

คู่มือการกำกับดูแล

ความเสี่ยงจาก

เทคโนโลยีควอนตัม

(Quantum Risk Governance
& PQC Transition)

สำหรับกรรมการบริษัท



จัดทำโดย

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

กันยายน 2569

การกำกับดูแลความเสี่ยงจากเทคโนโลยีควอนตัม

(Quantum Risk Governance & PQC Transition)

ความเสี่ยงสำคัญที่ควรเริ่มเตรียมความพร้อมตั้งแต่วันนี้

“ทุกนาทีคือการแข่งกับเวลา เพื่อเปลี่ยนผ่านสู่ยุค Quantum ให้ทัน ก่อนที่ความเสี่ยงจะเกิดขึ้นจริง”
เพราะภัยคุกคามรูปแบบใหม่อาจมาถึงเร็วกว่าที่คาด องค์กรที่เริ่มลงมือ ตั้งแต่วันนี้ ทั้งการกำกับดูแล การบริหารความเสี่ยง และการพัฒนาบุคลากร คือ ผู้ที่รักษาความเชื่อมั่น และสร้างความได้เปรียบอย่างยั่งยืนในระยะยาว



เหตุผลที่ควรเริ่มตั้งแต่วันนี้

1 ข้อมูลอาจเสี่ยงก่อนภัยมาถึง



ข้อมูลสำคัญอาจถูกดักเก็บในวันนี้ เพื่อรอถอดรหัสเมื่อเทคโนโลยี มีความพร้อมในอนาคต (HARVEST NOW, DECRYPT LATER)

2 ความน่าเชื่อถืออาจถูกโจมตี



หากลายมือชื่อดิจิทัล ในใบรอง หรือการยืนยันตัวตนถูกปลอมแปลง ระบบอาจยอมรับบุคคล เอกสาร ซอฟต์แวร์ หรือคำสั่งธุรกรรมปลอมว่าเป็นของจริง

3 การเปลี่ยนผ่านต้องใช้เวลา



ระบบเดิม ใบรับรอง อุปกรณ์บริหารจัดการ ญาแฉเข้ารหัส การเชื่อมต่อภายนอก และผู้ค้า ต้องใช้ระยะเวลาในการดำเนินการเปลี่ยนผ่าน



เป้าหมาย

ไม่ใช้การเร่งลงทุนในเทคโนโลยีหรือเปลี่ยนการเข้ารหัสทั้งหมดทันที แต่คือการตระหนักว่าความเสี่ยงอยู่ที่ใด จัดลำดับสิ่งที่ควรเร่งดำเนินการ และกำหนด Roadmap ในการเปลี่ยนผ่านโดยไม่กระทบความต่อเนื่องทางธุรกิจ

PQC เป็นแนวทางการเปลี่ยนผ่านที่องค์กรส่วนใหญ่เลือกใช้ ส่วน QKD และ QRNG เป็นทางเลือกเพิ่มเติมที่อาจพิจารณาตามความจำเป็นและความเหมาะสมกับรูปแบบของแต่ละองค์กร

5 ขั้นตอนสำคัญสำหรับองค์กร

1 กำหนดความรับผิดชอบ



- กำหนดผู้รับผิดชอบหลัก เพื่อบริหารจัดการในภาพรวม
- กำหนดโครงสร้างการกำกับดูแลที่มีการประสานความร่วมมือของ Three Lines Model

2 จัดทำบัญชีรายการการใช้รหัสลับ



จัดทำบัญชีรายการการใช้รหัสลับ (Cryptographic Bill of Materials: CBOM) เพื่อให้ทราบว่ามีระบบใช้อัลกอริทึมการเข้ารหัสใด มีผู้รับผิดชอบและพึ่งพาผู้ให้บริการรายใด เพื่อใช้จัดลำดับการเปลี่ยนผ่าน

3 จัดลำดับตามความเสี่ยงทางธุรกิจ



- พิจารณาตามรูปแบบธุรกิจ
- ความสำคัญของระบบ
- อายุความลับของข้อมูล
- ข้อผูกพันตามกฎหมาย
- การพึ่งพาผู้ให้บริการ

4 ทดสอบก่อนเปลี่ยนจริง



มีการทดสอบก่อนการเปลี่ยนผ่าน หรือการใช้งานจริง โดยอาจทดสอบกับโครงการนำร่อง ในขอบเขตที่ควบคุมได้ก่อน

5 สร้างความสามารถในการเปลี่ยนผ่านอย่างต่อเนื่อง



- พัฒนาความคล่องตัวทางวิทยาการรหัสลับ (Crypto Agility)
- ผนวกการดำเนินการเข้ากับวงจรการพัฒนา ระบบ การจัดซื้อจัดจ้าง และการตรวจสอบ พร้อมทบทวนมาตรฐาน ความเสี่ยง และแผนงานอย่างสม่ำเสมอ



ประเด็นติดตามสำหรับคณะกรรมการ

- กำหนดให้ Quantum Risk เป็นความเสี่ยงเชิงยุทธศาสตร์ และเชื่อมโยงกับระบบการบริหารความเสี่ยงขององค์กร
- กำหนดผู้บริหาร / ฝ่ายงานที่รับผิดชอบ จัดสรรงบประมาณ และทรัพยากรที่เหมาะสม
- มีการจัดทำบัญชีรายการการเข้ารหัส โดยให้ความสำคัญกับข้อมูลและระบบที่มีความเสี่ยงสูง
- มีการจัดทำ Roadmap การเตรียมความพร้อมในด้านที่เกี่ยวข้อง
- ติดตามความคืบหน้าและปัญหาอุปสรรคเป็นระยะ

ตัวอย่างผลลัพธ์ที่คาดหวังใน 12 เดือนแรก



มีผู้บริหารที่รับผิดชอบหลักและบทบาทของแต่ละฝ่ายชัดเจน



มีบัญชีรายการการใช้รหัสลับของระบบสำคัญ พร้อมระบุส่วนที่ยังสำรวจไม่ครบ



จัดลำดับความสำคัญ ระบุข้อมูล ระบบ และธุรกรรมที่ต้องดำเนินการก่อนพร้อมเหตุผล



มีการบริหารความเสี่ยงในด้านผู้ค้าและผู้ให้บริการที่เกี่ยวข้อง



มีการกำหนด Roadmap มีการจัดสรรงบประมาณเบื้องต้น



มีโครงการนำร่อง ทดสอบก่อนการเปลี่ยนผ่านหรือการใช้งานจริง



มีการรายงานความคืบหน้า ความเสี่ยงคงเหลือ ปัญหาอุปสรรคงบประมาณ และเรื่องที่ต้องตัดสินใจ ต่อคณะกรรมการ



“การเตรียมพร้อมรับยุค Quantum ไม่ใช่เรื่องของอนาคต แต่คือการตัดสินใจของวันนี้ การเริ่มตั้งแต่วันนี้ คือโอกาสในการรักษาความเชื่อมั่นได้อย่างยั่งยืน”

สารบัญ

หัวข้อ	หน้า
บทนำ	01
1. ความเสี่ยงเชิงยุทธศาสตร์จาก Quantum Computing: เหตุใดจึงเป็นวาระสำคัญของคณะกรรมการ	05
2. ทางเลือกเทคโนโลยีเพื่อรับมือความเสี่ยงด้านควอนตัม	09
3. กรอบเวลาการเตรียมความพร้อม: การดำเนินการและเป้าหมาย	12
4. การกำกับดูแลความเสี่ยงด้านควอนตัม: บทบาทและความรับผิดชอบของผู้เกี่ยวข้อง	14
5. บัญชีรายการการใช้รหัสลับ (CBOM) และการจัดลำดับความสำคัญของข้อมูลและระบบ	17
6. Crypto Agility ความคล่องตัวทางวิทยาการรหัสลับ: การเปลี่ยนรหัสลับรองรับความเสี่ยงใหม่โดยไม่กระทบความต่อเนื่องทางธุรกิจ	20
7. ความเสี่ยงจากห่วงโซ่อุปทาน: ความพร้อมของคู่ค้าและผู้ให้บริการภายนอกต่อการเปลี่ยนผ่านไปสู่ PQC	22
8. การเตรียมความพร้อมด้านบุคลากร	25
9. จากแผนสู่การปฏิบัติ: แผนการเปลี่ยนผ่าน 5 ระยะ	27
ภาคผนวกและเอกสารอ้างอิง	
ภาคผนวก ก — ชุดเครื่องมือสำหรับคณะกรรมการ	
เครื่องมือที่ 1 — ชุดคำถามเพื่อการกำกับดูแล	29
เครื่องมือที่ 2 — ตารางกลั่นกรองความเสี่ยงและลำดับงาน	33
เครื่องมือที่ 3 — Dashboard สำหรับคณะกรรมการ	34
เครื่องมือที่ 4 — สรุปภาพรวมคู่ค้า / ผู้ให้บริการรายสำคัญสำหรับคณะกรรมการ	36
ภาคผนวก ข — อภิธานศัพท์	37
เอกสารอ้างอิง	41

บทนำ

คอมพิวเตอร์ควอนตัมมีศักยภาพสร้างประโยชน์อย่างมาก แต่ในอีกด้านหนึ่ง หากพัฒนาไปถึงระดับที่ถอดรหัสข้อมูลซึ่งใช้อยู่ในปัจจุบันได้ หรือที่เรียกว่า **Cryptographically Relevant Quantum Computer (CRQC)** ก็อาจส่งผลกระทบต่อข้อมูลการทำธุรกรรม ลายมือชื่อดิจิทัล ใบรับรองอิเล็กทรอนิกส์ และข้อมูลสำคัญขององค์กร แม้ยังไม่มีผู้ใดระบุได้แน่ชัดว่าจะเกิดขึ้นเมื่อใด แต่จากการประเมินความเห็นของผู้เชี่ยวชาญตามรายงาน Quantum Threat Timeline ของ Global Risk Institute ชี้ให้เห็นว่าความเสี่ยงอาจมีนัยสำคัญตั้งแต่ช่วงทศวรรษ 2030 ดังนั้น การเตรียมความพร้อมจึงมีใช้เรื่องของอนาคตอันไกล แต่เป็นวาระที่ควรเริ่มพิจารณาตั้งแต่วันนี้

