการในการให้รหัสกับผู้ใช้งาน และเพิกถอนรหัสว่ามีการควบคุมอย่างรัดกุม และมีการดำเนินการผ่านกระบวนการบริหาร โดยควรกำหนดเงื่อนไขให้ผู้งานเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้หน่วยงานได้มีการพิจารณาถึงลำดับชั้นความลับของระบบ/ ข้อมูลในการเข้าถึงแล้ว	
	๕. มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานเป็นระยะ	๕. สอบทานว่าหน่วยงานจัดให้มีการทบทวนสิทธิของผู้ใช้งานเป็นปกติประจำ เช่น ทุก ๓ เดือน หรือทุก ๖ เดือน เป็นต้นและตรวจสอบจากเอกสารหลักฐานว่าดำเนินการทบทวนหรือไม่ ๖. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่ผู้ปฏิบัติงานเพื่อทราบปัญหา หรืออุปสรรคในการดำเนินการ ๗. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
๔. การกำหนดหน้าที่ความรับผิดชอบ (User Responsibilities) **<u>วัตถุประสงค์</u>** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมกำหนดหน้าที่ความรับผิดชอบเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตการเปิดเผย การล่วงรู้ หรือลักลอบทำสำเนาข้อมูลสารสนเทศ หรือ ลักขโมยอุปกรณ์ประมวลผลตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑. กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้รหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ๒. กำหนดข้อปฏิบัติในการป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งาน ๓. กำหนดวิธีการควบคุมข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ ๓ ด้านสารสนเทศ ๔. กำหนดการควบคุมป้องกันผู้ใช้งานนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ	๑. สอบทานกระบวนการในการกำหนดรหัสผ่านว่ามีข้อแนะนำในการกำหนดรหัสข้อกำหนดในการใช้งาน รวมถึงการเปลี่ยนรหัสหรือไม่ กรณีที่ผู้ใช้งานไม่ดำเนินการ ตามที่กำหนดดำเนินการอย่างไร ๒. สอบทานว่ามีข้อปฏิบัติในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานหรือไม่ดำเนินการสร้างความตระหนักให้ผู้ใช้งาน เอาใจใส่ต่อการป้องกันอุปกรณ์ของสำนักงานขณะที่ไม่มีผู้ใช้งานด้วยวิธีการใด ๓. หน่วยงานมีการกำหนดวิธีการควบคุมไม่ให้มีการทิ้งหรือปล่อยให้ข้อมูลสารสนเทศหรืออุปกรณ์สารสนเทศที่สำคัญไว้ในที่ที่ไม่ปลอดภัยมีการดำเนินการอย่างไร ๔. หน่วยงานได้มีการกำหนดข้อปฏิบัติและหลักเกณฑ์สำหรับการเข้าถึงข้อมูลลับและข้อมูลที่สำคัญขององค์กรหรือไม่อย่างไร ๕. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่เพื่อทราบปัญหาในการดำเนินการ ๖. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A3.4 **<u>หลักฐาน</u>** เอกสารหลักฐานแสดงการควบคุม **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
๕. การควบคุมการเข้าถึงระบบเครือข่าย (Network access control) **<u>วัตถุประสงค์</u>** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานระบบเครือข่าย ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑. ผู้ใช้งานสามารถเข้าถึงได้เฉพาะบริการที่ได้รับสิทธิให้เข้าถึงเท่านั้น	๑.๑ หน่วยงานต้องมีเอกสารหลักฐานที่แสดงว่ามีระบบสารสนเทศอะไรบ้างในหน่วยงานที่ต้องควบคุมการเข้าถึง ๑.๒ หน่วยงานต้องแสดงข้อปฏิบัติที่กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่อนุญาตให้เข้าถึงเท่านั้น ๑.๓ สำหรับหน่วยงานที่มีระบบคอมพิวเตอร์ขนาดใหญ่ที่มีการเชื่อมต่อเครื่อง terminal ให้สำหรับผู้ใช้งานหน่วยงานได้มีการควบคุมที่เข้มงวดในการเชื่อมต่อระหว่างเครื่อง Terminal ของผู้ใช้งาน กับระบบของหน่วยงานหรือไม่	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A3.5 **<u>หลักฐาน</u>** เอกสารหลักฐานแสดงการควบคุม **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง
	๒. การเข้าใช้งานจากภายนอกต้องได้รับการยืนยันบุคคลก่อนจึงจะสามารถเข้าใช้งานได้	๒. หน่วยงานต้องแสดงข้อปฏิบัติหรือกระบวนการที่จะช่วยยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้จากภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายหรือระบบสารสนเทศของหน่วยงานได้	
	๓. ต้องกำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้	๓. หน่วยงานต้องแสดงวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึงได้	

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
	๔. กำหนดการควบคุมป้องกัน Port ที่ใช้สำหรับการตรวจสอบและการปรับแต่งระบบทั้งจากการเข้าถึงภายในระบบและการเข้าถึงจากเครือข่าย	๔. หน่วยงานต้องกำหนดขั้นตอน/หลักเกณฑ์ในการควบคุมการเข้าถึง Port ที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ โดยจำแนกเป็น ๔.๑ การเข้าถึงทางกายภาพ ๔.๒การเข้าถึงทางเครือข่าย อย่างไรก็ตาม เนื่องจากการเข้าถึง Port เป็นเรื่องที่มีความเสี่ยงสูง การกำหนดขั้นตอน/หลักเกณฑ์ในการควบคุมจึงต้องไม่ระบุ Port ไว้ และต้องไม่กำหนดรายละเอียดใดๆไว้ในขั้นตอน/หลักเกณฑ์การควบคุมที่จะทำให้เข้าถึง Port ได้	
	๕. แบ่งแยกเครือข่ายสำหรับให้บริการสารสนเทศตามกลุ่มการให้บริการกลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ	๕. หน่วยงานมีการแบ่งแยกเครือข่ายสำหรับกลุ่มต่าง ๆ ดังนี้ (๑) กลุ่มของบริการสารสนเทศ (๒) กลุ่มของผู้ใช้งาน (๓) กลุ่มของระบบสารสนเทศ ทั้งนี้ผู้ตรวจสอบสามารถสอบทานได้จากเอกสาร Network diagram	
	๖. กำหนดการควบคุมการเชื่อมต่อเครือข่ายที่มาใช้ร่วมกันหรือใช้เชื่อมกันระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง	๖. ให้สอบทานว่าหน่วยงานได้มีการกำหนดขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงและการใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อกันระหว่างหน่วยงานว่าสอดคล้องหรือเป็นไปตามข้อปฏิบัติการควบคุมการเข้าถึงที่หน่วยงาน	

