คู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit)

หน่วยตรวจสอบภายใน

สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

คู่มือปฏิบัติงาน
การตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit)

สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศมีบทบาทในการดำเนินงานขององค์กรทั้งภาครัฐและภาคเอกชน ซึ่งสวพส. ได้นำระบบเทคโนโลยีสารสนเทศเข้ามาเป็นเครื่องมือในการขับเคลื่อนองค์กรทุกมิติ เป็นการตอบรับกับนโยบายภาครัฐ (ระบบ Thailand ๔.๐) ข้อมูลสารสนเทศและระบบเทคโนโลยี ซึ่งมีความจำเป็นอย่างมากที่ใช้เป็นเครื่องมือในการเพิ่มประสิทธิภาพการดำเนินงานให้บรรลุเป้าหมายด้วยความสะดวก รวดเร็ว ติดตามข้อมูลได้ตลอดเวลา หน่วยงานต่าง ๆ จึงต้องให้ความสำคัญกับความมั่นคงและการรักษาความปลอดภัยของสารสนเทศและระบบเทคโนโลยี เพื่อมิให้ก่อให้เกิดผลเสียต่อองค์กร

การตรวจสอบภายในเป็นเครื่องมือสำคัญของผู้บริหารที่สามารถสร้างความเชื่อมั่นและให้คำปรึกษาต่อการขับเคลื่อนองค์กรให้อยู่ภายใต้กฎระเบียบของภาครัฐ โดยมีระบบการควบคุมภายใน การบริหารความเสี่ยงการกำกับดูแล อย่างเพียงพอและเหมาะสม การตรวจสอบด้านเทคโนโลยีสารสนเทศ เป็นหนึ่งในประเภทงานตรวจสอบภายในที่กรมบัญชีกลางกำหนด ให้ผู้ตรวจสอบภายในต้องเป็นผู้ที่มีความรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมพื้นฐานด้านเทคโนโลยีสารสนเทศ รวมทั้งเทคนิค วิธีการตรวจสอบด้านเทคโนโลยีสารสนเทศ ตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ ส่วนที่ ๒ มาตรฐานด้านการปฏิบัติงาน รหัส ๒๑๒๐.A๑ : การปฏิบัติงานตรวจสอบภายในต้องประเมินความเสี่ยงที่เกี่ยวกับการกำกับดูแล การดำเนินงาน และระบบข้อมูลสารสนเทศฯ และรหัส ๒๑๓๐.A๑ : การปฏิบัติงานตรวจสอบภายในต้องประเมินถึงความเพียงพอและประสิทธิผลของการควบคุม เพื่อให้การควบคุมที่มีอยู่สามารถตอบสนองความเสี่ยงภายใต้การกำกับดูแล การดำเนินงานและระบบข้อมูลสารสนเทศในเรื่องต่างๆ แต่ปัญหาอุปสรรค คือ ยังไม่มีแนวทางการตรวจสอบที่ชัดเจน ดังนั้น หน่วยตรวจสอบภายใน สวพส. จึงได้จัดทำคู่มือการตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit) ของสถาบัน เพื่อให้ผู้ตรวจสอบภายในมีแนวทางปฏิบัติงานที่เป็นมาตรฐานเดียวกัน ลดการใช้ดุลยพินิจในการปฏิบัติงาน โดยให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องให้เป็นไปอย่างถูกต้อง มีประสิทธิภาพและประสิทธิผล ตลอดจนเพื่อให้ข้อเสนอแนะในการปรับปรุงการปฏิบัติงานที่เป็นประโยชน์ และพัฒนาระบบงานของ สวพส. ให้ดียิ่งขึ้นต่อไป หน่วยตรวจสอบภายใน หวังเป็นอย่างยิ่งว่าคู่มือการปฏิบัติงานฉบับนี้ จะเป็นประโยชนแก่ผู้ตรวจสอบภายใน ของ สวพส. และผู้ที่สนใจในการศึกษา และทำความเข้าใจในการปฏิบัติงานการตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit) ต่อไป

หน่วยตรวจสอบภายใน

สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

สิงหาคม ๒๕๖๗

สารบัญ

หน้า

บทที่ ๑
บทนำ

ความเป็นมา

ตามบทบัญญัติแห่งพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑ กระทรวงการคลัง ได้กำหนดหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสาหรับหน่วยงานของรัฐ พ.ศ. ๒๕๖๑ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๒ โดยกรมบัญชีกลางได้พิจารณากำหนดประเภทของงานตรวจสอบภายในไว้ตามหนังสือกรมบัญชีกลาง ที่ กค ๐๔๐๙.๒/ว ๖๑๔ ลงวันที่ ๒๓ ธันวาคม ๒๕๖๓ โดยกำหนดประเภทของงานตรวจสอบภายใน ดังนี้ **(๑) งานบริการให้ความเชื่อมั่น (Assurance Service)** ได้แก่ (๑.๑) การตรวจสอบการเงิน (Financial Audit) (๑. ๒) การตรวจสอบการปฏิบัติตาม กฎ ระเบียบ (Compliance Audit) (๑.๓) การตรวจสอบการดาเนินงาน (Performance Audit) และ (๑.๔) การตรวจสอบอื่น ๆ เช่น การตรวจสอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ และการตรวจสอบพิเศษ เป็นต้น **(๒) งานบริการให้คำปรึกษา (Consulting Service)** รวมทั้งหน่วยตรวจสอบภายในจะต้องประเมินความเสี่ยงของหัวข้อของงานตรวจสอบทั้งหมด (Audit Universe) พร้อมทั้ง รับนโยบายและความคิดเห็นจากหัวหน้าหน่วยงานของรัฐ และนาผลการประเมินความเสี่ยง นโยบายมาวางแผนการตรวจสอบประจำปีให้ครอบคลุมกับประเภทของงานตรวจสอบภายใน

หน่วยตรวจสอบภายใน ในฐานะที่เป็นหน่วยงานสร้างความเชื่อมั่นให้ผู้บริหารและช่วยสนับสนุนผู้ปฏิบัติงานในการบริหารงานและปฏิบัติงานของส่วนราชการให้บรรลุวัตถุประสงค์ด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุมและการกำกับดูแลอย่างเป็นระบบและเป็นระเบียบจากการวางแผนการตรวจสอบภายในประจำปี โดยที่ผ่านมาส่วนใหญ่เป็นการตรวจสอบด้านการเงิน (Financial Audit) การตรวจสอบการปฏิบัติตามกฎระเบียบ (Compliance Audit) และการตรวจสอบการดำเนินงาน (Performance Audit) เป็นสำคัญ อย่างไรก็ตาม ในการตรวจสอบเทคโนโลยีสารสนเทศ (IT Audit) ซึ่งเป็นส่วนหนึ่งของการตรวจสอบภายใน ได้มีการตรวจสอบและการรายงานผลการตรวจสอบเทคโนโลยีสารสนเทศของผู้ตรวจสอบภายในค่อนข้างน้อย ประกอบกับในปัจจุบันบทบาทของเทคโนโลยีสารสนเทศไม่ได้เพียงสนับสนุนการดำเนินงานของส่วนราชการเท่านั้น แต่ยังเป็นส่วนสำคัญในการช่วยส่วนราชการเพิ่มประสิทธิผลและประสิทธิภาพให้แก่กระบวนการทำงานต่างๆ และยังคงมีความเสี่ยงในการใช้งาน เช่น การบุกรุกเพื่อแก้ไขข้อมูลหรือปล่อยไวรัส ข้อมูลส่วนตัวรั่วไหล ระบบขัดข้องไม่สามารถทำงานได้ตามปกติ การลงทุนในเทคโนโลยีสารสนเทศไม่คุ้มค่า เป็นต้น หากส่วนราชการมีแนวทางการตรวจสอบและนำไปใช้ในการตรวจสอบดำเนินการเกี่ยวกับเทคโนโลยีสารสนเทศอย่างต่อเนื่องจะเป็นการช่วยให้บรรลุวัตถุประสงค์ของการควบคุมภายในด้านเทคโนโลยีสารสนเทศ อันได้แก่ การรักษาความลับของข้อมูล การประมวลผลที่ถูกต้อง ความพร้อมใช้และการรักษาความมั่นคงปลอดภัย จึงนับว่าการตรวจสอบเทคโนโลยีสารสนเทศมีความสำคัญอย่างมากเช่นเดียวกับประเภทการตรวจสอบภายในด้านต่างๆ ที่กรมบัญชีกลางกำหนด

การปฏิบัติงานตรวจสอบภายใน คือ กิจกรรมการให้ความเชื่อมั่นและการให้คำปรึกษา อย่างเที่ยงธรรม และเป็นอิสระ ซึ่งจัดให้มีขึ้นเพื่อเพิ่มคุณค่าและปรับปรุงการปฏิบัติงานของหน่วยงานของรัฐให้ดีขึ้น การตรวจสอบภายในจะช่วยให้หน่วยงานของรัฐบรรลุถึงเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ ด้วยการประเมิน และปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบ การปฏิบัติงานโดยอิสระปราศจาก

การแทรกแซงในการทำหน้าที่ตรวจสอบและประเมินผลการดำเนินกิจกรรมต่างๆ ภายในองค์กร ด้วยการปฏิบัติงานเกี่ยวกับการวิเคราะห์ ประเมิน ให้คำปรึกษา ให้ข้อมูลและข้อเสนอแนะ เพื่อสนับสนุนผู้ปฏิบัติงานทุกระดับขององค์กรให้สามารถปฏิบัติหน้าที่และดำเนินงานเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้องอย่างมีประสิทธิภาพยิ่งขึ้น จึงต้องได้รับการพัฒนาคุณภาพการบริหารจัดการของ หน่วยงานและบุคลากรอยู่เสมอ

วัตถุประสงค์

๑. เพื่อให้ผู้ตรวจสอบภายใน สวพส. มีคู่มือการปฏิบัติงานตรวจสอบเกี่ยวกับการตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit) ของสถาบัน ให้ปฏิบัติเป็นแนวทางเดียวกันและมีคุณภาพตามมาตรฐานการตรวจสอบภายในของส่วนราชการ

๒. เพื่อประเมินว่าระบบคอมพิวเตอร์ของ สวพส. มีความมั่นคงด้านข้อมูล มีการป้องกันทรัพย์สิน สามารถใช้ระบบได้อย่างมีประสิทธิภาพ และตอบสนองวัตถุประสงค์และบรรลุเป้าหมายได้อย่างมีประสิทธิผล

๓. เพื่อให้หน่วยตรวจสอบภายในสามารถสนับสนุนมาตรการหรือนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และข้อปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และประกาศธุรกรรมทางอิเล็กทรอนิกส์อย่างถูกต้อง

ขอบเขตและวิธีการตรวจสอบ

๑. ศึกษากฎหมาย ระเบียบ ข้อบังคับ นโยบายและแนวทางปฏิบัติที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของ สวพส.
๒. สอบทานการควบคุมภายในด้านสารสนเทศ การควบคุมทั่วไป (General Control) ของ สวพส. และวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จากข้อมูลและหลักฐานการปฏิบัติงานต่างๆ ที่เกี่ยวข้อง ติดตามผลการดำเนินงานตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สวพส.
๓. การสัมภาษณ์ผู้บริหารหรือผู้ปฏิบัติงานกระบวนการที่เกี่ยวข้อง

ประโยชน์ที่คาดว่าจะได้รับ

๑. ผู้ตรวจสอบภายใน สวพส. สามารถปฏิบัติงานตรวจสอบภายในเป็นแนวทางเดียวกันและมีคุณภาพตามมาตรฐานการตรวจสอบภายในของส่วนราชการ

๒. หน่วยตรวจสอบภายใน สามารถช่วยให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยมีการปฏิบัติงานกับระบบเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพถูกต้องตามกระบวนการ ไม่ละเมิดฝ่าฝืนกฎ ระเบียบ ข้อบังคับ กฎหมาย หรือมาตรฐาน

๓. สวพส. มีความมั่นใจในงานตรวจสอบภายในว่าสามารถสนับสนุนมาตรการป้องกัน ช่วยลดความเสี่ยง และมั่นใจว่าระบบงานเทคโนโลยีสารสนเทศของหน่วยงานไม่เกิดความเสี่ยงจากความไม่โปร่งใส