ความเสี่ยงไม่ได้มีเพียงข้อมูลลับถูกเปิดเผย แต่อาจกระทบถึง “ความเชื่อถือ” ในโลกดิจิทัลด้วย ประเด็นแรกคือ **Harvest Now, Decrypt Later (HNDL)** หรือ “ดักเก็บข้อมูลที่ยังอ่านไม่ได้ในวันนี้ แล้วรอถอดรหัสในอนาคต” ซึ่งกระทบความลับของข้อมูล อีกประเด็นหนึ่งมักเรียกว่า **Trust Now, Forge Later (TNFL)** หรือ “สิ่งที่เราเชื่อว่าเป็นของจริงในวันนี้ อาจถูกปลอมได้ในอนาคต” เมื่อผู้โจมตีสามารถปลอมลายมือชื่อดิจิทัลหรือใบรับรองอิเล็กทรอนิกส์ ระบบอาจแยกของจริงออกจากของปลอมไม่ได้ และอาจยอมรับผู้สวมรอยเป็นลูกค้า ผู้บริหาร คู่ค้า ผู้ให้บริการ หรือระบบที่เชื่อถือได้ รวมถึงรับเอกสาร คำสั่งธุรกรรม เว็บไซต์ หรือซอฟต์แวร์อัปเดตปลอมว่าเป็นของแท้ ความเสี่ยงจาก Quantum Computing จึงครอบคลุมทั้ง **ความลับของข้อมูล ความถูกต้องของข้อมูล และการยืนยันตัวตน** ขณะที่การสำรวจระบบ ปรับเทคโนโลยี การทดสอบ และการประสานคู่ค้าหรือผู้ให้บริการ อาจต้องใช้เวลาเป็นปีถึงหลายปี

สัญญาณจากทั่วโลกชัดเจนขึ้น หลายประเทศไม่ได้รอให้ Quantum Computing มาถึงก่อน แต่ได้กำหนดกรอบเตรียมพร้อมรองรับแล้ว สหรัฐอเมริกาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) ประกาศมาตรฐานการเข้ารหัสข้อมูลแบบใหม่ สหราชอาณาจักรและแคนาดา วางเป้าหมายเปลี่ยนผ่านเป็นระยะจนถึงปี 2035 และสหภาพยุโรปเร่งให้โครงสร้างพื้นฐานสำคัญดำเนินการเตรียมพร้อมรองรับภายในปี 2030 ทิศทางที่สอดคล้องกันของนานาประเทศมิได้เป็นการยืนยันช่วงเวลาที่จะเกิดขึ้น หากแต่สะท้อนว่าหน่วยงานกำกับดูแลและหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสากลประเมินสอดคล้องกันว่า ความเสี่ยงดังกล่าวมีนัยสำคัญเพียงพอที่จะกำหนดเป็นวาระเชิงนโยบาย และการเปลี่ยนผ่านเป็นกระบวนการที่ใช้ระยะเวลาดำเนินการหลายปี ดังนั้น การเตรียมความพร้อมจึงควรเริ่มดำเนินการตั้งแต่ปัจจุบัน

สำหรับประเทศไทย เพื่อให้การดำเนินงานของหน่วยงานภาครัฐ หน่วยงานกำกับดูแล ผู้ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และองค์กรภาคเอกชนเป็นไปในทิศทางเดียวกัน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้จัดทำ (ร่าง) กรอบการเตรียมความพร้อมเข้าสู่ยุคควอนตัม พ.ศ. 2569–2578 (ค.ศ. 2026–2035) เพื่อกำหนดทิศทางและเป้าหมายเชิงเวลาระดับประเทศ โดยสรุปตามภาพด้านล่าง



ในการนี้ องค์กรในภาคตลาดทุนอาจพิจารณาจัดทำแผนการเตรียมความพร้อมของตนเองให้สอดคล้องกับกรอบระยะเวลาและหมวดหมู่ระดับประเทศข้างต้น โดยปรับใช้ให้เหมาะสมกับลักษณะระบบงาน ระดับความเสี่ยง และข้อจำกัดในทางปฏิบัติของแต่ละองค์กร เพื่อให้การเตรียมความพร้อมของภาคตลาดทุนโดยรวมเป็นไปในทิศทางเดียวกันและบรรลุเป้าหมายตามกรอบเวลาระดับประเทศ

กรอบเวลาการเปลี่ยนผ่านระดับประเทศ และเป้าหมายการเตรียมความพร้อมขององค์กร		
ระยะที่ 1 2026	จัดตั้งกลไกและเตรียมพื้นฐาน	จัดตั้งกลไกขับเคลื่อนภายในองค์กร มอบหมายผู้รับผิดชอบ และเตรียมเครื่องมือพื้นฐานสำหรับการสำรวจและติดตาม
ระยะที่ 2 2026–2027	สำรวจระบบและวางแผนเปลี่ยนผ่าน	สำรวจการใช้งานรหัสลับ จัดทำบัญชีรายการการใช้รหัสลับ (CBOM) จัดระดับความเสี่ยง ระบุระบบสำคัญและระบบนำร่อง และจัดทำแผนการเปลี่ยนผ่าน
ระยะที่ 3 2028–2030	นำร่อง ทดสอบ และลดความเสี่ยงระบบผลกระทบสูง	ดำเนินโครงการนำร่อง ทดสอบความเหมาะสมและความเข้ากันได้ และเร่งลดความเสี่ยงของระบบที่มีผลกระทบสูง
ระยะที่ 4 2031–2035	ขยายผลและเลิกใช้อัลกอริทึมที่เปราะบาง	ขยายการเปลี่ยนผ่านในวงกว้าง ทดสอบเลิกใช้อัลกอริทึมรหัสลับที่เปราะบาง และประเมินความพร้อมอย่างต่อเนื่อง
เป้าหมายภายใน 2030	ระบบงานสำคัญและระบบที่มีความเสี่ยงสูง	โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ระบบงานสำคัญ ระบบโครงสร้างพื้นฐานความน่าเชื่อถือ เช่น PKI ลายมือชื่อดิจิทัล และระบบบริหารจัดการกฎหมาย รวมถึงระบบที่ถือครองข้อมูลที่ต้องรักษาความลับเป็นเวลานาน ควรลดความเสี่ยงหรือเปลี่ยนผ่านส่วนที่มีความเสี่ยงสูงให้แล้วเสร็จ
เป้าหมายภายใน 2035	ระบบงานทั่วไปและระบบบริการดิจิทัล	ควรเปลี่ยนผ่านให้แล้วเสร็จหรือมีมาตรการรองรับที่เหมาะสมตามระดับความเสี่ยงและความพร้อมของแต่ละระบบ สอดคล้องกับทิศทางของสหราชอาณาจักร แคนาดา ญี่ปุ่น และการเลิกใช้อัลกอริทึมรหัสลับที่เปราะบางตามแนวทางของ NIST
หมายเหตุ: กรอบเวลาข้างต้นใช้เพื่อวางแผนการเตรียมความพร้อม มิใช่การคาดการณ์ปีที่ภัยจากคอมพิวเตอร์ควอนตัมจะเกิดขึ้น		

คู่มือฉบับนี้เป็นแนวทางหรือข้อเสนอแนะในเบื้องต้นสำหรับคณะกรรมการ และผู้บริหารระดับสูงขององค์กรในตลาดทุน เพื่อสนับสนุนการกำกับดูแลความเสี่ยง และมีใช้ข้อกำหนดทางกฎหมายหรือมาตรฐานบังคับใช้สำหรับทุกองค์กร การนำไปใช้จึงควรพิจารณาตามรูปแบบธุรกิจ ความสำคัญของระบบ อายุความลับของข้อมูล การผูกพันตามกฎหมาย และการพึ่งพาผู้ค้าหรือผู้ให้บริการภายนอกของแต่ละแห่ง

สาระสำคัญของคู่มือนี้จึงมิใช่การเร่งเปลี่ยนอัลกอริทึมทั้งหมดในคราวเดียว แต่คือการเริ่มจากสิ่งที่องค์กรทำได้ทันทีและเกิดประโยชน์อย่างคุ้มค่า ได้แก่ กำหนดผู้บริหารที่รับผิดชอบหลัก จัดทำบัญชีรายการการใช้รหัสลับ ระบุข้อมูลและระบบที่มีความเสี่ยงสูง ประเมินความพร้อมของผู้ค้าและผู้ให้บริการ ทดลองในขอบเขตที่ควบคุมได้ และสร้างความสามารถการเปลี่ยนรหัสลับรองรับความเสี่ยงใหม่โดยไม่กระทบความต่อเนื่องทางธุรกิจ (Crypto Agility) การดำเนินการดังกล่าวจะช่วยให้องค์กรมีข้อมูลและทางเลือกเพียงพอ สามารถกำหนดจังหวะการเปลี่ยนผ่านได้ด้วยตนเองบนฐานความเสี่ยงที่เหมาะสม และดำเนินการได้อย่างเป็นลำดับภายในกรอบเวลาที่วางแผนไว้

บทที่ 1

ความเสี่ยงเชิงยุทธศาสตร์จาก Quantum Computing: เหตุใดจึงเป็นวาระสำคัญของคณะกรรมการ

ความก้าวหน้าของ Quantum Computing กำลังท้าทายกลไกที่โลกดิจิทัลใช้รักษาความลับ ยืนยันตัวตนบุคคล และรับรองว่าข้อมูลมีความถูกต้อง ซึ่งเป็นกลไกเดียวกับที่ระบบซื้อขายหลักทรัพย์ การชำระราคาและส่งมอบ และการให้บริการผู้ลงทุนใช้อยู่เป็นประจำ ความเสี่ยงนี้จึงไม่ใช่เพียงเรื่องของเครื่องคอมพิวเตอร์รุ่นใหม่ แต่เป็นความเสี่ยงต่อความน่าเชื่อถือของธุรกรรมและบริการดิจิทัลที่องค์กรในภาคตลาดทุนพึ่งพาอยู่ทุกวัน

ระบบงานสำคัญของภาคตลาดทุน ตั้งแต่การเปิดบัญชีและยืนยันตัวตนผู้ลงทุน การส่งคำสั่งซื้อขาย การชำระราคาและส่งมอบหลักทรัพย์ ไปจนถึงการเชื่อมต่อข้อมูลระหว่างผู้ประกอบการธุรกิจกับโครงสร้างพื้นฐานของตลาด ล้วนอาศัยการเข้ารหัสลับแบบกุญแจสาธารณะ (Asymmetric Key Encryption) เช่น RSA และ ECC เพื่อแลกเปลี่ยนกุญแจและสร้างลายมือชื่อดิจิทัล ระบบเหล่านี้ยังคงมีความมั่นคงปลอดภัยเพียงพอต่อการโจมตีด้วยคอมพิวเตอร์ทั่วไป หากใช้งานอย่างเหมาะสม แต่ Quantum Computing ที่มีขีดความสามารถเพียงพออาจใช้อัลกอริทึมของชอร์ (Shor's Algorithm) แก้ไขทฤษฎีคณิตศาสตร์ที่เป็นฐานความมั่นคงปลอดภัยของระบบดังกล่าวได้ ผลกระทบจึงไม่ได้จำกัดอยู่ที่การอ่านข้อความลับ แต่อาจรวมถึงการปลอมลายมือชื่อ ใบรับรอง เว็บไซต์ ซอฟต์แวร์ หรือคำสั่งธุรกรรมให้ระบบเชื่อว่าเป็นของจริง

ส่วนการเข้ารหัสแบบกุญแจเดียวกันทั้งสองฝ่าย (Symmetric Key Encryption) เช่น AES ซึ่งใช้ปกป้องข้อมูลปริมาณมากทั้งที่จัดเก็บไว้และที่รับส่งระหว่างระบบ จะได้รับผลกระทบน้อยกว่ามาก และยังสามารถจัดการความเสี่ยงได้ด้วยการเลือกขนาดกุญแจที่เหมาะสมตามมาตรฐานที่ได้รับการปรับปรุง ดังนั้น ประเด็นสำหรับคณะกรรมการจึงไม่ใช่การสั่งเลิกใช้การเข้ารหัสทั้งหมด แต่คือการให้ฝ่ายบริหารแยกให้ออกว่า ส่วนใดมีความเสี่ยงสูง ส่วนใดปรับปรุงได้ และส่วนใดต้องการเปลี่ยนผ่านร่วมกับคู่ค้าหรือผู้ให้บริการที่องค์กรใช้บริการอยู่

ความเร่งด่วนเกิดจากผลกระทบสองด้าน ด้านแรกคือ **Harvest Now, Decrypt Later (HNDL)** หรือ “ดักเก็บข้อมูลวันนี้เพื่อถอดรหัสในอนาคต” ด้านที่สองคือ **Trust Now, Forge Later (TNFL)** หรือ “ความน่าเชื่อถือที่ระบบยอมรับในวันนี้อาจถูกปลอมได้ในอนาคต” สำหรับภาคตลาดทุน ความเสี่ยงทั้งสองมีผลต่อระบบงานอย่างเป็นรูปธรรม ข้อมูลผู้ลงทุนและประวัติการซื้อขายที่ต้องจัดเก็บตามระยะเวลาที่กฎหมายกำหนด ตลอดจนข้อมูลที่ยังไม่เปิดเผยต่อสาธารณะ เช่น การควบรวมกิจการหรือคำสั่งซื้อขายขนาดใหญ่ อาจถูกดักเก็บไว้ตั้งแต่วันนี้และถูกเปิดเผยในภายหลัง ขณะที่การยืนยันตัวตนผู้ลงทุน ลายมือชื่อดิจิทัลบนคำสั่งซื้อขาย และใบรับรองที่ใช้เชื่อมต่อกับโครงสร้างพื้นฐานของตลาด หากถูกปลอมย่อนำไปสู่การสวมรอยทำรายการแทนผู้ลงทุนและข้อพิพาท

เรื่องการปฏิเสธรายการ ผลกระทบจึงอาจลุกลามจากเหตุข้อมูลรั่วไปสู่วิกฤตความเชื่อมั่น และเนื่องจากตลาดทุนมีลักษณะเป็นโครงสร้างที่ทุกฝ่ายเชื่อมต่อถึงกัน ความเสี่ยงจึงมิได้จำกัดอยู่ที่องค์กรใดองค์กรหนึ่งเพียงลำพัง

ตัวอย่าง ความเสี่ยงจากควอนตัมต่อระบบงานสำคัญในภาคตลาดทุน		
ข้อมูลหรือระบบงาน	ลักษณะความเสี่ยง	ผลกระทบต่อธุรกิจและความเชื่อมั่น
ข้อมูลผู้ลงทุนและประวัติการซื้อขายที่ต้องจัดเก็บตามระยะเวลาที่กฎหมายกำหนด	HNDL	ข้อมูลที่ถูกดักเก็บในวันนี้อาจถูกเปิดเผยภายหลัง พร้อมความรับผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล
ข้อมูลที่ยังไม่เปิดเผยต่อสาธารณะ เช่น การควบรวมกิจการ บทวิเคราะห์ คำสั่งซื้อขายขนาดใหญ่	HNDL	สูญเสียความได้เปรียบทางธุรกิจ และอาจกระทบความเป็นธรรมของตลาด
การยืนยันตัวตนผู้ลงทุนและการเปิดบัญชีทางอิเล็กทรอนิกส์	TNFL	การเปิดบัญชีสวมรอยหรือทำรายการแทนผู้ลงทุน
ลายมือชื่อดิจิทัลบนคำสั่งซื้อขายและเอกสารยืนยันรายการ	TNFL	ข้อพิพาทจากการปฏิเสธรายการ และการในการพิสูจน์ความถูกต้องของธุรกรรม
กุญแจที่ใช้ดูแลทรัพย์สินของลูกค้า	HNDL, TNFL	ความเสียหายต่อทรัพย์สินของลูกค้าโดยตรง และความรับผิดของผู้ประกอบธุรกิจ
การเชื่อมต่อระหว่างผู้ประกอบการธุรกิจกับโครงสร้างพื้นฐานของตลาด	HNDL, TNFL	ความเสี่ยงลุกลามทั้งระบบ มิใช่เฉพาะรายองค์กร จึงต้องเปลี่ยนผ่านอย่างประสานกัน



ด้วยเหตุที่ความเสี่ยงข้างต้นส่งผลถึงข้อมูล ธุรกิจ และความเชื่อมั่นของผู้ลงทุนโดยตรง การเตรียมความพร้อมจึงเป็นวาระของการกำกับดูแล มิใช่โครงการของฝ่ายเทคโนโลยีสารสนเทศเพียงลำพัง ตามหลักการกำกับดูแลกิจการที่ดี คณะกรรมการมีหน้าที่กำหนดทิศทาง ดูแลให้มีระบบบริหารความเสี่ยงและการควบคุมภายในที่เหมาะสม ตลอดจนติดตามผลการดำเนินงาน ในบริบทนี้ คณะกรรมการจึงมีบทบาทสำคัญในการทำให้องค์กรมองเห็นจุดเสี่ยงได้อย่างชัดเจน มีผู้รับผิดชอบที่ระบุได้ จัดลำดับความสำคัญบนฐานผลกระทบทางธุรกิจ และจัดสรรเวลางบประมาณ และบุคลากรอย่างเพียงพอต่อการดำเนินงาน

ในระดับสากล ภาคการเงินการธนาคารได้ก้าวจากการตระหนักรู้สู่การทดลองใช้งานจริงแล้ว เช่น Project Leap ของธนาคารเพื่อการชำระหนี้ระหว่างประเทศ (BIS Innovation Hub) ร่วมกับธนาคารกลางหลายแห่ง ได้ทดสอบการใช้วิทยาการรหัสลับหลังยุคควอนตัม (Post-Quantum Cryptography) กับการสื่อสารและระบบชำระเงิน และแสดงให้เห็นว่าการเปลี่ยนผ่านสามารถดำเนินการได้จริง โดยมีปัจจัยที่ต้องเตรียมการอย่างรอบคอบ ได้แก่ ประสิทธิภาพ ความเข้ากันได้กับระบบเดิม การประสานงาน และการทดสอบ บทเรียนสำหรับคณะกรรมการ จึงชัดเจนว่า การเริ่มดำเนินการตั้งแต่วันนี้มิได้หมายถึงการเปลี่ยนทุกระบบพร้อมกัน หากแต่เป็นการสร้างข้อมูลและทางเลือกให้พร้อม เพื่อให้องค์กรสามารถกำหนดจังหวะการเปลี่ยนผ่านได้ด้วยตนเองภายในกรอบเวลาที่วางแผนไว้

