แนวทางพัฒนาการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของกองทัพบก

“ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาเศรษฐกิจพอเพียง” การพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามที่กระทบต่อความมั่นคงของชาติจะต้องพร้อมรับมือกับปัญหาความมั่นคงทุกมิติทุกรูปแบบ ภัยคุกคามทางไซเบอร์เป็นภัยคุกคามหนึ่งที่ทวีความรุนแรงมากขึ้น แนวโน้มเหล่านี้ก่อให้เกิดความท้าทายต่อการพัฒนาประเทศในหลายมิติ ทั้งในส่วนของการจ้างงานและอาชีพ สาขาการผลิตและบริการใหม่ ภัยคุกคามและความเสี่ยงด้านอื่นๆ ที่ซับซ้อนขึ้น อาชญากรรมไซเบอร์ สงครามไซเบอร์ สิ่งต่างๆ เหล่านี้เป็นอุปสรรคต่อการพัฒนาประเทศทั้งสิ้น

ประเทศจะพัฒนาอย่างรวดเร็วได้นั้นจำเป็นต้องใช้เทคโนโลยีที่ทันสมัย ต้องสร้างความมั่นคงในการเชื่อมโยงเครือข่ายดิจิทัลเชื่อมต่อกับโลกเพื่อเพิ่มความสามารถในการแข่งขัน ให้ทุกคนสามารถเข้าถึงและใช้ข้อมูลในโลกอินเทอร์เน็ตให้เกิดประโยชน์สูงสุดได้ ช่วยพัฒนาองค์ความรู้เพิ่มศักยภาพคนในสังคมเพื่อส่งเสริมยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน ดังนั้นความปลอดภัยไซเบอร์จึงเป็นสิ่งจำเป็นเพราะหากขาดความมั่นคงปลอดภัยไซเบอร์ระบบย่อมพังทลายได้โดยง่าย

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้จัดทำร่างกรอบนโนบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติขึ้นเมื่อ พ.ศ. 2556 มียุทธศาสตร์หลัก 3 ด้าน[1] ได้แก่ การบูรณาการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ และการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ปัจจุบันมีกฎหมายด้านไซเบอร์ คือ “พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562” เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

แนวคิดทฤษฎีและมาตรฐานเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology audit : IT audit) ในระดับสากล

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศถูกพัฒนาขึ้นและนำมาใช้อย่างแพร่หลายในแต่ละประเทศรวมทั้งประเทศไทย ซึ่งมาตรฐานดังกล่าวกำหนดโดยองค์กรหรือหน่วยงานทางพลเรือน สำหรับการปฏิบัติทางทหารนั้น ในประเทศสหรัฐอเมริกายึดถือตามมาตรฐานของกระทรวงกลาโหมสหรัฐอเมริกา (United States Department of Defense : DoD) ในการปฏิบัติงานด้านไซเบอร์นั้นกองทัพบกมีหน่วยรับผิดชอบหลักคือศูนย์ไซเบอร์กองทัพบกโดยยึดถือแนวทางปฏิบัติตามมาตรฐานของสถาบันมาตรฐานเทคโนโลยีสารสนเทศแห่งชาติประเทศสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ซึ่งมีหลายเรื่องที่เกี่ยวข้อง งานที่สำคัญงานหนึ่ง คือ การตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ปัจจุบันยังมีแนวทางที่ไม่ชัดเจนและจะต้องปรับปรุงให้เหมาะสมต่อไป โดยศึกษาจากมาตรฐานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และแนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศในระดับสากล

องค์การระหว่างประเทศว่าด้วยการมาตรฐาน (The International Organization for Standardization : ISO)[2] เป็นองค์กรอิสระจัดตั้งขึ้นเมื่อ พ.ศ. 2490 มีวัตถุประสงค์เพื่อส่งเสริมการกำหนดมาตรฐานและกิจกรรมที่เกี่ยวข้อง ช่วยให้การแลกเปลี่ยนสินค้าและบริการเป็นไปโดยสะดวก และช่วยพัฒนาความร่วมมือระหว่างประเทศในด้านวิชาการ วิทยาศาสตร์ เทคโนโลยี และเศรษฐกิจ มาตรฐานที่กำหนดขึ้นเรียกว่า มาตรฐานระหว่างประเทศ (international standard) ปัจจุบันมีหน่วยงานมาตรฐาน 164 แห่งทั่วโลกเผยแพร่มากกว่า 22,677[3] มาตรฐานสากล ครอบคลุมเกือบทุกด้านของเทคโนโลยีและการผลิต ประเทศไทยเป็นหนึ่งในสมาชิกสมบูรณ์ของ ISO ตั้งแต่ พ.ศ. 2509 โดยมีสำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม (The Thai Industrial Standards Institute : TISI) หรือ สมอ. ทำหน้าที่เป็นผู้แทนประเทศไทยเข้าร่วมดำเนินงานกับ ISO ทั้งทางด้านบริหารและวิชาการ

คณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอเทคนิกส์ (International Electrotechnical Commission : IEC)[4] เป็นองค์กรอิสระที่เริ่มก่อตั้งขึ้นเมื่อ พ.ศ. 2449 โดยมีวัตถุประสงค์เพื่อจัดทำมาตรฐานระหว่างประเทศทางด้านไฟฟ้า

อิเล็กทรอนิกส์ และเทคโนโลยีที่เกี่ยวข้อง นอกจากนั้นยังดำเนินการจัดทำระบบการตรวจประเมิน เพื่อการรับรองคุณภาพให้กับมาตรฐานของ IEC และเป็นเครื่องมือในการอำนวยความสะดวกทางการค้าระหว่างประเทศ

ISO/IEC 27001 มาตรฐานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems) เป็นมาตรฐานที่พัฒนาขึ้นเป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ และมาตรฐาน ISO/IEC 17799 (Information technology - Security techniques - Code of practices for information security management) เป็นแนวปฏิบัติสำหรับการประเมิน และจัดการความเสี่ยงรวมถึงแนวทางในการควบคุมตามมาตรฐาน ISO/IEC 27001

มาตรฐาน ISO/IEC 27001:2013[5] แบ่งเนื้อหาออกเป็น 2 ส่วนได้แก่ แนวทางการบริหารความมั่นคงปลอดภัยสารสนเทศที่ขับเคลื่อนผ่านวงจร PDCA ประกอบด้วย การวางแผน (Plan) การลงมือทำ (Do) การตรวจสอบ (Check) และการปรับปรุงแก้ไข (Act) มาตรการจัดการความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (organization of Information Security) ความมั่นคงปลอดภัยสำหรับทรัพยากรบุคคล (Human Resource Security) การบริหารจัดการทรัพย์สิน (Asset Management) การควบคุมการเข้าถึง (Access Control) การเข้ารหัสข้อมูล (Cryptography) ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security) ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operations Security) ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security) การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance) ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships) การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management) ความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management) และการปฏิบัติตามกฎระเบียบ (Compliance)

ISO/IEC TR 27008:2011[6] เป็นมาตรฐานที่เกี่ยวกับเทคโนโลยีสารสนเทศ เทคนิคต่างๆ ด้านการรักษาความมั่นคงปลอดภัย รวมทั้งแนวทางสำหรับผู้ตรวจประเมินการควบคุมความปลอดภัยสารสนเทศ ครอบคลุมทุกประเภทและทุกขนาดขององค์กร ทั้งภาครัฐ ภาคเอกชน หน่วยงานราชการ และองค์กรที่ไม่แสวงหาผลกำไร ด้วยการตรวจสอบความปลอดภัยของข้อมูลและการตรวจสอบการปฏิบัติทางเทคนิค อ้างอิงตาม ISO/IEC 27001

ISO/IEC TR 27008 ให้แนวคิดในการเลือกมาตรการควบคุมที่เหมาะสมกับองค์กร โดยพิจารณาจากผลการประเมินความเสี่ยง การตรวจสอบมาตรการควบคุมและการตรวจสอบทางเทคนิคช่วยให้เข้าใจปัญหาที่อาจเกิดขึ้น ทราบถึงผลกระทบที่เกิดจากมาตรการที่ใช้ดำเนินการต่อภัยคุกคามและช่องโหว่ด้านความปลอดภัยที่ไม่เพียงพอ ช่วยจัดลำดับความสำคัญของกิจกรรมลดความเสี่ยง ยืนยันว่าจุดอ่อนหรือข้อบกพร่องที่ระบุไว้หรือที่เกิดขึ้นก่อนหน้านี้ได้รับการแก้ไขอย่างเพียงพอแล้ว และช่วยสนับสนุนการตัดสินใจด้านงบประมาณที่เกี่ยวข้องกับการปรับปรุงความปลอดภัยสารสนเทศขององค์กร

ภาพรวมของการตรวจสอบการควบคุมความปลอดภัยสารสนเทศ กระบวนการตรวจสอบเริ่มจากการรวบรวมข้อมูลเบื้องต้น ตรวจสอบขอบเขตการทำงานตามแผนที่วางไว้ ประสานงานกับผู้จัดการและส่วนอื่นๆ ที่เกี่ยวข้องขององค์กร ประเมินความเสี่ยงเพื่อจัดทำแนวทางในการตรวจสอบจริง ผู้ตรวจสอบที่ดีจะต้องเตรียมความพร้อมทั้งในด้านการควบคุมความปลอดภัยของข้อมูลที่ได้รับมอบและด้านการทดสอบ โดยกระบวนการตรวจสอบแบ่งเป็น ขั้นการตรวจสอบ ขั้นการรายงานผล และขั้นการติดตามผล

การจัดทำแผน ประกอบด้วย ภาพรวม ขอบเขต กระบวนการทบทวน ข้อพิจารณาเกี่ยวกับสิ่งที่ต้องทำการตรวจ ผลการตรวจสอบที่ผ่านมา การมอบหมายงาน ระบบภายนอก ข้อมูลสินทรัพย์และองค์กร ขั้นตอนการทบทวนเพิ่มเติม การปรับให้เหมาะสม และการสรุปผล หลังจากเลือกขั้นตอนการตรวจสอบ ปรับแต่งให้เหมาะสมกับเงื่อนไขเฉพาะขององค์กรแล้ว กำหนดขั้นตอนการตรวจสอบเพิ่มเติมตามความจำเป็น ระบุโอกาสที่จะเกิดเหตุการณ์ไม่คาดคิดที่ส่งผลกระทบต่อการดำเนินการตามแผนตรวจสอบและกำหนดเวลา รวมถึงเป้าหมายหลักสำหรับกระบวนการตรวจสอบจนได้แผนตรวจสอบที่เสร็จสมบูรณ์แล้วเสนอให้องค์กรรับการตรวจสอบอนุมัติแผน

