แผนการปฏิบัติงานตรวจสอบ
ระบบความมั่นคงปลอดภัยด้านสารสนเทศ

ปัจจุบันเทคโนโลยีสารสนเทศเพื่อการสื่อสาร มีความก้าวหน้าอย่างรวดเร็ว การทำธุรกรรมในระบบอิเล็กทรอนิกส์ขยายตัวเพิ่มมากขึ้น หน่วยงานภาครัฐจึงได้รับการสนับสนุนให้มีการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว ซึ่งจะเป็นการเพิ่มประสิทธิภาพและประสิทธิผลในการให้บริการ และเพื่อให้หน่วยงานภาครัฐสามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภายใต้มาตรฐานเดียวกัน และเพื่อเป็นการสร้างความเชื่อมั่นต่อประชาชน จึงได้มีการตราพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2549 ขึ้นตามลำดับ

แต่อย่างไรก็ตาม สิ่งที่พัฒนาพร้อมกับความก้าวหน้าทางด้านเทคโนโลยี คือ ปัญหาด้านความปลอดภัยของระบบสารสนเทศที่มีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ และมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทั้งในส่วนของผู้ประกอบการ องค์กร ภาครัฐ และภาคเอกชนที่มีการดำเนินงานในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ทำให้หน่วยงานเหล่านั้นขาดความเชื่อมั่นต่อการทำธุรกิจในทุกรูปแบบ และเพื่อเป็นการป้องกันและแก้ไขปัญหาดังกล่าว จึงได้มีการกำหนดกฎหมายและประกาศเพิ่มเติม ได้แก่ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ตามประกาศคณะกรรมการธุรกรรมฯ ในข้อ 13 (2) กำหนดให้หน่วยงานของรัฐจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัย (External Auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับ ความเสี่ยง และระดับความมั่นคงปลอดภัยของสารสนเทศของหน่วยงาน

กอปรกับมาตรฐานการตรวจสอบภายใน และแนวทางการประกันคุณภาพงานตรวจสอบภายในภาครัฐ กำหนดมาตรฐานด้านคุณสมบัติรหัส 1210.A3 ว่า ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านเทคโนโลยีสารสนเทศ ซึ่งได้แก่ การควบคุมที่สนับสนุนการบริหารจัดการและการกำกับดูแล โดยจัดให้มีระบบการควบคุมในส่วนโครงสร้างพื้นฐานด้านสารสนเทศ เช่น ระบบงานข้อมูล ระบบเครือข่าย และบุคลากร ซึ่งประกอบด้วย การควบคุมทั่วไป (General Controls) และแบบเฉพาะทาง (Technical Controls) รวมถึงเทคนิควิธีการตรวจสอบด้านเทคโนโลยีสารสนเทศ และประเด็นที่ใช้พิจารณา : การวางแผนตรวจสอบ การเสนอ และอนุมัติแผนการตรวจสอบ กำหนดให้ การวางแผนการตรวจสอบครอบคลุมประเภทงานให้ความเชื่อมั่นควรครอบคลุมการตรวจสอบด้านสารสนเทศ ด้วย

เพื่อให้การดำเนินงานของส่วนราชการเป็นไปตามกฎหมาย ประกาศแนวนโยบายฯ และผ่านเกณฑ์การประกันคุณภาพงานตรวจสอบภายในภาครัฐ กระทรวงศึกษาธิการจึงได้บูรณาการงานตรวจสอบภายในกับหน่วยงานในสังกัด ได้แก่ หน่วยงานหลัก และมหาวิทยาลัยในสังกัด

วัตถุประสงค์การตรวจสอบ

1. เพื่อให้มั่นใจว่า หน่วยงานจัดให้มีการควบคุมด้านการรักษาความปลอดภัยระบบสารสนเทศตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
2. เพื่อให้มั่นใจว่า หน่วยงานปฏิบัติงานด้านการรักษาความปลอดภัยระบบสารสนเทศตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
3. เพื่อให้ทราบปัญหา และอุปสรรคในการปฏิบัติงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอีเล็กทรอนิกส์ฯ และให้ข้อเสนอแนะเพื่อการพัฒนางาน