บทที่ ๒
การตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit)

คำนิยามศัพท์

“การตรวจสอบระบบงานสารสนเทศ” (Information System Auditing) เป็นการพิสูจน์ความถูกต้องและเชื่อถือได้ของระบบงานและข้อมูลที่ได้จากการประมวลผลด้วยคอมพิวเตอร์ รวมทั้งระบบการเข้าถึงข้อมูลในการปรับปรุงแก้ไขและการรักษาความปลอดภัยของข้อมูล

“การตรวจสอบด้านเทคโนโลยีสารสนเทศ” หมายถึง กิจกรรมการสร้างความเชื่อมั่น (Assurance) ต่อระบบเทคโนโลยีสารสนเทศ และการให้ข้อเสนอแนะรวมถึงแนวทางการปรับปรุงระบบงานด้านเทคโนโลยี สารสนเทศของหน่วยงานให้มีความสอดคล้องกับกฎ ระเบียบ และความเสี่ยงรวมถึงการตรวจสอบเพื่อช่วยให้หน่วยงานบรรลุเป้าหมายและวัตถุประสงค์ที่กำหนดไว้ ด้วยการประเมินและปรับปรุงประสิทธิผลของ กระบวนการควบคุมทั่วไปของระบบเทคโนโลยีสารสนเทศและการควบคุมเฉพาะระบบงาน

“การควบคุมภายในระบบเทคโนโลยีสารสนเทศ” หมายถึง กระบวนการหรือขั้นตอนการทำงานที่เป็น ผลมาจากการออกแบบ โดยผู้บริหาร หรือบุคลากรอื่นๆ ของหน่วยงาน เพื่อก่อให้เกิดความมั่นใจได้อย่าง สมเหตุสมผลว่าหน่วยงานจะสามารถบรรลุวัตถุประสงค์ความมีประสิทธิผล และประสิทธิภาพของการดำเนินงานระบบเทคโนโลยีสารสนเทศ

“ระบบเทคโนโลยีสารสนเทศ” (IT) หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลสารสนเทศ” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ระบบสารสนเทศ” หมายถึง ระบบของการจัดเก็บ ประมวลผลข้อมูล โดยอาศัยบุคคลและเทคโนโลยีสารสนเทศในการดำเนินการ เพื่อให้ได้สารสนเทศที่เหมาะสมกับงาน หรือภารกิจแต่ละอย่างหรือหมายถึงระบบที่ใช้ในการจัดเก็บ บันทึก ประมวลผล และจัดทำรายงานสารสนเทศให้ผู้บริหารและผู้ปฏิบัติใช้งานบางครั้งระบบสารสนเทศคือระบบสารสนเทศ คือระบบที่ใช้คอมพิวเตอร์ช่วยในการปฏิบัติงานนั่งเอง เช่น ระบบสารบรรณอิเล็กทรอนิกส์

“ผู้ตรวจสอบ” หมายถึง ผู้ตรวจสอบภายใน ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) (สวพส.)

“หน่วยรับตรวจ” หมายถึง หน่วยงานที่รับผิดชอบหรือเกี่ยวข้องกับกิจกรรมที่ดำเนินการตรวจสอบ

“กระดาษทำการ” หมายถึง เอกสารหลักฐานที่ได้มาจากการรวบรวมและจัดทำขึ้นในช่วงระยะเวลา ที่ถือปฏิบัติงานตรวจสอบภายใน อาจอยู่ในรูปแบบตาราง การวิเคราะห์เอกสาร หรือแบบฟอร์มที่จัดทำขึ้น เพื่อใช้บันทึกสรุปข้อตรวจพบ ผลการตรวจสอบ ซึ่งเป็นส่วนหนึ่งของภารกิจการตรวจสอบภายใน

IT Security หมายถึง ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (Information Technology Security) ซึ่งเป็นกระบวนการหรือมาตรการที่ใช้เพื่อปกป้องข้อมูล ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ จากการโจมตีหรือการบุกรุกที่อาจทำให้เกิดความเสียหายแก่ข้อมูล ความเสียหายทางการเงิน หรือการชีวิตของบุคคล โดยมุ่งเน้นไป

ที่การป้องกัน ตรวจสอบ และตอบสนองต่อความเสี่ยงที่เกิดจากการใช้เทคโนโลยีสารสนเทศและสารสนเทศที่ระบบต่างๆ ใช้งานอยู่ในรูปแบบที่ปลอดภัยที่สุด

การดำเนินการตามระบบ (Compliance) หมายถึง การปฏิบัติตามกฎหมาย ระเบียบ และมาตรฐานที่กำหนดขึ้นเพื่อให้ระบบสารสนเทศและเทคโนโลยีสารสนเทศปลอดภัย ซึ่งอาจเป็นการปฏิบัติตามกฎหมายที่เกี่ยวข้อง เช่น การปฏิบัติตาม GDPR (General Data Protection Regulation) ในยุโรป หรือ HIPAA (Health Insurance Portability and Accountability Act) ในสหรัฐอเมริกา เป็นต้น

Cyber Security (หรือเรียกว่า Security) จะเน้นไปที่การป้องกัน ตรวจสอบ และตอบสนองต่อความเสี่ยงจากการโจมตีทางด้านเทคโนโลยีสารสนเทศและความเสี่ยงที่เกิดจากภัยคุกคามทางด้านเทคโนโลยีอื่นๆ เช่น การป้องกันการเข้าถึงไม่จำเป็นเข้าสู่ระบบ (Unauthorized Access) การป้องกันการหลอกลวง (Phishing) การบุกรุกด้วยไวรัส (Malware) และการโจมตีทางด้านเครือข่าย (Network Attacks) ซึ่ง Cyber Security มุ่งเน้นไปที่การเพิ่มความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและสารสนเทศทั้งหมดขององค์กรได้มากที่สุด

แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินงานขององค์กรทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผลระบบงานสำคัญๆ ต่างๆ เทคโนโลยีสารสนเทศทำให้การดำเนินงานขององค์กรมีความสะดวกรวดเร็ว มีประสิทธิภาพ และเพิ่มโอกาสให้กับองค์กรต่างๆ อย่างไรก็ดี การใช้เทคโนโลยีสารสนเทศก็มีความเสี่ยงหลายประการ ดังนั้นการควบคุมความเสี่ยงด้านเทคโนโลยีจึงเป็นเรื่องที่ผู้ตรวจสอบภายในต้องให้ความสำคัญกับนโยบายที่จะกำกับดูแลและตรวจสอบเกี่ยวกับการบริหารจัดการการควบคุมความเสี่ยงอย่างจริงจัง เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการดำเนินงานขององค์กรให้เกิดประโยชน์สูงสุด

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑. ความเสี่ยงด้านความซื่อสัตย์ (Integrity Risk)
   - ความเสี่ยงจากความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์
   - สาเหตุ : การถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง ไม่มีระบบควบคุมและตรวจสอบ การบันทึกข้อมูล การประมวลผล และการแสดงผลอย่างเพียงพอ การจัดการและควบคุมการพัฒนาระบบคอมพิวเตอร์ไม่รอบคอบและรัดกุมเพียงพอ

๒. ความเสี่ยงด้านความพร้อมใช้งาน (Availability Risk)
   - ความเสี่ยงจากการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ
   - สาเหตุ : การไม่ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ ไม่มีการสำรองข้อมูลและระบบงานคอมพิวเตอร์ และไม่จัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน

๓. ความเสี่ยงในการเข้าถึงข้อมูล (Access Risk)

- ความเสี่ยงจากการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่ หรือบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ
- สาเหตุ : การกำหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจำเป็นการใช้งาน การไม่กำหนดรหัสผ่าน (Password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การไม่จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่เกี่ยวข้องในการเข้าออกศูนย์คอมพิวเตอร์

๔. ความเสี่ยงด้านโครงสร้างพื้นฐาน (Infrastructure Risk)

- ความเสี่ยงจากการไม่ได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี
- สาเหตุ : การแบ่งแยกอำนาจหน้าที่ไม่เหมาะสม ไม่มีนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ละเอียดเพียงพอในงานที่สำคัญ ไม่จัดให้มีระบบคอมพิวเตอร์และบุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการดำเนินงาน

ประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๑. ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ (IT Management Risk)

๑.๑ การควบคุมดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยผู้บริหารของหน่วยงาน (Oversight of Technology Risks)

๑.๒ การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Technology Management Risk)

๒. ความเสี่ยงด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (Operation Risk)

๒.๑ ความเสี่ยงเกี่ยวกับการรักษาความปลอดภัย (security)

- การรักษาความปลอดภัยให้กับโครงสร้างพื้นฐานของระบบปฏิบัติการ (Operational Infrastructure security Management) และการควบคุมการเข้าถึง (Access Controls)
- การควบคุมและป้องกันศูนย์ข้อมูล (Data Centers Protection and Controls)
- การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (Management of IT Outsourcing Risk)

๒.๒ ความเสี่ยงที่เกี่ยวกับความถูกต้องเชื่อถือได้ของข้อมูล (Data Integrity)

- การสร้างและพัฒนาระบบข้อมูล (Acquisition and Development of information Systems)

๒.๓ ความเสี่ยงที่เกี่ยวกับความพร้อมใช้งาน (Availability Risk)

- การบริหารจัดการบริการด้านเทคโนโลยีสารสนเทศ (IT Service Management)

- การทำให้ระบบเทคโนโลยีสารสนเทศมีความน่าเชื่อถือ พร้อมใช้งาน และสามารถนำกลับมาใช้งานใหม่ได้หากเกิดกรณีฉุกเฉิน (Systems Reliability Reliability, Availability and Recoverability)

๒.๔ ความเสี่ยงด้านชื่อเสียงและการปฏิบัติตามกฎหมาย (Reputation and Regulation)

เป็นเรื่องสำคัญที่องค์กรทุกแห่งต้องพิจารณาอย่างจริงจัง เพื่อปกป้องและรักษาความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย (stakeholders) และปฏิบัติตามข้อกำหนดทางกฎหมายอย่างเคร่งครัด นี่คือรายละเอียดของความเสี่ยงด้านชื่อเสียงและการปฏิบัติตามกฎหมาย:

ความเสี่ยงด้านชื่อเสียง (Reputation Risk)

๑. **สาเหตุของความเสี่ยง**:
   - **เหตุการณ์ฉุกเฉิน**: เช่น ข่าวลือไม่ดี หรือเหตุการณ์ที่ทำให้เกิดการเสียชื่อเสียง
   - **การให้บริการไม่ดี**: เช่น การร้องเรียนจากลูกค้า หรือผลิตภัณฑ์ที่ไม่เป็นไปตามมาตรฐาน
   - **การกระทำที่ผิดจรรยาบรรณ**: เช่น การทุจริตหรือการดำเนินการที่ไม่ซื่อสัตย์
๒. **ผลกระทบ**:
   - **การสูญเสียลูกค้า**: ความเชื่อมั่นของลูกค้าอาจลดลง
   - **ความเสียหายทางการเงิน**: การขายลดลงหรือการต้องจ่ายค่าชดเชย
   - **ปัญหาทางกฎหมาย**: การถูกฟ้องร้องหรือการถูกปรับ
๓. **การจัดการ**:
   - **การสร้างและรักษาภาพลักษณ์ที่ดี**: ใช้กลยุทธ์การสื่อสารที่มีประสิทธิภาพ
   - **การจัดการวิกฤต**: มีแผนการจัดการวิกฤตที่ชัดเจน
   - **การติดตามและประเมินผล**: การใช้เครื่องมือในการติดตามความคิดเห็นและความรู้สึกของลูกค้า

ความเสี่ยงด้านการปฏิบัติตามกฎหมาย (Regulation Risk)