เมื่อได้รับอนุมัติแผนการตรวจสอบแล้ว ผู้ตรวจสอบจะดำเนินการตามแผนและกำหนดเวลาที่ตกลงไว้ เกณฑ์การตรวจสอบได้แก่ พอใจ (S) : เป็นไปตามวัตถุประสงค์การควบคุม พอใจบางส่วน (P) : บางส่วนไม่เป็นไปตามวัตถุประสงค์การควบคุม หรืออยู่ในระหว่างดำเนินการโดยเชื่อได้ว่าจะสำเร็จเป็นไปตามวัตถุประสงค์การควบคุม และนอกเหนือจากความพึงพอใจ (O) : ความผิดปกติที่อาจเกิดขึ้นในการดำเนินงาน หรือข้อมูลไม่เพียงพอ

การวิเคราะห์และการรายงานผล ประกอบด้วย ประสิทธิผลของมาตรการควบคุม ประสิทธิผลในภาพรวมขององค์กร และสิ่งที่ตรวจพบ คำแนะนำในการแก้ไขจุดบกพร่องและลดช่องโหว่ของมาตรการควบคุม หากเป็นไปได้ควรให้หน่วยรับตรวจแก้ไขจุดบกพร่องให้เรียบร้อยและตรวจอีกครั้งก่อนที่จะรายงานสรุปขั้นสุดท้าย และควรให้มีการติดตามผลการแก้ไขข้อบกพร่อง เช่น 3 เดือนภายหลังการรายงานขั้นสุดท้าย

ผลการตรวจสอบ ควรรายงานอย่างเป็นกลางและเป็นข้อเท็จจริงในสิ่งที่พบเกี่ยวกับมาตรการควบคุมที่ตรวจสอบ รายงานส่วนที่ได้รับผลกระทบ หากตรวจพบแนวโน้มที่จะบกพร่องและเกิดความเสี่ยงต่อองค์กร ผู้ตรวจสอบควรแจ้งผู้รับผิดชอบเพื่อแก้ทันที

นอกจากนี้ ISO/IEC TR 27008 ยังให้แนวทางการตรวจสอบทางเทคนิค ที่เกี่ยวกับมาตรการควบคุมรหัสที่เป็นอันตราย การบันทึก log การจัดการสิทธิ์ การสำรองข้อมูล การจัดการความปลอดภัยเครือข่าย การควบคุมในความรับผิดชอบของผู้ใช้ และให้แนวทางการรวบรวมข้อมูลเบื้องต้นที่เกี่ยวกับ ทรัพยากรมนุษย์ ความปลอดภัย นโยบายองค์กร ความปลอดภัยทางกายภาพ สิ่งแวดล้อม และการจัดการเหตุการณ์

คณะกรรมการผู้สนับสนุนองค์กร (Committee of Sponsoring Organizations : COSO)[7] ก่อตั้งขึ้นในปี 2528 โดยสมาคมวิชาชีพ 5 แห่งในสหรัฐอเมริกา เพื่อสนับสนุนคณะกรรมการเพื่อการรายงานการทุจริตแห่งชาติในการศึกษาปัจจัยที่อาจนำไปสู่การรายงานทางการเงินที่หลอกลวง โดยพัฒนากรอบการทำงานและคำแนะนำเกี่ยวกับการบริหารความเสี่ยงขององค์กร การควบคุมภายใน และการป้องกันการฉ้อโกงที่ออกแบบมาเพื่อปรับปรุงประสิทธิภาพขององค์กรและธรรมาภิบาล

COSO ให้คำนิยาม การควบคุมภายใน (Internal Control)[8] คือ กระบวนการปฏิบัติงานที่บุคลากรในองค์กร โดยคณะกรรมการบริหาร ผู้บริหารทุกระดับ และพนักงานทุกคนมีบทบาทร่วมกันในการจัดให้มีขึ้นเพื่อสร้างความเชื่อมั่นอย่างสมเหตุสมผลว่าการปฏิบัติงาน

จะบรรลุวัตถุประสงค์ของการควบคุมภายใน มีวัตถุประสงค์ 3 ประการ ได้แก่ 1) ประสิทธิภาพและประสิทธิผลของการปฏิบัติงาน 2) ความเชื่อถือได้ของรายงานทางการเงิน 3) การปฏิบัติตามกฎหมายและกฎระเบียบ

องค์ประกอบของการควบคุมภายในตามแนวคิดของ COSO มี 5 ประการ ได้แก่ 1) สภาพแวดล้อมการควบคุม 2) การประเมินความเสี่ยง 3) กิจกรรมการควบคุม 4) ข้อมูลสารสนเทศและการสื่อสาร 5) การติดตามประเมินผล

การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management)[9] หมายถึง กระบวนการที่บุคลากรทั่วทั้งองค์กรได้มีส่วนร่วมในการคิด วิเคราะห์ และคาดการณ์ถึงเหตุการณ์ หรือความเสี่ยงที่อาจเกิดขึ้น รวมทั้งระบุแนวทางจัดการกับความเสี่ยงดังกล่าวให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ เพื่อช่วยให้องค์กรบรรลุวัตถุประสงค์ที่ต้องการตามกรอบวิสัยทัศน์ และพันธกิจขององค์กร

การบริหารความเสี่ยงตามมาตรฐาน COSO มีองค์ประกอบ 8 ประการ 1) สภาพแวดล้อมภายในองค์กร (Internal Environment) เป็นองค์ประกอบที่สำคัญในการกำหนดกรอบบริหารความเสี่ยง ได้แก่ วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติงาน บุคลากร กระบวนการทำงาน ระบบสารสนเทศ ระเบียบ เป็นต้น 2) กำหนดวัตถุประสงค์ (Objective Setting) ต้องสอดคล้องกับกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ 3) การบ่งชี้เหตุการณ์ (Event Identification) รวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงานทั้งปัจจัยเสี่ยงภายในและภายนอกองค์กร 4) การประเมินความเสี่ยง (Risk Assessment) การจำแนกและจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) 5) การตอบสนองความเสี่ยง (Risk Response) นำความเสี่ยงไปดำเนินการตอบสนองด้วยวิธีการที่เหมาะสมเพื่อลดความสูญเสียหรือโอกาสที่จะเกิดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้ 6) กิจกรรมการควบคุม (Control Activities) กำหนดกิจกรรมการปฏิบัติเพื่อลดความเสี่ยงทำให้การดำเนินงานบรรลุวัตถุประสงค์และเป้าหมายองค์กร 7) สารสนเทศและการสื่อสาร (Information and Communication) ช่วยสร้างความเข้าใจแก่ผู้มีส่วนเกี่ยวข้องกับการควบคุมภายใน 8) การติดตามประเมินผล (Monitoring) เพื่อให้ทราบถึงผลการดำเนินการว่ามีความเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

Control Objectives for Information and Related Technology (COBIT)[10] คือ กรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร ได้รับการพัฒนาและเผยแพร่เวอร์ชั่นแรกในปี พ.ศ. 2539 โดยสมาคมการควบคุมและการตรวจสอบระบบสารสนเทศ (The Information Systems Audit and Control Association : ISACA) และสถาบันเทคโนโลยีสารสนเทศภิบาล Information Technology Governance Institute : ITGI) ปัจจุบันเป็นเวอร์ชั่น COBIT 2019

COBIT 5 มีหลักพื้นฐานสำคัญ 5 ประการ[11] คือ 1) การตอบสนองความต้องการของผู้ที่เกี่ยวข้อง (Meeting Stakeholder Needs) 2) การครอบคลุมองค์กรทั้งองค์กร (Covering the Enterprise end-to-end) 3) การรวมมาตรฐานต่างๆ ให้อยู่ภายใต้ framework เดียวกัน (Applying a Single Integrated Framework) 4) การใช้ปัจจัยก่อเกิดร่วมกันทั้งหมดในการปฏิบัติ (Enabling a Holistic Approach) 5) การแยกเรื่องการกำกับดูแลออกจากเรื่องการบริหารจัดการ (Separating Governance from Management)

COBIT 5 ได้รวมมาตรฐานต่างๆ ของ ISACA และ IT Governance Institute ให้อยู่ภายใต้ framework เดียวกัน[12] โดยมี COBIT 4.1 เป็นหลักรวมกับมาตรฐานอื่นๆ ได้แก่ การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Business Model For Information Security : BMIS) ประโยชน์หรือคุณค่าของการนำเทคโนโลยีสารสนเทศมาใช้งาน (Val IT) การบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (Risk IT) การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Assurance Framework : ITAF) การนำการกำกับดูแลมาใช้งาน (Taking Governance Forward : TGF) บทบาทและอำนาจหน้าที่ของบอร์ดและผู้ที่เกี่ยวข้องในการกำกับดูแลเทคโนโลยีสารสนเทศ (Board Briefing on IT Governance) อีกทั้งยังสอดคล้องกับมาตรฐานอื่นที่มีลักษณะเดียวกัน เช่น Information Technology Infrastructure Library (ITIL), ISO, COSO เป็นต้น

ITAF[13] เป็นกรอบแนวทางที่ให้คำแนะนำเกี่ยวกับการออกแบบ การดำเนินการ และการรายงานการตรวจสอบสารสนเทศ รวมทั้งกำหนดมาตรฐาน หน้าที่ และความรับผิดชอบด้านวิชาชีพการตรวจสอบสารสนเทศและการประกันด้านเทคโนโลยีสารสนเทศ เผยแพร่โดย ISACA เนื้อหาแบ่งเป็น มาตรฐานทั่วไป มาตรฐานการปฏิบัติงาน มาตรฐานการรายงาน แนวทาง เครื่องมือ และเทคนิคการตรวจสอบ

มาตรฐานทั่วไป ผู้ตรวจสอบจะต้องมีความเป็นอิสระและความเที่ยงธรรม มีความคาดหวังที่สมเหตุสมผล ได้รับความร่วมมือจากฝ่ายบริหาร มีทักษะและความเชี่ยวชาญในการตรวจสอบ มีความรู้ในเรื่องที่จะตรวจสอบ มีการวางแผน การดำเนินการและการรายงานอย่างมืออาชีพ และประเมินตามเกณฑ์ที่เหมาะสม (เที่ยงธรรม สามารถวัดได้ ความเข้าใจครบถ้วน และความเกี่ยวข้อง) มีกำหนดเกณฑ์ที่แน่ชัด และเหมาะสมกับองค์กร

มาตรฐานการปฏิบัติงาน ประกอบด้วย การวางแผนและการกำกับดูแล (วัตถุประสงค์ของการตรวจสอบ เกณฑ์ที่ใช้ ระดับความเชื่อมั่นที่ต้องการ ลักษณะของเนื้อหา แหล่งข้อมูลและหลักฐาน ความพร้อมใช้งาน ข้อสรุปเบื้องต้น ความต้องการทรัพยากร ความเชี่ยวชาญ กำหนดเวลา งบประมาณค่าใช้จ่าย รวมทั้งเงื่อนไขในการขยายขอบเขตการตรวจสอบ) มีหลักฐานที่เพียงพอโดยใช้ขั้นตอนการรวบรวมที่เหมาะสม มีการกำหนดตารางการตรวจสอบร่วมกัน และจัดทำเอกสารรับรองการตรวจสอบเป็นลายลักษณ์อักษร

มาตรฐานการรายงาน ระบุประเภทของรายงาน วิธีการและข้อมูลที่จะสื่อสาร เนื้อหาควรประกอบด้วย ชื่อผู้รับรายงาน ลักษณะและวัตถุประสงค์ หน่วยรับตรวจ สาระสำคัญของการตรวจ คำอธิบายลักษณะขอบเขตงาน กำหนดกรอบเวลา ห้วงเวลาที่ดำเนินการ มาตรฐานอ้างอิง ความรับผิดชอบของฝ่ายบริหารและฝ่ายตรวจสอบ เกณฑ์ที่ใช้ประเมิน ระดับความเชื่อมั่นที่ได้รับ ข้อจำกัดการใช้และแจกจ่ายรายงาน วันที่บันทึก สถานที่บันทึก ผู้รายงาน และลายเซ็นของผู้ตรวจสอบ

แนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศ 1) การสร้างทีมตรวจสอบให้มีความพร้อม มีการแต่งตั้งเป็นลายลักษณ์อักษร มีขีดความสามารถในการปฏิบัติ มีความพร้อมทั้งคน เครื่องมือ เทคนิค แผนกลยุทธ์ กระบวนการ งบประมาณ รายชื่อผู้ติดต่อ ช่องทางการสื่อสาร และมีรูปแบบการรายงานอย่างเป็นทางการ 2) การวางแผนและกำหนดขอบเขตวัตถุประสงค์ วางแผนร่วมกับคณะกรรมการ ผู้บริหารระดับสูง และผู้รับตรวจ ให้ตรงตามวัตถุประสงค์ของผู้มีส่วนร่วม และคำนึงถึงความเสี่ยงในด้านเทคโนโลยี กระบวนการ โปรแกรมประยุกต์และระบบ 3) กำหนดขอบเขตงาน วางแผนตรวจสอบ 14 ขั้นตอน กำหนดวัตถุประสงค์ ขอบเขต มาตรฐาน ระบุและจัดทำเอกสารความเสี่ยง ระบุกระบวนการเปลี่ยนแปลง กำหนดความสำเร็จ ทรัพยากรที่จำเป็น กำหนดส่งมอบ รับการสนับสนุนจากผู้บริหาร ทบทวนทรัพยากรที่ต้องการ กำหนดทีมตรวจสอบสนับสนุน

กำหนดตารางปฏิบัติ ยืนยันเป้าหมายและวิธีการ แผนการสื่อสาร 4) ระบุความเสี่ยง ทั้งความเสี่ยงร่วมและความเสี่ยงระหว่างการปฏิบัติ 5) การจัดการตรวจสอบ กิจกรรมสำคัญ สิ่งที่ต้องบริหารจัดการได้แก่ การวางแผนและงบประมาณ ระยะเวลาและทรัพยากร หน้าที่และความรับผิดชอบ การกำกับดูแล การติดตามความคืบหน้า ข้อผิดพลาด ข้อบกพร่องในการปฏิบัติ การใช้ผู้เชี่ยวชาญ การสื่อสารระหว่างทีมตรวจสอบและผู้รับตรวจ การวางแผนฉุกเฉิน ความสัมพันธ์ของผู้ตรวจสอบและผู้รับตรวจ 6) การบูรณาการกระบวนการตรวจสอบและการประกันเป็นการรวมความคิดในการตรวจสอบด้านเทคโนโลยีสารสนเทศและด้านธุรกิจรวมทั้งการบริหารความเสี่ยงเข้าด้วยกัน 7) รวบรวมหลักฐาน 8) บันทึกการดำเนินการต่างๆ เกี่ยวกับประเภทของหลักฐานทั้งอิเล็กทรอนิกส์และหลักฐานจากบุคคลที่สาม ข้อกำหนดทางกฎหมาย การรักษาความปลอดภัยหลักฐาน การบันทึกและการเก็บรักษา เนื้อหาและเวลาตามลำดับที่ตรวจพบ 9) การจัดทำเอกสารรายงานการตรวจสอบ จะต้องได้รับการสนับสนุนจากหลักฐานที่เหมาะสม อาจเป็นคู่มือ อิเล็กทรอนิกส์ หรือสื่ออื่นๆ ทั้งทางตรง เช่น เอกสารที่ผิดพลาด หรือทางอ้อม เช่น การยืนยันเหตุการณ์ของบุคคลที่สาม หลักฐานต่างๆ อาจนำไปใช้ในการดำเนินคดีได้ บันทึกการตรวจสอบจะมีผลทางกฎหมายมากกว่า เอกสารที่ใช้จดระหว่างการตรวจ 10) การประเมินผลและข้อเสนอแนะ ยืนยันข้อสรุป หาสาเหตุที่แท้จริง เพื่อนำไปสู่คำแนะนำที่เหมาะสมและสามารถนำไปใช้ได้จริง ระบุขั้นตอนที่จำเป็นเพื่อให้เกิดการยอมรับของผู้มีส่วนร่วม 11) การรายงานการตรวจสอบอย่างมีประสิทธิภาพด้วยเนื้อหาที่เป็นลายลักษณ์อักษร ด้วยวาจา และการนำเสนอ presentation-style reports เพื่อระบุปัญหาและข้อกังวลต่างๆ 12) ข้อเสนอแนะควรรายงานแยกต่างหากและไม่เป็นส่วนหนึ่งของรายงานการตรวจสอบ การรายงานถึงผู้บริหารระดับสูงควรจัดการกับปัญหาและแนวคิด โดยมีรายละเอียดการตรวจสอบที่ใช้เป็นภาพประกอบของปัญหาหรือผลลัพธ์ การรายงานถึงผู้บริหารระดับกลางควรมีข้อมูลที่เพียงพอเพื่อให้พวกเขาเข้าใจปัญหาได้อย่างเต็มที่และจัดการกับปัญหา ข้อเสนอแนะควรรวมถึงการจัดให้มีการติดตามอย่างทันเวลา

The National Institute of Standards and Technology (NIST)[14] เป็นหน่วยงานหนึ่งของกระทรวงพาณิชย์ของสหรัฐอเมริกา ก่อตั้งขึ้นในปี 1901 มีภารกิจในการส่งเสริมนวัตกรรมของสหรัฐอเมริกาและความสามารถในการแข่งขันของอุตสาหกรรมโดยการ

พัฒนาวิทยาศาสตร์มาตรฐานและเทคโนโลยีการวัดในลักษณะที่ช่วยเพิ่มความมั่นคงทางเศรษฐกิจและปรับปรุงคุณภาพชีวิต

NIST SP 800-171[15] คือ ชุดข้อกำหนดความปลอดภัยที่แนะนำสำหรับหน่วยงานรัฐบาลกลางเพื่อปกป้องความลับของข้อมูลที่ไม่ได้รับการจำแนกประเภท (Controlled Unclassified Information - CUI) แบ่งเป็น 14 หมวด ได้แก่ 1) การควบคุมการเข้าถึง (Access Control) 2) การรับรู้และการฝึกอบรม (Awareness and Training) 3) การตรวจสอบและความรับผิดชอบ (Audit and Accountability) 4) การจัดการการตั้งค่า (Configuration Management) 5) การระบุและรับรองความถูกต้อง (Identification and Authentication) 6) การเผชิญเหตุ (Incident Response) 7) การซ่อมบำรุง (Maintenance) 8) การป้องกันสื่อ (Media Protection) 9) ความปลอดภัยของบุคลากร (Personnel Security) 10) การป้องกันทางกายภาพ (Physical Protection) 11) การประเมินความเสี่ยง (Risk Assessment) 12) การประเมินความปลอดภัย (Security Assessment) 13) การป้องกันระบบและการสื่อสาร (Systems and Communications Protection) 14) ความสมบูรณ์ของระบบและสารสนเทศ (System and Information Integrity)

NIST Handbook 162[16] คือ คู่มือสำหรับปฏิบัติตามข้อกำหนดของ NIST SP 800-171 เนื้อหาประกอบด้วยชุดคำถามซึ่งจำแนกเป็น 14 หมวด ให้เลือกตอบ 5 แบบ (Yes / No / Partially / Does Not Apply / Alternative Approach) พร้อมทั้งมีคำอธิบายข้อมูลเพิ่มเติมให้เข้าใจถึงมาตรการควบคุมในแต่ละข้อมากขึ้น คำแนะนำว่าสามารถตรวจสอบข้อมูลได้จากส่วนใดบ้าง ให้สอบถามข้อมูลกับบุคคลใด และวิธีทำการทดสอบ

การเตรียมการสำหรับการประเมินการควบคุมความปลอดภัย สร้างความมั่นใจว่าพนักงานเข้าใจแผนและนโยบายด้านความปลอดภัยของบริษัท กำหนดวัตถุประสงค์และขอบเขต แจ้งให้พนักงานที่รับผิดชอบเตรียมพร้อมรับการประเมิน สร้างช่องทางการสื่อสารระหว่างพนักงานที่มีความสนใจในการประเมิน กำหนดกรอบเวลา เลือกผู้ประเมิน/ทีมประเมิน รวบรวมทรัพยากร (นโยบาย ขั้นตอน แผน ข้อกำหนด การออกแบบ บันทึก คู่มือผู้ดูแลระบบ/ผู้ปฏิบัติงาน เอกสารระบบข้อมูล ข้อตกลงการเชื่อมต่อโครงข่าย ผลการประเมินก่อนหน้านี้ และข้อกำหนดทางกฎหมาย)