ขอบเขตและวิธีการตรวจสอบ

1. ดำเนินการสอบทานเอกสารหลักฐานที่เกี่ยวข้องกับการจัดให้มีการควบคุมและการปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ที่หน่วยงานใช้อยู่ในปัจจุบัน
2. ดำเนินการสุ่มสอบทานการปฏิบัติตามนโยบายและข้อปฏิบัติของหน่วยงาน
3. สังเกตการปฏิบัติงานจริงตามระบบควบคุมที่กำหนดตามนโยบายและข้อปฏิบัติ
4. สอบถามและสัมภาษณ์ ผู้บริหารและผู้ปฏิบัติงาน

ขั้นตอนการดำเนินงาน

1. ศึกษาข้อมูลพื้นฐานประกอบการตรวจสอบ แนวทางการปฏิบัติงานตรวจสอบ และกระดาษทำการ
2. ดำเนินการตรวจสอบโดย

2.1 แจ้งหน่วยรับตรวจ (หน่วยงานที่ดูแลระบบสารสนเทศขององค์กร) ถึงวันที่จะดำเนินการเปิดตรวจ

2.2 ประชุมเปิดตรวจเพื่อชี้แจงวัตถุประสงค์ ขอบเขต แนวทางและวิธีการตรวจสอบ พร้อมทั้งขอความร่วมมือในการให้ข้อมูล

2.3 ดำเนินการตรวจสอบตามแนวทางการปฏิบัติงานตรวจสอบ และบันทึกข้อมูลการตรวจสอบในกระดาษทำการ

2.4 เมื่อดำเนินการตรวจสอบแล้วเสร็จ ให้สรุปผลจากกระดาษทำการเก็บข้อมูลลงในกระดาษทำการสรุปผล

2.5 ประชุมปิดตรวจ เพื่อสรุปผลการตรวจสอบ ทำความเข้าใจ ชี้แจง และขอความเห็นเพิ่มเติมในบางประเด็นที่ยังเป็นที่สงสัย พร้อมขอบคุณผู้ที่มีส่วนเกี่ยวข้องในการให้ข้อมูลการตรวจสอบ

3. ร่างรายงานผลการตรวจสอบ พร้อมทั้งแจ้งให้หน่วยรับตรวจทราบผลเพื่อพิจารณาให้ความเห็น แล้วจัดทำรายงานผลการตรวจสอบพร้อมแนบความเห็นของหน่วยรับตรวจ เสนอผู้บริหารเพื่อพิจารณาสั่งการ

4. สำเนารายงานผลการตรวจสอบ ส่งกลุ่มตรวจสอบภายในระดับกระทรวง กระทรวงศึกษาธิการภายในเดือนมิถุนายน 2556

ข้อมูลพื้นฐานเพื่อประกอบการตรวจสอบ

1. **การตรวจสอบด้านสารสนเทศ** ตามมาตรฐานการตรวจสอบภายในของกรมบัญชีกลางที่กำหนดในมาตรฐานการตรวจสอบภายในรหัส 1210.A3 กำหนดให้ผู้ตรวจสอบภายในต้องมีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านสารสนเทศ

2. **โครงสร้างพื้นฐานด้านสารสนเทศ** ประกอบด้วย

   2.1 อุปกรณ์: Hardware

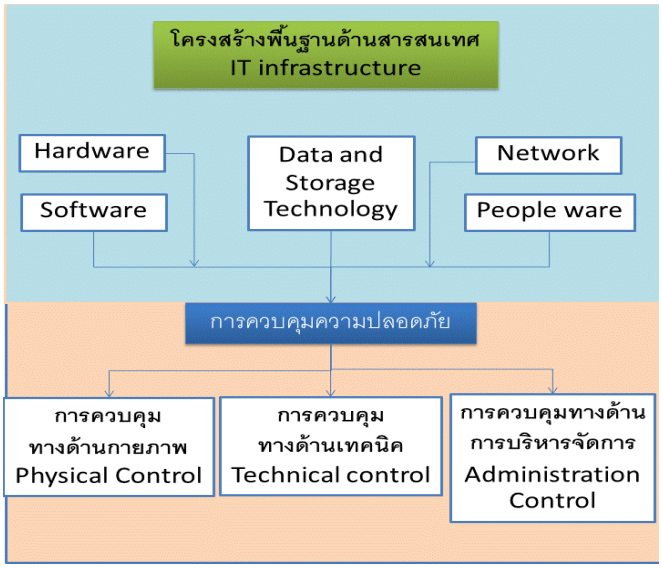
   2.2 โปรแกรม: Software

   2.3 ฐานข้อมูล: Data & Storage Technology

   2.4 เครือข่าย: Networks

   2.5 บุคลากร: People ware

ผังแสดงความเชื่อมโยงโครงสร้างพื้นฐานด้านสารสนเทศและการควบคุมความปลอดภัย



3. **การควบคุมความปลอดภัย** แบ่งเป็น 3 ด้าน คือ

   3.1 มุมมองทางด้านกายภาพ (Physical Control)

   3.2 มุมมองทางด้านเทคนิค (Technical Control)

   3.3 มุมมองทางด้านการบริหารจัดการ (Administrative Control)

การจำแนกงานตรวจสอบตามมุมมองการควบคุม จากมุมมองทางด้านการควบคุม ทำให้งานตรวจสอบทางด้าน IT แบ่งเป็น 3 ด้าน ได้แก่

3.1 ด้านกายภาพ

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

3.2 ด้านเทคนิค (Technical Control) ได้แก่

1). การตรวจสอบระบบปฏิบัติการ (NOS Audit) เช่น การตรวจสอบระบบ Server ที่ใช้ MS Windows เช่น Windows NT, Window 2000 Server ตลอดจน Workstation ที่ใช้ Windows XP เป็นต้น การตรวจสอบควรจะครอบคลุมถึงระบบปฏิบัติการอื่นด้วย เช่น การตรวจสอบระบบปฏิบัติการ Unix เช่น Sun Solaris, HP/UX, IBM AIX และ ระบบปฏิบัติการ Linux ที่ได้รับความนิยมเพิ่มขึ้นเรื่อยๆ

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

3). 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

4). การตรวจสอบโปรแกรมฐานข้อมูล (RDBMS Audit) เช่น การตรวจสอบ Oracle, IBM DB2, Microsoft SQL Server, Informix, SYBASE หรือ MySQL RDBMS การตรวจสอบโปรแกรมฐานข้อมูลควรกระทำ ควบคู่ไปกับการตรวจสอบระบบปฏิบัติการที่โปรแกรมฐานข้อมูลทำงานอยู่ เช่น Oracle ทำงานบน Unix เป็นต้น เพื่อที่จะเจาะลึกลงไปในด้านความปลอดภัยของตัวโปรแกรมฐานข้อมูลเองว่ามีช่องโหว่หรือไม่ ผู้ตรวจสอบควรเป็นผู้เชี่ยวชาญการใช้งานโปรแกรมฐานข้อมูลนั้นๆมาก่อน เพราะการตรวจสอบต้องใช้ความรู้เชิงลึกทางด้าน RDBMS ด้วย

5). การตรวจสอบโปรแกรมประยุกต์และโปรแกรมที่ให้บริการในลักษณะ Server (Application Specific Audit) เช่น การตรวจสอบ Web Server IIS บน Microsoft Windows Platform และ การตรวจสอบ Web Server Apache บน Unix/Linux Platform ซึ่งทั้ง 2 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 มีปัญหาจะทำให้ระบบไม่สามารถอ้างอิง Hostname ได้ ซึ่งจะก่อให้เกิดปัญหาใหญ่กับระบบ โดยรวม

3.3 ด้านการบริหารจัดการ (Administrative Control)

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

สำหรับการตรวจสอบระบบความมั่นคงปลอดภัยด้านสารสนเทศตามที่กำหนดนี้จะเป็นการตรวจสอบทางด้านกายภาพ และการตรวจสอบทางด้านการบริหารจัดการ

4. การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดในเรื่องต่อไปนี้

4.1 การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้แก่

1). การควบคุมระบบคอมพิวเตอร์ของหน่วยงานตาม มาตรา 15 เพื่อป้องกันผู้ใช้บริการที่เข้าไปกระทำความผิดตามพระราชบัญญัติคอมพิวเตอร์ เช่น นำเข้าข้อมูลอันเป็นเท็จทำให้เกิดความเสียหายต่อความมั่นคง สร้างความตื่นตระหนกต่อประชาชน หรือเผยแพร่ภาพลามกอนาจาร เป็นต้น

2). การเก็บข้อมูลจราจร ซึ่งหมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ และอื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ตามมาตรา 26 กำหนดให้หน่วยงานต้องจัดเก็บข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า 90 วันนับตั้งแต่การใช้บริการสิ้นสุดลง

การควบคุมทั้ง 2 เรื่องที่กล่าวมาข้างต้น หน่วยงานดำเนินการ ด้วยวิธีการ ดังนี้คือ

1). การควบคุมการเข้าสู่ระบบ (Access Control) ด้วยการกำหนด Username และ Password ให้กับผู้ใช้งาน

2). การเก็บ Log file ข้อมูลจราจรทางคอมพิวเตอร์ของหน่วยงาน

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

4.2 การควบคุมประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 กำหนดดังนี้

1). ให้จัดทำนโยบายและข้อปฏิบัติให้ครอบคลุมเนื้อหาตามที่ประกาศกำหนด

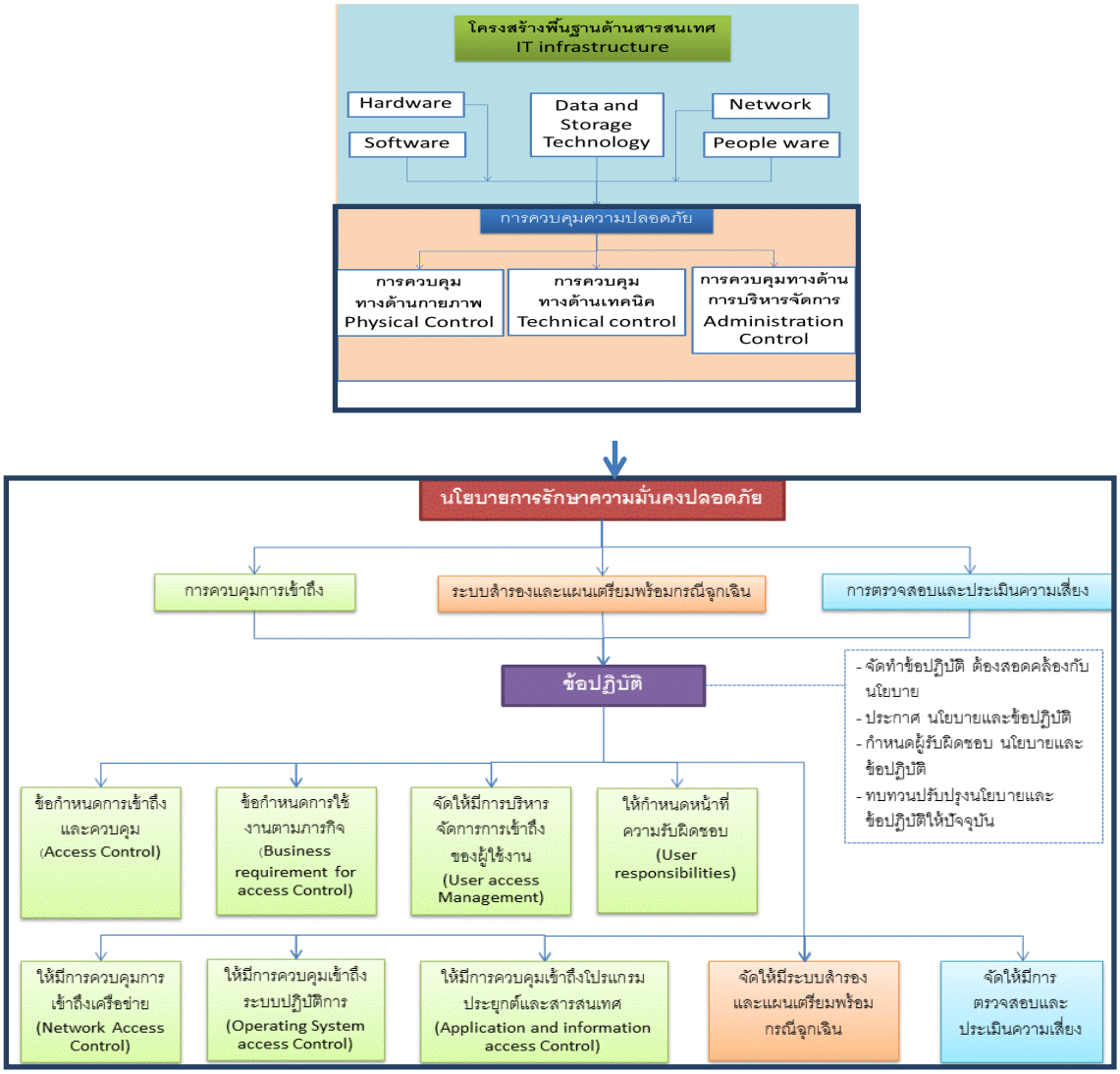
2). ให้ประกาศเผยแพร่นโยบายและข้อปฏิบัติ พร้อมทั้งทบทวนให้เป็นปัจจุบัน

3). ให้ปฏิบัติตามนโยบายและข้อปฏิบัติที่กำหนดและประกาศไว้

4). กรณีที่เกิดความเสียหายหรืออันตรายต่อองค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติ ผู้บริหารระดับสูงต้องรับผิดชอบต่อความเสียหายดังกล่าว

5). หน่วยงานสามารถเลือกใช้ข้อปฏิบัติที่ต่างจากประกาศได้ หากมีความเหมาะสมกว่าหรือเทียบเท่า

ผังแสดง ความเชื่อมโยงการควบคุมความปลอดภัยกับนโยบายและข้อปฏิบัติตามประกาศของหน่วยงาน



กรอบประเด็นการตรวจสอบ

ประเด็นที่ 1 นโยบายและข้อปฏิบัติเป็นไปตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ

1.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยและข้อปฏิบัติ คลอบคลุมข้อกำหนดตามกฎหมายและประกาศคณะกรรมการธุรกรรมฯ

1.2 การเผยแพร่นโยบายและข้อปฏิบัติ ให้ผู้ที่เกี่ยวข้องทราบสามารถเข้าถึงเข้าใจและปฏิบัติตามได้

1.3 กำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติที่ชัดเจน

1.4 ทบทวนนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ประเด็นที่ 2 การควบคุมตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ประเด็นที่ 3 การควบคุมตามประกาศคณะกรรมการธุรกรรมฯ

3.1 การเข้าถึงและการควบคุมการใช้งาน (Access Control)

3.1.1 การกำหนดการเข้าถึงสารสนเทศ

1). การควบคุมการเข้าถึงระบบสารสนเทศ

2). การควบคุมการเข้าถึงระบบเครือข่าย

3). การควบคุมการเข้าถึงระบบปฏิบัติการ

4). การควบคุมการเข้าถึงโปรแกรมประยุกต์ (Applications) และสารสนเทศ

3.1.2 การกำหนดการใช้งานตามภารกิจ

3.1.3 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

3.1.4 การกำหนดหน้าที่ความรับผิดชอบ

3.2 การจัดให้มีระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

3.3 การจัดให้มีการตรวจสอบและประเมินความเสี่ยง

นิยามศัพท์ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

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