แนวทางปฏิบัติในการตรวจสอบ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ของสำนักงานนโยบายและแผนการขนส่งและจราจร

โดย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร

แนวทางปฏิบัติในการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานนโยบายและแผนการขนส่งและจราจร

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

สารบัญ

เรื่อง	หน้า
บทที่ ๑ บทนำ	๑
๑.๑ หลักการและเหตุผล	๑
๒.๒ จุดประสงค์	๑
๑.๓ กลุ่มเป้าหมาย	๑
๑.๔ ขอบเขต	๑
๑.๕ การอนุมัติผู้ตรวจสอบ	๒
๑.๖ ความคาดหวังในการตรวจสอบ	๒
บทที่ ๒ หลักการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์	
๒.๑ หลักการตรวจสอบ	๓
๒.๒ วัตถุประสงค์ในการตรวจสอบ	๔
๒.๓ ขอบเขตการตรวจสอบ	๔
๒.๔ แนวทางการตรวจสอบ	๔
๒.๕ ข้อค้นพบการตรวจสอบ	๔
๒.๖ ขั้นตอนปฏิบัติในการตรวจสอบ	๕
บทที่ ๓ การสรุปผลการตรวจสอบ	
๓.๑ การสรุปผลการตรวจสอบ	๗
๓.๒ รูปแบบรายงานการตรวจสอบ	๗
๓.๓ การติดตามและรายงานผล	๘

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

ตามที่สำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) ได้ออกประกาศ เรื่อง ประมวลแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. พ.ศ. ๒๕๖๗ นั้น กำหนดให้มีการตรวจสอบความมั่นคงปลอดภัยไซเบอร์จะต้องดำเนินการอย่างน้อยปีละหนึ่ง หรือความถี่ที่สูงกว่านั้นตามที่หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแลกำหนดในกรณีใดกรณีหนึ่ง และดำเนินการโดยผู้ตรวจสอบที่ได้รับอนุมัติหรือแต่งตั้งโดย สนข.

๑.๒ จุดประสงค์

๑.๒.๑ เพื่อกำหนดความคาดหวังในการตรวจสอบ และใช้เป็นแนวทางสำหรับผู้ตรวจสอบที่ได้รับการอนุมัติ หรือได้รับการแต่งตั้งโดยหน่วยงานเพื่อทำการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

๑.๒.๒ เพื่อสร้างความเข้าใจร่วมกันระหว่างตรวจสอบและผู้ได้รับการตรวจสอบ

๑.๓ กลุ่มเป้าหมาย

กลุ่มเป้าหมายของเอกสารฉบับนี้

๑.๓.๑ ผู้ตรวจสอบที่ได้รับการอนุมัติ หรือแต่งตั้งอย่างเป็นทางการจากศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร (ศทท.) หรือจาก สนข.

๑.๓.๒ ผู้มีส่วนได้ส่วนเสีย ที่จำเป็นต้องรู้เกี่ยวกับความคาดหวังในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์สำหรับ สนข. เช่น หัวหน้าส่วนราชการ เจ้าของระบบหรือผู้ขาย เจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ เจ้าหน้าที่รักษาความมั่นคงปลอดภัยข้อมูล เป็นต้น

๑.๔ ขอบเขต

๑.๔.๑ เอกสารนี้ครอบคลุมการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๑.๔.๒ เอกสารนี้ไม่ได้หมายถึงแหล่งข้อมูลที่ละเอียดถี่ถ้วนสำหรับการดำเนินการตรวจสอบการรักษาความมั่นคง ปลอดภัยไซเบอร์ของหน่วยงาน ในกรณีที่การตรวจสอบความมั่นคงปลอดภัยไซเบอร์ไม่มีหัวข้อใดที่กำหนดในเอกสารนี้ ผู้ตรวจสอบควรใช้ดุลยพินิจเยี่ยงผู้ประกอบวิชาชีพและระบุสถานการณ์ดังกล่าวในรายงานการตรวจสอบเอกสารนี้ ได้กำหนดคำนิยาม ดังนี้