เริ่มต้นการประเมินโดยทำความเข้าใจเกี่ยวกับการดำเนินงานของหน่วยรับการตรวจและวิธีที่ระบบข้อมูลสนับสนุนการดำเนินงานขององค์กรเหล่านั้น ทำความเข้าใจโครงสร้างของระบบข้อมูล ระบุบุคลากรที่รับผิดชอบการพัฒนาและการปฏิบัติตามข้อกำหนดด้านความปลอดภัยและประชุมเพื่อให้เข้าใจถึงวัตถุประสงค์และขอบเขตของการประเมิน รับทรัพยากรที่จำเป็นสำหรับการประเมิน สร้างจุดติดต่อหน่วยรับตรวจ รับผลการประเมินก่อนหน้าที่อาจนำมาใช้ซ้ำ และพัฒนาแผนการประเมินผล

ผลการประเมิน มี 5 แนวทางซึ่งแต่ละแนวทางมีข้อกำหนดที่ต้องปฏิบัติตาม ประกอบด้วย 1) ใช่ (Yes) : อธิบายว่าระบบสารสนเทศใช้ข้อกำหนดอย่างไร 2) ไม่ใช่ (No) : อธิบายว่าทำไมไม่ปฏิบัติตามข้อกำหนดด้านความปลอดภัย 3) บางส่วน (Partially) : อธิบายว่าทำไมถึงต้องปฏิบัติตามข้อกำหนดด้านความปลอดภัยบางส่วน 4) ไม่ได้ใช้ (Does Not Apply) : อธิบายว่าทำไมไม่นำข้อกำหนดด้านความปลอดภัยไปใช้กับสภาพแวดล้อมการทำงานของคุณ 5) ทางเลือกวิธีการ (Alternative Approach) : อธิบายวิธีการทางเลือกทั้งหมดและมีประสิทธิภาพเท่ากันและอธิบายว่าระบบข้อมูลใช้ข้อกำหนดอย่างไร

IT Auditing: Using Controls to Protect Information Assets[17] เป็นหนังสือที่อธิบายหลักการสำหรับการตรวจสอบด้านเทคโนโลยีสารสนเทศ รวมทั้งให้แนวทางในการดำเนินการดังนี้ แนวคิดพื้นฐานของการตรวจสอบ คือ การควบคุมภายใน ภารกิจที่แท้จริงของแผนกตรวจสอบภายใน คือ การช่วยปรับปรุงสถานะของการควบคุมภายขององค์กร

การควบคุมภายใน คือ กลไกที่สร้างความเชื่อมั่นว่ากระบวนการทำงานขององค์กรมีความเหมาะสม สามารถทำให้บรรลุวัตถุประสงค์ขององค์กรได้ ผู้ตรวจสอบจะต้องค้นหาความเสี่ยงที่กระทบวัตถุประสงค์ขององค์กร และตรวจสอบให้แน่ใจว่ามีการควบคุมภายในเพื่อลดความเสี่ยงเหล่านั้น แบ่งเป็น 3 ประเภท 1) ควบคุมเชิงป้องกัน (Preventive Controls) เพื่อลดข้อผิดพลาด 2) ควบคุมเชิงสืบค้น ค้นหาหรือสืบหาความเสียหายที่เกิดขึ้นแล้ว 3) ควบคุมเชิงแก้ไข ตรวจสอบและแก้ไขปัญหาหรือข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง

ก่อนทำการตรวจสอบจะต้อง “กำหนดสิ่งที่จะตรวจสอบ” เสียก่อนเนื่องจากทรัพยากรที่มีอยู่อย่างจำกัดจะต้องใช้ให้เกิดประสิทธิภาพและประสิทธิผลสูงสุด ดังนั้นจึงต้องพิจารณาพื้นที่ที่มีความเสี่ยงมากที่สุด และเพิ่มมูลค่าให้กับองค์กรได้มากที่สุด

กระบวนการตรวจสอบด้านเทคโนโลยีสารสนเทศ มีขั้นตอนดังนี้ 1) วางแผน Planning กำหนดวัตถุประสงค์และขอบเขตของการตรวจสอบ ใช้ข้อมูลความคิดเห็นด้านการบริหารจัดการสารสนเทศไปสู่การกำหนดเวลาการตรวจสอบและรายชื่อผู้ติดต่อที่สำคัญสำหรับทีมตรวจสอบ สำรวจเบื้องต้นเพื่อทำความเข้าใจการทำงานของระบบ ทบทวนพื้นที่ตรวจสอบให้สอดคล้องกับผลการประเมินความเสี่ยง (บางครั้งหน่วยรับการตรวจอาจกันผู้ตรวจออกจากบางพื้นที่ที่ไม่ต้องการถูกตรวจสอบ) ใช้รายการตรวจสอบมาตรฐาน (Standard checklists) ค้นคว้าหาข้อมูลเพิ่มเติมเกี่ยวกับพื้นที่ที่กำลังจะทำการตรวจสอบประเมินความเสี่ยงในพื้นที่ที่ได้รับการทบทวน การกำหนดเวลาการตรวจสอบ การประชุมเริ่มโครงการเพื่อแจ้งกำหนดการและรับฟังความเห็นของหน่วยรับการตรวจ 2) ดำเนินการตรวจสอบ (Fieldwork and documentation) รับข้อมูลและสัมภาษณ์เพื่อวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นและตัดสินว่าความเสี่ยงใดที่ไม่ได้รับการบรรเทาอย่างเหมาะสม จัดทำเอกสารรายงานสิ่งที่ดำเนินการตรวจสอบ สิ่งที่พบ ข้อสรุป และเหตุผลของข้อสรุป 3) การค้นพบปัญหาและการตรวจสอบปัญหา (Issue discovery and issue validation) ผู้ตรวจสอบจะบันทึกรายการข้อบกพร่องหรือข้อกังวลที่อาจเกิดขึ้น โดยหารือกับผู้รับการตรวจเพื่อให้แน่ใจว่าปัญหาทั้งหมดนั้นถูกต้องและเชื่อถือได้ 4) การพัฒนาหนทางแก้ปัญหา (Solution development) หลังจากระบุปัญหาเป็นขั้นตอนพัฒนาแผนปฏิบัติการสำหรับจัดการปัญหาร่วมกับหน่วยรับการตรวจ ทำได้ 3 วิธีคือ วิธีแรกให้คำแนะนำสำหรับการจัดการกับปัญหา วิธีที่สองรายงานปัญหาพร้อมแนวทางแก้ไขให้หน่วยรับการตรวจดำเนินการและรายงานผลการแก้ไขให้ทราบ และวิธีที่สามพัฒนาแนวทางแก้ปัญหาร่วมกันโดยอาศัยความรู้ในการควบคุมของผู้ตรวจและแนวทางแก้ปัญหาตามความรู้ในการดำเนินงานในชีวิตจริงของหน่วยรับการตรวจ 5) การจัดทำรายงาน (Report drafting and issuance) รายงานการตรวจสอบเป็นบันทึกการตรวจสอบ ผลลัพธ์และแผนปฏิบัติในการแก้ปัญหา รวมทั้งเป็นการรายงานผู้บริหารถึงพื้นที่ที่ตรวจสอบแล้ว องค์ประกอบสำคัญของรายงานประกอบด้วย คำชี้แจงขอบเขตการตรวจสอบ บทสรุปผู้บริหาร และรายการปัญหาพร้อมกับแผนปฏิบัติการเพื่อแก้ไขปัญหา 6) การติดตามปัญหา (Issue tracking) การตรวจสอบไม่เสร็จสมบูรณ์อย่างแท้จริงจนกว่าปัญหาที่เกิดขึ้นจะได้รับการแก้ไข กระบวนการติดตาม อาจใช้ฐานข้อมูลที่มีคะแนนการตรวจสอบทั้งหมด และวันครบกำหนด พร้อมกับกลไกสำหรับการทำเครื่องหมายว่าปิด เกินกำหนด และอื่นๆ

ตัวอย่างแนวทางการตรวจสอบที่ระบุขั้นตอนการตรวจสอบ สิ่งที่ต้องตรวจสอบ และวิธีการตรวจสอบ แบ่งหัวข้อรายการตรวจสอบดังนี้ การตรวจสอบการควบคุมระดับนิติบุคคล (Auditing Entity-Level Controls) การตรวจสอบศูนย์ข้อมูลและการกู้คืนความเสียหาย (Auditing Data Centers and Disaster Recovery) การตรวจสอบสวิตช์เราเตอร์และไฟร์วอลล์ (Auditing Switches, Routers, and Firewalls) การตรวจสอบระบบปฏิบัติการ Windows (Auditing Windows Operating Systems) การตรวจสอบระบบปฏิบัติการ Unix และ Linux (Auditing Unix and Linux Operating Systems) การตรวจสอบเว็บเซิร์ฟเวอร์และเว็บแอปพลิเคชัน (Auditing Web Servers and Web Applications) การตรวจสอบฐานข้อมูล (Auditing Databases) การตรวจสอบการจัดเก็บข้อมูล (Auditing Storage) การตรวจสอบสภาพแวดล้อมเสมือนจริง (Auditing Virtualized Environments) การตรวจสอบ WLAN และอุปกรณ์มือถือ (Auditing WLAN and Mobile Devices) การตรวจสอบโปรแกรมประยุกต์ (Auditing Applications) การตรวจสอบระบบคลาวด์คอมพิวติ้งและการดำเนินงานจากภายนอก (Auditing Cloud Computing and Outsourced Operations) และการตรวจสอบโครงการของบริษัท (Auditing Company Projects)

