ประกาศกรมป่าไม้
เรื่อง แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

แนวทางการตรวจสอบด้านการรักษาความมั่นคงกำหนดให้หน่วยงานของรัฐดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ มีมาตรการในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมป่าไม้มีความมั่นคงปลอดภัย และสามารถสนับสนุนภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้เป็นไปอย่างเหมาะสม สอดคล้องกับมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งเป็นกรอบในการบริหารจัดการความมั่นคงปลอดภัยด้านไซเบอร์อย่างเป็นระบบ และอาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม กรมป่าไม้จึงกำหนดแนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ เพื่อให้หน่วยงานและบุคลากรในสังกัดถือปฏิบัติ กรมป่าไม้จึงประกาศไว้ ดังนี้

๑. ประกาศนี้เรียกว่า “แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้”

๒. การจัดทำแนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้ มีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อเป็นแนวทางให้หน่วยงานของกรมป่าไม้สามารถดำเนินการประเมินและตรวจสอบความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างเป็นระบบ

๒.๒ เพื่อกำหนดกรอบ มาตรการ และแนวทางในการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้อย่างเป็นระบบ

๒.๓ เพื่อประเมินความเสี่ยงและค้นหาจุดอ่อนของระบบสารสนเทศ ระบบเครือข่าย และมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

๒.๔ เพื่อให้การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้สอดคล้องกับกฎหมาย มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้อง

๓. เพื่อใช้เป็นกรอบและแนวทางในการบริหารจัดการ ประเมิน วิเคราะห์ และควบคุมความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานให้เป็นไปในทิศทางเดียวกัน และสอดคล้องตามกฎหมาย มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้อง

๔. ให้ใช้แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้ตามแนบท้ายประกาศนี้

๕. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๙ พฤษภาคม พ.ศ. ๒๕๖๙

(นายนิกร ศิรโรจนานนท์)
อธิบดีกรมป่าไม้

แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

แนบท้ายประกาศกรมป่าไม้ ลงวันที่ ๒๙ พฤษภาคม พ.ศ. ๒๕๖๙

เรื่อง แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

คำนำ

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งกำหนดกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อความมั่นคงของรัฐ การให้บริการสาธารณะ และระบบสารสนเทศสำคัญของหน่วยงานของรัฐนั้น ได้กำหนดให้หน่วยงานของรัฐต้องมีการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ครอบคลุม และตรวจสอบได้

ทั้งนี้ ตามมาตรา ๔๔ แห่งพระราชบัญญัติดังกล่าว กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบาย แนวทาง และมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายและแผนระดับชาติ และตามมาตรา ๕๘ กำหนดให้หน่วยงานต้องมีมาตรการในการเฝ้าระวัง ตรวจสอบ ประเมินความเสี่ยง และจัดการภัยคุกคามทางไซเบอร์อย่างเหมาะสม รวมถึงการตรวจสอบและประเมินประสิทธิผลของมาตรการด้านความมั่นคงปลอดภัยไซเบอร์อย่างสม่ำเสมอ

นอกจากนี้ ยังต้องปฏิบัติตามประกาศและแนวทางที่กำหนดโดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตลอดจนมาตรฐานและแนวปฏิบัติที่เกี่ยวข้อง เช่น แนวทางการตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Audit) การประเมินความสอดคล้องตามข้อกำหนด (Compliance Audit) และกรอบมาตรฐานสากลที่เกี่ยวข้อง เพื่อให้การดำเนินงานมีความโปร่งใส ตรวจสอบได้ และสามารถปรับปรุงพัฒนาได้อย่างต่อเนื่อง

ในการนี้ กรมป่าไม้จึงได้จัดทำแนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ขึ้น เพื่อใช้เป็นกรอบในการกำหนดหลักเกณฑ์ วิธีการ และขั้นตอนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ให้ครอบคลุมทั้งด้านนโยบาย กระบวนการ เทคโนโลยี และบุคลากร รวมถึงเพื่อประเมินความเพียงพอและประสิทธิผลของมาตรการที่มีอยู่