๑. **สาเหตุของความเสี่ยง**:
   - **การไม่ปฏิบัติตามกฎหมาย**: เช่น การละเมิดข้อกำหนดหรือข้อบังคับ
   - **การเปลี่ยนแปลงในกฎหมาย**: เช่น การปรับปรุงหรือเพิ่มข้อกำหนดใหม่
   - **ข้อบังคับที่ไม่ชัดเจน**: การตีความที่ไม่ถูกต้องหรือการปฏิบัติตามที่ผิดพลาด
๒. **ผลกระทบ**:
   - **ค่าปรับและบทลงโทษ**: การถูกปรับหรือการถูกลงโทษทางกฎหมาย
   - **ความเสียหายต่อองค์กร** : เช่น การหยุดชะงักขององค์กร
   - **ความเสียหายทางชื่อเสียง**: การถูกเปิดเผยหรือรายงานเกี่ยวกับการละเมิด
๓. **การจัดการ**:
   - **การติดตามการเปลี่ยนแปลงทางกฎหมาย**: การอัปเดตข้อมูลเกี่ยวกับกฎหมายและข้อบังคับ
   - **การฝึกอบรมและให้ความรู้**: ฝึกอบรมพนักงานให้เข้าใจและปฏิบัติตามกฎหมาย
   - **การจัดทำเอกสารและบันทึก**: การรักษาบันทึกที่ชัดเจนเกี่ยวกับการปฏิบัติตามข้อกำหนด

การจัดการความเสี่ยงด้านชื่อเสียงและการปฏิบัติตามกฎหมายต้องการการวางแผนและการติดตามอย่างต่อเนื่อง เพื่อให้แน่ใจว่าองค์กรสามารถดำเนินงานได้อย่างราบรื่นและสามารถตอบสนองต่อปัญหาได้อย่างมีประสิทธิภาพ

บทบาทของการตรวจสอบภายในในการกำกับดูแลเทคโนโลยีสารสนเทศ

ความรับผิดชอบหลัก ในการกำกับดูแลเทคโนโลยีสารสนเทศเป็นของคณะกรรมการและผู้บริหารระดับอาวุโส กิจกรรมการตรวจสอบภายในจะทำหน้าที่ประเมินว่าการกำกับดูแลเทคโนโลยีสารสนเทศช่วยสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรตามที่กำหนดไว้ใน Standard ๒๑๑๐ หรือไม่

การดำเนินการและการปฏิบัติตามระเบียบข้อบังคับ

ผู้ตรวจสอบภายในจะต้องดำเนินการตรวจสอบทั้งในด้านการดำเนินการและการปฏิบัติตามระเบียบข้อบังคับ โดยการตรวจสอบการปฏิบัติตามระเบียบข้อบังคับมักมุ่งเน้นที่การดำเนินการตามกฎระเบียบภายนอกองค์กร รวมทั้งนโยบายและขั้นตอนการปฏิบัติงานภายในที่เกี่ยวข้อง ในขณะที่การตรวจสอบการดำเนินการต้องอาศัยการวิเคราะห์และการประเมินที่มากกว่า ว่าสิ่งใดผลักดันการดำเนินการในองค์กร เพื่อพัฒนาแนวการตรวจสอบที่มีประสิทธิผล การประเมินประสิทธิผลและประสิทธิภาพขององค์กรเป็นเรื่องที่ต้องทำและต้องใช้เพื่อพิจารณาว่าการกำกับดูแลเทคโนโลยีสารสนเทศในองค์กรรักษาและสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรหรือไม่

ในการกำหนดขอบเขตและดำเนินการตรวจสอบการกำกับดูแลเทคโนโลยีสารสนเทศ ทีมตรวจสอบภายในควร

- พิจารณาว่าหน้าที่ด้านเทคโนโลยีสารสนเทศมีความสอดคล้องและมีความเข้าใจในกลยุทธ์และวัตถุประสงค์ขององค์กรหรือไม่
- พิจารณาความมีประสิทธิผลของการบริหารทรัพยากรและการดำเนินการด้านเทคโนโลยีสารสนเทศ
- ประเมินความเสี่ยงที่อาจมีผลกระทบเชิงลบต่อสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

การกำกับดูแลเทคโนโลยีสารสนเทศ ประกอบด้วย ๕ องค์ประกอบ ดังนี้

๑. โครงสร้างองค์กรและการกำกับดูแล

แม้ว่ากิจกรรมการตรวจสอบภายในจะไม่สามารถกำหนดโครงสร้างองค์กร อนุมัติระเบียบวิธีการดำเนินการ หรือวางนโยบายได้ แต่ก็ควรสอบทานในเรื่องดังกล่าวให้มีความสมบูรณ์ ถูกต้อง และตรงประเด็น ขณะเดียวกันก็สนับสนุนกิจกรรมการกำกับดูแลเทคโนโลยีสารสนเทศในขอบเขตที่กำหนดในกฎบัตรการตรวจสอบภายในและใน IPPF โดยอาจรวมถึงกิจกรรมดังต่อไปนี้

- สอบทานโครงสร้างองค์กรเพื่อบ่งชี้ว่ามีตำแหน่ง CIO หรือไม่ และอยู่ในคณะผู้บริหารระดับอาวุโสหรือไม่
- ประเมินระดับที่กิจกรรมและมาตรฐานการกำกับดูแลสอดคล้องกับความเข้าใจของกิจกรรมการตรวจสอบภายในเกี่ยวกับระดับความเสี่ยงที่องค์กรยอมรับได้
- ให้คำปรึกษาในขอบเขตที่กำหนดไว้ในกฎบัตรการตรวจสอบภายในและในขอบเขตที่ได้รับการอนุมัติจากคณะกรรมการ
- มีการแลกเปลี่ยนความคิดเห็นในกิจกรรมการกำกับดูแลเทคโนโลยีสารสนเทศอย่างสม่ำเสมอเพื่อให้มั่นใจว่ามีการจัดการกับการเปลี่ยนแปลงที่สำคัญขององค์กรและการเปลี่ยนแปลงด้านความเสี่ยงในเวลาที่เหมาะสม
- ตรวจสอบกิจกรรมการกำกับดูแลเทคโนโลยีสารสนเทศอย่างเป็นทางการให้คล้องคล้องกับ IIA Standard ๒๑๑๐

๒. ภาวะผู้นำและการสนับสนุนของผู้บริหาร

ประสิทธิผลของภาวะผู้นำในการสร้างและสื่อสารวัฒนธรรมหรือแนวคิดเกี่ยวกับท่าทีจากผู้บริหารระดับสูงเป็นสิ่งที่สำคัญที่สุดของแผนการกำกับดูแลที่มีประสิทธิผล นอกจากนี้ คณะกรรมการและผู้บริหารระดับอาวุโสของแผนการกำกับดูแลที่มีประสิทธิผล นอกจากนี้ คณะกรรมการและผู้บริหารระดับอาวุโสยังจำเป็นต้องทำให้มั่นใจว่า หน้าที่งานด้านเทคโนโลยีสารสนเทศมีความสอดคล้องและเป็นส่วนหนึ่งของแผนกลยุทธ์ขององค์กร

กิจกรรมการตรวจสอบภายในต้องประเมินความเพียงพอและความมีประสิทธิผลของการควบคุมความเสี่ยงในการกำกับดูแล การปฏิบัติการ และระบบข้อมูลสารสนเทศขององค์กร ดังนี้

- ความน่าเชื่อถือและความถูกต้องครบถ้วนของข้อมูลสารสนเทศด้านการเงินและการปฏิบัติการ
- ความมีประสิทธิผลและประสิทธิภาพของการปฏิบัติการ
- การปกป้องสินทรัพย์
- การปฏิบัติตามกฎหมาย ระเบียบ และสัญญา

๓. การวางแผนเชิงกลยุทธ์และแผนการดำเนินการ

การบริหารเทคโนโลยีสารสนเทศในเชิงกลยุทธ์และการดำเนินการ (ยุทธวิธี) และการวัดผลที่เกี่ยวข้องเป็นองค์ประกอบหลักของแผนการกำกับดูแลเทคโนโลยีสารสนเทศที่มีประสิทธิผล ตามที่ Standard ๒๑๑๐.A๒ ระบุว่า “กิจกรรมการตรวจสอบภายในต้องประเมินว่า การกำกับดูแล (เทคโนโลยีสารสนเทศ) ขององค์การสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรหรือไม่”

กิจกรรมการตรวจสอบภายใน (ซึ่งเป็นไปตาม Standard ๒๑๑๐) ควรดำเนินการตรวจสอบด้านกำกับดูแลรวมทั้งประเมินว่าการกำกับดูแลเทคโนโลยีสารสนเทศได้รักษาและสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กรหรือไม่ ผู้ตรวจสอบภายในอาจพบว่าองค์กรไม่มีแผนการกำกับดูแลเทคโนโลยีสารสนเทศ หรืออาจมีแผนการกำกับดูแลซึ่งได้รับการออกแบบอย่างเหมาะสมและมีการควบคุมอย่างเพียงพอหรืออาจจะน้อยหรือมากเกินไป เนื่องจากแต่ละองค์กรมีแผนการกำกับดูแลเทคโนโลยีสารสนเทศที่แตกต่างกัน จึงควรมีองค์ประกอบด้านการดำเนินการที่เพียงพอซึ่งจะบอกให้ผู้บริหารทราบว่ามีการกำกับดูแลเทคโนโลยีสารสนเทศอย่างเพียงพอเพื่อให้บรรลุวัตถุประสงค์เชิงกลยุทธ์หรือไม่

๔. การให้บริการและการวัดผล

การตรวจสอบองค์ประกอบการบริหารด้านการเงินของแผนการกำกับดูแลเทคโนโลยีสารสนเทศอาจแตกต่างกันออกไปแต่ละองค์กรตามทิศทางการบริหารงานของคณะกรรมการและผู้บริหารระดับอาวุโส ความกดดันและเงื่อนไขของอุตสาหกรรมรวมทั้งการแข่งขัน แต่ไม่ว่ากรณีใด การบริหารด้านการเงินก็เป็นส่วนสำคัญในการควบคุมและการติดตามดูแลต้นทุนและประโยชน์ที่จะได้รับจากเทคโนโลยีสารสนเทศ ผู้ตรวจสอบภายในควรมีความเข้าใจว่า ผู้บริหารระดับอาวุโสได้ออกแบบและมอบหมายงานบริหารด้านการเงินได้ดีเพียงใด ผู้ตรวจสอบภายในควรเริ่มจากการทำความเข้าใจนโยบายการบริหารด้านการเงินของงานเทคโนโลยีสารสนเทศ

๕. โครงสร้างด้านเทคโนโลยีสารสนเทศและการบริหารความเสี่ยง

กิจกรรมการตรวจสอบมักมุ่งเน้นไปที่ภาพรวมของการสอบทานโครงสร้างและกระบวนการกำกับดูแลเทคโนโลยีสารสนเทศก่อน ซึ่งจะช่วยสร้างความเข้าใจในแผนการกำกับดูแลเทคโนโลยีสารสนเทศ นโยบายที่เกี่ยวข้องและขั้นตอนการปฏิบัติงานต่างๆ นอกจากนี้การตรวจสอบยังสามารถใช้วิธีการเปรียบเทียบแผนการกำกับดูแลมาตรฐานที่เป็นอิสระได้ด้วย และตรวจสอบว่าผู้บริหารได้กำหนดเกณฑ์เปรียบเทียบของตนเองขึ้นหรือไม่ ซึ่งต้องสอบทานเกณฑ์ดังกล่าว จะช่วยสร้างความเชื่อมั่นต่อลักษณะของแผนการกำกับดูแลเทคโนโลยีสารสนเทศ

บทที่ ๓

ขั้นตอนและกระบวนการตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit)

ขั้นตอนและกระบวนการตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit)

มีกระบวนการเช่นเดียวกับตรวจสอบภายในประเภทอื่นๆ โดยเริ่มตั้งแต่ผู้ตรวจสอบภายในศึกษาทำความเข้าใจระบบงานสารสนเทศ (IT Audit) จัดทำแผนการตรวจสอบ (Planning) แนวการตรวจสอบ (Audit Program) ตามผลการประเมินความเสี่ยง กำหนดประเด็นการตรวจสอบ เพื่อกำหนดวัตถุประสงค์ของการตรวจสอบ และขอบเขตการตรวจสอบ นำผลการประเมินความเสี่ยงที่ได้มาจัดทำแผนปฏิบัติงานตรวจสอบ จัดทำกระดาษทำการ สรุปข้อเท็จจริง รายงานผลการตรวจสอบ และการติดตามผลการตรวจสอบ ทั้งนี้ ผู้ตรวจสอบระบบสารสนเทศต้องมีความรู้ ความเชี่ยวชาญเกี่ยวกับระบบเทคโนโลยีสารสนเทศ