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
		กำหนดหรือไม่ และในกรณีที่หน่วยงานมีการ Share network โดยอาจมีการโอน file ระหว่างกัน (file transfers) ต้องควบคุมให้มั่นใจว่าไม่สามารถขยายออกไปนอกหน่วยงานได้	
	๗. กำหนดการควบคุมการจัดเส้นทางบนเครือข่าย ให้สอดคล้องกับข้อปฏิบัติในการเข้าถึงและการประยุกต์ใช้งานตามภารกิจ	๗. ให้สอบทานว่าหน่วยงานได้มีการกำหนดขั้นตอนหรือหลักเกณฑ์ในการควบคุมการจัดเส้นทางบนเครือข่ายดังนี้ ๗.๑ การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านข้อมูลหรือไหลเวียนของข้อมูลหรือสารสนเทศต้องไม่ทำให้เกิดช่องโหว่ในการควบคุมการเข้าถึงหรือใช้งานในโปรแกรมประยุกต์ ๗.๒ ข้อกำหนดต้องสอดคล้องกับข้อปฏิบัติ การควบคุมการเข้าถึง และการประยุกต์ใช้งานตามภารกิจ	
		๘. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่ผู้ปฏิบัติงานเพื่อทราบปัญหา หรืออุปสรรคในการดำเนินการ	
		๙. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) **<u>วัตถุประสงค์</u>** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานระบบปฏิบัติการ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑. มีขั้นตอนปฏิบัติเพื่อเข้าใช้งานที่มั่นคงปลอดภัย และต้องควบคุมโดยการยืนยันตัวตน	๑. หน่วยงานต้องสามารถแสดงขั้นตอนการปฏิบัติในการเข้าถึงเรื่องต่อไปนี้ ว่าต้องใช้วิธีการยืนยันตัวตนจึงจะสามารถเข้าถึงได้ ๑.๑ การควบคุมการเข้าใช้งานในที่มั่นคงปลอดภัย ๑.๒ การเข้าถึงระบบปฏิบัติ	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A3.6 **<u>หลักฐาน</u>** เอกสารหลักฐานแสดงการควบคุม **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง
	๒. กำหนดให้ผู้ใช้งานมีข้อมูลจำเพาะที่สามารถระบุตันตนของผู้ใช้งานได้	๒. สอบทานหลักฐานที่แสดงให้เห็นว่า ๒.๑ หน่วยงานได้มีการกำหนดให้ผู้ใช้งานแสดงข้อมูลจำเพาะในการยืนยันตัวตนของผู้ใช้งานได้ ๒.๒ หน่วยงานได้กำหนดขั้นตอนการยืนยันตัวตนของผู้ใช้งาน	
	๓. กำหนดระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบได้ (interactive)	๓. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบหรือทำงานอัตโนมัติได้	
	๔. มีการจำกัดหรือควบคุมการใช้งานโปรแกรมอรรถประโยชน์	๔. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการใช้งานโปรแกรมอรรถประโยชน์ได้ โดยข้อกำหนดต้องครอบคลุมการป้องกันการละเมิด และการหลีกเลี่ยงมาตรการความมั่นคงปลอดภัย	
	๕. กำหนดให้เครื่องยุติการใช้งาน หากว่างเว้นการใช้งานใดๆ ระยะเวลาหนึ่ง	๕. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการให้เครื่องยุติการใช้งานหากว่างเว้นการใช้งานใดๆ	

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
		ระยะเวลาหนึ่ง (session time-out) ๖. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศหรือโปรแกรมประยุกต์ (Application) ที่มีความสำคัญหรือมีความเสี่ยงสูง ๗. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่ผู้ปฏิบัติงานเพื่อทราบปัญหา หรืออุปสรรคในการดำเนินการ ๘. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	
๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์ และสารสนเทศ **<u>วัตถุประสงค์</u>** เพื่อให้ทราบว่าหน่วยงานมีการควบคุมการเข้าถึงและควบคุมการใช้งานโปรแกรมประยุกต์และสารสนเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑. จำกัดหรือควบคุมการเข้าถึงสารสนเทศและฟังก์ชั่นต่างๆของโปรแกรมประยุกต์หรือ Application จากผู้ใช้งานและบุคลากรฝ่ายสนับสนุน ๒. จัดให้มีการควบคุมอุปกรณ์คอมพิวเตอร์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน	๑. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการจำกัดเวลาและการควบคุมการเข้าถึงหรือใช้งานของผู้ใช้งานหรือบุคลากร โดยให้สอดคล้องกับนโยบายการควบคุมการเข้าถึงสารสนเทศ ๒. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน ๓. ให้สอบทานว่าหน่วยงานได้มีการกำหนดข้อปฏิบัติและมาตรการเพื่อป้องกัน	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A3.7 **<u>หลักฐาน</u>** เอกสารหลักฐานแสดงการควบคุม **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
		สารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ๔. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่ผู้ปฏิบัติงานเพื่อทราบปัญหา หรืออุปสรรคในการดำเนินการ ๕. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	
๘. การจัดให้มีการสำรองและเตรียมความพร้อมกรณีฉุกเฉิน **<u>วัตถุประสงค์</u>** เพื่อให้มั่นใจว่าหน่วยงานมีการจัดระบบสำรองและจัดแผนเตรียมความพร้อมกรณีฉุกเฉินตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์	๑. มีการพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมและอยู่ในสภาพพร้อมใช้ ๒. มีแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติและต่อเนื่อง ๓. กำหนดหน้าที่ความรับผิดชอบของบุคลากรที่ทำหน้าที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบ	๑.๑ ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการคัดเลือกระบบสารสนเทศ ๑.๒ ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการจัดทำระบบสำรองที่เหมาะสมและพร้อมใช้งาน ทั้งนี้ให้สอบทานขั้นตอนปฏิบัติว่าได้มีการกำหนดให้มีการกู้คืนและรายงานผลการสำรองข้อมูลด้วย ๒. ให้หน่วยงานแสดงแผนเตรียมความพร้อมกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ รวมทั้งในกรณีที่ Site หลักทำงานไม่ได้ ว่าในระยะสั้น (เร่งด่วน) ดำเนินการอย่างไรระยะยาวดำเนินการอย่างไร และควรทบทวนแผน ๓ เดือนครั้ง ๓. ให้หน่วยงานระบุบุคลากร พร้อมทั้งแสดงรายละเอียดหน้าที่ความรับผิดชอบของบุคลากรใน	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A3.8 **<u>หลักฐาน</u>** เอกสารหลักฐานแสดงการควบคุม **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ประเด็นย่อย/ วัตถุประสงค์ย่อย	เกณฑ์การตรวจสอบ	วิธีการตรวจสอบ	กระดาษทำการ แหล่งข้อมูล/
	สำรองและจัดทำแผนความพร้อมกรณีฉุกเฉิน ๔. มีการทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรองและการดำเนินการตามแผนเตรียมความพร้อมอย่างสม่ำเสมอ	เรื่องดังต่อไปนี้ ๓.๑ ระบบสารสนเทศ ๓.๒ ระบบสำรอง ๓.๓ แผนเตรียมความพร้อมกรณีฉุกเฉิน ๔. ให้หน่วยงานแสดงข้อปฏิบัติหรือหลักเกณฑ์ในการทดสอบสภาพความพร้อมใช้ในเรื่องต่อไปนี้ ๔.๑ ระบบสารสนเทศ ๔.๒ ระบบสำรอง ๔.๓ แผนเตรียมความพร้อมกรณีฉุกเฉินและควรแสดงความถี่ในการปฏิบัติในเรื่องที่กล่าวมาข้างต้นด้วย ๕. ให้สอบถามหรือสัมภาษณ์ผู้บริหารหรือเจ้าหน้าที่ผู้ปฏิบัติงานเพื่อทราบปัญหา หรืออุปสรรคในการดำเนินการ ๖. บันทึกขอมูลลงในกระดาษทำการที่เกี่ยวข้อง	
๙. การจัดให้มีการตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ **<u>วัตถุประสงค์</u>** เพื่อให้มั่นใจว่าหน่วยงานจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ	หน่วยงานจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง โดยผู้ตรวจสอบภายในหรือผู้ประเมินความเสี่ยงจากภายนอกหน่วยงาน	๑. หน่วยงานมีการกำหนดนโยบายและมาตร การให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้น ๒. มีการรายงานผลการตรวจสอบหรือประเมินความเสี่ยงจากผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกแล้วแต่กรณี ๓. บันทึกข้อมูลลงในกระดาษทำการที่เกี่ยวข้อง	**<u>เครื่องมือ</u>** กระดาษทำการ IT.A3.9 **<u>หลักฐาน</u>** เอกสารหลักฐานแสดงการควบคุม **<u>แหล่งข้อมูล</u>** ๑. หน่วยงานที่ดูแลด้านเทคโนโลยีสารสนเทศ ๒. ผู้บริหารหรือผู้ปฏิบัติงานที่เกี่ยวข้อง