แนวทางฉบับนี้มุ่งหวังให้หน่วยงานและบุคลากรที่เกี่ยวข้องสามารถดำเนินการตรวจสอบได้อย่างเป็นระบบ มีมาตรฐาน และสอดคล้องตามข้อกำหนดของกฎหมายและระเบียบที่เกี่ยวข้อง อันจะช่วยเสริมสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และสนับสนุนการดำเนินภารกิจของกรมป่าไม้ให้เป็นไปอย่างมีประสิทธิภาพ โปร่งใส และตรวจสอบได้

พฤษภาคม ๒๕๖๙

สารบัญ

แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. บทนำ

กรมป่าไม้ได้มีการพัฒนาระบบสารสนเทศ ระบบภูมิศาสตร์สารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ เพื่อให้ให้บริการเทคโนโลยีสารสนเทศและการสื่อสาร แก่บุคลากรของกรมป่าไม้ ประชาชน และผู้ประกอบการ ให้สามารถเข้าถึงข้อมูลได้อย่างรวดเร็ว มีประสิทธิภาพ ถูกต้อง ทั้งนี้ยังมีการใช้บริการการเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆ เช่น กรมการปกครอง กรมศุลกากร สำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ (องค์การมหาชน) กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม เป็นต้น ซึ่งบริการดังข้างต้นที่ได้กล่าวมาเป็นเทคโนโลยีสารสนเทศหลักของกรมป่าไม้ เพื่อพัฒนาไปสู่นโยบายไทยแลนด์ ๔.๐ และแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย โดยในปัจจุบันมีภัยคุกคามทางไซเบอร์ที่มีรูปแบบการโจมตีแบบใหม่ๆ จะอาศัยช่องโหว่ที่เกิดขึ้นในระบบ เจาะเข้ามาเพื่อขโมยข้อมูล ทำลายข้อมูล เข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ และทำให้ระบบเครือข่ายอินเตอร์เน็ตล่ม ซึ่งหากเกิดเหตุการณ์ดังกล่าวจะสร้างความเสียหายต่อระบบสารสนเทศ ระบบฐานข้อมูล ข้อมูลส่วนบุคคล และระบบเครือข่ายของกรมป่าไม้ได้

การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นกระบวนการเพื่อประเมินและตรวจสอบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ และระบบเครือข่ายของหน่วยงาน เพื่อตรวจหาความบกพร่องหรือจุดอ่อน ที่อาจเป็นช่องทางการเข้าถึงของผู้ไม่ประสงค์ดี (hackers) หรือการละเมิดความปลอดภัยอื่น ๆ ที่อาจส่งผลกระทบสร้างความเสียหายหน่วยงาน และประชาชน

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดกรอบ มาตรการ และคุณสมบัติของผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ในการตรวจสอบและประมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๒ เพื่อกำหนดหลักการตรวจสอบและประมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. กลุ่มเป้าหมาย

๓.๑ ผู้ตรวจสอบที่ได้รับการอนุมัติหรือแต่งตั้งอย่างเป็นทางการจากคณะกรรมการ

๓.๒ ผู้มีส่วนได้ส่วนเสีย เช่น หัวหน้าหน่วยธุรกิจ ผู้ขาย เจ้าของระบบ และหัวหน้าเจ้าหน้าที่รักษาความมั่นคงปลอดภัยข้อมูล เป็นต้น

๓.๓ ผู้ที่จำเป็นต้องรู้เกี่ยวกับความคาดหวังในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์สำหรับการตรวจสอบหน่วยงานของตน

๔. ขอบเขต

ครอบคลุมการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมป่าไม้

๕. การอนุมัติผู้ตรวจสอบ

ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยหน่วยงาน เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ในหน่วยงาน โดยหน่วยงานและผู้ตรวจสอบจะต้องส่งแบบฟอร์มที่เกี่ยวข้องตามที่สำนักงานคณะกรรมการ

การรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) กำหนด โดยใบสมัครจะสมบูรณ์ก็ต่อเมื่อแบบฟอร์มที่เกี่ยวข้องทั้งหมดและเอกสารประกอบที่ส่งมาของหน่วยงาน และผู้ตรวจสอบนั้นครบถ้วนและเป็นไปตามลำดับ

๕.๑ เกณฑ์การพิจารณาแบ่งออกเป็น ๒ ประการ ได้แก่

๕.๑.๑ ความเป็นอิสระและความสามารถที่สำนักงานตรวจสอบหรือทีมงาน (audit firm/team)