การตรวจสอบ IT Audit เป็นกระบวนการที่สำคัญในองค์กรเพื่อประเมินและตรวจสอบระบบ IT ทั้งหมดหรือส่วนหนึ่งขององค์กร เพื่อให้แน่ใจว่ามีการควบคุมและการจัดการที่เหมาะสมกับความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสาร (IT) อย่างมีประสิทธิภาพ

ประเด็นหลักในการตรวจสอบ IT Audit ที่สำคัญสำหรับองค์กรได้แก่ :

๑. **การควบคุมภายใน (Internal Controls)**: การตรวจสอบว่ามีการควบคุมภายในที่เพียงพอเพื่อป้องกันการเข้าถึงไม่ชอบด้วยภัยคุกคามหรือการใช้ข้อมูลที่ไม่ถูกต้อง รวมถึงการตรวจสอบการเข้าถึงระบบและข้อมูลที่จำเป็น

๒. **ความสามารถในการดำเนินการ (Operational Capability)**: การตรวจสอบการดำเนินการของระบบ IT เพื่อให้แน่ใจว่ามีความสามารถในการทำงานตามที่ออกแบบไว้และเพื่อให้ตอบสนองต่อความต้องการของธุรกิจได้อย่างมีประสิทธิภาพ

๓. **การรักษาความปลอดภัย (Security Measures)**: การตรวจสอบมาตรการที่ใช้ในการรักษาความปลอดภัยของข้อมูลและระบบ IT ในองค์กร เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลที่ไม่ชอบด้วย

๔. **ความสอดคล้องกับกฎหมายและข้อบังคับ (Compliance)**: การตรวจสอบว่าระบบ IT ขององค์กรมีความสอดคล้องกับกฎหมายที่เกี่ยวข้อง เช่น การคุ้มครองข้อมูลส่วนบุคคล (GDPR) หรือกฎหมายด้านการเงิน (Financial Regulations)

๕. **การจัดการความเสี่ยง (Risk Management)**: การตรวจสอบว่าองค์กรมีกระบวนการจัดการความเสี่ยงในเทคโนโลยีสารสนเทศและการสื่อสารอย่างมีประสิทธิภาพและเหมาะสม

๖. **การวางแผนและการพัฒนา (Planning and Development)**: การตรวจสอบว่ามีการวางแผนและพัฒนาระบบ IT ในองค์กรอย่างเหมาะสมเพื่อรองรับความต้องการของธุรกิจในระยะยาว

การตรวจสอบ IT Audit เป็นกระบวนการที่มีความสำคัญในการรักษาความเชื่อมั่นในระบบ IT ขององค์กรและช่วยให้องค์กรสามารถปรับปรุงและป้องกันปัญหาที่เกิดจากระบบ IT ได้อย่างมีประสิทธิภาพ

การปฏิบัติงานตรวจสอบ

เมื่อผู้ตรวจสอบภายใน ได้กำหนดแผนการตรวจสอบประจำปี ที่ได้รับความเห็นชอบจาก ผอ. สวพส. และคณะกรรมการตรวจสอบ อนุมัติเรียบร้อยแล้ว และแผนปฏิบัติงาน (Engagement Plan) เป็นแผนย่อยของ Audit

Plan ที่หัวหน้าหน่วยตรวจสอบภายใน ได้อนุมัติแล้วผู้ตรวจสอบภายในควรปฏิบัติงานตรวจสอบ โดยขั้นตอน Engagement Plan ประกอบด้วย ๘ ขั้นตอน ดังนี้

(๑) การสำรวจข้อมูลเบื้องต้น

(๒) การประเมินการควบคุมภายใน

(๓) การประเมินความเสี่ยง

(๔) การวางแผนการตรวจสอบ

(๕) การปฏิบัติงานตรวจสอบ

(๖) สรุปผลการตรวจสอบ

(๗) รายงานผลการตรวจสอบ

(๘) การติดตามผลการแก้ไข

การจัดทำแผนปฏิบัติงานหรือ Engagement Plan เป็นขั้นตอนที่สำคัญในการวางแผนกิจกรรมหรือโครงการต่าง ๆ ซึ่งเป็นที่มาของคำว่า "Engagement" ที่หมายถึงการติดต่อสื่อสารและเชื่อมโยงกับกลุ่มเป้าหมายหรือผู้มีส่วนได้ส่วนเสียในโครงการนั้น ๆ ดังนั้น ขั้นตอนในการจัดทำแผนปฏิบัติงาน (Engagement Plan) มักจะประกอบด้วยขั้นตอนหลัก ๆ ดังนี้:

๑. **วิเคราะห์กลุ่มเป้าหมาย (Target Audience Analysis):**
   - กำหนดกลุ่มเป้าหมายที่ต้องการติดต่อสื่อสารหรือมีส่วนร่วมในโครงการ
   - ศึกษาและวิเคราะห์ลักษณะเฉพาะของกลุ่มเป้าหมาย เช่น คุณสมบัติทาง demographic (อายุ เพศ รายได้) และ psychographic (ความสนใจ พฤติกรรม) ของพวกเขา

๒. **กำหนดวัตถุประสงค์ (Objectives Setting):**
   - กำหนดเป้าหมายหรือผลลัพธ์ที่ต้องการให้กับแผนปฏิบัติงาน
   - ให้ระบุให้ชัดเจนว่าต้องการให้กลุ่มเป้าหมายมีพฤติกรรมหรือการกระทำบางอย่างอย่างไร

๓. **เลือกช่องทางการสื่อสาร (Communication Channels Selection):**
   - เลือกวิธีการสื่อสารที่เหมาะสมกับกลุ่มเป้าหมาย เช่น โซเชียลมีเดีย เว็บไซต์ งานประชาสัมพันธ์ หรือกิจกรรมอื่น ๆ
   - คำนึงถึงว่าช่องทางใดเหมาะสมที่สุดเพื่อให้มีการตอบรับและมีผลสัมพันธ์ที่ดีกับกลุ่มเป้าหมาย

๔. **สร้างเนื้อหาและข้อความ (Content and Messaging):**
   - สร้างเนื้อหาที่เหมาะสมและน่าสนใจสำหรับกลุ่มเป้าหมาย
   - ตระหนักถึงลักษณะของเนื้อหาที่เหมาะสมกับแต่ละช่องทางการสื่อสาร

๕. **วางแผนการดำเนินงาน (Implementation Plan):**
   - วางแผนการดำเนินการในแต่ละช่องทางการสื่อสาร
   - กำหนดเวลาที่เหมาะสมในการทำกิจกรรมและสื่อสาร

๖. **วัดและประเมินผล (Measurement and Evaluation):**
   - กำหนดวิธีการวัดผลและประเมินผลลัพธ์ของแผนปฏิบัติงาน
   - ใช้ตัวชี้วัดที่ชัดเจนเพื่อตรวจสอบว่าได้รับผลสัมพันธ์ตามเป้าหมายหรือไม่

๗. **ปรับปรุงและพัฒนา (Adjust and Develop):**

- พิจารณาผลการประเมินและทำการปรับปรุงแผนปฏิบัติงานต่อไปเพื่อเพิ่มประสิทธิภาพ

ขั้นตอนเหล่านี้จะช่วยให้การจัดทำแผนปฏิบัติงานเป็นไปอย่างมีระบบและมีประสิทธิภาพในการสร้างความสัมพันธ์และปฏิบัติตามเป้าหมายกับกลุ่มเป้าหมายได้ดียิ่งขึ้น

๑) การแจ้งกำหนดการเข้าตรวจสอบ ก่อนเข้าทำการตรวจสอบ หน่วยตรวจสอบภายในจะประสานหน่วยรับตรวจ และจัดให้มีหนังสือแจ้งกำหนดการเข้าตรวจสอบ แจ้งรายชื่อทีมผู้ตรวจสอบ และแจ้งให้ผู้รับผิดชอบของหน่วยรับตรวจจัดเตรียมข้อมูล เอกสารหลักฐานที่เกี่ยวข้อง

๒) การประชุมเปิดการตรวจสอบ เป็นการประชุมร่วมกันระหว่างผู้บริหารและผู้รับผิดชอบแผนงบประมาณ ผลผลิต โครงการ กิจกรรม ของหน่วยรับตรวจกับคณะผู้ตรวจสอบ เพื่อแจ้งให้ผู้บริหารทราบและเข้าใจถึงวัตถุประสงค์ในการตรวจสอบอันเป็นมารยาท ซึ่งจะเสริมสร้างทัศนคติและจะช่วยก่อให้เกิดมนุษย์สัมพันธ์ที่ดีต่อกันซึ่งรวมถึงการสอบถามความเห็นของผู้บริหารและเจ้าหน้าที่ผู้รับตรวจถึงปัญหา อุปสรรค แนวความคิดหรือแนวทางปฏิบัติในอนาคต

๓) การรวบรวมข้อมูล ผู้ตรวจสอบภายในควรตรวจสอบ สอบถาม สัมภาษณ์และรวบรวมข้อมูลต่าง ๆที่เกี่ยวข้องในระหว่างการปฏิบัติงานตรวจสอบ โดยข้อมูลที่รวบรวมควรมีลักษณะสำคัญ ดังนี้

- ความถูกต้องหรือเชื่อถือได้ ควรเป็นข้อมูลหลักฐานหรือข้อเท็จจริงที่แสดงเนื้อหาตามที่ต้องการอย่างถูกต้องตามความเป็นจริงและมาจากแหล่งที่น่าเชื่อถือ เช่น ข้อมูลหลักฐานที่ได้จากบุคคล/แหล่งภายนอกน่าเชื่อถือกว่าข้อมูลหลักฐานของหน่วยรับตรวจ ข้อมูลหลักฐานที่เป็นต้นฉบับน่าเชื่อถือกว่าภาพถ่ายสาเนา เป็นต้น

- ความเกี่ยวข้องหรือสัมพันธ์กับประเด็นการตรวจสอบ ควรเป็นข้อมูล หลักฐานหรือข้อเท็จจริงที่มีสาระสำคัญและตรงตามประเด็นการตรวจสอบที่กำหนดไว้ ซึ่งจะช่วยสนับสนุนในการสรุปผลการตรวจสอบ

- ความเพียงพอต่อการสรุปผลการตรวจสอบ ควรมีข้อมูลหลักฐานหรือ ข้อเท็จจริงในปริมาณหรือจำนวนที่เพียงพอต่อการสรุปผลการตรวจสอบได้อย่างสมเหตุสมผลหรือใช้อ้างอิงให้มั่นใจถึงเหตุการณ์ที่เกิดขึ้น ซึ่งทุกคนสามารถสรุปความเห็นได้อย่างเดียวกัน

- ความมีประโยชน์ต่อการปฏิบัติงาน ควรเป็นข้อมูลหลักฐานหรือข้อเท็จจริงที่ช่วยในการควบคุมและตัดสินใจของผู้บริหาร เพื่อให้การดำเนินงานของหน่วยงานบรรลุเป้าหมายที่กำหนด ทั้งนี้ ข้อมูลควรมีความทันเวลาในการใช้ประโยชน์และความมีสาระสำคัญในการสรุปความเห็นหรือตัดสินใจ

๔) วิเคราะห์และประเมินผล เป็นการนำข้อมูลที่รวบรวมได้มาวิเคราะห์และประเมินผลว่าผลของสภาพการดำเนินงานที่เกิดขึ้นจริงมีความแตกต่างกับแผนหรือเกณฑ์หรือสิ่งที่ควรจะเกิดขึ้นหรือควรจะเป็นสำหรับการดำเนินงานนั้นหรือไม่ หากแตกต่างจากแผนหรือเกณฑ์หรือสิ่งที่ควรจะเป็น ควรวิเคราะห์ต่อไปว่า จะเกิดผลกระทบอะไรบ้าง และมีสาเหตุมาจากอะไร ซึ่งควรมีการปรับปรุงแก้ไขการดำเนินงานหรือไม่ อย่างไร