ผู้มีส่วนได้ส่วนเสียหลักที่สำคัญที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๑. ผู้มีส่วนได้ส่วนเสียหลักที่สำคัญ

กลุ่ม	รายละเอียด
ผู้อำนวยการ อ.ต.ก.	ผู้มีอำนาจอนุมัติและรับผิดชอบเชิงนโยบาย
กองเทคโนโลยีและสารสนเทศ	ผู้รับผิดชอบการจัดการตรวจสอบและสนับสนุนข้อมูล
สำนักตรวจสอบภายใน	จัดทำนโยบายและมาตรฐานด้านข้อมูล
หน่วยงานเจ้าของข้อมูล	ให้ข้อมูลสนับสนุนและดำเนินการตามข้อเสนอแนะ
ผู้ใช้งานระบบ	ปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัย
หน่วยงานภายนอก	ผู้ให้คำปรึกษา/ตรวจสอบจากภายนอก

๒. บทบาทผู้มีส่วนได้ส่วนเสีย (RACI Metric)

กิจกรรมหลัก	ผู้อำนวยการ อ.ต.ก.	กองเทคโนโลยีและสารสนเทศ	สำนักตรวจสอบภายใน	หน่วยงานเจ้าของข้อมูล	ผู้ใช้งานระบบ	หน่วยงานภายนอก
จัดทำแผนการตรวจสอบ ISMS	A	R	C	I	I	C
อนุมัติแผนการตรวจสอบ	A	C	R	I	I	I
ดำเนินการตรวจสอบระบบ	I	C	R	C	I	C
จัดทำรายงานผลตรวจสอบ	I	C	R	C	I	C
ทบทวนผลการตรวจสอบ	A	R	C	C	I	I
ถ่ายทอดผลการตรวจสอบ	A	R	C	C	I	C



แนวทางถ่ายทอดแนวปฏิบัติการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

๑. วัตถุประสงค์ของการถ่ายทอดแนวทางปฏิบัติ

- สร้างความเข้าใจร่วมกันถึงความสำคัญและหลักการของการตรวจสอบความมั่นคงปลอดภัยสารสนเทศทั่วทั้งองค์กร
- กำหนดแนวทางปฏิบัติที่เป็นมาตรฐานและสอดคล้องกันในการดำเนินการตรวจสอบ รวมถึงการรายงานผล
- ส่งเสริมให้บุคลากรที่เกี่ยวข้องมีความรู้ความเข้าใจในบทบาทหน้าที่ของตนเองและสามารถนำแนวปฏิบัติไปใช้ได้อย่างมีประสิทธิภาพ
- สร้างวัฒนธรรมองค์กรที่ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยสารสนเทศและการปรับปรุงอย่างต่อเนื่อง

๒. วิเคราะห์สถานการณ์ (Context Analysis)

๒.๑ สถานการณ์ปัจจุบัน

- มีการจัดทำคู่มือการตรวจสอบสารสนเทศที่สอดคล้องกับกฎหมาย เช่น พ.ร.บ.คอมพิวเตอร์ พ.ศ. ๒๕๕๐/๒๕๖๐ และประกาศคณะกรรมการธุรกรรมฯ
- คู่มือระบุรายละเอียดแนวทางตรวจสอบตามกรอบ กายภาพ (Physical), เทคนิค (Technical), การบริหารจัดการ (Administrative) อย่างครบถ้วน
- กระบวนการตรวจสอบยังไม่ถูกถ่ายทอดไปยังทุกหน่วยงานอย่างเป็นระบบ และมักจำกัดอยู่เฉพาะฝ่ายตรวจสอบภายใน

๒.๒ ความท้าทาย

- บุคลากรนอกสายตรวจสอบขาดความเข้าใจเกี่ยวกับเกณฑ์การตรวจสอบและข้อกำหนดด้านความมั่นคงปลอดภัย
- ขาดระบบที่ทำให้การปฏิบัติตามแนวปฏิบัติการตรวจสอบกลายเป็น “เรื่องของทุกหน่วย” ไม่ใช่เพียงแค่ของผู้ตรวจสอบ

๒.๓ ความจำเป็น

- เพื่อให้การควบคุมความมั่นคงปลอดภัยสามารถประเมินได้อย่างโปร่งใสและเป็นมาตรฐานเดียวกันทั่วองค์กร
- เพื่อให้องค์กรพร้อมต่อการตรวจสอบจากหน่วยงานภายนอก และลดความเสี่ยงที่อาจนำไปสู่ความเสียหาย

๓. กลยุทธ์ถ่ายทอดแนวทางปฏิบัติ (Implementation Strategy)

๓.๑ หลักการสำคัญ

- ถ่ายโอนจาก “แนวทางของฝ่ายตรวจสอบ” ⟶ “แนวทางร่วมขององค์กร”
- ส่งเสริมให้หน่วยงานต้นทางตระหนักรู้และเตรียมพร้อมก่อนถูกตรวจสอบ

๓.๒ ขั้นตอนการถ่ายทอด

ขั้นตอน	รายละเอียด
จัดทำสรุปแนวปฏิบัติฉบับย่อ	แยกตามประเด็นตรวจสอบ เช่น Access Control, Log, Backup
จัดฝึกอบรมกลุ่มเป้าหมาย	อบรมผู้รับผิดชอบระบบ, เจ้าหน้าที่ Data Owner, Admin
ทำเอกสาร Self-Assessment	ใช้แบบฟอร์มกระดาษทำการ IT.A1 – A3 ที่อยู่ในคู่มือ

วางระบบ Pre-Audit ตรวจสอบตนเอง	ทบทวนระดับความพร้อมก่อนการตรวจจริง
ประเมินผลและสื่อสารผลการตรวจสอบ	รายงานแบบมี Dashboard เพื่อสื่อสารให้ทุกหน่วยเห็นภาพรวม

๓.๓ กลยุทธ์เสริม

- กำหนด KPI ความพร้อมก่อนตรวจสอบในระดับหน่วยงาน
- พัฒนาระบบให้แจ้งเตือนหน่วยงานก่อนถึงรอบตรวจประจำปี

