แผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ประจำปี พ.ศ. ๒๕๖๙

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

สารบัญ

คำนำ

การบริหารความเสี่ยงเป็นเครื่องมือสำคัญที่ช่วยเสริมสร้างความมั่นคงและประสิทธิภาพในการดำเนินงานขององค์กร ในยุคดิจิทัลที่เทคโนโลยีดิจิทัลมีบทบาทสำคัญในการจัดการข้อมูล การสื่อสารและการตัดสินใจของผู้บริหาร การบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัลจึงเป็นสิ่งที่ไม่สามารถละเลยได้ ด้วยเหตุนี้ สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ (สำนักงาน ป.ป.ท.) จึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ประจำปี พ.ศ. ๒๕๖๙ ขึ้น เพื่อเป็นแนวทางปฏิบัติงานในการป้องกันภัยคุกคามที่อาจเกิดขึ้นซึ่งจะส่งผลกระทบต่อประสิทธิภาพการให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน ป.ป.ท.

แผนนี้ครอบคลุมถึงการป้องกันและจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ที่มุ่งเน้นการป้องกันการโจมตีทางไซเบอร์ การบุกรุกระบบ และการละเมิดความปลอดภัยของข้อมูล เพื่อให้มั่นใจได้ว่าข้อมูลของประชาชนจะได้รับการคุ้มครองอย่างดีที่สุด ทั้งนี้ยังให้ความสำคัญกับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (Personal Data Protection Act: PDPA) เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลของประชาชนได้รับการปกป้องอย่างเหมาะสมและสอดคล้องกับ ข้อกำหนดของกฎหมาย

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

บทที่ 1
บทนำ

๑. หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

สำนักงาน ป.ป.ท. ได้นำเทคโนโลยีสารสนเทศมาใช้งานเพื่อช่วยเพิ่มประสิทธิภาพการดำเนินงานให้มีความสะดวกรวดเร็ว ขณะเดียวกันระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตีจากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอก ส่งผลกระทบต่อการดำเนินงานของสำนักงาน ป.ป.ท. ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ท. มีความมั่นคงปลอดภัย จึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลขึ้น โดยผู้บริหารและเจ้าหน้าที่กลุ่มงานคอมพิวเตอร์และการสื่อสาร ได้มีส่วนร่วมในการจัดทำแผนดังกล่าว และทุกภาคส่วนจำเป็นต้องมีการปฏิบัติตามแผน รวมทั้งมีการทบทวนและปรับปรุงนโยบายและแผนดังกล่าวให้เป็นปัจจุบันอยู่เสมอ

๒. วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

๒.๑ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒.๒ เพื่อลดความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๕ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหาร และผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและระบบสารสนเทศของสำนักงาน ป.ป.ท.

๒.๖ เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

๓. นิยามความเสี่ยง

ความเสี่ยง หมายถึง ความไม่แน่นอนที่อาจนำไปสู่ความสูญเสีย ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ความเสี่ยงมีทั้งประเภทที่เป็นความเสี่ยงที่แท้จริงที่เป็นความเสี่ยงที่มีโดยธรรมชาติ และความเสี่ยงที่เกิดจากการเก็งกำไร ความหมายของความเสี่ยงอาจมีการตีความแตกต่างกันไปหลายอย่างตามแต่ความเชี่ยวชาญและอาชีพของผู้ให้คำจำกัดความ

การบริหารจัดการความเสี่ยง หมายถึง กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่หน่วยงานยอมรับได้

ปัจจัยเสี่ยง หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้

การประเมินความเสี่ยง หมายถึง การคาดคะเน หรือคำนวณโอกาสที่จะเป็นเหตุให้เกิดความเสียหายและหรือความเสียหายที่จะส่งผลกระทบต่อการทำงานที่ไม่บรรลุเป้าหมายที่วางไว้เพื่อให้ทราบความสำคัญของความเสี่ยงที่แตกต่างกันและใช้การพิจารณาในการกำหนดจุดควบคุมความเสี่ยงที่มีนัยสำคัญ

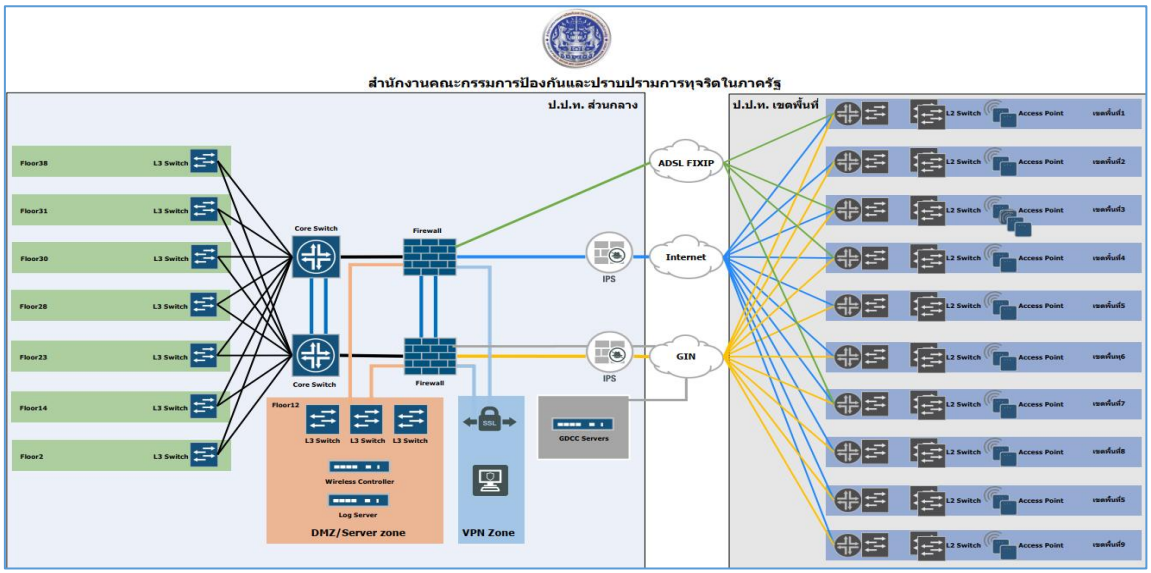
กิจกรรมควบคุม หมายถึง กระบวนการปฏิบัติที่ทุกคนในองค์กรร่วมกันพิจารณากำหนดขึ้นเพื่อสร้างความมั่นใจในระดับที่สมเหตุสมผลในการบรรลุวัตถุประสงค์ของหน่วยงาน

๔. สถานภาพเทคโนโลยีสารสนเทศและการบริหารจัดการ

๔.๑ ระบบการให้บริการบนเครือข่าย (Network)

๔.๑.๑ ภาพรวมระบบเครือข่าย

ระบบเครือข่ายของสำนักงาน ป.ป.ท. ประกอบด้วย ๓ ส่วน คือ เครือข่ายระบบสารสนเทศส่วนกลาง (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) เครือข่ายคอมพิวเตอร์สำหรับผู้ใช้งานของสำนักงานส่วนกลาง และเครือข่ายคอมพิวเตอร์สำหรับผู้ใช้งานของสำนักงานเขตในส่วนภูมิภาค โดยทั้ง ๓ ส่วน จะเชื่อมโยงเข้าสู่ระบบเครือข่ายส่วนกลางภายในศูนย์เทคโนโลยีสารสนเทศ เพื่อให้บุคลากรของสำนักงาน ป.ป.ท. สามารถใช้งานระบบสารสนเทศได้อย่างสมบูรณ์ โดยแบ่งได้ดังนี้



ภาพที่ ๑ ภาพรวมการเชื่อมโยงระบบสารสนเทศ

(๑) เครือข่ายระบบสารสนเทศส่วนกลาง (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประกอบด้วยส่วนหลัก คือ Core Switch จำนวน ๒ ชุดทำงานร่วมกันแบบ Stack รองรับการเชื่อมโยงระบบเครือข่ายของผู้ใช้งานภายในอาคารซอฟต์แวร์ปาร์ค ด้วยความเร็ว ๑Gbps และเชื่อมไปยังอุปกรณ์ Firewall ด้วยความเร็ว ๑๐ Gbps ผ่านไปยังส่วนของเครื่องแม่ข่ายและระบบงานต่างๆ ที่อยู่ภายใต้ DMZ/Server Zone นอกจากนี้ยังมีระบบป้องกันการบุกรุกสารสนเทศ (Intruder Prevention System : IPS) รองรับการเชื่อมต่อจาก สำนักงาน ป.ป.ท เขตพื้นที่ในส่วนภูมิภาคทั้งทางเครือข่ายอินเทอร์เน็ตและเครือข่าย GIN รวมทั้งระบบยืนยันตัวตน

(๒) เครือข่ายคอมพิวเตอร์สำหรับผู้ใช้งานของสำนักงานส่วนกลาง จะมีเครือข่ายภายในของตนเอง และมีอุปกรณ์ Switch เชื่อมต่อมายัง Core Switch ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ในแบบ Link Aggregation

(๓) เครือข่ายคอมพิวเตอร์สำหรับผู้ใช้งานของสำนักงานเขตในส่วนภูมิภาค เชื่อมโยงเครือข่ายเข้าสู่ ระบบสารสนเทศส่วนกลางได้ ๒ วิธี คือ การเชื่อมโยงด้วยระบบเครือข่ายสื่อสารข้อมูลภาครัฐ (GIN) และระบบอินเทอร์เน็ตซึ่งในการเข้าถึงระบบสารสนเทศผ่านทางอินเทอร์เน็ตจะต้องเข้าผ่าน Tunnel โดยผู้ใช้ต้องเชื่อมต่อกับ VPN

๔.๑.๒ การให้บริการระบบเครือข่าย

ปัจจุบันการให้บริการระบบเครือข่ายคอมพิวเตอร์ของ สำนักงาน ป.ป.ท. มีการแบ่งการให้บริการออกเป็น ๒ ส่วนคือ

(๑) ระบบเครือข่ายของสำนักงาน ป.ป.ท. ส่วนกลาง ที่ให้บริการในปัจจุบันประกอบไปด้วยสองส่วนหลัก คือ ระบบเครือข่ายที่ใช้สาย (LAN Network) และระบบเครือข่ายไร้สาย (Wireless Network) โดยระบบเครือข่ายทั้งสองมีการบริหารแบบศูนย์รวมโดยผ่านระบบยืนยันตัวตน (Authentication Radius Server) โดยการให้บริการเครือข่ายจะเป็นการให้บริการจากผู้ให้บริการอินเทอร์เน็ต (Internet service provider: ISP) และการให้บริการผ่านระบบเครือข่ายภายใน (Intranet) โดยมีรายละเอียดดังนี้

- การให้บริการอินเทอร์เน็ตผ่าน (ISP) มีความเร็วอยู่ที่ ๗๐๐/๗๐๐ MB
- การให้บริการอินทราเน็ต (Intranet) มีความเร็วอยู่ที่ ๑๐๐/๑๐๐ MB

(๒) ระบบเครือข่ายของสำนักงาน ปปท. เขต ๑ – ๙ ที่ให้บริการในปัจจุบันประกอบไปด้วยสองส่วนหลัก คือ ระบบเครือข่ายที่ใช้สาย (LAN Network) และระบบเครือข่ายไร้สาย (Wireless Network) โดยระบบเครือข่ายทั้งสองมีการให้บริการเครือข่ายจะเป็นการให้บริการจากผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider: ISP) ผ่านระบบ Asymmetric Digital Subscribers Line (ADSL) และการให้บริการผ่านระบบเครือข่ายภายใน (Intranet) โดยมีรายละเอียดดังนี้

ระบบอินเตอร์เน็ต ของสำนักงาน ป.ป.ท.

ชื่อสำนักงาน	ผู้ให้บริการอินเตอร์เน็ต (ISP)	จำนวนอุปกรณ์	ความเร็ว
สำนักงาน ปปท.เขต ๑	NT (FIX IP)	๑	๑๐๐๐/๑๐๐๐ MB
สำนักงาน ปปท.เขต ๒	NT	๑	๑๐๐๐/๕๐๐ MB
สำนักงาน ปปท.เขต ๓	NT (FIX IP)	๑	๑๐๐๐/๑๐๐๐ MB
สำนักงาน ปปท.เขต ๔	NT (FIX IP)	๑	๑๐๐๐/๑๐๐๐ MB
สำนักงาน ปปท.เขต ๕	NT	๒	๑๐๐๐/๕๐๐ MB ๑๐๐๐/๕๐๐ MB
สำนักงาน ปปท.เขต ๖	AIS	๑	๑๐๐๐/๕๐๐ MB
สำนักงาน ปปท.เขต ๗	NT (FIX IP)	๒	๑๐๐๐/๕๐๐ MB ๑๐๐๐/๕๐๐ MB
สำนักงาน ปปท.เขต ๘	NT (FIX IP)	๑	๑๐๐๐/๑๐๐๐ MB
สำนักงาน ปปท.เขต ๙	NT (FIX IP)	๑	๑๐๐๐/๑๐๐๐ MB

ระบบอินทราเน็ต ของสำนักงาน ป.ป.ท.

ชื่อสำนักงานงาน	ผู้ให้บริการอินทราเน็ต (ISP)	จำนวนอุปกรณ์	ความเร็ว
สำนักงาน ปปท.เขต ๑	GIN	๑	๒๐/๒๐ MB
สำนักงาน ปปท.เขต ๒	GIN	๑	๒๐/๒๐ MB
สำนักงาน ปปท.เขต ๓	GIN	๑	๒๐/๒๐ MB
สำนักงาน ปปท.เขต ๓ ส่วนหน้า (อุบลราชธานี)	-	-	-
สำนักงาน ปปท.เขต ๔	GIN	๑	๒๐/๒๐ MB
สำนักงาน ปปท.เขต ๔ ส่วนหน้า (สกลนคร)	-	-	-
สำนักงาน ปปท.เขต ๕	GIN	๑	๒๐/๒๐ MB
สำนักงาน ปปท.เขต ๖	GIN	๑	๒๐/๒๐ MB
สำนักงาน ปปท.เขต ๖ ส่วนหน้า (นครสวรรค์)	-	-	-
สำนักงาน ปปท.เขต ๗	GIN	๑	๒๐/๒๐ MB
สำนักงาน ปปท.เขต ๘	GIN	๑	๒๐/๒๐ MB
สำนักงาน ปปท.เขต ๙	GIN	๑	๒๐/๒๐ MB

๔.๑.๓ การป้องกันและรักษาความปลอดภัยเครือข่าย

(๑) Firewall ระบบสารสนเทศจะถูกป้องกันโดยอุปกรณ์ Firewall เพื่อป้องกันการโจมตีจากผู้ไม่ประสงค์ดี โดยสามารถกำหนดนโยบายในการเข้าถึงทรัพยากรสารสนเทศได้ และอุปกรณ์ตรวจจับการบุกรุกระบบ (IPS) ในการตรวจสอบพฤติกรรมการใช้ของผู้ใช้งานหรือซอฟต์แวร์ใดๆ ที่เชื่อมโยงมาจากเครือข่าย GIN และเครือข่ายอินเทอร์เน็ต อุปกรณ์ Firewall ประกอบด้วย Firewall จำนวน ๒ ชุด ทำงานแบบ High Availability (HA) โดยสามารถทำงานทดแทนกันเมื่อมีอุปกรณ์ใดเสียหายจนทำงานไม่ได้โดยเชื่อมต่อกับอุปกรณ์อื่น ดังนี้

- อุปกรณ์ DMZ Switch จำนวน ๒ ชุดในแบบขนานเพื่อป้องกันการเข้าถึงระบบเครื่องแม่ข่าย ระบบงาน ฮาร์ดแวร์ และซอฟต์แวร์อื่นๆ ที่อยู่ภายใน DMZ โดยไม่เหมาะสม
- อุปกรณ์ Core Switch ด้วยสายสัญญาณขนาด ๑๐ Gbps จำนวน ๒ ชุด แบบขนานเพื่อรองรับผู้ใช้งานจากสำนักงาน ป.ป.ท. ส่วนกลาง
- อุปกรณ์ Switch Cisco C๙๓๐๐-๔๘T-A จำนวน ๒ ชุด เพื่อรองรับการใช้งานจากผู้ใช้ของสำนักงาน ป.ป.ท. ในส่วนภูมิภาค
- ระบบ VPN เพื่อเข้าถึงระบบสารสนเทศแบบ Tunnel สำหรับผู้ใช้ที่ต้องการเข้าสู่ระบบสารสนเทศผ่านระบบอินเทอร์เน็ต

(๒) Intruder Prevention System (IPS) หมายถึงอุปกรณ์ฮาร์ดแวร์หรือซอฟต์แวร์ที่สามารถตรวจสอบวิเคราะห์หาพฤติกรรมการใช้งานที่อาจก่อให้เกิดอันตรายต่อระบบสารสนเทศ โดยตรวจสอบ Packet ข้อมูลที่ส่งผ่านระบบเครือข่าย ป้องกันการโจมตี และสามารถทำงานร่วมกับอุปกรณ์ Firewall โดยเพิ่ม Rule เข้าไปเพื่อป้องกันการโจมตีระบบ IPS ติดตั้งจำนวน ๑ ชุด แต่ละชุดต่อกับ Firewall เข้าไปยังระบบสารสนเทศภายใน เชื่อมต่อกับเครือข่าย GIN และเครือข่ายอินเทอร์เน็ต ตามลำดับเพื่อป้องกันการบุกรุกผ่านทางเครือข่ายดังกล่าว

๔.๑.๔ การสำรองข้อมูล

ปัจจุบันได้มีการติดตั้งอุปกรณ์ Data Domain บนตู้ Rack Server Rack ซึ่งยังไม่มีการใช้งานใดๆ ดังนั้น ปัจจุบันการ Backup ข้อมูลของสำนักงาน ป.ป.ท. จะใช้วิธีการดังต่อไปนี้

- Backup ลงฮาร์ดดิสก์โดยตรง โดยทำเป็น Windows Image
- อุปกรณ์ที่อยู่ในระยะ MA ผู้รับจ้างเป็นผู้ Backup ข้อมูล
- อุปกรณ์ที่ไม่อยู่ในระยะ MA เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้ Backup ข้อมูล

ทั้งนี้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้มีแนวทางในการจะสร้าง DR Site และนำข้อมูลที่ได้มีการสำรองไว้ ไปจัดเก็บ ณ สำนักงาน ปปท. เขต ๒ เพื่อลดความเสี่ยงต่อการสูญเสียข้อมูลกรณีเกิดเหตุการณ์ไม่ปกติ และไม่สามารถเข้าห้อง Data Center ได้

๔.๒ อุปกรณ์เครื่องคอมพิวเตอร์ (Hardware)

สำนักงาน ป.ป.ท. ได้ดำเนินการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างต่อเนื่อง ปัจจุบันมีเครื่องคอมพิวเตอร์แม่ข่าย แบ่งออกเป็น ๓ ประเภทดังต่อไปนี้

๔.๒.๑ เครื่องแม่ข่าย (Server) ของสำนักงาน ป.ป.ท. ที่ใช้บริการของ คลาวด์กลางภาครัฐ (GDCC) สามารถแสดงได้ ตามตารางที่ ๑

๔.๒.๒ Blade Server ข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายประเภท Server Farm ของสำนักงาน ป.ป.ท. สามารถแสดงได้ ตามตารางที่ ๒

ตารางที่ ๑ รายการเครื่องแม่ข่าย (Server) ของสำนักงาน ป.ป.ท. ที่ติดตั้งอยู่ GDCC

No	Name	Brand	CPU				RAM (GB)	Storage (GB)	ชื่อระบบงาน	ปีงบประมาณ	ผู้รับผิดชอบ
			GHz	Unit	Core/ Unit	Total Cores					
๑	Open Stack ๑ (Tier ๑)	GDCC	๔	๑	๒	๘	๘	๖๐	API Gateway (API๑)	๒๕๖๘	ศทส./GDCC
๒	Open Stack ๑ (Tier ๑)	GDCC	๔	๑	๒	๘	๘	๖๐	API Gateway (API๒)	๒๕๖๘	ศทส./GDCC
๓	Open Stack ๑ (Tier ๒)	GDCC	๔	๔	๘	๓๒	๓๒	๑๐๐	APP ๑	๒๕๖๘	ศทส./GDCC
๔	Open Stack ๑ (Tier ๒)	GDCC	๔	๔	๘	๓๒	๓๒	๑๐๐	APP ๒	๒๕๖๘	ศทส./GDCC
๕	Open Stack ๑ (Tier ๒)	GDCC	๔	๔	๘	๓๒	๓๒	๑๘๐	Mail + Ldap	๒๕๖๘	ศทส./GDCC
๖	Open Stack ๑ (Tier ๒)	GDCC	๔	๔	๘	๓๒	๓๒	๑๘๐	Mail + Ldap	๒๕๖๘	ศทส./GDCC
๗	Open Stack ๒ (Tier ๓)	GDCC	๔	๒	๔	๘	๘	๖๐	Proxy (SQL)	๒๕๖๘	ศทส./GDCC
๘	Open Stack (Tier ๓)	GDCC	๔	๒	๔	๘	๘	๖๐	Proxy (SQL)	๒๕๖๘	ศทส./GDCC
๙	Open Stack (Tier ๓)	GDCC	๔	๒	๘	๑๖	๖๔	๖๐	DB๑	๒๕๖๘	ศทส./GDCC
๑๐	Open Stack (Tier ๓)	GDCC	๔	๒	๔	๘	๑๖	๖๐	DB๒	๒๕๖๘	ศทส./GDCC
๑๑	Open Stack (Tier ๓)	GDCC	๔	๔	๔	๑๖	๑๖	๖๐	DB๓	๒๕๖๘	ศทส./GDCC
๑๒	Nginx_GDCC	GDCC	๔	๒	๔	๘	๑๖	๑๐๐	Nginx๑_GDCC	๒๕๖๘	ศทส./GDCC
๑๓	Nginx_GDCC	GDCC	๔	๒	๔	๘	๑๖	๑๐๐	Nginx๒_GDCC	๒๕๖๘	ศทส./GDCC
๑๔	DB_PACC	GDCC	๔	๔	๘	๑๖	๓๒	๓๐๐	DB_GDCC	๒๕๖๘	ศทส./GDCC
๑๕	Portal_PACC	GDCC	๔	๔	๘	๑๖	๓๒	๓๐๐	Portal_PACC	๒๕๖๘	ศทส./GDCC
๑๖	E_Service	GDCC	๔	๔	๘	๘	๑๖	๒๐๐	E_Service	๒๕๖๘	ศทส./GDCC

ตารางที่ ๒ รายการ Blade Server เครื่องคอมพิวเตอร์แม่ข่ายประเภท Server Farm ของสำนักงาน ป.ป.ท.

No	Name	Brand	CPU				RAM (GB)	Storage (GB)	ชื่อระบบงาน	ปีงบประมาณ	ผู้รับผิดชอบ
			GHz	Unit	Core /Unit	Total Cores					
๑	Intel Xeon X๓๔๕๐ ๒.๖๗GHz	Dell	๒.๖๗	๑	๔	๔	๑๖	๕๐๐	ระบบ Call Center ๑๒๐๖	๒๕๕๖	Commserv
๒	Intel Xeon X๓๔๕๐ ๒.๖๗GHz		๒.๖๗	๑	๔	๔	๘	๕๐๐	ระบบบันทึกเสียงการสนทนา (Voice Record)	๒๕๕๖	Commserv
๓	Dell EMC PowerEdge R๖๔๐ : Intel ® Xeon ® Gold ๖๑๓๔ CPU ๓.๒๐	Dell	๓.๒	๒	๘	๑๖	๖๔	๒๐๐๐	โครงการพัฒนาระบบไต่สวนข้อเท็จจริง	๒๕๖๑	CODE PROMPT
๔	HPE DL๓๘๕ GEN๑๑ ๘SFF CTO Svr	HP	๓.๐	๑	๑๖	๒	๑๒๘	๒๐๐๐	ระบบ e-Learning	๒๕๖๘	Clicknext
๕	HPE DL๓๘๕ GEN๑๑ ๘SFF CTO Svr	HP	๓.๐	๑	๑๖	๒	๑๒๘	๒๐๐๐	ระบบ e-Learning	๒๕๖๘	Clicknext
๖	HPE ProLiant DL๓๖๐ Gen๑๑ (SGHD๒FL๘๙C)	HP	๓.๖	๒	๑๖	๓๒	๑๒๘	Ssd ๙๖๐x๔	ระบบวินัย (ACOC)	๒๕๖๘	POLTELNET
๗	HPE ProLiant DL๓๖๐ Gen๑๑ (SGHD๒FL๘๘)	HP	๓.๖	๒	๑๖	๓๒	๑๒๘	Ssd ๙๖๐x๔	ระบบวินัย (ACOC)	๒๕๖๘	POLTELNET
๘	ThinkSystem / SR๖๓๐ V๒ (J๙๐๒ATM๔)	Lenovo	๓.๕	๒	๑๖	๓๒	๑๒๘	Ssd ๙๖๐x๔	ระบบ Feedback	๒๕๖๘	BlueSystem Tech.

๔.๒.๓ ข้อมูลครุภัณฑ์คอมพิวเตอร์ ประจำปี พ.ศ. ๒๕๖๘

สำหรับเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมทั้งโปรแกรมพื้นฐานต่างๆ ที่สำนักงาน ป.ป.ท. ได้ดำเนินการสำรวจในปัจจุบัน โดยได้ทำการสำรวจข้อมูล ณ ปีงบประมาณ พ.ศ. ๒๕๖๘ มีรายละเอียดดังนี้

ลำดับ	รายการครุภัณฑ์คอมพิวเตอร์	จำนวน
๑	เครื่องคอมพิวเตอร์แม่ข่าย	๒๗
๒	เครื่องคอมพิวเตอร์แม่ข่ายเสมือน (VM)	๓๓
๒	เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (PC)	๓๒๓
๓	เครื่องคอมพิวเตอร์แบบพกพา (Notebook)	๕๗๗
๔	เครื่องพิมพ์	๔๔๕
๕	เครื่องสแกนเนอร์	๗๘
๖	โปรแกรมระบบปฏิบัติการ (Windows)	๖๒๙
๗	โปรแกรม Microsoft Office	๕๑๐
๘	Microsoft SQL Server	๔
๙	Microsoft Windows Server	๒๕

๔.๓ ระบบฐานข้อมูลและสารสนเทศ (Database and Application)

สำนักงาน ป.ป.ท. มีระบบเทคโนโลยีสารสนเทศ สำหรับใช้งานภายในองค์กร โดยการเข้าใช้ระบบงาน สามารถเข้าใช้โดยผ่าน Website : workcenter.pacc.go.th โดยจะแบ่งการเข้าถึงระบบได้ ๒ ช่องทาง ได้แก่

๔.๓.๑ ระบบสำนักงานภายใน ที่ต้องเชื่อมต่อระบบ VPN ได้แก่

๑) ระบบ Linkage Center ประกอบด้วย

- ระบบสืบค้นข้อมูลทะเบียนราษฎร์ (ทร.๑๔)
- ระบบสืบค้นข้อมูลประกันสังคม
- ระบบสืบค้นข้อมูลกรมการขนส่งทางบก

๒) ระบบบริหารจัดการทรัพยากรบุคคล (DPIS)

๔.๓.๒ ระบบสำนักงานที่สามารถใช้งานผ่านระบบ Internet ประกอบด้วย

๑) ระบบสำนักงานอิเล็กทรอนิกส์ (New e-Office)

๒) ระบบจดหมายอิเล็กทรอนิกส์ (WorkD)

๓) ระบบแลกเปลี่ยนข้อมูลกระทรวงยุติธรรม (DXC)

๔) ระบบสืบค้นข้อมูลนิติบุคคล (GDX Linkage)

๕) ระบบสืบค้นรายการภาษี กรมสรรพากร

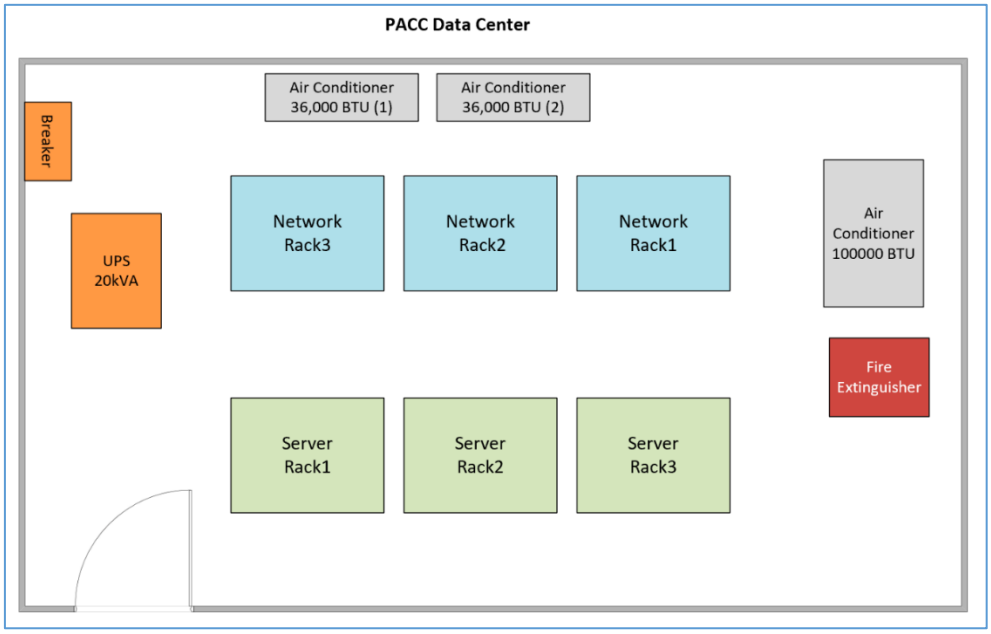
๖) ระบบสืบค้นสถานภาพบุคคลของเจ้าหน้าที่รัฐ กรมบัญชีกลาง

นอกจากนี้ ยังมีระบบงาน ที่สำนักงาน ป.ป.ท. ได้พัฒนาขึ้นเพื่อใช้งานตามภารกิจด้านการป้องกันและปราบปรามการทุจริต ที่มีการใช้งานอยู่ในปัจจุบัน ได้แก่

- ระบบรับเรื่องร้องเรียน PCMS
- ระบบไต่สวนข้อเท็จจริง
- ระบบบริหารจัดการผู้ใช้แบบรวมศูนย์
- ระบบระบบรายงานข้อร้องเรียนเจ้าหน้าที่รัฐกระทำการทุจริตหรือประพฤติมิชอบ

๔.๔ ห้องศูนย์ข้อมูล (Data Center)

ห้องศูนย์ข้อมูล Data Center ตั้งอยู่บนชั้น ๑๒ ภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ประกอบด้วยตู้ Rack ๑๙” ขนาด ๔๒U สำหรับอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายจำนวน ๓ ตู้ และอุปกรณ์เครือข่ายจำนวน ๓ ตู้ รวมมีตู้ Rack ทั้งหมด ๖ ตู้ จ่ายกระแสไฟฟ้าแบบ ๓ เฟสผ่านอุปกรณ์ UPS ขนาด ๒๐KVA ๑ ชุด และมีระบบปรับอากาศ โดยมีเครื่องปรับอากาศที่ติดตั้งระบบปรับอากาศใต้พื้นห้องขนาด ๑๐๐,๐๐๐ BTU สำหรับระบายความร้อนช่วงกลางวัน และมีเครื่องปรับอากาศขนาด ๓๖,๐๐๐ BTU จำนวน ๒ เครื่อง สำหรับระบายความร้อนในตอนกลางคืน มีอุณหภูมิเฉลี่ยที่ประมาณ ๒๒-๒๔ องศาเซลเซียส ภายในห้องติดตั้งอุปกรณ์ดับเพลิง สำหรับกรณีฉุกเฉินหากเกิดเพลิงไหม้



ภาพที่ ๒ แผนผังห้อง Data Center

๔.๕ ระบบรักษาความปลอดภัยเครือข่าย

๔.๕.๑ FireWall

Firewall ระบบสารสนเทศจะถูกป้องกันโดยอุปกรณ์ Firewall เพื่อป้องกันการโจมตีจากผู้ไม่ประสงค์ดี โดยสามารถกำหนดนโยบายในการเข้าถึงทรัพยากรสารสนเทได้ และอุปกรณ์ตรวจจับการบุกรุกระบบ (IPS) ในการตรวจสอบพฤติกรรมการใช้ของผู้ใช้งานหรือซอฟต์แวร์ใด ๆ ที่เชื่อมโยงมาจากเครือข่าย GIN และเครือข่ายอินเทอร์เน็ต โดยจะมีการอัพเดทข้อมูลเป็นปัจจุบันเสมอตลอดระยะเวลารับประกันอุปกรณ์

๔.๕.๒ IPS

Intruder Prevention System (IPS) หมายถึงอุปกรณ์ฮาร์ดแวร์หรือซอฟต์แวร์ที่สามารถตรวจสอบวิเคราะห์หาพฤติกรรมการใช้งานที่อาจก่อให้เกิดอันตรายต่อระบบสารสนเทศ โดยตรวจสอบ Packet ข้อมูลที่ส่งผ่านระบบเครือข่าย ป้องกันการโจมตี และสามารถทำงานร่วมกับอุปกรณ์ Firewall โดยเพิ่ม Rule เข้าไปเพื่อป้องกันการโจมตีระบบ IPS ติดตั้งจำนวน ๑ ชุด โดยจะมีการอัพเดทข้อมูลเป็นปัจจุบันเสมอตลอดระยะเวลารับประกันอุปกรณ์

๔.๕.๓ ระบบปฏิบัติการ (OS)

ปัจจุบันสำนักงาน ป.ป.ท. ใช้ระบบปฏิบัติการวินโดวส์พัฒนาโดย Microsoft Corporation เพื่อใช้กับเครื่องคอมพิวเตอร์ส่วนบุคคล โน้ตบุ๊ก มีหลายเวอร์ชั่นเนื่องจากการจัดหาระบบปฏิบัติการในแต่ละรุ่นมีระยะเวลาการจัดหาที่ไม่เท่ากัน ทำให้มีหลายเวอร์ชั่น เช่น Windows ๗, Windows ๑๐ และ Window ๑๑ เป็นต้น โดยจะมีการอัพเดทข้อมูลเป็นปัจจุบันเสมอ

๔.๖ ข้อมูลอาคารสถานที่ตั้งของสำนักงาน ป.ป.ท.

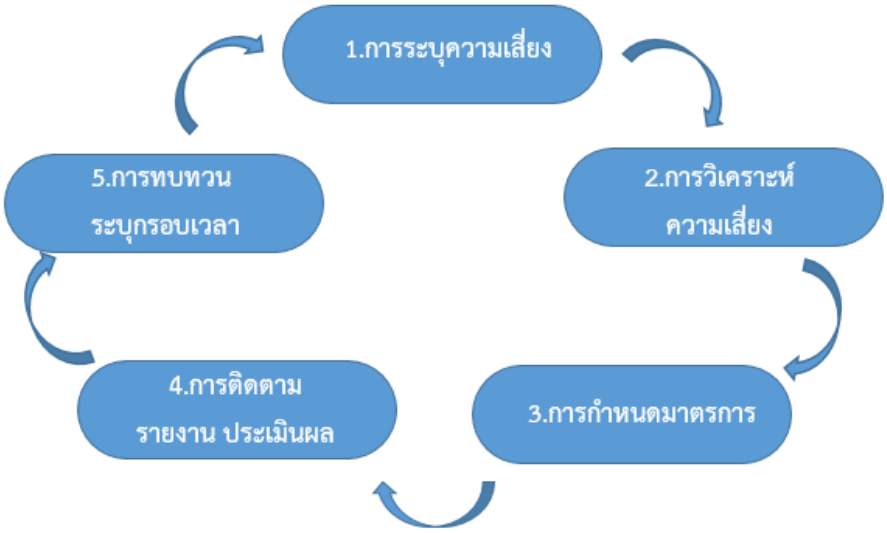
หน่วยงาน	ที่อยู่	ชั้น	สถานะอาคาร	ที่วางตู้ RACK	จำนวนตู้ RACK	ระบบ Intranet/Internet
สำนักงาน ป.ป.ท. ส่วนกลาง	๙๙ หมู่ ๔ อาคารซอฟต์แวร์ปาร์ค ถ.แจ้งวัฒนะ อ.ปากเกร็ด จ.นนทบุรี ๑๑๑๒๐	๓๘	อาคารเช่า	ชั้น ๒	๑๕ U x ๒	GIN/MPLS
				ชั้น ๑๒ A	Data Center	
				ชั้น ๑๔	๒๗ U	
				ชั้น ๒๓	๔๒ U	
				ชั้น ๒๘	๑๕ U	
				ชั้น ๓๐	๑๕ U x ๒	
				ชั้น ๓๑	๔๒ U	
				ชั้น ๓๘	๑๕ U	
สำนักงาน ปปท.เขต ๑	๒๒/๒๕ ถ.นเรศวร ต.ประตูชัย อ.พระนครศรีอยุธยา จ.พระนครศรีอยุธยา ๑๓๐๐๐	๔	อาคารเช่า	ชั้น ๑ ชั้น ๒	๑๕ U ๔๒ U	GIN/ADSL/FFTX
สำนักงาน ปปท.เขต ๒	เลขที่ ๓๔๘ หมู่ที่ ๑ ตำบลหนองไม้แดง อำเภอเมือง จังหวัดชลบุรี ๒๐๐๐๐	๑	ที่ตั้งของตัวเอง	ชั้น ๒	๔๒ U	GIN/ADSL/FFTX
สำนักงาน ปปท.เขต ๓	เลขที่ ๑๑๘ หมู่ ๑๐ ถ.มิตรภาพ ต.โคกกรวด อ.เมือง จ.นครราชสีมา ๓๐๒๘๐	๒	อาคารเช่า	ชั้น ๑	๑๕ U	GIN/ADSL/FFTX
				ชั้น ๒	๔๒ U	
สำนักงาน ปปท.เขต ๔	เลขที่ ๔/๓๓ อาคารปริ้นซ์ออฟฟิตเพล็กซ์ ถ.หน้าเมือง ต.ในเมือง อ.เมือง จ.ขอนแก่น ๔๐๐๐๐	๒	อาคารเช่า	ชั้น ๒	๑๕ U	GIN/ADSL/FFTX
				ชั้น ๒	๔๒ U	

หน่วยงาน	ที่อยู่	ชั้น	สถานะอาคาร	ที่วางตู้ RACK	จำนวนตู้ RACK	ระบบ Intranet/Internet
สำนักงาน ปปท.เขต ๕	๙๙/๕ ศูนย์ราชการจังหวัดเชียงใหม่ ถนนโชตนา ตำบลช้างเผือก อำเภอเมืองเชียงใหม่ เชียงใหม่ ๕๐๓๐๐	๑	ที่ตั้งของตัวเอง	ชั้น ๑	๑๕ U / ๔๒ U	GIN/ADSL/FFTX
สำนักงาน ปปท.เขต ๖	เลขที่ ๗๒๓/๑๓-๑๗ ถ.พิชัยสงคราม ต.ในเมือง อ.เมือง จ.พิษณุโลก ๖๕๐๐๐	๔	อาคารเช่า	ชั้น ๒	๑๕ U / ๔๒ U	GIN/ADSL/FFTX
สำนักงาน ปปท.เขต ๗	เลขที่ ๔๔๕/๒ ถ.เทศา ถ.พระประโทน อ.เมือง จ.นครปฐม ๗๓๐๐๐	๓	อาคารเช่า	ชั้น ๑ ชั้น ๓	๑๕ U ๔๒ U	GIN/ADSL/FFTX
สำนักงาน ปปท.เขต ๘	เลขที่ ๙๑/๑ หมู่ที่ ๑ อาคาร ซี.พี.ทาวเวอร์ ชั้น ๒ ถ.กาญจนวิถี ต.นางกุ้ง อ.เมือง จ.สุราษฎร์ธานี ๘๔๐๐๐	๑	อาคารเช่า	ชั้น ๒	๑๕ U / ๔๒ U	GIN/ADSL/FFTX
สำนักงาน ปปท.เขต ๙	ตึก NT ชั้น ๑-๒ เลขที่ ๗๗๗ หมู่ที่ ๑ ถนนเลี่ยงเมือง (สายเอเชีย) ตำบลควนลัง อำเภอหาดใหญ่ จังหวัดสงขลา , ๙๐๑๑๐	๓	อาคารเช่า	ชั้น ๓	๔๒ U	GIN/ADSL/FFTX

บทที่ ๒
กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล

๑. กระบวนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยงเป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน และจัดลำดับความเสี่ยงที่มีผลต่อการดำเนินงานของหน่วยงาน การบริหารความเสี่ยงอย่างมีประสิทธิภาพต้องมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม ๕ ขั้นตอน ดังนี้



ภาพที่ ๓ แสดงกระบวนการบริหารความเสี่ยง

๑.๑ การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กรวิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

- การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย
- การใช้ Checklist
- การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”
- การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน
- การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

๑.๒ การวิเคราะห์และประเมินความเสี่ยง

เป็นการประเมินถึงผลกระทบของความเสี่ยงและโอกาสที่จะเกิดความเสี่ยง โดยการให้คะแนนความน่าจะเป็น และหามาตรการในการบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้หรือลดน้อยลง ประกอบด้วย ๔ ขั้นตอน

๑.๒.๑ การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้นซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ ๕ ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และ น้อยมาก)ส่วนระดับของความ เสี่ยงอาจกำหนดเป็นเกณฑ์ ๔ ระดับ (สูงมาก สูง ปานกลาง และ น้อย)

๑.๒.๒ การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยงซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้ การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้นก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน ๒ มิติ ได้แก่มิติผลกระทบ และมิติโอกาสของความเสี่ยงที่จะเกิดขึ้นโดยมีเกณฑ์การพิจารณาให้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีผลกระทบจากการเกิดความเสี่ยงต่อการปฏิบัติงานที่หน่วยงานได้ ดังนี้

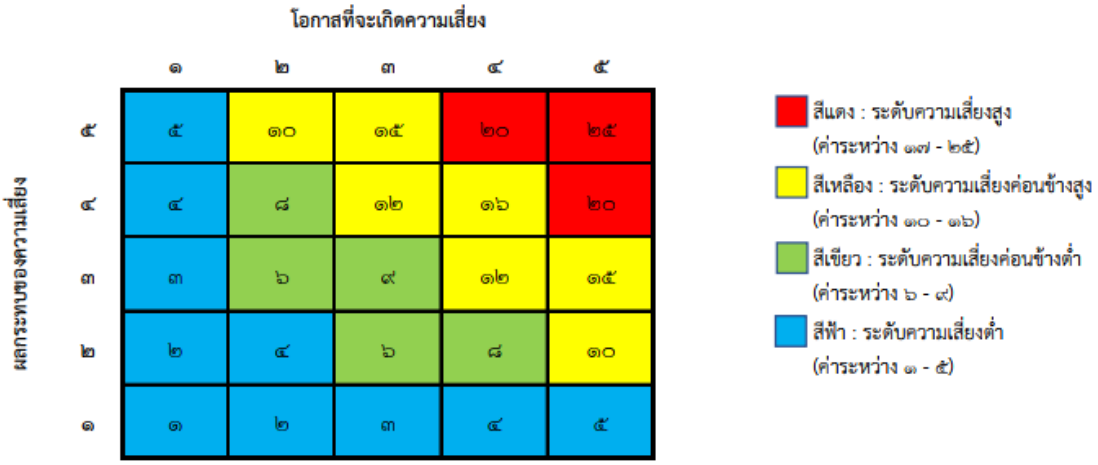
เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง (Likelihood)

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
๕	สูงมาก	บ่อยมาก (อาจเกิดขึ้นได้ทุกวัน)
๔	สูง	บ่อย (อาจเกิดขึ้นได้ทุกสัปดาห์)
๓	ปานกลาง	ปานกลาง (อาจเกิดขึ้นได้ทุกเดือน)
๒	น้อย	ไม่บ่อย (อาจเกิดขึ้นได้ทุกไตรมาส)
๑	น้อยมาก	นานๆ ครั้ง (อาจเกิดขึ้นได้ปีละ ๑ ครั้ง)

เกณฑ์การประเมิน ผลกระทบ (Impact)

ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมด และเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ
๔	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบ ความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
๓	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

๑.๒.๓ การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน ดังภาพที่ ๒



ภาพที่ ๒ แผนผังประเมินความเสี่ยง

๑.๒.๔ การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณาการกำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสม โดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

๑.๓ การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้การควบคุมอาจแบ่งได้เป็น ๔ ประเภท คือ

๑) ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุมการเข้าถึงเอกสาร เป็นต้น

๒) การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

๓) การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์

๔) การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้วจะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรกอาจใช้ขั้นตอนดังนี้

ก) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมีเพื่อป้องกัน ความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

ข) พิจารณาหรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

ค) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

๑.๔ การติดตาม รายงานและประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงที่ได้กำหนดไว้

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการ หรือแนวทางมาใช้ปฏิบัติเพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง ในโครงการ/กิจกรรม ที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอและนำมาวางแผนจัดการความเสี่ยงทางเลือกในการบริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสม โดยพิจารณา ได้ ดังนี้

๑) พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๒) เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

๓) กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

๔) ในรอบปีต่อไปให้พิจารณาผลการติดตามการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการมาบริหารความเสี่ยงตามกระบวนการเหล่านั้น หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมิน และบริหารจัดการความเสี่ยงว่ามีความเสี่ยงที่ยังเหลือ อยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

๑.๕ การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวนอย่างชัดเจน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

๒. ความเสี่ยงด้านเทคโนโลยีดิจิทัล

สำนักงาน ป.ป.ท. ได้กำหนดประเภทความเสี่ยงด้านเทคโนโลยียีดิจิทัลตามแนวทางของ COSO (Committee of Sponsoring Organization) ออกได้ เป็น ๕ ประเภท ดังนี้

๒.๑ ด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสาร ที่มีประสิทธิภาพเพียงพอ

๒.๒ ด้านบุคลากร (Human Risk)

หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีดิจิทัล ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดเพื่อให้บุคลากรมีความรู้ ความเข้าใจ ในการใช้งานการดูแลรักษาความปลอดภัยระบบเทคโนโลยีดิจิทัล รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม รวมถึงบุคลากรตามสัญญาต่าง ๆ ที่ได้ดำเนินการตามสัญญาจ้าง ซึ่งล้วนแต่เป็นความเสี่ยงทั้งสิ้น

๒.๓ ด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร (Hardware and Data Communication Risk)

หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่าง ๆ ประกอบด้วย

สปายแวร์ : ฝังตัว จ้องขโมยข้อมูล
แรนซัมแวร์ : แฮกข้อมูล เรียกค่าไถ่
โทรจัน : สอดแนม ซุ่มโจมตี
ฟิชชิ่ง : ฝังลิงค์หลอกให้กด

หรือ ไวรัสคอมพิวเตอร์ อื่น ๆ ซึ่งมีการตรวจพบและแพร่กระจายในโลกไซเบอร์ทั้งที่เป็นการโจมตีจากภายในระบบเครือข่าย LAN หรือ VPN และจากภายนอกองค์กรโดยผ่านทางเครือข่าย (Networks) WAN, MAN หรือ จากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น

