แผนบริหารความเสี่ยง ด้านเทคโนโลยีสารสนเทศ (ICT DOPA Risk Management) ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

DOPA

ศูนย์สารสนเทศเพื่อการบริหารพัฒนางานปกครอง
กรมการปกครอง กระทรวงมหาดไทย

2024

แผนบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ
(ICT DOPA Risk Management)
ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

ศูนย์สารสนเทศเพื่อการบริหารพัฒนางานปกครอง
กรมการปกครอง กระทรวงมหาดไทย

คำนำ

แผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของกรมการปกครอง ฉบับนี้จัดทำ ขึ้นเพื่อเป็นกรอบแนวทางในการดำเนินงานการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ในการระบุความเสี่ยง วิเคราะห์ความเสี่ยง และการกำหนดแนวทาง หรือมาตรการควบคุมเพื่อป้องกันหรือลดความเสี่ยง โดยมุ่งหวังให้ส่วนราชการบรรลุผลตามเป้าประสงค์ขององค์กร เนื่องจากความเสี่ยงอาจนำไปสู่ผลเสียหรือความสูญเสียได้ทั้งทางตรงและทางอ้อม องค์กรจึงต้องเข้าใจประเภทของความเสี่ยงที่เผชิญอยู่เพื่อที่จะได้เลือกวิธีการที่เหมาะสมในการบริหารความเสี่ยงเหล่านั้นได้อยู่ระดับที่องค์กรสามารถรองรับได้และทำให้องค์กรบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง หวังเป็นอย่างยิ่งว่าแผนบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศของกรมการปกครอง ฉบับนี้จะช่วยให้ผู้รับผิดชอบใช้เป็นแนวทางในการลดความเสียหายต่างๆ ที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศของกรมการปกครอง ต่อไป

ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง
กรมการปกครอง กระทรวงมหาดไทย
มีนาคม ๒๕๖๗

สารบัญ

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดีโดยจะช่วยให้การบริหารงาน และการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูลการใช้งานอุปกรณ์คอมพิวเตอร์การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่าง ๆ ภายใต้สภาวะการดำเนินงานของทุก ๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรดังนั้น ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร/ส่วนราชการ วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยงแล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

๑.๒ วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง

๑.๒.๑ เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑.๒.๒ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๑.๓ เป้าหมาย

มีแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของ กรมการปกครอง

๑.๔ ขอบเขตการดำเนินงาน

เป็นการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายในความรับผิดชอบของศูนย์สารสนเทศเพื่อการบริหารงานปกครอง กรมการปกครอง

๑.๕ ประโยชน์ที่คาดว่าจะได้รับ

๑.๕.๑ มีความพร้อมในการรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑.๕.๒ มีแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

บทที่ ๒
แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

- **ประสิทธิผล** มีระบบฐานข้อมูลและระบบสารสนเทศให้บริการในลักษณะ Web Application
- **คุณภาพการให้บริการ** ผู้รับบริการและประชาชนได้รับข้อมูล ข่าวสารที่ถูกต้อง เป็นปัจจุบัน และสะดวกในการเข้าถึงข้อมูล
- **ประสิทธิภาพของการปฏิบัติราชการ** การพัฒนาระบบข้อมูลสารสนเทศให้เป็นปัจจุบัน และการเชื่อมโยงเครือข่ายเทคโนโลยีสารสนเทศอย่างมีเสถียรภาพ

การบริหารความเสี่ยง มีความสำคัญต่อการบริหารราชการแบบมุ่งผลสัมฤทธิ์ ตามพระราชกฤษฎีกาว่าด้วย การบริหารกิจการบ้านเมืองที่ดี พ.ศ. ๒๕๔๖ และยุทธศาสตร์ชาติ ๒๐ ปี พ.ศ. ๒๕๖๑ – ๒๕๘๐ ในด้านยุทธศาสตร์ชาติด้านความมั่นคง ให้รองรับการพัฒนาระบบเตรียมพร้อมแห่งชาติและการบริหารจัดการภัยคุกคามให้มีประสิทธิภาพเพื่อให้มีความพร้อมเผชิญกับสภาวะไม่ปกติ ภัยคุกคามทุกมิติทุกรูปแบบและทุกระดับ รวมทั้งภัยพิบัติและภัยคุกคามรูปแบบต่าง ๆ ได้อย่างแท้จริง เนื่องจากการบริหารความเสี่ยง เป็นส่วนหนึ่งของกระบวนการบริหารเชิงกลยุทธ์ เป็นการเพิ่มโอกาสและช่วยให้องค์กร ส่วนราชการ หน่วยงาน บรรลุเป้าประสงค์และยุทธศาสตร์ที่ตั้งไว้ และเป็นการพัฒนาผลการปฏิบัติงานขององค์กร/ส่วนราชการ ที่จะนำไปสู่การใช้ทรัพยากรด้านสารสนเทศอย่างมีประสิทธิภาพ และคุ้มค่าตลอดจนความสามารถพัฒนาคุณภาพบริการที่ดีให้แก่ผู้รับบริการและประชาชนทั่วไป

๒.๑ สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น ฐานข้อมูลด้านฐานข้อมูลการเงินงบประมาณ ฐานข้อมูลงานบริการ ฐานข้อมูลคุมทะเบียนทรัพย์สิน ระบบบริการออนไลน์ (CITIZEN SERVICE) เป็นต้น

ระบบฐานข้อมูลบริหารงานภายใน (Back Office) หรือระบบฐานข้อมูลสารสนเทศสำหรับบุคลากรกรมการปกครอง (Intranet) ได้แก่ ฐานข้อมูลระบบสารบรรณอิเล็กทรอนิกส์ (e-Document) ฐานข้อมูลสารสนเทศทรัพยากรบุคคล และฐานข้อมูลครุภัณฑ์คอมพิวเตอร์ และฐานข้อมูลระบบรายงานผลต่างๆ เป็นต้น

ระบบการให้บริการบนเครือข่ายคอมพิวเตอร์ ได้แก่ บริการเครือข่ายของกรมการปกครอง ณ ส่วนกลาง และส่วนภูมิภาค (DOPA_AP , DOPA_FreeWIFI) เป็นต้น

อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบเครือข่าย (Network Server) เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server) เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server) เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์ (Web Server) อุปกรณ์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall) เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) เครื่องเครื่องคอมพิวเตอร์ชนิดพกพา (Notebook) เครื่องสแกนเนอร์ (Scanner) เครื่องพิมพ์เลเซอร์ (Laser Printer) เครื่องพิมพ์แบบพ่นหมึก (Ink-Jet Printer) อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS) อุปกรณ์กระจายสัญญาณเครือข่าย (Switching) และอุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access point) เป็นต้น

๒.๒ ความหมายและความสำคัญของการจัดการความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ใดๆ ที่อาจจะเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือ ก่อให้เกิดความล้มเหลว หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจหลัก และตามแผนปฏิบัติราชการของส่วนราชการ

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุของความเสี่ยง ที่จะทำให้ไม่บรรลุวัตถุประสงค์ตามขั้นตอนการดำเนินงานที่กาหนดไว้ ทั้งปัจจัยภายในองค์กรเช่น โครงสร้างพื้นฐาน (Infrastructure) พนักงาน (Personnel) กระบวนการ (Process) เทคโนโลยี (Technology) และภายนอกองค์กร เช่น ภัยธรรมชาติ (Natural Environment) ภาวะเศรษฐกิจ (Economic) ภาวะการเมือง (Political) เทคโนโลยี (Technology) ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ(Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึงสถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น ๔ ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง ระบบการบริหารปัจจัยและควบคุมพฤติกรรม รวมทั้งกระบวนการดำเนินงานต่างๆ โดยลดสาเหตุของแต่ละโอกาสที่จะทำให้เกิดความเสียหาย เพื่อให้ระดับของความเสี่ยง และผลกระทบ ที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้ อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามภารกิจหลักตามกฎหมายการจัดตั้งส่วนราชการ และเป้าหมายตามแผนปฏิบัติราชการประจำปีเป็นสำคัญ การบริหารความเสี่ยงจะอาศัยขั้นตอนที่ต่อเนื่อง เนื่องจากการระบุความเสี่ยงที่จะส่งผลกระทบจากความเสี่ยง และกำหนดแนวทางในการจัดการความเสี่ยงนั้นได้ถูกดำเนินการตามแผนที่วางไว้

การควบคุม (Control) หมายถึง นโยบาย แนวทางหรือขั้นตอนปฏิบัติต่าง ๆ ซึ่งกระทำเพื่อลดความเสี่ยง โดยทำตามแนวทางการตอบสนองต่อความเสี่ยงที่วางไว้ ประกอบด้วยกิจกรรมการควบคุมเกิดขึ้นในทุกระดับ ทุกหน้าที่งานและทั่วทั้งองค์กร และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ ๔ ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ค้นพบ การควบคุมแบบส่งเสริม และการควบคุมแบบแก้ไข