๔. เครื่องมือสนับสนุน

เครื่องมือ	วัตถุประสงค์
กระดาษทำการต้นแบบ	แบบฟอร์ม IT.A1.1–A3.9 สำหรับประเด็นตรวจสอบแต่ละหมวด เช่น นโยบาย, การเข้าถึง, แผนฉุกเฉิน
Infographic ความเข้าใจเร็ว	เช่น “๑๐ ประเด็นตรวจสอบที่หน่วยงานต้องรู้”, “ความเสี่ยงทั่วไปที่พบบ่อย”
หลักสูตรอบรมสำหรับหน่วยรับตรวจ	ฝึกอบรมเจ้าหน้าที่ IT และตรวจสอบภายใน ให้เข้าใจบทบาทและเอกสารที่ใช้ในการตรวจ
Dashboard การประเมินผลการตรวจสอบ	ติดตามผลการตรวจ, เปรียบเทียบความพร้อมของแต่ละฝ่าย

๕. วิธีการสื่อสารกับกลุ่มผู้มีส่วนได้ส่วนเสียในแต่ละกลุ่ม

กลุ่มผู้มีส่วนได้ส่วนเสีย	รูปแบบ/วิธีการสื่อสาร
ผู้อำนวยการ อ.ต.ก.	การจัดการประชุม และ รายงานสรุปผู้บริหาร
กองเทคโนโลยีและสารสนเทศ	การประชุมทางเทคนิค, ระบบแจ้งเตือน, การประสานงานโดยตรง
สำนักตรวจสอบภายใน	การประชุมเปิดตรวจและประชุมปิดตรวจ, หนังสือแจ้งกำหนดวันตรวจ
หน่วยงานเจ้าของข้อมูล	การแจ้งเวียน, การประเมินตนเอง, การประชุมชี้แจง
ผู้ใช้งานระบบ	การสร้างความตระหนักรู้, การจัดอบรมเชิงปฏิบัติการ (Workshops), การแจ้งเวียนหนังสือ, ประกาศผ่าน Intranet
หน่วยงานภายนอก	กำหนดเอกสาร TOR, หนังสือราชการภายนอก, ประกาศผ่านเว็ปไซต์ขององค์กร

๖. การวัดผลและประเมินผลการถ่ายทอดแนวทางปฏิบัติ

กำหนดตัวชี้วัดความสำเร็จของการถ่ายทอด เช่น จำนวนบุคลากรที่เข้าร่วมอบรม, คะแนนความเข้าใจในเนื้อหา, การนำแนวปฏิบัติไปปรับใช้จริง, ผลลัพธ์จากการตรวจประเมินภายใน

๗. สรุปแนวทางการถ่ายทอดแนวทางปฏิบัติ

๑. จัดทำคู่มือและเอกสารประกอบที่เข้าใจง่าย สรุปเนื้อหาสำคัญจากคู่มือเป็นเอกสารที่กระชับและเข้าใจง่ายสำหรับบุคลากรทั่วไป (Non-IT) พร้อมตัวอย่างประกอบ

๒. จัดการอบรมเชิงปฏิบัติการ (Workshop) สำหรับหน่วยงานที่เกี่ยวข้องโดยตรงกับความมั่นคงปลอดภัยสารสนเทศ ควรจัดอบรมที่เน้นการลงมือปฏิบัติจริง และกรณีศึกษา เพื่อให้เข้าใจวิธีการตรวจสอบและการปฏิบัติตามเกณฑ์

๓. การสื่อสารผ่านช่องทางภายในองค์กร ใช้ Intranet, E-mail, หรือบอร์ดประชาสัมพันธ์ เพื่อเผยแพร่ข้อมูลข่าวสาร, ประกาศ, หรือข้อควรปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ

๔. แต่งตั้งผู้ประสานงานประจำหน่วยงาน (Security Champion) อาจพิจารณาแต่งตั้งผู้ประสานงานด้านความมั่นคงปลอดภัยสารสนเทศในแต่ละหน่วยงาน เพื่อเป็นจุดเชื่อมโยงในการสื่อสาร แนะนำ และช่วยเหลือบุคลากรในหน่วยงานของตน

๕. การสร้างแบบประเมินตนเอง (Self-Assessment Tool) พัฒนาแบบประเมินตนเองอย่างง่ายๆ ให้แต่ละหน่วยงานสามารถนำไปใช้ตรวจสอบความพร้อมของตนเองก่อนการตรวจสอบจริง

๖. การให้คำปรึกษาและสนับสนุน จัดให้มีช่องทางในการขอคำปรึกษาและสนับสนุนจากผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศภายในองค์กร

๗. การยกย่องและให้รางวัล สร้างแรงจูงใจโดยการยกย่องหรือให้รางวัลแก่หน่วยงานหรือบุคคลที่มีผลการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศดีเด่น

การกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (Outcome) การตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

เพื่อให้การตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของ อ.ต.ก. มีประสิทธิภาพ โปร่งใส และเป็นไปตามมาตรฐานที่กำหนด เพื่อให้ผู้บริหารได้รับข้อมูลที่ถูกต้อง ครบถ้วน และทันเวลาสำหรับใช้ในการปรับปรุงมาตรการควบคุมและลดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างต่อเนื่อง

๑. ตัวชี้วัดเชิงกระบวนการ (In-process KPIs)

เน้นการติดตามความก้าวหน้า ความรวดเร็ว และความครบถ้วนของ "กระบวนการตรวจสอบ" เพื่อให้มั่นใจว่าการปฏิบัติงานเป็นไปตามแผนที่วางไว้

ตัวชี้วัด (KPIs)	คำนิยาม	วิธีการวัดผล	หน่วยวัด	ความถี่ในการวัดผล	เป้าหมาย	ผู้กำกับดูแลกระบวนการ
๑. ความสำเร็จของการดำเนินการตรวจสอบตามแผน	ความสามารถในการเข้าตรวจสอบระบบสารสนเทศตามแผนการตรวจสอบประจำปีที่ได้รับอนุมัติ	(จำนวนระบบ/หน่วยงานที่ได้รับการตรวจสอบจริง / จำนวนระบบ/หน่วยงานตามแผน) x ๑๐๐	ร้อยละ	รายปี	ไม่น้อยกว่าร้อยละ ๙๕	ผู้อำนวยการสำนักตรวจสอบภายใน
๒. ระยะเวลาในการออกรายงานผลการตรวจสอบ	ความรวดเร็วในการจัดทำและส่งมอบรายงานฉบับสมบูรณ์ (Final Report) ให้หน่วยรับตรวจหลังเสร็จสิ้นการประเมิน	นับจำนวนวันทำการตั้งแต่การประชุมปิดตรวจ (Closing Meeting) จนถึงวันที่ออกรายงานฉบับสมบูรณ์	วันทำการ	ทุกรอบการตรวจสอบ	ไม่เกิน ๑๕ วันทำการ	ผู้อำนวยการสำนักตรวจสอบภายใน
๓. ความครอบคลุมของการประเมินความเสี่ยง	สัดส่วนของระบบสารสนเทศและโครงสร้างพื้นฐานหลักที่ได้รับการระบุและประเมินความเสี่ยงอย่างครบถ้วนตามมาตรฐาน	(จำนวนระบบหลักที่ได้รับการประเมินความเสี่ยง / จำนวนระบบสารสนเทศหลักทั้งหมด) x ๑๐๐	ร้อยละ	รายปี	ไม่น้อยกว่าร้อยละ ๙๐	คณะทำงานบริหารความเสี่ยง ฯ