๕.๑.๒ ผู้ตรวจสอบ (auditors) ที่เสนอจำเป็นต้องปฏิบัติตาม

๕.๒ สำนักงานตรวจสอบหรือทีมงาน และผู้ตรวจสอบที่ได้รับการแต่งตั้ง มีคุณสมบัติดังนี้

๕.๒.๑ ไม่ควรอยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of interest) ใด ๆ ไม่ว่าจะเกิดขึ้นจริง มีแนวโน้ม หรือได้รับรู้ ผลประโยชน์ทับซ้อน หมายถึง สถานการณ์ใด ๆ ที่ผลประโยชน์ของผู้ตรวจสอบอาจแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบอย่างเป็นอิสระและมีวัตถุประสงค์

๕.๒.๒ ควรมีความสามารถทางเทคนิคที่จำเป็น เช่น คุณวุฒิวิชาชีพ/ใบรับรอง ทักษะ ความรู้และประสบการณ์ที่เกี่ยวข้อง เป็นต้น เพื่อดำเนินการตรวจสอบ

ทั้งนี้ หน่วยงานอาจพิจารณาแตกต่างไปตามที่หน่วยงานเห็นสมควร ในประเด็นต่อไปนี้

๑) จำนวนผู้ตรวจสอบของแต่ละหน่วยงาน

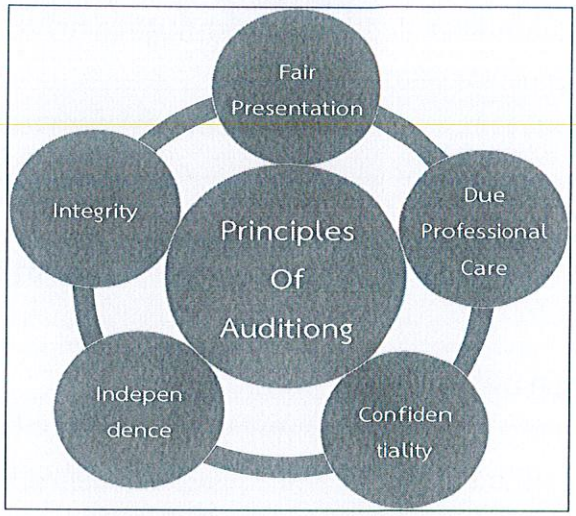
๒) ระยะเวลาในการขออนุญาต เช่น รายปีหรือตามรอบการตรวจสอบ เป็นต้น ในกรณีผู้ตรวจสอบของหน่วยงานที่ลงทะเบียนแล้วลาออกจากการเป็นพนักงานก่อนการดำเนินการตรวจสอบ หรือมีการเปลี่ยนแปลงพนักงานที่ลงทะเบียนไว้ ให้หน่วยงานแจ้ง สกมช. ภายใน ๓๐ วันนับจากวันที่การเปลี่ยนแปลงอย่างเป็นทางการของหน่วยงาน

๖. ความคาดหวังในการตรวจสอบ

ผู้ตรวจสอบต้องตรวจสอบอย่างสร้างสรรค์รัดกุมมีประสิทธิภาพ เพียงพอที่จะป้องกันความเสียหายและทันต่อเหตุการณ์ เน้นการตรวจสอบที่มีคุณภาพ คุ้มค่า เป็นไปตามมาตรฐาน โปร่งใส ถูกต้อง มีความน่าเชื่อถือ จะทำให้เกิดกระบวนการกำกับที่ดี (Good Governance) และความโปร่งใสในการปฏิบัติงาน (Transparency) โดยระบุความคาดหวังไว้ ๗ ด้าน ในหัวข้อ ๖.๑ ถึง ข้อ ๖.๗

๖.๑ หลักการตรวจสอบ

หลักการตรวจสอบควรยึดหลักการ ๕ ข้อดังต่อไปนี้ เพื่อให้ข้อสรุปการตรวจสอบที่เกี่ยวข้องและเพียงพอ ทั้งนี้ เพื่อช่วยให้ผู้ตรวจสอบ ซึ่งทำงานอย่างอิสระสามารถบรรลุข้อสรุปที่คล้ายคลึงกันในสถานการณ์ที่คล้ายคลึงกัน ดังภาพที่ ๑