๒.๓ วัตถุประสงค์ของการจัดทำแผนบริหารความเสี่ยง ๕ ประการ

๑) เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ

๒) เพื่อให้มีการวางแผน ควบคุม แก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓) เพื่อนำเทคโนโลยีสารสนเทศมาสนับสนุนการทำงานให้เกิดประสิทธิภาพสูงสุด และลดโอกาสความเสียหายที่อาจเกิดขึ้น

๔) เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และกาเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงของระบบฐานข้อมูลด้านเทคโนโลยีสารสนเทศ ให้ส่วนราชการ/องค์กร/หน่วยงาน นำไปใช้ประโยชน์

๕) เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่างๆ ที่น่าจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกัน หรือจัดการกับความเสี่ยงเหล่านั้น ก่อนที่จะเริ่มปฏิบัติงาน หรือดำเนินงานตามแผน

๒.๔ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ปัจจุบันเทคโนโลยีสารสนเทศ ได้เข้ามามีบทบาทสำคัญในการดำเนินงานขององค์การและหน่วยงานอื่นๆ ทั้งในส่วนของการบริหารจัดการ การจัดเก็บข้อมูล การใช้เครื่องคอมพิวเตอร์แม่ข่าย การจัดทำและพัฒนาระบบเทคโนโลยีสารสนเทศในภาพรวม มุ่งหวังที่จะให้ระบบสารสนเทศช่วยในการปฏิบัติงานของหน่วยงานมีความสะดวก รวดเร็ว และมีประสิทธิภาพมากยิ่งขึ้น แต่การนำเทคโนโลยีสารสนเทศมาใช้ ย่อมมีความเสี่ยงหลายประการด้วยกัน ด้งนั้น การวางแผนและการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ จึงเป็นเรื่องสำคัญ และควรมีการเตรียมการที่ดี หากหน่วยงานไม่มีการบริหารจัดการและรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศที่รัดกุมเพียงพอ อาจส่งผลกระทบต่อการดำเนินงานและสร้างความเสียหายต่อหน่วยงานได้ทั้งในด้านการพัฒนาระบบราชการ การพัฒนาองค์กร การพัฒนาบุคลากร ความคุ้มค่าทางงบประมาณ ดังนั้น การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศจึงต้องมีทั้งการวางแผน การประเมิน ทั้งโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น สามารถประเมินเป็นเชิงปริมาณหรือเชิงคุณภาพได้

๒.๕ ความเสี่ยงหลักด้านระบบเทคโนโลยีสารสนเทศ

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร คือ กระบวนการการทำงานที่ช่วยให้ IT Managers สามารถองค์กรดำเนินธุรกิจให้บรรลุผลสำเร็จของพันธกิจ และปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กร

๒.๕.๑ ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ (Access Risk) ความเสี่ยงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือเป็นความเสี่ยงในกรณีที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ ซึ่งหากหน่วยงานมิได้มีวิธีการจัดการและควบคุมความเสี่ยงด้าน access risk ที่รอบคอบและรัดกุมเพียงพอแล้ว อาจทำให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้ล่วงรู้ข้อมูล และอาจนำข้อมูลไปแสวงหาประโยชน์โดยมิชอบ อีกทั้งข้อมูลและการทำงานของระบบคอมพิวเตอร์ ก็อาจถูกแก้ไขเปลี่ยนแปลงได้ ส่วนกรณีบุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลและระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบได้นั้น อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพเท่าที่ควร โดยที่ความเสี่ยงด้าน access risk อาจเกิดจากหลายสาเหตุ เช่น การกาหนดสิทธิในการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ที่ไม่เหมาะสมกับหน้าที่และความรับผิดชอบหรือเกินความจาเป็นในการใช้งาน การมิได้มีการกำหนดรหัสผ่าน (password) ในการเข้าสู่ระบบงานคอมพิวเตอร์อย่างรัดกุมเพียงพอ การมิได้จำกัดและควบคุมให้เฉพาะเจ้าหน้าที่ที่มีอำนาจหน้าที่เกี่ยวข้องในการเข้าออก Network Operation Center (NOC) เป็นต้น

๒.๕.๒ ความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูลและการทำงานของระบบคอมพิวเตอร์ Integrity Risk ความเสี่ยงซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องหรือมีการบันทึกข้อมูล การประมวลผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานมิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องที่รอบคอบ

และรัดกุมเพียงพอ (access risk) ซึ่งส่งผลให้ข้อมูล รวมทั้งการทำงานของระบบคอมพิวเตอร์ อาจถูกแก้ไข เปลี่ยนแปลงโดยมิชอบได้ หรือมีสาเหตุมาจากการมิได้มีระบบการควบคุมและตรวจสอบอย่างเพียงพอเพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประมวลผล และการแสดงผลมีความถูกต้องครบถ้วน นอกจากนี้ การบริหารจัดการและการควบคุมเกี่ยวกับการพัฒนา การแก้ไข หรือเปลี่ยนแปลงระบบคอมพิวเตอร์ที่ไม่รอบคอบและรัดกุมเพียงพอ ก็อาจส่งผลให้ระบบคอมพิวเตอร์มีการประมวลผลที่ไม่ถูกต้องครบถ้วน หรือไม่สอดคล้องกับความต้องการของผู้ใช้งานได้

๒.๕.๓ ความเสี่ยงเกี่ยวกับการไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ Availability Risk ความเสี่ยงซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากการมิได้ควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการมิได้มีการสำรองข้อมูล และระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน นอกจากนี้ หากหน่วยงานมิได้มีการควบคุมเกี่ยวกับการเข้าถึงข้อมูล และระบบคอมพิวเตอร์ที่รอบคอบและรัดกุมเพียงพอแล้ว (access risk) ก็อาจส่งผลให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องสามารถเข้ามาทำให้ข้อมูลและการทำงานของระบบคอมพิวเตอร์เสียหายได้

๒.๕.๔ ความเสี่ยงเกี่ยวกับการที่หน่วยงานมิได้จัดให้มีการบริหารจัดการด้านเทคโนโลยีสารสนเทศที่สะท้อนระบบควบคุมภายในที่ดี Infrastructure Risk รวมทั้งมิได้จัดให้มีระบบคอมพิวเตอร์และบุคลากร ให้เหมาะสมและเพียงพอแก่การสนับสนุนการประกอบธุรกิจ โดยความเสี่ยงนี้อาจเกิดจากการแบ่งแยกอำนาจหน้าที่ที่ไม่เหมาะสม ซึ่งทำให้ขาดระบบการสอบยันและการตรวจสอบการปฏิบัติงานที่เพียงพอ รวมถึงการมิได้จัดให้มีนโยบายเกี่ยวกับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ซึ่งทำให้ไม่มีแนวทางในการควบคุมความเสี่ยงต่างๆ หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานที่ครอบคลุมงานสำคัญทุกด้านและมีรายละเอียดเพียงพอเพื่อใช้เป็นแนวทางในการปฏิบัติงาน นอกจากนี้ ก็อาจเกิดจากการมิได้จัดให้มีระบบคอมพิวเตอร์ที่มีประสิทธิภาพเพียงพอแก่การสนับสนุนการดำเนินงาน และการมิได้จัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอเพื่อให้มีความรอบรู้และเชี่ยวชาญในงานที่รับผิดชอบ

๒.๖ ประเภทความเสี่ยง

ความเสี่ยงด้านเทคโนโลยีสารสนเทศของกลุ่มงานปฏิบัติการและประมวลผลข้อมูล ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง สามารถแบ่งออกได้เป็น ๗ ประเภท คือ

- ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม
- ความเสี่ยงด้านบุคลากร (People Ware)
- ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hard Ware)
- ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Soft Ware)
- ความเสี่ยงด้านระบบข้อมูล
- ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)
- ความเสี่ยงด้านการเงิน (Financial Risk)

๒.๖.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม

หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ การไม่มีระบบรักษาความปลอดภัยห้องคอมพิวเตอร์แม่ข่าย (Network Operation Center) และการก่อการร้าย เป็นต้น

๒.๖.๑.๑ การบริหารจัดการความเสี่ยงด้านกายภาพและสิ่งแวดล้อม

๑) การกำหนดที่ตั้งของเครื่องคอมพิวเตอร์ การเดินสายไฟฟ้า สายวงจร สายสัญญาณของระบบต่างๆ อย่างเน้นความปลอดภัยและหลีกเลี่ยงไม่ตั้งระบบไว้ในจุดที่มีความเสี่ยงสูง รวมทั้งมีอุปกรณ์ป้องกันและบรรเทาภัยพิบัติเบื้องต้น เช่น เครื่องปรับอากาศ, ตู้ Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย, หน้าต่างระบายความร้อน, ถังดับเพลิง เป็นต้น

๒) การควบคุมการเข้า – ออก Network Operation Center (NOC) ห้องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง เป็นพื้นที่เขตหวงห้ามเฉพาะ โดยกำหนดสิทธิการเข้า-ออก ห้องคอมพิวเตอร์แม่ข่ายให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องรับผิดชอบ

๓) การป้องกันความเสียหาย โดยการวางระบบป้องกันไฟที่เหมาะสม โดยทำการติดตั้งระบบดับเพลิงอัตโนมัติด้วยสารเคมีห้องปฏิบัติการคอมพิวเตอร์เครือข่าย และห้องศูนย์ปฏิบัติการสื่อสารโทรคมนาคม และส่งผ่านข้อมูล

๔) การป้องกันความเสี่ยงจากระบบไฟฟ้าขัดข้อง โดยมีการติดตั้งเครื่องสำรองไฟสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และการติดตั้งระบบสายดิน (Ground) ที่ได้มาตรฐานอุปกรณ์ป้องกันไฟ

๕) การป้องกันความเสี่ยงจากระบบควบคุมอุณหภูมิและความชื้นให้เหมาะสม โดยการติดตั้งอุณหภูมิเครื่องปรับอากาศ และค่าความชื้นให้มีระดับเหมาะสมกุบคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์

๖) ความเสี่ยงในเรื่องงบประมาณที่จะดำเนินการได้อย่างมีประสิทธิภาพสูงสุดและเกิดความต่อเนื่อง

๗) ความเสี่ยงในเรื่องประเด็นนโยบายของผู้บริหาร ที่ให้น้ำหนักและความสำคัญเกี่ยวกับเทคโนโลยีสารสนเทศ หากมีการเปลี่ยนแปลงจะส่งผลกระทบต่อการปฏิบัติงานและแนวทางในการดำเนินการขั้นตอนต่อไป

๘) ความเสี่ยงในเรื่องของการบริหารจัดการ โดยสามารถวางแผนบริหารความเสี่ยงและดำเนินการเพื่อลดความเสี่ยงได้ ดังนี้

- จัดทำแผนแม่บทและแผนปฏิบัติการเทคโนโลยีสารสนเทศ
- บริหารจัดการ ติดตาม ควบคุม กำกับดูแล และให้คำปรึกษา แก้ไขปัญหาระบบ
- การจัดการประเมินผลแผนแม่บทและแผนปฏิบัติการเทคโนโลยีสารสนเทศและการสื่อสาร
- ติดตาม จัดทำ ควบคุม กำกับ ดูแล และให้คำปรึกษา แก้ไขปัญหาระบบการจัดการและไหลเวียนเอกสารไร้กระดาษ (paperless) ให้กลุ่มงาน/ฝ่าย ของสำนักงานจังหวัด และหากสามารถดำเนินการได้อย่างมีประสิทธิภาพสูงสุดแล้ว จะขยายไปยังองค์กร/หน่วยงานต่างๆ
- ศึกษา วิเคราะห์ และจัดทำระบบข้อมูลเพื่อการบริหารราชการ เพื่อสนับสนุนการตัดสินใจของผู้บริหารระดับสูง (Executive Information System : EIS)

- ศึกษา วิเคราะห์ข้อมูลที่เกี่ยวข้องเพื่อการวางแผน และคาดการณ์แนวโน้มความต้องการบุคลากรด้านเทคโนโลยีสารสนเทศ
- ให้บริการฝึกอบรม เพื่อพัฒนาความรู้ด้านเทคโนโลยีสารสนเทศแก่บุคลากรขององค์กร/หน่วยงานต่างๆ

๒.๖.๒ ความเสี่ยงด้านบุคลากร (People Ware)

ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ เช่น การวางแผน การตรวจสอบ การทำงาน การมอบหมายหน้าที่และสิทธิของบุคลากร/คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดถี่ถ้วน เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งาน การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมทั้ง บุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม ซึ่งเป็นความเสี่ยงทั้งสิ้น

๒.๖.๒.๑ การบริหารจัดการความเสี่ยงด้านบุคลากร

๑) การกำหนดโครงสร้าง/มอบหมายงานในหน้าที่ให้แก่บุคลากรด้านเทคโนโลยีสารสนเทศ ที่มีความเหมาะสม คือ มีความรู้ ประสบการณ์ ในระดับที่สามารถรับการถ่ายทอดเทคโนโลยีสารสนเทศด้านการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ และสามารถถ่ายทอดความรู้นั้นให้แก่ผู้ใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ

๒) การว่าจ้าง/จัดจ้างบุคลากรภายนอก (Outsourcing) เพื่อจัดทำโครงการพัฒนาระบบข้อมูลสารสนเทศ เนื่องจากเป็นผู้มีความชำนาญเป็นพิเศษหรือเป็นผู้มีมือโดยเฉพาะทาง มีเครื่องมือและเทคโนโลยีที่ทันสมัยทันต่อการพัฒนาระบบฐานข้อมูลสารสนเทศมากกว่าภาคราชการ โดยการว่าจ้างบุคคลภายนอกนี้จะมีความเสี่ยงในเรื่องของความรู้ ความเข้าใจในระบบราชการ และผลสัมฤทธิ์ที่เกิดจากการทำงาน อีกทั้งในแง่ของความคุ้มค่าของการใช้จ่ายงบประมาณ ดังนั้น หน่วยงานเจ้าของงบประมาณต้องกำกับดูแล ควบคุมอย่างต่อเนื่อง ตั้งแต่เริ่มกระบวนการจนถึงสิ้นสุดกระบวนการ โดยยึดหลักการบริหารกิจการบ้านเมืองที่ดี รักษาประโยชน์ของทางราชการให้มากที่สุด

๓) บุคลากรของภาคราชการ ขาดความรู้ความเข้าใจในเรื่องของระบบเทคโนโลยีสารสนเทศโดยเฉพาะในเรื่องเชิงเทคนิคด้านโปรแกรมและนวัตกรรมใหม่ ทำให้เกิดช่องว่างในการที่จะประสานงานและรับผิดชอบงานอย่างมีประสิทธิภาพ ดังนั้น แนวทางในการวางแผนบริหารความเสี่ยงในประเด็นนี้ โดยการส่งเจ้าหน้าที่เข้ารับการอบรมความรู้ทางเทคโนโลยีสารสนเทศเพิ่มมากขึ้น เพื่อพัฒนาประสิทธิภาพการดำเนินงานด้านสารสนเทศของกรมการปกครอง

๔) แผนการบริหารความเสี่ยงด้านบุคลากร คือ ต้องมีการฝึกอบรมในด้านที่เกี่ยวข้องกับระบบสารสนเทศ สำหรับบุคลากรใน ๓ ระดับ คือ ระดับผู้บริหาร (CIO) ระดับผู้ดูแลระบบ (Administrator) และผู้ใช้งานทั่วไป (User) ทำให้บุคลากรระดับผู้บริหาร วิเคราะห์และวางแผนงานด้านสารสนเทศ บุคลากรระดับผู้ดูแลระบบ สามารถดูแล ปรับปรุง และพัฒนาระบบสารสนเทศให้เป็นไปตามนโยบายของผู้บริหาร รวมทั้งผู้ใช้งานทั่วไปมีความรู้ด้านการรักษาความปลอดภัยระบบสารสนเทศได้อย่างมีประสิทธิภาพ

๒.๖.๓ ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware)

ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ ไม่ว่าจะเป็นความเสี่ยงที่เกิดจากการทำงานผิดพลาดหรือช่องโหว่ของอุปกรณ์ ตลอดจนการเคลื่อนย้ายตัวเครื่อง อุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ (Computer Virus), มัลแวร์ (Malware), สปายแวร์ (Spyware) เป็นต้น

๒.๖.๓.๑ การบริหารจัดการความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ

๑) ความเสี่ยงในเรื่องของการจัดหาอุปกรณ์เทคโนโลยีสารสนเทศที่เหมาะสมกับลักษณะของงาน/โครงการ และขององค์กร ที่ต้องมีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศให้เหมาะสมตามลักษณะของโครงการ (Acquisition and Implementation) และเหมาะสมกับงบประมาณ

๒) ความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ (Support) โดยมีข้อควรปฏิบัติ ๒ ด้าน คือ

<u>ด้านการบำรุงรักษาและลดความเสี่ยง</u>

(๑) สามารถแก้ไขปัญหาเบื้องต้นของเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงได้โดยผู้ดูแลระบบเครื่องคอมพิวเตอร์ (Administrator) รวมถึงมีการรับประกันความเสียหายจากผู้ขาย และการดูแลอย่างถูกต้องและต่อเนื่อง