๒. ตัวชี้วัดเชิงผลลัพธ์ (Outcome KPIs)

เน้นการประเมิน "ผลกระทบเชิงบวก" หรือมูลค่าเพิ่มที่องค์กรได้รับหลังจากการตรวจสอบเสร็จสิ้น เช่น ความปลอดภัยที่เพิ่มขึ้น หรือการแก้ไขปัญหาอย่างเป็นรูปธรรม

ตัวชี้วัด (KPIs)	คำนิยาม	วิธีการวัดผล	หน่วยวัด	ความถี่ในการวัดผล	เป้าหมาย	ผู้กำกับดูแลกระบวนการ
๑. อัตราการแก้ไขข้อบกพร่อง (Findings) แล้วเสร็จ	สัดส่วนของข้อค้นพบ ความเสี่ยง หรือข้อเสนอแนะจากการตรวจสอบ ที่หน่วยรับตรวจสามารถดำเนินการแก้ไขได้ตามกำหนดเวลา	(จำนวนข้อบกพร่องที่แก้ไขเสร็จตามกำหนด / จำนวนข้อบกพร่องทั้งหมดที่ถึงกำหนดเวลาแก้ไข) x ๑๐๐	ร้อยละ	รายไตรมาส	ไม่น้อยกว่าร้อยละ ๘๐	ผู้บริหารระดับสูง / คณะกรรมการตรวจสอบฯ
๒. จำนวนอุบัติการณ์ด้านความปลอดภัย (Security Incidents)	จำนวนครั้งของเหตุการณ์ละเมิดความมั่นคงปลอดภัยหรือระบบสารสนเทศหยุดชะงัก อันเกิดจากช่องโหว่ที่ตรวจสอบพบแต่ยังไม่ได้รับการแก้ไข	นับจำนวนอุบัติการณ์ระดับรุนแรง (High/Critical) ที่ส่งผลกระทบต่อระบบหลักขององค์กร	ครั้ง	รายเดือน	๐ ครั้ง (สำหรับเหตุการณ์ระดับรุนแรง)	ผู้อำนวยการ อ.ต.ก.
๓. ระดับความสอดคล้องกับนโยบาย (Compliance Rate)	ระดับความสอดคล้องของระบบและการปฏิบัติงานของบุคลากร เมื่อเทียบกับนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร	ค่าเฉลี่ยของคะแนนการประเมินตนเอง (Self-Assessment) และผลจากการสุ่มตรวจสอบทางเทคนิค	ร้อยละ	รายปี	ไม่น้อยกว่าร้อยละ ๘๕	ผู้อำนวยการสำนักตรวจสอบภายใน

ภาคผนวก

กระดาษทำการตรวจสอบแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หน่วยงาน .....

ลำดับ	แนวนโยบาย	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
		มี/ใช่	ไม่มี/ไม่ใช่		
๑	มีการจัดทำนโยบายเป็นลายลักษณ์อักษร				
๒	มีการจัดทำนโยบายเกี่ยวกับการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ครอบคลุม				
	๒.๑ การเข้าถึงระบบสารสนเทศ				
	๒.๒ การเข้าถึงระบบเครือข่าย				
	๒.๓ การเข้าถึงระบบปฏิบัติการ				
	๒.๔ การเข้าถึงโปรแกรมประยุกต์หรือ Application				
๓	มีกำหนดนโยบายเกี่ยวข้องกับการจัดทำระบบสำรองโดยมีเนื้อหาอย่างน้อย ๒ เรื่อง				
	๓.๑ การสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน				
	๓.๒ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน				
๔	มีการตรวจสอบประเมินผลไว้เป็นนโยบายข้อหนึ่งด้านสารสนเทศ				
๕	มีการประกาศเผยแพร่นโยบายให้ผู้ใช้งานทราบ โดย				
	๕.๑ ทาง website, intranet				
	๕.๒ แจ้งเวียน				
	๕.๓ อื่นๆ ระบุ.....				
๖	หน่วยงานมีการกำหนดผู้รับผิดชอบตามนโยบายที่ชัดเจน				
๗	หน่วยงานมีการทบทวนนโยบายเป็นปัจจุบัน				

สรุปผลการตรวจสอบ

.....

.....

.....

.....

ผู้ตรวจสอบ .....

วันที่.....

ผู้สอบทาน.....

วันที่.....

กระดาษทำการตรวจสอบข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

หน่วยงาน .....

ลำดับ	แนวนโยบาย	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
		มี/ใช่	ไม่มี/ไม่ใช่		
๑	มีการจัดทำข้อปฏิบัติเป็นลายลักษณ์อักษร				
๒	ข้อปฏิบัติมีเนื้อหาเกี่ยวกับข้อกำหนดการควบคุมการเข้าถึง				
๓	ข้อปฏิบัติมีเนื้อหาเกี่ยวกับข้อกำหนดการใช้งานตามภารกิจ				
๔	ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการจัดการการเข้าถึงของผู้ใช้งาน				
๕	ข้อปฏิบัติมีเนื้อหาเกี่ยวกับหน้าที่ความรับผิดชอบของผู้ใช้งาน				
๖	ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการควบคุมการเข้าถึงระบบเครือข่าย				
๗	ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการควบคุมการเข้าถึงระบบปฏิบัติการ				
๘	ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ				
๙	ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการจัดทำระบบสำรองข้อมูลสารสนเทศ				
๑๐	ข้อปฏิบัติมีเนื้อหาเกี่ยวกับการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน				
๑๑	ข้อปฏิบัติกำหนดเดี่ยวกับการตรวจสอบและประเมินความเสี่ยง				
๑๒	ข้อปฏิบัติสอดคล้องกับนโยบายรักษาความมั่นคงปลอดภัย				
๑๓	มีการประกาศเผยแพร่ข้อปฏิบัติให้ผู้ใช้งานทราบ โดย				
	๑๓.๑ ทาง website, intranet				
	๑๓.๒ แจ้งเวียน				
	๑๓.๓ อื่นๆ ระบุ.....				
๑๔	หน่วยงานมีการกำหนดผู้รับผิดชอบตามข้อปฏิบัติที่ชัดเจน				
๑๕	หน่วยงานมีการทบทวนข้อปฏิบัติเป็นปัจจุบัน				

สรุปผลการตรวจสอบ

.....

.....

.....

ผู้ตรวจสอบ ..... ผู้สอบทาน.....

วันที่..... วันที่.....

กระดาษทำการตรวจสอบแนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่กระทบ พ.ร.บ. คอมพิวเตอร์

หน่วยงาน .....