ภาพที่ ๑ หลักการตรวจสอบ

๖.๑.๑ ความซื่อสัตย์ (Integrity) รากฐานของความเป็นมืออาชีพ

๑) ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ

๒) มีความรู้ ทักษะ และมีความสามารถในการดำเนินการตรวจสอบ

๓) ดำเนินการตรวจสอบอย่างเป็นกลาง

๔) มีความยุติธรรม และเป็นกลางในการติดต่อสื่อสาร ระมัดระวังต่ออิทธิพลใด ๆ ที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ

๖.๑.๒ การนำเสนออย่างยุติธรรม (Fair Presentation) หน้าที่ในการรายงานตามความเป็นจริงและถูกต้อง

๑) ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง

๒) รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่างทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ

๓) ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจน และครบถ้วน

๖.๑.๓ การปฏิบัติอย่างมืออาชีพ (Due Professional Care) การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ

๑) ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ

๒) ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

๖.๑.๔ การรักษาความลับ (Confidentiality) ความมั่นคงปลอดภัยของข้อมูล

๑) ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ

๒) ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ตรวจสอบ

๓) จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม

๖.๑.๕ ความเป็นอิสระ (Independence) พื้นฐานสำหรับความเป็นกลางของการตรวจสอบและความเที่ยงธรรมของข้อสรุปการตรวจสอบ

๑) ตรวจสอบความเป็นอิสระของกิจกรรมที่กำลังตรวจสอบ

๒) ดำเนินการในลักษณะที่ปราศจากอคติและผลประโยชน์ทับซ้อนในทุกกรณี

๓) รักษาความเป็นกลางตลอดกระบวนการตรวจสอบ

๔) ตรวจสอบให้แน่ใจว่าผลการตรวจสอบและข้อสรุปขึ้นอยู่กับหลักฐานการตรวจสอบ (audit evidence) เท่านั้น

๖.๒ วัตถุประสงค์ในการตรวจสอบ

๖.๒.๑ ตรวจสอบการปฏิบัติตามของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

๖.๒.๒ ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

๖.๓ ขอบเขตการตรวจสอบ

การตรวจสอบครอบคลุม ดังนี้

ขอบเขต	คำอธิบาย
หัวข้อการตรวจสอบ (Audit Subject)	หัวข้อการตรวจสอบควรครอบคลุมหน่วยงานทั้งหมดที่กำหนดภายใต้กฎหมาย
ระยะเวลาการตรวจสอบ (Audit Period)	ระยะเวลาการตรวจสอบขั้นต่ำควรมีการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง
เกณฑ์การตรวจสอบ (Audit Criteria)	เกณฑ์การตรวจสอบควรรวมถึงการปฏิบัติตามกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

๖.๔ แนวทางการตรวจสอบ

การตรวจสอบควรใช้ทั้งแนวทางการปฏิบัติตามข้อกำหนด (compliance approach) และตามความเสี่ยง (risk-based approach)

๖.๔.๑ การปฏิบัติตามข้อกำหนด

ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

๖.๔.๒ การปฏิบัติตามความเสี่ยง

ระบุความเสี่ยงและภัยคุกคามที่หน่วยงานเผชิญ และตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบหรือไม่

๖.๕ ข้อค้นพบการตรวจสอบ

ผู้ตรวจสอบควรเน้นสิ่งต่อไปนี้

๖.๕.๑ ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

๖.๕.๒ เน้นการค้นหาอย่างเป็นระบบ (systemic finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงาน ซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม

๖.๕.๓ เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำ ในการตรวจสอบในปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (corrective action) แล้วก็ตาม

๖.๕.๔ เน้นแนวปฏิบัติที่ดี (good practices) ในด้านการกำกับดูแลและการควบคุม ซึ่งระบุไว้ในระหว่างการตรวจสอบ

๖.๕.๕ เมื่อเสนอข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรระบุคุณลักษณะของข้อค้นพบการตรวจสอบอย่างชัดเจน ต่อไปนี้