มาตรฐาน IT audit ของหน่วยงานทางพลเรือนในประเทศไทย

ชมรมผู้ตรวจสอบภายในธนาคารและสถาบันการเงิน (Bank & Financial Institution Internal Auditors Club - BFIIA)[18] เป็นการรวมกลุ่มของผู้ตรวจสอบธนาคารแห่งประเทศไทยและธนาคารพาณิชย์ต่างๆ โดยมีวัตถุประสงค์เพื่อแลกเปลี่ยนความรู้ข่าวสารระหว่างกัน การแจ้งกรณีทุจริตต่างๆ ที่เกิดขึ้นและร่วมกันหาวิธีป้องกัน รวมถึงการพิจารณาให้มีการจัดอบรมสำหรับผู้ที่ประกอบวิชาชีพการตรวจสอบภายในเพื่อพัฒนาศักยภาพในการปฏิบัติงานของผู้ตรวจสอบภายในธนาคารพาณิชย์ มาตรฐานด้าน IT audit ที่ใช้ได้แก่ COBIT ปัจจุบันยังคงใช้ เวอร์ชั่น 5 เป็นกรอบการทำงาน

ฝ่ายตรวจสอบเทคโนโลยีสารสนเทศ สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงินของธนาคารแห่งประเทศไทย[19] จัดทำแนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศ (SA-IT Examination Guideline) ให้สอดคล้องตามกรอบมาตรฐานสากล โดยศึกษาเปรียบเทียบแนวทางการตรวจสอบของหน่วยงานกำกับดูแลในต่างประเทศที่มี

การพัฒนาแนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศเป็นที่ยอมรับในระดับสากล ได้แก่ FFIEC (สหรัฐอเมริกา) และ MAS (สิงคโปร์) เพื่อนำมาปรับปรุงแนวทางการตรวจสอบให้เหมาะสมกับระบบสถาบันการเงินในประเทศไทย

สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.)[20] จัดทำคู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศ ตามแนวทางการกำกับดูแลตามความเสี่ยง (IT Audit Manual - Risk Based Supervision) เพื่อเป็นแนวทางในการกำกับดูแลตรวจสอบและติดตามการใช้เทคโนโลยีสารสนเทศของบริษัทประกันภัยให้มีความสอดคล้องกับระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยยึดถือตามกรอบมาตรฐาน COBIT 5 for Assurance ของสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (ISACA)

บริษัทเอกชนที่ให้บริการปรึกษาด้านความปลอดภัยเทคโนโลยีสารสนเทศ และตรวจสอบด้านเทคโนโลยีสารสนเทศ มีการให้บริการเป็นแนวทางเดียวกันคือ กรอบมาตรฐานด้านความปลอดภัยเทคโนโลยีสารสนเทศ ยึดถือตามมาตรฐาน ISO 27001 และการตรวจสอบด้านเทคโนโลยีสารสนเทศ ยึดถือตามแนวทางของ COBIT ตัวอย่างเช่น บริการด้าน IT Audit / Assurance Services ของบริษัท ACIS Professional Center Co., Ltd.[21] ให้บริการตรวจสอบด้านเทคโนโลยีสารสนเทศครอบคลุมงานตรวจสอบระบบสารสนเทศอ้างอิงตามมาตรฐานและแนวปฏิบัติที่ดี อาทิ IT Assurance with COBIT, IT Assurance Framework, Risk IT Framework, หรือ ISO สำหรับบริษัท ACinfotec Co., Ltd.[22] บริการให้คำปรึกษา ฝึกอบรม ตรวจประเมิน พัฒนาและปรับปรุงกระบวนการด้านสารสนเทศให้สอดคล้องกับมาตรฐานสากล ตลอดจนกฎระเบียบและข้อกำหนดต่างๆ อาทิ เช่น มาตรฐาน ISO 27001, ISO 20000, ISO 22301, ISO 31000, FFIEC, PCI DSS, CMMI-DEV, COBIT, GDPR เป็นต้น

มาตรฐาน IT audit ของหน่วยงานทางทหารในระดับสากล

ประเทศสหรัฐอเมริกาเป็นประเทศที่มีการพัฒนาวิทยาการด้านเทคโนโลยีสารสนเทศเป็นอย่างมาก รวมทั้งได้จัดทำและเผยแพร่เอกสารตำราวิชาการต่างๆ จำนวนมาก ดังนั้นข้อมูลที่ใช้อ้างอิงส่วนใหญ่จึงมาจากประเทศสหรัฐอเมริกา ด้วยข้อจำกัดด้านภาษาและเวลาผู้วิจัยจึงขอกล่าวถึงเฉพาะหน่วยงานทางทหารในประเทศสหรัฐอเมริกาเท่านั้น

กระทรวงกลาโหมสหรัฐอเมริกาเป็นหนึ่งในหน่วยงานด้านความมั่นคงของประเทศ ได้จัดทำแผนภูมินโยบายการรักษาความปลอดภัยทางไซเบอร์[23] ขึ้นเพื่อเชื่อมโยงข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่หน่วยงานด้านความมั่นคงของประเทศได้พัฒนาขึ้น จัดเป็นหมวดหมู่ ง่ายต่อความเข้าใจ และให้ผู้ใช้สามารถเรียกดูได้โดยง่าย รวมทั้งมีการปรับปรุงให้มีความทันสมัยอยู่เสมอ (แผนภูมิปรับปรุงล่าสุด เมื่อ 22 พฤษภาคม 2562)

หน่วยงานด้านความมั่นคงแต่ละหน่วยงานได้พัฒนามาตรฐานและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเป็นของตนเอง ซึ่งส่วนใหญ่กระทรวงกลาโหมสหรัฐอเมริกาเลือกใช้ตามมาตรฐานของ 3 หน่วยงาน ได้แก่ หัวหน้าเจ้าหน้าที่สารสนเทศกระทรวงกลาโหม (The Department of Defense Chief Information Officer) คณะกรรมการระบบความมั่นคงแห่งชาติ (Committee on National Security Systems) และสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology)

กระทรวงกลาโหมสหรัฐอเมริกาเลือกใช้มาตรฐานด้านการตรวจสอบเทคโนโลยีสารสนเทศตามคณะกรรมการระบบความมั่นคงแห่งชาติ (Committee on National Security Systems) ซึ่งเป็นมาตรฐานด้านการประกันข้อมูลข่าวสาร (Information Assurance) และ NIST Special Publication 800-53A ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ

NIST Special Publication 800-53A[24] เป็นแนวทางการประเมินความปลอดภัยและการควบคุมความเป็นส่วนตัวในระบบสารสนเทศและองค์กรของรัฐบาลกลาง เนื้อหาประกอบด้วย 1) การเตรียมการ 2) การพัฒนาแผน (กำหนดความปลอดภัยหรือการควบคุม เลือกขั้นตอนเพื่อประเมินความปลอดภัย ขั้นตอนการประเมิน พัฒนากระบวนการประเมินสำหรับการควบคุมเฉพาะขององค์กร ปรับกระบวนการประเมินผลให้เหมาะสมเพื่อประสิทธิภาพสูงสุด สรุปแผนการประเมินและขอรับการอนุมัติเพื่อดำเนินการตามแผน) 3) ดำเนินการประเมิน 4) การวิเคราะห์ผลการประเมินและการรายงาน 5) การประเมินความปลอดภัยและความเป็นส่วนตัว

ระบบการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของกองทัพบกในปัจจุบัน

กองทัพบกได้นำเทคโนโลยีสารสนเทศเข้ามาใช้งานเป็นจำนวนมากเช่นเดียวกับองค์กรอื่นๆ ดังนั้นการรักษาความปลอดภัยระบบสารสนเทศจึงเป็นสิ่งจำเป็นเพื่อป้องกันความเสียหายกับข้อมูลสารสนเทศ ซึ่งได้มีการจัดหาอุปกรณ์ป้องกันต่างๆ แต่ยังคงไม่เพียงพอต่อการป้องกันเนื่องจากกองทัพบกเป็นองค์กรขนาดใหญ่ และหน่วยมีที่ตั้งกระจายกันอยู่ทั่วประเทศ อีกทั้งองค์ความรู้ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศยังคงจำกัด โดยมีศูนย์ไซเบอร์กองทัพบกเป็นหน่วยงานรับผิดชอบหลักในการตรวจสอบความมั่นคงปลอดภัยสารสนเทศของกองทัพบก **คณะกรรมการพัฒนาการปฏิบัติด้านไซเบอร์ของกองทัพบก** (ในขณะนั้นศูนย์เทคโนโลยีทางทหารเป็นหน่วยงานรับผิดชอบและได้แปรสภาพเป็นศูนย์ไซเบอร์กองทัพบกในเวลาต่อมา) ได้เห็นความสำคัญของการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ได้ตั้ง**คณะทำงานการรักษาความปลอดภัยไซเบอร์และคณะทำงานตรวจกิจด้านไซเบอร์ของกองทัพบก**ขึ้นเมื่อ 19 ก.พ. 58 ทั้งสองคณะได้ร่วมกันจัดทำหลักเกณฑ์และวิธีการในการปฏิบัติงานตรวจกิจด้านไซเบอร์ของกองทัพบก ได้ร่างและขออนุมัติหลักการใช้รายการตรวจสอบการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ **กำหนดหัวข้อการตรวจประกอบด้วย 9 หัวข้อหลัก**[25] ได้แก่ 1) การตรวจสอบการควบคุมระดับองค์กร 2) การตรวจสอบศูนย์ข้อมูลและการบรรเทาภัยพิบัติ (Data Center and Disaster Recovery) 3) การตรวจสอบอุปกรณ์เครือข่าย 4) การตรวจสอบระบบปฏิบัติการ 5) การตรวจสอบ Web Servers และ Web Applications 6) การตรวจสอบฐานข้อมูล (Database) 7) การตรวจสอบพื้นที่จัดเก็บ (Storage) 8) การตรวจสอบ WLAN และอุปกรณ์พกพา 9) การตรวจสอบ Applications

เมื่อได้รับอนุมัติหลักการแล้วจึงได้นำหัวข้อการตรวจสอบมาจัดทำเป็นแบบฟอร์มการตรวจสอบ ในการตรวจสอบแต่ละครั้งต้องได้รับอนุมัติจากกองทัพบก โดยออกคำสั่งแต่งตั้งคณะกรรมการตรวจสอบการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ระบุเจ้าหน้าที่ตรวจสอบ วันเวลา หน่วยรับตรวจ และวิธีการตรวจสอบ ซึ่งแบ่งเป็น 2 ขั้นตอน คือ การตรวจทางเอกสาร และตรวจทางเทคนิค วิธีการตรวจสอบและประเมินที่ใช้วิธีการตรวจทางเอกสาร ได้แก่ การสัมภาษณ์กำลังพลระดับเจ้าหน้าที่ปฏิบัติการ และ**การสำรวจสภาพแวดล้อมทางด้านระบบสารสนเทศของหน่วยรับการตรวจสอบ แบ่งเป็น 5 ด้าน**

ประกอบด้วย 1) ด้านโครงสร้างการจัดหน่วยรองรับภารกิจเทคโนโลยีสารสนเทศ 2) ด้านนโยบายการรักษาความปลอดภัยเทคโนโลยีสารสนเทศและการสื่อสาร 3) ด้านบุคลากร (ระดับผู้ใช้งานทั่วไปและผู้ดูแลระบบ) 4) ด้านซอฟแวร์/โปรแกรมประยุกต์ 5) ด้านอุปกรณ์ฮาร์ดแวร์ เมื่อดำเนินการตรวจสอบเรียบร้อยแล้วได้นำผลมา**ประเมินความพร้อม**ในการรักษาความมั่นคงปลอดภัยไซเบอร์ และระดับความมั่นคงปลอดภัยระบบสารสนเทศ ตามเกณฑ์การตรวจสอบขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กองทัพบกกำหนด[26] **ทั้ง 5 ด้าน ด้านละ 100 คะแนน** รวม 500 คะแนน **รายงานให้กองทัพบกและหน่วยรับการตรวจสอบทราบ**พร้อมทั้งให้คำแนะนำในการปรับปรุงแก้ไข กองทัพบกได้พิจารณาเห็นว่าการตรวจสอบและประเมินความพร้อมการรักษาความปลอดภัยระบบสารสนเทศเป็นกิจกรรมที่สำคัญในการยกระดับขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพบกจึงกำหนดให้มีการตรวจสอบการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ปีละ 1 ครั้ง และให้มี**กระบวนการติดตาม**ความคืบหน้าในการแก้ไขปรับปรุงข้อบกพร่องจากการตรวจสอบและ**รายงานให้กองทัพบกทราบทุก 6 เดือน** (ภายในเดือน มี.ค. และ ก.ย.)

กระบวนการตรวจสอบการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของกองทัพบกเป็นการตรวจสอบเพื่อแก้ไขปรับปรุงให้ระบบสารสนเทศของหน่วยงานต่างๆ ในกองทัพบกมีความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 สำหรับรายละเอียดการดำเนินการได้แนวทางจากหนังสือ IT Auditing: Using Controls to Protect Information Assets, Second Edition โดยคัดเลือกรายการตรวจสอบ (Checklists) จากในหนังสือมาปรับให้เหมาะสมกับระบบสารสนเทศของกองทัพบก

ปัจจัยที่มีผลกระทบต่อระบบสารสนเทศของกองทัพบก

ระบบสารสนเทศที่มีความมั่นคงปลอดภัยจะต้องมีองค์ประกอบ 3 ประการ คือ ความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) **ปัจจัยหลัก**ที่กระทบต่อความมั่นคงปลอดภัยระบบสารสนเทศ คือ องค์ประกอบของระบบสารสนเทศ โดยทั่วไปประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล บุคลากร และขั้นตอนการปฏิบัติงาน **ด้านฮาร์ดแวร์** อุปกรณ์ที่ทันสมัยย่อมมีประสิทธิภาพในการทำงานที่ดี ในทางกลับกันฮาร์ดแวร์เก่าล้าสมัยย่อมส่งผลต่อความพร้อมใช้งานของ

ระบบ **ด้านซอฟต์แวร์** ประกอบด้วย ซอฟต์แวร์ระบบหรือระบบปฏิบัติการ และซอฟต์แวร์ประยุกต์ หากมีช่องโหว่หรือข้อผิดพลาดของโปรแกรมอาจส่งผลให้เกิดความเสียหายต่อข้อมูล และกระบวนการทำงานของระบบสารสนเทศได้ **ด้านข้อมูล** หากมีปริมาณมากจะส่งผลต่อพื้นที่จัดเก็บและเวลาในการค้นหา ข้อมูลอาจสูญหายจากการถูกเขียนทับหรือหยุดการบันทึกเนื่องจากไม่มีพื้นที่จัดเก็บได้ **ด้านบุคลากร** เป็นองค์ประกอบที่สำคัญที่สุดถึงแม้ว่าระบบการรักษาความมั่นคงปลอดภัยมีประสิทธิภาพเพียงไรก็ตามแต่ถ้าหากบุคลากรมีพฤติกรรมการใช้งานที่ไม่เหมาะสมย่อมส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบได้ **ด้านขั้นตอนการปฏิบัติงาน** จะต้องชัดเจน ง่าย ปฏิบัติได้จริง และควรจัดทำเป็นเอกสารคู่มือการใช้งาน ปัจจัยที่สำคัญอีกประการหนึ่งคือ **ด้านเครือข่ายคอมพิวเตอร์** เนื่องจากปัจจุบันระบบสารสนเทศไม่ได้ถูกใช้งานเป็นเครื่องเดี่ยว แต่มีการเชื่อมต่อเป็นเครือข่าย โดยเฉพาะเครือข่ายอินเทอร์เน็ตซึ่งเป็นเครือข่ายขนาดใหญ่เชื่อมโยงกันทั่วโลก ช่องทางการสื่อสารที่มีประสิทธิภาพส่งผลดีต่อความพร้อมใช้งาน แต่สิ่งที่ตามมาคือความเสี่ยงที่จะถูกโจมตีได้มากขึ้นเพราะสามารถเข้าถึงระบบสารสนเทศได้จากทุกที่ในโลก **ปัจจัยอื่นๆ** ได้แก่ สภาพแวดล้อมที่เหมาะสมไม่เป็นอันตรายต่อระบบสารสนเทศ อุปกรณ์พกพา (เช่น Mobile Phone, Smart Phone, Tablet PC) อุปกรณ์อินเทอร์เน็ตประสานสรรพสิ่ง (Internet of Things : IoT) เป็นต้น

ปัจจัยด้านนโยบาย ระเบียบ ข้อบังคับ ข้อตกลง และกฎหมาย สิ่งเหล่านี้เป็นสิ่งที่มาตรฐานระดับสากลให้ความสำคัญเป็นอย่างมาก เป็นสิ่งแรกที่จะต้องตรวจในกระบวนการตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ เนื่องจากเป็นสิ่งที่กำหนดแนวทางปฏิบัติขององค์กร เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562[27] มาตรา 48 และ 49 กำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นกิจการที่มีความสำคัญต่อความมั่นคงของรัฐ ความมั่นคงทางทหาร ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ ให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีอำนาจประกาศกำหนดหน่วยงานที่มีภารกิจหรือให้บริการในด้านต่างๆ ดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 1) ด้านความมั่นคงของรัฐ 2) ด้านบริการภาครัฐที่สำคัญ 3) ด้านการเงินการธนาคาร 4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม 5) ด้านการขนส่งและโลจิสติกส์ 6) ด้านพลังงานและ

สาธารณูปโภค 7) ด้านสาธารณสุข 8) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม ซึ่งเกี่ยวข้องกับกองทัพบกโดยตรงเนื่องจากเป็นหน่วยงานด้านความมั่นคงของรัฐ

ปัจจัยด้านภัยคุกคามทางไซเบอร์ที่มุ่งโจมตีภาครัฐ[28] ได้แก่ การก่อการร้ายด้านเทคโนโลยีสารสนเทศและภัยคุกคามต่อโครงสร้างพื้นฐานที่สำคัญของรัฐ (Cyber Terrorism and Threats to Critical Infrastructure) การจารกรรมข้อมูลที่เป็นความลับหรือข้อมูลที่สำคัญต่ออธิปไตยของประเทศ (Theft of Confidential or Sovereign Data) การโจมตีแบบ Denial of Service ต่อโครงสร้างพื้นฐานสำคัญของรัฐ (Denial of Service Attacks on Key Government Infrastructure) การจารกรรมทางเทคโนโลยีสารสนเทศต่อรัฐ (Cyber Espionage) และ Advanced Persistent Threats (APT)

ปัจจัยทางทหาร พันเอก อนิวรรต เหมนิธิ[29] ได้เสนอแนวคิด **"การประเมินความเสี่ยงทางไซเบอร์"** กรอบการประเมินความเสี่ยงของเครือข่าย (Network Risk Evaluation : NRE) ประกอบด้วย ภัยคุกคาม การควบคุมที่มีอยู่ ช่องโหว่ของระบบ รวมทั้งช่องโหว่จากนโยบาย แผน ขั้นตอน และอื่นๆ โดยมุ่งเน้นไปที่ช่องโหว่ทางเทคนิคเพราะมีความชัดเจนที่สุด และการประเมินความเสี่ยงทางทหาร (Military Risk Evaluation : MRE) ปัจจัยทางทหารที่ต้องมีเพื่อประกันความสำเร็จ ได้แก่ ความตั้งใจ, จิตวิญญาณ, ความตระหนัก, สุขภาพ, ความกังวล, ความเชื่อ, การฝึกฝน, เป้าหมาย, การเฝ้าระวัง, การลาดตระเวน, การป้องกัน, การโจมตี, สายการบังคับบัญชา, การบังคับบัญชาและการควบคุม, ความเป็นผู้นำ, ความสามัคคี, หลักการปฏิบัติ, กลยุทธ์, ความรู้ และประสบการณ์ เป็นต้น

ผู้วิจัยมีความเห็นว่า "ภาวะผู้นำ" หรือ "ความเป็นผู้นำ" เป็นปัจจัยสำคัญและเด่นชัดที่สุด เนื่องจากผู้นำที่กล้าตัดสินใจปฏิบัติหรือออกคำสั่งให้ปฏิบัติในภาวะฉุกเฉิน ช่วยให้แก้ไขสถานการณ์และปฏิบัติภารกิจสำเร็จได้ ปกติแล้วเป็นความรับผิดชอบของผู้บัญชาการเหตุการณ์ โดยการแต่งตั้งหรือกำหนดตามแผนแก้ไขสถานการณ์ฉุกเฉินทางไซเบอร์