ลำดับ	ความผิดตาม พ.ร.บ. คอมพิวเตอร์	แนวทางการควบคุม	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
			มี	ไม่มี		
๑	การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน	มีการประกาศไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันเข้าถึงโดยโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน				
๒	การเปิดเผยวิธีการที่จะเข้าไปยังระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน	มีการประกาศไม่ให้ผู้ใช้บริการมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น				
๓	การเข้าข้อมูลคอมพิวเตอร์ของผู้อื่นที่มีการป้องกัน	มีการประกาศไม่ให้ผู้ใช้บริการเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน				
๔	การดักข้อมูลคอมพิวเตอร์ที่อยู่ระหว่างการส่งของระบบคอมพิวเตอร์	มีการประกาศไม่ให้ผู้ใช้บริการกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์				
๕	การทำลาย แก้ไขเปลี่ยนแปลงเพิ่มเติมโดยมิได้รับอนุญาต	มีการประกาศไม่ให้ผู้ใช้บริการทำให้เสียหาย ทำลายแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ				

ลำดับ	ความผิดตาม พ.ร.บ. คอมพิวเตอร์	แนวทางการควบคุม	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
			มี	ไม่มี		
๖	การระงับ ชะลอ ขัดขวาง หรือรบกวนคอมพิวเตอร์ของผู้อื่น	มีการประกาศไม่ให้ผู้ใช้บริการกระทำด้วยประการใดโดยมิชอบเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้				
๗	การส่งข้อมูลคอมพิวเตอร์หรือจดหมายที่มีการปกปิดหรือปลอมแปลงแหล่งที่มาเพื่อรบกวนข้อมูลการทำงานของผู้อื่น	มีการประกาศไม่ให้ผู้ใช้บริการส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดตปกปิดหรือปลอมแปลงที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข				
๘	ก่อให้เกิดความเสี่ยงหายแก่ประชาชนความมั่นคงของประเทศชาติ	มีการประกาศไม่ให้ผู้ใช้บริการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศชาติความปลอดภัยสาธารณะความมั่นคงในทางเศรษฐกิจของประเทศหรือการบริการสาธารณะผรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ				
๙	การจำหน่ายหรือเผยแพร่ชุดคำสั่ง	มีการประกาศไม่ให้ผู้ใช้บริการจำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม พ.ร.บ.คอมพิวเตอร์				
๑๐	การเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงของชาติเข้าสู่ระบบคอมพิวเตอร์	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน				

ลำดับ	ความผิดตาม พ.ร.บ. คอมพิวเตอร์	แนวทางการควบคุม	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
			มี	ไม่มี		
๑๑	การเผยแพร่ข้อมูลที่เท็จเข้าสู่ระบบคอมพิวเตอร์	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมหรือเป็นเท็จไม่ว่าทั้งหมดหรือบางส่วนโดยที่น่าจะเกิดความเสียหายแก่ผู้อื่น				
๑๒	การนำเข้าหรือเผยแพร่เนื้อหาอันไม่เหมาะสม	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน				
๑๓	การเผยแพร่ข้อมูลความผิดที่เกี่ยวกับการเข้าสู่ระบบคอมพิวเตอร	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา				
๑๔	การเผยแพร่ข้อมูลที่มีลักษณะลามก อนาจาร เข้าสู่ระบบคอมพิวเตอร์	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆที่มีลักษณะ ลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้				
๑๕	การเผยแพร่ภาพตัดต่อแต่งเติม หรือดัดแปลงภาพ ที่ทำให้คนอื่นเสียหาย ถูกดูหมิ่นเข้าสู่ระบบคอมพิวเตอร์	มีการประกาศไม่ให้ผู้ใช้บริการนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงภาพ หรือวิธีการใดๆทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง				

ลำดับ	ความผิดตาม พ.ร.บ. คอมพิวเตอร์	แนวทางการควบคุม	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
			มี	ไม่มี		
๑๖	ผู้ให้บริการการเข้าถึงอินเทอร์เน็ต ไม่มีจราจรคอมพิวเตอร์ไว้ ๙๐ วัน	กองเทคโนโลยีและสารสนเทศมีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้อย่างน้อย ๙๐ วัน				

สรุปผลการตรวจสอบ

.....

.....

.....

.....

.....

.....

.....

.....

ผู้ตรวจสอบ .....

วันที่.....

ผู้สอบทาน.....

วันที่.....

กระดาษทำการตรวจสอบการควบคุมการเข้าถึงและควบคุมการใช้งาน

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	เอกสารที่เกี่ยวข้อง
		มี/ใช่	ไม่มี/ไม่ใช่		
๑	การควบคุมทางกายภาพ				
	๑.๑ พื้นที่ศูนย์/สารสนเทศเป็นพื้นที่เฉพาะสำหรับบุคคลที่ได้รับอนุญาตเท่านั้น				
	๑.๒ ศูนย์ฯ รวมถึงห้องเก็บสารสนเทศภายในและห้องทำงานปิดล็อก เมื่อไม่มีการใช้งาน				
	๑.๓ ศูนย์ฯ มีการควบคุมเพื่อป้องกันภัย				
	- ขโมย				
	- ไฟไหม้				
	- น้ำท่วม				
	๑.๔ มีนโยบายไม่ให้กิน ดื่ม และสูบบุหรี่ภายในศูนย์				
	๑.๔ มีอุปกรณ์ UPS สำรองไฟ เพื่อป้องกันข้อมูลสารสนเทศเสียหายกรณีไฟฟ้าดับ/ตก/ไม่สม่ำเสมอ				
	๑.๖ อุปกรณ์ UPS มีระยะเวลาการใช้งานเพียงพอที่จะสำรองข้อมูลได้				
	๑.๗ มีการตรวจสอบ และบำรุงรักษาสายไฟฟ้าภายในศูนย์ฯ อย่างสม่ำเสมอ				
	๑.๘ มีการตรวจสอบ และบำรุงรักษาสายเคเบิลโทรคมนาคมที่อยู่ในความรับผิดชอบของหน่วยงานอย่างสม่ำเสมอ				
	๑.๙ มีการบำรุงรักษาอุปกรณ์คอมพิวเตอร์และ Hardware ของหน่วยงานเป็นระยะ				
๒	มีการกำหนดสิทธิในการเข้าถึงสอดคล้องกับการอนุญาตและการมอบอำนาจ				
๓	มีการดำเนินการเกี่ยวกับข้อมูลและสารสนเทศต่างๆ ในเรื่องต่อไปนี้				
	๓.๑ จัดประเภทของข้อมูลและสารสนเทศ				
	๓.๒ จัดชั้นความลับของข้อมูลและสารสนเทศ				
	๓.๓ จัดชั้นการเข้าถึง				
	๓.๔ กำหนดเวลาในการเข้าถึง				
	๓.๕ กำหนดช่องทางในการเข้าถึง				

สรุปผลการตรวจสอบ

.....

.....

.....

ผู้ตรวจสอบ ..... ผู้สอบทาน.....

วันที่..... วันที่.....

กระดาษทำการตรวจสอบการใช้งานตามภารกิจ

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
๑	หน่วยงานได้กำหนดข้อปฏิบัติสำหรับการใช้งานตามภารกิจ				
๒	กรณีที่กำหนดข้อปฏิบัติ ดำเนินการแยกรายภารกิจหรือไม่				
๓	ข้อปฏิบัติครอบคลุม เรื่องต่อไปนี้หรือไม่				
	๓.๑ มีการควบคุมการเข้าถึงสารสนเทศหรือไม่				
	๓.๒ การควบคุมการเข้าถึงสารสนเทศสอดคล้องกับนโยบายและข้อปฏิบัติ หรือไม่				
	๓.๓ มีการกำหนดในส่วนของการปรับปรุงหรือไม่				
	๓.๔ การควบคุมการปรับปรุงสอดคล้องกับนโยบายและข้อปฏิบัติ				

สรุปผลการตรวจสอบ

.....

