แผนบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ฉบับที่ 1 ประจำปีพ.ศ. 2564

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

แผนบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
ฉบับที่ 1 ประจำปีพ.ศ. 2564

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

คำรับรอง

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับที่ 1 ประจำปีพ.ศ. 2564 ฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการเทคโนโลยีดิจิทัล ของสำนักงาน ป.ป.ท. จากการประชุมครั้งที่ 2/2564 เมื่อวันที่ 17 กุมภาพันธ์ 2564 โดยที่ประชุมมีมติเห็นชอบแผนบริหารความเสี่ยงฯ ดังกล่าว เพื่อให้เจ้าหน้าที่ภายในสำนักงาน ป.ป.ท. นำไปใช้เป็นแนวทางในการปฏิบัติงานตามภารกิจได้อย่างมีความมั่นคงปลอดภัย และสามารถบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

ลงชื่อ.....

(นายภูมิวิศาล เกษมศุข)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO)

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

สารบัญ

คำนำ

การบริหารงานขององค์กรทุกประเภท ทั้งภาครัฐ และภาคเอกชนต่างมีวัตถุประสงค์ของตนเองและมุ่งหวังที่จะทำงานไปให้ถึงเป้าหมายที่วางไว้อย่างดีที่สุด สูญเสียทรัพยากรให้น้อยที่สุดแต่การดำเนินการใดๆ เพื่อบรรลุวัตถุประสงค์ที่วางไว้มักจะต้องประสบความไม่แน่นอนที่จะประสบความสำเร็จมากน้อย แล้วแต่สภาวะที่แวดล้อมอยู่ ดังนั้นความเสี่ยงจึงเป็นภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาสที่ทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้หรือก่อผลเสียหายแก่องค์กรทั้งในด้านยุทธศาสตร์การดำเนินงาน การเงิน ทรัพยากรต่างๆ หรือแม้แต่ชื่อเสียง ภาพลักษณ์

ประเด็นที่สำคัญในเรื่องความเสี่ยง (RISK) คือ ความไม่แน่นอน (Uncertainty) ของผลลัพธ์ที่อาจเป็นในเชิงบวกหรือเชิงลบก็ได้ หากองค์กรสามารถเข้าไปบริหารความเสี่ยงได้อย่างถูกต้อง ภาวะคุกคาม ปัญหา อุปสรรคทั้งหลายที่คาดไว้อาจก่อให้เกิดโอกาสและนำไปสู่นวัตกรรมได้ ทั้งยังเกิดโอกาสในการพัฒนาประสิทธิภาพในการทำงานและการให้บริการความเสี่ยงเป็นเรื่องประกอบกันระหว่างองค์ประกอบที่สำคัญ 2 ส่วน คือโอกาสที่น่าจะเกิดขึ้นของสิ่งที่ไม่พึงประสงค์กับผลกระทบที่ตามมา การบริหารความเสี่ยงอย่างเหมาะสมจะเป็นการสนับสนุนกลยุทธ์และแผนงานให้บรรลุเป้าหมายตามที่วางไว้เข้าใจภัยคุกคามของการปฏิบัติงานในองค์กรมีประสิทธิภาพมากขึ้นสนับสนุนให้มีการปรับปรุงงานอย่างต่อเนื่องมีการสื่อสารในองค์กรมากขึ้น ความสัมพันธ์ต่างๆ ก็ดีตามมา การบริหารความเสี่ยงระดับองค์กร เป็นการผสมผสานการบริหารความเสี่ยงโดยพิจารณาจากความเสี่ยงทั้งหมดเป็นกระบวนการเชิงระบบเพื่อระบุ ประเมิน ควบคุม และสื่อสารความเสี่ยง โดยให้คลอบคลุมทั้งองค์กร ให้มีกระบวนคิดในการที่จะมองไปข้างหน้าโดยได้รับการสนับสนุน และมีส่วนร่วมจากผู้บริหารในทุกระดับและจากทุกคนในองค์กรนั้นๆ

สำนักงาน ป.ป.ท. ตระหนักและเห็นความสำคัญของการบริหารความเสี่ยง จึงจัดให้มีการจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของสำนักงาน ป.ป.ท. ขึ้นเพื่อการบริหารปัจจัยและควบคุม กิจกรรม รวมทั้งกระบวนงานต่างๆ โดยลดโอกาส และผลกระทบที่อาจจะเกิดขึ้นในอนาคตให้อยู่ในระดับที่ยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามยุทธศาสตร์เป็นอันดับแรกและเป้าหมายตามแผนการปฏิบัติราชการ

การบริหารความเสี่ยงเป็นการพิจารณาว่าจะมีสิ่งใด เหตุการณ์ใดที่อาจจะเป็นปัญหา อุปสรรคทำให้ไม่สามารถบรรลุเป้าหมาย และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจหลักตามกฎหมายจัดตั้งส่วนราชการ และเป้าหมายตามแผนปฏิบัติราชการ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

บทที่ 1 บทนำ

1.1 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 อาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอก ส่งผลกระทบต่อการดำเนินงานของสำนักงาน ป.ป.ท. ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงาน ป.ป.ท. มีความมั่นคงปลอดภัย จึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารขึ้น โดยผู้บริหารและเจ้าหน้าที่กลุ่มงานคอมพิวเตอร์และการสื่อสาร ได้มีส่วนร่วมในการจัดทำแผนดังกล่าว และทุกภาคส่วนจำเป็นต้องมีการปฏิบัติตามแผน รวมทั้งมีการทบทวนและปรับปรุงนโยบายและแผนดังกล่าวให้เป็นปัจจุบันอยู่เสมอ

1.2 วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

1.2.1 เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

1.2.2 เพื่อลดความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

1.2.3 เพื่อให้ระบบเทคโนโลยีสารสนเทศดำเนินงานได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

1.2.4 เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

1.2.5 เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหาร และผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและระบบสารสนเทศของสำนักงาน ป.ป.ท.

1.2.6 เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

1.3 นิยามความเสี่ยง

ความเสี่ยง คือ ความไม่แน่นอนที่อาจนำไปสู่ความสูญเสีย ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ความเสี่ยงมีทั้งประเภทที่เป็นความเสี่ยงที่แท้จริงที่เป็นความเสี่ยงที่มีโดยธรรมชาติ และความเสี่ยงที่เกิดจากการเก็งกำไร ความหมายของความเสี่ยงอาจมีการตีความแตกต่างกันไปหลายอย่างตามแต่ความเชี่ยวชาญและอาชีพของผู้ให้คำจำกัดความ

การบริหารความเสี่ยง เป็นการบริหารปัจจัยและควบคุมกิจกรรม หรือกระบวนการต่างๆ เพื่อลดโอกาสที่จะทำให้เกิดความเสียหาย หรือล้มเหลว ดังนั้นเพื่อควบคุมให้ระดับความเสียหายและผลกระทบที่อาจจะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถรับได้ ประเมินได้ ควบคุมได้ และสามารถตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามภารกิจหลักตามกฎหมายจัดตั้งส่วนราชการและเป้าหมายตามแผนปฏิบัติราชการ ประจำปีงบประมาณของส่วนราชการ

ความเสี่ยงในการบริหารองค์กร หมายถึงเหตุการณ์ที่ไม่มีความแน่นอนที่อาจเกิดขึ้นและส่งผลกระทบในเชิงลบต่อการบรรลุวัตถุประสงค์หรือเป้าหมายขององค์กร

ปัจจัยเสี่ยง หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้

การประเมินความเสี่ยง หมายถึง การคาดคะเน หรือคำนวณโอกาสที่จะเป็นเหตุให้เกิดความเสียหาย และหรือความเสียหายที่จะส่งผลกระทบต่อการทำงานที่ไม่บรรลุเป้าหมายที่วางไว้เพื่อให้ทราบความสำคัญของความเสี่ยงที่แตกต่างกันและใช้การพิจารณาในการกำหนดจุดควบคุมความเสี่ยงที่มีนัยสำคัญ

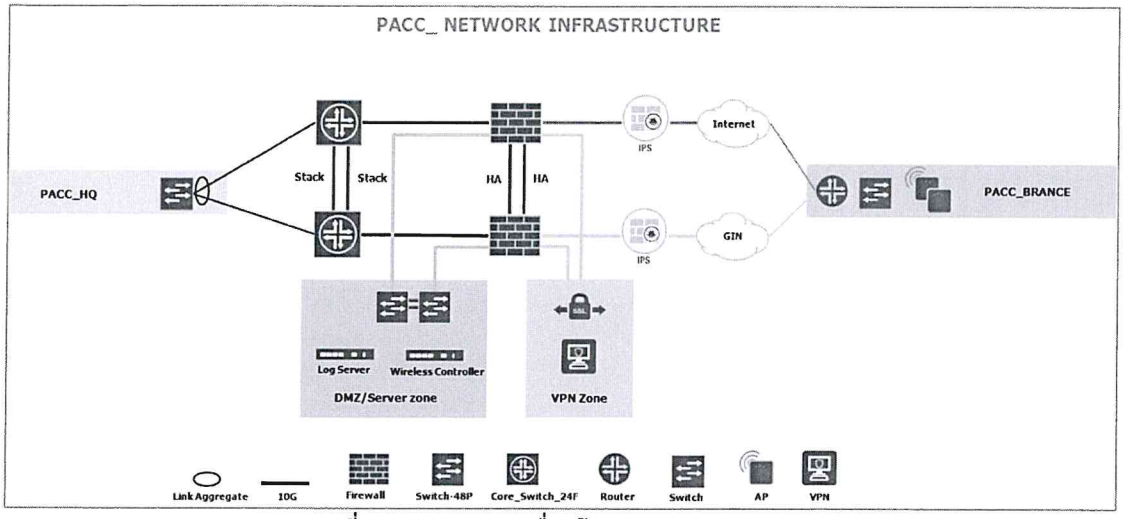
กิจกรรมควบคุม หมายถึง กระบวนการปฏิบัติที่ทุกคนในองค์กรร่วมกันพิจารณากำหนดขึ้นเพื่อสร้างความมั่นใจในระดับที่สมเหตุสมผลในการบรรลุวัตถุประสงค์ของหน่วยงาน

1.4 สถานภาพเทคโนโลยีสารสนเทศและการบริหารจัดการ

1.4.1 ระบบการให้บริการบนเครือข่าย (Network)

1.4.1.1 ภาพรวมระบบเครือข่าย

ระบบเครือข่ายของสำนักงาน ป.ป.ท. ประกอบด้วย 3 ส่วน คือ เครือข่ายระบบสารสนเทศส่วนกลาง (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) เครือข่ายคอมพิวเตอร์สำหรับผู้ใช้งานของสำนักงานส่วนกลาง และเครือข่ายคอมพิวเตอร์สำหรับผู้ใช้งานของสำนักงานเขตในส่วนภูมิภาค โดยทั้ง 3 ส่วนจะเชื่อมโยงเข้าสู่ระบบเครือข่ายส่วนกลางภายในศูนย์เทคโนโลยีสารสนเทศ เพื่อให้บุคลากรของสำนักงาน ป.ป.ท. สามารถใช้งานระบบสารสนเทศได้อย่างสมบูรณ์ โดยแบ่งได้ดังนี้



รูปที่ 1 ภาพรวมการเชื่อมโยงระบบสารสนเทศ

(1) เครือข่ายระบบสารสนเทศส่วนกลาง (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประกอบด้วยส่วนหลัก คือ Core Switch จำนวน 2 ชุดทำงานร่วมกันแบบ Stack รองรับการเชื่อมโยงระบบเครือข่ายของผู้ใช้งานภายในอาคารซอฟต์แวร์ปาร์ค ด้วยความเร็ว 1Gbps และเชื่อมไปยังอุปกรณ์ Firewall ด้วยความเร็ว 10 Gbps ผ่านไปยังส่วนของเครื่องแม่ข่ายและระบบงานต่างๆ ที่อยู่ภายใต้ DMZ/Server Zone นอกจากนี้ยังมีระบบป้องกันการบุกรุกสารสนเทศ (Intruder Prevention System : IPS) รองรับการเชื่อมต่อจาก สำนักงาน ป.ป.ท เขตพื้นที่ในส่วนภูมิภาคทั้งทางเครือข่ายอินเทอร์เน็ตและเครือข่าย GIN รวมทั้งระบบยืนยันตัวตน

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

(3) เครือข่ายคอมพิวเตอร์สำหรับผู้ใช้งานของสำนักงานเขตในส่วนภูมิภาค เชื่อมโยงเครือข่ายเข้าสู่ ระบบสารสนเทศส่วนกลางได้ 2 วิธี คือ การเชื่อมโยงด้วยระบบเครือข่ายสื่อสารข้อมูลภาครัฐ (GIN) และระบบอินเทอร์เน็ตซึ่งในการเข้าถึงระบบสารสนเทศผ่านทางอินเทอร์เน็ตจะต้องเข้าผ่าน Tunnel โดยผู้ใช้ต้องเชื่อมต่อกับ VPN

1.4.1.2 การให้บริการระบบเครือข่าย

ปัจจุบันการให้บริการระบบเครือข่ายคอมพิวเตอร์ของ สำนักงาน ป.ป.ท. มีการแบ่งการให้บริการออกเป็น 2 ส่วนคือ

(1) ระบบเครือข่ายของสำนักงาน ป.ป.ท. ส่วนกลาง

ระบบเครือข่ายของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่ให้บริการในปัจจุบันประกอบไปด้วยสองส่วนหลัก คือ ระบบเครือข่ายที่ใช้สาย (LAN Network) และระบบเครือข่ายไร้สาย (Wireless Network) โดยระบบเครือข่ายทั้งสองมีการบริหารแบบศูนย์รวมโดยผ่านระบบยืนยันตัวตน

(Authentication Radius Server) โดยการให้บริการเครือข่ายจะเป็นการให้บริการจากผู้ให้บริการอินเทอร์เน็ต (Internet service provider: ISP) และการให้บริการผ่านระบบเครือข่ายภายใน (Intranet) โดยมีรายละเอียดดังนี้

- การให้บริการอินเทอร์เน็ตผ่าน (ISP) มีความเร็วอยู่ที่ 150/100 MB
- การให้บริการอินทราเน็ต (Intranet) มีความเร็วอยู่ที่ 40/40 MB

(2) ระบบเครือข่ายของสำนักงาน ปปท.เขต 1 - 9

ระบบเครือข่าย สำนักงาน ป.ป.ท. เขตพื้นที่ ที่ให้บริการในปัจจุบันประกอบไปด้วยสองส่วนหลัก คือ ระบบเครือข่ายที่ใช้สาย (LAN Network) และระบบเครือข่ายไร้สาย (Wireless Network) โดยระบบเครือข่ายทั้งสองมีการให้บริการเครือข่ายจะเป็นการให้บริการจากผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider: ISP) ผ่านระบบ Asymmetric Digital Subscribers Line (ADSL) และการให้บริการผ่านระบบเครือข่ายภายใน (Intranet) โดยมีรายละเอียดดังนี้

ระบบอินเตอร์เน็ต

ลำดับที่	ชื่อสำนักงานงาน	ผู้ให้บริการอินเตอร์เน็ต (ISP)	จำนวนอุปกรณ์	ความเร็ว
1	สำนักงาน ปปท.เขต 1	TOT	1	35/15 MB
2	สำนักงาน ปปท.เขต 2	AIS	1	300/300 MB
3	สำนักงาน ปปท.เขต 3	TOT	1	100/50MB
4	สำนักงาน ปปท.เขต 4	TOT	1	35/35 MB
5	สำนักงาน ปปท.เขต 5	3BB	2	500/200 MB 500/200 MB
6	สำนักงาน ปปท.เขต 6	AIS	1	200/50 MB
7	สำนักงาน ปปท.เขต 7	3BB TOT	2 1	200/200 MB 500/500 MB 200/200 MB
8	สำนักงาน ปปท.เขต 8	CAT		40/20 MB
9	สำนักงาน ปปท.เขต 9	TOT	1	100/100MB

ระบบอินทราเน็ต

ลำดับที่	ชื่อสำนักงานงาน	ผู้ให้บริการอินทราเน็ต (ISP)	จำนวนอุปกรณ์	ความเร็ว
1	สำนักงาน ปปท.เขต 1	GIN	1	20/20 MB
2	สำนักงาน ปปท.เขต 2	GIN	1	20/20 MB
3	สำนักงาน ปปท.เขต 3	GIN	1	20/20 MB
4	สำนักงาน ปปท.เขต 4	GIN	1	20/20 MB
5	สำนักงาน ปปท.เขต 5	GIN	1	20/20 MB
6	สำนักงาน ปปท.เขต 6	GIN	1	20/20 MB
7	สำนักงาน ปปท.เขต 7	GIN	1	20/20 MB
8	สำนักงาน ปปท.เขต 8	GIN	1	20/20 MB
9	สำนักงาน ปปท.เขต 9	GIN	1	20/20 MB

1.4.1.3 การป้องกันและรักษาความปลอดภัยเครือข่าย

(1) Firewall ระบบสารสนเทศจะถูกป้องกันโดยอุปกรณ์ Firewall เพื่อป้องกันการโจมตีจากผู้ไม่ประสงค์ดี โดยสามารถกำหนดนโยบายในการเข้าถึงทรัพยากรสารสนเทศได้ และอุปกรณ์ตรวจจับการบุกรุกระบบ (IPS) ในการตรวจสอบพฤติกรรมการใช้ของผู้ใช้งานหรือซอฟต์แวร์ใดๆ ที่เชื่อมโยงมาจากเครือข่าย GIN และเครือข่ายอินเทอร์เน็ต

อุปกรณ์ Firewall ประกอบด้วย Firewall จำนวน 2 ชุด ทำงานแบบ High Availability (HA) โดยสามารถทำงานทดแทนกันเมื่อมีอุปกรณ์ใดเสียหายจนทำงานไม่ได้โดยเชื่อมต่อกับอุปกรณ์อื่น ดังนี้

- อุปกรณ์ DMZ Switch จำนวน 2 ชุดในแบบขนานเพื่อป้องกันการเข้าถึงระบบเครื่องแม่ข่าย ระบบงาน ฮาร์ดแวร์ และซอฟต์แวร์อื่นๆ ที่อยู่ภายใน DMZ โดยไม่เหมาะสม
- อุปกรณ์ Core Switch ด้วยสายสัญญาณขนาด 10 Gbps จำนวน 2 ชุด แบบขนานเพื่อรองรับผู้ใช้งานจากสำนักงาน ป.ป.ท. ส่วนกลาง
- อุปกรณ์ Switch Cisco C9300-48T-A จำนวน 2 ชุด เพื่อรองรับการใช้งานจากผู้ใช้ของสำนักงาน ป.ป.ท. ในส่วนภูมิภาค
- ระบบ VPN เพื่อเข้าถึงระบบสารสนเทศแบบ Tunnel สำหรับผู้ใช้ที่ต้องการเข้าสู่ระบบสารสนเทศผ่านระบบอินเทอร์เน็ต

(2) Intruder Prevention System (IPS) หมายถึงอุปกรณ์ฮาร์ดแวร์หรือซอฟต์แวร์ที่สามารถตรวจสอบวิเคราะห์หาพฤติกรรมการใช้งานที่อาจก่อให้เกิดอันตรายต่อระบบสารสนเทศ

โดยตรวจสอบ Packet ข้อมูลที่ส่งผ่านระบบเครือข่าย ป้องกันการโจมตี และสามารถทำงานร่วมกับอุปกรณ์ Firewall โดยเพิ่ม Rule เข้าไปเพื่อป้องกันการโจมตีระบบ IPS ติดตั้งจำนวน 1 ชุด แต่ละชุดต่อกับ Firewall เข้าไปยังระบบสารสนเทศภายใน เชื่อมต่อกับเครือข่าย GIN และเครือข่ายอินเทอร์เน็ต ตามลำดับเพื่อป้องกันการบุกรุกผ่านทางเครือข่ายดังกล่าว

1.4.1.4 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

โดย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้มีการนำข้อมูลที่ได้มีการสำรองไว้ไปจัดเก็บ ณ สำนักงาน ปปท. เขต 3 เพื่อลดความเสี่ยงต่อการสูญเสียข้อมูล กรณีเกิดเหตุการณ์ไม่ปกติ และไม่สามารถเข้าห้อง Data Center ได้

1.4.2 อุปกรณ์เครื่องคอมพิวเตอร์ (Hardware)

สำนักงาน ป.ป.ท. ได้ดำเนินการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างต่อเนื่อง ปัจจุบันมีเครื่องคอมพิวเตอร์แม่ข่าย แบ่งออกเป็น 2 ประเภทดังต่อไปนี้

1.4.2.1 Server Farm ข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายประเภท Server Farm ของสำนักงาน ป.ป.ท. มีดังนี้

No	Name	Brand	CPU				RAM (GB)	Storage (GB)	ชื่อระบบงาน	ปีงบประมาณ	ผู้รับผิดชอบ
			GHz	Unit	Core /Unit	Total Cores					
1	Intel Xeon 2.53 Quad Core (X3440) Full Entry Server 3400 Series	-	2.53	1	4	4	4	1000	ระบบค้นคว้ากฎหมาย ระยะที่ 1	2553	ศทส.
2	Intel Xeon E5630 2.53GHz Quad Core (X3440) ProLiant DL380 G7	HP	2.53	1	4	4	8	500	ระบบบริหารนโยบาย แผนงน งบประมาณ และตัวชี้วัด	2554	ศทส.
3	Intel Xeon X5660 2.83GHz Fujitsu Primergy RX300 S6	Fujitsu	2.83	1	4	4	8	438	ฐานข้อมูลระบบรับเรื่องและติดตามการร้องเรียน ระยะที่ 1 (Application)	2554	ศทส.
4	Intel Xeon X5660 2.83GHz Fujitsu Primergy RX300 S6	Fujitsu	2.83	1	6	6	8	900	ฐานข้อมูลระบบรับเรื่องและติดตามการร้องเรียน ระยะที่ 1 (Database)	2554	ศทส.

No	Name	Brand	CPU				RAM (GB)	Storage (GB)	ชื่อระบบงาน	ปีงบประมาณ	ผู้รับผิดชอบ
			GHz	Unit	Core /Unit	Total Cores					
5	Intel Xeon E3120 3.10GHz ProLiant DL120 G7 Server	HP	3.1	1	2	2	4	500	ระบบรักษาความมั่นคงปลอดภัยระบบสารสนเทศ	2555	ศทส.
6	Intel ® Xeon ® L5506 2.13 GHz	HP	2.13	1	2	2	4	292	ระบบบริหารจัดการเครือข่ายไร้สาย	2553	ศทส.
7	Intel Xeon X3450 2.67GHz	Dell	2.67	1	4	4	16	500	ระบบ Call Center 1206	2556	TOT
8	Intel Xeon X3450 2.67GHz		2.67	1	4	4	8	500	ระบบบันทึกเสียงการสนทนา (Voice Record)	2556	ศทส.
9	Dell EMC PowerEdge R640 : Intel ® Xeon ® Gold 6134 CPU 3.20	Dell	3.2	2	8	16	64	2000	โครงการระบบไต่สวนข้อเท็จจริง	2561	มหาวิทยาลัยธรรมศาสตร์

1.4.2.2 Blade Server ข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายประเภท Blade Server ของสำนักงาน ป.ป.ท. มีดังนี้

No	Name	Brand	CPU				RAM (GB)	Storage (GB)	ชื่อระบบงาน	ปีงบประมาณ	ผู้รับผิดชอบ
			GHz	Unit	Core /Unit	Total Cores					
1	Blade Server 1: Intel ® Xeon ® E5620 2.4GHz Blade HS22	IBM	2.4	2	4	8	6	292	ระบบ Backup ข้อมูล	2554	ศทส.
2	Blade Server 2: Intel ® Xeon ® E5620 2.4GHz Blade HS22	IBM	2.4	2	4	8	6	292	ระบบสำนักงานอิเล็กทรอนิกส์ (E-Office) ระยะที่ 1	2554	ศทส. (ยกเลิกการใช้งาน)
3	Blade Server 3: Intel ® Xeon ® E5620 2.4GHz Blade HS22	IBM	2.4	2	4	8	6	292	ระบบบัญชีและการเงิน	2554	บริษัท ฟิวชั่น โซลูชั่น จำกัด
4	Blade Server 4: Intel ® Xeon ® E5620 2.4GHz Blade HS22	IBM	2.4	2	4	8	6	292	ระบบบริหารงานพัสดุ	2554	กลุ่มงานพัสดุ
5	Blade Server 5: Intel ® Xeon ® E5620 2.4GHz Blade HS22	IBM	2.4	2	4	8	6	292	ระบบสารสนเทศภูมิศาสตร์ด้านการป้องกันและปราบปรามทุจริตในภาครัฐ (GIS) ระยะที่ 1	2555	ศทส.
6	Blade Server 6: Intel ® Xeon ® E5620 2.4GHz Blade HS22	IBM	2.4	2	4	8	6	292	ระบบทะเบียนราษฎร์	2556	ศทส.
7	Blade Server 7: Intel ® Xeon ® E5607 2.4GHz Blade HS22	IBM	2.27	2	4	8	4	600	ระบบป้องกันโปรแกรมไม่พึงประสงค์แบบรวมศูนย์	2555	ศทส. (ยกเลิกการใช้งาน)

No	Name	Brand	CPU				RAM (GB)	Storage (GB)	ชื่อระบบงาน	ปีงบประมาณ	ผู้รับผิดชอบ
			GHz	Unit	Core /Unit	Total Cores					
8	Blade Server 8: Intel ® Xeon ® E5607 2.4GHz Blade HS23	IBM	2.27	2	4	8	16	600	ระบบจัดการเครื่องลูกข่ายและครุภัณฑ์คอมพิวเตอร์	2557	ศทส.
9	Blade Server 9: Intel ® Xeon ® E5607 2.6GHz	IBM	2.6	2	4	8	8	600	ระบบ Visual Link	2558	ศทส.
10	Blade Server 10: Intel ® Xeon ® E5607 2.6GHz	IBM	2.6	2	4	8	8	600	ระบบเชื่อมโยงข้อมูลพื้นฐาน	2558	ศทส.
11	Blade Server 11: Intel ® Xeon ® E5607 2.6GHz	IBM	2.6	2	4	8	8	600	IBM Cognos	2558	ศทส.

1.4.2.3 ข้อมูลครุภัณฑ์คอมพิวเตอร์ ประจำปี พ.ศ. 2562

สำหรับเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมทั้งโปรแกรมพื้นฐานต่างๆ ที่สำนักงาน ป.ป.ท. ได้ดำเนินการสำรวจในปัจจุบัน โดยได้ทำการสำรวจข้อมูล ณ ปีงบประมาณ พ.ศ. 2562 มีรายละเอียดดังนี้

ลำดับ	รายการครุภัณฑ์คอมพิวเตอร์	จำนวน
1	เครื่องคอมพิวเตอร์แม่ข่าย	22
2	เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (PC)	191
3	เครื่องคอมพิวเตอร์แบบพกพา (Notebook)	438
4	เครื่องพิมพ์	154
5	เครื่องสแกนเนอร์	25
6	โปรแกรมระบบปฏิบัติการ (Windows)	629
7	โปรแกรม Microsoft Office	510
8	Microsoft SQL Server	4
9	Microsoft Windows Server	25

1.4.3 ระบบฐานข้อมูลและสารสนเทศ (Database and Application)

สำนักงาน ป.ป.ท. มีระบบเทคโนโลยีสารสนเทศ สำหรับใช้งานภายในองค์กร โดยการเข้าใช้ระบบงาน สามารถเข้าใช้โดยผ่าน Website : workcenter.pacc.go.th โดยจะแบ่งการเข้าถึงระบบได้ 2 ช่องทาง ได้แก่

1) ระบบสำนักงานภายใน ที่ต้องเชื่อมต่อระบบ VPN ประกอบด้วย

- ระบบสืบค้นข้อมูลทะเบียนราษฎร์ (ทร.14)
- ระบบสืบค้นข้อมูลประกันสังคม
- ระบบสืบค้นข้อมูลกรมการขนส่งทางบก
- ระบบบริหารจัดการทรัพยากรบุคคล (DPIS)
- ระบบสำนักงานอิเล็กทรอนิกส์ (e-Office)

2) ระบบสำนักงานที่สามารถใช้งานผ่านระบบ Internet ประกอบด้วย

-ระบบสารบรรณอิเล็กทรอนิกส์ (e-Sarabun)

- ระบบจดหมายอิเล็กทรอนิกส์ (e-Mail)
- ระบบแลกเปลี่ยนข้อมูลกระทรวงยุติธรรม (DXC)

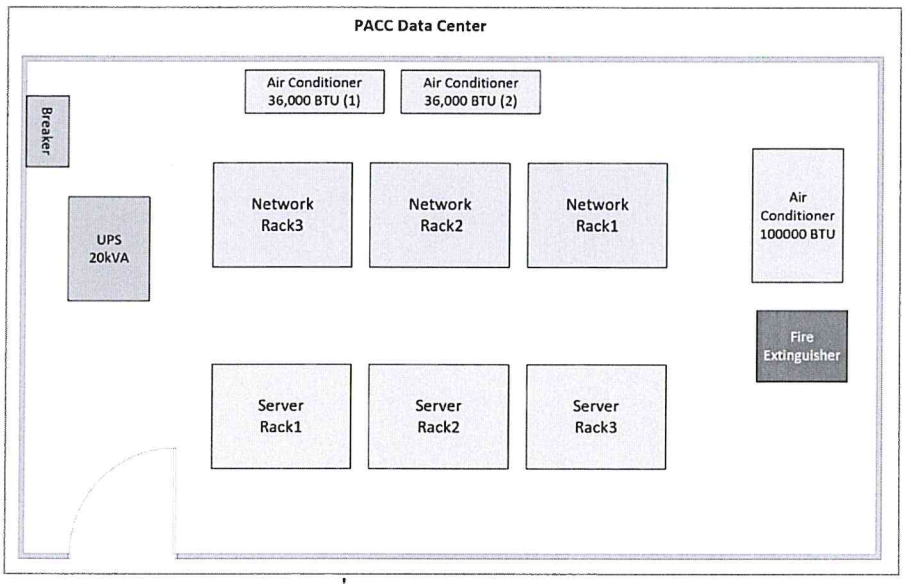
- ระบบสืบค้นข้อมูลนิติบุคคล (GDX Linkage)
- ระบบสืบค้นรายการภาษี กรมสรรพากร
- ระบบสืบค้นสถานภาพบุคคลของเจ้าหน้าที่รัฐ กรมบัญชีกลาง

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

- ระบบรับเรื่องร้องเรียน
- ระบบบริหารจัดการผู้ใช้แบบรวมศูนย์
- ระบบเครือข่ายภาคประชาสังคม (CONNECT)
- ระบบระบบรายงานข้อร้องเรียนเจ้าหน้าที่รัฐกระทำการทุจริตหรือประพฤติมิชอบ

1.4.4 ห้องศูนย์ข้อมูล (Data Center)

ห้องศูนย์ข้อมูล Data Center ตั้งอยู่บนชั้น 12 ภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสารประกอบด้วยตู้ Rack 19" ขนาด 42U สำหรับอุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายจำนวน 3 ตู้ และอุปกรณ์เครือข่ายจำนวน 3 ตู้ รวมมีตู้ Rack ทั้งหมด 6 ตู้ จ่ายกระแสไฟฟ้าแบบ 3 เฟสผ่านอุปกรณ์ UPS ขนาด 20KVA 1 ชุด และมีระบบปรับอากาศ โดยมีเครื่องปรับอากาศที่ติดตั้งระบบปรับอากาศใต้พื้นห้องขนาด 100,000 BTU สำหรับระบายความร้อนช่วงกลางวัน และมีเครื่องปรับอากาศขนาด 36,000 BTU จำนวน 2 เครื่อง สำหรับระบายความร้อนในตอนกลางคืน มีอุณหภูมิเฉลี่ยที่ประมาณ 22-24 องศาเซลเซียส ภายในห้องติดตั้งอุปกรณ์ดับเพลิง สำหรับกรณีฉุกเฉินหากเกิดเพลิงไหม้



รูปที่ 2 PACC Data Center

1.4.5 ระบบรักษาความปลอดภัยเครือข่าย

1.4.5.1 FireWall

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

1.4.5.2 IPS

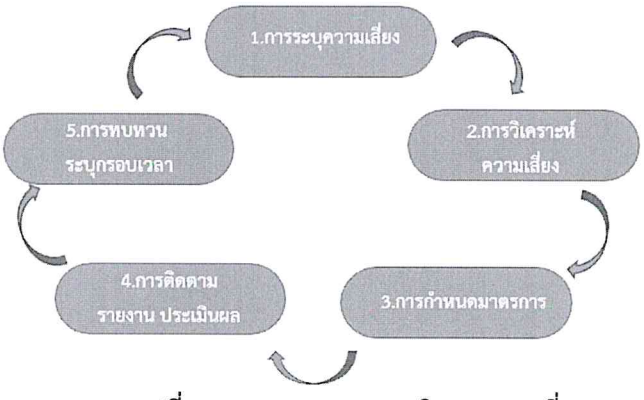
Intruder Prevention System (IPS) หมายถึงอุปกรณ์ฮาร์ดแวร์หรือซอฟต์แวร์ที่สามารถตรวจสอบวิเคราะห์หาพฤติกรรมการใช้งานที่อาจก่อให้เกิดอันตรายต่อระบบสารสนเทศ โดยตรวจสอบ Packet ข้อมูลที่ส่งผ่านระบบเครือข่าย ป้องกันการโจมตี และสามารถทำงานร่วมกับอุปกรณ์ Firewall โดยเพิ่ม Rule เข้าไปเพื่อป้องกันการโจมตีระบบ IPS ติดตั้งจำนวน 1 ชุด โดยจะมีการอัพเดทข้อมูลเป็นปัจจุบันเสมอตลอดระยะเวลารับประกันอุปกรณ์

1.4.5.3 ระบบปฏิบัติการ (OS)

ปัจจุบันสำนักงาน ป.ป.ท. ใช้ระบบปฏิบัติการวินโดวส์พัฒนาโดย Microsoft Corporation เพื่อใช้กับเครื่องคอมพิวเตอร์ส่วนบุคคล โน้ตบุ๊ก มีหลายเวอร์ชั่นเนื่องจากการจัดหาระบบปฏิบัติการในแต่ละรุ่นมีระยะเวลาการจัดหาที่ไม่เท่ากัน ทำให้มีหลายเวอร์ชั่น เช่น Windows 7,Windows 10 เป็นต้น โดยจะมีการอัพเดทข้อมูลเป็นปัจจุบันเสมอ

1.5 กระบวนการบริหารความเสี่ยง

เป็นกระบวนการที่ใช้ในการระบุ วิเคราะห์ ประเมิน จัดระดับความเสี่ยง ที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานของหน่วยงานหรือขององค์กร รวมทั้งการบริหาร/จัดการความเสี่ยงรวมทั้งการกำหนดแนวทางการดำเนินงานหรือมาตรการควบคุมหรือป้องกันหรือลดความเสี่ยง ซึ่งมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม โดยครอบคลุม 5 ขั้นตอน ดังนี้



รูปที่ 3 แสดงกระบวนการบริหารความเสี่ยง

1.5.1 การระบุความเสี่ยงหรือปัจจัยเสี่ยง

เป็นกระบวนการที่ผู้บริหารและผู้ปฏิบัติงานร่วมกันระบุความเสี่ยงและปัจจัยเสี่ยงที่เกี่ยวข้องโครงการ/กิจกรรม เพื่อให้ทราบถึงเหตุการณ์ที่เป็นความเสี่ยง ที่อาจมีผลกระทบต่อการบรรลุผลสำเร็จตามวัตถุประสงค์ ซึ่งต้องคำนึงถึงสภาพแวดล้อมทั้งภายนอกและภายในองค์กร วิธีการในการระบุความเสี่ยงมีหลายวิธี เช่น

1.5.1.1 การระดมสมองเพื่อให้ได้ความเสี่ยงที่หลากหลาย

1.5.1.2 การใช้ Checklist

1.5.1.3 การวิเคราะห์สถานการณ์จากการตั้งคำถาม “What-if”

1.5.1.4 การวิเคราะห์ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอน

1.5.1.5 การรวบรวมปัญหาที่เกิดขึ้นมาแล้ว

ในขั้นตอนนี้ ควรมีการเก็บข้อมูลความสูญเสียที่เกิดขึ้นในรูปของความถี่ของการเกิดความสูญเสียและความรุนแรงของความสูญเสีย รวมทั้งข้อมูลการดำเนินการใด ๆ เพื่อลดความสูญเสียที่เกิดขึ้นในอดีตทั้งที่ประสบผลสำเร็จ และปัญหาอุปสรรคซึ่งจะเป็นประโยชน์ในการดำเนินการต่อไป

1.5.2 การวิเคราะห์และประเมินความเสี่ยง

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วยการวิเคราะห์ การประเมิน และการจัดระดับความเสี่ยง ประกอบด้วย 4 ขั้นตอน คือ

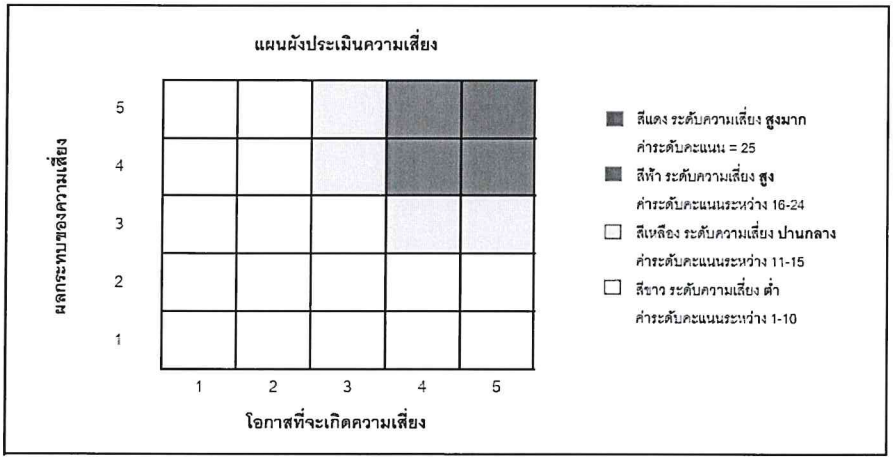
1.5.2.1 การกำหนดเกณฑ์การประเมินมาตรฐาน เป็นเกณฑ์ที่จะใช้ประเมินความเสี่ยง ได้แก่ โอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) คณะกรรมการบริหารความเสี่ยงต้องกำหนดเกณฑ์ของหน่วยงานขึ้น ซึ่งอาจกำหนดได้ทั้งเกณฑ์เชิงปริมาณและเชิงคุณภาพ การกำหนดเกณฑ์ของโอกาสที่เกิดความเสี่ยงอาจกำหนดเป็นเกณฑ์ 5 ระดับ (สูงมาก/รุนแรงมากที่สุด สูง/ค่อนข้างรุนแรง ปานกลาง น้อย และน้อยมาก) ส่วนระดับของความเสี่ยงอาจกำหนดเป็นเกณฑ์ 4 ระดับ (สูงมาก สูง ปานกลาง และน้อย)

1.5.2.2 การประเมินโอกาสและผลกระทบของความเสี่ยง เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินโอกาสที่จะเกิดเหตุการณ์ความเสี่ยงเหล่านั้นและประเมินระดับความรุนแรงหรือมูลค่าความเสียหายจากความเสี่ยงตามเกณฑ์มาตรฐานที่กำหนดเพื่อให้เห็นระดับความเสี่ยงซึ่งแต่ละความเสี่ยงก็จะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้นก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน โดยมีการประเมินใน 2 มิติ ได้แก่ มิติผลกระทบและมิติโอกาสของความเสี่ยงที่จะเกิดขึ้น

เกณฑ์การประเมินโอกาสของการเกิดความเสี่ยง	
ระดับ	การประเมิน
1	โอกาสเกิดขึ้นน้อยมาก
2	โอกาสเกิดขึ้นน้อย
3	โอกาสเกิดขึ้นปานกลาง
4	โอกาสเกิดขึ้นสูง
5	โอกาสเกิดขึ้นสูงมาก

เกณฑ์การประเมินผลกระทบความรุนแรง	
ระดับ	การประเมิน
1	ผลกระทบน้อยมาก
2	ผลกระทบน้อย
3	ผลกระทบปานกลาง
4	ผลกระทบสูง
5	ผลกระทบสูงมาก

1.5.2.3 การวิเคราะห์ความเสี่ยง เป็นการดูความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยงต่อองค์กร ว่าจะก่อให้เกิดระดับความเสี่ยงในระดับใด โดยใช้ตารางระดับความเสี่ยงสูงสุดที่จะต้องบริหารจัดการก่อน



รูปที่ 4 แสดงแผนผังประเมินความเสี่ยง

1.5.2.4 การจัดลำดับความเสี่ยง เป็นการจัดลำดับความรุนแรงของความเสี่ยงที่มีผลต่อองค์กร เพื่อพิจารณากำหนดกิจกรรมการควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมโดยพิจารณาจากระดับความเสี่ยงที่ประเมินได้ เลือกความเสี่ยงที่มีระดับสูงมาก หรือสูงมาจัดทำแผนการบริหารความเสี่ยงเป็นลำดับแรก

1.5.3 การกำหนดมาตรการจัดการความเสี่ยงอย่างรัดกุม

มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยงเพื่อให้สามารถบรรลุเป้าหมาย หรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ในการวางแผน จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้น เพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้ดูแลรักษาความมั่นคงปลอดภัย ป้องกัน/แก้ไข/ควบคุมความเสี่ยง

ไม่ให้มีผลกระทบต่อระบบที่วางไว้ โดยสามารถดำเนินการตามแผนได้ การควบคุมอาจแบ่งได้เป็น 4 ประเภท ดังต่อไปนี้

1.5.3.1 ควบคุมเพื่อการป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาดตั้งแต่แรก เช่น การอนุมัติ การจัดโครงสร้างองค์กร การควบคุม การเข้าถึงเอกสาร เป็นต้น

1.5.3.2 การควบคุมเพื่อให้ตรวจพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นแล้ว เช่น การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น

1.5.3.3 การควบคุมโดยการชี้แนะ (Direction Control) เป็นวิธีควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสาเร็จตามวัตถุประสงค์

1.5.3.4 การควบคุมเพื่อการแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดนั้นซ้ำอีกในอนาคตหลังจากประเมินความเสี่ยงแล้ว จะต้องวิเคราะห์การควบคุมที่มีอยู่ว่าได้มีการจัดการควบคุมเพื่อลดความเสี่ยงดังกล่าวหรือไม่ โดยนำผลการจัดระดับความเสี่ยงในระดับสูงมากและสูง มาประเมินมาตรการควบคุมเป็นอันดับแรก อาจใช้ขั้นตอนดังนี้

1) นำปัจจัยเสี่ยงที่อยู่ในระดับสูงมาก หรือสูงมากำหนดวิธีควบคุมที่ควรจะมี เพื่อป้องกันความเสี่ยงหรือปัจจัยเสี่ยงเหล่านั้น

2) พิจารณาหรือประเมินว่าในปัจจุบันความเสี่ยงหรือปัจจัยเสี่ยงนั้นมีการควบคุมอยู่แล้วหรือไม่

3) ถ้ามีการควบคุมแล้ว ให้ประเมินต่อไปว่าการควบคุมนั้นได้ผลตามความต้องการหรือไม่

1.5.4 การติดตาม รายงาน และประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยง

การติดตามผลการดำเนินงาน การนำกลยุทธ์ มาตรการหรือแนวทางมาใช้ปฏิบัติ เพื่อลดโอกาสที่เกิดความเสี่ยง หรือลดความเสียหายของผลที่อาจเกิดขึ้นจากความเสี่ยง โครงการ/กิจกรรมที่ยังไม่มีกิจกรรมควบคุมความเสี่ยง หรือมีแต่ไม่เพียงพอ และนำมาวางแผนจัดการความเสี่ยง ทางเลือกในการบริหารความเสี่ยงมีหลายวิธีซึ่งสามารถปรับเปลี่ยนหรือนำมาผสมผสานให้เหมาะสมกับสถานการณ์ อาจเป็นการยอมรับความเสี่ยง การลด/การควบคุมความเสี่ยง การกระจายความเสี่ยง หรือการหลีกเลี่ยงความเสี่ยง เมื่อองค์กรทราบความเสี่ยงที่ยังเหลืออยู่จากการประเมินความเสี่ยง และการประเมินการควบคุมแล้วให้พิจารณาความเป็นไปได้และค่าใช้จ่ายแต่ละทางเลือก เพื่อตัดสินใจเลือกมาตรการลดความเสี่ยงที่เหมาะสมโดยพิจารณาจาก

- พิจารณาว่ายอมรับความเสี่ยง หรือจะกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

- เปรียบเทียบค่าใช้จ่ายหรือต้นทุนในการจัดการให้มีมาตรการควบคุมกับผลประโยชน์ที่จะได้รับจากมาตรการดังกล่าวว่าคุ้มค่าหรือไม่

- กรณีเลือกกำหนดกิจกรรมควบคุมเพื่อลดความเสี่ยงให้กำหนดวิธีควบคุมในแผนบริหารความเสี่ยง

- ในรอบปีต่อไป ให้พิจารณาผลการติดต่อการบริหารความเสี่ยงในงวดก่อนที่ดำเนินการแล้วมาทำการบริหารความเสี่ยงตามกระบวนการเหล่านั้นอีกครั้ง หากพบว่ายังมีความเสี่ยงที่มีนัยสำคัญซึ่งอาจมีผลต่อการบรรลุวัตถุประสงค์และเป้าหมายตามแผนปฏิบัติงานขององค์กร ให้นำมาระบุการควบคุมในแผนบริหารความเสี่ยงด้วยการรายงานผลการวิเคราะห์ประเมินและบริหารจัดการความเสี่ยง ว่ามีความเสี่ยงที่ยังเหลืออยู่หรือไม่ ถ้าไม่มีเหลืออยู่ มีอยู่ในระดับความเสี่ยงสูงมากเพียงใด และมีวิธีการจัดการความเสี่ยงนั้นอย่างไรเสนอต่อผู้บริหารเพื่อทราบและสั่งการ

1.5.5 การทบทวนการบริหารความเสี่ยงโดยระบุกรอบเวลาในการทบทวน

เป็นการติดตามภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยง ว่ามีความเสี่ยงแล้วเพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ ทั้งนี้ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยงที่ใช้ และเป็นการตรวจสอบความคืบหน้าของมาตรการควบคุม โดยอาจติดตามผลเป็นรายครั้งตามรอบระยะเวลา หรือการติดตามผลในระหว่างการปฏิบัติงาน

1.6 การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกันเพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance) หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

1.6.1 การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้นจึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

1.6.2 การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการ หรือป้องกันความเสี่ยง

1.6.3 การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิดขึ้น หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรกำจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยง โดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น

1.6.4 การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่นอุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขาย

1.7 ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงาน ป.ป.ท. ได้แก่

1.7.1 ปัจจัยภายนอก

1.7.1.1 ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

1.7.1.2 การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

1.7.1.3 การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server)

1.7.1.4 ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหายหรือขัดข้อง

1.7.1.5 ระบบกระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

1.7.1.6 การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

1.7.2 ปัจจัยภายใน

1.7.2.1 ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

1.7.2.2 การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ จากผู้ใช้ภายในองค์กร

1.7.2.3 เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

1.8 การประเมินความเสียหาย

1.8.1 ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

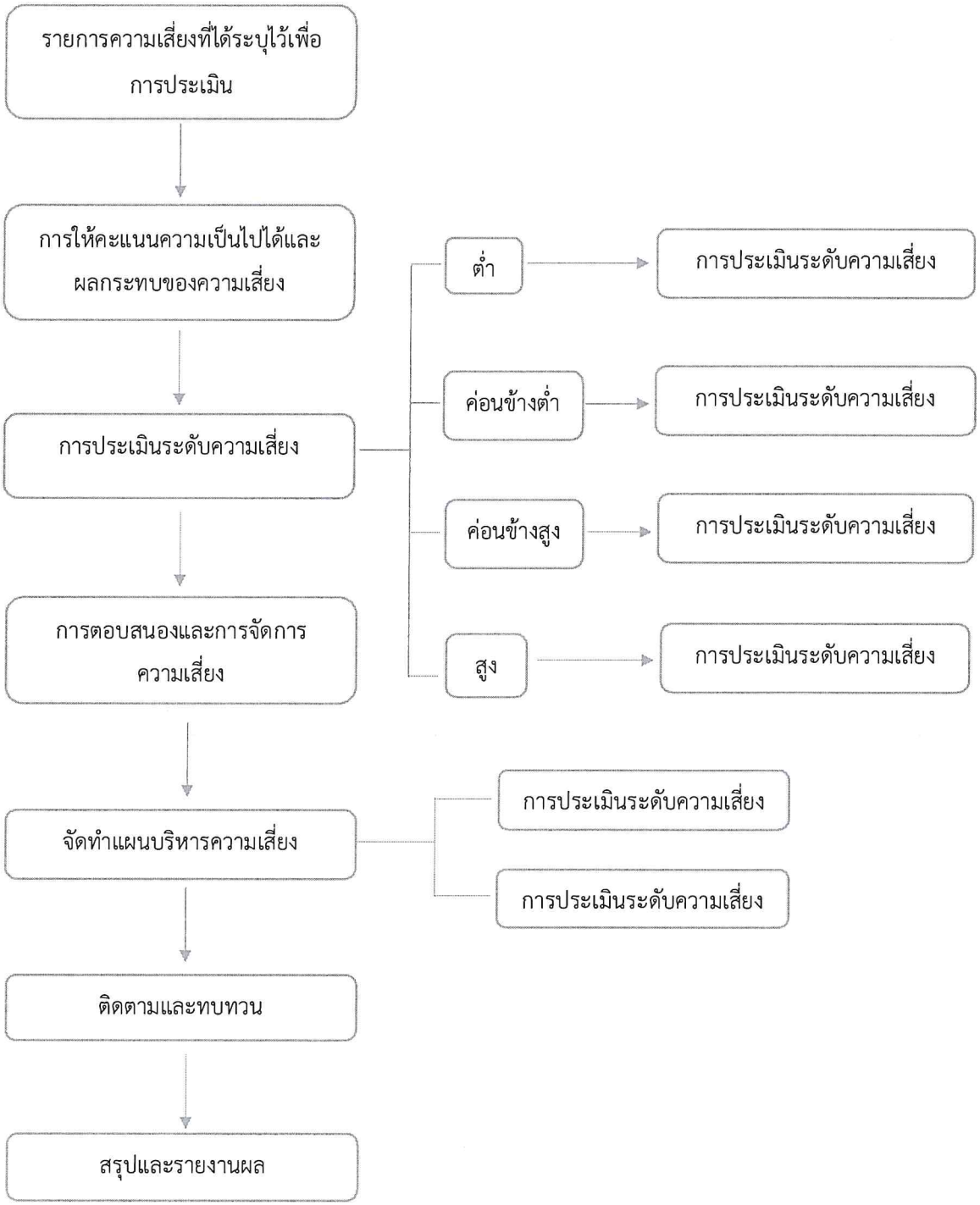
1.8.2 ความเสียหายที่เกิดผลเสียหายและต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

1.9 การติดตามและรายงานผล

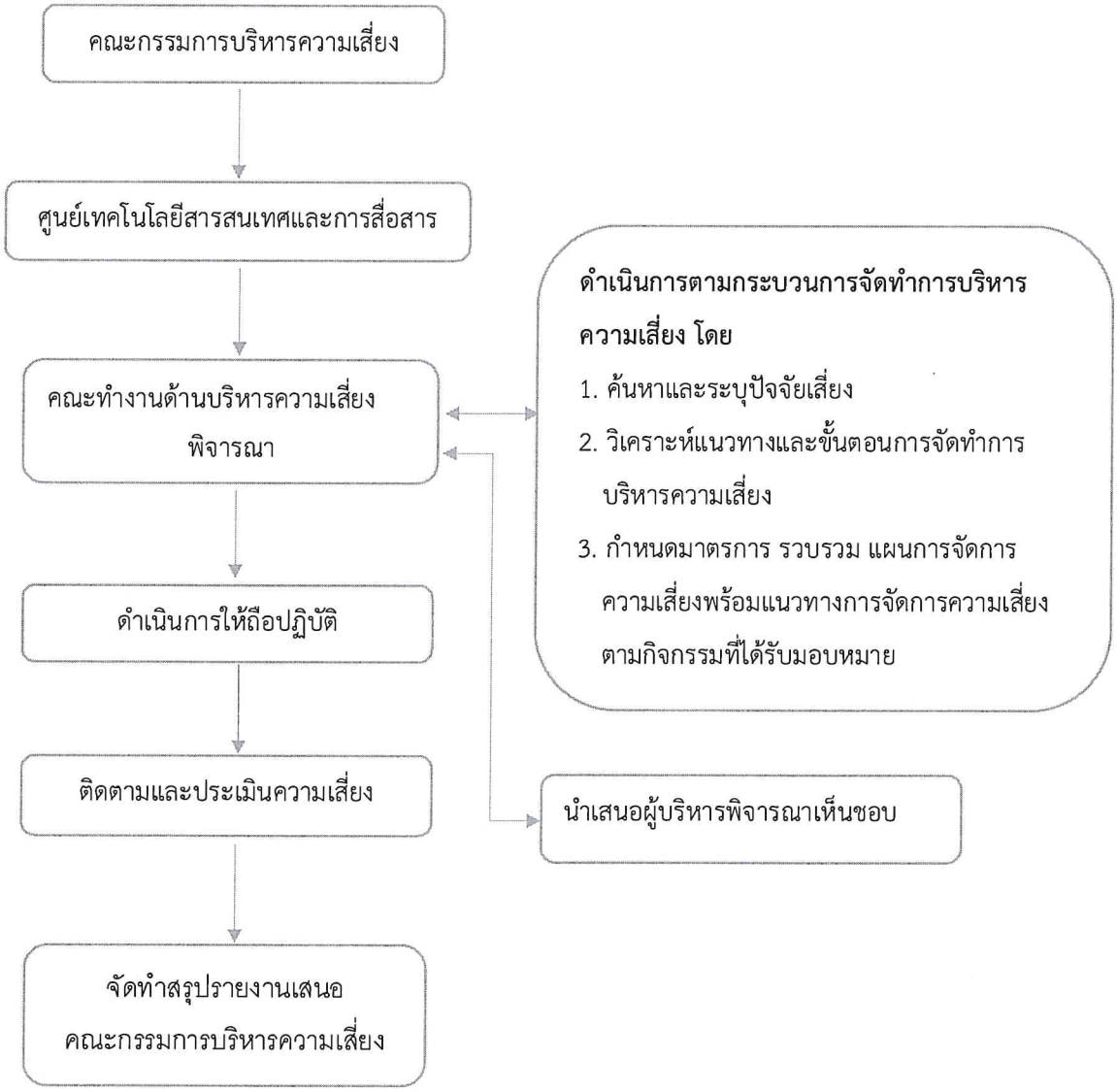
กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุ

บทที่ 2 การวิเคราะห์การบริหารจัดการความเสี่ยง

2.1 แผนภูมิแนวทางและขั้นตอนการบริหารความเสี่ยง

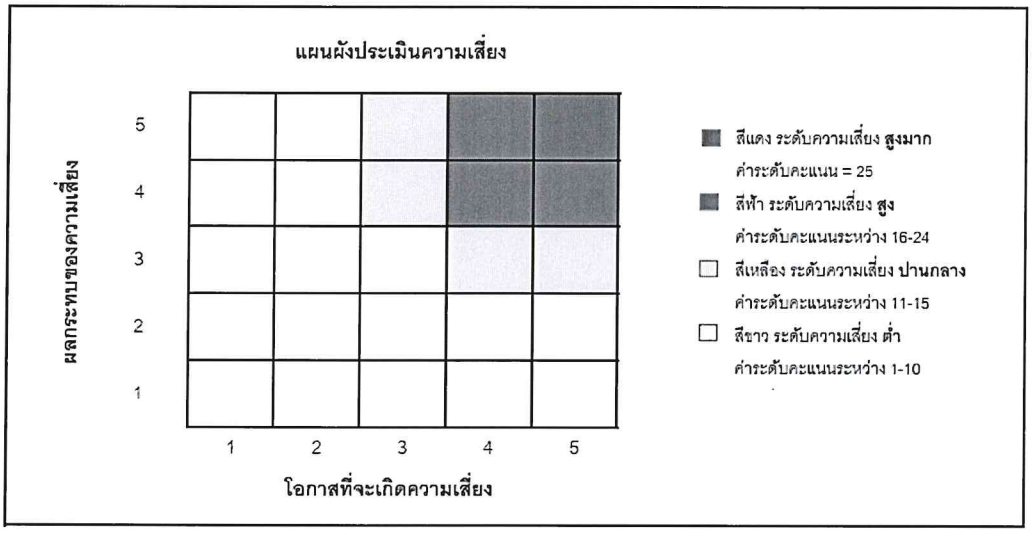


2.2 กระบวนการจัดทำการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร



2.3 การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk Identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่ โดยแหล่งที่มาของความเสี่ยงมาจากปัจจัยภายในและภายนอก และจะต้องครอบคลุมความเสี่ยงทั้ง 4 ประเภท คือ ความเสี่ยงด้านกลยุทธ์ (S) ความเสี่ยงด้านปฏิบัติงาน (O) ความเสี่ยงดานการเงิน (F) และความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ/กฎหมาย (C) การกำหนดประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการประเมินระดับความเป็นไปได้ และผลกระทบมีดังนี้



2.4 ผลการประเมินแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

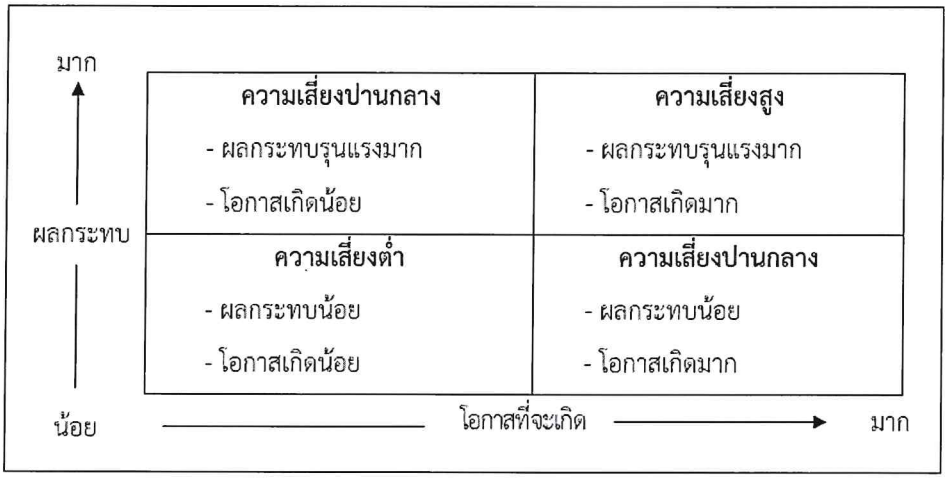
2.4.1 การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง, ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบและประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยง ที่ได้จากการพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

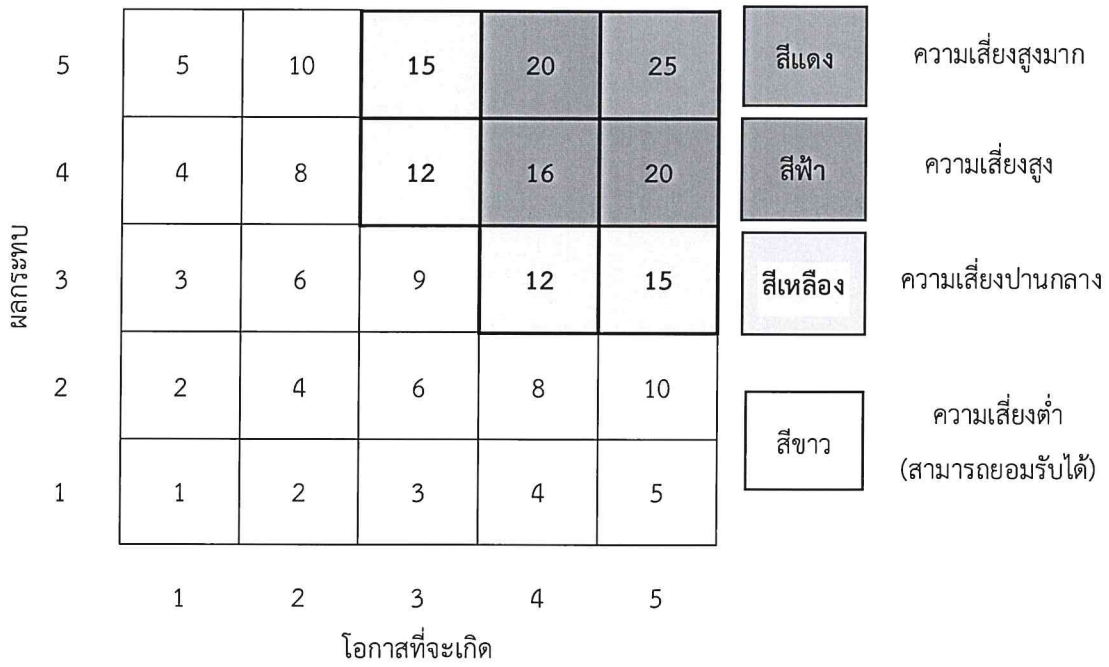
ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่างๆ x ความรุนแรงของเหตุการณ์ต่างๆ ซึ่งใช้เกณฑ์ในการจัดแบ่งดังนี้

ระดับคะแนน	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี
1 – 10	ต่ำ	ยอมรับความเสี่ยง	ขาว
11 – 15	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง
16 – 24	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า
25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง

การวัดระดับความเสี่ยง



แผนภูมิการประเมินความเสี่ยง



การประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน ป.ป.ท. ได้มีการรวบรวมวิเคราะห์ และกำหนดประเภทความเสี่ยงตามแนวทางของ COSO (Committee of Sponsoring Organization) ไว้ทั้งสิ้น 7 ประเภทความเสี่ยง มีรายละเอียดดังนี้

(1) ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในด้านการวางแผน การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากร และคณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียด มีเกณฑ์การประเมินดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	20 ครั้ง/เดือน
4	สูง	16 ครั้ง/เดือน
3	ปานกลาง	12 ครั้ง/ เดือน
2	น้อย	8 ครั้ง/เดือน
1	น้อยมาก	น้อยกว่า 4 ครั้ง/เดือน

ระดับความรุนแรงของผลกระทบของความเสี่ยง

ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

แผนการรองรับความเสี่ยง

ระดับคะแนน	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี	แผนการรองรับ
1 – 10	ต่ำ	ยอมรับความเสี่ยง	ขาว	- การให้ความรู้เบื้องต้น - สร้างความตระหนักรู้เกี่ยวกับข้อกฎหมาย
11 – 15	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง	- มีกระบวนการติดตาม รายเดือน หรือสัปดาห์
16 – 20	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า	- แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง	- การปรับปรุง กฎระเบียบและแนวปฏิบัติ ที่เกี่ยวข้อง

(2) ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม คือ ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย อัคคีภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง การก่อการร้าย รวมถึงการไม่มีระบบรักษาความปลอดภัยห้องปฏิบัติการระบบเครือข่ายและคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย และระบบสื่อสารที่มีประสิทธิภาพเพียงพอ มีเกณฑ์การประเมินดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	5 ครั้ง/ เดือนขึ้นไป
4	สูง	4 ครั้ง/ เดือน
3	ปานกลาง	3 ครั้ง/ เดือน
2	น้อย	2 ครั้ง/ เดือน
1	น้อยมาก	1 ครั้ง/ เดือน

ระดับความรุนแรงของผลกระทบของความเสี่ยง

ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

แผนการรองรับความเสี่ยง

ระดับคะแนน	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี	แผนการรองรับ
1 – 10	ต่ำ	ยอมรับความเสี่ยง	ขาว	- มีการซักซ้อมแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้น
11 – 15	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง	- มีการตรวจสอบระบบ - มีการสำรองข้อมูล
16 – 20	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า	- แผนรองรับสถานการณ์ฉุกเฉิน
25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง	- การจัดตั้ง DR Site

(3) ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร คือ ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ Malware, Trojan, Adware เป็นต้น ทั้งที่เป็นการโจมตีจากภายใน และมาจากภายนอกโดยผ่านทางเครือข่าย (Networks) หรือจากคอมพิวเตอร์โดยตรง เช่น จาก USB Flash Drive หรือ USB External Hard Disk Drive เป็นต้น มีเกณฑ์การประเมินดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	50 เครื่องขึ้นไป
4	สูง	40 เครื่อง
3	ปานกลาง	30 เครื่อง
2	น้อย	20 เครื่อง
1	น้อยมาก	น้อยกว่า 10 เครื่อง

ระดับความรุนแรงของผลกระทบของความเสี่ยง

ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

แผนการรองรับความเสี่ยง

ระดับคะแนน	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี	แผนการรองรับ
1 – 10	ต่ำ	ยอมรับความเสี่ยง	ขาว	- การตรวจสอบอุปกรณ์เทคโนโลยีสารสนเทศให้พร้อมใช้งานอย่างสม่ำเสมอ
11 – 15	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง	- การจัดทำการบำรุงรักษาระบบ (MA) - มีการสำรองข้อมูล
16 – 20	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า	- แผนรองรับสถานการณ์ฉุกเฉิน
25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง	- ดำเนินการแจ้ง Thaicert - แจ้งหน่วยงานภายนอกที่เกี่ยวข้องเพื่อร่วมแก้ไข

(4) ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ คือ ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น การใช้โปรแกรมที่ไม่มีการอัพเดทให้ทันสมัย เพื่อลดช่องโหว่ที่อาจเกิดจาก Bug ของซอฟต์แวร์นั้นๆ หรือการถูกผู้ไม่หวังดี (Hacker) เข้ามาทำลายระบบ หรือการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ซึ่งหน่วยงานอาจถูกฟ้องร้องให้ต้องชำระค่าละเมิดลิขสิทธิ์ เป็นต้น มีเกณฑ์การประเมินดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	8 ครั้ง/ เดือนขึ้นไป
4	สูง	6-7 ครั้ง/ เดือน
3	ปานกลาง	4-5 ครั้ง/ เดือน
2	น้อย	2-3 ครั้ง/ เดือน
1	น้อยมาก	1 ครั้ง/ เดือน

ระดับความรุนแรงของผลกระทบของความเสี่ยง

ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

แผนการรองรับความเสี่ยง

ระดับคะแนน	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี	แผนการรองรับ
1 – 10	ต่ำ	ยอมรับความเสี่ยง	ขาว	- ติดตั้งระบบ Firewall /IPS/ Log
11 – 15	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง	- การจัดทำการบำรุงรักษาระบบ (MA) - การสำรองข้อมูลอย่างสม่ำเสมอ
16 – 20	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า	- แผนรองรับสถานการณ์ฉุกเฉิน
25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง	- การจัดหา Software ลิขสิทธิ์

(5) ความเสี่ยงด้านระบบข้อมูล คือความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศและการสื่อสารอันอาจจะก่อให้เกิดความเสียหาย เนื่องจากข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล เพื่อการโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ทำให้เกิดความเสียหาย ขาดความน่าเชื่อถือและสร้างความเสื่อมเสียแก่องค์กร มีเกณฑ์การประเมินดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	มากกว่า 5 ระบบขึ้นไป
4	สูง	4 ระบบ
3	ปานกลาง	3 ระบบ
2	น้อย	2 ระบบ
1	น้อยมาก	1 ระบบ

ระดับความรุนแรงของผลกระทบของความเสี่ยง

ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
4	สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
3	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
2	น้อย	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
1	น้อยมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

แผนการรองรับความเสี่ยง

ระดับคะแนน	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี	แผนการรองรับ
1 – 10	ต่ำ	ยอมรับความเสี่ยง	ขาว	- การตรวจสอบและแก้ไขปัญหาเบื้องต้น
11 – 15	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง	- การจัดทำการบำรุงรักษาระบบ (MA) - มีการตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test)
16 – 20	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า	- การกำหนดมาตรฐานความปลอดภัยในการพัฒนาระบบ
25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง	- การดำเนินการจัดหาระบบและอุปกรณ์ใหม่เพื่อทดแทน

(6) ความเสี่ยงด้านงบประมาณ คือความเสี่ยงต่อการได้รับงบประมาณสนับสนุนไม่เพียงพอ และการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา มีเกณฑ์การประเมินดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	ได้รับงบประมาณตามแผนน้อยกว่า 50%
4	สูง	ได้รับงบประมาณตามแผน ≥ 50%
3	ปานกลาง	ได้รับงบประมาณตามแผน ≥ 70%
2	น้อย	ได้รับงบประมาณตามแผน ≥ 90%
1	น้อยมาก	ได้รับงบประมาณตามแผน 100%

ระดับความรุนแรงของผลกระทบของความเสี่ยง

ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	ไม่สามารถดำเนินงานตามแผนและไม่บรรลุตามเป้าหมายที่กำหนดไว้
4	สูง	สามารถดำเนินงานตามแผนได้มากกว่าร้อยละ 40 ของแผน และไม่บรรลุตามเป้าหมายที่กำหนดไว้
3	ปานกลาง	สามารถดำเนินงานตามแผนได้มากกว่าร้อยละ 60 ของแผน แต่บรรลุตามเป้าหมายที่กำหนดไว้เพียงบางส่วน
2	น้อย	สามารถดำเนินงานตามแผนได้มากกว่าร้อยละ 80 ของแผนแต่ยังบรรลุตามเป้าหมายที่กำหนดไว้
1	น้อยมาก	สามารถดำเนินงานตามแผนและบรรลุตามเป้าหมายที่กำหนดไว้

แผนการรองรับความเสี่ยง

ระดับคะแนน	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี	แผนการรองรับ
1 – 10	ต่ำ	ยอมรับความเสี่ยง	ขาว	- การจัดประชุมภายในทบทวนการใช้จ่ายงบประมาณ
11 – 15	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง	- มีการกำกับติดตามการเบิกจ่ายงบประมาณ
16 – 20	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า	- มีแผนการบริหารจัดการงบประมาณให้ครอบคลุมทุกด้าน
25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง	- ของบประมาณสนับสนุนจากหน่วยงานภายนอก - สร้างความร่วมมือ เพื่อใช้ทรัพยากรร่วมกับหน่วยงานอื่น

(7) ความเสี่ยงในด้านการบริหารจัดการ คือความเสี่ยงเนื่องจากการบริหารที่ไม่รัดกุม ไม่มีแผนงานในการดำเนินงานที่ดี มีเกณฑ์การประเมินดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	ทุก 1 เดือน
4	สูง	ทุก 3 เดือน
3	ปานกลาง	ทุก 6 เดือน
2	น้อย	ทุก 9 เดือน
1	น้อยมาก	ทุก 1 ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง

ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	เกิดผลกระทบต่อกระบวนการ และการดำเนินงาน ของโครงการ/กิจกรรมที่วางแผนไว้ เกินกว่าร้อยละ 80 หรืออาจไม่สามารถดำเนินการได้สำเร็จ
4	สูง	เกิดผลกระทบต่อกระบวนการ และการดำเนินงาน ของโครงการ/กิจกรรมที่วางแผนไว้ เกินกว่าร้อยละ 50
3	ปานกลาง	เกิดผลกระทบต่อกระบวนการ และการดำเนินงาน ของโครงการ/กิจกรรมที่วางแผนไว้ เกินกว่าร้อยละ 30
2	น้อย	เกิดผลกระทบต่อกระบวนการ และการดำเนินงาน ของโครงการ/กิจกรรมที่วางแผนไว้ เกินกว่าร้อยละ 30
1	น้อยมาก	ไม่เกิดผลกระทบต่อกระบวนการ และการดำเนินงานในแต่ละกิจกรรม

แผนการรองรับความเสี่ยง

ระดับคะแนน	จัดระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	พื้นที่สี	แผนการรองรับ
1 – 10	ต่ำ	ยอมรับความเสี่ยง	ขาว	- การทบทวนแผนการบริหารจัดการอย่างสม่ำเสมอ
11 – 15	ปานกลาง	ยอมรับความเสี่ยง (มีมาตรการติดตาม)	เหลือง	- การติดตามการทำงาน ให้เป็นไปตามแผน
16 – 20	สูง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	ฟ้า	- การกำหนดแผนริหารงานที่มีประสิทธิภาพและรัดกุม
25	สูงมาก	ถ่ายโอนความเสี่ยง	แดง	- ปรับปรุง ระเบียบ แนวปฏิบัติ และนโยบายในการบริหารจัดการ ให้สอดคล้องกับทำงาน

2.4.2 ผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศในทุกด้าน ตามเกณฑ์การประเมินความเสี่ยงที่ได้กำหนดขึ้นโดยพิจารณาจาก ความถีหรือโอกาสที่เกิดขึ้น และความรุนแรงของผลกระทบ ทำให้ได้ผลลัพธ์ตามตารางด้านล่าง ดังนี้

รหัส	ชื่อความเสี่ยง	ประเภทความเสี่ยง	โอกาสที่เกิดขึ้น	ความรุนแรง	ระดับคะแนน
RIT01	ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	(1)	3	4	12
RIT02	ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	(2)	3	5	15
RIT03	ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	(2)	1	5	5
RIT04	ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	(2)	1	5	5
RIT05	ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	(2)	2	5	10
RIT06	ความเสี่ยงจากสถานการณ์โรคระบาดร้ายแรง	(2)	3	5	15
RIT07	ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	(3)	3	5	15
RIT08	ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	(3)	5	5	25
RIT09	ความเสี่ยงจากความชื้นและอุณภูมิในห้องแม่ข่าย	(3)	5	5	25
RIT010	ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี (Hacker)	(4)	3	5	15
RIT11	ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	(4)	3	5	15
RIT12	ความเสี่ยงจากการโจมตีเว็บไซต์	(4)	3	5	15
RIT13	ความเสียงในการให้บริการระบบ 1206	(5)	3	3	9

รหัส	ชื่อความเสี่ยง	ประเภทความเสี่ยง	โอกาสที่เกิดขึ้น	ความรุนแรง	ระดับคะแนน
RIT14	ความเสี่ยงจากชองโหว่จากการพัฒนาระบบงานภายในองค์กร	(5)	5	5	25
RIT15	ความเสี่ยงจากการใช้ระบบที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	(5)	5	5	25
RIT16	ความเสี่ยงต่อการได้รับงบประมาณสนับสนุนไม่เพียงพอ	(6)	4	4	16
RIT17	ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	(7)	4	4	16
RIT18	ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	(7)	3	4	12

2.4.3 การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ระดับความเสี่ยงที่ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท. ยอมรับได้คือ ความเสี่ยงที่อยู่ในระดับ ≤ 10 โดย สำนักงาน ก.พ.ร. และ สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ได้กำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูงตั้งแต่ 16 ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า 16 ถือว่ามีความเสี่ยงค่อนข้างต่ำ อาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้ ทั้งนี้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ประเมินความเสี่ยงโดยแบ่งตามระดับความเสี่ยง ได้ดังนี้

2.4.3.1 การวิเคราะห์และการจัดการความเสี่ยง แยกตามปัจจัยภายใน

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
ความเสี่ยงสูง มีค่าคะแนน ระหว่าง 16 -25							
RIT09 ความเสี่ยงจากความชื้นและอุณภูมิในห้องแม่ข่าย	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	- ขาดการตรวจสอบความชื้น และอุณหภูมิของห้องแม่ข่าย - การทำงานของเครื่องปรับอากาศมีปัญหา	- ระบบงานต่างๆไม่สามารถใช้งานได้ - สร้างความเสียหายต่อเครื่องแม่ข่าย - อาจเกิดความร้อนสูง และเกิดเหตุอัคคีภัยได้	ศทส.	25	- มีการควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม - ตรวจสอบการทำงานของเครื่องปรับอากาศอย่างสม่ำเสมอ	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)
RIT14 ความเสี่ยงจากช่องโหว่จากการพัฒนาระบบงานภายในองค์กร	ความเสี่ยงด้านระบบข้อมูล	- เกิดจากการทำงานผิดพลาดของอุปกรณ์และระบบงาน	- ลดความน่าเชื่อถือต่อหากข้อมูลถูกขโมยไปและนำไปเผยแพร่	ศทส.	25	- ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP- Top 10 Web Application Security Risks เพื่อลดความเสี่ยง	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
		- เกิดจากการพัฒนาระบบที่ไม่ได้มาตรฐานด้านความปลอดภัย - มีการเขียนโปรแกรมซ่อน Script ไว้เพื่อวัตถุประสงค์แอบแฝง	- กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อหน่วยงานเป็นอย่างยิ่ง - อาจเกิดการขโมยข้อมูล ที่มีชั้นความลับ หรือเป็นข้อมูลส่วนบุคคล			- มีการตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test)	
RIT15 ความเสี่ยงจากการใช้ระบบที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	ความเสี่ยงด้านระบบข้อมูล	- เสี่ยงต่อการถูกขโมยข้อมูล - เสี่ยงต่อการทำความเสียหายแก่โปรแกรม - ไม่สามารถแก้ไขข้อบกพร่องได้เอง - ขาดการดูแลบำรุงรักษาโปรแกรมและข้อมูล ทำให้ไม่สามารถใช้งานได้ใน	- ลดความน่าเชื่อถือต่อ สนข. หากข้อมูลถูกขโมยไปและนำไปเผยแพร่ - กรณีที่เป็นข้อมูลลับอาจสร้างความเสียหายต่อสำนักงานฯ เป็นอย่างยิ่ง - จัดหางบประมาณเพื่อทำการบำรุงรักษาโปรแกรมและข้อมูลพร้อมกับการทำการ	ศทส.	25	- การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level 2 - การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล (ER Diagram) - ให้มีการส่งมอบ Source Code รวมถึง Library ที่มีการพัฒนาขึ้นเอง ในรูปแบบ Flash Drive ในฟอร์แมตที่ไม่เข้ารหัสใดๆ และ	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
		ระยะยาว - เสียค่าใช้จ่ายสูง	บำรุงรักษาเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้องที่ต้องมีการอัพเดทอยู่เสมอ			สามารถปรับปรุงแก้ไขได้ - มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม - มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) - การอัพเดท เมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหาย เป็นต้น	
RIT16 ความเสี่ยงต่อการได้รับงบประมาณ	ความเสี่ยงด้านงบประมาณ	- ได้รับการจัดสรรงบประมาณไม่เพียงพอต่อการดำเนินงานขับเคลื่อน	- การขับเคลื่อนโครงการตามแผนแม่บท ไม่สามารถดำเนินการได้ตามแผน	ศทส.	16	- จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ เพื่อแสดงความจำเป็นในการขอสนับสนุนงบประมาณใน	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
สนับสนุนไม่เพียงพอ		โครงการตามแผนฯ และในเวลาที่เหมาะสม - งบประมาณที่ได้รับอนุมัติให้ดำเนินงานไม่ต่อเนื่อง	- ระบบงานต่างๆ ไม่สามารถให้บริการได้ต่อเนื่อง			การดำเนินการด้านเทคโนโลยีสารสนเทศ - สร้างความร่วมมือระหว่างหน่วยงาน เพื่อใช้ทรัพยากรร่วมกัน - ขอสนับสนุนงบประมาณ จากหน่วยงานภายนอก	
RIT17 ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	ความเสี่ยงด้านการบริหารจัดการ	- การขาดแคลนบุคลากรด้านสารสนเทศ ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ - จำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่	- การพัฒนาและควบคุมดูแลระบบขาดประสิทธิภาพ	ศทส.	16	**สำหรับส่วนกลาง** - ปรับปรุงโครงสร้างศูนย์สารสนเทศ และสรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสม - จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากร	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
		เพิ่มขึ้นตามความต้องการของผู้ใช้งาน				ผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ **สำหรับส่วนภูมิภาค** - มีการเพิ่มอัตรากำลัง และสรรหาบุคลากรด้านเทคโนโลยีสารสนเทศเพื่อสนับสนุนงานตามภารกิจ	
ความเสี่ยงปานกลาง มีค่าคะแนน ระหว่าง 11 - 15							
RIT01 ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	ความเสี่ยงด้านบุคลากร	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ - การอำพรางหรือสวมรอยผู้ใช้	- การเข้าถึงระบบเครือข่ายภายในจากบุคคลภายนอก - ข้อมูลส่วนบุคลลหรือข้อมูลที่เป็นความลับรั่วไหลสู่ภายนอก	ผู้ใช้งานระบบ	12	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - การจัดทำระบบการยืนยันตัวตนผู้ใช้งาน ที่สามารถระบุตัวบุคคลที่ชัดเจน	ยอมรับความเสี่ยง (มีมาตรการติดตาม)

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
		- การเข้าถึงข้อมูล/เปลี่ยนแปลงข้อมูล โดยไม่ได้รับอนุญาต				- มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ	
RIT07 ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้องไม่สามารถทำงานได้ตามปกติ	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	- เครื่องคอมพิวเตอร์หรืออุปกรณ์ชำรุดขัดข้องด้วยสาเหตุทางเทคนิค - เนื่องจากมีสัตว์กัดแทะ เช่น หนูหรือแมลง เป็นต้น	- อุปกรณ์ต่างๆได้รับความเสียหาย - ระบบไม่สามารถใช้งานได้ - เสียงบประมาณในการซ่อมแซมหรือจัดหาทดแทน	ศทส. และทุกสำนัก/กอง/ศูนย์	15	- ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack - มีการบำรุงรักษา และทดสอบการทำงานของเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ - ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง - การให้ความสำคัญกับการทำ 5 ส ภายในองค์กร อย่างสม่ำเสมอ	ยอมรับความเสี่ยง (มีมาตรการติดตาม)

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
RIT11 ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	- ผู้ใช้งาน Download ซอฟท์แวร์ที่มีลิขสิทธิ์มาใช้งาน โดยไม่ได้รับอนุญาต - ผู้ใช้งานขาดความตระหนักรู้เรื่องของข้อกฎหมายและความมั่นคงปลอดภัยทางคอมพิวเตอร์ - การใช้งานด้วยซอฟต์แวร์ฟรี อาจไม่สามารถตอบสนองต่อความต้องการใช้งาน	- อาจถูกฟ้องร้องเรียกค่าเสียหายจากผู้เป็นเจ้าของลิขสิทธิ์นั้นๆ - อาจเกิดความเสียหายต่อชื่อเสียงและความน่าเชื่อถือขององค์กร - อาจเกิดช่องโหว่ที่ทำให้ข้อมูลรั่วไหลได้	ศทส.	15	- การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็	ยอมรับความเสี่ยง (มีมาตรการติดตาม)
RIT18 ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	ความเสี่ยงด้านการบริหารจัดการ	- การเปลี่ยนแปลงผู้บริหาร อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลง	- การดำเนินโครงการต่างๆ ไม่บรรลุผลสำเร็จตามระยะเวลาที่กำหนด	ทุกสำนัก/กอง/ศูนย์	12	- ติดตามและวิเคราะห์นโยบายของผู้บริหาร	ยอมรับความเสี่ยง (มีมาตรการติดตาม)

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
		ด้วย ทำให้การดำเนินการโครงการต่างๆได้รับผลกระทบ - จากกระบวนการภายในที่ไม่เป็นระบบและไม่มีประสิทธิภาพ	- การดำเนินโครงการไม่เป็นไปตามแผนที่ได้กำหนดไว้ - ผลสัมฤทธิ์ของโครงการขาดประสิทธิภาพ			- จัดทำแผนสำรองการบริหารจัดการหรือดำเนินโครงการ เพื่อให้บรรลุเป้าหมาย	
ความเสี่ยงต่ำ มีค่าคะแนน ระหว่าง 1 - 10							
RIT13 ความเสี่ยงในการให้บริการระบบ 1206	ความเสี่ยงด้านระบบข้อมูล	- อุปกรณ์ขาดการบำรุงรักษาอย่างต่อเนื่อง - การให้บริการหยุดชะงัก - ความไม่แน่นอนของภารกิจหน่วยงาน	- ระบบไม่สามารถให้บริการได้อย่างต่อเนื่อง - ไม่มีเครื่องมือในการบริหารจัดการ - ไม่สามารถดำเนินงานตามภารกิจที่ได้รับมอบหมายได้อย่างเต็มประสิทธิภาพ	ศทส.	9	- การของบประมาณในการบำรุงรักษาอย่างต่อเนื่อง	ยอมรับความเสี่ยง

2.4.3.2 การวิเคราะห์และการจัดการความเสี่ยง แยกตามปัจจัยภายนอก

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
ความเสี่ยงสูง มีค่าคะแนน ระหว่าง 16 - 25							
RIT08 ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศและการสื่อสาร	- โปรแกรมหรือข้อมูลถูกทำลาย - ไม่สามารถเรียกใช้โปรแกรมหรือระบบงานได้ตามปกติ - การถูกขโมยข้อมูล	- เครื่องคอมพิวเตอร์และระบบงานต่างๆ ไม่สามารถใช้งานได้ - ข้อมูลที่สำคัญสูญหาย	ศทส.	25	- ตรวจสอบการตั้งค่าของ Firewall, IPS และ Log อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุง - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - การติดตั้ง Anti-Virus บนเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
ความเสี่ยงปานกลาง มีค่าคะแนน ระหว่าง 11 - 15							
RIT02 ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- ไม่สามารถใช้งานเครื่องแม่ข่าย และเครือข่ายได้ - ความเสี่ยงต่อการ Crash ของเครื่องแม่ข่าย ทั้งส่วนระบบปฏิบัติการ (Operating System) ระบบฐานข้อมูล (RDBMS) อันเนื่องมาจากเครื่องไม่ได้ถูกทำการ Shutdown อย่างเหมาะสม	- ข้อมูลเสียหาย - ระบบปฏิบัติการ โปรแกรม หรือฐานข้อมูลเสียหาย ต้องมีการติดตั้งใหม่	ศทส.	15	- จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)	ยอมรับความเสี่ยง (มีมาตรการติดตาม)
RIT06 ความเสี่ยงจากสถานการณ์โรคระบาดร้ายแรง	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การเกิดสถานการณ์โรคระบาดร้ายแรง จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- ผู้ปฏิบัติงานไม่สามารถเข้าปฏิบัติงานในพื้นที่ได้	ศทส.	15	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)	ยอมรับความเสี่ยง (มีมาตรการติดตาม)

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
						- จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้	
RIT10 ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี (Hacker)	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	- การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- ทำให้ระบบเครื่องแม่ข่ายหรือลูกข่ายติดไวรัสและแพร่กระจายสู่เครื่องอื่นๆ ทั้งหมดในเครือข่าย - ถูกโจรกรรมข้อมูลที่เป็นความลับ	ศทส.	15	- ตรวจสอบการตั้งค่าของ Firewall อย่างสม่ำเสมอ - ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย - มีการตรวจสอบช่องโหว่ (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Test)	ยอมรับความเสี่ยง (มีมาตรการติดตาม)

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
RIT12 ความเสี่ยงจากการโจมตีเว็บไซต์	ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์	- การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งข้อมูลคำสั่งเจตนาร้าย การติดไวรัสหรือเวิร์ม	- ถูกแก้ไขหรือปลี่ยนแปลงข้อมูล หรือ รูปภาพบน Web Site ของสำนักงาน - ถูกโจรกรรมข้อมูลที่เป็นความลับ	ศทส.	15	- ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย - มีการตรวจสอบช่องโหว่ (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Test)	ยอมรับความเสี่ยง (มีมาตรการติดตาม)
ความเสี่ยงต่ำ มีค่าคะแนน ระหว่าง 1 - 10							
RIT03 ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การเกิดไฟไหม้อาคาร แผ่นดินไหวจนอาคารถล่ม ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และ	- เสียงบประมาณในการจัดหาระบบทดแทน - การไม่สามารถใช้งานระบบระหว่างที่มีการจัดหาระบบทดแทน	ศทส.	5	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง - ติดตั้งระบบตรวจจับควันแจ้งเตือนไฟไหม้ระบบดับเพลิง	ยอมรับความเสี่ยง

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
		อุปกรณ์ต่างๆได้ ทำให้ได้รับความเสียหายทั้งหมด - การบาดเจ็บหรือเสียชีวิตของเจ้าหน้าที่หรือลูกจ้างภายในอาคาร	- ระบบคอมพิวเตอร์และเครือข่ายถูกทำลาย			- มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	

ความเสี่ยง	ประเภทความเสี่ยง	ปัจจัยความเสี่ยง	ผลกระทบที่อาจเกิดขึ้น	ผู้รับผิดชอบ	ค่าคะแนนความเสี่ยง	แนวทางการควบคุม	วิธีจัดการความเสี่ยง
RIT04 ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนภายในเครื่อง เช่น CPU และ Ram ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	- เสียงบประมาณในการจัดหาเครื่องแม่ข่ายทดแทนที่มีมูลค่าสูง - เสียเวลาในการกู้ระบบ - เสียภาพลักษณ์ของสำนักงาน	ศทส.	5	- ตรวจสอบระบบการป้องกันรักษาความปลอดภัย - การตรวจสอบการเข้าออกของบุคคลภายนอก - ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ ที่มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	ยอมรับความเสี่ยง
RIT05 ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม	- การเกิดสถานการณ์ความรุนแรง หรือความไม่สงบเรียบร้อย จนทำให้บุคลากรไม่สามารถปฏิบัติงานได้ตามปกติ	- ผู้ปฏิบัติงานไม่สามารถเข้าปฏิบัติงานในพื้นที่ได้ - อุปกรณ์และข้อมูลอาจจะเกิดความเสียหาย จากการถูกทำลายด้วยวิธีการต่างๆ	ศทส.	10	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้	ยอมรับความเสี่ยง

ความเสี่ยงด้านสถานที่ตั้งของสำนักงาน ป.ป.ท.

หน่วยงาน	ที่อยู่	ชั้น	สถานะอาคาร	วิธีเดินทาง	ระยะเวลาเดินทาง	ที่วางตู้ RACK	จำนวนตู้ RACK	ระบบ Intranet/Internet	ความเสี่ยง/อุปสรรค	ความเหมาะสมในการตั้ง DR Site (5 คะแนน)
สำนักงาน ป.ป.ท. ส่วนกลาง	99 หมู่ 4 อาคาร ซอฟต์แวร์ปาร์ค ถ.แจ้งวัฒนะ อ.ปากเกร็ด จ.นนทบุรี 11120	8	อาคารเช่า	-	-	ชั้น 2	15 U จำนวน 2 ตู้	GIN/MPLS	-	-
						ชั้น 12 A	Data Center			
						ชั้น 14	27 U			
						ชั้น 23	42 U			
						ชั้น 28	15 U			
						ชั้น 30	15 U จำนวน 2 ตู้			
						ชั้น 31	42 U			
						ชั้น 38	15 U			
สำนักงาน ป.ป.ท. เขตพื้นที่ 1	22/25 ถ.นเรศวร ต.ประตูชัย อ.พระนครศรีอยุธยา จ.พระนครศรีอยุธยา 13000	4	อาคารเช่า	รถยนต์	1 ชั่วโมง	ชั้น 1 ชั้น 2	15 U 42 U	GIN/ADSL/FFTX	- การติดต่อประสานงานมีความยากลำบาก - มีแผนการย้ายสำนักงานในอนาคต	3

หน่วยงาน	ที่อยู่	ชั้น	สถานะอาคาร	วิธีเดินทาง	ระยะเวลาเดินทาง	ที่วางตู้ RACK	จำนวนตู้ RACK	ระบบ Intranet/Internet	ความเสี่ยง/อุปสรรค	ความเหมาะสมในการตั้ง DR Site (5 คะแนน)
สำนักงาน ป.ป.ท. เขตพื้นที่ 2	เลขที่ 99/88 หมู่ 3 ถ.สุขุมวิท ต.เสม็ด อ.เมือง จ.ชลบุรี 20000	1	อาคารเช่า	รถยนต์	2 ชั่วโมง	ชั้น 2	42 U	GIN/ADSL/FFTX	- พื้นที่สำนักงานมีขนาดเล็ก - มีแผนในการสร้างและย้ายสถานที่ตั้งสำนักงานในอนาคต	2
สำนักงาน ป.ป.ท. เขตพื้นที่ 3	บริษัท ทีโอที จำกัด (มหาชน) เลขที่ 118 หมู่ 10 ถ.มิตรภาพ ต.โคกกรวด อ.เมือง จ.นครราชสีมา 30280	2	อาคารเช่า	รถยนต์	3 ชั่วโมง	ชั้น 1 ชั้น 2	15 U 42 U	GIN/ADSL/FFTX	- สถานที่กว้างขวางและเป็นอาคารของภาครัฐ - ยังไม่มีแผนในการย้ายสำนักงาน	5
สำนักงาน ป.ป.ท. เขตพื้นที่ 4	อาคารปริ๊นซ์ ออฟ ฟิตเฟล็กค์ เลขที่ 4/33 ถ.หน้าเมือง ต.ในเมือง อ.เมือง จ.ขอนแก่น 40000	2	อาคารเช่า	เครื่องบิน	4 ชั่วโมง	ชั้น 2 ชั้น 2	15 U 42 U	GIN/ADSL/FFTX	- การติดต่อประสานงานไม่เอื้ออำนวย - มีแผนการย้ายที่ตั้งสำนักงานในอนาคต	2

หน่วยงาน	ที่อยู่	ชั้น	สถานะอาคาร	วิธีเดินทาง	ระยะเวลาเดินทาง	ที่วางตู้ RACK	จำนวนตู้ RACK	ระบบ Intranet/Internet	ความเสี่ยง/อุปสรรค	ความเหมาะสมในการตั้ง DR Site (5 คะแนน)
สำนักงาน ป.ป.ท. เขตพื้นที่ 5	อาคารแอร์พอร์ต บิสซิเนส พาร์ค เลขที่ 92/1 ถ.มหิดล ต.หายยา อ.เมือง จ.เชียงใหม่ 50100	1	อาคารเช่า	เครื่องบิน	4 ชั่วโมง	ชั้น 1	15 U / 42 U	GIN/ADSL/FFTX	อยู่ระหว่างการตั้งอาคารเป็นของตัวเอง คาดว่าแล้วเสร็จปีงบประมาณ พ.ศ. 2564	5 (กรณีย้ายสถานที่ตังสำนักงานแล้ว)
สำนักงาน ป.ป.ท. เขตพื้นที่ 6	เลขที่ 723/13-17 ถ.พิชัยสงคราม ต.ในเมือง อ.เมือง จ.พิษณุโลก 65000	4	อาคารเช่า	เครื่องบิน	4 ชั่วโมง	ชั้น 2	15 U / 42 U	GIN/ADSL/FFTX	- อยู่ระหว่างการเจรจาขอซื้ออาคารเพื่อสร้างเป็นอาคารสำนักงาน - ระบบไฟฟ้าไม่เสถียรเท่าที่ควร	4
สำนักงาน ป.ป.ท. เขตพื้นที่ 7	เลขที่ 445/2 ถ.เทศา ถ.พระประโทน อ.เมือง จ.นครปฐม 73000	3	อาคารเช่า	รถยนต์	1 ชั่วโมง	ชั้น 1 ชั้น 3	15 U 42 U	GIN/ADSL/FFTX	- การติดต่อประสานงานค่อนข้างยาก - สถานที่คับแคบ - มีแผนการย้ายสถานที่ในอนาคต	3

หน่วยงาน	ที่อยู่	ชั้น	สถานะอาคาร	วิธีเดินทาง	ระยะเวลาเดินทาง	ที่วางตู้ RACK	จำนวนตู้ RACK	ระบบ Intranet/Internet	ความเสี่ยง/อุปสรรค	ความเหมาะสมในการตั้ง DR Site (5 คะแนน)
สำนักงาน ป.ป.ท. เขตพื้นที่ 8	เลขที่ 91/1 หมู่ที่ 1 อาคารซี.พี.ทาวเวอร์ ชั้น 2 ถ.กาญจนวิถี ต.นางกุ้ง อ.เมือง จ.สุราษฎร์ธานี 84000	1	อาคารเช่า	เครื่องบิน 4 ชั่วโมง		ชั้น 2	15 U / 42 U	GIN/ADSL/FFTX	- การติดต่อประสานงานค่อนข้างยาก - สถานที่คับแคบ - มีแผนการย้ายสถานที่ในอนาคต	3
สำนักงาน ป.ป.ท. เขตพื้นที่ 9	เลขที่ 116 ถ.เพชรเกษม หมู่ที่ ๒ ต.ควนลัง อ.หาดใหญ่ จ.สงขลา 90110	4	อาคารเช่า	เครื่องบิน	4 ชั่วโมง	ชั้น 1	42 U	GIN/ADSL/FFTX	- สถานที่ตั้งระบบเครือข่ายอยู่ชั้น 1 - มีแผนการย้ายสถานที่ตั้งในอนาคต	3

2.4.4 การวางแผนบริหารความเสี่ยง

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท. ได้ดำเนินการวางแผนบริหารความเสี่ยง โดยดำเนินการดังนี้

2.4.4.1 มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกัน หรือลดการเกิดความเสียหายในรูปแบบต่างๆ ด้วยการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

2.4.4.2 มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน หรือภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ (IT Contingency Plan)

2.4.4.3 มีการตรวจสอบควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหาย

2.4.4.4 มีระบบการรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล เช่น ระบบ Antivirus ระบบไฟฟ้าสำรอง, ระบบ Firewall, ระบบ Backup และระบบคอมพิวเตอร์เพื่อรองรับ พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เป็นต้น

2.4.4.5 มีการกำหนดสิทธิ์ให้ผู้ใช้ในแต่ละระดับ (Access Rights)

2.4.4.6 มีการบันทึกเพื่อตรวจสอบ (Audit Logs) เช่น ให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก โดยการบันทึกการเข้าออกระบบ (Login-Logout Log)

2.4.5 การกำหนดแบ่งอำนาจหน้าที่ผู้รับผิดชอบ

การกำหนดแบ่งอำนาจหน้าที่ มีวัตถุประสงค์เพื่อลดความเสี่ยงด้านโครงสร้างพื้นฐาน ซึ่งมีแนวทางปฏิบัติดังนี้ คือ ต้องแบ่งแยกบุคลากรที่ปฏิบัติหน้าที่ ในส่วนการพัฒนาระบบงานออกจากบุคลากรที่ทำหน้าที่บริหารระบบ ซึ่งปฏิบัติงานอยู่ในส่วนระบบคอมพิวเตอร์ที่ใช้งานจริงและต้องจัดให้มีการระบุหน้าที่ความรับผิดชอบของแต่ละหน้าที่งาน และความรับผิดชอบของบุคลากรแต่ละคนภายในฝ่ายคอมพิวเตอร์อย่างชัดเจนเป็นลายลักษณ์อักษร ซึ่งควรจัดให้มีบุคลากรสำรองในงานที่มีความสำคัญ เพื่อให้สามารถทำงานทดแทนกันได้ในกรณีจำเป็น โดยกำหนดหน้าที่ ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

(1) ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

นายภูมิวิศาล เกษมศุข	รองเลขาธิการคณะกรรมการ ป.ป.ท.
	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม สำนักงาน ป.ป.ท.
นายจิรวัฒน์ สุภาพ	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(2) ระดับปฏิบัติการ

2.1 รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผู้รับผิดชอบ ได้แก่

นายมรุต อาภาอดุล นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ

นายนักสิทธิ์ อิ่งสกุล นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ

2.2 รับผิดชอบดูแลบำรุงรักษา ระบบเครื่อง ระบบเครือข่ายและการสำเนาฐานข้อมูล ผู้รับผิดชอบ ได้แก่

นายพชฎ ศริพันธุ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

นายวิกร แก้วกำไร นักวิชาการคอมพิวเตอร์ปฏิบัติการ

มีหน้าที่รับผิดชอบ ดังนี้

2.2.1 ควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์ตามการกำหนดสิทธิ์การเข้าถึงห้องควบคุมระบบคอมพิวเตอร์

2.2.2 ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ เครื่องคอมพิวเตอร์แม่ข่าย (Server Computer) และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมด

2.2.3 ควบคุม ติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

2.2.4 ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

2.2.5 ป้องกันการถูกเจาะระบบ และ แก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2.2.6 ดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก

2.3 รับผิดชอบในการรักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล ผู้รับผิดชอบ ได้แก่

นางสาวณัฐกฤตา วงษ์สายตา นักวิชาการคอมพิวเตอร์ชำนาญการ

นายวิกร แก้วกำไร นักวิชาการคอมพิวเตอร์ปฏิบัติการ

นายอานันท์ มากบัวแก้ว นักวิชาการคอมพิวเตอร์ปฏิบัติการ

มีหน้าที่รับผิดชอบ ดังนี้

2.3.1. ทำการสำรองข้อมูลและเรียกคืนข้อมูลของระบบฐานข้อมูลสารสนเทศ (Backup and Recovery)

2.3.2. ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

2.4 รับผิดชอบในการรักษาความปลอดภัย ระบบอินเตอร์เน็ต ผู้รับผิดชอบ ได้แก่

นายพชฎ ศริพันธุ์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

มีหน้าที่รับผิดชอบ ดังนี้

ควบคุมการใช้งานของผู้ใช้งานระบบอินเตอร์เน็ต ของสำนักงาน ป.ป.ท. รวมถึงบุคคลภายนอกที่เข้ามาขอใช้งาน

2.5 รับผิดชอบความปลอดภัยทั่วไป ผู้รับผิดชอบ ได้แก่

นางสาวพรทิพย์ อยู่สุข นักจัดการงานทั่วไปชำนาญการ

มีหน้าที่รับผิดชอบ ดังนี้

ติดต่อประสานงานกับทางฝ่ายอาคาร สถานที่ หากเกิดเหตุการณ์ต่าง ๆ อาทิ เช่น ไฟฟ้าดับ สถานการณ์ทางการเมือง

2.5 แผนการดำเนินงานการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ชื่อความเสี่ยง	แผนการดำเนินงาน	ระยะเวลา
ความเสี่ยงในการเข้าถึงข้อมูลของบุคคลอื่น	- สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ - การจัดทำระบบการยืนยันตัวตนผู้ใช้งานที่สามารถระบุตัวบุคคลที่ชัดเจน - มีมาตรการกำหนดชั้นความลับของข้อมูลและการเข้าถึงข้อมูลที่เป็นความลับ	- อยู่ระหว่างดำเนินการ - ทุกครั้งที่มีการเข้าใช้งานระบบ - อยู่ระหว่างดำเนินการ
ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	- จัดหาเครื่องสำรองไฟฟ้าแบบป้องกันปัญหาแรงดันไฟฟ้าไม่คงที่ - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)	- อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ
ความเสี่ยงจากการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง - ติดตั้งระบบตรวจจับควัน แจ้งเตือนไฟไหม้ระบบดับเพลิง - มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ - จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP)	- ทุกวัน - ทุกวัน - อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ

ชื่อความเสี่ยง	แผนการดำเนินงาน	ระยะเวลา
	- จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	- อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ
ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	- ตรวจสอบระบบการป้องกันรักษาความปลอดภัย - การตรวจสอบการเข้าออกของบุคคลภายนอก - ติดตั้งกล้องวงจรปิดให้ครอบคลุมทุกที่ ที่มีเครื่องคอมพิวเตอร์และอุปกรณ์ติดตั้งอยู่	- ทุกวัน - ทุกวัน - อยู่ระหว่างดำเนินการ
ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้	- อยู่ระหว่างดำเนินการตรวจสอบ - อยู่ระหว่างดำเนินการ
ความเสี่ยงจากเครื่องคอมพิวเตอร์หรืออุปกรณ์ขัดข้อง ไม่สามารถทำงานได้ตามปกติ	- ไม่ปล่อยให้มีสายไฟฟ้าหรือสายสัญญาณไม่มีท่อห่อหุ้มจนถึงจุดทางเข้าตู้ Rack - มีการบำรุงรักษา และทดสอบการทำงานของเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ - ไม่นำอาหารหรือเครื่องดื่มมาทานหรือเก็บไว้ในบริเวณที่มีความเสี่ยง - การให้ความสำคัญกับการทำ 5 ส ภายในองค์กร อย่างสม่ำเสมอ	- อยู่ระหว่างดำเนินการ - ทุกวัน - ทุกวัน - ทุกวัน
ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์หรือ Malware	- ตรวจสอบการตั้งค่าของ Firewall, IPS และ Log อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุง - ตรวจสอบการทำงานโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ	- ทุกวัน - ทุกวัน - ทุกวัน

ชื่อความเสี่ยง	แผนการดำเนินงาน	ระยะเวลา
	- ตรวจสอบระบบ Anti-Virus บนเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย	- ทุกวัน
ความเสี่ยงจากความชื้นและอุณภูมิในห้องแม่ข่าย	- ตรวจสอบสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม - ตรวจสอบการทำงานของเครื่องปรับอากาศอย่างสม่ำเสมอ	- ทุกวัน - ทุกวัน
ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี (Hacker)	- ตรวจสอบการตั้งค่าของ Firewall อย่างสม่ำเสมอ - ตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ตรวจสอบ Policy และ Log ของระบบป้องกันการบุกรุกระบบเครือข่าย - ตรวจสอบช่องโหว่ (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Test)	- ทุกวัน - ทุกวัน - ทุกวัน - ทุกวัน
ความเสี่ยงจากการใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์	- การจัดหาซอฟต์แวร์ที่ถูกกฎหมายมาใช้งานตามความจำเป็น	- อยู่ระหว่างดำเนินการ
ความเสียงในการให้บริการระบบ 1206	- การของบประมาณในการบำรุงรักษาอย่างต่อเนื่อง	- อยู่ระหว่างดำเนินการ
ความเสี่ยงจากชองโหว่จากการพัฒนาระบบงานภายในองค์กร	- ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP- Top 10 Web Application Security Risks เพื่อลดความเสี่ยง - มีการตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test)	- อยู่ระหว่างดำเนินการ - ทุกวัน

ชื่อความเสี่ยง	แผนการดำเนินงาน	ระยะเวลา
ความเสี่ยงจากการใช้ระบบที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง	- การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level 2 - การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล (ER Diagram) - ให้มีการส่งมอบ Source Code รวมถึง Library ที่มีการพัฒนาขึ้นเอง ในรูปแบบ Flash Drive ในฟอร์แมตที่ไม่เข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้ - มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม - มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug) - การอัพเดท เมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหาย เป็นต้น	- อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ
ความเสี่ยงต่อการได้รับงบประมาณสนับสนุน ไม่เพียงพอ	- จัดทำแผนแม่บทเทคโนโลยีสารสนเทศเพื่อแสดงความจำเป็นในการขอสนับสนุนงบประมาณในการดำเนินการด้านเทคโนโลยีสารสนเทศ - สร้างความร่วมมือระหว่างหน่วยงานเพื่อใช้ทรัพยากรร่วมกัน - ขอสนับสนุนงบประมาณ จากหน่วยงานภายนอก	- อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ
ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน	สำหรับส่วนกลาง - ปรับปรุงโครงสร้างศูนย์สารสนเทศ และสรรหาบุคลากรเพื่อรองรับงานอย่างเหมาะสม	- อยู่ระหว่างดำเนินการ

ชื่อความเสี่ยง	แผนการดำเนินงาน	ระยะเวลา
	- จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้ สำหรับส่วนภูมิภาค - มีการเพิ่มอัตรากำลัง และสรรหาบุคลากรด้านเทคโนโลยีสารสนเทศ เพื่อสนับสนุนงานตามภารกิจ	- อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ
ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	- ติดตามและวิเคราะห์นโยบายของผู้บริหาร - จัดทำแผนสำรองการบริหารจัดการหรือดำเนินโครงการ เพื่อให้บรรลุเป้าหมาย	- อยู่ระหว่างดำเนินการ - อยู่ระหว่างดำเนินการ

บทที่ 3 สรุปและข้อเสนอแนะ

การจัดการความเสี่ยง (Risk Management) คือ กระบวนการในการระบุ วิเคราะห์ ประเมิน ดูแลตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่ และกระบวนการทำงานเพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่ง เมื่อเทคโนโลยีสารสนเทศก้าวเข้ามามีบทบาทสำคัญในฐานะกลไกอันทรงพลังในการขับเคลื่อน การดำเนินงานขององค์กร ทุกกิจกรรมที่เกิดขึ้นภายในองค์กรจึงล้วนมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศแทบทั้งสิ้นในแต่ละวันข้อมูลมหาศาลถูกส่งผ่านเครือข่ายเทคโนโลยีสารสนเทศเพื่ออานวยความสะดวกให้แก่ผู้ปฏิบัติงานของทุกหน่วยงานภายในสำนักงาน ป.ป.ท. ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหาย และถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือการจัดการความเสี่ยงในองค์กร นั่นเอง

3.1 การวิเคราะห์ปัจจัยเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

การระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงด้านต่างๆ ที่องค์กรเผชิญอยู่จากการกำหนดแนวทางปฏิบัติเพื่อควบคุมความเสี่ยงที่มีผลคะแนนสูงสุด 6 อันดับแรก ได้ข้อสรุปดังนี้

3.1.1 ความเสี่ยงจากการติดไวรัสคอมพิวเตอร์ หรือ Malware มีแนวทางปฏิบัติดังนี้

- ตรวจสอบการตั้งค่าของ Firewall, IPS และ Log อย่างสม่ำเสมอ
- บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุง
- ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ
- การติดตั้ง Anti-Virus บนเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่าย

3.1.2 ความเสี่ยงจากความชื้นและอุณภูมิในห้องแม่ข่าย มีแนวทางปฏิบัติดังนี้

- มีการควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม
- ตรวจสอบการทำงานของเครื่องปรับอากาศอย่างสม่ำเสมอ

3.1.3 ความเสี่ยงจากช่องโหว่จากการพัฒนาระบบงานภายในองค์กร มีแนวทางปฏิบัติดังนี้

- ตั้งมาตรฐานในการพัฒนาซอฟต์แวร์ตามคำแนะนำของ OWASP- Top 10 Web Application Security Risks เพื่อลดความเสี่ยง
- มีการตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Test)

3.1.4 ความเสี่ยงจากการใช้ระบบที่พัฒนาโดยผู้รับจ้างภายนอก (Outsource) และการขาดแผนบริหารความต่อเนื่อง มีแนวทางปฏิบัติดังนี้

- การออกแบบระบบให้อิงมาตรฐาน Data Flow Diagram (DFD) Level 2
- การออกแบบอ้างอิงแผนผังความสัมพันธ์ระหว่างกลุ่มข้อมูล (ER Diagram)
- ให้มีการส่งมอบ Source Code รวมถึง Library ที่มีการพัฒนาขึ้นเอง ในรูปแบบ Flash Drive ในฟอร์แมตที่ไม่เข้ารหัสใดๆ และสามารถปรับปรุงแก้ไขได้
- มีมาตรการในการกำหนดให้นำข้อมูลใดออกไปนอกสถานที่ได้ให้ชัดเจนและมีการควบคุมอย่างรัดกุม
- มีแผนการบำรุงรักษาระบบงานที่ดี รวมถึงการแก้ไขข้อผิดพลาดในการเขียนโปรแกรม (Bug)
- การอัพเดท เมื่อมี Version หรือ Release ใหม่ การแก้ไขเมื่อเกิดการ Crash ของโปรแกรมหรือฐานข้อมูล (Database) เกิดความเสียหาย เป็นต้น

3.1.5 ความเสี่ยงต่อการได้รับงบประมาณสนับสนุนไม่เพียงพอ มีแนวทางปฏิบัติดังนี้

- จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ เพื่อแสดงความจำเป็นในการขอสนับสนุนงบประมาณในการดำเนินการด้านเทคโนโลยีสารสนเทศ
- สร้างความร่วมมือระหว่างหน่วยงาน เพื่อใช้ทรัพยากรร่วมกัน
- ขอสนับสนุนงบประมาณ จากหน่วยงานภายนอก

3.1.6 ความเสี่ยงจากการขาดแคลนบุคลากรผู้ปฏิบัติงาน มีแนวทางปฏิบัติดังนี้

สำหรับส่วนกลาง

- ปรับปรุงโครงสร้างศูนย์สารสนเทศ และสรรหาบุคลากรเพื่อรองรับปริมาณงานอย่างเหมาะสม
- จัดทำคู่มือกระบวนการทำงานเพื่อให้บุคลากรอื่นสามารถปฏิบัติตามคู่มือได้กรณีที่บุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้

สำหรับส่วนภูมิภาค

- มีการเพิ่มอัตรากำลัง และสรรหาบุคลากรด้านเทคโนโลยีสารสนเทศ เพื่อสนับสนุนงานตามภารกิจ

3.2 สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเพื่อวัตถุประสงค์ดังนี้

3.2.1 เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ

3.2.2 เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

3.2.3 ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

3.3 ข้อเสนอแนะ

3.3.1 การควบคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้น โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

3.3.1.1 พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน

3.3.1.2 พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น

3.3.1.3 กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

3.3.2 การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพ และมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ

3.3.3 การสนับสนุนงบประมาณในการบำรุงรักษา เนื่องจากในช่วงที่ผ่านมา (2557 ถึงปัจจุบัน) สำนักงาน ป.ป.ท. ได้มีการพัฒนาระบบสารสนเทศที่เพิ่มขึ้น ทั้งในส่วนของ Hardware และ Software ซึ่งมีมูลค่าการลงทุนในแต่ละอุปกรณ์สูง แต่ในส่วนของการบำรุงรักษาจะได้รับการจัดสรรเพียงปีละ 2,000,000.-บาท (สองล้านบาทถ้วน) ทำให้ต้องเลือกบำรุงรักษาอุปกรณ์ที่สำคัญบางส่วน โดยที่เหลือจะไม่สามารถบำรุงรักษาได้ และหากเกิดการเสียหายขึ้นมาก็จะมีค่าดูแลที่สูงขึ้น เนื่องจากปัจจุบันการบำรุงรักษาจะถูกคิดราคาในแบบการบำรุงรักษาย้อนหลัง (คิดราคาตั้งแต่ขาดอายุการประกัน) ทำให้มีค่าใช้จ่ายที่สูง ทั้งนี้เพื่อให้ประหยัดค่าใช้จ่ายในการซ่อมบำรุง สำนักงาน ป.ป.ท. ควรสนับสนุนงบประมาณในการบำรุงรักษาเพิ่มขึ้นจากปัจจุบัน

3.3.4 การสนับสนุนอัตรากำลังของนักวิชาการคอมพิวเตอร์ ปัจจุบัน สำนักงาน ป.ป.ท. เป็นองค์กรขนาดกลาง มีทั้งในส่วนกลาง และส่วนภูมิภาค แต่หากมองถึงอัตรากำลังด้านเทคโนโลยีสารสนเทศแล้วค่อนข้างขาดแคลน เนื่องจากจะมีเจ้าหน้าที่อยู่ในส่วนกลางเพียง 10 อัตรา (รวมผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) และทั้งหมดจะต้องดูแลทั้งประเทศ ซึ่งไม่สอดคล้องกับภารกิจงานที่เพิ่มขึ้น