(๑) คณะทำงานการรักษาความมั่นคงปลอดภัยไซเบอร์ หมายถึง คณะทำงานในการขับเคลื่อนงานด้านการรักษาความมั่นคงปลอดภัยให้แก่ระบบเทคโนโลยีสารสนเทศและดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ให้เป็นไปตามกฎหมาย ระเบียบ และประกาศที่เกี่ยวข้อง

(๒) ผู้ให้บริการภายนอก หมายถึง บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ทั้งนี้ผู้ให้บริการภายนอกไม่ครอบคลุมถึงผู้ใช้บริการที่ใช้ผลิตภัณฑ์และบริการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) หน่วยงาน หมายถึง สำนักงานนโยบายและแผนการขนส่งและจราจร

๑.๕ การอนุมัติผู้ตรวจสอบ

ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยหน่วยงาน เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ในหน่วยงาน โดยหมายถึงและผู้ตรวจสอบจะต้องส่งแบบฟอร์มที่เกี่ยวข้อง ศทท. กำหนด โดยมีเกณฑ์การพิจารณามี ๒ ประการ ได้แก่

๑.๕.๑ ไม่ควรอยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of Interest) ใด ๆ ไม่ว่าจะเกิดขึ้นจริง มีแนวโน้มหรือได้รับรู้ (ผลประโยชน์ทับซ้อน หมายถึง สถานการณ์ใด ๆ ที่ผลประโยชน์ของ ผู้ตรวจสอบอาจแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบอย่างเป็นอิสระและมีวัตถุประสงค์)

๑.๕.๒ ควรมีความสามารถทางเทคนิคที่จำเป็น (เช่น คุณวุฒิวิชาชีพ/ใบรับรอง ทักษะ ความรู้ และประสบการณ์ที่เกี่ยวข้อง) เพื่อดำเนินการตรวจสอบ

ทั้งนี้ หน่วยงานอาจพิจารณาแตกต่างกันไปตามแต่ละหน่วยงานจะเห็นสมควร ในประเด็นดังต่อไปนี้ (๑) จำนวนผู้ตรวจสอบของแต่ละหน่วยงาน (๒) ระยะเวลาในการขออนุญาต เช่น รายปีหรือตามรอบการตรวจสอบ เป็นต้น ในกรณีที่ผู้ตรวจสอบของสถาบันที่ลงทะเบียนแล้วลาออกจากการเป็นเจ้าหน้าที่ก่อนการดำเนินการตรวจสอบ หรือมีการเปลี่ยนแปลงเจ้าหน้าที่ที่ลงทะเบียนไว้แล้วสถาบันจะแจ้ง ศทท. ภายใน ๓๐ วัน นับจากวันที่มีการเปลี่ยนแปลงอย่างเป็นทางการของหน่วยงาน

๑.๖ ความคาดหวังในการตรวจสอบ

การกำหนดความคาดหวังในการตรวจสอบ ช่วยให้เข้าใจว่า ผู้ตรวจสอบควรจะดำเนินการและรายงานผลการตรวจสอบความมั่นคงปลอดภัยไซเบอร์อย่างไร

๑.๖.๑ หลักการตรวจสอบ

การตรวจสอบควรยึดหลักการต่อไปนี้เพื่อให้ข้อสรุปการตรวจสอบที่เกี่ยวข้องและเพียงพอ ทั้งนี้เพื่อช่วยให้ผู้ตรวจสอบซึ่งทำงานอย่างอิสระสามารถบรรลุข้อสรุปที่คล้ายคลึงกันในสถานการณ์ที่คล้ายคลึงกัน

(๑) ความซื่อสัตย์ (Integrity) ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ ปราศจากอคติ มีความยุติธรรมและเป็นกลาง ปราศจากอิทธิพลใด ๆ ที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบ

(๒) การนำเสนออย่างยุติธรรม (Fair Presentation) รายงานตามความเป็นจริง และตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจน และครบถ้วน

(๓) การปฏิบัติอย่างมืออาชีพ (Due Professional Care) มีความรอบคอบและวิจารณญาณในการตรวจสอบอย่างระมัดระวัง และใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

(๔) การรักษาความลับ (Confidentiality) ใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบและรักษาความลับ ไม่ใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหาย

(๕) ความเป็นอิสระ (Independence) ตรวจสอบด้วยความเป็นอิสระ แต่คงไว้ซึ่งเที่ยงธรรมปราศจากอคติและผลประโยชน์ทับซ้อนในทุกกรณี