.....

.....

.....

.....

.....

.....

.....

.....

ผู้ตรวจสอบ .....

วันที่.....

ผู้สอบทาน.....

วันที่.....

กระดาษทำการตรวจสอบการบริหารจัดการการเข้าถึงผู้ใช้งาน

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
๑	หน่วยงานจัดให้มีการให้ความรู้ ความเข้าใจกับผู้ปฏิบัติงานอย่างต่อเนื่อง				
	โดยวิธีการ ต่อไปนี้				
	๑.๑ เผยแพร่ทาง Website, Intranet				
	๑.๒ แจ้งเวียน				
	๑.๓ วิธีอื่นๆ ระบุ.....				
๒	มีการให้ลงทะเบียนสำหรับผู้เข้าใช้งาน				
	๒.๑ มีข้อกำหนดในการลงทะเบียน				
	๒.๒ มีข้อกำหนดและหลักเกณฑ์ในการอนุญาตให้ใช้งาน				
	๒.๓ มีข้อกำหนดและหลักเกณฑ์ในการยกเลิก/เพิกถอนการอนุญาตให้เข้าใช้งานในระบบ				
๓	มีการควบคุมและจำกัดสิทธิ				
	๓.๑ มีเอกสารแสดงการกำหนดสิทธิ (ตารางกำหนดสิทธิ)				
	๓.๒ ไม่มีการสร้าง User ร่วม				
	๓.๓ สิทธิที่กำหนดในแต่ละกลุ่มชัดเจนและเหมาะสม				
๔	มีการกำหนดเงื่อนไขการให้รหัสและเพิกถอนการให้รหัส โดยผ่านกระบวนการด้านการบริหาร				
	๔.๑ กระบวนการให้รหัสผ่านความเห็นชอบตามเงื่อนไขที่ฝ่ายบริหารกำหนด				
	๔.๒ มีการดำเนินการเพิกถอนรหัสตามเงื่อนไขที่กำหนด				
	๔.๓ มีการกำหนดเงื่อนไขให้ผู้ใช้งานเก็บรหัสไว้เป็นความลับ				
๕	มีการทบทวนสิทธิเข้าถึงของผู้ใช้งานหรือไม่				
	๕.๑ การทบทวนสิทธิดำเนินการอย่างต่อเนื่องเป็นระยะ โดยมีการกำหนดระยะเวลาในการทบทวนที่แน่นอน หรือไม่				

สรุปผลการตรวจสอบ

.....

.....

.....

ผู้ตรวจสอบ ..... ผู้สอบทาน.....

วันที่..... วันที่.....

กระดาษทำการตรวจสอบการกำหนดหน้าที่ความรับผิดชอบ

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
๑	หน่วยงานกำหนดแนวปฏิบัติสาหรับผู้ที่ใช้งานเกี่ยวกับ				
	๑.๑ วิธีการกำหนดรหัสที่ดี				
	๑.๒ การใช้รหัสผ่าน				
	๑๓ การเปลี่ยนรหัสผ่าน				
๒	ผู้ใช้งานรับทราบแนวปฏิบัติเกี่ยวกับรหัสผ่านทางใด				
	๒.๑ ทาง website, Intranet				
	๒.๒ หนังสือเวียน				
	๒.๓ อื่นๆ ระบุ.....				
๓	หน่วยงานกำหนดข้อปฏิบัติสำหรับผู้ใช้งานเกี่ยวกับการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน				
๔	ผู้ใช้งานรับทราบข้อปฏิบัติเกี่ยวกับการป้องกันผ่านช่องทางใด				
	๔.๑ ทาง website, Intranet				
	๔.๒ หนังสือเวียน				
	๔.๓ อื่นๆ ระบุ.....				
๕	หน่วยงานกาหนดข้อปฏิบัติสาหรับผู้ใช้งานเกี่ยวกับการควบคุมข้อมูล สื่อ และสินทรัพย์ด้านสารสนเทศ				
๖	ผู้ใช้งานรับทราบข้อปฏิบัติเกี่ยวกับการควบคุมผ่านช่องทางใด				
	๖.๑ ทาง website, Intranet				
	๖.๒ หนังสือเวียน				
	๖.๓ อื่นๆ ระบุ.....				
๗	หน่วยงานกำหนดการควบคุมเพื่อป้องกันผู้ใช้งานนาการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับโดย				
	๗.๑ กำหนดข้อปฏิบัติและหลักเกณฑ์ สำหรับการเข้าถึงข้อมูลที่เป็นความลับและข้อมูลที่สำคัญของหน่วยงาน				

สรุปผลการตรวจสอบ

.....

.....

ผู้ตรวจสอบ ..... ผู้สอบทาน.....

วันที่..... วันที่.....

กระดาษทำการตรวจสอบการเข้าถึงระบบเครือข่าย

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
๑	กำหนดให้ผู้ใช้งานสามารถเข้าได้เฉพาะบริการที่ได้รับสิทธิเท่านั้น				
	๑.๑ หน่วยงานมีเอกสารที่แสดงว่ามีระบบสารสนเทศใดที่หน่วยงานต้องควบคุมการเข้าถึง				
	๑.๒ หน่วยงานได้แสดงข้อปฏิบัติในการเข้าถึงให้ผู้ใช้งานทราบ				
	๑๓ หน่วยงานมีการควบคุมการเชื่อมต่อ Terminal กับระบบคอมพิวเตอร์หลักอย่างรัดกุม				
๒	ผู้ใช้งานรับทราบแนวปฏิบัติเกี่ยวกับการเข้าถึงบริการ ผ่านช่องทางใด				
	๒.๑ ทาง website, Intranet				
	๒.๒ หนังสือเวียน				
	๒.๓ อื่นๆ ระบุ.....				
๓	หน่วยงานมีข้อปฏิบัติหรือกระบวนการในการยืนยันตัวบุคคลก่อนอนุญาตให้ผู้ใช้งานจากภายนอกเชื่อมต่อเข้าระบบสารสนเทศ/เครือข่ายของหน่วยงาน				
๔	หน่วยงานสามารถระบุอุปกรณ์บนเครือข่ายได้				
๕	หน่วยงานใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึงได้				
๖	หน่วยงานกำหนดให้มีการควบคุม Port ต่อไปนี้				
	๖.๑ Port สำหรับการตรวจสอบ				
	(๑) การเข้าถึงทางกายภาพ				
	(๒) การเข้าถึงทางเครือข่าย				
	๖.๒ Port สำหรับการปรับแต่งระบบ				
	(๑) การเข้าถึงทางกายภาพ				
	(๒) การเข้าถึงทางเครือข่าย				
๗	ข้อห้าม				
	๗.๑ ไม่มีการระบุ Port ตามข้อ ๖.๑ และ ๖.๒ ไว้ในเอกสารการควบคุมหรือข้อปฏิบัติ				
	๗.๒ ไม่มีการระบุวิธีการเข้าถึง Port ตามข้อ ๖.๑ และ๖.๒ ไว้ในเอกสารการควบคุมหรือข้อปฏิบัติ				

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
๘	หน่วยงานมีการแบ่งแยกเครือข่ายดังนี้				
	๘.๑ สำหรับกลุ่มบริการสารสนเทศ				
	๘.๒ สำหรับกลุ่มผู้ใช้งาน				
	๘.๓ สำหรับกลุ่มระบบสารสนเทศ				
๙	หน่วยงานมีเอกสาร Network diagram เป็นปัจจุบัน				
๑๐	หน่วยงานกำหนดการควบคุมเส้นทางบนเครือข่าย ดังนี้				
	๑๐.๑ กำหนดขั้นตอนและหลักเกณฑ์การเชื่อมต่อคอมพิวเตอร์ และการส่งผ่านข้อมูลสอดคล้องกับการควบคุมการเข้าถึงและการใช้โปรแกรมในนโยบายและข้อปฏิบัติ				

สรุปผลการตรวจสอบ

.....