๕) สรุปประเด็นข้อตรวจพบ เป็นการนำข้อมูลที่วิเคราะห์และประเมินผลได้มาสรุปว่าจากการตรวจสอบได้ข้อเท็จจริงหรือข้อตรวจพบอะไรบ้างในแต่ละประเด็นการตรวจสอบ สรุปประเด็นข้อตรวจพบใน ๕ เรื่องดังนี้

๕.๑ หลักเกณฑ์/สิ่งที่ควรจะเป็น (Criteria) คือ สิ่งที่ใช้เป็นเกณฑ์ในการเปรียบเทียบกับสภาพการดำเนินงานที่เกิดขึ้นจริงของแผนงบประมาณ ผลผลิต โครงการ กิจกรรมที่ตรวจสอบ ซึ่งส่วนใหญ่ ได้แก่ เกณฑ์การตรวจสอบตามที่กำหนดไว้ในแผนการปฏิบัติงานตรวจสอบ

๕.๒ ข้อเท็จจริง/สิ่งที่เป็นอยู่ (Condition) คือ ข้อเท็จจริงที่ผู้ตรวจสอบภายในได้ค้นพบในการตรวจสอบและได้รับการตรวจสอบแน่ชัดแล้วว่าถูกต้องและมีข้อมูลหลักฐานสนับสนุน

๕.๓ ผลกระทบ (Effects) คือ ความเสี่ยง/ผลเสียหาย/ปัญหาที่จะได้รับ เนื่องจากสิ่งที่เป็นอยู่แตกต่างไป

จากสิ่งที่ควรจะเป็น ซึ่งควรระบุผลกระทบที่ชัดเจนว่าเกิดจากการดำเนินงานนั้นโดยตรงหรือโดยอ้อม ผลกระทบอาจเกิดขึ้นได้ทั้งด้านบวก และด้านลบ อย่างไรก็ดีการพิจารณาว่าผลกระทบนั้นมีสาระสำคัญที่ควรรายงานหรือไม่ อาจพิจารณาจากความมากน้อยของผลกระทบ ความถี่ของผลกระทบที่เกิดขึ้น ผลกระทบมีขอบเขตของการเกิดกว้างไกลเพียงใด และมีระยะเวลาในการเกิดผลกระทบมากน้อยเพียงใด

๕.๔ สาเหตุ (Causes) คือเหตุผลของความแตกต่างระหว่างสิ่งที่ควรจะเป็นกับสิ่งที่เป็นอยู่ซึ่งควรพิสูจน์ให้แน่ชัดว่าเกิดจากเหตุผลหรือสาเหตุที่แท้จริงใดบ้าง และมีความสำคัญหรือไม่ อย่างไรเพื่อจะได้นำไปสู่ข้อเสนอแนะในการแก้ไขปัญหาให้ตรงกับสาเหตุที่เกิดขึ้น ซึ่งสาเหตุที่เกิดปัญหาส่วนใหญ่มักเกิดจากการไม่มีระบบการควบคุมภายในที่ดี หรือมีระบบการควบคุมภายในแต่ไม่ปฏิบัติตามระบบที่กำหนด

๕.๕ ข้อเสนอแนะ (Recommendation) คือ ข้อคิดเห็น/ความเห็นเกี่ยวกับการปรับปรุงแก้ไขหรือพัฒนาการดำเนินงานให้มีประสิทธิภาพยิ่งขึ้น อันจะทำให้บรรลุผลสัมฤทธิ์ ข้อเสนอแนะควรสอดคล้องและเป็นเหตุเป็นผลสนับสนุนซึ่งกันและกันกับสาเหตุ อย่างไรก็ตาม ผู้ตรวจสอบภายในอาจขอความเห็น/ข้อเสนอแนะจากหน่วยรับตรวจ ผู้เชี่ยวชาญและหรือผู้เกี่ยวข้องก็ได้ เพื่อให้ข้อเสนอแนะนั้นมีคุณค่าเป็นที่ยอมรับของทุกฝ่ายที่เกี่ยวข้องและสามารถนำไปปฏิบัติได้

๖) บันทึกข้อมูล เป็นการนำข้อมูลที่ได้มาบันทึกไว้ในกระดาษทำการ โดยให้มีรายละเอียดเพียงพอต่อการสนับสนุนผลการตรวจสอบในรายงานผลการปฏิบัติงานที่เสนอต่อหัวหน้าส่วนราชการ ทั้งนี้ผู้ตรวจสอบภายในควรบันทึกข้อมูลที่สำคัญ/จำเป็นและเกี่ยวข้องกับเรื่องที่ตรวจสอบ และระมัดระวังมิให้มีการนำข้อมูลที่ไม่ถูกต้อง ไม่สมบูรณ์หรือไม่ครบถ้วนมาบันทึก พร้อมทั้งระบุแหล่งที่มาของข้อมูลไว้ด้วย

๗) การประชุมปิดการตรวจ ดำเนินการปิดตรวจโดยการประชุมร่วมกันระหว่างผู้บริหารและผู้รับผิดชอบแผนงบประมาณ ผลผลิต โครงการ กิจกรรม ของหน่วยรับตรวจกับคณะผู้ตรวจสอบ เพื่อกระชับเวลาในการติดตามผล โดยได้หารือปัญหาที่เกิดขึ้น และแลกเปลี่ยนความคิดเห็นในการแก้ไขปัญหา ซึ่งจะเป็นการสร้างสัมพันธภาพที่ดีระหว่างคณะผู้ตรวจและผู้รับผิดชอบของหน่วยรับตรวจ และทำให้รายงานนำไปสู่การปฏิบัติตามข้อเสนอแนะได้อย่างมีประสิทธิภาพ

ขอบเขตการตรวจสอบ :

๑. การสอบทานการควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control)

๑) การกำหนดนโยบายในการใช้สารสนเทศ

๒) การแบ่งแยกหน้าที่ในระบบสารสนเทศ

๓) การควบคุมการกำหนดแผนระยะยาว แผนงานพัฒนาระบบ กำหนดการประมวลผลข้อมูล มอบหมายหน้าที่และความรับผิดชอบ

๔) การควบคุมโครงสร้างการพัฒนาระบบสารสนเทศ

๕) การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์

๖) การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์

๗) การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ

๘) การควบคุมการเข้าระบบงาน

๒. การควบคุมเฉพาะระบบงาน (Application Control)

๑) การควบคุมการนำเข้าข้อมูล

๒) การควบคุมการทำรายการป้อนเข้าสู่ระบบงาน

๓) การควบคุมการสื่อสารข้อมูลให้มีความถูกต้องและครบถ้วน

๔) การควบคุมการประมวลผลด้วยคอมพิวเตอร์ให้มีความแม่นยำ ถูกต้อง

๕) การควบคุมการจัดเก็บข้อไว้ในระบบ การกำหนดสิทธิการใช้ข้อมูล การรักษาความปลอดภัย การแก้ไขข้อผิดพลาด การสำรองข้อมูล และการกำหนดอายุการจัดเก็บแฟ้มข้อมูล

๖) การควบคุมผลลัพธ์ การกระทบยอดข้อมูลนำเข้าและผลลัพธ์

๓. การสอบทานการดำเนินการตามระบบ IT Security

IT Security คือ พื้นฐานของการรักษาความปลอดภัยของ Network ในรูปแบบ Digital Format หรือ Digital Information ให้เป็นความลับ รวมไปถึงการจัดการข้อมูลให้เป็นระบบ และมีการป้องกันความปลอดภัยอย่างเหมาะสม เพื่อให้พร้อมใช้งานภายในองค์กรมากที่สุด ประเภทของ IT Security

๑) การรักษาความปลอดภัยเครือข่าย (Network Security)

จะช่วยป้องกันและคัดกรองไม่ให้ผู้ใช้ที่ไม่ได้รับอนุญาตหรือผู้ใช้ที่เป็นอันตรายเข้ามาภายในเครือข่ายได้

๒) การรักษาความปลอดภัยอินเทอร์เน็ต (Internet Security)

จะช่วยสร้างความมั่นใจในการใช้งานได้ ทั้งในการป้องกันข้อมูลที่มีการรับส่งบนเบราว์เซอร์ ต่างๆ หรือแม้กระทั่งบนเว็บแอปพลิเคชัน ที่มีการออกแบบเพื่อตรวจสอบข้อมูล ซึ่งจะช่วยในการป้องกันการโจมตีด้านต่าง ๆ ได้อย่างมีประสิทธิภาพ

๓) การรักษาความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Security)

เพื่อป้องกันไม่ให้อุปกรณ์เหล่านั้นเข้าถึงหน้าเว็บไซต์ที่อาจจะก่อให้เกิดความเสียหายต่อองค์กรซึ่งเป็นระบบความปลอดภัยที่มีการป้องกันอีกชั้นหนึ่งก่อนเข้าถึงการใช้งาน

๔) การรักษาความปลอดภัยระบบคลาวด์ (Cloud Security)

ผ่านการเข้ามาเป็นตัวการ เพื่อเพิ่มความปลอดภัยให้กับระบบ โดยมี gateway ที่ปลอดภัยสามารถจัดการกับภัยคุกคามต่างๆ บนคลาวด์ได้อย่างดี

๕) การรักษาความปลอดภัยการเข้าใช้งานแอปพลิเคชั่น (Application Security)

สามารถมั่นใจถึงความปลอดภัยได้ เมื่อมีการใช้งาน Application Security เข้ามา เพราะมีระบบสำหรับทำการยืนยันตัวตน อีกทั้งยังช่วยให้บริษัทสามารถประเมินความเสี่ยงของช่องโหว่ต่าง ๆ ที่อาจจะเกิดขึ้นได้

๔. การสอบทานการดำเนินการตามระบบ Cyber Security

Cyber Security หรือ ความปลอดภัยทางไซเบอร์ คือ กระบวนการในการลดความเสี่ยงจากการโจมตีทางอินเทอร์เน็ต ช่วยในการปกป้องข้อมูลจากการโจรกรรมของแฮกเกอร์ ตลอดจนการรั่วไหลของข้อมูล หรือเหตุการณ์ใดๆ ที่อาจส่งผลต่อการทำงาน อุปกรณ์ และบริการที่ใช้งาน จนก่อให้เกิดความเสียหายแก่องค์กรและ

ชื่อเสียงขององค์กรได้ หลายองค์กรจึงเลือกที่จะให้ความสำคัญกับ Cyber Security และ ตำแหน่งงาน Cyber Security ในการสร้างความปลอดภัยด้านข้อมูลข่าวสารภายในองค์กร ประเภทของ Cyber Security

๑) การรักษาความปลอดภัยของระบบโครงสร้างพื้นฐาน (Critical Infrastructure Security) มีความเสี่ยงในการถูกโจมตีสูงกว่าระบบอื่น ๆ

๒) การรักษาความปลอดภัยระบบแอปพลิเคชั่น (Application Security)

ซึ่งจะมีการอัปเดตและทดสอบอย่างต่อเนื่อง เพื่อป้องกันการโจมตีหรือการแฝงตัว เช่น โปรแกรม Antivirus, Firewall หรือโปรแกรมการเข้ารหัส เป็นต้น

๓) การรักษาความปลอดภัยของระบบอินเทอร์เน็ต (Network Security)

กระบวนการปกป้องเครือข่ายจากแฮกเกอร์หรือภัยคุกคามภายนอก โดยจะมีระบบแจ้งเตือนความผิดปกติที่เกิดขึ้น

๔) การรักษาความปลอดภัยให้กับข้อมูลที่เก็บในคลาวด์ (Cloud Security)

ระบบเก็บข้อมูลที่มีความปลอดภัยและประหยัดค่าใช้จ่าย ทั้งยังมีการพัฒนาและปรับปรุงระบบอยู่เสมอ ทำให้ในปัจจุบันหลายองค์กรนิยมเก็บข้อมูลในรูปแบบดิจิทัลหรือคลาวด์มากขึ้น

