สรุปเนื้อหาสาระสำคัญ

สาระสำคัญขององค์ความรู้ แนวทางการตรวจสอบระบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย

ประเภทของการตรวจสอบระบบสารสนเทศ

๑. การตรวจสอบการควบคุมทั่วไป

๒. การตรวจสอบการควบคุมทางด้านเทคนิค

๓. การตรวจสอบระบบงาน

๔. การใช้เทคนิคคอมพิวเตอร์ช่วยในการตรวจสอบ

ประเด็นการตรวจสอบที่ ๑

- นโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

วัตถุประสงค์

๑. เพื่อให้มั่นใจว่าหน่วยงานกำหนดนโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒. เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินการที่ไม่เป็นไปตามกฎหมายและประกาศ รวมทั้งให้ข้อเสนอแนะ ข้อสังเกต และ/หรือข้อคิดเห็นเกี่ยวกับการแก้ไขปรับปรุงเพื่อการปฏิบัติงานให้มีประสิทธิภาพ

ประเด็นการตรวจสอบที่ ๒

- หน่วยงานดำเนินการควบคุมความปลอดภัยตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

วัตถุประสงค์

๑. เพื่อให้มั่นใจว่า หน่วยงานดำเนินการควบคุมความปลอดภัย ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๒. เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินการที่ไม่เป็นไปตามกฎหมาย รวมทั้งให้ข้อเสนอแนะ ข้อสังเกต และ/หรือข้อคิดเห็นเกี่ยวกับการแก้ไขปรับปรุงเพื่อการปฏิบัติงานให้มีประสิทธิภาพ

ประเด็นการตรวจสอบที่ ๓

- หน่วยงานดำเนินการควบคุมตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

วัตถุประสงค์

๑. เพื่อให้มั่นใจว่าหน่วยงานดำเนินการควบคุมตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

๒. เพื่อให้ทราบปัญหาอุปสรรค และสาเหตุในการดำเนินการที่ไม่เป็นไปตามประกาศ รวมทั้งให้ข้อเสนอแนะ ข้อสังเกต และ/หรือข้อคิดเห็นเกี่ยวกับการแก้ไขปรับปรุงเพื่อการปฏิบัติงานให้มีประสิทธิภาพ

กฎหมายและประกาศที่เกี่ยวข้อง

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

การตรวจสอบระบบสารสนเทศ เฉพาะการควบคุมทั่วไป (General Control)

วัตถุประสงค์

1. ป้องกันสินทรัพย์จากการทุจริต ผิดพลาด
2. รักษาความถูกต้องของข้อมูล
3. ความมีประสิทธิผลของระบบงาน
4. ความมีประสิทธิภาพในการใช้ทรัพยากรของระบบ

การควบคุม

1. การควบคุมทั่วไป (General Control)
2. การควบคุมระบบงาน (Application Control)

การควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุม นโยบายและวิธีการในการควบคุมระบบสารสน เทศ การควบคุมความปลอดภัย การควบคุมการพัฒนาและปรับปรุง และการป้องกัน/ลดความเสียหายของระบบ เป็นการควบคุมภายในสำหรับองค์กรในภาพรวมหรือควรมีในทุก ๆ ส่วนของระบบสารสนเทศ ตัวอย่างเช่น

1. การกำหนดนโยบายในการใช้สารสนเทศ *2. การแบ่งแยกหน้าที่งานในระบบสารสนเทศ*
3. การควบคุมโครงการพัฒนาระบบสารสนเทศ *4. การควบคุมการเปลี่ยนแปลงแก้ไขระบบ*
5. การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์ *6. การควบคุมเข้าถึงอุปกรณ์คอมพิวเตอร์*
7. การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ *8. การควบคุมการเข้าถึงระบบงาน*

เป็นการควบคุมที่กำหนดขึ้นเพื่อให้มั่นใจในความครบถ้วนสมบูรณ์ ถูกต้อง ได้รับการอนุมัติ และเกิดขึ้นอย่างถูกต้องตามกฎหมาย ระเบียบและนโยบาย ของรายการทั้งหมดที่นำเข้าสู่การประมวลผลของระบบงาน ความถูกต้องการประมวลผล และการแสดงผลลัพธ์การควบคุมในระบบงาน มีผลกระทบแต่เพียงการประมวลผลในระบบงานนั้นเท่านั้น แบ่งเป็น

1. การควบคุมข้อมูลเบื้องต้น จะช่วยทำให้เกิดความถูกต้อง ความเป็นเหตุเป็นผล และความครบถ้วนของข้อมูลนำเข้า เช่น การพิสูจน์การพิมพ์ข้อมูล การพิสูจน์ตัวเลขตรวจสอบ การทดสอบการเรียงลำดับของเอกสารที่ให้เลขที่ไว้ล่วงหน้า

2. โปรแกรมตรวจสอบความถูกต้องของข้อมูลนำเข้า เช่น การตรวจสอบฟิลด์ที่ขาดข้อมูล การตรวจสอบเครื่องหมาย การตรวจสอบความถูกต้อง การตรวจสอบขีดจำกัด การตรวจสอบโดยใช้ข้อมูลมากกว่าหนึ่งฟิลด์ การตรวจสอบการเรียงลำดับ การตรวจสอบชนิดของฟิลด์ การทดสอบความสมเหตุสมผล

3. การควบคุมการประมวลผลข้อมูลและการเก็บรักษาแฟ้มข้อมูล

4. การควบคุมส่วนผลลัพธ์

ปัญหาด้านความปลอดภัยของระบบสารสนเทศที่มีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ และมีแนวโน้มที่จะสูงผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทั้งในส่วนของผู้ประกอบการ องค์กรภาครัฐและภาคเอกชนที่มีการดำเนินงานในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ทำให้หน่วยงานเหล่านั้นขาดความเชื่อมั่นต่อการทำธุรกิจในทุกรูปแบบ และเพื่อเป็นการป้องกันและแก้ไขปัญหาดังกล่าว จึงได้มีการกำหนดกฎหมายและประกาศเพิ่มเติม ได้แก่

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ตามประกาศคณะกรรมการธุรกรรมฯ ในข้อ 13 (2) กำหนดให้หน่วยงานของรัฐจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยผู้ตรวจสอบภายใน

หน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัย (External Auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับ ความเสี่ยง และระดับความมั่นคงปลอดภัยของสารสนเทศของหน่วยงาน

แนวทางการประกันคุณภาพงานตรวจสอบภายในภาครัฐ กำหนดมาตรฐานดานคุณสมบัติรหัส 1210.A3 ว่า ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านเทคโนโลยีสารสนเทศ ซึ่งได้แก่ การควบคุมที่สนับสนุนการบริหารจัดการและการกำกับดูแล โดยจัดให้มีระบบการควบคุมในส่วนโครงสร้างพื้นฐานด้านสารสนเทศ เชน ระบบงานขอมูล ระบบเครือข่าย และบุคลากร ซึ่งประกอบด้วยการควบคุมทั่วไป (General Controls) และแบบเฉพาะทาง (Technical Controls) รวมถึงเทคนิควิธีการตรวจสอบด้านเทคโนโลยีสารสนเทศ และประเด็นที่ใช้พิจารณา : การวางแผนตรวจสอบ การเสนอ และอนุมัติแผนการตรวจสอบ กำหนดให้การวางแผนการตรวจสอบครอบคลุมประเภทงานให้ความเชื่อมั่นควรครอบคลุมการตรวจสอบด้านสารสนเทศด้วย