๑.๖.๒ ข้อค้นพบการตรวจสอบ

สิ่งที่ผู้ตรวจสอบควรมุ่งเน้น ได้แก่

(๑) เน้นการค้นหาอย่างเป็นระบบ (Systemic Finding)

(๒) เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบสิ่งที่เคยเกิดขึ้นในอดีตแม้ว่าจะมีการแก้ไข (Corrective Action) แล้วก็ตาม

(๓) เน้นแนวปฏิบัติที่ดี(Good Practices) ในด้านการก ากับดูแลและการควบคุม

บทที่ ๒
หลักการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

๒.๑ หลักการตรวจสอบ

หลักการตรวจสอบควรยึดหลักการดังต่อไปนี้

๒.๑.๑ ความซื่อสัตย์ (Integrity) คือ รากฐานของความเป็นมืออาชีพ

๑) ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ

๒) ทำให้แน่ใจว่ามีความสามารถในขณะดำเนินการตรวจสอบ

๓) ดำเนินการตรวจสอบอย่างเป็นกลาง

๔) ทำให้แน่ใจว่ามีความยุติธรรมและเป็นกลางในการติดต่อทั้งหมด ระมัดระวังต่ออิทธิพลใด ๆ ที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ

๒.๑.๒ การนำเสนออย่างยุติธรรม (Fair Presentation) คือ หน้าที่ในการรายงานตามความเป็นจริงและถูกต้อง

๑) ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง

๒) รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่างทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ

๓) ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจนและครบถ้วน

๒.๑.๓ การปฏิบัติอย่างมืออาชีพ (Due Professional Care) คือ การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ

๑) ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ

๒) ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

๒.๑.๔ การรักษาความลับ (Confidentiality) คือ ความมั่นคงปลอดภัยของข้อมูล

๑) ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ

๒) ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ตรวจสอบ

๓) จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม

๒.๑.๕ ความเป็นอิสระ (Independence) คือ พื้นฐานสำหรับความเป็นกลางของการตรวจสอบ และความเที่ยงธรรมของข้อสรุปการตรวจสอบ

๑) ตรวจสอบความเป็นอิสระของกิจกรรมที่กำลังตรวจสอบ

๒) ดำเนินการในลักษณะที่ปราศจากอคติและผลประโยชน์ทับซ้อนในทุกกรณี

๓) รักษาความเป็นกลางตลอดกระบวนการตรวจสอบ

๔) ตรวจสอบให้แน่ใจว่าผลการตรวจสอบและข้อสรุปขึ้นอยู่กับหลักฐานการตรวจสอบ (Audit Evidence) เท่านั้น

๒.๒ วัตถุประสงค์ในการตรวจสอบ

การตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ มีวัตถุประสงค์ ดังนี้

๒.๒.๑ ตรวจสอบการปฏิบัติตามของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย และคำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

๒.๒.๒ ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงานตามหลักการบริหารความเสี่ยง

๒.๓ ขอบเขตการตรวจสอบ

การตรวจสอบจะครอบคลุมสิ่งต่อไปนี้

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

๒.๔ แนวทางการตรวจสอบ

การตรวจสอบควรใช้ทั้งแนวทางการปฏิบัติตามข้อกำหนด (Compliance Approach) และตามความเสี่ยง (Risk-Based Approach)

๒.๔.๑ การปฏิบัติตามข้อกำหนด

ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

๒.๔.๒ ตามความเสี่ยง

ระบุความเสี่ยงและภัยคุกคามที่หน่วยงานเผชิญ และตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคาม

๒.๕ ข้อค้นพบการตรวจสอบ

ผู้ตรวจสอบควรตรวจสอบโดยมุ่งเน้นสิ่งต่อไปนี้

๒.๕.๑ ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

๒.๕.๒ เน้นการค้นหาอย่างเป็นระบบ (Systemic Finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงาน ซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม

๒.๕.๓ เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำในการตรวจสอบปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (Corrective Action) แล้วก็ตาม

๒.๕.๔ เน้นแนวปฏิบัติที่ดี (Good Practices) ในด้านการกำกับดูแลและการควบคุม ซึ่งระบุไว้ในระหว่างการตรวจสอบ และเมื่อผู้ตรวจสอบทำการตรวจสอบแล้วลำทำการเสนอข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรระบุคุณลักษณะต่อไปนี้ของข้อค้นพบ การตรวจสอบอย่างชัดเจนอย่างน้อย ดังนี้

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

๒.๖ ขั้นตอนการปฏิบัติในการตรวจสอบ

๒.๖.๑ ผู้ตรวจสอบทำการวางแผน และจัดทำแผนการตรวจสอบพร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง

๒.๖.๒ ผู้ตรวจสอบและคณะทำงานของหน่วยงานร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตถุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

๑) เพื่อชี้แจงวัตถุประสงค์ ขอบเขต และแผนการตรวจสอบ

๒) การสรุปวิธีการตรวจสอบ เกณฑ์การพิจารณา และกิจกรรมที่จะทำการตรวจสอบ

๓) การกำหนดผู้รับผิดชอบหรือช่องทางการสื่อสาร

๔) การชี้แจงรูปแบบการรายงาน และการปิดตรวจสอบ

๕) ยืนยันแผนการตรวจสอบ

๒.๖.๓ ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานทำหน้าที่ตอบข้อซักถามและจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๖.๔ ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้น โดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

๑) ยืนยันข้อค้นพบการตรวจสอบจากการตรวจสอบ

๒) ระดับความไม่สอดคล้องของข้อตรวจพบ

๓) ข้อเสนอแนะในการปรับปรุง

๔) สรุปผลการตรวจสอบ

๕) กำหนดการตรวจติดตาม (ถ้ามี)

๒.๖.๕ ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

๒.๖.๖ คณะทำงานรับทราบผลการตรวจสอบ

๒.๖.๗ ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้องจากข้อตรวจพบลงแบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report Form : NCR) ของหน่วยงาน และจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนด เพื่อรักษาความลับในการตรวจสอบ

๒.๖.๘ คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

๒.๖.๙ คณะทำงานดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของหน่วยงาน

๒.๖.๑๐ ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน

บทที่ ๓
การสรุปผลการตรวจสอบ

๓.๑ การสรุปผลการตรวจสอบ

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่อง ดังต่อไปนี้

๓.๑.๑ ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ

๓.๑.๒ ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของหน่วยงาน

๓.๒ รูปแบบรายงานการตรวจสอบ

ผู้ตรวจสอบควรจัดทำรายงานการตรวจสอบ โดยมีรายละเอียดอย่างน้อย ดังนี้

เนื้อหา	คำอธิบาย (Description)
บทสรุปผู้บริหาร (Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหาความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและ ประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคง ปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯ)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๒.๒ ของเอกสารนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๒.๓ ของเอกสารนี้
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง ในส่วนคำอธิบายควรระบุ ดังนี้ ๑) มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่และขอบเขตของการพึ่งพาดังกล่าว ๒) ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์คำแนะนำการตรวจสอบเอกสาร) และวิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)

เนื้อหา	คำอธิบาย (Description)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในส่วน ๒.๕ ของเอกสารนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในส่วน ๓.๑ ของเอกสารนี้

๓.๓ การติดตามและรายงานผล

กำหนดให้ผู้รับผิดชอบรายงานผลการดำเนินการซักซ้อมฯ ให้ผู้บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) ประจำ สนข. ทราบ เพื่อรายงานสรุปให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) ทราบ เป็นลำดับชั้นไป และหากมีเหตุฉุกเฉินร้ายแรงต้องรีบรายงานให้ผู้บริหารสูงสุดของหน่วยงานทราบโดยทันที

เอกสารอ้างอิง

๑. แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. GUIDELINES FOR AUDITING CRITICAL INFORMATION INFRASTRUCTURE, Cyber Security Agency of Singapore, JANUARY ๒๐๒๐

๓. SO ๑๙๐๑๑:๒๐๑๘ Guidelines for auditing management systems, ISO, July ๒๐๑๘

ผู้จัดทำร่าง

๑. นายทรงเกียรติ ตะเภาทอง
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

ที่ปรึกษา

๑. นางสาวจิรังรัก ห้วยหงษ์ทอง
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

๒. นายนฤทธิ์ มัยรัตน์
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร