

RISK MANAGEMENT PLAN

MITIGATION PLAN & EXISTING CONTROL

แผนบริหารความเสี่ยง (แผนจัดการความเสี่ยง และแผนการควบคุมภายใน)

ประจำปีงบประมาณ พ.ศ. 2570



สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
Digital Government Development Agency
(Public Organization)

จัดทำโดย ส่วนบริหารความเสี่ยงและควบคุมภายใน (CSR)
ฝ่ายกลยุทธ์องค์กร

 csr_division@dga.or.th



บทสรุปผู้บริหาร

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร. ได้ดำเนินการบริหารความเสี่ยงตามนโยบาย และคู่มือบริหารความเสี่ยง ของสำนักงานพัฒนารัฐบาลดิจิทัล ประจำปีงบประมาณ พ.ศ. 2570 เพื่อใช้เป็นแนวทางในการปฏิบัติเรื่องการบริหารความเสี่ยงขององค์กร โดยมีวัตถุประสงค์เพื่อให้องค์กรมีความพร้อม ในการป้องกันความเสี่ยงที่จะกลายเป็นปัญหาในอนาคต ลดความเสียหาย และผลกระทบจากความเสี่ยง และเพิ่มโอกาสในการสร้างมูลค่าเพิ่มให้กับองค์กร ซึ่งการบริหารความเสี่ยงของ สพร. จะแบ่งออกเป็น 2 ระดับ คือ

1. ความเสี่ยงระดับองค์กร และความเสี่ยงระดับฝ่าย/ส่วนงาน ซึ่งในส่วนของความเสี่ยงระดับองค์กร จะมีการรวบรวมติดตามผลการบริหารความเสี่ยง จากเจ้าของความเสี่ยง (Risk Owner) โดยส่วนบริหารความเสี่ยงและควบคุมภายใน ฝ่ายกลยุทธ์องค์กร แล้วนำเสนอต่อฝ่ายบริหาร คณะอนุกรรมการด้านการบริหารความเสี่ยงและควบคุมภายใน และคณะกรรมการ สพร. เพื่อพิจารณาผลการบริหารความเสี่ยง พร้อมทั้งให้ข้อเสนอแนะ เพื่อให้ความเสี่ยงอยู่ในระดับที่องค์กร สามารถยอมรับได้
2. ความเสี่ยงระดับฝ่าย/ส่วนงาน จะมีผู้ประสานงานด้านการบริหารความเสี่ยง (Risk Agent) ของแต่ละ ฝ่าย/ส่วนงาน ทำหน้าที่ในการติดตามและรายงานผลการบริหารความเสี่ยง เพื่อเสนอต่อ ผู้อำนวยการฝ่ายพิจารณาสั่งการเพื่อให้การดำเนินงานอยู่ในระดับความเสี่ยงที่ฝ่าย/ส่วนงาน ยอมรับได้

อย่างไรก็ตาม ในปีงบประมาณ พ.ศ. 2570 คณะอนุกรรมการด้านการบริหารความเสี่ยงและควบคุม ภายใน และคณะกรรมการ สพร. ได้เห็นชอบแผนการบริหารความเสี่ยงของสำนักงานพัฒนารัฐบาลดิจิทัล ประจำปี งบประมาณ พ.ศ. 2570 ซึ่งมีจำนวน 5 ประเภทความเสี่ยง 6 เหตุการณ์ความเสี่ยง ประกอบด้วย

ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

S1: การดำเนินงานโครงการสำคัญตามยุทธศาสตร์/นโยบายรัฐบาลไม่บรรลุเป้าหมาย

ความเสี่ยงด้านการดำเนินงาน (Operational Risk)

O1: สมรรถนะของบุคลากรอาจไม่เพียงพอต่อการขับเคลื่อนนโยบายสำคัญ

ความเสี่ยงด้านการเงิน (Financial Risk)

F1: การหารายได้และการบริหารต้นทุนไม่เป็นไปตามเป้าหมาย

ความเสี่ยงด้านกฎหมาย ระเบียบ (Compliance Risk)

C1: กระบวนการทำงานอาจไม่สามารถปรับตัวได้ทันต่อการเปลี่ยนแปลงของกฎหมาย หลักเกณฑ์ หรือ มาตรฐานที่สำคัญ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)

IT1: ระบบหรือข้อมูลสำคัญเผชิญภัยคุกคามทางไซเบอร์จนเกิดการหยุดชะงักหรือข้อมูลรั่วไหล

IT2: บริการดิจิทัลสำคัญไม่สามารถให้บริการได้ตามความต่อเนื่องที่กำหนด

ทั้งนี้ แผนการบริหารความเสี่ยงของสำนักงานพัฒนารัฐบาลดิจิทัล ประจำปีงบประมาณ พ.ศ. 2570 ได้มีการกำหนดฝ่าย/ส่วนงาน เจ้าของปัจจัยเสี่ยง, แผนจัดการความเสี่ยง และแผนการควบคุมภายใน, ค่าตัวชี้วัดการบริหารความเสี่ยง (KRI) เพื่อสะท้อนให้เห็นถึงผลการบริหารความเสี่ยง, ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ (Risk Appetite และ Risk Tolerance) รวมทั้งระดับความรุนแรงของความเสี่ยงก่อนบริหาร และระดับความรุนแรงของความเสี่ยงที่คาดหวังหลังการบริหารความเสี่ยง เพื่อให้การบริหารความเสี่ยงดังกล่าวบรรลุวัตถุประสงค์และเป้าหมายขององค์กร ต่อไป

สารบัญ

1. กระบวนการจัดทำแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยงและแผนการควบคุมภายใน) ของสำนักงานพัฒนารัฐบาลดิจิทัล ประจำปีงบประมาณ พ.ศ. 2570	1
2. กระบวนการจัดทำแผนบริหารความเสี่ยง	4
2.1 การระบุปัจจัยเสี่ยง (Risk Identification)	4
2.2 การวิเคราะห์ความเสี่ยง (Risk Analysis)	5
2.3 การประเมินความเสี่ยง (Risk Evaluation)	12
3. ความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) ของรายการความเสี่ยง	31

1. กระบวนการจัดทำแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยงและแผนการควบคุมภายใน) ของสำนักงานพัฒนารัฐบาลดิจิทัล ประจำปีงบประมาณ พ.ศ. 2570

ตามที่ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) ได้วางระบบการบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ. 2570 ซึ่งเป็นไปตามพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 หมวด 4 การบัญชี การรายงาน และการตรวจสอบ มาตรา 79 บัญญัติให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายใน และการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามหลักเกณฑ์กระทรวงการคลังว่าด้วย มาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 และหลักเกณฑ์ กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 รวมทั้ง กรอบแนวทาง COSO ERM 2017: Enterprise Risk Management Integrated Framework มาตรฐาน ISO 27001: 2022 และมาตรฐาน ISO 27701: 2019

ดังนั้น เพื่อให้การดำเนินการบริหารความเสี่ยงของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) มีความต่อเนื่องและสอดคล้องตามมาตรฐานและหลักเกณฑ์ฯ ดังกล่าว รวมถึงสอดคล้องกับกรอบ การประเมินองค์การมหาชนประจำปีงบประมาณ พ.ศ. 2569 ตามกลไกและขั้นตอนการประเมินองค์ประกอบที่ 2 ตัวชี้วัดที่ 2.3 การควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน ประเด็นการประเมินการควบคุมภายใน และการบริหารความเสี่ยง ซึ่งมีการระบุให้คณะกรรมการพิจารณาแผนและรายงานผลการควบคุมภายใน และการบริหารความเสี่ยง

ฝ่ายกลยุทธ์องค์กร โดยส่วนบริหารความเสี่ยงและควบคุมภายใน จึงได้ดำเนินการจัดทำแผนบริหาร ความเสี่ยง (แผนจัดการความเสี่ยงและแผนการควบคุมภายใน) ของปัจจัยเสี่ยงระดับองค์กร ของสำนักงานพัฒนา รัฐบาลดิจิทัล (องค์การมหาชน) ประจำปีงบประมาณ พ.ศ. 2570 เพื่อใช้เป็นกรอบแนวทางการดำเนินงานด้านการ บริหารความเสี่ยงและการควบคุมภายใน ให้ดำเนินงานเป็นไปอย่างมีประสิทธิภาพ ภายใต้การกำกับดูแลกิจการที่ดี และนำไปสู่การลดความเสี่ยงขององค์กร ตามกระบวนการ ดังนี้

1. ส่วนบริหารความเสี่ยงและควบคุมภายในทำการศึกษาและวิเคราะห์ข้อมูล ระหว่างวันที่ 1 – 31 กรกฎาคม 2569 เพื่อจัดทำและสรุปประเด็นความเสี่ยง เหตุการณ์ความเสี่ยง และปัจจัยเสี่ยงจากแหล่งต่างๆ (Risk Universe) ประกอบด้วย

1. กฎหมายที่เกี่ยวข้อง	■ พ.ร.ฎ. จัดตั้งสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) พ.ศ. 2561 ■ พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ■ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรอง ■ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายลำดับรอง ■ พ.ร.บ. การอำนวยความสะดวกในการพิจารณาอนุญาตและให้บริการแก่ประชาชน พ.ศ. 2569 ■ พ.ร.บ. การเปิดเผยข้อมูลข่าวสารส่วนบุคคลฯ พ.ศ. 2569
------------------------	--

2. แผนระดับชาติที่เกี่ยวข้อง และนโยบายรัฐบาล	■ แผนยุทธศาสตร์ชาติ 20 ปี (ระยะที่ 2 ปี พ.ศ. 2566 – 2570) ■ แผนแม่บท ภายใต้แผนยุทธศาสตร์ชาติ ■ (ร่าง) แผนพัฒนาการเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 14 ■ แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย (พ.ศ. 2570 - 2575) ■ แผนปฏิบัติการด้านปัญญาประดิษฐ์แห่งชาติฯ (พ.ศ. 2565-2570) ■ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) ■ (ร่าง) แผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม 2561-2580 (ฉบับปรับปรุง) ■ คำแถลงนโยบายของคณะรัฐมนตรี (นายกรัฐมนตรี นายอนุทิน ชาญวีรกูล)
3. นโยบายคณะกรรมการ/ ผู้บริหาร/อนุกรรมการด้าน การบริหารความเสี่ยงและ ควบคุมภายใน	■ ให้ความสำคัญกับการดำเนินงานในโครงการสำคัญ เช่น การพัฒนา Super App, GDX, AI เป็นต้น ■ พัฒนากลไกการเชื่อมโยงการทำงานแบบ GRC (Governance-Risk Management-Compliance) ■ ผลักดันการขับเคลื่อนงานสำหรับเตรียมความพร้อมเข้าเป็นสมาชิก OECD ■ วางแผนการใช้ทรัพยากร (Resource planning) สำหรับดำเนินโครงการต่าง ๆ
4. ยุทธศาสตร์องค์กร	(ร่าง) กรอบแผนปฏิบัติการ พ.ศ. 2570-2575 ของ สพร. ■ สร้างประสบการณ์บริการภาครัฐให้เชื่อมโยงเป็นหนึ่งเดียว ■ พัฒนาโครงสร้างพื้นฐานดิจิทัลสาธารณะและบริการพื้นฐานกลางภาครัฐ ■ ขับเคลื่อนภาครัฐด้วยข้อมูลและปัญญาประดิษฐ์อย่างมีธรรมาภิบาล ■ เสริมสร้างขีดความสามารถของระบบสนับสนุนดิจิทัลภาครัฐ ■ พัฒนา สพร. ศูนย์การดิจิทัลอัจฉริยะ
5. Supply chain	■ Core Business Process 14 กระบวนการ ■ Supporting Process 10 กระบวนการ ■ Standard & Law & Compliance & Monitor & Evaluate 12 กระบวนการ
6. ตัวชี้วัดของ ก.พ.ร.	กรอบประเมินองค์การมหาชน พ.ศ. 2569-2570 ■ องค์ประกอบที่ 1 การประเมินประสิทธิภาพ ประสิทธิผลของการดำเนินงาน ■ องค์ประกอบที่ 2 การประเมินศักยภาพขององค์การมหาชน