๕) การรักษาความปลอดภัยให้กับอุปกรณ์ Internet of Thing (Internet of Thing Security) ซึ่งมีการรับ-ส่งข้อมูลกันอย่างต่อเนื่องผ่านระบบอินเทอร์เน็ต

<u>สรุป</u> กระบวนการตรวจสอบ IT Audit มีหลายขั้นตอนหลักๆ ที่มักใช้เพื่อประเมินความถูกต้องและความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ดังนี้:

๑. **การวางแผน (Planning):**
   - ระบุขอบเขตของการตรวจสอบ
   - ตั้งเป้าหมายและวัตถุประสงค์
   - จัดทำแผนการตรวจสอบและกำหนดทรัพยากรที่ต้องใช้

๒. **การเตรียมข้อมูล (Preparation):**
   - รวบรวมข้อมูลพื้นฐานเกี่ยวกับระบบ IT
   - วิเคราะห์ความเสี่ยงและปัญหาที่อาจเกิดขึ้น
   - กำหนดเกณฑ์และมาตรฐานการตรวจสอบ

๓. **การดำเนินการตรวจสอบ (Execution):**
   - ตรวจสอบและทดสอบการควบคุมภายในของระบบ IT
   - เก็บรวบรวมหลักฐานและข้อมูลจากการตรวจสอบ
   - วิเคราะห์ข้อมูลและประเมินความเสี่ยงที่พบ

๔. **การรายงานผล (Reporting):**
   - จัดทำรายงานผลการตรวจสอบ
   - ระบุปัญหาและข้อเสนอแนะเพื่อการปรับปรุง
   - นำเสนอผลการตรวจสอบต่อผู้บริหารหรือผู้ที่เกี่ยวข้อง

๕. **การติดตามผล (Follow-up):**

- ติดตามการดำเนินการแก้ไขปัญหาหรือข้อเสนอแนะ
- ประเมินประสิทธิภาพของการแก้ไข รายงานผลการดำเนินงานตามข้อเสนอแนะ
- อัปเดตและปรับปรุงกระบวนการตรวจสอบตามความจำเป็น

ขั้นตอนเหล่านี้ช่วยให้มั่นใจได้ว่าระบบ IT จะมีความปลอดภัยและทำงานได้อย่างมีประสิทธิภาพตามมาตรฐานที่กำหนดค่ะ

ภาคผนวก

การบริหารจัดการและการควบคุมความเสี่ยงที่สำคัญ

การบริหารจัดการและการควบคุมความเสี่ยงที่สำคัญ ประกอบด้วย

๑. โครงสร้างหน่วยงานและการบริหารจัดการ

๒. การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์

๓. การควบคุมการพัฒนา การแก้ไขหรือเปลี่ยนแปลงระบบคอมพิวเตอร์ (Change Management)

๔. การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน

๕. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์ รายละเอียด ดังนี้

๑. โครงสร้างหน่วยงานและการบริหารจัดการ	
✠ **<u>การแบ่งแยกอำนาจหน้าที่</u>** ควรเป็นไปตามหลักการควบคุมภายในที่ดี โดยไม่ควรมอบหมายให้บุคลากรคนหนึ่งคนใดรับผิดชอบการปฏิบัติงานตลอดกระบวนการ ซึ่งการมอบหมายให้บุคลากรคนหนึ่งคนใดปฏิบัติงานหลายหน้าที่ควบคู่กันในบางกรณี ยังอาจเป็นช่องทางให้ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ถูกแก้ไขหรือเปลี่ยนแปลงได้โดยง่าย (integrity risk)	**<u>แนวทางการกำกับดูแล</u>** ให้ความสำคัญกับระบบการสอบยันการปฏิบัติงานระหว่างบุคลากรภายในหน่วยงาน กรณีมีข้อจำกัดของบุคลากร ก็ควรกำหนดวิธีการกำกับดูแลและควบคุมการปฏิบัติงานของบุคลากรดังกล่าวอย่างรอบคอบและรัดกุม
✠ **<u>การกำหนดนโยบาย แผนงานและขั้นตอนการปฏิบัติงาน</u>** จะทำให้บุคลากรสามารถปฏิบัติงานได้อย่างถูกต้อง ครบถ้วน และเป็นไปในแนวทางเดียวกันซึ่งจะส่งผลให้การปฏิบัติงานโดยรวมมีประสิทธิภาพ นอกจากนี้ ยังลดโอกาสการปฏิบัติงานผิดพลาดในกรณีที่มีการสับเปลี่ยนหน้าที่และความรับผิดชอบหรือมีการมอบหมายงานให้บุคลากรรายใหม่	**<u>แนวทางการกำกับดูแล</u>** ให้ความสำคัญกับความครบถ้วนและความชัดเจนของนโยบาย แผนงาน และขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูลและระบบคอมพิวเตอร์การพัฒนา แก้ไขหรือเปลี่ยนแปลง การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการปฏิบัติงานประจาอื่นที่สำคัญ
✠ **<u>การกำกับดูแลและตรวจสอบการปฏิบัติงานของพนักงานระดับปฏิบัติการอย่างใกล้ชิดโดยผู้บังคับบัญชา</u>** จะทำให้การปฏิบัติงานโดยรวมมีความถูกต้องและละเอียดรอบคอบมากขึ้น ซึ่งจะเป็นการลดโอกาสการเกิดข้อผิดพลาดและป้องกันกาปฏิบัติงานนอกเหนืออำนาจหน้าที่และความรับผิดชอบที่ได้รับมอบหมาย	**<u>แนวทางการกำกับดูแล</u>** ให้ความสำคัญกับการรายงานการปฏิบัติงานและตรวจสอบการปฏิบัติงาน เพื่อให้มั่นใจได้ว่าการปฏิบัติงานถูกต้อง ครบถ้วน เป็นไปตามนโยบายและขั้นตอนการปฏิบัติงาน และอยู่ในกรอบอำนาจหน้าที่และความรับผิดชอบตามที่องค์กรกำหนด

๒. การรักษาความปลอดภัยข้อมูลและระบบคอมพิวเตอร์	
💻 **<u>การควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย (Physical Security)</u>** จะเป็นการป้องกันไม่ให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าถึง ล่วงรู้ (access risk) แก้ไขเปลี่ยนแปลง (integrity risk) หรือก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ ซึ่งรวมถึงความเสียหายจากปัจจัยสภาวะแวดล้อมหรือภัยพิบัติต่างๆ (availability risk)	**<u>แนวทางการกำกับดูแล</u>** ให้ความสำคัญกับการควบคุมการเข้าออกศูนย์คอมพิวเตอร์ที่รัดกุมเพียงพอ โดยจำกัดสิทธิการเข้าออกและการตรวจสอบการเข้าออกอย่างสม่ำเสมอ รวมทั้งจัดให้มีระบบป้องกันความเสียหายจากปัจจัยสภาวะแวดล้อมและภัยพิบัติที่อาจเกิดขึ้น
💻 **การควบคุมการใช้ข้อมูลและระบบงานคอมพิวเตอร์และการป้องกันการบุกรุกผ่านระบบเครือข่าย (Logical Security)** อาจเกิดจากบุคคลภายในองค์กร เช่น ไม่ได้มีการกำหนดรหัสผ่านในการเข้าสู่ระบบงานอย่างรัดกุมหรือกำหนดสิทธิให้แก่ผู้ใช้งานภายในเพื่อเข้าถึงข้อมูลและระบบงานคอมพิวเตอร์ที่มากเกินความจำเป็น เป็นต้น อาจเกิดจากการเชื่อมต่อระบบเครือข่ายภายในกับภายนอก ที่จะเป็นช่องทางให้บุคคลภายนอกเข้าถึงข้อมูลและระบบคอมพิวเตอร์ รวมทั้งไวรัส หรือ malicious code อื่นๆ ผ่านเข้ามาทางระบบเครือข่าย	**<u>แนวทางการกำกับดูแล</u>** ให้ความสำคัญกับการจัดให้มีระบบ การตรวจสอบผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์ (authentication) การกำหนดให้มีการใส่รหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์ การกำหนดสิทธิผู้ใช้งานให้เหมาะสมกับหน้าที่ความรับผิดชอบและระบบป้องกันการบุกรุกจากบุคคลภายนอกผ่านระบบเครือข่าย

๓. การควบคุมการพัฒนา การแก้ไขหรือเปลี่ยนแปลงระบบคอมพิวเตอร์ (Change Management)	
<u>เป็นเรื่องที่ต้องให้ความสำคัญ</u> โดยหากไม่มีวิธีการจัดการและการควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจทาให้ระบบงานคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องหรืออาจไม่เป็นไปตามความต้องการของผู้ใช้งานได้ (integrity risk)	**<u>แนวทางการกำกับดูแล</u>** ให้ความสำคัญกับการจัดให้มีระบบการตรวจสอบ ผู้ใช้งานก่อนเข้าสู่ระบบคอมพิวเตอร์ (authentication) และการกำหนดให้มีการใส่รหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์โดยรหัสดังกล่าว ควรมีการกำหนดความยาวขั้นต่ำอายุการใช้งานจำนวนครั้งที่ยอมให้ใส่รหัสผ่านผิด และควรกำหนดรหัสผ่านให้มีความยากแก่การคาดเดา และควรมีการกำหนดสิทธิผู้ใช้งานให้เหมาะสมกับหน้าที่ความรับผิดชอบ

๔. การสำรองข้อมูลและระบบงานคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน	
🖫 **<u>การสำรองข้อมูลและระบบงานคอมพิวเตอร์</u>** หากมิได้ดำเนินการที่เพียงพอจะทำให้ไม่มีข้อมูล หรือระบบงานคอมพิวเตอร์สาหรับใช้งานได้อย่างต่อเนื่องมีประสิทธิภาพและในเวลาที่ต้องการ	**<u>แนวทางการกำกับดูแล</u>** ให้ความสำคัญกับการสำรองข้อมูลและการทำงานของระบบงานคอมพิวเตอร์ ในเรื่องความครบถ้วนของการเก็บรักษาสื่อที่ใช้บันทึก และการทดสอบความถูกต้องครบถ้วนของข้อมูลและระบบงานคอมพิวเตอร์ที่สำรองไว้
🖫 การเตรียมพร้อมกรณีฉุกเฉิน เป็นการจัดทำแผนฉุกเฉินเพื่อรองรับเหตุการณ์ฉุกเฉินที่อาจเกิดขึ้น ซึ่งจะทำให้การควบคุมความเสี่ยงด้าน availability risk มีประสิทธิภาพมากขึ้น	**<u>แนวทางการกำกับดูแล</u>** ให้ความสำคัญกับการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินต่างๆ ที่ควรมีรายละเอียดที่ชัดเจนเกี่ยวกับขั้นตอนปฏิบัติและผู้รับผิดชอบ ควรมีการสื่อสารให้ผู้เกี่ยวข้องเข้าใจและรับทราบหน้าที่ความรับผิดชอบ รวมทั้งการทดสอบแผนดังกล่าวเพื่อให้มั่นใจว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ

๕. การควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์	
<u>เป็นเรื่องของการควบคุมการประมวลผล</u> การดูแลการทำงานของระบบคอมพิวเตอร์การย้ายโปรแกรมที่พัฒนาแล้วสู่ระบบงานจริง การสำรองข้อมูลและระบบงานคอมพิวเตอร์และงานประจำอื่นๆ หากไม่ได้มีวิธีการปฏิบัติและควบคุมที่รอบคอบและรัดกุมเพียงพอ อาจก่อให้เกิดความเสี่ยงในด้านต่างๆ เช่น ความเสี่ยงด้าน integrity risk ในกรณีที่ย้ายโปรแกรมที่พัฒนาแล้วสู่ระบบงานจริงไม่ครบถ้วน ความเสี่ยงด้าน availability risk ในกรณีที่มิได้มีการดูแลการทำงานของระบบคอมพิวเตอร์อย่างเพียงพอ เป็นต้น	**<u>แนวทางการกำกับดูแล</u>** ให้ความสำคัญกับการกำกับดูแลและควบคุมการปฏิบัติงานประจำด้านคอมพิวเตอร์อย่างใกล้ชิดของผู้บังคับบัญชาการปฏิบัติงานที่มีขั้นตอนที่ชัดเจนและสามารถตรวจสอบได้ รวมทั้งควรจัดให้มีระบบการรายงาน และการตรวจสอบการปฏิบัติงานประจำดังกล่าวอย่างสม่ำเสมอ

กระดาษทำการการสอบทานข้อมูลการควบคุมภายในด้านเทคโนโลยีสารสนเทศ ของ สวพส.
หน่วยตรวจสอบภายใน สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)
ณ วันที่ .....เดือน.....พ.ศ.....

ด้านการควบคุมทั่วไป (General Control)

หมายถึง การควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อมของการควบคุม นโยบายและวิธีการในการควบคุมระบบสารสนเทศ การควบคุมความปลอดภัย การควบคุมการพัฒนาและปรับปรุง และการป้องกัน/ลดความเสียหายของระบบ เป็นการควบคุมภายในสำหรับองค์กรในภาพรวม

การควบคุมภายในทั่วไป	มี/ใช่	ไม่มี/ไม่ใช่	ผลการประเมินระบบควบคุมภายใน
๑. การกำหนดนโยบายในการใช้สารสนเทศ มีนโยบายการรักษาความปลอดภัย ด้านระบบเทคโนโลยีสารสนเทศที่ชัดเจนว่าใครต้องการเข้าถึงข้อมูลอะไร เมื่อไหร่ ในระบบงานใด การให้สิทธิในการเข้าถึงข้อมูลเฉพาะบุคคลที่มีสิทธิในการเข้าถึงข้อมูล			
๒. การแบ่งแยกหน้าที่งานในระบบสารสนเทศ มีการแบ่งแยกหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานในระบบงานคอมพิวเตอร์ให้ชัดเจน เช่น แยกหน้าที่การพัฒนาระบบออกจากหน้าที่ผู้ปฏิบัติงานคอมพิวเตอร์ ผู้บริหารฐานข้อมูล (Database Administrator) ต้องไม่ทำหน้าที่อื่น ผู้พัฒนาระบบออกจากผู้ดูแลบำรุงรักษาระบบ			
๓. การควบคุมโครงการพัฒนาระบบสารสนเทศ กำหนดแผนระยะยาว แผนงานพัฒนาระบบ กำหนดการประมวลผลข้อมูล มอบหมายหน้าที่ และความรับผิดชอบ การประเมินผลงานระหว่างการดำเนินโครงการ การสอบทานภายหลังการติดตั้งระบบ และนำมาใช้งาน การวัดผลการดำเนินงานของระบบ			
๔. การควบคุมการเปลี่ยนแปลงแก้ไขระบบ กำหนดระเบียบวิธีปฏิบัติในการแก้ไขระบบที่เป็นลายลักษณ์อักษร มีการศึกษาถึงผลกระทบต่างๆ มีการทดสอบระบบที่แก้ไขแล้วก่อนนำไปใช้ จัดทำเอกสารคู่มือประกอบการแก้ไข ประเมินผลและสอบทานระบบงานภายหลังเริ่มใช้			

การควบคุมภายในทั่วไป	มี/ใช่	ไม่มี/ไม่ใช่	ผลการประเมินระบบควบคุมภายใน
๕. การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์ การประมวลผลข้อมูลของระบบงานต่างๆ มีความถูกต้อง ครบถ้วน การกู้ระบบ และการสำรองข้อมูล การทดสอบ การจัดการกับปัญหาของระบบ จัดทำแผนสำรอง			
๖. การควบคุมเข้าถึงอุปกรณ์คอมพิวเตอร์ มีสถานที่จัดเก็บอุปกรณ์คอมพิวเตอร์มิดชิด ไม่มีอากาศร้อน ชื้น และแม่เหล็ก มีการรักษาความปลอดภัยหนาแน่น กำหนดการเข้าออกได้เฉพาะผู้ที่เกี่ยวข้อง กำหนดนโยบายรักษาความปลอดภัยที่ชัดเจน ติดระบบเตือนภัยกรณีมีผู้บุกรุก จำกัดให้ใช้โทรศัพท์เรื่องที่เกี่ยวกับงาน ติดอุปกรณ์ป้องกันเครื่องคอมพิวเตอร์			
๗. การควบคุมการเข้าถึงข้อมูลและทรัพยากรสารสนเทศ การกำหนดผู้ใช้ (User Views or Subschema) ตารางแสดงสิทธิในการเข้าถึงฐานข้อมูล (Database Authorization Table) และการเข้ารหัสข้อมูล (Data Encryption)			
๘. การควบคุมการเข้าถึงระบบงาน ดังนี้ - การพิสูจน์ตัวจริง (Authentication) โดยกำหนดรหัสผ่าน (Password) การระบุตัวด้วยสิ่งที่มีทางกายภาพ (Physical Possession Identification) - การกำหนดสิทธิ์ (Authorization) - การบันทึกกิจกรรมต่างๆ ในระบบเพื่อการตรวจสอบ (Audit Logging)			

การตรวจสอบการควบคุมทั่วไป

โดยตรวจสอบในเรื่อง การวางแผนระยะยาวและแผนระยะสั้น การจัดโครงสร้างงานสารสนเทศมีความเหมาะสม ชัดเจน (การแบ่งแยกหน้าที่เหมาะสม) การพัฒนาและการเปลี่ยนแปลงแก้ไขระบบงาน การรักษาความปลอดภัยระบบสารสนเทศ การปฏิบัติการคอมพิวเตอร์ (การปิดเปิดระบบ การบำรุงรักษา การจัดเก็บ) การจัดทำแผนกู้ระบบสารสนเทศ

สรุปผลการตรวจสอบ

.....

.....

.....

.....

.....

ผู้ตรวจสอบ .....
( )
ตำแหน่ง
วันที่

ผู้สอบทาน .....
( )
ตำแหน่ง
วันที่

ผู้รับตรวจ .....
( )
ตำแหน่ง
วันที่

ด้านการควบคุมเฉพาะระบบงาน (Application Control)

การควบคุมรายการข้อมูลในแต่ละระบบงานให้มีความถูกต้องและครบถ้วน โดยอาศัยทางเดินของข้อมูลเป็นแนวทางในการกำหนดขอบเขตการควบคุม เช่น ระบบ Winspeed ระบบ ERP

การควบคุมภายในทั่วไป	มี/ใช่	ไม่มี/ไม่ใช่	ผลการประเมินระบบควบคุมภายใน
๑. การควบคุมการนำเข้าข้อมูล การควบคุมเกี่ยวกับงานจัดทำข้อมูลก่อนป้อนเข้าสู่ระบบคอมพิวเตอร์ การเตรียมข้อมูลนำเข้า การป้องกันข้อผิดพลาด การค้นหาข้อผิดพลาด และการแก้ไขข้อผิดพลาด เช่น การตรวจสอบตัวเลขตรวจสอบ (Check digit) ว่าเป็นตัวเลขที่ถูกหรือไม่ โดยเลขประจำตัว หรือรหัสสินค้า หรือเลขที่บัญชี			
๒. การควบคุมการทำรายการป้อนเข้าสู่ระบบงาน ข้อมูลที่ป้อนเข้าสู่ระบบจะต้องถูกหลักเกณฑ์ ในการทำรายการ นอกจากนี้ยังรวมถึงเรื่องที่เกี่ยวกับการกระทบยอดข้อมูลนำเข้าเพื่อพิสูจน์ความถูกต้อง			
๓. การควบคุมการสื่อสารข้อมูลให้มีความถูกต้องและครบถ้วน ต้องคำนึงถึง Hardware และ Software ที่ใช้ในการสื่อสารข้อมูลการมอบอำนาจ			
๔. การควบคุมการประมวลผลด้วยคอมพิวเตอร์ มีความแม่นยำ ถูกต้อง และครบถ้วนเป็นไปตามหลักเกณฑ์การใช้แฟ้มข้อมูล การชี้แนะให้เห็นข้อผิดพลาดและการรายงาน			
๕. การควบคุมการจัดเก็บข้อมูลไว้ในระบบ การกำหนดสิทธิการใช้ข้อมูล การรักษาความปลอดภัย การแก้ไขข้อผิดพลาด การสำรองข้อมูล การกำหนดอายุการจัดเก็บแฟ้มข้อมูล			
๖. การควบคุมผลลัพธ์ การกระทบยอดข้อมูลนำเข้าและผลลัพธ์ เพื่อพิสูจน์ความถูกต้องด้วยระบบ Manual ซึ่งเป็นหน้าที่โดยตรงของหน่วยงานควบคุมคุณภาพข้อมูล			

การตรวจสอบการควบคุมเฉพาะระบบงาน

โดยการตรวจสอบในเรื่อง การกำหนดสิทธิในการใช้งานมีความเหมาะสมกับหน้าที่ความรับผิดชอบหรือไม่ การแบ่งแยกหน้าที่ในระบบงานสารสเทศ การนำเข้าข้อมูลและรายการ การรับส่งข้อมูลระหว่างระบบงานการประมวลผลในระบบงาน การนำผลลัพธ์ไปใช้งานครบถ้วน ถูกต้องหรือไม่ มีการจัดเก็บเหมาะสมหรือไม่

สรุปผลการตรวจสอบ

.....
.....
.....
.....

ผู้ตรวจสอบ ..... **ผู้สอบทาน .....**
( ) **( )**
ตำแหน่ง **ตำแหน่ง**
วันที่ **วันที่**

ผู้รับตรวจ .....
( )
ตำแหน่ง
วันที่

<u>ตัวอย่าง</u> การประเมินความเสี่ยงการตรวจสอบ

IT Security & Cyber Security (IT General Control)

ความเสี่ยง	การควบคุมที่มีอยู่	กิจกรรมที่จะตรวจสอบ
๑. การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control) ไม่มีประสิทธิภาพเพียงพอ	๑. นโยบายและแนวปฏิบัติในการักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของ สวพส. ๒. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องเรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่งคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ.๒๕๕๓ และฉบับที่ ๒ พ.ศ.๒๕๕๖ ๓. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ.๒๕๕๕ ๔. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ.๒๕๕๐ และ(ฉบับที่ ๒) พ.ศ.๒๕๖๐	๑. นโยบายและแนวปฏิบัติในการักษาความมั่นคงปลอดภัยด้านสานสนเทศ ๒. โครงสร้างทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ๓. การควบคุมการเข้าถึง เช่น การควบคุมการเข้าถึงระบบสารสนเทศการจัดการการเข้าถึงระบบของบุคลากร การควบคุมระบบและโปรแกรมประยุกต์ เป็นต้น ๔. ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมของส่วนงาน เช่น บริเวณที่ต้องมีการรักษาความปลอดภัย และการป้องกันอุปกรณ์ต่างๆ ของหน่วยงาน เป็นต้น ๕. ความปลอดภัยในการปฏิบัติงาน เช่น การกำหนดหน้าที่ความรับผิดชอบ และวิธีการปฏิบัติงาน การป้องกันมัลแวร์ การติดตั้งโปรแกรมบนระบบปฏิบัติการ การบันทึก Log และการเฝ้าดูเป็นต้น ๖. การควบคุมการพัฒนา และการบำรุงรักษาระบบสารสนเทศ
๒. การควบคุมเฉพาะระบบงาน (Application Control) ไม่มีความเหมาะสม เพียงพอ	๑. ตารางบัญชีคุมมือเพื่อใช้เทียบเคียงข้อมูลผลลัพธ์	๑) การควบคุมการนำเข้าข้อมูล ๒) การควบคุมการทำรายการป้อนเข้าสู่ระบบงาน ๓) การควบคุมการสื่อสารข้อมูลให้มีความถูกต้อง และครบถ้วน ๔) การควบคุมการประมวลผลด้วยคอมพิวเตอร์ให้ มีความแม่นยำ ถูกต้อง ๕) การควบคุมการจัดเก็บข้อไว้ในระบบการกำหนดสิทธิการใช้ข้อมูล การรักษาความปลอดภัย การแก้ไขข้อผิดพลาด การสำรองข้อมูลและการกำหนดอายุการจัดเก็บแฟ้มข้อมูล ๖) การควบคุมผลลัพธ์ การกระทบยอดข้อมูลนำเข้าและผลลัพธ์
๓. IT Security ไม่มีความเหมาะสม เพียงพอ	๑. คณะกรรมการพัฒนาระบบข้อมูลสารสนเทศของหน่วยงาน ๒. การปฏิบัติงานด้านการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอาจไม่ตรงกัน และ/หรือไม่สอดคล้องตามกลยุทธ์ หรือ	๑. การรักษาความปลอดภัยเครือข่าย(Network Security)