.....

.....

.....

.....

.....

ผู้ตรวจสอบ .....

วันที่.....

ผู้สอบทาน.....

วันที่.....

กระดาษทำการตรวจสอบการเข้าถึงระบบปฏิบัติการ

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
๑	หน่วยงานกำหนดขั้นตอนการปฏิบัติต่อไปนี้				
	๑.๑ การควบคุมการเข้าใช้งานในที่มั่นคง				
	๑.๒ การควบคุมการเข้าถึงระบบปฏิบัติการ				
๒	หน่วยงานมีหลักฐานที่แสดงให้เห็นว่า				
	๒.๑ หน่วยงานกำหนดให้ผู้ใช้งานแสดงข้อมูลจำเพาะในการยืนยันตัวตนของผู้ใช้งาน				
	๒.๒ หน่วยงานกำหนดขั้นตอนการยืนยันตัวตนของผู้ใช้งาน				
๓	หน่วยงานมีการบริหารจัดการรหัสผ่าน ที่สามารถทำงานเชิงโต้ตอบ หรือทำงานอัตโนมัติได้				
๔	หน่วยงานกำหนดการจำกัดหรือการควบคุมการใช้งานโปรแกรมอรรถประโยชน์				
๕	หน่วยงานกำหนดให้เครื่องยุติ หากมีการว่างเว้นการใช้งาน				
๖	หน่วยงานแจ้งข้อปฏิบัติในการให้เครื่องยุติการใช้งานหากว่างเว้นการใช้งานใดๆ ระยะเวลาหนึ่ง ให้ผู้ใช้งานทราบ				
๗	หน่วยงานจำกัดเวลาในการเชื่อมต่อระบบสารสนเทศหรือโปรแกรมประยุกต์สำคัญๆ				

สรุปผลการตรวจสอบ

.....

.....

.....

.....

.....

.....

ผู้ตรวจสอบ .....

วันที่.....

ผู้สอบทาน.....

วันที่.....

กระดาษทำการตรวจสอบการเข้าถึงโปรแกรมประยุกต์ หรือ Application และสารสนเทศ

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
๑	หน่วยงานมีการจำกัดหรือควบคุมการเข้าถึงสารสนเทศและฟังก์ชัน ต่างๆ ของโปรแกรมประยุกต์จากผู้ใช้งาน				
๒	หน่วยงานมีการจำกัดหรือควบคุมการเข้าถึงสารสนเทศและฟังก์ชัน ต่างๆ ของโปรแกรมประยุกต์จากบุคลากรฝ่ายสนับสนุน				
๓	ข้อจำกัดที่กำหนดเป็นไปตามนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน				
๔	หน่วยงานมีข้อกำหนดในการควบคุมคอมพิวเตอร์เคลื่อนที่การเข้าถึงสารสนเทศ				
๕	หน่วยงานมีข้อกำหนดในการควบคุมโทรศัพท์เคลื่อนที่การเข้าถึงสารสนเทศ				
๖	หน่วยงานมีข้อกำหนดในการควบคุมการใช้จากภายนอกผ่านคอมพิวเตอร์เคลื่อนที่และโทรศัพท์เคลื่อนที่				
๗	หน่วยงานมีข้อปฏิบัติหรือข้อกำหนดและมาตรการเพื่อป้องกันความเสี่ยงจากการใช้คอมพิวเตอร์เคลื่อนที่และโทรศัพท์เคลื่อนที่				

สรุปผลการตรวจสอบ

.....

.....

.....

.....

.....

.....

ผู้ตรวจสอบ .....

วันที่.....

ผู้สอบทาน.....

วันที่.....

กระดาษทำการตรวจสอบการจัดระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
๑	หน่วยงานมีการพิจารณาคัดเลือกและจัดทำระบบสำรองโดย				
	๑.๑ หน่วยงานมีข้อปฏิบัติหรือหลักเกณฑ์ในการคัดเลือกระบบสารสนเทศ				
	๑.๒ หน่วยงานมีข้อปฏิบัติหรือหลักเกณฑ์ในการจัดทำระบบสำรอง				
	๑.๓ ระบบที่จัดทำกำหนดให้มีการกู้คืนและรายงานผลได้				
	๑.๔ ทุกระบบที่จัดทำสำรองมีการรายงานผลการสำรอง				
๒	หน่วยงานมีการเตรียมแผนการเตรียมความพร้อมกรณีฉุกเฉิน ดังนี้				
	๒.๑ กรณีที่ไม่สามารถดำเนินงานด้วยระบบอิเล็กทรอนิกส์ได้				
	๒.๒ กรณีที่ Site หลักไม่ทำงาน				
	๒.๓ มีการกำหนดแผนระยะสั้น				
	๒.๔ มีการกำหนดแผนระยะยาว				
	๒.๕ มีการทบทวนแผน				
๓	หน่วยงานกำหนดหน้าที่ความรับผิดชอบของบุคลากร ดังนี้				
	๓.๑ ด้านระบบสารสนเทศ				
	๓.๒ ด้านระบบสำรอง				
	๓.๓ ด้านการจัดทำแผนและทบทวนแผน				
๔	หน่วยงานจัดให้มีการทดสอบระบบให้อยู่ในสภาพพร้อมใช้งาน				

สรุปผลการตรวจสอบ

.....

.....

.....

.....

.....

.....

ผู้ตรวจสอบ .....

วันที่.....

ผู้สอบทาน.....

วันที่.....

กระดาษทำการสอบทานการจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

หน่วยงาน .....

ลำดับ	รายการ	ผลการตรวจสอบ		ผู้ที่เกี่ยวข้อง	ระบุรายละเอียด
		มี/ใช่	ไม่มี/ไม่ใช่		
๑	หน่วยงานกำหนดนโยบายหรือมาตรการให้มีการตรวจสอบ โดยหน่วยตรวจสอบภายใน				
๒	หน่วยงานกำหนดนโยบายหรือมาตรการให้มีการตรวจสอบหรือประเมินความเสี่ยง โดยผู้ประเมินภายนอก				
๓	มีการกำหนดให้ดำเนินการอย่างน้อยปีละ ๑ ครั้ง				
๔	มีการรายงานผลการตรวจสอบหรือประเมินเสนอต่อผู้บริหารหน่วยงานเพื่อทราบและพิจารณาสั่งการ				

สรุปผลการตรวจสอบ

.....

.....

.....

.....

.....

.....

ผู้ตรวจสอบ .....

วันที่.....

ผู้สอบทาน.....

วันที่.....