๒.๔ ด้านโปรแกรมคอมพิวเตอร์ (Software Risk)

หมายถึง ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้น ๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งทางสำนักงาน ป.ป.ท. อาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น

๒.๕ ด้านระบบข้อมูล (Database Risk)

หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่าง ๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูลเพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสีย

แก่องค์กร ความเสี่ยงเหล่านี้ทำให้มีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยงด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศและการสื่อสารเป็นปัจจัยสำคัญสำหรับผู้บริหาร ผู้มีส่วนได้ส่วนเสียโดยตรง รวมถึงประชาชนทั่วไป ดังนั้นการรักษาความปลอดภัยของระบบข้อมูลและคอมพิวเตอร์จากภัยต่าง ๆ ทั้งภัยจากคน ภัยจากธรรมชาติหรือเหตุการณ์ใด ๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกัน เพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศและเทคโนโลยีและการสื่อสาร

๓. การจัดการความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกันเพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

ประการที่ ๑ การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยงการดำเนินการเพื่อหลีกเลี่ยงเหตุการณ์ที่ก่อให้เกิดความเสี่ยง องค์กรอาจจะเผชิญกับความเสี่ยงที่ผู้บริหารพิจารณาแล้วพบว่า ไม่มีแนวทางในการจัดการ กับความเสี่ยงนั้น กล่าวคือ ไม่มีวิธีการลดโอกาสหรือผลกระทบ หรือไม่สามารถหาผู้อื่นมาร่วมจัดการ ความเสี่ยงได้ แต่ความเสี่ยงดังกล่าวยังอยู่ในระดับที่ไม่สามารถยอมรับได้ ผู้บริหารควรเลือกหลีกเลี่ยง ความเสี่ยงด้วยการหยุดดำเนินงานหรือกิจกรรมนั้น ๆ หรือเปลี่ยนวัตถุประสงค์ของงานหรือกิจกรรมนั้นไป เพื่อหลีกเลี่ยงไม่ให้เกิดเหตุการณ์ที่จะก่อให้เกิดความเสี่ยง อย่างไรก็ตาม การหลีกเลี่ยงความเสี่ยง ต้องคำนึงถึงต้นทุนค่าเสียโอกาสที่จะเกิดขึ้นจากการหยุดดำเนินการงานหรือกิจกรรมนั้นด้วย

ประการที่ ๒ การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง

ประการที่ ๓ การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ก็ควรขจัดให้หมดไปหรือลดความรุนแรงของความเสี่ยงลง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

ประการที่ ๔ การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์ เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย หรือการจ้างให้บุคคลภายนอกดำเนินกิจกรรมหรืองานบางอย่างแทน (Outsource)

การพิจารณาว่าจะเลือกตอบสนองความเสี่ยงด้วยวิธีใด สิ่งที่ควรคำนึงมากที่สุด คือ ต้นทุนทุนที่จะใช้ในการดำเนินการและผลประโยชน์ที่จะได้รับ เมื่อเลือกวิธีการตอบสนองความเสี่ยงได้แล้ว ควรจัดทำแผนบริหารความเสี่ยงโดยละเอียด โดยกำหนดวัตถุประสงค์ของแผน เป้าหมายตามยุทธศาสตร์ขององค์กร ระดับความเสี่ยงที่ยอมรับได้ ระยะเวลาดำเนินการ ผู้รับผิดชอบ และผลที่ศาดว่าจะได้รับ

๔. ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของสำนักงาน ป.ป.ท. ได้แก่

๔.๑ ปัจจัยภายนอก ได้แก่

- ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ
- การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
- การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)
- ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง
- ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ
- การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๔.๒ ปัจจัยภายใน ได้แก่

- ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย
- การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่าง ๆ จากผู้ใช้ภายในองค์กร
- เจ้าหน้าที่หรือบุคลการของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร เสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๕. การประเมินความเสียหาย

๕.๑ ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด

ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๕.๒ ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ

ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

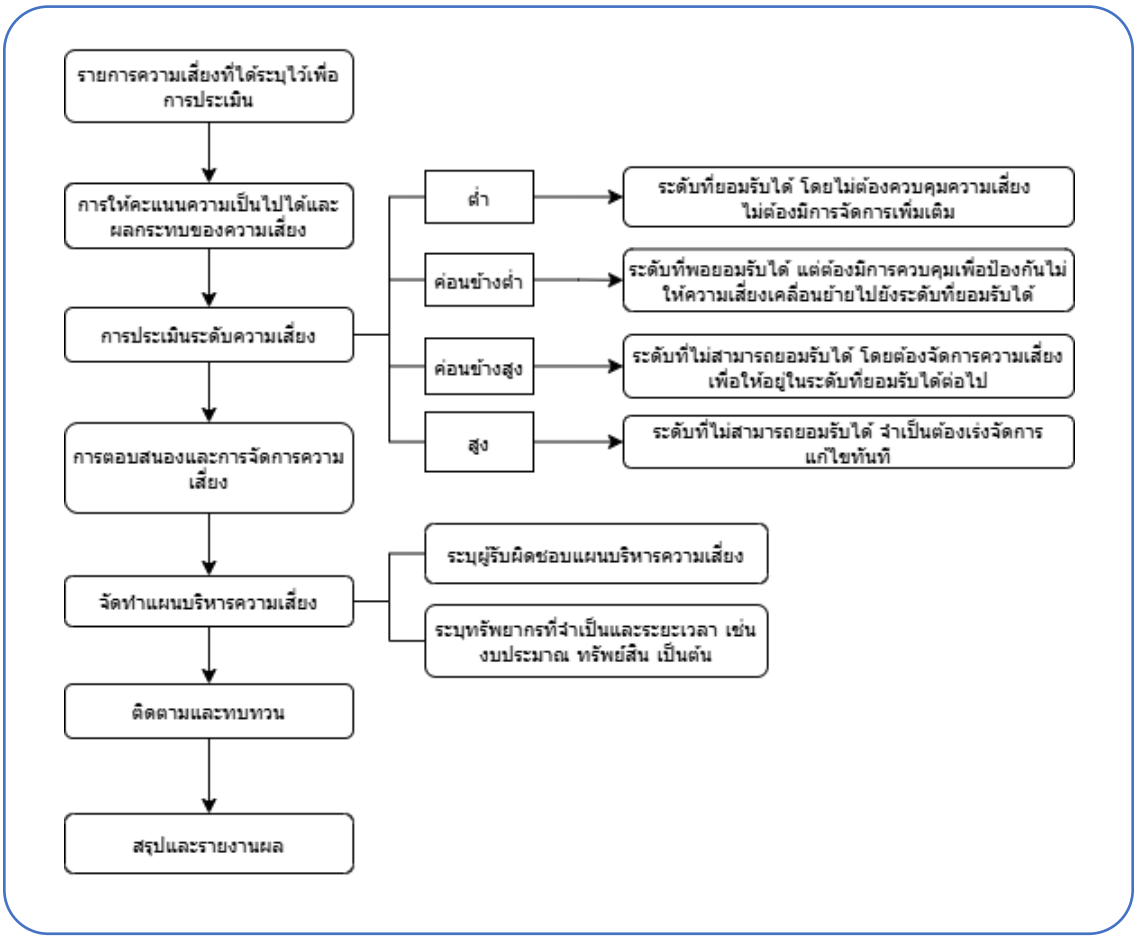
๖. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบตามรอบการรายงานผล และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณี

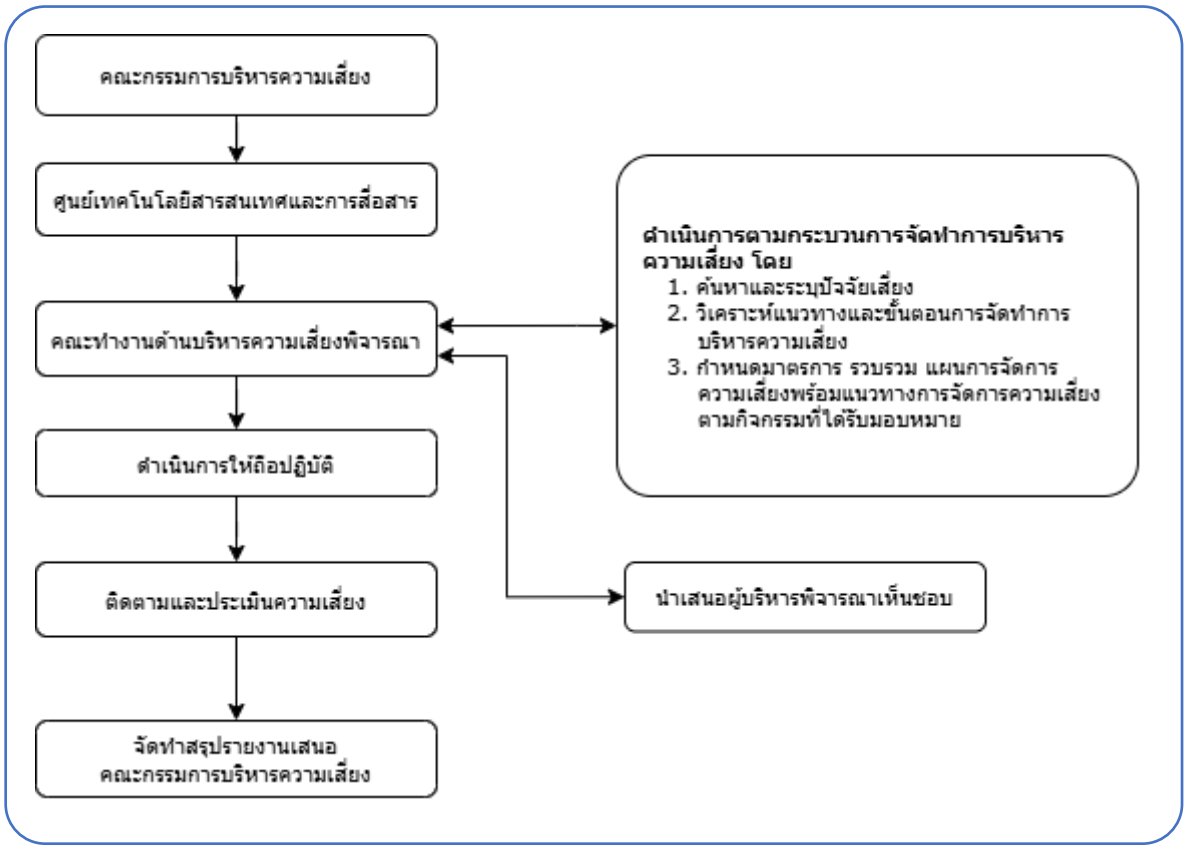
บทที่ ๓
การวิเคราะห์การบริหารจัดการความเสี่ยง

สำนักงาน ป.ป.ท. ได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่าง ๆ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) จึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ประจำปีพ.ศ. ๒๕๖๙ โดยกระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยียีดิจิทัล และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้น ๆ ดังตารางการบริหารจัดการความเสี่ยง ที่ได้จัดทำการวิเคราะห์โดยแยกการวิเคราะห์ออกเป็นกิจกรรม ต่าง ๆ ดังต่อไปนี้

๑. แนวทางและขั้นตอนการบริหารความเสี่ยง



๒. กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร



๓. ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศในทุกด้าน ตามเกณฑ์การประเมินความเสี่ยงที่ได้กำหนดขึ้นโดยพิจารณาจาก ความถีหรือโอกาสที่เกิดขึ้น และความรุนแรงของผลกระทบ โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท. สำนักงาน ได้พิจารณาคัดเลือกความเสี่ยงตั้งแต่ระดับคะแนน ๑๐ - ๒๕ เพื่อนำมาเข้าสู่กระบวนการบริหารจัดการความเสี่ยงเพื่อจัดการและควบคุมความเสี่ยงให้ลดลง ส่วนความเสี่ยงในระดับค่า ๙ และที่ต่ำกว่า ถือว่าเป็นความเสี่ยงที่สามารถยอมรับได้