	วิสัยทัศน์ของส่วนงาน ทำให้ไม่สามารถปฏิบัติงานด้านบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ ๓. มีการรักษาความปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security) ที่ครอบคลุมถึงการบริหารจัดการการเปลี่ยนแปลง การบริหารจัดการขีดความสามารถของระบบ การรักษาความปลอดภัยของเครื่องแม่ข่าย การจัดเก็บข้อมูลบันทึกเหตุการณ์และตามตามดูแลระบบและการเฝ้าระวังภัยคุกคาม ๔. มีการติดตามดูแลระบบและการเฝ้าระวังภัยคุกคาม(Security Monitoring)	๒. การรักษาความปลอดภัยอินเทอร์เน็ต (Internet Security) ๓. การรักษาความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Security) ๔. การรักษาความปลอดภัยระบบคลาวด์ (Cloud Security) ๕. การรักษาความปลอดภัยการเข้าใช้งานแอปพลิเคชั่น (Application Security)
๔. Cyber Security) ไม่มีความเหมาะสม เพียงพอ : การป้องกันระบบเทคโนโลยีสารสนเทศจากภัยคุกคามทางไซเบอร์เนื่องจากเป็นเทคโนโลยีเก่าและมีอายุการใช้งานนานกว่า ๕ ปี รวมถึงภัยคุกคามที่มีการพัฒนาและปรับเปลี่ยนรูปแบบตลอดเวลา	๑. พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ๒. คณะกรรมการพัฒนาระบบข้อมูลสารสนเทศของหน่วยงาน ๓. มีแนวปฏิบัติด้านการเข้ารหัสข้อมูล(Cryptography) ในการรักษาความมั่งคงปลอดภัยของข้อมูลที่เหมาะสมตามชั้นความลับและความสำคัญของข้อมูลสารสนเทศ ๔. มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของบริษัท (Network and Communication Security) โดยมีการป้องกันข้อมูลที่มีการรับส่งผ่านเครือข่ายให้มีความปลอดภัย สามารถป้องกันและเฝ้าระวังการถูกบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้นได้ ๕. มีการจัดเก็บข้อมูลบันทึกเหตุการณ์(Logging) ของเครื่องแม่ข่าย ระบบงานและอุปกรณ์เครือข่ายที่สำคัญ โดยจะต้องมีความมั่นคงปลอดภัยเพียงพอในการป้องกันการเปลี่ยนแปลง แก้ไขหรือทำลาย รวมถึงมีการสอบทาน log ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ๖. ปรับปรุงสถาปัตยกรรมระบบเครือข่าย ได้แก่ ๖.๑ แยกเครือข่ายสำรองข้อมูลออกจากเครือข่ายหลักและจำกัดสิทธิการเข้าถึงเครือข่ายสำรอง ๖.๒ สำรองข้อมูลตามรายละเอียด ดังนี้ ๑) กำหนดตารางการสำรองข้อมูลส่วนเพิ่ม (Incremental Backup) ในทุกวัน ตั้งแต่วันจันทร์ถึงวันศุกร์ และสำรองข้อมูลทั้งระบบ (Full Backup) ในทุกวันศุกร์ ๒) จัดทำสำเนาการสำรองข้อมูลแบบ Offline Backup บนอุปกรณ์จัดเก็บข้อมูลภายนอกทุกวันจันทร์และวันพุธ ๓) แจ้งผู้พัฒนาระบบให้ทำการสำรองข้อมูลระบบงานทุกระบบเป็นประจำทุกสิ้นสัปดาห์ ๖.๓ ใช้ระบบอีเมล์กลาง ของสวพส. เพื่อป้องกันความสูญหายของข้อมูลที่รับส่งผ่านจดหมายอิเล็กทรอนิกส์ และเพื่อให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง	๑. การรักษาความปลอดภัยของระบบโครงสร้างพื้นฐาน (Critical Infrastructure Security) ๒. การรักษาความปลอดภัยระบบแอปพลิเคชั่น (Application Security) เช่น โปรแกรม Antivirus, Firewall หรือ โปรแกรมการเข้ารหัส เป็นต้น ๓. การรักษาความปลอดภัยของระบบอินเทอร์เน็ต (Network Security) ๔. การรักษาความปลอดภัยให้กับข้อมูลที่เก็บในคลาวด์ (Cloud Security ๕. การรักษาความปลอดภัยให้อุปกรณ์ Internet of Thing (Internet of Thing Security)

ตัวอย่างกระดาษทำการ การตรวจสอบ IT Security & Cyber Security

(IT General Control)

กระดาษทำการ IT xx-xx

กระดาษทำการตรวจสอบหมายเลข :

เรื่องที่ตรวจสอบ : IT Security & Cyber Security (IT General Control)

ประเด็นการตรวจสอบ : การควบคุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control) มีประสิทธิภาพ ครอบคลุมการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของส่วนงาน

วัตถุประสงค์ : เพื่อให้มั่นใจว่า การควบคลุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control) มีความเพียงพอและเหมาะสม

ขอบเขตการตรวจสอบ : การสอบทานการควบคลุมทั่วไปด้านเทคโนโลยีสารสนเทศ (General Control)

ผลการตรวจสอบ :

รายละเอียด	**ผลการตรวจสอบ**		
	มี	**ไม่มี**	**เอกสารอ้างอิง**
๑. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และการคุ้มครองข้อมูลส่วนบุคคลของส่วนงาน			
๑.๑ การทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลของส่วนงาน			
๑.๒ การสำรองข้อมูลของระบบงาน			
๑.๓ การทดสอบระบบสารสนเทศ การทสอบระบบสำรองข้อมูล การทดสอบการกู้คืนข้อมูล			
๑.๔ การบริหารจัดการคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆ			
๒. โครงสร้างทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศ			
๒.๑ การมอบหมายเจ้าหน้าที่ผู้รับผิดชอบด้านความมั่นคงปลอดภัย			
๒.๒ ความรู้ความสามารถพื้นฐานของเจ้าหน้าที่ผู้รับผิดชอบด้านความมั่นคงปลอดภัย เพียงพอ เหมาะสมต่อการปฏิบัติงาน			
๒.๓ การบริหารจัดการความมั่นคงปลอดภัย เช่น ระบบงานเกิดปัญหาหยุดชะงักไม่สามารดำเนินการได้อย่างต่อเนื่อง			
๓. การควบคุมการเข้าถึง			
๑.๑ การกำหนดรหัสผ่านเข้าเครื่องคอมพิวเตอร์			
๑.๒ มีการกำหนดสิทธิ์ผู้ดูแลระบบ ผู้ใช้งานระบบและการเก็บรักษารหัสผ่าน มีตารางแสดงสิทธิ์การเข้าถึงฐานข้อมูล มีการควบคุมและจำกัดสิทธิ์ (มีเอกสารการกำหนดสิทธิ์ : ตารางกำหนดสิทธิ์) รวมทั้งมีการทบทวนสิทธิ์เข้าถึงของผู้ใช้งานอย่าง			

ต่อเนื่องเป็นระยะตามที่กำหนดไว้ รวมทั้งมีการกำหนด			
รายละเอียด	**ผลการตรวจสอบ**		
	มี	**ไม่มี**	**เอกสารอ้างอิง**
รหัสผ่านสำหรับการเข้าถึงข้อมูลที่สำคัญ			
๔. ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อมของส่วนงาน			
๔.๑ มีการบริหารจัดการรักษาความปลอดภัยทางกายภาพ (Physical security Management) และการควบคุมพื้นที่การเข้า – ออกพื้นที่ควบคุม ได้แก้ ห้องปฏิบัติการคอมพิวเตอร์			
๕. ความปลอดภัยในการปฏิบัติงาน			
๕.๑ การติดตั้งระบบรักษาความปลอดภัย เช่น การตรวจจับการแจ้งเตือนการบุกรุก โปรแกรมสแกนไวรัส			
๕.๒ การบันทึก Log			
๖. มีการวางแผนการพัฒนาระบบ			
๖.๑ มีการวางแผนการพัฒนาระบบ			

กระดาษทำการ IT xx-xx

กระดาษทำการตรวจสอบหมายเลข :

เรื่องที่ตรวจสอบ : IT Security & Cyber Security (IT General Control)

ประเด็นการตรวจสอบ : การดำเนินการตามระบบ IT Security

วัตถุประสงค์ : เพื่อให้มั่นใจว่าการดำเนินการตามระบบ IT Security ว่ามีความเพียงพอ และเหมาะสม

ขอบเขตการตรวจสอบ : การสอบทานการดำเนินการตามระบบ IT Security

ผลการตรวจสอบ :

รายละเอียด	**ผลการตรวจสอบ**		
	มี	**ไม่มี**	**เอกสารอ้างอิง**
๑. การรักษาความปลอดภัยเครือข่าย (Network Security)			
๑.๑ การกำหนดหน้าที่ความรับผิดชอบ			
๑.๒ การเชื่อมต่อเครือข่าย			
๑.๓ มีการกำหนดชั้นความลับของข้อมูล			
๑.๔ การดูแลเส้นทางของอุปกรณ์เครือข่าย			
๑.๕ การเชื่อมต่อเครือข่าย			
๑.๖ การตรวจจับและการป้องกันการบุกรุก			
๑.๗ แผนผังระบบเครือข่าย			
๑.๘ การบันทึกการทำงานของระบบป้องกันการบุกรุก			
๒. การรักษาความปลอดภัยอินเทอร์เน็ต (Internet Security)			
๒.๑ การเข้าสู่ระบบเครือข่ายในส่วนงาน			
๒.๒ การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของอุปกรณ์เครือข่าย			
๓. การรักษาความปลอดภัยอุปกรณ์ปลายทาง (Endpoint Security)			
๓.๑ การยืนยันตัวตนในการเข้าใช้งานระบบสารสนเทศ			
๓.๒ การจัดการกับมัลแวร์หรือการโจมตีของไวรัส			
๔. การรักษาความปลอดภัยระบบคลาวด์ (Cloud Security)			
๔. การรักษาความปลอดภัยระบบคลาวด์ (Cloud Security)			
๕. การรักษาความปลอดภัยการปลอดภัยการเข้าใช้งานแอปพลิเคชั่น (Application Security)			
๕.๑ การใช้งานแอปพลิเคชั่น			
๕.๒ Application Security			

กฎ/ระเบียบ/เอกสารที่เกี่ยวข้อง

๑. พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๑) พ.ศ.๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
๒. พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒
๓. พระราชกฤษฎีการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙
๔. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่งคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๑) พ.ศ.๒๕๕๓ และฉบับที่ ๒ พ.ศ.๒๕๕๖
๕. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕
๖. กรมบัญชีกลาง, แนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศ การควบคุมภายในด้านเทคโนโลยีสารสนเทศ
๗. กรมบัญชีกลาง, จุลสารตรวจสอบภายใน ปีที่ ๒๑ ฉบับที่ ๑๑๖ ประจำเดือน กุมภาพันธ์-มีนาคม ๒๕๖๐ แนวทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศ
๘. คู่มือปฏิบัติงานการตรวจ IT Security & Cyber Security (IT General Control) กลุ่มตรวจสอบภายในสำนักบริหารหนี้สาธารณะ กระทรวงการคลัง
๙. การตรวจสอบการกำกับดูแลเทคโนโลยีสารสนเทศ Auditing IT Governance สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย (GTAG GLOBAL TECHNOLOGY AUDIT GUIDE)
๑๐. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) ปีงบประมาณ ๒๕๖๕
๑๑. นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)