ปัจจัยที่แตกต่างกันระหว่างทหารกับพลเรือน[30] การปฏิบัติการไซเบอร์ทางทหารของแต่ละประเทศมีขอบเขตที่แตกต่างกัน บางประเทศได้รวมการปฏิบัติการไซเบอร์ทางยุทธศาสตร์เป็นขีดความสามารถทางสงครามไซเบอร์ ขีดความสามารถทางไซเบอร์เป็นหนึ่งในสภาพแวดล้อมในการรบ เช่น การใช้ขีดความสามารถทางไซเบอร์ต่อต้านระบบป้องกันภัยทางอากาศของข้าศึก นอกจากการป้องกันระบบสารสนเทศของตนเองแล้วยัง

อาจรวมถึงความสามารถในการโจมตีภัยคุกคามที่อาจส่งผลกระทบต่อองค์กร การตอบโต้การโจมตี หรือแม้กระทั่งความสามารถเชิงรุก รวมทั้งการจัดกำลังสนับสนุนภารกิจการจัดการเหตุฉุกเฉินทางไซเบอร์ระดับชาติ ซึ่งอาจมีกำลังพลหรือทรัพยากรไม่เพียงพอ บางประเทศ (เช่น สหราชอาณาจักรและเนเธอร์แลนด์) ใช้วิธีการสร้างองค์กรไซเบอร์สำรองสนับสนุนกองกำลังไซเบอร์ทางทหารในกรณีฉุกเฉิน ซึ่งเป็นวิธีที่มีประโยชน์อย่างยิ่ง เนื่องจากกองทัพไม่สามารถที่จะรักษาระดับความสามารถทางเทคนิคในโลกไซเบอร์ในองค์กรของตนได้ตลอดเวลา

ตารางแสดงปัจจัยที่แตกต่างกันระหว่างทหารกับพลเรือน

ทหาร	พลเรือน
เชิงรับ เพื่อความมั่นคงองค์กร/ประเทศ	เชิงรับ เพื่อความมั่นคงองค์กร/ประเทศ
เชิงรุก ขอบเขตการปฏิบัติการไซเบอร์ทางทหาร	-
การจัดการเหตุฉุกเฉินทางไซเบอร์ระดับชาติ	การจัดการเหตุฉุกเฉินทางไซเบอร์เฉพาะองค์กร
ความเสี่ยงทางทหาร	ความเสี่ยงทางธุรกิจองค์กร

การพึ่งพาเทคโนโลยีสารสนเทศของกองทัพบกในการปฏิบัติงานและในการรบย่อมมีความแตกต่างกัน ในการรบนั้นภารกิจเป็นสิ่งสำคัญที่สุด ซึ่งจะต้องใช้ทุกวิถีทางเพื่อให้บรรลุภารกิจ ด้านข้อมูล ความสำคัญของข้อมูล ระดับชั้นความลับ เป็นตัวกำหนดผลกระทบที่จะเกิดขึ้นต่อหน่วยทหาร เช่น หากฝ่ายตรงข้ามล่วงรู้แผนปฏิบัติการทางทหาร หรือจุดอ่อนของหน่วยงาน อาจทำให้เกิดการสูญเสียชีวิตและทรัพย์สิน รวมทั้งอำนาจต่อรองทางการเมืองกับฝ่ายตรงข้ามได้

ปัจจัยเหล่านี้ ล้วนส่งผลกระทบต่อการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ และส่งผลต่อการวางแผนในการตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพบกทั้งสิ้น

แนวทางการพัฒนาระบบตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของกองทัพบก

สามารถนำกรอบแนวคิดการควบคุมภายในของ COSO ซึ่งประกอบด้วย สภาพแวดล้อมการควบคุม การประเมินความเสี่ยง กิจกรรมการควบคุม ข้อมูลสารสนเทศและการสื่อสาร และการติดตามประเมินผลมาพัฒนาเป็นแนวทางการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของกองทัพบกได้โดยแบ่งขั้นตอนการปฏิบัติออกเป็น 4 ขั้นตอน

ขั้นเตรียมการ เตรียมความพร้อมสำหรับหน่วยงานที่รับผิดชอบงานตรวจสอบด้านเทคโนโลยีสารสนเทศ หรือการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของกองทัพบกให้พร้อมปฏิบัติงานอย่างมีประสิทธิภาพ ดังนี้ **ด้านนโยบาย**กองทัพบกจะต้องมีนโยบายด้านความปลอดภัยขององค์กรที่ชัดเจนและมีนโยบายที่กำหนดให้มีการตรวจสอบ ซึ่งปัจจุบันกองทัพบกมีระเบียบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพบก พ.ศ. 2560 เป็นกรอบนโยบายในการปฏิบัติงาน และมีอนุมัติหลักการให้ดำเนินการตรวจสอบแล้ว **ด้านบุคลากร** การสร้างทีมตรวจสอบจะต้องมีการแต่งตั้งเป็นลายลักษณ์อักษร เจ้าหน้าที่ตรวจสอบควรมีทักษะและความเชี่ยวชาญในงานการตรวจสอบด้านเทคโนโลยีสารสนเทศ และควรสร้างความรู้ความเข้าใจแก่บุคลากรของกองทัพบกในการตรวจสอบด้านเทคโนโลยีสารสนเทศ หรือให้สามารถตรวจประเมินตนเองได้ รวมทั้งจัดทำคู่มือตรวจสอบด้านเทคโนโลยีสารสนเทศแบ่งเป็นคู่มือสำหรับผู้ตรวจสอบและผู้รับการตรวจ **ด้านเครื่องมือ** ควรจัดหาเครื่องมือสำหรับงานการตรวจสอบด้านเทคโนโลยีสารสนเทศ เช่น การรวบรวมหลักฐาน การวิเคราะห์หลักฐาน การสรุปรายงาน เป็นต้น **ด้านกระบวนการทำงาน** ควรจัดทำกรอบและแนวทางปฏิบัติของมาตรการควบคุมความปลอดภัยด้านเทคโนโลยีสารสนเทศที่ชัดเจน (แบ่งตามขนาดองค์กรและความสำคัญของสินทรัพย์ ขึ้นอยู่กับการประเมินความเสี่ยงขององค์กร) กำหนดเกณฑ์มาตรฐานสำหรับใช้ประเมินหน่วยงานของกองทัพบก **ด้านงบประมาณ** ขึ้นอยู่กับรายละเอียดของการปฏิบัติงานและนโยบายจากกองทัพบก เช่น จำนวนหน่วยรับการตรวจ รูปแบบการตรวจ เวลาที่ใช้ในการตรวจ เป็นต้น

ขั้นการตรวจสอบ ประกอบด้วย 1) สำรวจสินทรัพย์ด้านเทคโนโลยีสารสนเทศ ทำความเข้าใจเกี่ยวกับการดำเนินงานและวิธีที่ระบบข้อมูลสนับสนุนการดำเนินงานของของหน่วย

รับการตรวจ ทำความเข้าใจโครงสร้างของระบบข้อมูลของหน่วย 2) ประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยรับตรวจเพื่อทราบขอบเขตในการดำเนินการ 3) วางแผนตรวจสอบหน่วยตามความจำเป็น 4) ดำเนินการตรวจสอบ บันทึกการปฏิบัติในการตรวจสอบและการรวบรวมหลักฐานต่างๆ รวมทั้งข้อมูลการสัมภาษณ์หน่วยรับตรวจ

ขั้นการรายงานผล นำข้อมูลที่ได้จากการตรวจสอบมาวิเคราะห์และประเมินประสิทธิผลของมาตรการควบคุม และประสิทธิผลในภาพรวมขององค์กรที่นำมาตรการควบคุมมาใช้ พร้อมทั้งหาแนวทางในการแก้ปัญหาสำหรับเป็นข้อแนะนำแก่หน่วยรับตรวจ การรายงานจะต้องเป็นกลางและเป็นข้อเท็จจริงในสิ่งที่พบเกี่ยวกับมาตรการควบคุมที่ทำการตรวจสอบ หากตรวจพบแนวโน้มที่จะบกพร่องและเกิดความเสี่ยงต่อองค์กร ผู้ตรวจสอบควรแจ้งผู้รับผิดชอบเพื่อแก้ไขทันที การจัดทำรายงานการตรวจสอบควรกำหนดรูปแบบการรายงานอย่างเป็นทางการของกองทัพบก โดยมี **องค์ประกอบสำคัญ** ประกอบด้วย คำชี้แจงขอบเขตการตรวจสอบ บทสรุปผู้บริหาร และรายการปัญหาพร้อมกับแผนปฏิบัติการเพื่อแก้ไขปัญหา **องค์ประกอบอื่น** ได้แก่ ชื่อผู้รับรายงาน วัตถุประสงค์ หน่วยรับตรวจ กำหนดกรอบเวลา ห้วงเวลาที่ดำเนินการ มาตรฐานอ้างอิง เกณฑ์ที่ใช้ประเมินระดับความเชื่อมั่นที่ได้รับ ข้อจำกัดการใช้และแจกจ่ายรายงาน วันที่บันทึก สถานที่บันทึก ผู้รายงาน ลายมือชื่อผู้ตรวจสอบ และสาระสำคัญของการตรวจ **องค์ประกอบเพิ่มเติม** ได้แก่ มาตรการควบคุมที่หน่วยรับการตรวจได้ดำเนินการซึ่งส่งผลที่ดีต่อการประเมิน ปัญหาที่ได้รับการแก้ไขแล้ว และปัญหาเล็กน้อยที่ระบุไว้เพื่อให้ตระหนักถึงข้อสังเกตของผู้ตรวจสอบ

ขั้นการติดตามผล จัดให้มีกระบวนการติดตามการแก้ไขปรับปรุงภายหลังการตรวจสอบ ปัญหาที่เกิดขึ้นจะต้องได้รับการแก้ไขหรือยอมรับความเสี่ยงได้ตามที่กองทัพบกเห็นสมควร (ผ่านการพิจารณาจากคณะกรรมการพัฒนาการปฏิบัติด้านไซเบอร์ของกองทัพบก) โดยกองทัพบกกำหนดให้มีการตรวจสอบการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศปีละ 1 ครั้ง และให้มีกระบวนการติดตามความคืบหน้าในการแก้ไขปรับปรุงข้อบกพร่องจากการตรวจสอบและรายงานให้กองทัพบกทราบทุก 6 เดือน (ภายในเดือน มี.ค. และ ก.ย.) ซึ่งหน่วยรับตรวจจะต้องกำหนดกลไกในการแก้ปัญหาและระยะเวลาสำหรับดำเนินการ