ตารางที่ ๑ ประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

รหัส	ชื่อความเสี่ยง	โอกาส	ผลกระทบ	คะแนน
R๐๑	ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น โดยไม่ได้รับอนุญาต	๓	๕	๑๕
R๐๒	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	๓	๕	๑๕
R๐๓	ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	๑	๕	๕
R๐๔	ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	๓	๕	๑๕
R๐๕	ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	๒	๔	๘
R๐๖	ความเสี่ยงจากสถานการณ์โรคระบาดร้ายแรง	๓	๔	๑๒
R๐๗	ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	๓	๕	๑๕
R๐๘	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware Ransomware	๕	๕	๒๕
R๐๙	ความเสี่ยงจากความชื้นและอุณภูมิในห้องแม่ข่าย	๔	๕	๒๐
R๑๐	ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี (Hacker)	๕	๕	๒๕
R๑๑	ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	๒	๕	๑๐
R๑๒	ความเสี่ยงจากกรณีเว็บไซต์ถูกโจมตีเปลี่ยนหน้าเว็บ (Website Defacement)	๓	๕	๑๕
R๑๓	ความเสี่ยงในการให้บริการระบบรับเรื่องร้องเรียนและบริการประชาชน ๑๒๐๖	๓	๔	๑๒
R๑๔	ความเสี่ยงจากช่องโหว่จากการพัฒนาระบบงานภายในองค์กร	๔	๕	๒๐
R๑๕	ความเสี่ยงจากการใช้ระบบที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	๔	๕	๒๐
R๑๖	ความเสี่ยงจากการได้รับการสนับสนุนงบประมาณด้านเทคโนโลยีดิจิทัลไม่เพียงพอ	๔	๕	๒๐
R๑๗	ความเสี่ยงจากการบุคลากรสายงานคอมพิวเตอร์ขาดทักษะและความรู้ที่ทันสมัยในการปฏิบัติงานด้านคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง	๒	๔	๘
R๑๘	ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	๒	๔	๘
R๑๙	ความเสี่ยงจากระบบเครือข่ายและระบบคอมพิวเตอร์แม่ข่ายถูกโจมตี	๕	๕	๒๕

ตารางที่ ๒ ผลการประเมินความเสี่ยงและแนวทางการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ความเสี่ยง	ประเภทความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
		ปัจจัยความเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	กิจกรรม
1. <u>ความเสี่ยงสูง</u> มีค่าคะแนน ระหว่าง 17 -25									
R๐๘ ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware Ransomware	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	- -การดาวน์โหลดและติดตั้งซอฟต์แวร์ที่ไม่รู้แหล่งที่มา -การเข้าเว็บไซต์ที่มีความเสี่ยงและฝัง Spyware ไว้ - อุปกรณ์รักษาความมั่นคงปลอดภัยไม่มีการ Update - เครื่องคอมพิวเตอร์ไม่ได้ติดตั้งโปรแกรม Antivirus และโปรแกรมที่ถูกต้องตามลิขสิทธิ์ - การดาวน์โหลดและติดตั้งซอฟต์แวร์ที่ไม่รู้แหล่งที่มา -การเข้าเว็บไซต์ที่มีความเสี่ยงและฝัง Spyware ไว้	- ระบบงานต่างๆไม่สามารถใช้งานได้ - สร้างความเสียหายต่อเครื่องแม่ข่าย -ข้อมูลสูญหาย -ทำให้มีปริมาณข้อมูลจราจรคอมพิวเตอร์ (Traffic) ที่เป็นอันตรายต่อระบบเครือข่ายและสารสนเทศเป็นจำนวนมาก	๕	๕	๒๕	-- ดำเนินการจัดทำแนวทางการเข้าถึงอุปกรณ์ด้านเครือข่ายและระบบคอมพิวเตอร์ - มีการตรวจสอบเฝ้าระวังอย่างสม่ำเสมอ -ติดตั้งโปรแกรมป้องกันไวรัส (Anti-Virus) ให้ผู้ใช้งาน -ขอความร่วมมือจากผู้ใช้งานไม่เข้าเว็บไซต์ที่มีความเสี่ยง และไม่ดาวน์โหลดซอฟต์แวร์ที่ไม่รู้แหล่งที่มา - ประกาศนโยบายและแนวปฏิบัติการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ - การขับเคลื่อนให้ผู้ใช้งานสำรองข้อมูลไว้ที่ workD Storage	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	๑. การจัดอบรมสร้างความตระหนักรู้และอบรมให้ความรู้กับผู้ใช้งานด้านความมั่นคงปลอดภัย ๒. การจัดหาโปรแกรม Anti Virus ที่ทันสมัยและมีลิขสิทธิ์มาติดตั้งทุกเครื่องที่มีการนำเข้ามาใช้งานในสำนักงาน ป.ป.ท. ๓. การขับเคลื่อนให้ผู้ใช้งานสำรองข้อมูลไว้ที่ workD Storage ๔. การสำรองข้อมูลไว้ที่อุปกรณ์ภายนอก (Externel Harddisk)
							- มีการเข้าร่วมโครงการของหน่วยงานด้านความมั่นคงปลอดภัย	☐ การหลีกเลี่ยง ☐ การยอมรับ ☐ การควบคุม ☑ การถ่ายโอน	

ความเสี่ยง	ประเภทความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
		ปัจจัยความเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	กิจกรรม
R๑๙ ความเสี่ยงจากระบบเครือข่ายและระบบคอมพิวเตอร์แม่ข่ายถูกโจมตี	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	- ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์ ลักลอบเข้าระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่มีการใช้บัญชีผู้ใช้สำหรับเชื่อมต่อ VPN โดยใช้เพียงชื่อผู้ใช้และรหัสผ่าน (Credential based Authentication)	- เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถใช้งานได้ - ข้อมูลถูกจารกรรม หรือสูญหาย - ระบบเครือข่ายไม่สามารถใช้งานได้	๕	๕	๒๕	- จัดหาอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น IPS, SIEM - มีการทบทวนและจัดการบัญชีผู้ใช้งานที่ไม่ได้ใช้งานอย่างสม่ำเสมอ - แยกเครือข่ายสำหรับการบริหารจัดการ (Management Network) ของ ESXi ออกจากเครือข่ายผู้ใช้งานทั่วไป	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	๑. กำหนดนโยบายการจัดการ Credential สำหรับบัญชีผู้ดูแลระบบให้มีความซับซ้อนและเปลี่ยนรหัสผ่านตามรอบระยะเวลา ๒. การซักซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์ (CIRP) ๓. จัด Group Policy และ Access Control Policy สำหรับ VPN โดยมีการจำกัดสิทธิ์การเข้าถึงตามความจำเป็น (Least Privilege)
R๑๐ ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี (Hacker)	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	-การถูกโจรกรรม (Hack) หรือเปลี่ยนแปลงข้อมูล -โปรแกรมเสียหาย -การใช้ช่องโหว่ของโปรแกรม หรือซ่อน Script ไว้เพื่อวัตถุประสงค์แอบแฝง -รหัสผ่านที่ใช้เข้าสู่ระบบสามารถคาดเดาได้ง่ายหรือไม่มีความปลอดภัย	- ลดความน่าเชื่อถือต่อองค์กรหากข้อมูลถูกขโมยไปและนำไปเผยแพร่ - อาจเกิดการจารกรรมข้อมูล ที่มีชั้นความลับ หรือเป็นข้อมูลส่วนบุคคล	๕	๕	๒๕	- ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP- Top ๑๐ Web Application Security Risks เพื่อลดความเสี่ยง - มีการตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test) - มีการตรวจสอบเฝ้าระวังอย่างสม่ำเสมอ	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	๑. การตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test) ๒. จัดเก็บข้อมูลจราจรคอมพิวเตอร์ (logfile) อย่างต่อเนื่อง

ความเสี่ยง	ประเภทความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
		ปัจจัยความเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	กิจกรรม
R๐๙ ความเสี่ยงจากความชื้นและอุณภูมิในห้องแม่ข่าย	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	- ขาดการตรวจสอบความชื้นและอุณหภูมิของห้องแม่ข่าย - การทำงานของเครื่อง ปรับอากาศมีปัญหา	- ระบบงานต่างๆไม่สามารถใช้งานได้ - สร้างความเสียหายต่อเครื่องแม่ข่าย - อาจเกิดความร้อนสูง และเกิดเหตุอัคคีภัย	๔	๕	๒๐	- มีการควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม - ตรวจสอบการทำงานของเครื่องปรับอากาศอย่างสม่ำเสมอ	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	๑. การตรวจสอบและบำรุงรักษาเครื่องปรับอากาศอย่างสม่ำเสมอ เพื่อลดความเสี่ยงจากการทำงานขัดข้อง ๒. มีเครื่องปรับอากาศสำรองเพื่อให้ระบบทำความเย็นทำงานสลับกันได้
R๑๔ ความเสี่ยงจากช่องโหว่จากการพัฒนาระบบงานภายในองค์กร	ความเสี่ยงด้านระบบข้อมูล	- การทำงานผิดพลาดของอุปกรณ์และระบบงาน - การพัฒนาระบบที่ไม่ได้มาตรฐานด้านความปลอดภัย - มีการเขียนโปรแกรมซ่อน Script ไว้เพื่อวัตถุประสงค์แอบแฝง	- ลดความน่าเชื่อถือต่อองค์กรหากข้อมูลถูกขโมยไปและนำไปเผยแพร่ - อาจเกิดการจารกรรมข้อมูล ที่มีชั้นความลับ หรือเป็นข้อมูลส่วนบุคคล	๔	๕	๒๐	- กำหนดมาตรฐานในการพัฒนาซอฟต์แวร์ OWASP- Top ๑๐ WebApplication Security Risks เพื่อลดความเสี่ยง - มีการตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test)	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	๑. การตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test) ๒. กำหนดแนวทางการพัฒนาระบบให้มีการอ้างอิงมาตรฐานการออกแบบและพัฒนาระบบหรือซอฟต์แวร์ ที่เป็นสากล
R๑๕ ความเสี่ยงจากการใช้ระบบที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	ความเสี่ยงด้านระบบข้อมูล	- เสี่ยงต่อการถูกขโมยข้อมูล - เสี่ยงต่อการทำความเสียหายแก่โปรแกรม - ไม่สามารถแก้ไขข้อบกพร่องได้เอง - ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ในระยะยาว	- ลดความน่าเชื่อถือ - อาจเกิดปัญหาผู้รับจ้างทิ้งงาน - ระบบที่พัฒนามีข้อบกพร่อง และไม่สามารถแก้ไข หรือนำไปใช้งานได้จริง - สำนักงาน ป.ป.ท. ไม่สามารถดูแลต่อได้ ในกรณี	๔	๕	๒๐	- การออกแบบระบบให้ให้เป็นไปตามมาตรฐานสากล - มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) - การอัพเดท เมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	๑. กำหนดแนวทางการพัฒนาระบบให้มีการอ้างอิงมาตรฐานการออกแบบและพัฒนาระบบหรือซอฟต์แวร์ ที่เป็นสากล ๒. กำหนดแผนการบำรุงรักษาระบบในระยะยาว