7. กระบวนการปฏิบัติงาน/ ความเสี่ยงส่วนงาน	ผลประโยชน์ความเพียงพอของการควบคุมภายใน และการวิเคราะห์ความเสี่ยง ■ การดำเนินงานเพื่อตอบสนองต่อการขับเคลื่อนแผนพัฒนารัฐบาลดิจิทัล ■ การประยุกต์ใช้ AI ในการทำงานอย่างปลอดภัย ■ ความเสี่ยงต่อการรั่วไหลของข้อมูลส่วนบุคคล ■ การบริหารจัดการสิทธิในการใช้งานระบบ
8. ปัจจัยเสี่ยงปี 2569	ความเสี่ยงที่ต้องเฝ้าระวังอย่างต่อเนื่อง O2: การบริหารทรัพยากรบุคคลไม่สามารถสนับสนุนการดำเนินงานตามนโยบาย F1: การหารายได้และการบริหารต้นทุนไม่เป็นไปตามเป้าหมาย C1: กระบวนการทำงานอาจจะไม่สอดคล้องกับกฎหมาย IT1: ระบบสารสนเทศที่สำคัญของสำนักงานอาจถูกบุกรุก/โจมตีความมั่นคงปลอดภัย IT2: การให้บริการประชาชนอาจจะไม่เป็นไปตาม SLA

2. ส่วนบริหารความเสี่ยงและควบคุมภายใน ประเมินความเสี่ยง และจัดลำดับความรุนแรงของความเสี่ยง เพื่อนำเสนอต่อผู้บริหาร เมื่อวันที่ 11 สิงหาคม 2568 เพื่อพิจารณาคัดเลือกประเด็นความเสี่ยงที่สำคัญสำหรับนำมาใช้ในการกำหนดปัจจัยเสี่ยงระดับองค์กร

3. จัดอบรมเชิงปฏิบัติการเพื่อจัดทำแผนบริหารความเสี่ยงองค์กร ประจำปีงบประมาณ พ.ศ. 2570 กับผู้รับผิดชอบซึ่งเป็นเจ้าของปัจจัยเสี่ยง (Risk Owner) ระหว่างวันที่ 19 – 31 สิงหาคม 2569 ในรูปแบบ Focus Group เพื่อจัดทำแผนจัดการความเสี่ยง และแผนการควบคุมภายใน โดยใช้กรอบการวิเคราะห์ PMBOK และ Bow-Tie Diagram เพื่อปรับปรุงมาตรการการควบคุมภายใน รวมทั้งลดโอกาสเกิดความเสี่ยง และลดผลกระทบหรือความเสียหายของเหตุการณ์ความเสี่ยง

4. นำเสนอแผนบริหารความเสี่ยง ของ สพร. ประจำปีงบประมาณ พ.ศ. 2570 ต่อผู้บริหารระดับสูง เพื่อพิจารณาให้ความเห็นชอบก่อนนำเสนอต่อคณะกรรมการด้านการบริหารความเสี่ยงและควบคุมภายใน พิจารณาให้ความเห็นชอบ เมื่อวันที่ 14 กันยายน 2569

5. นำเสนอแผนบริหารความเสี่ยง ของ สพร. ประจำปีงบประมาณ พ.ศ. 2570 ต่อคณะกรรมการด้านการบริหารความเสี่ยงและควบคุมภายใน พิจารณาให้ความเห็นชอบ เมื่อวันที่ 24 กันยายน 2569 ก่อนนำเสนอต่อคณะกรรมการ สพร.

6. นำเสนอแผนบริหารความเสี่ยง (แผนจัดการความเสี่ยง และแผนการควบคุมภายใน) ของสำนักงานพัฒนารัฐบาลดิจิทัล ประจำปีงบประมาณ พ.ศ. 2570 ต่อคณะกรรมการ สพร. พิจารณา และให้ความเห็นชอบ ในการประชุมคณะกรรมการ สพร. ครั้งที่ 9/2569 เมื่อวันที่ 28 กันยายน 2569

2. กระบวนการจัดทำแผนบริหารความเสี่ยง



2.1 การระบุปัจจัยเสี่ยง (Risk Identification)

สพร. ได้นำแหล่งที่มาของความเสี่ยง (Risk Universe) มาประเมินร่วมกับการวิเคราะห์ปัจจัยภายนอกและการวิเคราะห์ปัจจัยภายในมากำหนดเหตุการณ์ความเสี่ยงที่สำคัญ (Key Risk) รวมทั้งผลกระทบ หรือความสูญเสียที่อาจเกิดขึ้นกับองค์กร โดยมีหลักในการกำหนดปัจจัยเสี่ยงระดับองค์กร ดังนี้

1. เป็นเหตุการณ์สำคัญ (Key Success/Failure Factors)
2. ไม่ใช่ข้อเท็จจริง และมีความไม่แน่นอน (Uncertainty)
3. ส่งผลกระทบต่อองค์กรอย่างมีนัยสำคัญ ต่อวัตถุประสงค์/เป้าหมาย

2.2 การวิเคราะห์ความเสี่ยง (Risk Analysis)

จากการกำหนดเหตุการณ์ความเสี่ยงที่สำคัญ (Key Risk) รวมทั้งผลกระทบ หรือความสูญเสียที่อาจเกิดขึ้นกับองค์กร พบว่า สพร. มี 6 เหตุการณ์ความเสี่ยงที่สำคัญ และเมื่อนำมาวิเคราะห์ความเสี่ยง เพื่อประเมินความเพียงพอของการควบคุมภายใน โดยใช้กรอบ PMBOK ในการวิเคราะห์ความเสี่ยง S1 ที่มีลักษณะการติดตามโครงการสำคัญ และ Bow-tie Diagram สำหรับความเสี่ยงอื่น และทั้ง 6 เหตุการณ์ความเสี่ยงที่สำคัญ ยังคงมีความเสี่ยงที่ยังเหลืออยู่ (Residual Risk) ดังนี้

เหตุการณ์ความเสี่ยง (Key Risk)	การควบคุมภายในที่มีอยู่ (Existing Control)	ความเสี่ยงที่ยังคงเหลือ (Residual Risk)	
		ปัจจัยภายใน (Internal)	ปัจจัยภายนอก (External)
1. S1: การดำเนินงาน โครงการสำคัญตาม ยุทธศาสตร์/นโยบายรัฐบาล ไม่บรรลุเป้าหมาย		ศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX) - เจ้าหน้าที่ไม่เพียงพอกับความ เร่งด่วนของโครงการ	- หน่วยงานมีข้อกังวลถึงความไม่สอดคล้องกับกฎหมาย PDPA - กระบวนการภายในของหน่วยงานมีความล่าช้า - หน่วยงานขาดความพร้อมในการเชื่อมโยงข้อมูล

เหตุการณ์ความเสี่ยง (Key Risk)	การควบคุมภายในที่มีอยู่ (Existing Control)	ความเสี่ยงที่ยังคงเหลือ (Residual Risk)	
		ปัจจัยภายใน (Internal)	ปัจจัยภายนอก (External)
		AI Data Verification and Government Process Automation Platform - ขั้นตอนหรือเอกสารการดำเนินงานของระบบอาจไม่สอดคล้องกับกฎหมายสำคัญ - เกิดเหตุละเมิดแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลจากการดำเนินงาน - เกิดปัญหาการ Maintain จากการเปลี่ยน vendor หรือ model AI	- ข้อมูล (Knowledge) ที่ใช้สำหรับฝึกฝน AI ไม่สมบูรณ์หรือไม่มีคุณภาพ - การดำเนินงานของผู้รับจ้างประสบปัญหาจนกระทบต่อแผนการดำเนินงาน - หน่วยงานภายนอกขาดความพร้อมในการปรับปรุงเพื่อเชื่อมต่อบระบบ - หน่วยงานผู้ให้บริการมีจำนวนการใช้งานสูงกว่าที่คาดการณ์ไว้ - หน่วยงานไม่สามารถใช้บริการแพลตฟอร์มได้ตามเป้าหมาย

เหตุการณ์ความเสี่ยง (Key Risk)	การควบคุมภายในที่มีอยู่ (Existing Control)	ความเสี่ยงที่ยังคงเหลือ (Residual Risk)	
		ปัจจัยภายใน (Internal)	ปัจจัยภายนอก (External)
		ท้องถิ่นดิจิทัล - ระบบไม่ตอบโจทย์ความคาดหวัง ของหน่วยงานท้องถิ่นผู้ใช้งานและ ประชาชนผู้รับบริการ - จำนวนข้อสอบถาม, ร้องเรียน, แจ้ง ปัญหาที่มีจำนวนมาก จนไม่สามารถ แก้ไขได้จนกระทบต่อความพึงพอใจ	- โครงการขาดแนวทางการขับเคลื่อนที่จำเป็นสำหรับการ ขยายผลตามเป้าหมาย - หน่วยงานท้องถิ่นไม่มีความ พร้อมในการนำระบบไปใช้งาน - หน่วยงานท้องถิ่นไม่ทราบถึง โครงการทำให้ไม่สามารถขยาย ผลได้ตามเป้าหมายที่กำหนดไว้
2. O1: สมรรถนะของ บุคลากรอาจไม่เพียงพอต่อ การขับเคลื่อนนโยบายสำคัญ	- มีนโยบายการทำงาน Hybrid Workforce & Flexible Work ต่อเนื่อง - มีระบบพื้นฐานที่สนับสนุนการทำงาน นอกสถานที่ตั้งของสำนักงาน (Work from Home) - มีการดำเนินงานตามแผนปฏิบัติงาน ทรัพยากรบุคคล	- เส้นทางความก้าวหน้า (Career Path) อาจไม่สอดคล้องกับบริบท การทำงานในปัจจุบัน - การเรียนรู้ทักษะทางเทคโนโลยี ใหม่ๆ ของเจ้าหน้าที่ไม่ทันต่อการ นำมาใช้ในการทำงานให้เกิด ประสิทธิภาพ - แนวทางการปฏิบัติงานหากรัฐบาล มีมติยกเลิกการ WFH	- ตลาดแรงงานด้านดิจิทัล มี การแข่งขันสูง โครงสร้าง เงินเดือนไม่สามารถดึงดูด บุคลากรที่มีทักษะสูงด้าน ดิจิทัล - การเปลี่ยนแปลงทาง เทคโนโลยีดิจิทัลของโลกยุคใหม่ เช่น AI Tools /Cyber

เหตุการณ์ความเสี่ยง (Key Risk)	การควบคุมภายในที่มีอยู่ (Existing Control)	ความเสี่ยงที่ยังคงเหลือ (Residual Risk)	
		ปัจจัยภายใน (Internal)	ปัจจัยภายนอก (External)
	- มีระเบียบการจัดสวัสดิการ ประโยชน์ เกื้อกูล และผลประโยชน์อื่น ๆ แก่ เจ้าหน้าที่ที่อยู่ในระดับต้นๆ ขององค์การมหาชน		
3. F1: การหารายได้และการบริหารต้นทุนไม่เป็นไปตามเป้าหมาย	- มีการวิเคราะห์ต้นทุนและผลตอบแทนโครงการ ประกอบการขออนุมัติโครงการ - มีการจัดทำแผนหารายได้ประจำปี - มีการศึกษาบริการใหม่ ๆ ที่มีศักยภาพเพื่อหารายได้เพิ่มขึ้น - มีการจัดทำแผนรายได้รายเดือนและรายงานผลต่อผู้บริหาร	- ต้นทุนและค่าใช้จ่ายในการดำเนินงานมีแนวโน้มเพิ่มสูงขึ้น - ทรัพยากรไม่เพียงพอต่อการดำเนินการหารายได้และการดำเนินงานตามภารกิจของสำนักงาน - กฎหมายของสำนักงานไม่เอื้อให้สามารถจัดเก็บรายได้กับบริการในบางรูปแบบได้	- มติคณะรัฐมนตรีที่เกี่ยวข้องกับการบริหารงบประมาณของหน่วยงาน ซึ่งรวมถึงการงดศึกษาดูงานต่างประเทศ และการควบคุมค่าใช้จ่ายบุคลากร - หน่วยงานรัฐมีนโยบายในการพัฒนาหลักสูตรอบรมในด้านดิจิทัลเพิ่มมากขึ้น - หน่วยงานรัฐประยุกต์ใช้นวัตกรรมในการเพิ่มศักยภาพบุคลากรทดแทนการอบรมในรูปแบบเดิม - หน่วยงานรัฐมีการปรับเปลี่ยนหรือปรับปรุงระบบใหม่

เหตุการณ์ความเสี่ยง (Key Risk)	การควบคุมภายในที่มีอยู่ (Existing Control)	ความเสี่ยงที่ยังคงเหลือ (Residual Risk)	
		ปัจจัยภายใน (Internal)	ปัจจัยภายนอก (External)
4. C1: กระบวนการทำงาน อาจไม่สามารถปรับตัวได้ทัน ต่อการเปลี่ยนแปลงของ กฎหมาย หลักเกณฑ์ หรือ มาตรฐานที่สำคัญ	- มีการติดตามการออกกฎหมาย หลักเกณฑ์ หรือมาตรฐานใหม่ ที่เกี่ยวกับ ภารกิจ หรือที่มีความสำคัญกับ สพร. - นำผลการตรวจประเมินของ Auditor มาปรับปรุงกระบวนการการทำงาน ภายในให้เป็นปัจจุบัน - ตรวจประเมินการปฏิบัติตามกฎหมาย (Law Compliance) สรุป รายงานผล และแจ้งรายการข้อมูลความไม่สอดคล้อง ไปยังผู้บริหาร และส่วนงานที่รับผิดชอบ - ให้เจ้าหน้าที่เข้ารับการอบรม/สัมมนา เกี่ยวกับกฎหมายที่เกี่ยวข้องกับภารกิจ - มีการปรับปรุงกระบวนการและเอกสาร ให้สอดคล้องกับกฎหมาย PDPA	- การสื่อสารข้อมูลกฎหมายใหม่ให้ ผู้บริหารและเจ้าหน้าที่ได้รับทราบ ล่าช้า หรือไม่ครบถ้วน - บุคลากรขาดความเชี่ยวชาญ เกี่ยวกับหลักของ ISO27701 PDPA และมาตรฐานด้านเทคนิคที่จำเป็น - อาจขาดการวิเคราะห์ความ สอดคล้องของการดำเนินงานกับ กฎหมายอย่างครบถ้วน หรือทันต่อ สถานการณ์	- มีการออกกฎหมายสำคัญที่ อาจส่งผลกระทบต่อดำเนินงานของ สำนักงาน ได้แก่ 1) พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมาย ลำดับรอง 2) พรบ. การอำนวยความสะดวก สะดวกในการพิจารณาอนุญาต และการให้บริการแก่ประชาชน พ.ศ. 2569 3) พรบ. การรักษาความมั่นคง ปลอดภัยไซเบอร์ พ.ศ. 2562 4) (ร่าง) พรบ. ว่าด้วย ปัญญาประดิษฐ์ พ.ศ.
5. IT1: ระบบหรือข้อมูล สำคัญเผชิญภัยคุกคามทาง ไซเบอร์จนเกิดการหยุดชะงัก หรือข้อมูลรั่วไหล	- มีการพัฒนาทักษะบุคลากรภายในที่ ครอบคลุมเรื่องเทคโนโลยีที่เกิดขึ้นใหม่ เช่น AI, Quantum ในระดับเจ้าหน้าที่ และผู้บริหาร	- ขาดความต่อเนื่องของงบประมาณ ในการบำรุงรักษา (MA) และการ จัดซื้อจัดจ้างของระบบ DG CERT - เจ้าหน้าที่ขาดความรู้ความเข้าใจ เกี่ยวกับข้อมูลที่ถือครองที่สอดคล้อง	- แนวโน้มความรุนแรงและ รูปแบบในการโจมตีจาก เทคโนโลยีที่เกิดขึ้นใหม่เพิ่ม มากขึ้น (เช่น AI, Quantum, สถานการณ์ความขัดแย้งทาง

เหตุการณ์ความเสี่ยง (Key Risk)	การควบคุมภายในที่มีอยู่ (Existing Control)	ความเสี่ยงที่ยังคงเหลือ (Residual Risk)	
		ปัจจัยภายใน (Internal)	ปัจจัยภายนอก (External)
	- มีการทบทวนและจัดทำกระบวนการดำเนินงานที่สอดคล้องกับมาตรฐานสากล และกฎหมายด้านเทคโนโลยีสารสนเทศในการรับมือภัยคุกคามทางด้านไซเบอร์ เช่น แผนรับมือด้านไซเบอร์, แผนความต่อเนื่องทางธุรกิจ เป็นต้น - มีการประยุกต์เทคโนโลยีในการตรวจสอบและรับมือด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การเฝ้าระวังระบบ, VA, PenTest, 2FA เป็นต้น - มีการทดสอบประเมินความพร้อมของสำนักงานในการรับมือด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การทดสอบ Phishing Test, BCP เป็นต้น	ตามกฎหมายและมาตรฐานสากลใหม่ และนโยบาย IS Policy - เจ้าหน้าที่บริหารจัดการโครงการ/เจ้าของบริการ ขาดความตระหนักในการบริหารจัดการการควบคุมผู้ให้บริการภายนอกให้มีความมั่นคงปลอดภัย	การเมืองระหว่างประเทศ เป็นต้น) - หน่วยงานภายนอก (ผู้รับจ้าง) ขาดความตระหนักด้านความมั่นคงปลอดภัยในการให้บริการทำให้เกิดข้อมูลรั่วไหลจากบุคคลภายนอก - มีคำสั่งประกาศกฎหมายลำดับรองที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ให้สำนักงานต้องปฏิบัติตาม เช่น 2FA, Cloud security, มาตรฐานความมั่นคงปลอดภัยสำหรับเว็บไซต์ เป็นต้น

เหตุการณ์ความเสี่ยง (Key Risk)	การควบคุมภายในที่มีอยู่ (Existing Control)	ความเสี่ยงที่ยังคงเหลือ (Residual Risk)	
		ปัจจัยภายใน (Internal)	ปัจจัยภายนอก (External)
6. IT2: บริการดิจิทัลสำคัญ ไม่สามารถให้บริการได้ตาม ความต่อเนื่องที่กำหนด	- มีศูนย์ Call Center เพื่อรับเรื่องและ แก้ไขปัญหา พร้อมรับคำติชมบริการ - มีช่องทางในการรับเรื่องหลากหลาย ช่องทาง เช่น มีเครื่องมือ AI Chatbot สำหรับ Contact center เพื่อปรับปรุง การให้บริการ - รายงานผลข้อร้องเรียนและปัญหาการ ให้บริการตาม SLA ที่กำหนด เป็นประจำ ทุกเดือน และมีการแจ้งเตือนกรณีมีเคสคง ค้างในระบบ - มีการติดตามสถานการณ์ใช้งานของแต่ละ บริการเป็นประจำ - มีการจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP) ในบริการสำคัญทุกปี	- ระบบทำงานผิดพลาด (Bug) - ระบบโครงสร้างพื้นฐานไม่รองรับ หรือไม่เพียงพอ	- ปริมาณการใช้งานในระบบมี เป็นจำนวนมากในช่วงเวลา เดียวกัน - ระบบ Cloud จากผู้ให้บริการ ภายนอกขัดข้อง

2.3 การประเมินความเสี่ยง (Risk Evaluation)

เป็นการประเมินระดับความรุนแรงของเหตุการณ์ความเสี่ยงที่สำคัญ โดยใช้โอกาสที่จะเกิด ความเสี่ยง และผลกระทบ หรือความเสียหาย ที่เกิดจากความเสี่ยงภายหลังจากที่มีการควบคุมภายในไปแล้ว ซึ่งแต่ละเหตุการณ์ความเสี่ยงจะใช้เกณฑ์การประเมินที่มีความแตกต่างกันไป โดยสอดคล้องกับตัวชี้วัดนำ (Leading KRI) และตัวชี้วัดตาม (Lagging KRI) ซึ่งสามารถสรุปผลได้ ดังนี้

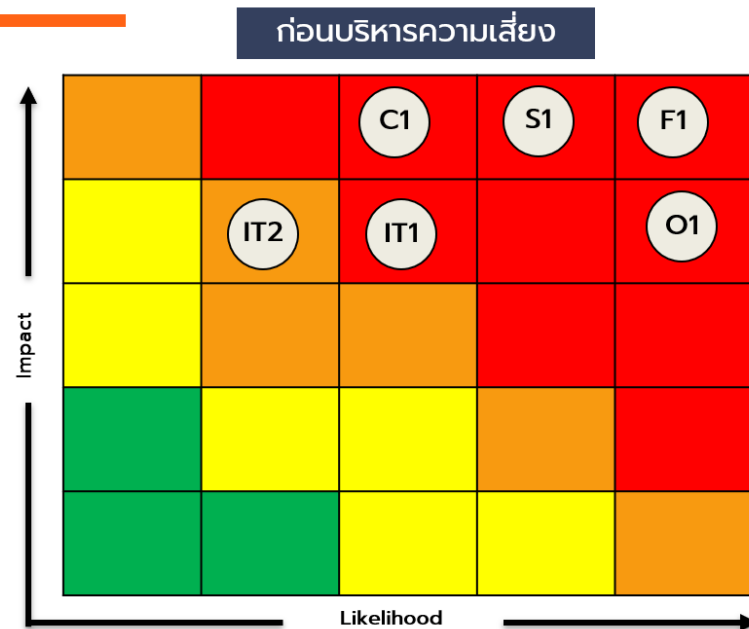
Key Risk	เกณฑ์การประเมิน โอกาสเกิด	ระดับโอกาส เกิด	เกณฑ์การประเมินผล กระทบ	ระดับ ผลกระทบ	ระดับความรุนแรง ของความเสี่ยง
1. S1: การดำเนินงานโครงการสำคัญตามยุทธศาสตร์/นโยบายรัฐบาลไม่บรรลุเป้าหมาย	ศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX) - ร้อยละความสำเร็จของกิจกรรมที่ดำเนินการ	4	- ความสำเร็จในการเชื่อมโยงชุดข้อมูลจากจำนวนหน่วยงานที่มีความท้าทาย - จำนวนชุดข้อมูล Master data ที่ดำเนินการจัดทำและแลกเปลี่ยนผ่าน GDX (สะสม)	5	20 (ค่าความเสี่ยงของโครงการที่มีค่าสูงสุด)

Key Risk	เกณฑ์การประเมิน โอกาสเกิด	ระดับโอกาส เกิด	เกณฑ์การประเมินผล กระทบ	ระดับ ผลกระทบ	ระดับความรุนแรง ของความเสี่ยง
	AI Data Verification and Government Process Automation Platform - ร้อยละความสำเร็จของกิจกรรมที่ดำเนินการ - ระดับความแม่นยำของระบบ	4	- ระดับการป้องกันการใช้งาน AI ผิดวัตถุประสงค์ของทุก Use case - การบรรลุเป้าหมายโครงการ	5	
	ท้องถิ่นดิจิทัล - จำนวนหน่วยงานนำร่อง	5	- ระดับความสำเร็จของการปรับปรุงประสิทธิภาพการใช้งานระบบให้สอดคล้องกับความต้องการของหน่วยงานใช้บริการ - ระดับความพึงพอใจของผู้ใช้บริการ	4	

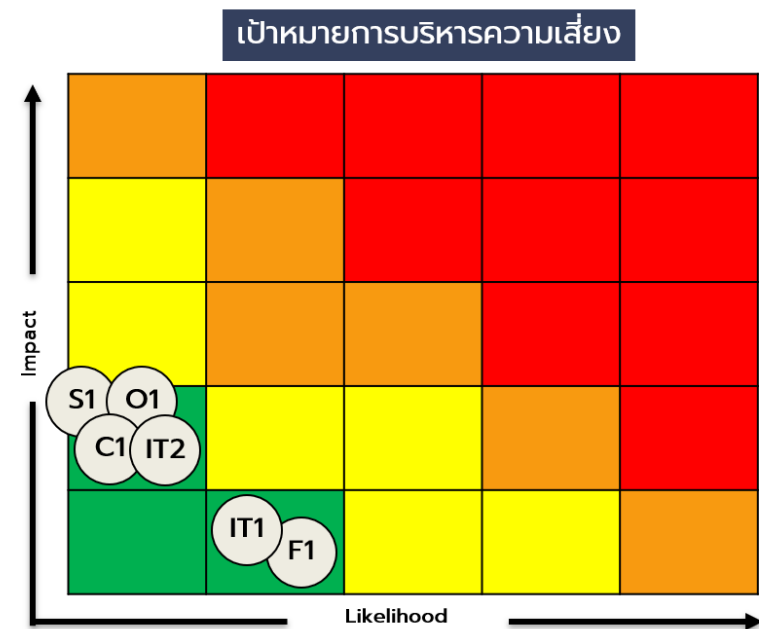
Key Risk	เกณฑ์การประเมิน โอกาสเกิด	ระดับโอกาส เกิด	เกณฑ์การประเมินผล กระทบ	ระดับ ผลกระทบ	ระดับความรุนแรง ของความเสี่ยง
2. O1: สมรรถนะของบุคลากรอาจ ไม่เพียงพอต่อการขับเคลื่อน นโยบายสำคัญ	-ระดับผลสำรวจ Energy Check-in -ร้อยละการปิดช่องโหว่ของ ทักษะ (Skill Gap)	5	-อัตราการลาออกของกลุ่ม ผู้มีศักยภาพสูง (Talent) (ร้อยละ) -ความสำเร็จจากการนำ ทักษะด้าน Future Skill ไปใช้ประโยชน์ (ร้อยละ)	4	20
3. F1: การหารายได้และการ บริหารต้นทุนไม่เป็นไปตาม เป้าหมาย	จำนวนผลิตภัณฑ์หรือกิจกรรม หารายได้รูปแบบใหม่ ที่สามารถดำเนินการได้	5	การสร้างรายได้ชัดเจนส่วน ต่างเป้าหมายรายได้	5	25
5. C1: กระบวนการทำงานอาจไม่ สามารถปรับตัวได้ทันต่อการ เปลี่ยนแปลงของกฎหมาย หลักเกณฑ์ หรือมาตรฐานที่สำคัญ	จำนวนการเกิดเหตุการณ์ที่ไม่ ปฏิบัติตามหรือปฏิบัติตามล่าช้า	3	ผลกระทบจากการไม่ปฏิบัติ หรือปฏิบัติล่าช้าในการ ดำเนินการตามกฎหมาย หลักเกณฑ์ หรือมาตรฐานที่ สำคัญ	5	15

Key Risk	เกณฑ์การประเมิน โอกาสเกิด	ระดับโอกาส เกิด	เกณฑ์การประเมินผล กระทบ	ระดับ ผลกระทบ	ระดับความรุนแรง ของความเสี่ยง
6. IT1: ระบบหรือข้อมูลสำคัญเผชิญภัยคุกคามทางไซเบอร์จนเกิดการหยุดชะงักหรือข้อมูลรั่วไหล	ร้อยละของบริการตาม Service Catalog ที่สามารถจัดการช่องโหว่ได้ตามนโยบายของสำนักงาน, จำนวนครั้งที่มีการรั่วไหลของข้อมูลของข้อมูลจากระบบของสำนักงาน	3	ผลกระทบจากการถูกบุกรุก/โจมตีความมั่นคงปลอดภัย การละเมิดข้อมูลส่วนบุคคลของระบบสารสนเทศของสำนักงาน รวมทั้ง ข้อมูลรั่วไหล หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต	4	12
7. IT2: บริการดิจิทัลสำคัญไม่สามารถให้บริการได้ตามความต่อเนื่องที่กำหนด	ร้อยละการแก้ไข Incident ตาม SLA	2	ร้อยละการให้บริการอย่างต่อเนื่อง ตาม SLA ที่กำหนด	4	8

ระดับความเสี่ยงก่อนการบริหารและเป้าหมายการบริหารความเสี่ยง



- S1: การดำเนินงานโครงการสำคัญตามยุทธศาสตร์/นโยบายรัฐบาล
ไม่บรรลุเป้าหมาย
- O1: สมรรถนะของบุคลากรอาจไม่เพียงพอต่อการขับเคลื่อนนโยบายสำคัญ
- F1: การหารายได้และการบริหารต้นทุนไม่เป็นไปตามเป้าหมาย



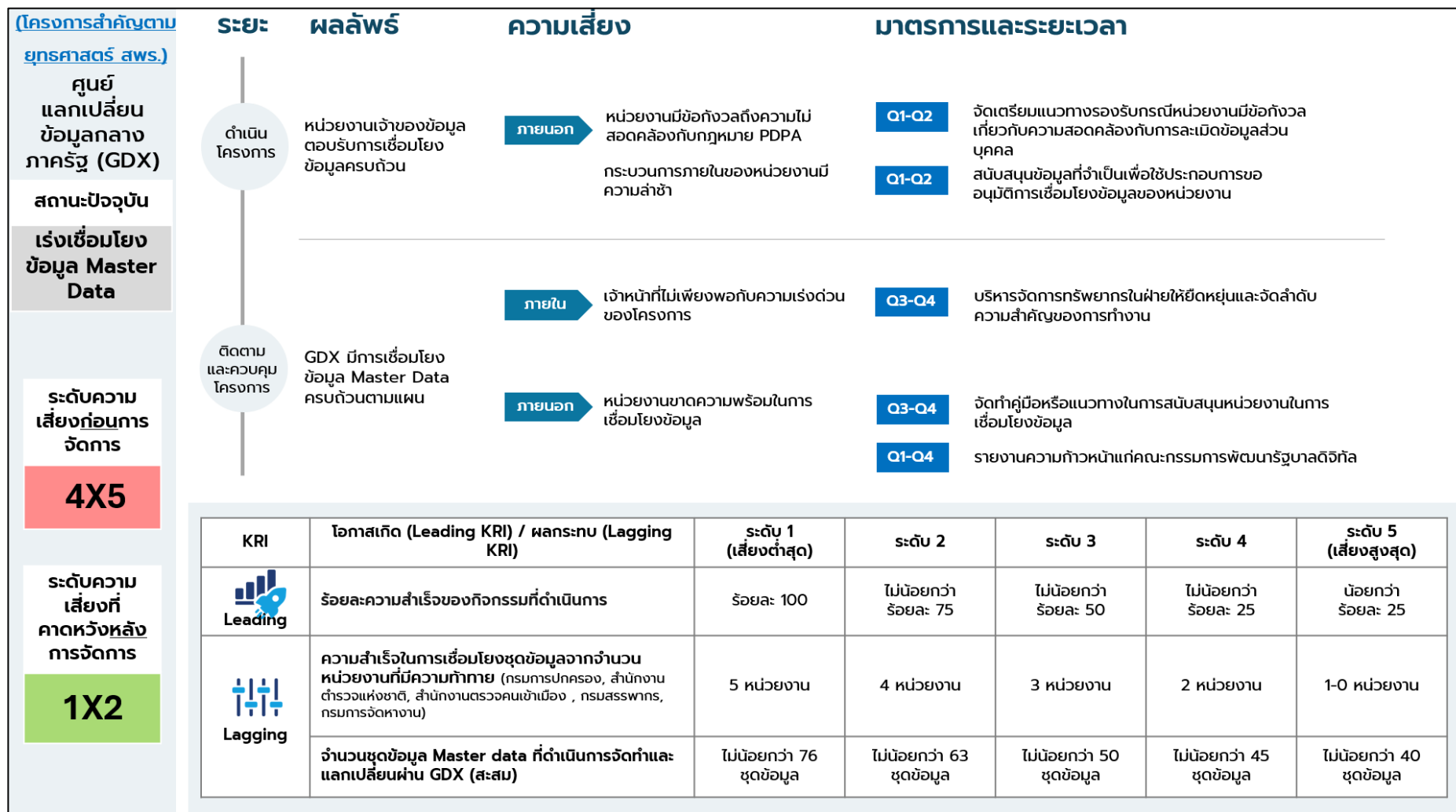
- C1: กระบวนการทำงานอาจไม่สามารถปรับตัวได้ทันต่อการเปลี่ยนแปลงของ
กฎหมาย หลักเกณฑ์ หรือมาตรฐานที่สำคัญ
- IT1: ระบบหรือข้อมูลสำคัญเผชิญภัยคุกคามทางไซเบอร์จนเกิดการ
หยุดชะงักหรือข้อมูลรั่วไหล
- IT2: บริการดิจิทัลสำคัญไม่สามารถให้บริการได้ตามความต่อเนื่องที่กำหนด

2.4 การตอบสนองและจัดการความเสี่ยง (Risk Treatment)

เป็นการจัดทำแผนการควบคุมภายใน เพื่อปรับปรุงมาตรการควบคุมภายในที่มีอยู่ให้มีประสิทธิภาพมากยิ่งขึ้น โดยเฉพาะการลดผลกระทบหรือความเสียหายซึ่งสามารถดำเนินการได้ ภายใต้ทรัพยากรที่มีอยู่ รวมทั้ง เป็นการจัดทำแผนจัดการความเสี่ยง เพื่อป้องกันไม่ให้เกิดความเสี่ยงใหม่ และลดความเสียหายที่ยังคงเหลือ ภายหลังจากที่ได้มีมาตรการควบคุมภายในไปแล้ว โดย สพร. ได้ใช้การวิเคราะห์ในรูปแบบ PMBOK และ Bow-Tie Diagram เพื่อนำมากำหนดแผนการควบคุมภายใน และแผนจัดการความเสี่ยงดังกล่าว รวมไปถึงการกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite, Risk Tolerance), ตัวชี้วัดความเสี่ยง (Leading KRI, Lagging KRI) ซึ่งจะนำไปใช้ในการแจ้งเตือนความเสี่ยงล่วงหน้า (Early Warning System) ให้แก่ผู้บริหารและเจ้าของความเสี่ยง (Risk Owner) และระดับความเสี่ยงที่คาดหวังของแต่ละเหตุการณ์ความเสี่ยงที่สำคัญ ตามรายละเอียด ดังนี้

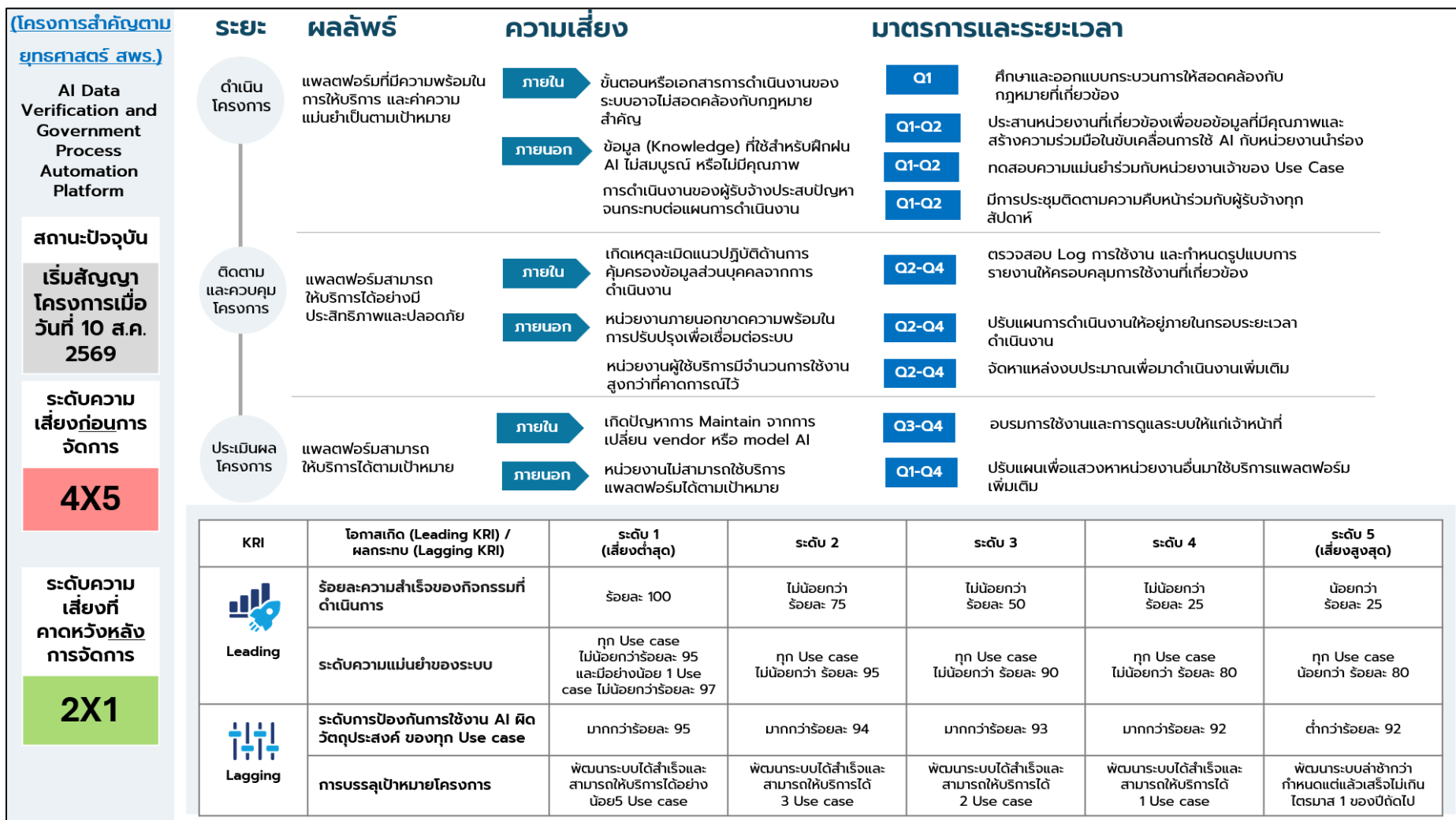
S1 การดำเนินงานโครงการสำคัญตามยุทธศาสตร์/นโยบายรัฐบาล ไม่บรรลุเป้าหมาย

- โครงการ ศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX)



S1 การดำเนินงานโครงการสำคัญตามยุทธศาสตร์/นโยบายรัฐบาล ไม่บรรลุเป้าหมาย

- โครงการ AI Data Verification and Government Process Automation Platform

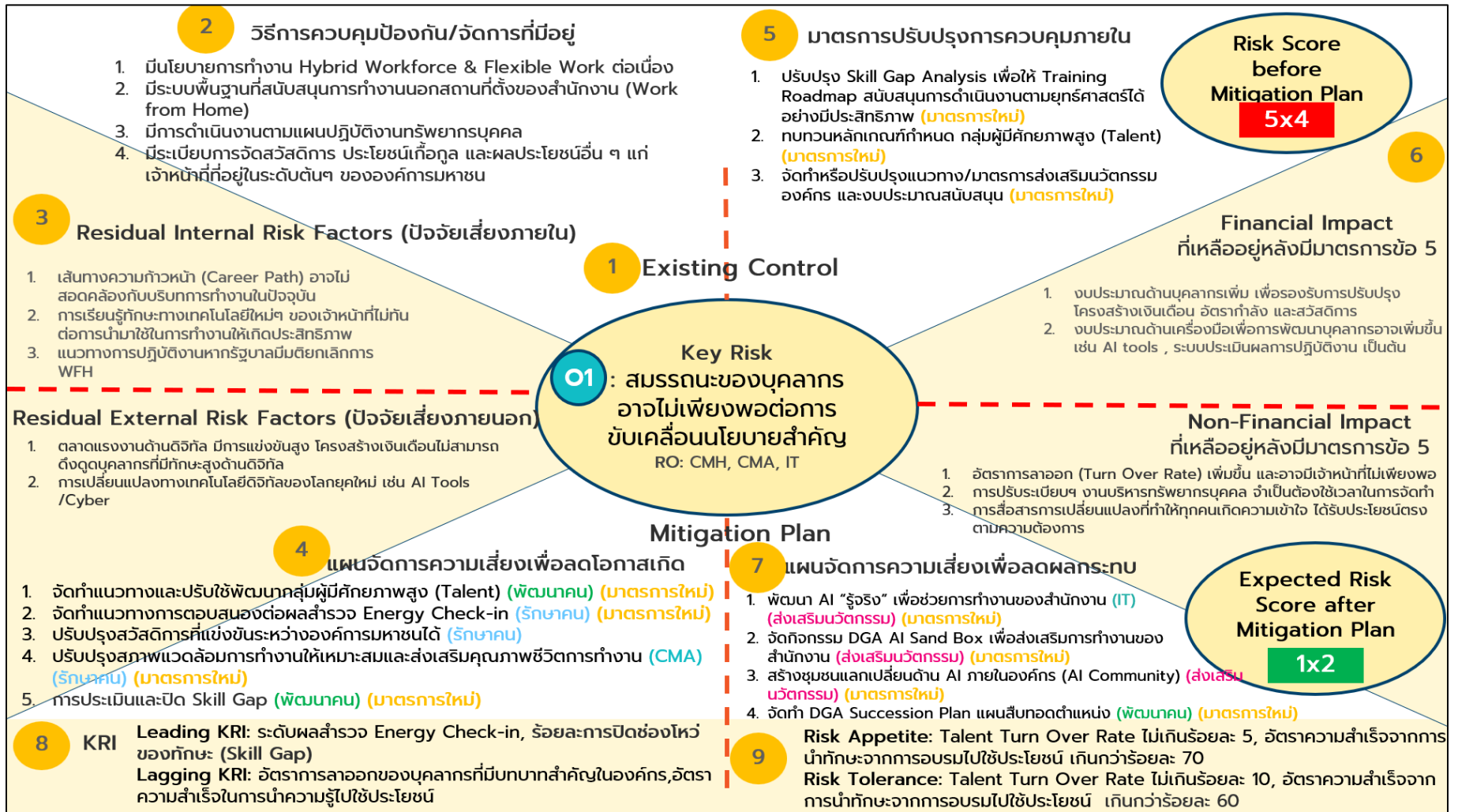


S1 การดำเนินงานโครงการสำคัญตามยุทธศาสตร์/นโยบายรัฐบาล ไม่บรรลุเป้าหมาย

- โครงการ ท้องถิ่นดิจิทัล

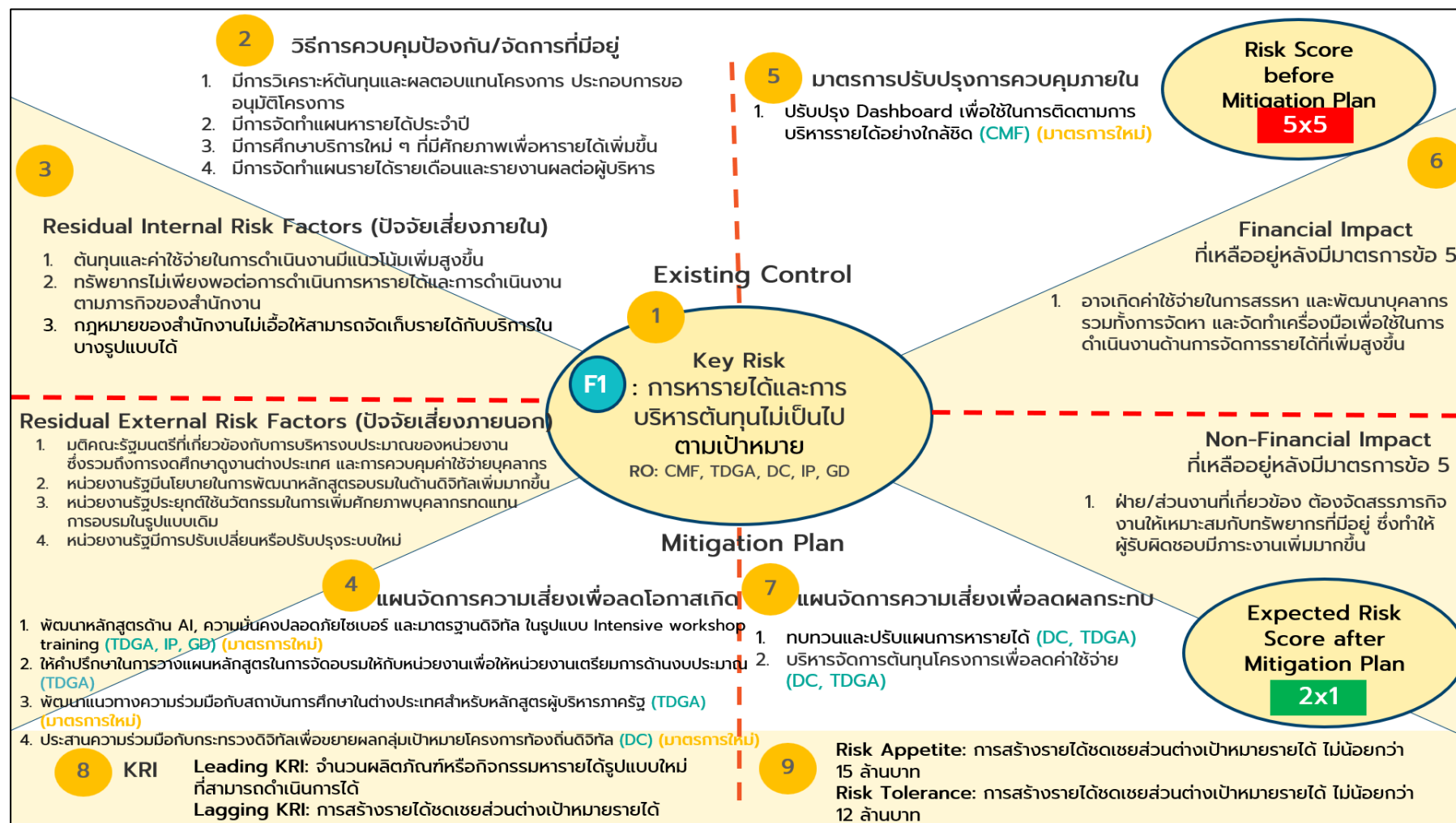
</

O1 สมรรถนะของบุคลากรอาจไม่เพียงพอต่อการขับเคลื่อนนโยบายสำคัญ



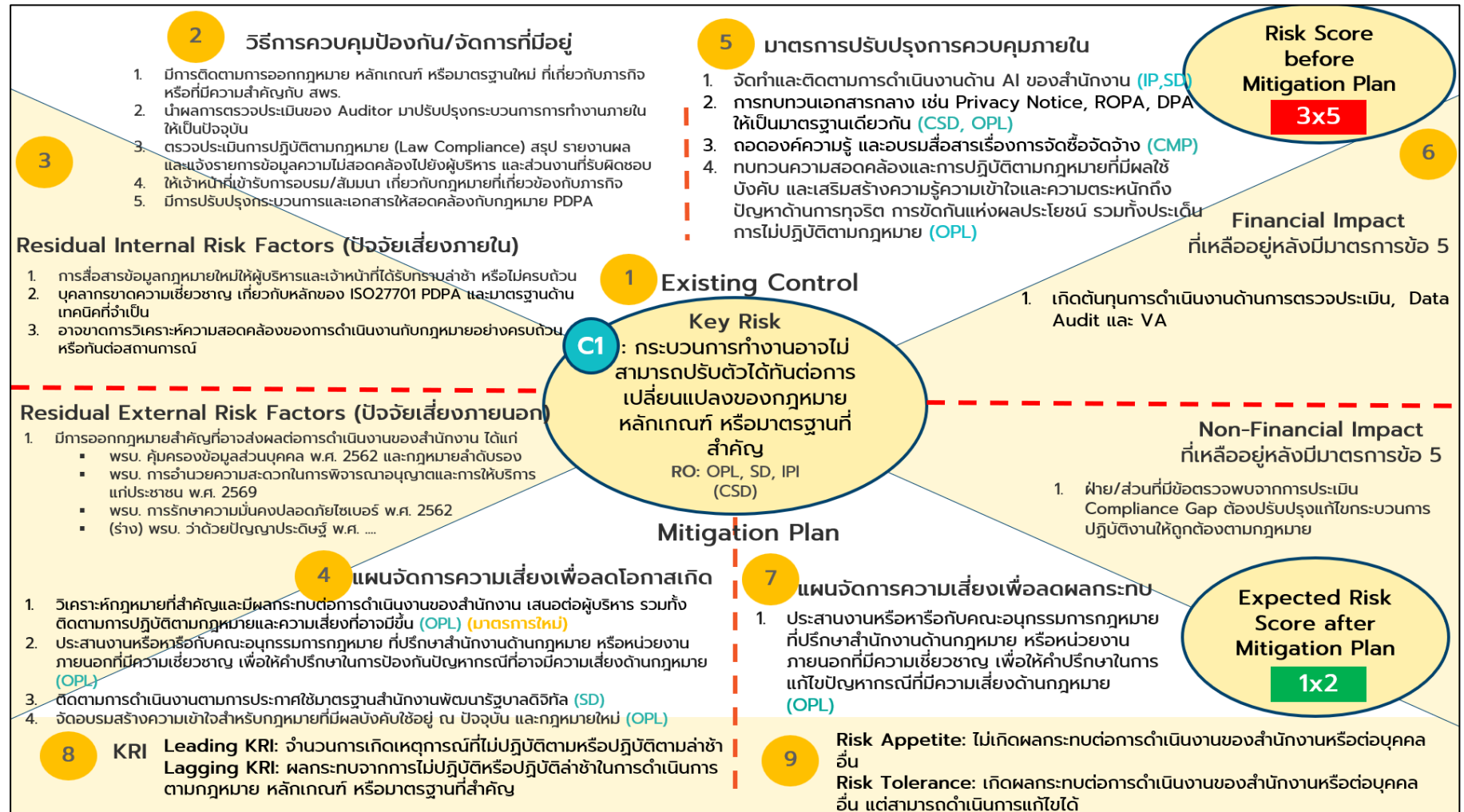
แผนการควบคุมภายใน และแผนจัดการความเสี่ยง	ไตรมาส 1/2570			ไตรมาส 2/2570			ไตรมาส 3/2570			ไตรมาส 4/2570			
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
แผนการควบคุมภายใน													
1. ทบทวนหลักเกณฑ์ที่กำหนด กลุ่มผู้มีศักยภาพสูง (Talent)	←		→										
2. จัดทำหรือปรับปรุงแนวทาง/มาตรการส่งเสริมวัฒนธรรมองค์กร และงบประมาณสนับสนุน	←					→							
แผนจัดการความเสี่ยง (ลดโอกาสเกิด)													
1. พัฒนาและติดตามผลกลุ่มผู้มีศักยภาพสูง (Talent) (พัฒนาคน)				←								→	
2. จัดทำหลักเกณฑ์และการประเมิน Energy Check-in และจัดกิจกรรม Energy Recharge (รักษาคน)	←	จัดทำหลักเกณฑ์และการประเมิน			←		จัดกิจกรรม Energy Recharge				→		
3. ปรับปรุงสวัสดิการที่แข่งขันระหว่างองค์การมหาชนได้ (รักษาคน)		เสนอแนวทางที่จะปรับปรุง			วิเคราะห์ห้ระบียบที่เกี่ยวข้องและกระบวนการ				จัดทำร่างและขออนุมัติบังคับใช้				
4. ปรับปรุงสภาพแวดล้อมการทำงานให้เหมาะสมและส่งเสริมคุณภาพชีวิตการทำงาน (CMA) (รักษาคน)													
5. การประเมินและปิด Skill Gap	←	รวบรวม Skill Gap ขององค์กร		←	จัดการปิด Skill Gap โดยฝึกอบรม, OJT, ศึกษาดูงาน เป็นต้น							→	
แผนจัดการความเสี่ยง (ลดผลกระทบ)													
1. พัฒนา AI “รู้จริง” เพื่อช่วยการทำงานของสำนักงาน (IT) (ส่งเสริมนวัตกรรม)	←	จัดทำ Business Use Case		←	ทดสอบกับกลุ่มเป้าหมาย		←	ขึ้นระบบ Production		←	ปรับปรุงความแม่นยำ		
2. จัดกิจกรรม DGA AI Sand Box เพื่อส่งเสริมการใช้ AI ในการทำงานของสำนักงาน (ส่งเสริมนวัตกรรม)	←	จัดเตรียมเครื่องมือเพื่อพัฒนาโครงการต้นแบบ		←		ใช้งานจริง			←	ประเมินผลลัพธ์การใช้งาน			
3. สร้างชุมชนแลกเปลี่ยนด้าน AI ภายในองค์กร (AI Community) (ส่งเสริมนวัตกรรม)	←	สื่อสารทำความเข้าใจการใช้งานแก่นักวิชาการ และเริ่มใช้งาน		←	จัดกิจกรรม, แลกเปลี่ยนความรู้			←	สรุปผลกิจกรรมและผลประโยชน์				
4. จัดทำ DGA Succession Plan แผนสืบทอดตำแหน่ง (พัฒนาคน)				←	กำหนดตำแหน่งสำคัญ		←	ประเมินและพัฒนาผู้มีศักยภาพ					→

F1 การหารายได้และการบริหารต้นทุนไม่เป็นไปตามเป้าหมาย



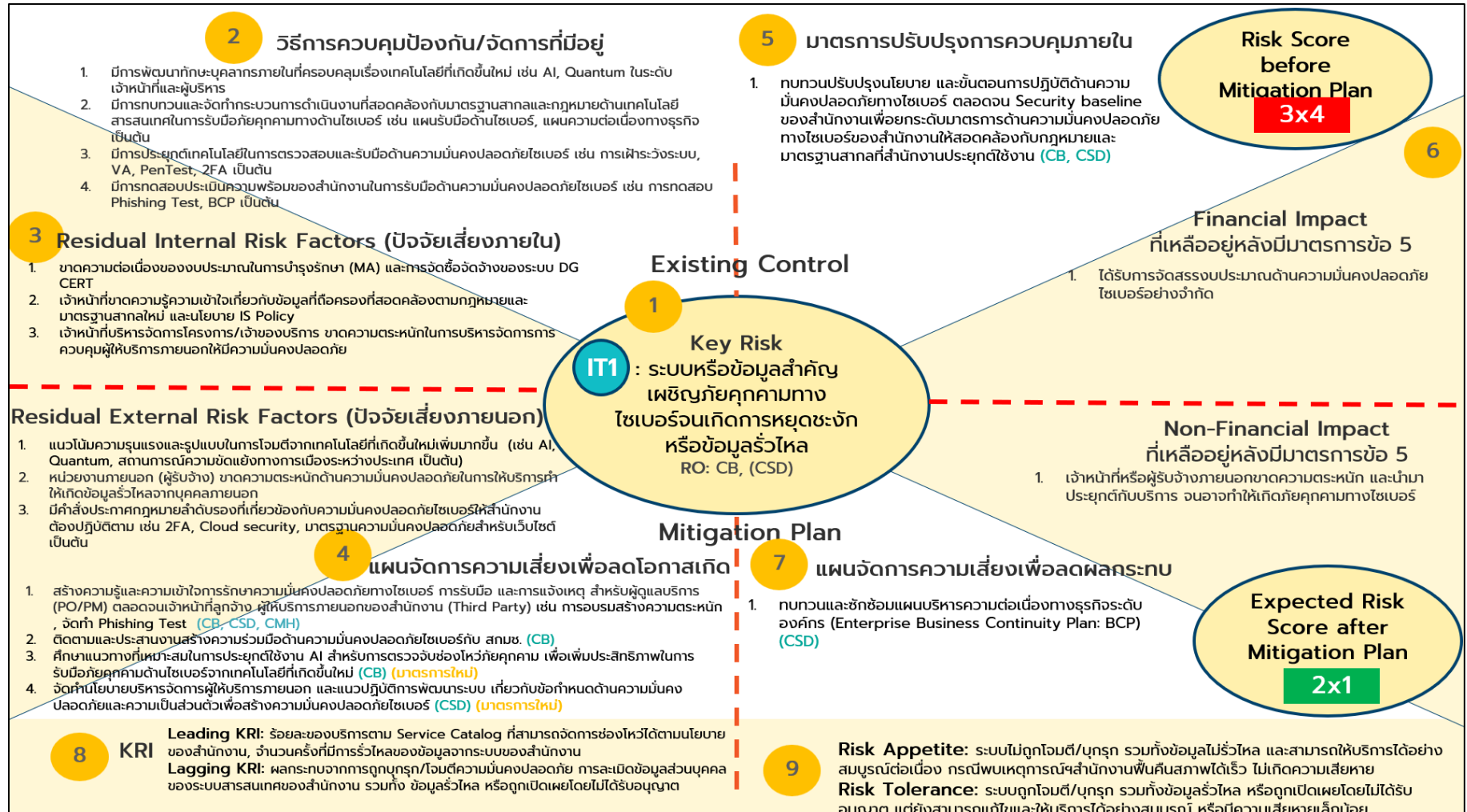
แผนการควบคุมภายใน และแผนจัดการความเสี่ยง	ไตรมาส 1/2570			ไตรมาส 2/2570			ไตรมาส 3/2570			ไตรมาส 4/2570		
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
แผนการควบคุมภายใน												
1. ปรับปรุง Dashboard เพื่อใช้ในการติดตามการบริหารรายได้อย่างใกล้ชิด (DC, TDGA, CMF)	←		→									
แผนจัดการความเสี่ยง (ลดโอกาสเกิด)												
1. พัฒนาหลักสูตรด้าน AI, ความมั่นคงปลอดภัยไซเบอร์ และมาตรฐานดิจิทัล ในรูปแบบ Intensive workshop training (TDGA, IP)	←	พัฒนาหลักสูตร	→	←				เปิดหลักสูตรอบรม				→
2. ให้คำปรึกษาในการวางแผนหลักสูตรในการจัดอบรมให้กับหน่วยงานเพื่อให้หน่วยงานเตรียมการด้านงบประมาณ (TDGA)			←				→					
3. พัฒนาแนวทางความร่วมมือกับสถาบันการศึกษาในต่างประเทศสำหรับหลักสูตรผู้บริหารภาครัฐ (TDGA)	←				→							
4. ประสานความร่วมมือกับกระทรวงดิจิทัลเพื่อขยายผลกลุ่มเป้าหมายโครงการท้องถิ่นดิจิทัล (DC)	←						→					
แผนจัดการความเสี่ยง (ลดผลกระทบ)												
1. ทบทวนและปรับแผนการหารายได้ (DC, TDGA)			←		→		←		→			
2. บริหารจัดการต้นทุนโครงการเพื่อลดค่าใช้จ่าย (DC, TDGA)	←											→

C1 กระบวนการทำงานอาจไม่สามารถปรับตัวได้ทันต่อการเปลี่ยนแปลงของกฎหมาย หลักเกณฑ์ หรือมาตรฐานที่สำคัญ



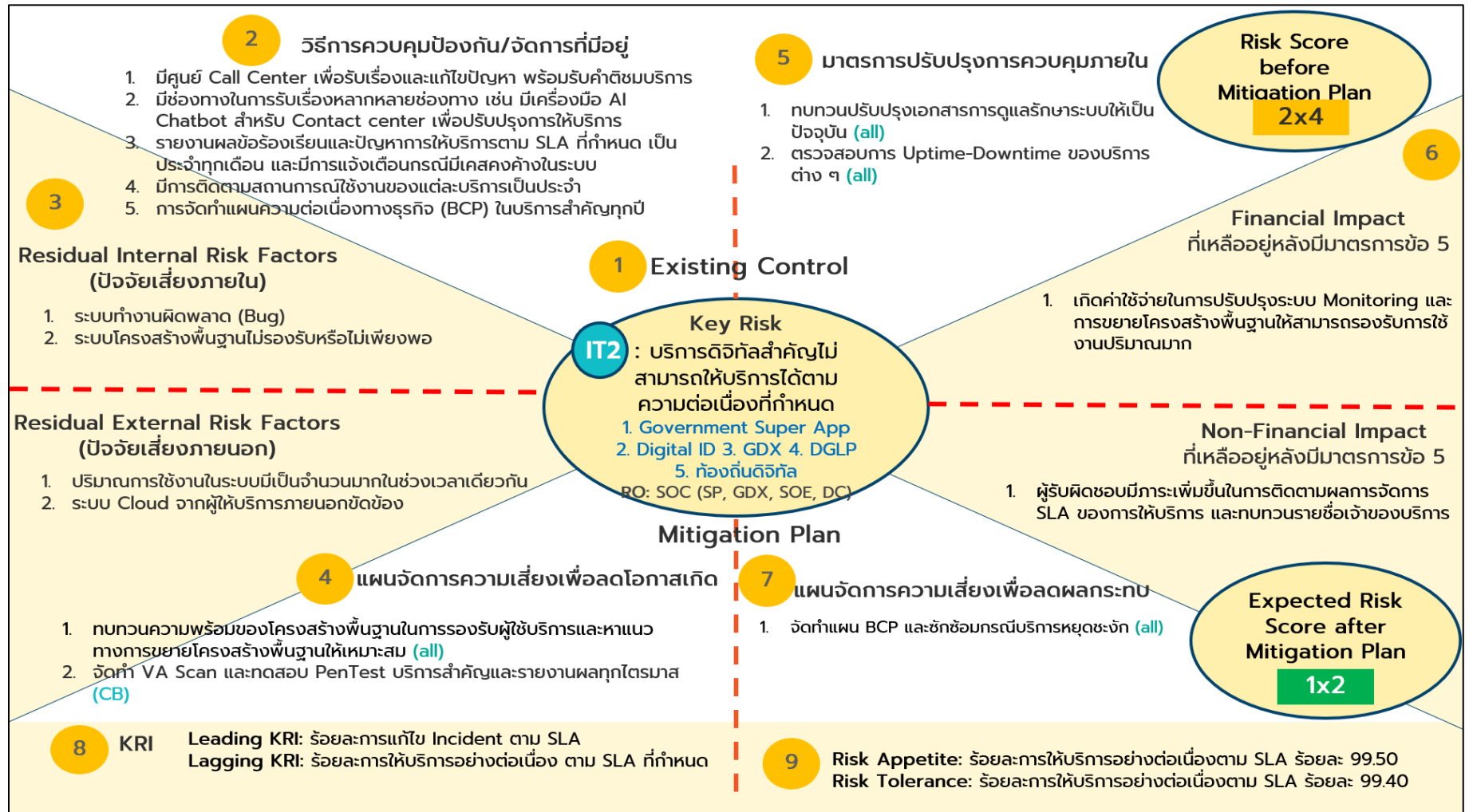
แผนการควบคุมภายใน และแผนจัดการความเสี่ยง	ไตรมาส 1/2570			ไตรมาส 2/2570			ไตรมาส 3/2570			ไตรมาส 4/2570		
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
แผนการควบคุมภายใน												
1. จัดทำและติดตามการดำเนินงานด้าน AI ของสำนักงาน (IP,SD)												
2. ทบทวนเอกสารกลาง เช่น Privacy Notice, ROPA, DPA ให้เป็นมาตรฐานเดียวกัน (CSD, OPL)				ปรับปรุง Template ของแต่ละบริการให้ได้มาตรฐานเดียวกัน								
				ศูนย์กลางข้อมูลและเอกสารด้านความเป็นส่วนตัว								
3. ทดสอบความรู้ และอบรมสื่อสารเรื่องการจัดซื้อจัดจ้าง (CMP)												
4. ทบทวนความสอดคล้องและการปฏิบัติตามกฎหมายที่มีผลใช้บังคับ และเสริมสร้างความรู้ความเข้าใจและความตระหนักถึงปัญหาด้านการทุจริต การขัดกันแห่งผลประโยชน์ รวมทั้งประเด็นการไม่ปฏิบัติตามกฎหมาย(OPL)												
แผนจัดการความเสี่ยง (ลดโอกาสเกิด)												
1. วิเคราะห์กฎหมายที่สำคัญและมีผลกระทบต่อการทำงานของสำนักงาน เสนอต่อผู้บริหาร รวมทั้งติดตามการปฏิบัติตามกฎหมาย และความเสี่ยงที่อาจมีขึ้น (OPL)												
2. ประสานงานหรือหารือกับคณะอนุกรรมการกฎหมาย ที่ปรึกษาสำนักงานด้านกฎหมาย หรือหน่วยงานภายนอกที่มีความเชี่ยวชาญ เพื่อให้คำปรึกษาในการป้องกันปัญหากรณีที่มีความเสี่ยงด้านกฎหมาย (OPL)												
3. ติดตามการดำเนินงานตามการประกาศใช้มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (SD)												
4. จัดอบรมสร้างความเข้าใจสำหรับกฎหมายที่มีผลบังคับใช้อยู่ ณ ปัจจุบัน และกฎหมายใหม่ (OPL)												
แผนจัดการความเสี่ยง (ลดผลกระทบ)												
1. ประสานงานหรือหารือกับคณะอนุกรรมการกฎหมาย ที่ปรึกษาสำนักงานด้านกฎหมาย หรือหน่วยงานภายนอกที่มีความเชี่ยวชาญ เพื่อให้คำปรึกษาในการแก้ไขปัญหากรณีที่มีความเสี่ยงด้านกฎหมาย (OPL)												

IT1 ระบบหรือข้อมูลสำคัญเผชิญภัยคุกคามทางไซเบอร์จนเกิดการหยุดชะงักหรือข้อมูลรั่วไหล



แผนการควบคุมภายใน และแผนจัดการความเสี่ยง	ไตรมาส 1/2570			ไตรมาส 2/2570			ไตรมาส 3/2570			ไตรมาส 4/2570		
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
แผนการควบคุมภายใน												
1. ทบทวนปรับปรุงนโยบาย และขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจน Security baseline ของสำนักงานเพื่อยกระดับมาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานให้สอดคล้องกับกฎหมายและ มาตรฐานสากลที่สำนักงานประยุกต์ใช้งาน (CB, CSD)												
แผนจัดการความเสี่ยง (ลดโอกาสเกิด)												
1. สร้างความรู้และความเข้าใจการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การรับมือ การแจ้งเหตุการณ์ สำหรับผู้ดูแลบริการ (PO/PM) ตลอดจนเจ้าหน้าที่ลูกจ้าง ผู้ให้บริการภายนอกของสำนักงาน (Third Party) และประชาชนทั่วไป เช่น การอบรมสร้างความตระหนัก, จัดทำ Phishing Test (PO, CB, CSD, CMH)												
2. ศึกษาแนวทางที่เหมาะสมในการประยุกต์ใช้งาน AI สำหรับการตรวจจับช่องโหว่ภัยคุกคาม เพื่อเพิ่มประสิทธิภาพในการรับมือภัยคุกคามด้านไซเบอร์จากเทคโนโลยีที่เกิดขึ้นใหม่ (CB)				ศึกษาแนวทาง								
3. ติดตามและประสานงานสร้างความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์กับ สกมช.												
4. สร้างความมั่นคงปลอดภัยไซเบอร์และมาตรการควบคุมผู้ให้บริการภายนอก (Third-Party Risk Management)												
แผนจัดการความเสี่ยง (ลดผลกระทบ)												
1. ทบทวนหลักเกณฑ์ในการวิเคราะห์ผลกระทบทางธุรกิจให้เหมาะสมกับสถานการณ์ปัจจุบัน เพื่อระบุบริการสำคัญที่ต้องนำไปจัดทำแผน BCP (CSR)												

IT2 บริการดิจิทัลสำคัญไม่สามารถให้บริการได้ตามความต่อเนื่องที่กำหนด



แผนการควบคุมภายใน และแผนจัดการความเสี่ยง	ไตรมาส 1/2570			ไตรมาส 2/2570			ไตรมาส 3/2570			ไตรมาส 4/2570		
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.

แผนการควบคุมภายใน

1. ทบทวนปรับปรุงเอกสารการดูแลรักษาระบบให้เป็นปัจจุบัน	←			←			←			←		
2. ตรวจสอบการ Uptime-Downtime ของบริการต่าง ๆ	←			←			←			←		

แผนจัดการความเสี่ยง (ลดโอกาสเกิด)

1. ทบทวนความพร้อมของโครงสร้างพื้นฐานในการรองรับผู้ใช้บริการและหาแนวทางการขยายโครงสร้างพื้นฐานให้เหมาะสม (all)	←			←			←			←		
2. จัดทำ VA Scan และทดสอบ PenTest บริการสำคัญและรายงานผลทุกไตรมาส	←			←			←			←		

แผนจัดการความเสี่ยง (ลดผลกระทบ)

1. จัดทำแผน BCP และซักซ้อมกรณีบริการหยุดชะงัก (all)				←								
---	--	--	--	---	--	--	--	--	--	--	--	--

3. ความเสี่ยงที่ยอมรับได้ (Risk Appetite) และความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) ของรายการความเสี่ยง

เหตุการณ์ความเสี่ยง (Key Risk)	ความเสี่ยงที่ยอมรับได้ (Risk Appetite)	ความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance)
S1: การดำเนินงานโครงการสำคัญ ตามยุทธศาสตร์/นโยบายรัฐบาล ไม่บรรลุเป้าหมาย	ศูนย์แลกเปลี่ยนข้อมูลกลางภาครัฐ (GDX) - เชื่อมโยงชุดข้อมูลจากจำนวนหน่วยงานที่มีความท้าทายได้ จำนวน 4 หน่วยงาน - ไม่น้อยกว่า 63 ชุดข้อมูล	- เชื่อมโยงชุดข้อมูลจากจำนวนหน่วยงานที่มีความท้าทายได้ จำนวน 3 หน่วยงาน - ไม่น้อยกว่า 50 ชุดข้อมูล
	AI Data Verification and Government Process Automation Platform - ระดับการป้องกันการใช้งาน AI ผิดวัตถุประสงค์ ของ ทุก Use case มากกว่าร้อยละ 95 - พัฒนาระบบได้สำเร็จและสามารถให้บริการได้อย่าง น้อย 5 Use case	- ระดับการป้องกันการใช้งาน AI ผิดวัตถุประสงค์ ของ ทุก Use case มากกว่าร้อยละ 94 - พัฒนาระบบได้สำเร็จและสามารถให้บริการได้ 3 Use case
	ท้องถิ่นดิจิทัล - สามารถปรับปรุงกระบวนการและพัฒนาฟังก์ชันการ ใช้งานได้เกือบครบถ้วน โดยยังมีประเด็นปรับปรุงเพียง เล็กน้อย ไม่ส่งผลกระทบต่อการใช้งาน - ระดับความพึงพอใจของผู้ใช้บริการ 3.99 – 3.50 คะแนน	- สามารถปรับปรุงกระบวนการและพัฒนาฟังก์ชันการ ใช้งานได้ในระดับที่ยอมรับได้ รองรับการให้บริการ ดิจิทัลเฉพาะกระบวนการสำคัญ แต่ยังมีบางส่วนที่ต้อง ดำเนินการเพิ่มเติม - ระดับความพึงพอใจของผู้ใช้บริการ 3.49 – 3.00 คะแนน

เหตุการณ์ความเสี่ยง (Key Risk)	ความเสี่ยงที่ยอมรับได้ (Risk Appetite)	ความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance)
O1: สมรรถนะของบุคลากรอาจไม่เพียงพอต่อการขับเคลื่อนนโยบายสำคัญ	1) อัตราการลาออกของกลุ่มผู้มีศักยภาพสูง (Talent) ร้อยละ 5 2) อัตราความสำเร็จจากการนำทักษะจากการอบรมไปใช้ประโยชน์ เกินกว่าร้อยละ 70	1) อัตราการลาออกของกลุ่มผู้มีศักยภาพสูง (Talent) ไม่เกินกว่าร้อยละ 10 2) อัตราความสำเร็จจากการนำทักษะจากการอบรมไปใช้ประโยชน์ เกินกว่าร้อยละ 60
F1: การหารายได้ไม่เป็นไปตามเป้าหมาย	- การสร้างรายได้ขดเชยส่วนต่างเป้าหมายรายได้ ไม่น้อยกว่า 15 ล้านบาท	- การสร้างรายได้ขดเชยส่วนต่างเป้าหมายรายได้ ไม่น้อยกว่า 12 ล้านบาท
C1: กระบวนการทำงานอาจไม่สามารถปรับตัวได้ทันต่อการเปลี่ยนแปลงของกฎหมาย หลักเกณฑ์ หรือมาตรฐานที่สำคัญ	- ไม่เกิดผลกระทบต่อการดำเนินงานของสำนักงานหรือต่อบุคคลอื่น	- เกิดผลกระทบต่อการดำเนินงานของสำนักงานหรือต่อบุคคลอื่น แต่สามารถดำเนินการแก้ไขได้
IT1: ระบบหรือข้อมูลสำคัญเผชิญภัยคุกคามทางไซเบอร์จนเกิดการหยุดชะงักหรือข้อมูลรั่วไหล	- ระบบไม่ถูกโจมตี/บุกรุก รวมทั้งข้อมูลไม่รั่วไหล และสามารถให้บริการได้อย่างสมบูรณ์ต่อเนื่อง กรณีพบเหตุการณ์สำนักงานฟื้นคืนสภาพได้เร็ว ไม่เกิดความเสียหาย	- ระบบถูกโจมตี/บุกรุก รวมทั้งข้อมูลรั่วไหล หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต แต่ยังสามารถแก้ไขและให้บริการได้อย่างสมบูรณ์ หรือมีความเสียหายเล็กน้อย
IT2: บริการดิจิทัลสำคัญไม่สามารถให้บริการได้ตามความต่อเนื่องที่กำหนด	- ร้อยละการให้บริการอย่างต่อเนื่องตาม SLA ร้อยละ 99.50	- ร้อยละการให้บริการอย่างต่อเนื่องตาม SLA ร้อยละ 99.40



สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

**Digital Government Development Agency
(Public Organization)**

www.dga.or.th



DGA THAILAND



จัดทำโดย ส่วนบริหารความเสี่ยงและควบคุมภายใน (CSR)

ฝ่ายกลยุทธ์องค์กร



csr_division@dga.or.th