(๒) ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อใช้งานเสร็จเรียบร้อยแล้ว

(๓) มีการตรวจเช็คไวรัส และกำจัดอย่างสม่ำเสมอ ทั้งอุปกรณ์ต่อพ่วง เช่น Flash Drive และเครื่องคอมพิวเตอร์ที่ใช้งาน

(๔) การติดตั้ง Firewall เพื่อป้องกันเบื้องต้นไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่าย Internet สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศขององค์กรได้

(๕) การตรวจสอบและดูแลคอมพิวเตอร์แม่ข่ายเป็นประจำสม่ำเสมอ

(๖) ระบบปฏิบัติการ Windows ควรทำการ Update เป็นประจำ

(๗) ฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงานเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง และการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ เช่น การกำหนดรหัสผู้ใช้ และการใช้รหัสผ่าน

(๘) การจัดทำคู่มือผู้ดูแลอุปกรณ์เทคโนโลยีสารสนเทศ

(๙) การสำรองข้อมูล (Backup) สารสนเทศ

<u>ด้านการรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่าย (Server)</u>

(๑) กำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย ในกรณีพบว่ามีการใช้งาน หรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติ จะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับบัญชาทราบทันที

(๒) ทำการทดสอบ system software เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานอย่างสม่ำเสมอ

(๓) ติดตั้งโปรแกรมระบบรักษาความปลอดภัย

(๔) กำหนดบุคลากรรับผิดชอบในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบคอมพิวเตอร์แม่ข่ายอย่างชัดเจน

๒.๖.๔ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software)

ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ ที่ได้จัดทำและพัฒนาขึ้น รวมถึงโปรแกรมประยุกต์อื่นๆ เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม และการถูกผู้ไม่หวังดีทำลายระบบ (Hacker) เป็นต้น

๒.๖.๔.๑ การบริหารจัดการความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software) สามารถดำเนินการได้โดยการพัฒนามาตรฐานและการบริการโปรแกรมคอมพิวเตอร์ ดังนี้

๑) พัฒนาและปรับปรุงมาตรฐาน Hardware, Software , People ware, Data และ Network ให้เป็นฐานข้อมูลกลางของงานเทคโนโลยีสารสนเทศ และเป็นไปในทิศทางเดียวกัน

๒) สร้างกลไกการจัดการฐานข้อมูล การจัดระบบสารสนเทศ เพื่อการบริหารจัดการของหน่วยงานให้ครอบคลุม ถูกต้อง และทันสมัย มากยิ่งขึ้น

๓) พัฒนาโปรแกรมให้สามารถบริหารจัดการฐานข้อมูลให้มีมาตรฐาน และแบ่งสรรการใช้ทรัพยากรฐานข้อมูลจากโปรแกรมร่วมกันได้

๔) ศึกษาแนวโน้มและทิศทางของ Software ในอนาคตเป็นอย่างไร เพื่อนำมาวิเคราะห์เปรียบเทียบวางแผนในการปรับปรุงใช้งานกับภายในองค์กร

๕) พัฒนาโปรแกรมให้สามารถจัดเก็บ รวบรวม ประมวลผลข้อมูล ศึกษา วิเคราะห์เพื่อการนำเสนอและสนับสนุนการตัดสินใจของผู้บริหาร

๖) การใช้โปรแกรมที่ถูกต้องตามลิขสิทธิ์ ไม่ลักลอบใช้งาน เพราะผิดต่อกฎหมายและทำให้องค์กรขาดความน่าเชื่อถือ

๒.๖.๕ ความเสี่ยงด้านระบบข้อมูล (Data)

ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศอันอาจจะก่อให้เกิดความเสียหาย ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล การโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล ความเสี่ยงเหล่านี้ล้วนมีความจำเป็นที่จะต้องมีการบริหารจัดการความเสี่ยง ด้านข้อมูล ดังนั้น การรักษาความปลอดภัยของข้อมูลจึงเป็นเรื่องสำคัญ เนื่องจากข้อมูลสารสนเทศเป็นปัจจัย สำคัญสำหรับผู้บริหาร ที่จะนำมาเป็นเครื่องมือสำหรับการตัดสินใจในการวางแผน ดังนั้น การรักษาความปลอดภัยของระบบข้อมูล และคอมพิวเตอร์จากภัยต่างๆ ทั้งภัยจากคน ภัยจากธรรมชาติ หรือเหตุการณ์ใดๆ จึงมีความสำคัญและจำเป็นที่จะต้องมีการป้องกันเพื่อให้เกิดความมั่นคงต่อระบบข้อมูลสารสนเทศ และเทคโนโลยี

๒.๖.๕.๑ การบริหารจัดการความเสี่ยงด้านข้อมูล โดยการบริหารจัดการความเสี่ยงด้านข้อมูลของกรมการปกครอง มีแนวทางดำเนินการ ดังนี้

๑) ฐานข้อมูลของกรมการปกครอง มีความเสี่ยงเกี่ยวกับความไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) และการทำงานของระบบคอมพิวเตอร์ ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาด โดยอาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลของระบบคอมพิวเตอร์ โดยบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (access risk) ส่งผลให้ข้อมูลและการทำงานของ

ระบบคอมพิวเตอร์อาจถูกแก้ไขเปลี่ยนแปลงได้ หรือมีสาเหตุมาจากการที่ไม่มีระบบการควบคุมและตรวจสอบอย่างเพียงพอ เพื่อให้มั่นใจได้ว่าการบันทึกข้อมูล การประเมินผล และการแสดงผลมีความถูกต้องครบถ้วน

๒) ฐานข้อมูลของกรมการปกครอง มีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่อง หรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้โดยความเสี่ยงนี้อาจเกิดจากไม่มีการควบคุมดูแลการทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ และยังรวมไปถึงการที่ไม่ได้สำรองข้อมูลและระบบงานคอมพิวเตอร์ และจัดให้มีแผนรองรับเหตุการณ์ฉุกเฉิน

๓) ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการที่ไม่ได้จัดให้มีระบบคอมพิวเตอร์ที่ทันสมัยและบุคลากรให้เหมาะสมและเพียงพอแก่การสนับสนุนการทำงาน หรือเกิดจากการไม่มีแผนงานและขั้นตอนการปฏิบัติงานสำคัญทุกด้าน และการจัดให้มีการอบรมบุคลากรด้านคอมพิวเตอร์อย่างเพียงพอ เพื่อให้มีความรู้และเชี่ยวชาญในงานที่รับผิดชอบสำหรับการควบคุมการปฏิบัติงาน

๔) ฐานข้อมูล มีความเสี่ยงเกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Back Up) ที่สำคัญคือ เพื่อไม่ให้ข้อมูลเกิดการสูญหาย ตลอดจนเป็นแนวทางในการปฏิบัติในการบริหารจัดการในการเก็บข้อมูล (Back Up) การกู้คืนข้อมูล (Recovery) ดังนั้น การสำรองข้อมูลและการเตรียมข้อมูลให้พร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan) ของกรมการปกครอง จึงมีวัตถุประสงค์เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพและในเวลาที่ต้องการ (Availability Risk) โดยมีเนื้อหาครอบคลุมเกี่ยวกับแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ รวมทั้งการทดสอบ และการเก็บรักษา นอกจากนี้ยังมีเนื้อหาครอบคลุมเกี่ยวกับการจัดทำและการทดสอบแผนฉุกเฉิน ดังนี้

- การสำรองข้อมูล (Back Up) สำรองข้อมูลด้าน Soft ware ให้มีความพร้อมใช้งานได้ตลอดเวลาและต่อเนื่องเพื่อป้องกันการสูญหายที่อาจจะเกิดขึ้นได้ ดังนั้น จึงทำการสำรองข้อมูลเป็นประจำทุกสัปดาห์ ดังนี้
  - กำหนดสถานที่ในการเก็บรักษาข้อมูลสำรองโดยเฉพาะ
  - การสำรองข้อมูลโดยการบันทึกไว้ที่แผ่น CD ROM
- การทดสอบ กำหนดทดสอบข้อมูลสำรองอย่างน้อยเดือนละ ๑ ครั้ง เพื่อตรวจสอบได้ว่าข้อมูลรวมทั้งโปรแกรมต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและใช้งานได้
- การกู้ข้อมูลสู่ระบบ มีการกำหนดบุคลากรผู้ที่ได้รับสิทธิ์กู้คืนข้อมูลที่ได้ทำการสำรองไว้โดย Login ผ่าน USER NAME, PASSWORD ที่กำหนดไว้ตั้งแต่ขั้นต้น
- การบำรุงรักษาอุปกรณ์เครือข่ายและระบบคอมพิวเตอร์เป็นประจำ

๒.๖.๗ ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของนโยบายรัฐบาล ผู้บริหาร องค์กร เนื่องจากการเปลี่ยนแปลงรัฐบาล และผู้บริหารองค์กรต่างๆ ในด้านเทคโนโลยีสารสนเทศ ทำให้การกำหนดยุทธศาสตร์และแผนการดำเนินงานเปลี่ยนแปลงไป อันส่งผลกระทบต่อการบรรลุวิสัยทัศน์พันธกิจ หรือสถานะขององค์กร

การบริหารจัดการความเสี่ยงด้านกลยุทธ์ โดยการสื่อสารนโยบายและผลักดันให้มีการจัดทำแผนเทคโนโลยีสารสนเทศ ในหน่วยงาน ทุกระดับ อย่างทั่วถึง และมีการแปลงแผนไปสู่การปฏิบัติอย่างจริงจัง

แหล่งที่มาของความเสี่ยงด้านกลยุทธ์สามารถจำแนกได้๒ ประเภท คือ ปัจจัยความเสี่ยงภายนอก ได้แก่ ภาวการณ์การแข่งขัน การเปลี่ยนแปลงนโยบาย กระแสสังคม การเปลี่ยนแปลงทางเทคโนโลยี ปัจจัยทางเศรษฐกิจ ปัจจัยทางการเมือง และปัจจัยความเสี่ยงภายใน ได้แก่ ปัจจัยภายในที่องค์กรสามารถควบคุมได้แต่สามารถส่งผลกระทบหรือเป็นอุปสรรคต่อการดำเนินการตามแผนกลยุทธ์เพื่อให้บรรลุเป้าหมาย ได้แก่ โครงสร้างองค์กร กระบวนการ และวิธีปฏิบัติงาน ความเพียงพอของข้อมูล และเทคโนโลยีสำหรับการให้บริการ เป็นต้น

๒.๖.๘ ความเสี่ยงด้านการเงิน (Financial Risk)

ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ และการเบิกจ่ายงบประมาณไม่ทันตามกำหนดเวลา การบริหารจัดการความเสี่ยงด้านการเงิน

- มีการจัดทำแผนบริหารจัดการการใช้จ่ายงบประมาณ
- การติดตามงบประมาณรายจ่ายอย่างต่อเนื่อง

๒.๗ การวิเคราะห์ความเสี่ยง (Risk assessment)

๒.๗.๑ การวิเคราะห์ความเสี่ยง จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศสามารถแยกประเภทความเสี่ยงด้านเป็น ๔ ประเภท ดังนี้

๑) ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Hacker เป็นต้น

๒) ความเสี่ยงจากผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓) ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๔) ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

๒.๘ การประเมินความเสี่ยง (Risk Estimation)

เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไรและผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใดเกณฑ์การประมาณ เป็นการกาหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบ และระดับความเสี่ยง ใช้เกณฑ์ดังนี้

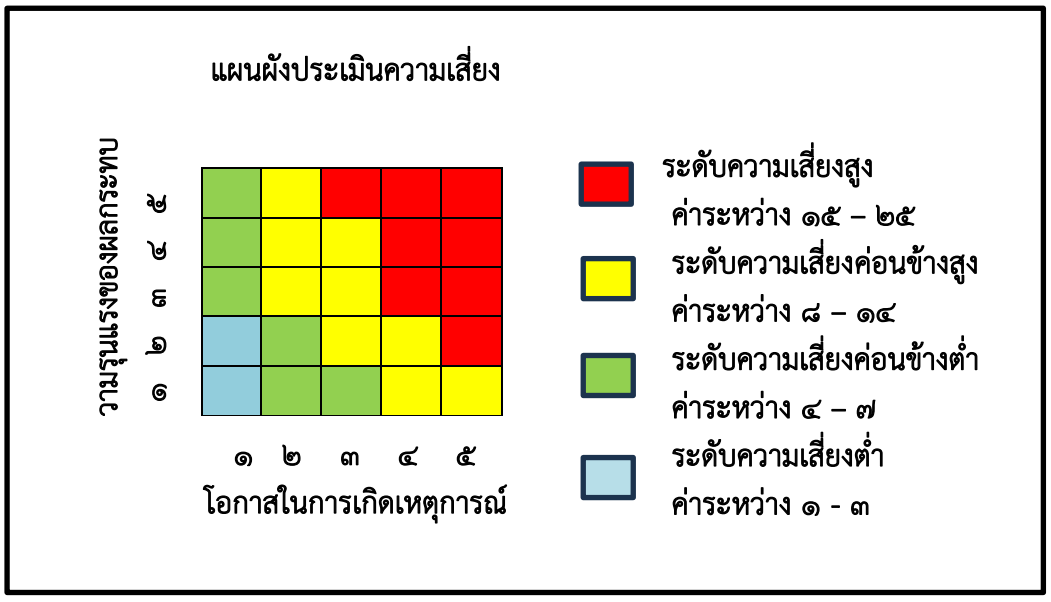
ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ

ระดับ	โอกาส	คำอธิบาย
5	สูงมาก	5 ครั้ง/ปี
4	สูง	4 ครั้ง/ปี
3	ปานกลาง	3 ครั้ง/ปี
2	น้อย	2 ครั้ง/ปี
1	น้อยมาก	ไม่เกิน 1 ครั้ง/ปี

ระดับความรุนแรงของผลกระทบของความเสี่ยง

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

การระบุความเสี่ยง (Risk identification)



๒.๙ วิธีการจัดการความเสี่ยง (Risk treatment)

การกำหนดวิธีการจัดการความเสี่ยง เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยใช้กลยุทธ์การจัดการความเสี่ยงอย่างใดอย่างหนึ่งผสมผสานกันดังต่อไป

๒.๙.๑ การยอมรับความเสี่ยง (Take) ความเสี่ยงที่เหลืออยู่ในปัจจุบันอยู่ภายในระดับที่ต้องการและยอมรับได้แล้วโดยไม่ต้องมีการดำเนินการเพิ่มเติมเพื่อลดโอกาสหรือความรุนแรงที่อาจเกิดขึ้นได้อีก เนื่องจากค่าใช้จ่ายในการจัดการหรือสร้างระบบควบคุมอาจมีมูลค่าสูงกว่าผลลัพธ์ที่ได้ แต่ก็ควรมีมาตรการติดตามและดูแล เช่น การกำหนดระดับของผลกระทบที่ยอมรับได้ เตรียมแผนการตั้งรับ/จัดการความเสี่ยง เป็นต้น

๒.๙.๒ การลดหรือควบคุม (Treat) การดำเนินการเพิ่มเติมเพื่อลดโอกาสที่อาจเกิดขึ้นหรือความรุนแรงของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยการออกแบบระบบควบคุม การแก้ไขปรับปรุงการทำงานเพื่อป้องกันหรือจำกัดผลกระทบ และโอกาสเกิดความเสียหาย เช่น ติดตั้งอุปกรณ์ความปลอดภัย ฝึกอบรมเพื่อพัฒนาทักษะวางมาตรการเชิงรุก เป็นต้น

๒.๙.๓ การถ่ายโอนหรือกระจาย (Transfer) การโอนหรือการกระจายความรับผิดชอบกับผู้อื่นในการจัดการความเสี่ยง โดยการกระจาย/โอนความเสี่ยง (Risk Sharing/Spreading) การกระจายทรัพย์สินหรือกระบวนการต่าง ๆ เพื่อลดความเสี่ยงจากการสูญเสีย เช่น การ Maintenance Service (MA) การให้มีการรับประกัน เพื่อโอนความเสี่ยงไปยังบริษัทรับประกัน การจ้างบริษัทภายนอก (Outsource) ให้ทำงานบางส่วนแทน การทำสำนาเอกสารหลายๆ ชุด การกระจายที่เก็บข้อมูลสารสนเทศที่สำคัญ เป็นต้น

๒.๙.๔ การหยุดหรือการหลีกเลี่ยง (Terminate) การหยุดหรือการดำเนินการเพื่อหลีกเลี่ยงเหตุการณ์ที่ก่อให้เกิดความเสี่ยงผู้บริหารควรจัดการลดระดับความเสี่ยงตามหลักการตอบสนองข้างต้นและดำเนินการประเมินความเสี่ยงอีกครั้งหลังจากที่ได้มีการจัดการความเสี่ยงในช่วงเวลาที่เหมาะสมเพื่อดูว่าการบริหารความเสี่ยงมีประสิทธิผลหรือไม่ เช่น งดทำขั้นตอนที่ไม่จำเป็นและจะนำมาซึ่งความเสี่ยง ปรับเปลี่ยนรูปแบบการทำงาน ลดขอบเขตการดำเนินการ เป็นต้น

๒.๑๐ ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศของ สนข. มีดังนี้

๒.๑๐.๑ ปัจจัยภายนอก

๒.๑๐.๑.๑ ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูลและระบบเครือข่ายคอมพิวเตอร์ได้แก่ ไฟไหม้ แผ่นดินไหว น้ำท่วม และภัยพิบัติอื่นๆ

๒.๑๐.๑.๒ การขโมยอุปกรณ์เครื่องข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๒.๑๐.๑.๓ การขำรุดเสียหายของตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย (Server) จากการเคลื่อนย้าย หรืออื่นๆ

๒.๑๐.๑.๔ ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหาย/ ขัดข้อง

๒.๑๐.๑.๕ ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ

๒.๑๐.๒ ปัจจัยภายใน

๒.๑๐.๒.๑ ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๑๐.๒.๒ การถูกไวรัสคอมพิวเตอร์ (Virus Computer) ทำลายฐานข้อมูลและโปรแกรมปฏิบัติการต่างๆ

๒.๑๐.๒.๓ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลหรือระบบเครือข่ายคอมพิวเตอร์จากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๒.๑๑ การประเมินความเสียหาย

๒.๑๑.๑ ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลงได้แก่ ภัยธรรมชาติตัวเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒.๑๑.๒ ความเสียหายที่เกิดผลเสียหายแจะต้องหยุดระบบชั่วขณะ ได้แก่การถูกเจาะเข้าระบบฐานข้อมูลระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

๒.๑๒ การรายงานผลการวิเคราะห์ความเสี่ยง (Risk reporting)

เมื่อประเมินความเสี่ยงแล้วเสร็จ จำเป็นต้องออกรายงานการประเมินเป็นเอกสารที่ผู้อื่นสามารถอ่านได้เอกสารนี้จะเป็นสาระสำคัญในการสื่อสารให้บุคลากรทั้งองค์กรได้รับรู้ รายงานประกอบด้วยรายละเอียดอย่างน้อยตามลักษณะรายละเอียดของความเสี่ยง และการออกรายงานมีวัตถุประสงค์ให้ส่วนต่างๆได้รับรู้ดังต่อไปนี้

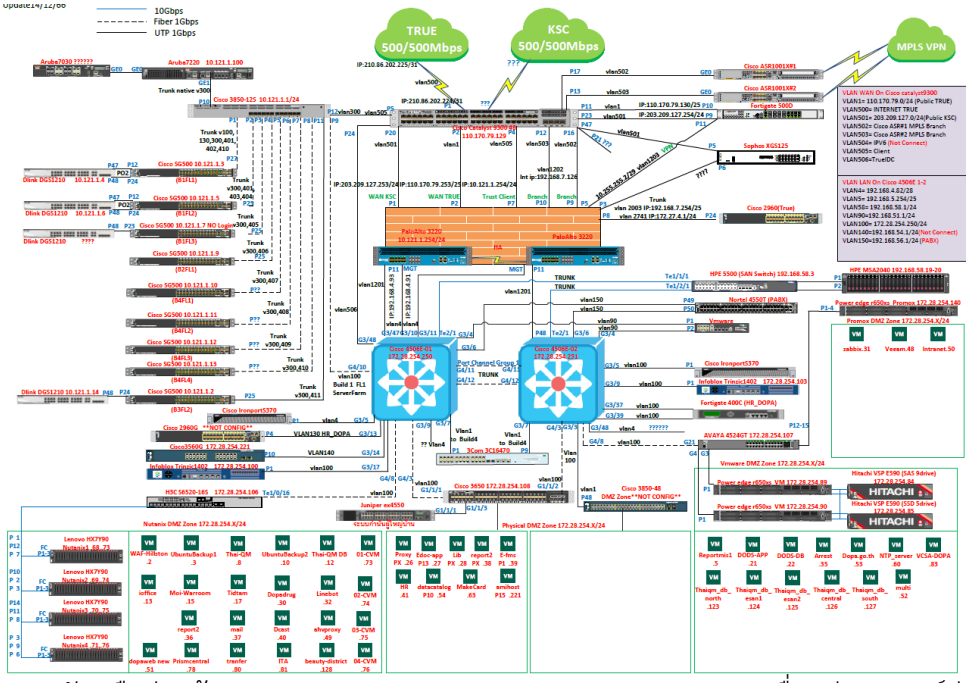
- **ฝ่ายบริหาร** ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น
  - รับรู้ความเสี่ยงที่องค์กรเผชิญอยู่
  - เข้าใจผลที่กระทบต่อผู้มีส่วนได้เสียต่างๆในกรณีที่เกิดมีเหตุ หรือเหตุการณ์และเกิดผลเสียต่อภารกิจและผลประกอบการ
  - ดำเนินการเพื่อสร้างความตระหนักในปัญหาความเสี่ยงให้เกิดการรับรู้ทั่วทั้งองค์กร
  - เข้าใจผลกระทบที่อาจมีต่อความมั่นใจของผู้ที่ได้รับผลกระทบ
  - ให้แน่ใจว่ากระบวนการบริหารความเสี่ยงกาลังเป็นไปอย่างได้ผล
  - ออกนโยบายบริหารความเสี่ยงและความรับผิดชอบของหน่วยงานและบุคลากรต่างๆในการบริหารความเสี่ยง
- **หัวหน้ากลุ่มงาน** ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น
  - ตระหนักในความเสี่ยงอันเกี่ยวข้องกับภาระหน้าที่ของตน ผลกระทบที่อาจมีต่อหน่วยงานอื่น หรือกิจกรรมอื่นในองค์กร
  - มีดัชนีชี้วัดสมรรถนะของกิจกรรมในหน่วยงานเพื่อดูว่าระบบงานของตนเองได้รับผลกระทบจากความเสี่ยงมากน้อยเพียงใด
  - รายงานผลกระทบจากความเสี่ยงในกรณีเกิดหรือจะเกิดเหตุและเสนอแนะแนวทางในการแก้ไข
  - รายงานความเสี่ยงใดๆที่เกิดใหม่หรือความล้มเหลวใดๆ ในมาตรการการควบคุมหรือป้องกันสารสนเทศที่มีอยู่

- **ผู้ปฏิบัติงาน** ควรได้ข้อมูลการรายงานเพื่อวัตถุประสงค์ดังต่อไปนี้ เช่น
  - เข้าใจบทบาทภาระหน้าที่และความรับผิดชอบในความเสี่ยงแต่ละรายการ
  - เข้าใจบทบาทในการดำเนินการพัฒนาอย่างต่อเนื่องด้านการบริหารความเสี่ยง
  - เข้าใจการบริหารความเสี่ยงและความตระหนักต่อความเสี่ยงในการเป็นวัฒนธรรมองค์กรที่สำคัญอย่างหนึ่ง

๒.๑๓ ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์ของกรมการปกครอง ได้พัฒนาอย่างต่อเนื่อง เพื่อให้การทำงานผ่านระบบเครือข่ายคอมพิวเตอร์ของกรมการปกครอง เป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยศูนย์สารสนเทศเพื่อการบริหารงานปกครอง ตั้งอยู่ที่ ๔๔๒ วังไชยา อาคาร ๓ ชั้น ๒ ถนนนครสวรรค์ แขวงสี่แยกมหานาค เขตดุสิต กรุงเทพฯ ๑๐๓๐๐ และมีเครือข่ายเชื่อมโยงไปยังหน่วยงานในส่วนกลางในหลายสถานที่ ทั้ง กรมการปกครอง คลองหลอด , สำนักบริหารการทะเบียน คลอง ๙ , วิทยาลัยปกครอง คลอง ๖ และสำนักอาสารักษาดินแดน พหลโยธิน เพื่อการสื่อสารข้อมูลคอมพิวเตอร์หรือการสื่อสารรูปแบบอื่นในอนาคต ระบบเครือข่ายคอมพิวเตอร์ กรมการปกครอง มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ทำงานร่วมกันเพื่อป้องกันการโจมตีและบุกรุกเข้ามายังระบบเครือข่าย โดยในส่วนของฮาร์ดแวร์มีการกำหนดมาตรการ (Policy) ผ่านอุปกรณ์ Firewall ซึ่งใช้ในการกรองกลุ่มของข้อมูล (Package Filter) ที่ผ่านเข้ามาภายในระบบเครือข่ายคอมพิวเตอร์ส่วนกลางของ กรมการปกครอง จากเครือข่ายภายนอก เช่น เครือข่ายอินเทอร์เน็ต เป็นต้น

นอกจากนั้นยังมีการกำหนดมาตรการ (Policy) ให้ทำหน้าที่ป้องกันการบุกรุกในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Network Operation Center : NOC) ที่ดูแลเครื่องแม่ข่ายทั้งหมดของกรมการปกครอง ให้บุคคลภายนอกเข้าถึงได้เช่น Web Server และ Mail Server เป็นต้น รวมถึงการใช้โปรแกรมป้องกันไวรัสแบบClient-Server ในการตรวจสอบเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของกรมการปกครอง เพื่อให้ได้รับความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด



รูปภาพ ผังเครือข่ายห้อง Network Operation Center : NOC และการเชื่อมต่ออุปกรณ์ต่างๆ

บทที่ ๓

การวิเคราะห์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการปกครอง

กรมการปกครองได้ตระหนักถึงความสำคัญของข้อมูลที่อาจประสบกับความเสียหายจากปัจจัยเสี่ยงต่างๆ จึงมอบหมายให้ศูนย์สารสนเทศเพื่อการบริหารงานปกครอง (ศสป.) ทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ปค. ประจำปี พ.ศ. ๒๕๖๗ ให้สอดคล้องกับแผนปฏิบัติการด้านดิจิทัลของกรมการปกครอง (พ.ศ. ๒๕๖๖ - ๒๕๖๘) โดยกระบวนการบริหารจัดการความเสี่ยงของหน่วยงานเริ่มต้นจากการรวบรวมข้อมูลที่เกี่ยวข้องกับกิจกรรม/ปัจจัยเสี่ยง หรือกระบวนงานที่มีผลต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ และทำการศึกษาข้อมูล ระดมความคิดเห็นร่วมกับผู้ปฏิบัติงานด้านกิจกรรมนั้นๆ

การวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมการปกครอง จัดทำตารางประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เกิดขึ้น หรือมีโอกาสเกิดขึ้นได้ เพื่อหาผลกระทบและดำเนินการ หาวิธีจัดการความเสี่ยงที่เกิดขึ้น

๓.๑ การวิเคราะห์รายการความเสี่ยง

๓.๑.๑ ปัญหาจากผู้ใช้งาน (USER)
๓.๑.๒ ฮาร์ดแวร์ และซอฟต์แวร์ใช้งานไม่ได้ตามประสิทธิภาพ
๓.๑.๓ การแฮกเข้าระบบ และการโจมตีของไวรัส
๓.๑.๔ เหตุที่นอกเหนือจากการคาดหมาย
๓.๑.๕ ผู้ดูแลระบบไม่สามารถบริหารจัดการระบบได้อย่างต่อเนื่อง
๓.๑.๖ ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ
๓.๑.๗ ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร
๓.๑.๘ ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ
๓.๑.๙ ความเสี่ยงจากการโจรกรรม เครื่องคอมพิวเตอร์และอุปกรณ์

ตารางการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมการปกครอง

รายการความเสี่ยง	ที่มา (Cause)	ผลกระทบ/ผู้ได้รับผลกระทบ	วิธีการจัดการความเสี่ยง	กิจกรรมรองรับ	ตัวชี้วัด
ปัญหาจากผู้ใช้งาน (USER)	ผู้ใช้ลงซอฟท์แวร์ที่ไม่จำเป็นในการใช้งาน ทำให้มีผลกระทบต่อเครือข่าย	เกิดความขัดข้องไปสู่ระบบล่มได้	การควบคุมความเสี่ยง (Treat)	ออกมาตรการการใช้อุปกรณ์คอมพิวเตอร์ และตรวจดูประสิทธิภาพปริมาณการใช้งาน (Load) ผ่านช่องทางเครือข่าย (Traffic)	มาตรการในการจำกัดการลงโปรแกรม
	ผู้ใช้ใช้งานระบบเครือข่ายในส่วนที่นอกเหนือจากงานราชการ ทำให้ประสิทธิภาพลดลง	ประสิทธิภาพของระบบลดลง	การควบคุมความเสี่ยง (Treat)	วางระบบอินเตอร์เน็ตแยกระหว่างการใช้งานอินเตอร์เน็ตทั่วไป และระบบงานหลักของกรมการปกครอง	รายงานการใช้งาน
	ผู้ใช้มีความหละหลวมต่อการระวังในการใช้สิทธิที่กำหนดไว้ ซึ่งมีการมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน	ข้อมูลสูญหาย หรือได้รับการเปลี่ยนแปลง	การยอมรับความเสี่ยง (Take)	ตั้งระยะเวลา user ให้เปลี่ยน password ใหม่ทุก ๓ เดือน	มาตรการการใช้งานระบบ
	ผู้ใช้ใช้อุปกรณ์ต่อพ่วงที่มีไวรัส	ไวรัสเข้าสู่ระบบทำให้ข้อมูลสูญหายหรือทำลายระบบ	การควบคุมความเสี่ยง (Treat)	มีการติดตั้งระบบป้องกันไวรัส และอับเดตอย่างสม่ำเสมอ	รายงานหรือขั้นตอนการปฏิบัติงาน
ฮาร์ดแวร์ และซอฟต์แวร์ใช้งานไม่ได้ตามประสิทธิภาพ	ซอฟต์แวร์มีความล้าสมัย	เกิดการขัดข้องของระบบ และมีประสิทธิภาพการใช้งานลดลง จนอาจทำให้ระบบล่ม	การถ่ายโอนความเสี่ยง (Transfer)	มีการต่ออายุการรับประกันอย่างต่อเนื่อง	สัญญาการบำรุงรักษาและสัญญาการรับประกัน

รายการความเสี่ยง	ที่มา (Cause)	ผลกระทบ/ผู้ได้รับผลกระทบ	วิธีการจัดการความเสี่ยง	กิจกรรมรองรับ	ตัวชี้วัด
	การปรับปรุงรุ่นเวอร์ชัน หรือเฟิร์มแวร์ของบริษัทผู้ผลิต/ผู้ให้บริการ ทำให้เกิดความไม่เข้ากันกันระบบที่มีอยู่เดิม	ทำให้การเข้าใช้งานระบบได้ช้าลงหรือเข้าใช้งานไม่ได้	การควบคุมความเสี่ยง (Treat)	มีการติดตามข่าวสารของผู้ผลิตซอฟต์แวร์อย่างสม่ำเสมอ เพื่อตรวจสอบและอัปเดต	รายงานผล
การแฮกเข้าระบบ และการโจมตีของไวรัส	เนื่องจากเป็นหน่วยงานรัฐ และเป็นเป้าหมายโจมตีของแฮกเกอร์	ทำให้ระบบล่ม ข้อมูลหาย	การควบคุมความเสี่ยง (Treat)	มีระบบไฟร์วอลล์ (Firewall) ระบบป้องกันไวรัส และ ระบบ Web Application Firewall (WAF) โดยต้องทำการปรับปรุงค่ากำหนดด้านมาตรฐานความปลอดภัย	รายงานการปรับปรุงระบบ
			การยอมรับความเสี่ยง (Take)	มีมาตรการในการสำรองข้อมูล	มาตรการการสำรองข้อมูลเป็นประจำ

รายการความเสี่ยง	ที่มา (Cause)	ผลกระทบ/ผู้ได้รับผลกระทบ	วิธีการจัดการความเสี่ยง	กิจกรรมรองรับ	ตัวชี้วัด
เหตุที่นอกเหนือจากการคาดหมาย	ไฟฟ้าดับ ไฟกระชาก	คอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือ เมื่อกระแสไฟฟ้าขัดข้อง ทำให้เครื่องแม่ข่ายคอมพิวเตอร์ถูกปิดไปโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถใช้งานได้	การยอมรับความเสี่ยง (Take)	มีคู่มือในการติดต่อประสานงานหน่วยที่เกี่ยวข้อง และจัดให้มีเครื่องสำรองไฟ	คู่มือการดำเนินการด้านการรักษาความปลอดภัยในสถานที่ราชการ
	สัตว์กัดแทะอุปกรณ์และสายส่งระบบ	ระบบล่ม	การถ่ายโอนความเสี่ยง (Transfer)	ประสานบริษัทเข้ามาดูแลเรื่องสัตว์กัดแทะ	รายงานการตรวจเช็ค
	ไฟไหม้ น้ำท่วม เกิดจลาจล อาคารถล่ม	เจ้าหน้าที่เข้ามาแก้ไขไม่ได้ ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ทำให้ได้รับความเสียหายทั้งหมด	การควบคุมความเสี่ยง (Treat)	พิจารณาจัดทำโครงการจัดหา DR Site	สัญญาจ้าง / ประสานหน่วยงานภายในที่มีห้อง Data Center
	ระบบเครือข่ายสื่อสารหลักที่เชื่อมต่อจากภายนอกขัดข้อง	ไม่สามารถใช้งานระบบทั้งหมดได้	การควบคุมความเสี่ยง (Treat)	ตรวจสอบปัญหาเบื่องต้น / จัดทำรายละเอียดในการติดต่อประสานงานหน่วยที่เกี่ยวข้อง	คู่มือการตรวจสอบปัญหา และรายชื่อผู้ประสานงาน

รายการความเสี่ยง	ที่มา (Cause)	ผลกระทบ/ผู้ได้รับผลกระทบ	วิธีการจัดการความเสี่ยง	กิจกรรมรองรับ	ตัวชี้วัด
ผู้ดูแลระบบไม่สามารถบริหารจัดการระบบได้อย่างต่อเนื่อง	บุคลากรไม่เพียงพอ	ไม่สามารถแก้ไขได้ทันเวลา ทำให้การทำงานอาจหยุดชะงัก หากบุคลากรผู้รับผิดชอบไม่สามารถมาปฏิบัติงานได้และจำนวนบุคลากรที่มีไม่เพียงพอต่อระบบเทคโนโลยีสารสนเทศที่เพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลกระทบต่อการพัฒนาและควบคุมดูแลระบบ	การหลีกเลี่ยงความเสี่ยง (Terminate)	จัดทำระบบรับเรื่องการแจ้งซ่อมการแก้ไขระบบ	ระบบรับแจ้งปัญหา / ใบรับแจ้งปัญหา
	ผู้ดูแลระบบมีความรู้ไม่เพียงพอ	ทำให้การเข้าใช้งานระบบได้ช้าลงหรือเข้าใช้งานไม่ได้	การควบคุมความเสี่ยง (Treat)	วางแผนการจัดอบรม	การเข้าฝึกหลักสูตรอบรมเฉพาะทาง
	ผู้ดูแลระบบไม่ทำตามขั้นตอนที่กำหนดไว้	เมื่อมีความผิดพลาดเกิดขึ้นจะทำให้ติดตามหาสาเหตุได้ยาก	การควบคุมความเสี่ยง (Treat)	มีคู่มือปฏิบัติงาน	คู่มือปฏิบัติงาน
	บริษัทที่ดูแลระบบไม่สามารถมาดำเนินการให้ทันเวลา	ไม่สามารถแก้ไขได้ทันเวลา ทำให้การทำงานอาจหยุดชะงัก	การถ่ายโอนความเสี่ยง (Transfer)	ใช้มาตรการบริหารสัญญาให้มีประสิทธิภาพ	รายงานการเข้าทำงานช้าของบริษัท

รายการความเสี่ยง	ที่มา (Cause)	ผลกระทบ/ผู้ได้รับผลกระทบ	วิธีการจัดการความเสี่ยง	กิจกรรมรองรับ	ตัวชี้วัด
ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	การเปลี่ยนแปลงผู้บริหาร	อาจทำให้นโยบายการบริหารจัดการสารสนเทศเปลี่ยนแปลงด้วย ทำให้การดำเนินการโครงการต่างๆ ได้รับผลกระทบ	การหลีกเลี่ยงความเสี่ยง (Terminate)	แผนแม่บทด้าน ICT ระยะยาว	แผนแม่บท ICT
ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	การขาดแคลนงบประมาณในการดำเนินการ	ทำให้ระบบสารสนเทศไม่สามารถดำเนินการได้ต่อเนื่องอย่างมีประสิทธิภาพ	การหลีกเลี่ยงความเสี่ยง (Terminate)	แผนงานงบประมาณระยะยาว	แผนงบประมาณ
ความเสี่ยงจากการโจรกรรมเครื่องคอมพิวเตอร์และอุปกรณ์	การโจรกรรมเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือชิ้นส่วนอุปกรณ์ภายในเครื่องคอมพิวเตอร์ เช่น CPU Hard disk และ Memory	ทำให้ไม่สามารถปฏิบัติงาน หรือเกิดการสูญหายของข้อมูลบนเครื่องคอมพิวเตอร์นั้นได้	การควบคุมความเสี่ยง (Treat)	มีระบบตรวจเช็คบำรุงรักษาตามอายุงาน รวมทั้งมีกล้องรักษาความปลอดภัยในอาคาร	ตารางการตรวจเช็ค

ตารางการประเมินความรุนแรงของความเสี่ยงด้านเทคโนโลยีสารสนเทศกรมการปกครอง

ลำดับที่	รายการความเสี่ยง	ระดับโอกาสในการเกิดเหตุการณ์	ระดับความรุนแรงของผลกระทบ	คะแนน
๑	ปัญหาจากผู้ใช้งาน (USER)	๕	๒	๑๐
๒	ฮาร์ดแวร์ และซอฟต์แวร์ใช้งานไม่ได้ตามประสิทธิภาพ	๓	๓	๙
๓	การแฮกเข้าระบบ และการโจมตีของไวรัส	๕	๕	๒๕
๔	เหตุที่นอกเหนือจากการคาดหมาย	๑	๕	๕
๕	ผู้ดูแลระบบไม่สามารถบริหารจัดการระบบได้อย่างต่อเนื่อง	๓	๔	๑๒
๖	ความเสี่ยงจากการนำเอาอุปกรณ์อื่นที่ไม่ได้รับอนุญาตมาเชื่อมต่อ	๕	๔	๒๐
๗	ความเสี่ยงจากการเปลี่ยนแปลงนโยบายผู้บริหาร	๑	๒	๒
๘	ความเสี่ยงต่อการได้รับการสนับสนุนงบประมาณไม่เพียงพอ	๕	๓	๑๕
๙	ความเสี่ยงจากการโจรกรรม เครื่องคอมพิวเตอร์และอุปกรณ์	๕	๔	๒๐

บทที่ ๔

บทสรุปและข้อเสนอแนะ

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (ICT Risk Management) เป็นการบริหารเพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศ มีการพัฒนาและใช้งานได้อย่างต่อเนื่อง เพื่อสนับสนุนภารกิจของหน่วยงานภายในองค์กร ช่วยป้องกันหรือลดเหตุการณ์ที่จะทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารให้อยู่ในระดับที่สามารถ ยอมรับ ควบคุม และตรวจสอบได้อย่างมีระบบ ซึ่งการบริหารจัดการนอกจากผู้ปฏิบัติงานโดยตรงจะต้องรับทราบแล้ว ผู้บริหารควรได้รับทราบถึงความเสี่ยงในด้านต่างๆ เพื่อนำไปจัดการและวางแผนการบริหาร ให้กรมการปกครองดำเนินงานได้อย่างต่อเนื่องต่อไป

ในปัจจุบัน “ข้อมูล” ถือว่าเป็นทรัพย์สินอันทรงคุณค่ามหาศาลต่างตกอยู่ในสภาวะเสี่ยงต่อการถูกล่วงละเมิด ถูกทำให้เสียหายหรือเสียหาย และถูกนำไปใช้ในทางที่ผิด ทั้งจากบุคคลภายในและภายนอกองค์กรโดยเจตนาหรือไม่เจตนาก็ตาม ดังนั้น หนทางที่ดีที่สุดในการแก้ไขปัญหานี้จึงควรเริ่มตั้งแต่การบริหารจัดการองค์กรให้ได้มาตรฐานด้านความปลอดภัย ซึ่งก็คือ การจัดการวามเสี่ยงภายในองค์กรนั่นเอง

๔.๑ สรุป

แผนการบริหารความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ ได้ดำเนินการจัดทำเพื่อ

๔.๑.๑ เตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของกรมการปกครอง

๔.๑.๒ เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๔.๑.๓ ให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๔.๒ ข้อเสนอแนะ

๔.๒.๑ การควบคุมคุมนโยบายและกระบวนการปฏิบัติงานถือเป็นสำคัญ เพื่อให้มั่นใจว่าได้มีการจัดการความเสี่ยง ดังนั้น ควรมีการกำหนดบุคลากรภายในหน่วยงานเพื่อรับผิดชอบการควบคุมนั้น โดยบุคลากรแต่ละคนที่ได้รับมอบหมายในการควบคุมควรมีความรับผิดชอบ ดังนี้

- พิจารณาประสิทธิผลของการจัดการความเสี่ยงที่ได้ดำเนินการอยู่ในปัจจุบัน
- พิจารณาการปฏิบัติเพิ่มเติมที่จำเป็น เพื่อเพิ่มประสิทธิผลของการจัดการความเสี่ยงนั้น
- กำกับกิจกรรมลดความเสี่ยงให้แล้วเสร็จตามกำหนดวันตามแผนที่วางไว้

๔.๒.๒ การติดตามการบริหารความเสี่ยงเพื่อให้มั่นใจว่าการจัดการความเสี่ยงมีคุณภาพและมีความเหมาะสม ดังนั้น จึงควรมีการติดตามการบริหารความเสี่ยงอย่างต่อเนื่องและดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงที และถือเป็นส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ถึงปัญหาที่เกิดขึ้นและการแก้ไขอย่างถูกต้องได้อย่างมีประสิทธิภาพ