ความเสี่ยง	ประเภทความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
		ปัจจัยความเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	กิจกรรม
			ที่ไม่ได้รับงบประมาณในการบำรุงรักษา				(Database) เกิดความเสียหาย เป็นต้น		
R๑๖ ความเสี่ยงจากการได้รับการสนับสนุนงบประมาณด้านเทคโนโลยีดิจิทัลไม่เพียงพอ	ความเสี่ยงด้านงบประมาณ	- การได้รับงบประมาณไม่เพียงพอ และไม่เป็นไปตามแผนงานที่กำหนด	- การขับเคลื่อนโครงการตามแผนแม่บท ไม่สามารถดำเนินการได้ตามแผน - ระบบงานต่างๆ ไม่สามารถให้บริการได้ต่อเนื่อง	๔	๕	๒๐	- จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ เพื่อแสดงความจำเป็นในการขอสนับสนุนงบประมาณในการดำเนินการด้านเทคโนโลยีสารสนเทศ - การเสนอแผนการจัดสรรงบให้มีประสิทธิภาพ	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	๑. การทบทวนแผนปฏิบัติการด้านเทคโนโลยีสารสนเทศ
							- สร้างความร่วมมือระหว่างหน่วยงาน เพื่อใช้ทรัพยากรร่วมกัน - ขอสนับสนุนงบประมาณ จากหน่วยงานภายนอก	☐ การหลีกเลี่ยง ☐ การยอมรับ ☐ การควบคุม ☑ การถ่ายโอน	
2. ความเสี่ยงค่อนข้างสูง มีค่าคะแนน ระหว่าง 10 -16									
R๐๑ ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น โดยไม่ได้รับอนุญาต	ความเสี่ยงด้านระบบข้อมูล	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ - การอำพรางหรือสวมรอยผู้ใช้ - การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต	- การเข้าถึงระบบเครือข่ายภายในจากบุคคลภายนอก - ข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับรั่วไหลสู่ภายนอก	๓	๕	๑๕	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - การจัดทำระบบการยืนยันตัวตนผู้ใช้งาน ที่สามารถระบุตัวบุคคลที่ชัดเจน	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	๑. การจัดอบรมสร้างความตระหนักรู้และอบรมให้ความรู้กับผู้ใช้งานด้านความมั่นคงปลอดภัย

ความเสี่ยง	ประเภทความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
		ปัจจัยความเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	กิจกรรม
							- มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ		
R๐๒ ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- ไม่สามารถใช้งานเครื่องแม่ข่าย และเครือข่ายได้ - ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่าย ทั้งส่วนระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูล (RDBMS) อันเนื่องมาจากเครื่องไม่ได้ถูกทำการ Shutdown อย่างเหมาะสม	- ข้อมูลเสียหาย - ระบบปฏิบัติการ โปรแกรม หรือฐานข้อมูลเสียหาย ต้องมีการติดตั้งใหม่	๓	๕	๑๕	- จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ -ติดตั้งเครื่องสำรอง ไฟฟ้า (UPS) -ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator)	☐ การหลีกเลี่ยง ☐การยอมรับ ☑ การควบคุม ☐การถ่ายโอน	๑. การจัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP) ๒. การซักซ้อมแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศเทศ (IT Contingency Plan)
R๐๔ ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์ และอุปกรณ์	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- เสียงบประมาณในการจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง - เสียเวลาในการกู้ระบบ - เสียภาพลักษณ์ของสำนักงาน	๓	๕	๑๕	- ตรวจสอบระบบการป้องกันรักษาความปลอดภัย - การตรวจสอบการเข้าออกของบุคคลภายนอก - ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ ที่มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่ - ตรวจสอบข้อมูลผู้มีสิทธิผ่านเข้าออกอย่างสม่ำเสมอ	☐ การหลีกเลี่ยง ☐การยอมรับ ☑ การควบคุม ☐การถ่ายโอน	๑. การควบคุมระบบสแกนใบหน้าผ่านเข้า - ออก ศูนย์เทคโนโลยีสารสนเทศลการสื่อสาร
R๐๖ ความเสี่ยงจากสถานการณ์โรคระบาดร้ายแรง	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การเกิดสถานการณ์โรคระบาดร้ายแรง จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- ผู้ปฏิบัติงานไม่สามารถเข้าปฏิบัติงานในพื้นที่ได้ - หากอุปกรณ์เกิดความเสียหายไม่สามารถติดตั้ง	๓	๔	๑๒	-อบรมเจ้าหน้าที่เพื่อให้สามารถปฏิบัติงานแทนกันได้ -การแก้ไขปัญหาและ	☐ การหลีกเลี่ยง ☐การยอมรับ ☑ การควบคุม	๑. การจัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP)

ความเสี่ยง	ประเภทความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
		ปัจจัยความเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	กิจกรรม
			หรือแก้ไขได้ทันที ทำให้ระบบสารสนเทศไม่สามารถให้บริการได้อย่างต่อเนื่อง				ควบคุมคอมพิวเตอร์จากระยะไกล	☐การถ่ายโอน	
R๐๗ ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	- เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดขัดข้องด้วยสาเหตุทางเทคนิค - มีสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น	- อุปกรณ์ต่างๆได้รับความเสียหาย - ระบบไม่สามารถใช้งานได้ - เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน - สายไฟหรือสายสัญญาณขาด และอาจเกิดไฟฟ้าลัดวงจร	๓	๕	๑๕	- มีการบำรุงรักษา และทดสอบการทำงานของเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ - รักษาความสะอาดในพื้นที่ป้องกันไม่ให้มีเศษอาหารซึ่งเป็นสิ่งดึงดูดสัตว์รบกวน	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	๑. การทำ ๕ ส ภายในองค์กรโดยมีการตรวจสอบสายไฟและอุปกรณ์คอมพิวเตอร์
							- ทำท่อ/รางห่อหุ้มสายไฟและสายสัญญาณ ปิดรอยแตก รอยแยก และช่องว่างในอาคาร เพื่อไม่ให้หนูหรือแมลงเข้าไปได้	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	
R๑๒ ความเสี่ยงจากกรณีเว็บไซต์ถูกโจมตีเปลี่ยนหน้าเว็บ (Website Defacement)	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	- เว็บไซต์ที่ถูกเปลี่ยนหน้า (เช่น หน้าเว็บเป็นสีดำ, มีข้อความแฮกเกอร์) - การทำลายหน้าเว็บอาจทำให้เว็บไซต์หยุดทำงาน (Down) หรือทำงานผิดปกติ - หน้าเว็บที่ถูกแก้ไขอาจถูกฝังมัลแวร์ (Malware) หรือทำลิงก์ปลอมแปลง (Phishing)	- แฮกเกอร์อาจใช้ช่องโหว่เดียวกันนี้ในการเข้าถึงระบบฐานข้อมูล และขโมยข้อมูลสำคัญ (Data Breach) - ผู้ใช้งานที่เข้ามายังเว็บไซต์อาจถูกโจมตี	๓	๕	๑๕	- ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย - มีการตรวจสอบช่องโหว่ (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Test)	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐การถ่ายโอน	๑. การตรวจสอบช่องโหว่ (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Test)

ความเสี่ยง	ประเภทความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
		ปัจจัยความเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	กิจกรรม
R๑๓ ความเสี่ยงในการให้บริการระบบรับเรื่องร้องเรียนและบริการประชาชน ๑๒๐๖	ความเสี่ยงด้านระบบข้อมูล	- อุปกรณ์ที่ใช้งานในระบบมีความล้าสมัย - ระบบมีข้อจำกัดในการบำรุงรักษา และปรับปรุงคุณภาพการใช้งาน - เทคโนโลยีที่ใช้งานอยู่ล้าสมัย	- ระบบไม่สามารถให้บริการได้อย่างต่อเนื่อง - ไม่มีเครื่องมือในการบริหารจัดการที่ทันสมัย	๓	๔	๑๒	- การพัฒนาระบบใหม่ เพื่อเพิ่มประสิทธิภาพระบบการให้บริการ - การนำเทคโนโลยีใหม่เข้ามาใช้ในการพัมนาระบบ	☐ การหลีกเลี่ยง ☑การยอมรับ ☐ การควบคุม ☐การถ่ายโอน	๑. การจัดหาระบบรับเรื่องร้องเรียนและบริการประชาชนเพื่อเพิ่มประสิทธิภาพการทำงาน
3. ความเสี่ยงค่อนข้างต่ำ มีค่าคะแนน ระหว่าง 6 -9									
R๐๕ ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- ผู้ปฏิบัติงานไม่สามารถเข้าปฏิบัติงานในพื้นที่ได้ - อุปกรณ์และข้อมูลอาจจะเกิดความเสียหาย จากการถูกทำลายด้วยวิธีการต่างๆ	๒	๔	๘	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐การถ่ายโอน	๑. การจัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP)
							- จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐การถ่ายโอน	
R๑๑ ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	- ผู้ใช้งาน Download ซอฟท์แวร์ที่มีลิขสิทธิ์มาใช้งานโดยไม่ได้รับอนุญาต - ผู้ใช้งานขาดความตระหนักรู้เรื่องข้อกฎหมาย - การใช้งานด้วยซอฟต์แวร์ฟรี อาจไม่สามารถตอบสนองต่อความต้องการใช้งาน	- อาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ - อาจเกิดความเสียหายต่อชื่อเสียงและความน่าเชื่อถือขององค์กร - อาจเกิดช่องโหว่ที่ทำให้ข้อมูลรั่วไหลได้	๒	๕	๑๐	- ลงทุนในซอฟต์แวร์ลิขสิทธิ์เพื่อให้ได้การสนับสนุน และการอัปเดตที่ปลอดภัย - ทำ Asset Management ตรวจสอบรายการซอฟต์แวร์ทั้งหมดในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ	☐ การหลีกเลี่ยง ☑การยอมรับ ☐ การควบคุม ☐การถ่ายโอน	๑. กำหนดนโยบายที่ชัดเจนในการห้ามติดตั้งซอฟต์แวร์ที่ไม่ได้อนุญาต (Unauthorized Software) ๒. การจัดทำการบริหารจัดการสินทรัพย์ (Asset Management) เพื่อตรวจสอบรายการซอฟต์แวร์ทั้งหมดในเครื่องคอมพิวเตอร์

ความเสี่ยง	ประเภทความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
		ปัจจัยความเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	กิจกรรม
R๑๗ ความเสี่ยงจากการบุคลากรสายงานคอมพิวเตอร์ขาดทักษะและความรู้ที่ทันสมัยในการปฏิบัติงานด้านคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง	ความเสี่ยงด้านการบริหารจัดการ	- การเกิดช่องว่างในการประสานงานและ รับผิดชอบงานอย่างมีประสิทธิภาพ - เจ้าหน้าที่ปฏิบัติงานไม่ตรงตามสายงาน - มีการเปลี่ยนงานบ่อย	- เจ้าหน้าที่ไม่สามารถดูแล ปรับปรุง พัฒนาระบบทางด้านเทคโนโลยีสารสนเทศได้ - เจ้าหน้าที่ไม่สามารถแก้ไขปัญหาได้	๒	๔	๘	- ปรับปรุงโครงสร้างศูนย์สารสนเทศ และสรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสม - จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ - การนำเทคโนโลยีที่สามารถทำงานแทนคนเข้ามาใช้	☐ การหลีกเลี่ยง ☑ การยอมรับ ☐ การควบคุม ☐ การถ่ายโอน	๑. การจัดการองค์ความรู้ (KM) ในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศเพื่อเป็นแนวทางในการแก้ปัญหา ๒. จัดทำคู่มือการปฏิบัติงานด้านระบบเทคโนโลยีสารสนเทศ ๓. ส่งเสริมการอบรมให้แก่เจ้าหน้าที่ ศทส.
R๑๘ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	- การเปลี่ยนแปลงผู้บริหารอาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ - จากกระบวนการภายในที่ไม่เป็นระบบและไม่มีประสิทธิภาพ	- ทิศทางองค์กรไม่ต่อเนื่อง - การดำเนินงานโครงการต่าง ๆ ได้รับผลกระทบ - มีการเปลี่ยนแผลงแผนงานแบบฉับพลัน	๒	๔	๘	- ติดตามและวิเคราะห์นโยบายของผู้บริหาร - จัดทำแผนสำรองการบริหารจัดการหรือดำเนินโครงการเพื่อให้บรรลุเป้าหมาย - การถ่ายทอดนโยบายของผู้บริหารในมิติต่างๆ และการเผยแพร่อย่างเป็นทางการ	☐ การหลีกเลี่ยง ☑ การยอมรับ ☐ การควบคุม ☐ การถ่ายโอน	๑. การทบทวนแผนปฏิบัติการด้านเทคโนโลยีสารสนเทศ
ความเสี่ยงต่ำ มีค่าคะแนน ระหว่าง 1 -5									
R๐๓ ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด	- เสียงบประมาณในการจัดหาระบบทดแทน - การไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทน	๑	๕	๕	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง - ติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง - มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	๑. ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ป้องกันต่างๆให้พร้อมใช้งานอยู่เสมอ เช่น ระบบเตือนภัย ถังดับเพลิง ๒. การซักซ้อมแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิด

ความเสี่ยง	ประเภทความเสี่ยง	การประเมินความเสี่ยง					วิธีการบริหารความเสี่ยง		
		ปัจจัยความเสี่ยง	ผลกระทบที่เกี่ยวข้อง	โอกาส (L)	ผลกระทบ (I)	ระดับความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง	กิจกรรม
		- การบาดเจ็บหรือเสียชีวิตของเจ้าหน้าที่หรือลูกจ้างภายในอาคาร	- ระบบคอมพิวเตอร์และเครือข่ายถูกทำลาย				- จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้	☐ การหลีกเลี่ยง ☐ การยอมรับ ☑ การควบคุม ☐ การถ่ายโอน	ขึ้นกับระบบเทคโนโลยีสารสนเทศเทศ (IT Contingency Plan) ๓. การจัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP)

๔. แผนการดำเนินงานการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๙						ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๗๐						ผู้รับผิดชอบ
		เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	
ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware Ransomware ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่นโดยไม่ได้รับอนุญาต	การจัดอบรมสร้างความตระหนักรู้และอบรมให้ความรู้กับผู้ใช้งานด้านความมั่นคงปลอดภัย			⟷	⟷	⟷			⟷	⟷	⟷			ศทส. /สลธ.
ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware Ransomware	การขับเคลื่อนให้ผู้ใช้งานสำรองข้อมูลไว้ที่ workD Storage	⟷												ศทส. (กลุ่มงานคอมพิวเตอร์ฯ)
ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware Ransomware	การจัดหาโปรแกรม Anti Virus ที่ทันสมัยและมีลิขสิทธิ์มาติดตั้งทุกเครื่องที่มีการนำเข้ามาใช้งานในสำนักงาน ป.ป.ท.	⟷												ศทส. /กยผ.
ความเสี่ยงจากระบบเครือข่ายและระบบคอมพิวเตอร์แม่ข่ายถูกโจมตี	กำหนดนโยบายการ Credential สำหรับบัญชีผู้ดูแลระบบให้มีความซับซ้อน และเปลี่ยนรหัสผ่านตามรอบระยะเวลา	⟷	⟷											ศทส. (กลุ่มงานคอมพิวเตอร์ฯ)
ความเสี่ยงจากระบบเครือข่ายและระบบคอมพิวเตอร์แม่ข่ายถูกโจมตี	การซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (CIRP)			⟷	⟷									ทุกหน่วยงาน
ความเสี่ยงจากระบบเครือข่ายและระบบคอมพิวเตอร์แม่ข่ายถูกโจมตี	การจัด Group Policy และ Access ControlPolicy สำหรับ VPN โดยมีการจำกัดสิทธิ์การเข้าถึงตามความจำเป็น (Least Privilege)	⟷												ศทส. (กลุ่มงานคอมพิวเตอร์ฯ)

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๙						ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๗๐						ผู้รับผิดชอบ
		เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	
ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี (Hacker)	การตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test)							←	—	→				ศทส. (กลุ่มงานบริหารเทคโนโลยีฯ)
ความเสี่ยงจากช่องโหว่จากการพัฒนาระบบงานภายในองค์กร														
ความเสี่ยงจากกรณีเว็บไซต์ถูกโจมตีเปลี่ยนหน้าเว็บ (Website Defacement)														
ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี (Hacker)	จัดเก็บข้อมูลจราจรคอมพิวเตอร์ (logfile) อย่างต่อเนื่อง	←	—	—	—	—	—	—	—	—	—	—	→	ศทส. (กลุ่มงานคอมพิวเตอร์ฯ)
ความเสี่ยงจากความชื้นและอุณภูมิในห้องแม่ข่าย	ตรวจสอบและบำรุงรักษาเครื่องปรับอากาศอย่างสม่ำเสมอ เพื่อลดความเสี่ยงจากการทำงานขัดข้อง	←	—	—	—	—	—	—	—	—	—	—	→	ศทส./สลธ.
ความเสี่ยงจากความชื้นและอุณภูมิในห้องแม่ข่าย	มีเครื่องปรับอากาศสำรองเพื่อให้ระบบทำความเย็นทำงานสลับกันได้	←	—	—	—	—	—	—	—	—	—	—	→	ศทส./สลธ.
ความเสี่ยงจากช่องโหว่จากการพัฒนาระบบงานภายในองค์กร	การกำหนดแนวทางการพัฒนาระบบให้มีการอ้างอิงมาตรฐานการออกแบบและพัฒนาระบบหรือซอฟต์แวร์ที่เป็นสากล				←	→								ศทส. (กลุ่มงานบริหารเทคโนโลยีฯ)
ความเสี่ยงจากการใช้ระบบที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง														
ความเสี่ยงจากการใช้ระบบที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	กำหนดแผนการบำรุงรักษาระบบในระยะยาว		←	—	—	→								ศทส. (กลุ่มงานบริหารเทคโนโลยีฯ)
ความเสี่ยงจากการได้รับการสนับสนุนงบประมาณด้านเทคโนโลยีดิจิทัลไม่เพียงพอ	การทบทวนแผนปฏิบัติการด้านเทคโนโลยีสารสนเทศ	←	—	—	→									ศทส. (กลุ่มงานบริหารเทคโนโลยีฯ)
ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร														
ความเสี่ยงจากการบุคลากรสายงานคอมพิวเตอร์ขาดทักษะและความรู้ที่ทันสมัยในการปฏิบัติงานด้านคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง	การจัดการองค์ความรู้ (KM) ในการปฏิบัติงาน ด้านเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการแก้ปัญหา	←	—	—	—	—	—	—	—	—	—	—	→	ศทส./สลธ.

ความเสี่ยง	กิจกรรม	ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๖๙						ระยะเวลาดำเนินการ ปีงบประมาณ พ.ศ. ๒๕๗๐						ผู้รับผิดชอบ
		เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	
ความเสี่ยงจากการบุคลากรสายงานคอมพิวเตอร์ขาดทักษะและความรู้ที่ทันสมัยในการปฏิบัติงานด้านคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง	จัดทำคู่มือการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ	←	—	—	—	—	—	—	—	—	—	—	→	ศทส.
ความเสี่ยงจากการบุคลากรสายงานคอมพิวเตอร์ขาดทักษะและความรู้ที่ทันสมัยในการปฏิบัติงานด้านคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง	ส่งเสริมการอบรมให้แก่เจ้าหน้าที่ ศทส.	←	—	—	—	—	—	—	—	—	—	—	→	ศทส./ สลธ.
ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่ ความเสี่ยงจากสถานการณ์โรคระบาดร้ายแรง ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP)							←	—	—	—	—	→	ศทส. /ทุกหน่วยงาน
ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่ ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	การซักซ้อมแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศเทศ (IT Contingency Plan)			←	—	→			←	—	→			ศทส./ทุกหน่วยงาน
ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	การควบคุมระบบสแกนใบหน้าผ่านเข้า - ออก ศูนย์เทคโนโลยีสารสนเทศลการสื่อสาร	←	—	—	—	—	—	—	—	—	—	—	→	ศทส. (กลุ่มงานคอมพิวเตอร์ฯ)
ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	การทำ ๕ ส ภายในองค์กร โดยมีการตรวจสอบสายไฟ และอุปกรณ์คอมพิวเตอร์					←	→							ทุกหน่วยงาน
ความเสี่ยงในการให้บริการระบบรับเรื่องร้องเรียนและบริการประชาชน ๑๒๐๖	การจัดหาระบบรับเรื่องร้องเรียนและบริการประชาชน เพื่อเพิ่มประสิทธิภาพการทำงาน		←	—	→									ศทส. (กลุ่มงานคอมพิวเตอร์ฯ)
ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ป้องกันต่างๆ ให้พร้อมใช้งานอยู่เสมอ เช่น ระบบเตือนภัย ถังดับเพลิง	←	—	—	—	—	—	—	—	—	—	—	→	ศทส. (กลุ่มงานคอมพิวเตอร์ฯ)
ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	กำหนดนโยบายที่ชัดเจนในการห้ามติดตั้งซอฟต์แวร์ที่ไม่ได้อนุญาต (Unauthorized Software)		←	—	→									ศทส. (กลุ่มงานคอมพิวเตอร์ฯ)
ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	การจัดทำการบริหารจัดการสินทรัพย์ (Asset Management) เพื่อตรวจสอบรายการซอฟต์แวร์ทั้งหมดในเครื่องคอมพิวเตอร์							←	—	—	→			ศทส. (กลุ่มงานคอมพิวเตอร์ฯ)

บทที่ ๔
การติดตามและรายงานผล

การติดตามผล

เป็นการติดตามผลหลังจากที่ได้ดำเนินการตามแผนการบริหารจัดการความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารจัดการความเสี่ยงนั้นมีประสิทธิภาพ รวมทั้งสาเหตุของความเสี่ยงที่มีผลต่อโอกาสที่จะเกิดและความรุนแรงของผลกระทบ วิธีการจัดการความเสี่ยง รวมถึงแนวทางการจัดการความเสี่ยง มีความเหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงไป และรับทราบปัญหาอุปสรรคที่เกิดขึ้นจากการดำเนินการตามกิจกรรมที่กำหนดไว้ ในแผนบริหารความเสี่ยง รวมทั้งข้อเสนอแนะ เพื่อนำไปใช้ประกอบการพิจารณาทบทวนและกำหนดแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ของสำนักงาน ป.ป.ท. ในปีงบประมาณถัดไป

การรายงานผล

เป็นการรายงานผลการวิเคราะห์และจัดการความเสี่ยงว่า กิจกรรมที่ใช้ในการจัดการความเสี่ยงใดที่มีประสิทธิภาพ ควรดำเนินการต่อเนื่อง วิธีการจัดการความเสี่ยงใดควรปรับเปลี่ยน และนำผลการติดตามดังกล่าว มาจัดทำรายงาน โดยให้หน่วยงานที่รับผิดชอบตามกิจกรรม ดำเนินการจัดทำ “แบบรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ประจำปี พ.ศ. ๒๕๖๙” และส่งให้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จากนั้นให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารดำเนินการวิเคราะห์ผลจากแบบรายงานดังกล่าว เพื่อจัดทำสรุปและข้อเสนอแนะเสนอต่อผู้บริหาร โดยมีแนวทาง ดังนี้

๑. รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ต่อคณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยทางดิจิทัล ของสำนักงาน ป.ป.ท. ทุกสิ้นไตรมาส เพื่อทราบและมั่นใจว่าการบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศมีคุณภาพและมีความเหมาะสม
๒. รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ต่อคณะกรรมการเทคโนโลยีดิจิทัล ของสำนักงาน ป.ป.ท. ทุกสิ้นปีงบประมาณ เพื่อทราบและมั่นใจว่าการบริหารความเสี่ยงและความปลอดภัยด้านเทคโนโลยีสารสนเทศมีคุณภาพ และมีความเหมาะสม
๓. รายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) ภายในไตรมาสแรกของงบประมาณถัดไปเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และวิเคราะห์ถึงปัญหาที่เกิดขึ้นเพื่อเสนอแนวทางแก้ไขอย่างถูกต้องและมีประสิทธิภาพ

แบบฟอร์มรายงานผลการดำเนินงานตามแผนบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ประจำปี พ.ศ. ๒๕๖๙

ความเสี่ยง	กิจกรรม	ผลลัพธ์ของกิจกรรม	ระยะเวลาดำเนินการ	เปอร์เซ็น (%) ความคืบหน้า	ปัญหาอุปสรรค	แนวทางการแก้ไข

ผู้รายงาน.....

(.....)

วันที่รายงาน.....

ภาคผนวก

๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๓. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
๔. แผนบริหารจัดการความเสี่ยงระดับองค์กรของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