องค์ประกอบ	คำอธิบาย
สภาพหรือเงื่อนไข (Condition)	ถ้อยแถลงที่อธิบายผลลัพธ์ของการค้นพบการตรวจสอบ
เกณฑ์ (Criteria)	มาตรฐาน/ กฎ/ เกณฑ์มาตรฐาน (เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบาย และแนวทางปฏิบัติที่ดีที่สุด) ที่ใช้เทียบกับสภาพหรือเงื่อนไขที่ตรวจสอบ
สาเหตุ (Cause)	สาเหตุที่แท้จริง (root cause) และเหตุผลที่สนับสนุนสำหรับสภาพหรือเงื่อนไขที่ตรวจสอบ
ผลกระทบ (Effect)	ผลกระทบและนัยสำคัญของสภาพหรือเงื่อนไขที่ตรวจสอบ (ทันทีในอนาคตหรือที่อาจเกิดขึ้น) ผู้ตรวจสอบควรเชื่อมโยงการค้นพบการตรวจสอบกับผลกระทบต่อบริการที่จำเป็นของหน่วยงาน ซึ่งฝ่ายบริหารคุ้นเคย เช่น ผลกระทบเชิงปริมาณ (เช่น ต้นทุน เวลา และการผลิต) และผลกระทบเชิงคุณภาพ (เช่น การบริการและการตัดสินใจที่ไม่เหมาะสม) สิ่งนี้ช่วยโน้มน้าวฝ่ายบริหารถึงความจำเป็นในการดำเนินการแก้ไข
คำแนะนำ (Recommendation)	แนะนำให้ดำเนินการแก้ไขสาเหตุเพื่อป้องกันการเกิดการตรวจสอบซ้ำซ้อน

๖.๖ สรุปผลการตรวจสอบ

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่องต่อไปนี้

๖.๖.๑ ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ

๖.๖.๒ ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของหน่วยงาน

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร (Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๖.๒ ของเอกสารฉบับนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๖.๓ ของเอกสารฉบับนี้
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ ๑) มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ๒) ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) และ ๓) วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในข้อ ๖.๕ ของเอกสารฉบับนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในข้อ ๖.๖ ของเอกสารฉบับนี้

๖.๗ รูปแบบรายงานการตรวจสอบ

รายงานการตรวจสอบควรมีอย่างน้อย ดังต่อไปนี้

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร(Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๖.๒ ของเอกสารฉบับนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๖.๓ ของเอกสารฉบับนี้
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ ๑) มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ๒) ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) และ ๓) วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในข้อ ๖.๕ ของเอกสารฉบับนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในข้อ ๖.๖ ของเอกสารฉบับนี้

๗. ขั้นตอนการปฏิบัติในการตรวจสอบ

๗.๑ ผู้ตรวจสอบ ทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง

๗.๒ ผู้ตรวจสอบและคณะทำงานของหน่วยงาน ร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตถุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

๗.๒.๑ เพื่อชี้แจงวัตถุประสงค์ ขอบเขต และแผนการตรวจสอบ

๗.๒.๒ การสรุปวิธีการตรวจสอบ เกณฑ์การพิจารณา และกิจกรรมที่จะทำการตรวจสอบ

๗.๒.๓ การกำหนดผู้รับผิดชอบหรือช่องทางการสื่อสาร

๗.๒.๔ การชี้แจงรูปแบบการรายงานและการปิดตรวจสอบ

๗.๒.๕ ยืนยันแผนการตรวจสอบ

๗.๓ ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานทำหน้าที่ตอบข้อซักถาม และจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๗.๔ ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้น โดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

๗.๔.๑ ยืนยันข้อค้นพบการตรวจสอบจากการตรวจสอบ

๗.๔.๒ ระดับความไม่สอดคล้องของข้อตรวจพบ

๗.๔.๓ ข้อเสนอแนะในการปรับปรุง

๗.๔.๔ สรุปผลการตรวจสอบ

๗.๔.๕ กำหนดการตรวจติดตาม (ถ้ามี)

๗.๕ ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

๗.๖ คณะทำงานรับทราบผลการตรวจสอบ

๗.๗ ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้อง จากข้อตรวจพบลงแบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report (NCR) Form) ของหน่วยงาน และจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนด เพื่อรักษารักษาความลับ ในการตรวจสอบ

๗.๘ คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

๗.๙ คณะทำงาน ดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของหน่วยงาน

๗.๑๐ ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน