# แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
# ของสำนักงานเศรษฐกิจการคลัง

| | |
|---|---|
| วัตถุประสงค์การตรวจประเมิน (Objective) : | เพื่อตรวจประเมินความสอดคล้องของการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีต่อ<br>๑) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ (พระราชบัญญัติฯ)<br>๒) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ ๒๕๖๔ (ประมวลฯ)<br>๓) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๕ (นโยบายฯ) |
| เกณฑ์/มาตรฐานที่ใช้ในการตรวจประเมิน (Audit Criteria) : | ๑) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒<br>๒) ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ ๒๕๖๔<br>๓) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๕ |
| ขอบเขตที่ตรวจประเมิน (Scope of Audit) : | การรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบเทคโนโลยีสารสนเทศของสำนักงานเศรษฐกิจการคลัง (สศค.) ซึ่งสนับสนุนการทำงานของ สศค. ที่ศูนย์เทคโนโลยีสารสนเทศ (ศทส.) ถนนพระรามที่ ๖ อารีย์สัมพันธ์ แขวงพญาไท เขตพญาไท กรุงเทพฯ ๑๐๔๐๐ |

/Opening Meeting ...

| ระยะเวลาดำเนินการ | ข้อกำหนดในการตรวจประเมิน (Area of Audit) | ผู้ตรวจประเมิน | ผู้รับการตรวจประเมิน | หมายเหตุ |
|---|---|---|---|---|
| ภายในปีงบประมาณ ๒๕๖๙ | Opening Meeting (ประชุมชี้แจงแผนการตรวจ) | ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบภายนอก | ศทส. และผู้เกี่ยวข้อง | |
| ภายในปีงบประมาณ ๒๕๖๙ | สัมภาษณ์ผู้บริหารระดับสูงของหน่วยงาน<br>- ทิศทางการบริหารจัดการ<br>- วิสัยทัศน์ พันธกิจ กลยุทธ์ และวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์<br>- บทบาท หน้าที่ และความรับผิดชอบ<br>- การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)<br>- การบริหารความเสี่ยง (Risk Management)<br>- นโยบาย และแนวปฏิบัติ (Policies and Guidelines) | ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบภายนอก | ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO) | พระราชบัญญัติฯ มาตรา ๔๒, ๔๓, ๔๔, ๔๕, ๔๖, ๕๒, ๕๔, ๕๕, ๕๖, ๕๗, ๕๘<br>ประมวลฯ ข้อ ๑๗, ๑๘, ๑๙<br>นโยบายฯ ข้อ ๑, ๒, ๓ |

/ระยะเวลา ...

| ระยะเวลาดำเนินการ | ข้อกำหนดในการตรวจประเมิน (Area of Audit) | ผู้ตรวจประเมิน | ผู้รับการตรวจประเมิน | หมายเหตุ |
|---|---|---|---|---|
| ภายในปีงบประมาณ ๒๕๖๙ | สอบถามแนวทางปฏิบัติของหน่วยงาน ตามพระราชบัญญัติฯ ตามประมวลฯ และตามนโยบายฯ โดยมีหัวข้อ ดังนี้<br>๑. การจัดทำแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์<br>- หน่วยงานมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง หรือไม่<br>- หน่วยงานมีการส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จ หรือไม่<br>- หน่วยงานมีการจัดทำแผนดำเนินการแก้ไขอย่างไร<br>- หน่วยงานมีขั้นตอนการปรับปรุงแผนหรือไม่หากมีการทักท้วงจากผู้ตรวจประเมิน<br>- หน่วยงานมีการดำเนินการแก้ไขให้อยู่ในกรอบระยะเวลาอย่างไร และมีการติดตามผลอย่างไร<br>๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์<br>- หน่วยงานมีการประเมินความเสี่ยง (Risk Assessment) อย่างไร<br>- หน่วยงานมีการจัดการความเสี่ยง (Risk Treatment) อย่างไร | ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบภายนอก | ศทส. | พระราชบัญญัติฯ มาตรา ๔๒, ๔๓, ๔๔, ๔๕, ๔๖, ๕๒, ๕๔, ๕๕, ๕๖, ๕๗, ๕๘ ประมวลฯ ข้อ ๑๗, ๑๘, ๑๙ นโยบายฯ ข้อ ๑, ๒, ๓ |

/๓. ระยะเวลา ...

| ระยะเวลาดำเนินการ | ข้อกำหนดในการตรวจประเมิน (Area of Audit) | ผู้ตรวจประเมิน | ผู้รับการตรวจประเมิน | หมายเหตุ |
|---|---|---|---|---|
| | - หน่วยงานมีการติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review) อย่างไร<br>- หน่วยงานมีการรายงานความเสี่ยง (Risk Reporting) อย่างไร<br>๓. การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์<br>- หน่วยงานมีการจัดทำแผน มีการสื่อสาร และมีการทบทวนแผนการรับมืออย่างไร<br>๔. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)<br>- หน่วยงานมีการกำกับดูแลที่ดี ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างไร<br>๕. นโยบาย และแนวปฏิบัติ (Policies and Guidelines)<br>- หน่วยงานมีการจัดทำ นโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างไร | | | |

/ระยะเวลา ...

| ระยะเวลาดำเนินการ | ข้อกำหนดในการตรวจประเมิน (Area of Audit) | ผู้ตรวจประเมิน | ผู้รับการตรวจประเมิน | หมายเหตุ |
|---|---|---|---|---|
| ภายในปีงบประมาณ ๒๕๖๙ | **การระบุความเสี่ยง (Identify)**<br>- การจัดการทรัพย์สิน (Asset Management)<br>- การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)<br>- การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)<br>- การจัดการผู้ให้บริการภายนอก (Third Party Management) | ผู้ตรวจสอบภายใน<br>หรือ<br>ผู้ตรวจสอบภายนอก | ศทส. | พระราชบัญญัติฯ มาตรา ๕๔, ๕๕ ประมวลฯ ข้อ ๒๑ นโยบายฯ ข้อ ๒ |
| ภายในปีงบประมาณ ๒๕๖๙ | **มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)**<br>- การควบคุมการเข้าถึง (Access Control)<br>- การทำให้ระบบมีความแข็งแกร่ง (System Hardening)<br>- การเชื่อมต่อระยะไกล (Remote Connection)<br>- สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)<br>- การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)<br>- การแบ่งปันข้อมูล (Information Sharing) | ผู้ตรวจสอบภายใน<br>หรือ<br>ผู้ตรวจสอบภายนอก | ศทส. | พระราชบัญญัติฯ มาตรา ๕๔, ๕๕ ประมวลฯ ข้อ ๒๒ นโยบายฯ ข้อ ๓ |
| ภายในปีงบประมาณ ๒๕๖๙ | **มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)**<br>- การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) | ผู้ตรวจสอบภายใน<br>หรือ<br>ผู้ตรวจสอบภายนอก | ศทส. | พระราชบัญญัติฯ มาตรา ๕๖, ๕๗, ๕๘ ประมวลฯ ข้อ ๒๓ นโยบายฯ ข้อ ๑ |

/ระยะเวลา ...

| ระยะเวลาดำเนินการ | ข้อกำหนดในการตรวจประเมิน (Area of Audit) | ผู้ตรวจประเมิน | ผู้รับการตรวจประเมิน | หมายเหตุ |
|---|---|---|---|---|
| ภายในปีงบประมาณ ๒๕๖๙ | **มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)**<br>- แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)<br>- แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)<br>- การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) | ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบภายนอก | ศทส. | พระราชบัญญัติฯ มาตรา ๕๖, ๕๗, ๕๘ ประมวลฯ ข้อ ๒๔ นโยบายฯ ข้อ ๑ |
| ภายในปีงบประมาณ ๒๕๖๙ | **มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)**<br>- การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)<br>- การรายงานผลต่อคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ | ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบภายนอก | ศทส. | พระราชบัญญัติฯ มาตรา ๕๖, ๕๗, ๕๘ ประมวลฯ ข้อ ๒๕ นโยบายฯข้อ ๑ |

/ระยะเวลา ...

| ระยะเวลาดำเนินการ | ข้อกำหนดในการตรวจประเมิน (Area of Audit) | ผู้ตรวจประเมิน | ผู้รับการตรวจประเมิน | หมายเหตุ |
|---|---|---|---|---|
| ภายในปีงบประมาณ ๒๕๖๙ | Auditor Time ประชุมคณะผู้ตรวจประเมิน | ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบภายนอก | - | |
| ภายในปีงบประมาณ ๒๕๖๙ | สรุปผลการตรวจประเมินภายใน ร่วมกับทีมผู้ตรวจประเมินและผู้ที่เกี่ยวข้อง | ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบภายนอก | ศทส. | |