เพื่อให้กระบวนการติดตามการแก้ปัญหาทำได้อย่างมีประสิทธิภาพ และให้หน่วยตรวจสอบนำข้อมูลที่ใช้ในกระบวนการติดตามไปใช้ในการวางแผนตรวจสอบในปีถัดไป

สรุปผลการวิจัย

จากการศึกษาวิจัยทฤษฎีและมาตรฐานต่างๆ ด้านการบริหารจัดการเทคโนโลยีสารสนเทศ กรอบแนวทางในการสร้างความปลอดภัยระบบสารสนเทศ การตรวจสอบความปลอดภัยด้านเทคโนโลยีสารสนเทศ พบว่ามาตรฐานต่างๆ เหล่านี้มีจำนวนมากทั้งที่เกี่ยวข้องโดยตรงและทางอ้อม ในการศึกษาวิจัยที่มีเวลาจำกัดจึงไม่สามารถศึกษาได้ทั้งหมด

มาตรฐานการตรวจสอบด้านเทคโนโลยีสารสนเทศที่หน่วยงานพลเรือนและหน่วยงานทางทหารใช้ล้วนเป็นกรอบแนวทางที่คล้ายกัน มีข้อแตกต่างบ้างในรายละเอียดปลีกย่อย ขั้นตอนการปฏิบัติ และวัฒนธรรมประเพณีปฏิบัติของแต่ละองค์กร พื้นฐานที่สำคัญคือการศึกษาสภาพแวดล้อมขององค์กร ทำความเข้าใจการดำเนินงานและความเกี่ยวข้องในการนำเทคโนโลยีสารสนเทศมาใช้งานในองค์กร การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศจะช่วยให้ทราบขอบเขตการดำเนินการและทรัพยากรที่จำเป็นต้องใช้ ในการตรวจสอบจะต้องวางแผน และปฏิบัติตามแผนด้วยความรอบครอบ โดยเฉพาะงานการทดสอบระบบทางเทคนิคที่ดำเนินการเพื่อให้ได้ข้อมูลที่แท้จริงและมาเปรียบเทียบกับเกณฑ์มาตรฐานที่กำหนด ซึ่งจะต้องดำเนินการด้วยความระมัดระวังโดยผู้เชี่ยวชาญที่มีความสามารถ เนื่องจากผลกระทบในการทดสอบอาจสร้างความเสียหายได้ทั้งด้านการเงินและชื่อเสียงขององค์กร ดังนั้นในการดำเนินการทดสอบจะต้องได้รับการพิจารณาและอนุมัติจากฝ่ายบริหารก่อน จากข้อมูลที่กล่าวมาแล้วนั้นสามารถนำมาประยุกต์ใช้ให้เหมาะสมกับแนวทางปฏิบัติของกองทัพบกได้โดยกำหนดเป็น 4 ขั้นตอน ได้แก่ ขั้นเตรียมการ ขั้นการตรวจสอบ ขั้นการรายงานผล และขั้นการติดตามผล

การตรวจสอบด้านเทคโนโลยีสารสนเทศเป็นเพียงกระบวนการหนึ่งที่จะช่วยให้ทราบถึงข้อบกพร่องที่ต้องได้รับการแก้ไข ดังนั้น ประโยชน์ที่องค์กรจะได้รับไม่ใช่เพียงรายงานผลการตรวจสอบแต่เป็นสภาพที่หน่วยรับการตรวจสอบได้ดำเนินการปรับปรุงแก้ไขตามคำแนะนำของเจ้าหน้าที่ผู้เชี่ยวชาญที่ทำการตรวจประเมินแล้วนั้นเอง

เอกสารอ้างอิง

[1] กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. ข่าวกระทรวง [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 22 กุมภาพันธ์ 2562]. เข้าถึงได้จาก : http://mdes.go.th/view/1/ข่าวกระทรวงฯ/160/

[2] สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม. องค์กรระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization - ISO) [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 24 กุมภาพันธ์ 2562]. เข้าถึงได้จาก https://www.tisi.go.th/website/interstandard/iso

[3] International Organization for Standardization. All about ISO [Internet]. 2019 [cited 2019 Feb 24]. Available from : https://www.iso.org/about-us.Html

[4] สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม. คณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอเทคนิกส์ (International Electrotechnical Commission - IEC) [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 24 กุมภาพันธ์ 2562]. เข้าถึงได้จาก https://www.tisi.go.th/website/interstandard/iec

[5] บริษัท ที-เน็ต จำกัด. มาตรฐาน ISO 27001:2013 ฉบับภาษาไทย [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 24 กุมภาพันธ์ 2562]. เข้าถึงได้จาก : http://www.tnetsecurity.com/content_audit/27001-2013.pdf

[6] Scribd [Internet]. 2019 [cited 2019 Feb 25]. Available from : https://www.scribd.com/document/373918792/Iso-Iec-Tr-27008-2011-English

[7] The Committee of Sponsoring Organizations. About Us [Internet]. 2019 [cited 2019 Feb 25]. Available from : https://www.coso.org/Pages/aboutus.aspx

[8] กรมตรวจบัญชีสหกรณ์. การควบคุมภายใน [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 25 กุมภาพันธ์ 2562]. เข้าถึงได้จาก : https://www.cad.go.th/download/1_3control.pdf

[9] ERM Thailand. การบริหารจัดการความเสี่ยง (ERM และ COSO) [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 25 กุมภาพันธ์ 2562]. เข้าถึงได้จาก : http://ermthailand.blogspot.com/p/erm-coso.html

[10] Chris Davis, Mike Schiller, Kevin Wheeler. IT auditing: using controls to protect information assets. 2nd ed. n.p.: The McGraw-Hill companies; 2011.

[11] บรรจง หะรังษี, ดร. หลักการทั้ง 5 หลักการของ COBIT 5 [อินเทอร์เน็ต]. 2561 [เข้าถึงเมื่อ 4 กรกฎาคม 2562]. เข้าถึงได้จาก : http://www.tnetsecurity.com/content_audit/COBIT5-Principles/COBIT5-Principles.html]

[12] บรรจง หะรังษี, ดร. ภาพรวมและคุณลักษณะสำคัญของ COBIT 5 [อินเทอร์เน็ต]. 2561 [เข้าถึงเมื่อ 4 กรกฎาคม 2562]. เข้าถึงได้จาก : http://www.tnetsecurity.com/content_audit/COBIT5-Summary/COBIT5-Summary.html

[13] ISACA. ITAF: a professional practices framework for IT assurance. U.S.: ISACA; 2008.

[14] The National Institute of Standards and Technology. About NIST [Internet]. 2019 [cited 2019 Jun 18]. Available from : https://www.nist.gov/about-nist

[15] The National Institute of Standards and Technology. NIST SP 800-171 [Internet]. 2019 [cited 2019 Jun 18]. Available from : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

[16] The National Institute of Standards and Technology. NIST Handbook 162 [Internet]. 2019 [cited 2019 Jun 18]. Available from : https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf

[17] Chris Davis, Mike Schiller, Kevin Wheeler. IT auditing: using controls to protect information assets. 2nd ed. n.p.: The McGraw-Hill companies; 2011.

[18] ชมรมผู้ตรวจสอบภายในธนาคารและสถาบันการเงิน. เกี่ยวกับชมรม [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 16 มิถุนายน 2562]. เข้าถึงได้จาก : http://www.bfiia.org/index.php?lay=show&ac=article&Id=324238

[19] ธนาคารแห่งประเทศไทย. แนวทางการตรวจสอบด้านเทคโนโลยีสารสนเทศ [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 16 มิถุนายน 2562]. เข้าถึงได้จาก : https://www.

bot.or.th/Thai/FinancialInstitutions/PruReg_HB/RiskMgt_Manual/Documents/SA-IT_ExaminationGuideline.pdf

[20] สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย. คู่มือการตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางการกำกับดูแลตามความเสี่ยง [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 16 มิถุนายน 2562]. เข้าถึงได้จาก : http://www.oic.or.th/sites/default/files/content/88539/khuumuuekaartrwcchsbrabbethkhonolyiisaarsneths-it-audit-manual.pdf

[21] ACIS Professional Center. Consulting Services [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 16 มิถุนายน 2562]. เข้าถึงได้จาก : https://www.acisonline.net/?page_id=3009

[22] ACinfotec. Compliance consulting & auditing services [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 16 มิถุนายน 2562]. เข้าถึงได้จาก : https://www.acinfotec.com/home/compliance-consulting-auditing/

[23] Defense Technical Information Center. Cybersecurity-related policies and issuances [Internet]. 2019 [cited 2019 Jul 11]. Available from : https://dodiac.dtic.mil/wp-content/uploads/2019/05/ia-policychart-22-May-19.pdf

[24] The National Institute of Standards and Technology. NIST SP 800-53A [Internet]. 2019 [cited 2019 Jul 11]. Available from : https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

[25] หนังสือ ยก.ทบ. ด่วนมาก ที่ กห 0403/8851 เรื่อง ขออนุมัติหลักการใช้รายการตรวจสอบการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ลง 8 มิถุนายน 2558.

[26] กรมยุทธการทหารบก. เกณฑ์การตรวจสอบขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 15 มิถุนายน 2562]. เข้าถึงได้จาก : http://doo.rta.mi.th/img/Cyber.pdf

[27] ราชกิจจานุเบกษา. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 [อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 15 มิถุนายน 2562]. เข้าถึงได้จาก : http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF

[28] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). ความเสี่ยงของข้อมูลที่เปิดเผยสู่สาธารณะ ภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อภาครัฐ

[อินเทอร์เน็ต]. 2562 [เข้าถึงเมื่อ 15 มิถุนายน 2562]. เข้าถึงได้จาก : https://www.thaicert.or.th/downloads/files/Cyber_Threats_To_The_Networked_Government.pdf

[29] Aniwat Hemanidhi, Sanon Chimmanee. Military-based cyber risk assessment framework for supporting cyber warfare in Thailand [Internet]. 2019 [cited 2019 Feb 22]. Available from : http://www.jict.uum.edu.my/images/pdf4/vol16no22017/192-222.pdf

[30] Alexander Klimburg. National cyber security framework manual. NATO CCD COE Publication: Tallinn; 2012.