✓ สิ่งที่ต้องทำ	✗ สิ่งที่ไม่ควรทำ
✓ กำกับให้ฝ่ายบริหารนำความเสี่ยงจากควอนตัมเข้าสู่กระบวนการบริหารความเสี่ยงองค์กร และเชื่อมโยงกับผลกระทบทางธุรกิจ	✗ มองเป็นเรื่องเทคนิคของฝ่ายเทคโนโลยีสารสนเทศเท่านั้น จนไม่มีผู้รับผิดชอบทางธุรกิจและไม่เชื่อมกับความเสี่ยงองค์กร
✓ ขอภาพรวมที่เข้าใจได้และมีหลักฐาน ว่าข้อมูล ระบบ และธุรกิจใดเสี่ยง รวมถึงดำเนินการถึงขั้นใดแล้ว	✗ รับรายงานว่า “อยู่ระหว่างดำเนินการ” โดยไม่มีขอบเขตระบบเสี่ยงสูง กรอบเวลา หรือหลักฐานประกอบ
✓ กำกับให้ฝ่ายบริหารเริ่มสำรวจและจัดลำดับความเสี่ยงตั้งแต่วันนี้ โดยเริ่มจากข้อมูลที่ต้องเก็บเป็นความลับเป็นเวลานาน ระบบที่ใช้ยืนยันตัวตน และระบบงานสำคัญ	✗ รอให้รู้วันเกิดเหตุแน่นอนจึงเริ่ม ทั้งที่ข้อมูลอาจถูกดักเก็บแล้วและการเปลี่ยนระบบต้องใช้เวลาเป็นปีถึงหลายปี
✓ ขอให้ฝ่ายบริหารเสนอการเปลี่ยนผ่านเป็นลำดับและมีผลทดสอบก่อนขยายผล โดยเริ่มจากระบบสำคัญตามความเสี่ยงและตรวจสอบความเข้ากันได้กับระบบเดิม	✗ เร่งซื้อเทคโนโลยีหรือเปลี่ยนทุกระบบพร้อมกัน ก่อนรู้จุดเสี่ยง ผลกระทบ และความพร้อมของระบบเดิม
✓ ขอแผนและหลักฐานจากคู่ค้า / ผู้ให้บริการที่สำคัญ พร้อมข้อผูกพัน ผลทดสอบ และแผนสำรองหากเปลี่ยนผ่านไม่ทัน	✗ เชื่อคำรับรองของคู่ค้า / ผู้ให้บริการเพียงอย่างเดียว โดยไม่มีผลทดสอบ ข้อผูกพันตามสัญญา หรือทางเลือกสำรอง

คำถามเพื่อการกำกับดูแล

1. องค์กรได้นำความเสี่ยงจากเทคโนโลยีควอนตัมเข้าสู่ทะเบียนความเสี่ยงองค์กรแล้วหรือไม่ และผู้บริหารท่านใดเป็นผู้รับผิดชอบหลักต่อผลลัพธ์โดยรวม?
2. ข้อมูลหรือธุรกรรมใดขององค์กรต้องได้รับการคุ้มครองเป็นเวลานาน และมีความเสี่ยงจากการถูกดักเก็บวันนี้เพื่อรอถอดรหัสในอนาคต?
3. ระบบใดอาจได้รับผลกระทบหากลายมือชื่อดิจิทัล ใ้รับรอง หรือการยืนยันตัวตนถูกปลอมได้ และผลกระทบต่อธุรกิจรวมถึงความเชื่อมั่นจะเป็นอย่างไร?
4. ฝ่ายบริหารประเมินหรือยังว่าองค์กรต้องใช้เวลาเท่าใดในการสำรวจ ทดสอบ และเปลี่ยนผ่านระบบสำคัญ และสมมติฐานดังกล่าวอาศัยข้อมูลใด?
5. ภายใน 12 เดือนข้างหน้า คณะกรรมการควรคาดหวังผลลัพธ์ใดจากฝ่ายบริหาร และมีเรื่องใดที่ต้องการการตัดสินใจงบประมาณ หรือการยกระดับจากคณะกรรมการ?

บทที่ 2

ทางเลือกเทคโนโลยีเพื่อรับมือความเสี่ยงด้านควอนตัม

เมื่อองค์กรเข้าใจแล้วว่าภัยควอนตัมกระทบทั้งความลับ ความถูกต้อง และการยืนยันตัวตน คำถามถัดไปคือ “ควรใช้เทคโนโลยีใดรับมือ” คำตอบไม่ได้มีเพียงทางเลือกเดียว ปัจจุบันมี 3 แนวทางที่มักกล่าวถึง ได้แก่ **แนวทางที่ 1 วิทยาการรหัสลับหลังยุคควอนตัม (Post-Quantum Cryptography: PQC)** **แนวทางที่ 2 การแจกจ่ายกุญแจเชิงควอนตัม (Quantum Key Distribution: QKD)** และ **แนวทางที่ 3 เครื่องสร้างเลขสุ่มเชิงควอนตัม (Quantum Random Number Generator: QRNG)** ทั้งนี้ ทั้ง 3 แนวทางช่วยคนละหน้าที่และไม่สามารถใช้แทนกันได้ทั้งหมด

PQC คือการเปลี่ยนระบบการเข้ารหัสข้อมูลใหม่ที่ปลอดภัยและทนต่อการถอดรหัสดังจาก Quantum Computing จากคณิตศาสตร์ที่ควอนตัมอาจแก้ได้ ไปเป็นคณิตศาสตร์แบบใหม่ที่ออกแบบให้ทนต่อทั้งคอมพิวเตอร์ทั่วไปและคอมพิวเตอร์ควอนตัม จุดเด่นคือเป็นแนวทางซอฟต์แวร์ที่นำไปผนวกกับผลิตภัณฑ์ บริการ และระบบเดิมได้ในวงกว้าง จึงเป็นฐานหลักของการเปลี่ยนผ่านสำหรับองค์กรส่วนใหญ่ NIST ประกาศมาตรฐาน FIPS 203–205 แล้ว และแนะนำให้องค์กรเริ่มนำมาตรฐานดังกล่าวไปใช้และวางแผนเปลี่ยนผ่านได้ทันที อย่างไรก็ตาม คำว่า “ติดตั้งได้บนระบบเดิม” ไม่ได้แปลว่าเป็นเพียงการกดอัปเดต เพราะอาจต้องปรับโปรโตคอล แอปพลิเคชัน อุปกรณ์ และการเชื่อมต่อกับคู่ค้าหรือผู้ให้บริการ รวมถึงทดสอบประสิทธิภาพและความเข้ากันได้ก่อนใช้งานจริง

QKD ใช้คุณสมบัติทางฟิสิกส์ควอนตัมในการสร้างและส่งกุญแจระหว่างจุดสื่อสาร โดยเป็นช่องทางส่งกุญแจที่สามารถตรวจพบได้เมื่อมีการดักฟังหรือแทรกแซง อย่างไรก็ตาม QKD ปกป้องเฉพาะขั้นตอนการแจกจ่ายกุญแจ ไม่ได้เข้ารหัสข้อมูลหรือยืนยันตัวตนได้ครบถ้วนด้วยตัวเอง จึงยังต้องใช้ร่วมกับกลไกอื่น รวมถึง PQC นอกจากนี้ ยังต้องพึ่งอุปกรณ์และโครงข่ายเฉพาะ มีข้อจำกัดด้านระยะทาง การขยายระบบ การเชื่อมต่อหลายจุด และต้นทุน จึงเหมาะกับกรณีเฉพาะที่มีความจำเป็นสูงและผ่านการวิเคราะห์ความคุ้มค่า มีใช้คำตอบเริ่มต้นสำหรับทุกองค์กร

QRNG ใช้ปรากฏการณ์ควอนตัมในการสร้างเลขสุ่มสำหรับกุญแจและกระบวนการด้านความมั่นคงปลอดภัย จึงช่วยให้วัตถุดิบที่ใช้สร้างกุญแจมีความคาดเดายากยิ่งขึ้น อย่างไรก็ตาม QRNG มิได้เปลี่ยนรหัสที่เปราะบางให้ทนต่อควอนตัม และมีใช้มาตรการทดแทน PQC คุณค่าของ QRNG จึงไม่ได้อยู่ที่ตัวอุปกรณ์เพียงอย่างเดียว แต่อยู่ที่หลักฐานว่าเลขสุ่มที่ใช้สร้างกุญแจมีคุณภาพ ตรวจสอบความผิดปกติได้ และเชื่อมต่อกับระบบบริหารจัดการกุญแจขององค์กรอย่างปลอดภัย

สำหรับองค์กรส่วนใหญ่ ลำดับคิดที่เหมาะสมคือ **เริ่มจาก PQC เป็นฐาน** แล้วพิจารณา QKD หรือ QRNG เฉพาะเมื่อมีกรณีใช้งานรองรับ ในช่วงเปลี่ยนผ่าน องค์กรอาจใช้ **แนวทางแบบผสมผสาน (Hybrid Approach)** คือใช้รหัสแบบเดิมร่วมกับ PQC เพื่อลดการพึ่งพาเทคโนโลยีใหม่เพียงขั้นเดียว แต่ต้องกำหนดวิธีผสมให้ถูกต้องและ

ผ่านการทดสอบ เพราะการมีสองอัลกอริทึมไม่ได้ทำให้ระบบปลอดภัยขึ้นโดยอัตโนมัติ ประเด็นที่คณะกรรมการควรกำกับจึงไม่ใช่ “จะเลือกเทคโนโลยีใด” แต่คือฝ่ายบริหารมีเหตุผลทางธุรกิจ หลักฐานการทดสอบ ต้นทุนรวม และแผนรองรับเพียงพอหรือไม่

ทางเลือก	ช่วยเรื่องใด	เหมาะเมื่อใด	ข้อจำกัดสำคัญ
PQC รหัสแบบใหม่	แลกเปลี่ยนกุญแจและ ลงลายมือชื่อให้ทนต่อควอนตัม	เป็นฐานหลักสำหรับองค์กร ส่วนใหญ่และระบบทั่วไป	ต้องปรับและทดสอบระบบเดิม ประสิทธิภาพ และการทำงาน ร่วมกับคู่ค้าหรือผู้ให้บริการ
QKD ส่งกุญแจผ่าน ควอนตัม	ช่วยตรวจพบการดักฟังระหว่าง ส่งกุญแจ	การเชื่อมต่อเฉพาะจุดที่มี ความสำคัญและมีเหตุผล รองรับสูง	ไม่ยืนยันตัวตนด้วยตัวเอง ต้องใช้ โครงข่ายเฉพาะและมีต้นทุนสูง
QRNG สร้างเลขสุ่ม	เพิ่มคุณภาพของเลขสุ่มที่ใช้ สร้างกุญแจ	ระบบที่ต้องการแหล่งเลขสุ่ม คุณภาพสูงและตรวจสอบได้	ไม่ทดแทน PQC และต้องประเมิน คุณภาพอุปกรณ์กับการเชื่อม ระบบ

✓ สิ่งที่ต้องทำ	✗ สิ่งที่ไม่ควรทำ
✓ พิจารณาเริ่มจาก PQC หรือเทคโนโลยีที่เหมาะสมเป็นฐาน และให้ฝ่ายบริหารประเมินระบบที่ต้องปรับพร้อมผลกระทบ	✗ เริ่มจากเทคโนโลยีที่ดูทันสมัยที่สุด โดยยังไม่รู้ว่าช่วยลดความเสี่ยงใดขององค์กร
✓ ขอผลทดสอบกับระบบงานขององค์กร ทั้งประสิทธิภาพ ความเข้ากันได้ และผลต่อบริการ โดยอาจทำ เป็นโครงการนำร่องบางระบบก่อน	✗ เชื่อว่า PQC เป็นเพียงการอัปเดตซอฟต์แวร์ แล้วนำไปใช้โดยไม่ทดสอบผลกระทบกับระบบและบริการ ที่เชื่อมต่อก่อน
✓ พิจารณาข้อเสนอใช้ QKD กรณีที่มีความจำเป็นและมีเหตุผล รองรับ พร้อมขอการประเมินการยืนยันตัวตน โครงข่าย และ ต้นทุนรวม	✗ เข้าใจว่า QKD ทำให้การสื่อสารปลอดภัยครบทุกด้าน ทั้งที่ยังต้องใช้กลไกยืนยันตัวตนและการเข้ารหัสอื่นร่วมด้วย
✓ พิจารณาข้อเสนอใช้ QRNG เมื่อมีความต้องการเพิ่ม คุณภาพของเลขสุ่มที่ใช้สร้างกุญแจ และขอหลักฐานวิธี ตรวจสอบคุณภาพ	✗ เข้าใจว่าเพิ่ม QRNG แล้วระบบจะทนต่อควอนตัม แม้อัลกอริทึมหลักยังมีความเปราะบาง
✓ กำหนดให้ทุกโครงการนำร่องมีเกณฑ์ตัดสินใจและทางออก ที่ชัดเจน รวมถึงเงื่อนไขหยุด เปลี่ยนแนวทาง หรือขยายผล	✗ ดำเนินการโครงการนำร่องโดยขาดการพิจารณา ไม่มีเกณฑ์ วัดผล หรือแผนถอยกลับ

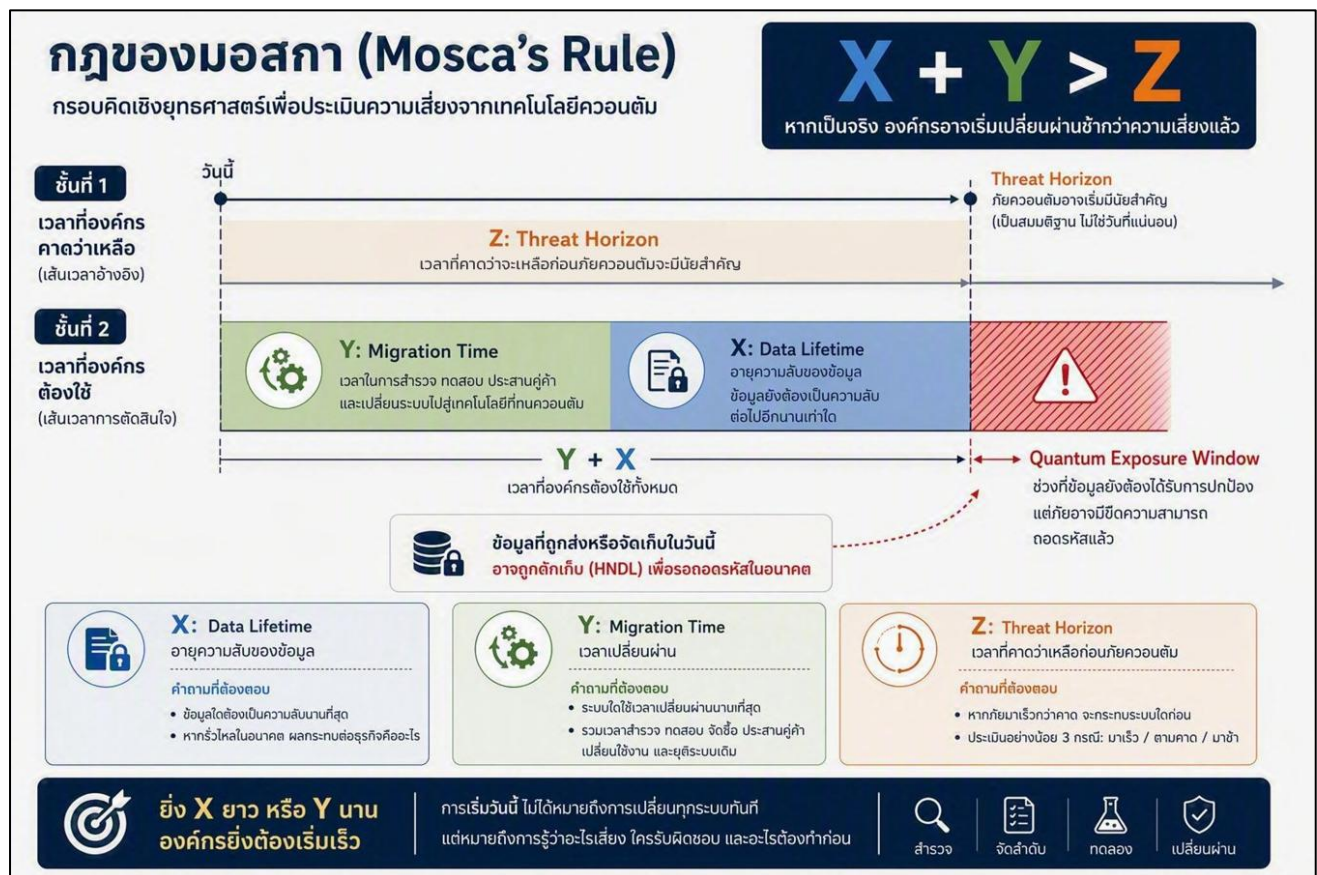
คำถามเพื่อการกำกับดูแล

1. ฝ่ายบริหารกำหนดให้ PQC เป็นแนวทางของการเปลี่ยนผ่านแล้วหรือไม่ และระบบใดควรเริ่มประเมินหรือนำร่องก่อน ด้วยเหตุผลใด?
2. ผลทดสอบ PQC ครอบคลุมผลต่อความเร็ว ความจุ ความเข้ากันได้ ความต่อเนื่องของบริการ และการเชื่อมต่อกับลูกค้า หรือผู้ให้บริการแล้วหรือยัง?
3. หากมีข้อเสนอให้ลงทุนใน QKD องค์กรกำลังแก้ความเสี่ยงใด เหตุใด PQC เพียงอย่างเดียวจึงไม่เพียงพอ และต้นทุนรวมตลอดอายุโครงการเป็นเท่าใด?
4. หากใช้ QRNG องค์กรมีวิธีพิสูจน์หรือไม่ว่าแหล่งความสุ่มมีคุณภาพ ตรวจสอบความผิดปกติได้ และเชื่อมกับระบบบริหาร ภัยอย่างปลอดภัย?
5. โครงการนำร่องแต่ละโครงการมีเกณฑ์ความสำเร็จ ผู้รับผิดชอบ งบประมาณ แผนถอยกลับ และเงื่อนไขตัดสินใจว่าจะขยายผลหรือปรับเปลี่ยนแนวทางไว้อย่างชัดเจนหรือไม่?

บทที่ 3

กรอบเวลาการเตรียมความพร้อม: การดำเนินการและเป้าหมาย

คำถามสำคัญสำหรับคณะกรรมการไม่ใช่ “คอมพิวเตอร์ควอนตัมจะมาในปีใด” แต่คือ “หากเหตุการณ์ดังกล่าวเกิดขึ้นเร็วกว่าที่คาด องค์กรจะเปลี่ยนผ่านทันหรือไม่” กฎของมอสกา (Mosca’s Theorem) ซึ่งมีอธิบายในรูปอสมการของมอสกา (Mosca’s Inequality) ช่วยตอบคำถามนี้ด้วยการพิจารณา 3 ช่วงเวลา ได้แก่ **อายุความลับของข้อมูล (X)** **เวลาที่องค์กรต้องใช้เพื่อเปลี่ยนระบบ (Y)** และ **เวลาที่คาดว่าจะเหลือก่อนที่คอมพิวเตอร์ควอนตัมจะทำลายรหัสปัจจุบันได้ (Z)** หาก $X + Y$ มากกว่า Z ข้อมูลอาจไม่ปลอดภัยตลอดอายุที่องค์กรต้องการ แม้ระบบยังไม่ถูกถอดรหัสนี้



ทั้งสามค่ามิใช่ตัวเลขตายตัว เนื่องจากข้อมูลแต่ละประเภทมีระยะเวลาที่ต้องรักษาความลับแตกต่างกัน ระบบแต่ละระบบใช้ระยะเวลาในการเปลี่ยนผ่านไม่เท่ากัน และยังไม่อาจระบุได้แน่ชัดว่าคอมพิวเตอร์ควอนตัมที่สามารถทำลายรหัสในปัจจุบันจะเกิดขึ้นเมื่อใด แนวทางที่รอบคอบคือการกำหนดให้ฝ่ายบริหารประเมินอย่างน้อย 3 กรณี ได้แก่ (1) กรณีเกิดขึ้นเร็วกว่าที่คาด (2) กรณีเป็นไปตามที่คาด และ (3) กรณีเกิดขึ้นช้ากว่าที่คาด แล้วพิจารณาว่า

ระบบใดอาจเปลี่ยนผ่านไม่ทันหากเหตุการณ์เกิดขึ้นเร็วกว่าประมาณการ แนวทางดังกล่าวช่วยให้องค์กรจัดลำดับการดำเนินงานจากจุดที่มีความเสี่ยงอย่างแท้จริง แทนการมุ่งหาข้อยุติว่าปีใดเป็นการคาดการณ์ที่แม่นยำที่สุด

สรุปกฎของมอสกา

X — ข้อมูลต้องเป็นความลับอีกนานเท่าใด: เช่น ข้อมูลลูกค้า ความลับทางการค้า หรือข้อมูลควบรวมกิจการ เป็นต้น

Y — องค์กรต้องใช้เวลาที่ปีในการเปลี่ยน: ครอบคลุมการสำรวจ การจัดซื้อ การทดสอบ ระบบเดิม และคู่ค้า / ผู้ให้บริการ

Z — คาดว่าองค์กรยังมีเวลาเหลือเท่าใด: ยังไม่มีคำตอบแน่นอน จึงควรลองคำนวณทั้งกรณีมาเร็ว ตามคาด และมาช้า

หาก $X + Y > Z$ แล้วองค์กรควรเร่งจัดลำดับและเริ่มเปลี่ยนผ่าน เพราะข้อมูลอาจเสี่ยงแล้วตั้งแต่วันนี้

✓ สิ่งที่ต้องทำ	✗ สิ่งที่ไม่ควรทำ
✓ ขอให้ฝ่ายบริหารใช้ข้อมูลเฉพาะขององค์กรเป็นฐาน ทั้งอายุ ความลับของข้อมูลและเวลาที่ต้องใช้เปลี่ยนระบบ	✗ ใช้ตัวเลขเฉลี่ยของอุตสาหกรรมแทนทั้งหมด จนมองข้ามระบบเก่าหรือข้อมูลเฉพาะขององค์กร
✓ กำกับให้ฝ่ายบริหารประเมินอย่างน้อยสามกรณี: มาเร็ว ตามคาด และมาช้า เพื่อระบุระบบที่อาจเปลี่ยนผ่านไม่ทัน	✗ ยึดปีคาดการณ์เพียงปีเดียว แล้วหยุดรอเมื่อผู้เชี่ยวชาญให้ความเห็นไม่ตรงกัน
✓ ใช้ปี 2030–2035 เป็นกรอบเวลาสำหรับวางแผนและจัดลำดับการดำเนินงาน ไม่ใช่วันที่คาดว่าเหตุการณ์จะเกิดขึ้น	✗ เข้าใจว่าแผนเปลี่ยนผ่านคือวันเกิดเหตุ หรือคิดว่าระบบจะยังปลอดภัยแน่นอนจนถึงปีนั้น
✓ กำหนดให้ฝ่ายบริหารจัดลำดับระบบสำคัญก่อน และเสนอเป้าหมายตามความเสี่ยงกับความพร้อมของระบบและคู่ค้า / ผู้ให้บริการ	✗ กำหนดกรอบเวลาเดียวกันทุกระบบ โดยไม่ดูผลกระทบและเวลาที่ต้องใช้จริง

คำถามเพื่อการกำกับดูแล

1. ข้อมูลประเภทใดต้องรักษาความลับนานที่สุด และฝ่ายบริหารกำหนดค่า X จากข้อกำหนดทางธุรกิจ กฎหมาย และสัญญาไว้อย่างไร?
2. ค่า Y ของระบบสำคัญรวมเวลาสำรวจ จัดซื้อ ทดสอบ แกะระบบเดิม และประสานคู่ค้า / ผู้ให้บริการครบแล้วหรือไม่ และมีหลักฐานใดสนับสนุน?
3. ฝ่ายบริหารลองคำนวณทั้งกรณีที่เหตุการณ์เกิดขึ้นเร็วกว่าที่คาด เป็นไปตามที่คาด และช้ากว่าที่คาดแล้วหรือยัง และหากเกิดขึ้นเร็วกว่าประมาณการ ระบบใดอาจจะเปลี่ยนไม่ทัน?
4. หมายเหตุขององค์กรสอดคล้องกับกรอบของ สกมช. และแนวนโยบายเพียงใด และระบบความเสี่ยงสูงควรมีเป้าหมายเร็วกว่ากรอบทั่วไปหรือไม่?
5. คณะกรรมการมีการทบทวนสมมติฐาน กรอบมาตรฐาน ความคืบหน้า และเรื่องที่ต้องตัดสินใจเป็นระยะหรือเมื่อมีการเปลี่ยนแปลงสำคัญหรือไม่?

บทที่ 4

การกำกับดูแลความเสี่ยงด้านควอนตัม: บทบาทและความรับผิดชอบของผู้เกี่ยวข้อง

การเปลี่ยนผ่านไปสู่วิทยาการรหัสลับหลังยุคควอนตัม (PQC) มิใช่ภารกิจของฝ่ายเทคโนโลยีสารสนเทศเพียงลำพัง เนื่องจากส่งผลกระทบต่อข้อมูลสำคัญ การให้บริการลูกค้า ข้อผูกพันตามสัญญากับลูกค้าหรือผู้ให้บริการ การจัดสรรงบประมาณ ตลอดจนความต่อเนื่องในการดำเนินธุรกิจ สิ่งที่ต้องพิจารณาจึงมีจึงมิใช่การจัดตั้งคณะทำงานเพิ่มขึ้นอีกหนึ่งชุด หากแต่เป็นการกำหนดความรับผิดชอบให้ชัดเจนว่า **ผู้ใดเป็นผู้ตัดสินใจ ผู้ใดเป็นผู้ดำเนินการ ผู้ใดเป็นผู้ติดตาม และผู้ใดเป็นผู้ตรวจสอบ**

คณะกรรมการบริษัท มีบทบาทสำคัญในการกำหนดทิศทางและระดับความเสี่ยงที่องค์กรยอมรับได้ พิจารณาอนุมัติทรัพยากรที่จำเป็น ติดตามผลการดำเนินงาน ตลอดจนสอบถามและทักทายข้อมูลเมื่อความคืบหน้ามิได้เป็นไปตามแผนที่กำหนด ทั้งนี้ ควรกำหนดให้ความเสี่ยงด้านควอนตัมเป็นส่วนหนึ่งของระบบบริหารความเสี่ยงองค์กรและแผนการลงทุนตามปกติ โดยไม่จำเป็นต้องจัดทำนโยบายฉบับใหม่ที่แยกออกจากกรอบการกำกับดูแลที่องค์กรมีอยู่แล้ว ไม่ว่าจะเป็นกรอบด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) การบริหารความเสี่ยงด้านเทคโนโลยี (Technology Risk) หรือการบริหารความเสี่ยงองค์กร (Enterprise Risk Management)

องค์กรควรแบ่งหน้าที่ตาม**หลักการ Three Lines Model** ของสถาบันผู้ตรวจสอบภายในสากล (The Institute of Internal Auditors: IIA) เพื่อให้ผู้ปฏิบัติงาน ผู้กำกับดูแล และผู้ตรวจสอบ มีบทบาทชัดเจนและถ่วงดุลกันอย่างเหมาะสมโดย

ระดับที่ 1 (First Line) ได้แก่ หน่วยธุรกิจ เจ้าของระบบ และฝ่ายเทคโนโลยีสารสนเทศ ซึ่งเป็นผู้ปฏิบัติงานและรับผิดชอบความเสี่ยงจากงานของตนโดยตรง

ระดับที่ 2 (Second Line) คือการบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง มีหน้าที่กำหนดกรอบ ให้คำแนะนำ ติดตาม และสอบถามการดำเนินงานของระดับที่ 1 เพื่อให้เกณฑ์ประเมินวิธีรายงาน และการยกระดับปัญหาเป็นมาตรฐานเดียวกัน

ระดับที่ 3 (Third Line) คือการตรวจสอบ ซึ่งให้ความเชื่อมั่นอย่างเป็นอิสระต่อคณะกรรมการบริษัทและคณะกรรมการตรวจสอบว่า การกำกับดูแล การบริหารความเสี่ยง และการควบคุมการทำงานตามที่กำหนด ซึ่งการตรวจสอบควรเน้นคุณภาพของหลักฐาน เช่น ความครบถ้วนของขอบเขตสำรวจ เหตุผลในการจัดลำดับระบบการอนุมัติข้อยกเว้น และการติดตามแผนแก้ไข

องค์กรควรแต่งตั้งหรือกำหนด **ผู้บริหารและฝ่ายงานที่รับผิดชอบหลัก** เพื่อรับผิดชอบผลลัพธ์โดยรวม และมีอำนาจในการประสานการดำเนินงานระหว่างสายงาน โดยผู้บริหารดังกล่าวควรได้รับมอบอำนาจในการตัดสินใจสามารถเข้าถึงงบประมาณที่จำเป็น และนำเสนอประเด็นสำคัญต่อประธานเจ้าหน้าที่บริหารหรือคณะกรรมการบริษัท ได้โดยตรง สำหรับคณะทำงานข้ามสายงานนั้น มีบทบาทสนับสนุนการขับเคลื่อนการดำเนินงานให้เป็นไปตามแผน โดยยังคงความรับผิดชอบต่อผลลัพธ์ไว้ที่ผู้บริหารที่รับผิดชอบหลักอย่างชัดเจน เพื่อให้การติดตามและการแก้ไขปัญหาเป็นไปอย่างมีประสิทธิภาพ

รายงานต่อคณะกรรมการควรจัดทำอย่างน้อยรายไตรมาส โดยนำเสนอสาระสำคัญอย่างกระชับและเพียงพอต่อการกำกับดูแลใน 5 ประเด็น ได้แก่ **ความเสี่ยงสำคัญอยู่ที่ใด การดำเนินงานเป็นไปตามแผนหรือไม่ มีอุปสรรคสำคัญประการใด จำเป็นต้องจัดสรรทรัพยากรเพิ่มเติมหรือไม่ และมีเรื่องใดที่ต้องขอการตัดสินใจจากคณะกรรมการ** รายงานควรแสดงสถานะเทียบแผน แนวโน้ม ความเสี่ยงที่ยังคงเหลือ ข้อยกเว้นที่เกินกำหนด และระบบหรือคู่ค้าหรือผู้ให้บริการรายสำคัญที่เป็นข้อจำกัดต่อการเปลี่ยนผ่าน โดยหลีกเลี่ยงการใช้เปอร์เซ็นต์ที่ไม่ระบุขอบเขต หรืออาจทำให้เข้าใจว่าความเสี่ยงลดลงแล้วโดยยังไม่มีหลักฐานรองรับ

✓ สิ่งที่ต้องทำ	✗ สิ่งที่ไม่ควรทำ
✓ กำหนดให้มีผู้บริหาร / ฝ่ายงานที่รับผิดชอบหลัก ซึ่งมีอำนาจตัดสินใจและรับผิดชอบต่อผลลัพธ์โดยรวม	✗ ตั้งคณะทำงานแต่ไม่ระบุว่าใครรับผิดชอบภาพรวมจนปัญหาค้างระหว่างหลายฝ่าย
✓ กำหนดให้เจ้าของระบบและหน่วยธุรกิจรับผิดชอบความเสี่ยง โดยมีฝ่ายเทคโนโลยีสารสนเทศสนับสนุนการดำเนินงาน	✗ มอบหมายความรับผิดชอบต่อทั้งหมดให้ฝ่ายเทคโนโลยีสารสนเทศ ทั้งที่ผลกระทบและอำนาจในการตัดสินใจอยู่ที่หน่วยธุรกิจ
✓ กำกับให้บทบาทผู้ปฏิบัติ ผู้ติดตาม และผู้ตรวจสอบแยกจากกันอย่างชัดเจน พร้อมรักษาความเป็นอิสระของหน่วยงานตรวจสอบ	✗ มอบหมายให้หน่วยงานเดียวเป็นทั้งผู้ปฏิบัติงานและผู้สอบทานผลงานของตนเอง จนขาดการตรวจสอบและถ่วงดุลจากผู้ที่เป็นอิสระ
✓ กำกับผ่านโครงสร้างและคณะกรรมการที่องค์กรมีอยู่ โดยบูรณาการความเสี่ยงควอนตัมเข้ากับ ERM งบประมาณ และการจัดซื้อ	✗ จัดตั้งโครงสร้างการกำกับดูแลขึ้นใหม่โดยซ้ำซ้อนกับกลไกที่มีอยู่ ซึ่งเพิ่มภาระการประชุม โดยความรับผิดชอบต่อผลลัพธ์ยังไม่ชัดเจนขึ้น
✓ ขอรายงานที่บอกความเสี่ยง อุปสรรค และเรื่องต้องตัดสินใจ พร้อมขอบเขตและหลักฐาน	✗ พิจารณารายงานที่แสดงเพียงกิจกรรมหรือร้อยละความคืบหน้าโดยไม่ระบุขอบเขต ซึ่งไม่อาจสะท้อนได้ว่าความเสี่ยงลดลงอย่างแท้จริงหรือไม่

คำถามเพื่อการกำกับดูแล

1. ใครคือผู้บริหารที่รับผิดชอบผลลัพธ์ของการเตรียมความพร้อมด้านควอนตัมโดยรวม และผู้บริหารดังกล่าวมีอำนาจตัดสินใจ เข้าถึงงบประมาณ และเสนอเรื่องต่อผู้บริหารระดับสูงหรือคณะกรรมการได้เพียงพอหรือไม่?
2. เจ้าของระบบและหน่วยธุรกิจเข้าใจหรือไม่ว่าตนยังเป็นเจ้าของความเสี่ยง และไม่สามารถโอนความรับผิดชอบทั้งหมดให้ฝ่ายเทคโนโลยีหรือฝ่ายบริหารความเสี่ยง?
3. บทบาทของผู้ลงมือ ผู้กำหนดกรอบ ผู้ติดตาม และผู้ตรวจสอบแยกจากกันชัดเจนเพียงใด และตรวจสอบภายในยังคงความเป็นอิสระหรือไม่?
4. เมื่อแผนล่าช้า เกินงบ หรือคู่ค้า / ผู้ให้บริการไม่พร้อม มีเกณฑ์ในการยกระดับและรายงานต่อคณะกรรมการความเสี่ยงหรือคณะกรรมการบริษัทอย่างชัดเจนหรือไม่?
5. รายงานที่คณะกรรมการได้รับบอกความเสี่ยงที่ยังเหลือ อุปสรรค หลักฐาน ความต้องการทรัพยากร และเรื่องที่ต้องตัดสินใจ หรือเป็นเพียงรายงานกิจกรรมและเปอร์เซ็นต์ความคืบหน้า?

บทที่ 5

บัญชีรายการการใช้รหัสลับ (CBOM) และการจัดลำดับความสำคัญของข้อมูลและระบบ

องค์กรไม่อาจวางแผนเปลี่ยนผ่านวิทยาการรหัสลับได้ หากยังไม่ทราบว่ามีการใช้รหัสลับอยู่ ณ จุดใดบ้าง ในทางปฏิบัติ รหัสลับมิได้ปรากฏเฉพาะในระบบรักษาความมั่นคงปลอดภัย หากแต่แฝงอยู่ในเว็บไซต์ แอปพลิเคชัน การเชื่อมต่อระหว่างระบบ ลายมือชื่อดิจิทัล ใบรับรองอิเล็กทรอนิกส์ ฐานข้อมูล อุปกรณ์ ตลอดจนบริการของคู่ค้า การกิจลำดับแรกจึงมิใช่การเลือกเทคโนโลยีใหม่ หากแต่เป็นการทำให้สิ่งที่มองไม่เห็นกลายเป็นข้อมูลที่ใช้ประกอบการตัดสินใจได้

Cryptographic Bill of Materials (CBOM) หรือ “บัญชีรายการการใช้รหัสลับ” เป็นทะเบียนที่บอกว่า ระบบใดใช้รหัสอะไร เพื่อกำหนดว่าใครเป็นเจ้าของ และพึ่งพาใครบ้าง คุณค่าของ CBOM ไม่ได้อยู่ที่จำนวนรายการ แต่อยู่ที่การตอบคำถามว่า **จุดใดเสี่ยง จุดใดต้องเปลี่ยนก่อน และหากเปลี่ยนแล้วจะกระทบระบบ คู่ค้าหรือผู้ให้บริการรายใด**

สำหรับคณะกรรมการ ความครบถ้วนของ **CBOM ควรพิจารณาจากความสามารถในการตอบว่า รหัสลับอยู่ในระบบใด ปกป้องข้อมูลหรือกระบวนการใด ทำหน้าที่อะไร ใครเป็นเจ้าของ พึ่งพาระบบจากคู่ค้าหรือผู้ให้บริการรายใด และต้องดำเนินการอย่างไรต่อ** ทั้งนี้ องค์กรควรมอบหมายให้เจ้าของระบบและหน่วยงานที่เกี่ยวข้องจัดทำ และดูแลรายละเอียดทางเทคนิคของแต่ละรายการ เช่น อัลกอริทึม กุญแจ ใบรับรอง โปรโตคอล ไลบรารี และอุปกรณ์บริหารกุญแจ พร้อมกำหนดผู้รับผิดชอบในการสอบทานและปรับปรุงข้อมูลให้ถูกต้อง เป็นปัจจุบัน และสามารถตรวจสอบได้

ขอบเขตต้องรวมสิ่งที่องค์กรไม่ได้ควบคุมโดยตรงด้วย เช่น ระบบคลาวด์ ซอฟต์แวร์สำเร็จรูป ช่องทางเชื่อมต่อข้อมูลระหว่างระบบ (Application Programming Interface: API) ระบบชำระเงิน ผู้ให้บริการใบรับรอง และอุปกรณ์จากผู้ขาย หากรู้เฉพาะระบบภายใน CBOM จะให้ภาพความเสี่ยงที่ไม่ครบ เพราะการเปลี่ยนรหัสขององค์กรอาจติดอยู่ที่ผลิตภัณฑ์ที่ คู่ค้าหรือผู้ให้บริการที่เปลี่ยนไม่ทัน

เมื่อจัดทำบัญชีรายการแล้ว ขั้นตอนถัดไปคือ **“การจัดลำดับว่าระบบใดควรดำเนินการก่อน”** โดยไม่ควรกำหนดระดับ “สูง-กลาง-ต่ำ” จากความลับของข้อมูลเพียงอย่างเดียว แต่ควรพิจารณาอย่างน้อย 5 ปัจจัยประกอบกัน ได้แก่ (1) ระยะเวลาที่ข้อมูลต้องได้รับการคุ้มครอง (2) ความสำคัญของระบบต่อการดำเนินธุรกิจ (3) การใช้รหัสที่คอมพิวเตอร์ควอนตัมอาจทำลายได้ (4) ความเสี่ยงต่อการสวมรอยหรือการปลอมลายมือชื่อดิจิทัล และ (5) ระดับการพึ่งพาคู่ค้า / ผู้ให้บริการ หรือระบบเดิม

ข้อมูลที่ต้องรักษาความลับเป็นระยะเวลานาน เช่น ข้อมูลลูกค้า ข้อมูลทางธุรกิจ หรือความลับทางการค้า มักมีความเร่งด่วนสูง เนื่องจากอาจถูกดักเก็บไว้ตั้งแต่วันนี้เพื่อรอถอดรหัสในภายหลัง นอกจากนี้ ในกรณีของข้อมูลส่วนบุคคล องค์กรมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 การรั่วไหลที่เกิดขึ้นจึงอาจนำไปสู่ความรับผิดตามกฎหมาย เพิ่มเติมจากผลกระทบทางธุรกิจ ขณะเดียวกัน ระบบที่ใช้ยืนยันตัวตน ลงลายมือชื่อ หรือทำธุรกรรม อาจมีความสำคัญสูงเช่นกัน แม้มิได้จัดเก็บข้อมูลไว้เป็นเวลานาน เนื่องจากหากถูกปลอมย้อมส่งผลกระทบต่อความน่าเชื่อถือและการดำเนินธุรกิจโดยทันที

ผลลัพธ์ของการจัดลำดับจึงควรปรากฏเป็นรายการระบบที่ต้องดำเนินการก่อน พร้อมเหตุผลประกอบ ผู้รับผิดชอบ ระยะเวลา และทางเลือกในการแก้ไข ทั้งนี้ ไม่ควรกำหนดเกณฑ์ตายตัวว่าข้อมูลที่ต้องจัดเก็บเกิน 10 ปี เท่านั้นจึงถือเป็นความเสี่ยงสูง หรือข้อมูลที่มีอายุสั้นย่อมรอดำเนินการได้เสมอ เนื่องจากข้อกำหนดทางกฎหมาย ผลกระทบต่อธุรกิจ และความเสี่ยงจากการปลอมแปลงหรือการสวมรอย อาจทำให้ลำดับความสำคัญเปลี่ยนแปลงไป

คณะกรรมการควรกำกับให้ผู้รับผิดชอบใช้ข้อมูลจากหลายแหล่งในการจัดทำและตรวจทาน CBOM รวมทั้งเจ้าของระบบ เอกสาร เครื่องมือค้นหา และข้อมูลจากผู้ขาย พร้อมเชื่อมกับทะเบียนสินทรัพย์ที่มีอยู่ และมีกลไกปรับข้อมูลเมื่อระบบ ใบรับรอง ซอฟต์แวร์ หรือสัญญาคู่ค้าหรือผู้ให้บริการเปลี่ยนแปลง เพื่อให้ทะเบียนยังใช้ตัดสินใจได้และไม่ล้าสมัย

✓ สิ่งที่ต้องทำ	✗ สิ่งที่ไม่ควรทำ
✓ กำหนดให้ผู้รับผิดชอบจัดทำข้อมูลขั้นต้นและระบุเจ้าของทุกรายการ เพื่อให้ CBOM ใช้ติดตามและแก้ไขได้	✗ จัดทำเพียงรายการอัลกอริทึมที่ใช้งาน โดยไม่ระบุว่าใช้ในระบบใด ปกป้องข้อมูลหรือกระบวนการใด และผู้ใดเป็นผู้รับผิดชอบ
✓ กำกับให้ผู้รับผิดชอบใช้หลายวิธีจัดทำและตรวจทาน CBOM และขอรายงานความครบถ้วนของขอบเขต	✗ อาศัยผลจากเครื่องมือค้นหาหรือแบบสอบถามเพียงแหล่งเดียว แล้วสรุปว่าขอบเขตการสำรวจครอบคลุมครบถ้วนแล้ว
✓ ขอให้ผู้รับผิดชอบรวมระบบภายนอกและการพึ่งพาคู่ค้า / ผู้ให้บริการไว้ในขอบเขต CBOM เพื่อให้เห็นข้อจำกัดของการเปลี่ยนผ่านจริง	✗ ทำบัญชีเฉพาะระบบที่องค์กรดูแลเอง โดยมองข้ามคลาวด์ API ซอฟต์แวร์สำเร็จรูป หรือใบรับรอง
✓ กำกับให้ผู้รับผิดชอบจัดลำดับจากหลายปัจจัย ทั้งอายุข้อมูล ความสำคัญทางธุรกิจ ความเสี่ยงจากการสวมรอย ระบบเดิม และคู่ค้า / ผู้ให้บริการ	✗ ใช้เกณฑ์เดียวหรือเส้นแบ่ง 10 ปีแบบตายตัว จนมองข้ามระบบธุรกรรมหรือการยืนยันตัวตนที่สำคัญ
✓ ขอความมั่นใจว่าผู้รับผิดชอบมีกลไกปรับ CBOM ให้เป็นปัจจุบันเมื่อระบบ ใบรับรอง หรือสัญญาเปลี่ยนแปลง	✗ ทำ CBOM ครั้งเดียวแล้วถือว่าเสร็จ ทั้งที่ระบบ ใบรับรอง และคู่ค้า / ผู้ให้บริการ อาจมีการเปลี่ยนแปลง

คำถามเพื่อการกำกับดูแล

1. CBOM ครอบคลุมระบบสำคัญ ข้อมูล ลายมือชื่อดิจิทัล ใบรับรองอิเล็กทรอนิกส์ การยืนยันตัวตน ระบบคลาวด์ API และคู่ค้าหลักในสัดส่วนเท่าใด และยังมีส่วนใดที่องค์กรยังไม่สามารถตรวจสอบได้?
2. ฝ่ายบริหารมีวิธีการใดในการพิสูจน์ความครบถ้วนและความถูกต้องของ CBOM และได้สอบถามข้อมูลจากเจ้าของระบบ เครื่องมือค้นหา และผู้ขาย ประกอบกันแล้วหรือไม่?
3. ระบบที่ถูกจัดให้มีความเสี่ยงสูงใช้เกณฑ์ใด และได้พิจารณาทั้งอายุความลับ ความสำคัญทางธุรกิจ การสวมรอยระบบเดิม และการพึ่งพาผู้ค้า / ผู้ให้บริการแล้วหรือไม่?
4. รายการเสี่ยงสูงแต่ละรายการมีเจ้าของ กำหนดเวลา ทางเลือกแก้ไข และเรื่องที่ต้องการงบประมาณหรือการตัดสินใจแล้วหรือยัง?
5. มีกลไกใดทำให้ CBOM ปรับตามระบบใหม่ การเปลี่ยนใบรับรอง การอัปเดต และการต่อสัญญาผู้ค้า / ผู้ให้บริการ โดยไม่ต้องรอทำสำรวจครั้งใหญ่ใหม่ทั้งหมด?

บทที่ 6

Crypto Agility ความคล่องตัวทางวิทยาการรหัสลับ: การเปลี่ยนรหัสลับรองรับความเสี่ยงใหม่โดยไม่กระทบความต่อเนื่องทางธุรกิจ

การเปลี่ยนผ่านไปสู่การใช้อัลกอริทึมรหัสลับที่ทนต่อการประมวลผลเชิงควอนตัมมิใช่ภารกิจที่ดำเนินการเพียงครั้งเดียวแล้วเสร็จสมบูรณ์ เนื่องจากมาตรฐาน ช่องโหว่ ผลิตภัณฑ์ และผู้ให้บริการภายนอกอาจเปลี่ยนแปลงได้ตลอดเวลา องค์กรจึงจำเป็นต้องมี **Crypto Agility** อันหมายถึงความสามารถในการเปลี่ยนหรือยกเลิกการใช้อัลกอริทึมที่ใช้อยู่ได้อย่างทันการณ์ โดยไม่ทำให้การให้บริการหยุดชะงัก และไม่จำเป็นต้องปรับรื้อระบบครั้งใหญ่ในทุกครั้ง

แม้อัลกอริทึมหรือเทคโนโลยีจะผ่านการพิจารณารับรองในระดับสากลแล้ว องค์กรยังอาจมีความจำเป็นต้องเปลี่ยนแปลงในอนาคต อันเนื่องมาจากการค้นพบช่องโหว่ การประกาศข้อกำหนดใหม่ หรือความไม่เหมาะสมกับบางระบบ ข้อพึงตระหนักที่สำคัญคือ องค์กรไม่ควรออกแบบระบบให้ผูกติดกับอัลกอริทึมใดอัลกอริทึมหนึ่งจนยากต่อการเปลี่ยนแปลง และควรคงไว้ซึ่งทางเลือกในการปรับเปลี่ยนเมื่อมาตรฐานหรือภัยคุกคามเปลี่ยนแปลงไป

ระบบที่มีความสำคัญควรได้รับการออกแบบให้สามารถเปลี่ยนวิธีการเข้ารหัสได้โดยไม่จำเป็นต้องแก้ไขในหลายจุดหรือปรับรื้อระบบทั้งหมด เพื่อให้องค์กรสามารถปรับตัวได้อย่างทันการณ์เมื่อมาตรฐานหรือภัยคุกคามเปลี่ยนแปลง คณะกรรมการควรกำหนดความคาดหวังเชิงนโยบายและขอหลักฐานยืนยันว่าฝ่ายบริหารได้จัดให้มีการควบคุมสิทธิ การอนุมัติ การบันทึกเหตุการณ์ และแผนสำรองที่เหมาะสม ทั้งนี้ รายละเอียดเชิงสถาปัตยกรรมและการพัฒนาถือเป็นความรับผิดชอบของฝ่ายบริหารและทีมเทคนิค

Crypto Agility มิได้จำกัดอยู่เฉพาะในระดับซอฟต์แวร์ หากแต่ครอบคลุมถึงโปรโตคอล ฮาร์ดแวร์ เฟิร์มแวร์ อุปกรณ์บริหารจัดการกุญแจ ใบรับรอง และบริการของผู้ให้บริการภายนอกด้วย องค์กรจึงควรทราบว่าในกรณีที่จำเป็นต้องเปลี่ยนอัลกอริทึมอย่างเร่งด่วน จะต้องดำเนินการแก้ไข ณ จุดใดบ้าง ใช้ระยะเวลาเท่าใด ผู้ใดเป็นผู้มีอำนาจอนุมัติ และมีระบบหรือผู้ให้บริการรายใดที่เป็นข้อจำกัดสำคัญของการเปลี่ยนผ่าน ทั้งนี้ ข้อมูลจาก CBOM ตามที่กล่าวไว้ในบทก่อนหน้า ควรถูกใช้เป็นฐานข้อมูลประกอบคำตอบดังกล่าว

ก่อนการนำไปใช้งานจริง จำเป็นต้องทดสอบทั้งความเข้ากันได้และผลกระทบต่อการให้บริการ เนื่องจากอัลกอริทึม PQC แต่ละประเภทมีขนาดกุญแจ ลายมือชื่อดิจิทัล และภาระการประมวลผลที่แตกต่างจากอัลกอริทึมเดิม ผลกระทบอาจเกิดขึ้นกับระยะเวลาการเข้าสู่ระบบ ความเร็วในการทำธุรกรรม ปริมาณข้อมูล เครือข่าย อุปกรณ์ปลายทาง และวงจรชีวิตของใบรับรอง ทั้งนี้ คณะกรรมการควรได้รับการยืนยันว่าบริการที่มีความสำคัญได้ผ่านการทดสอบภายใต้ปริมาณงานจริงตามเกณฑ์ที่กำหนด และมีแผนถอยกลับรองรับในกรณีเกิดปัญหา

✓ สิ่งที่ต้องทำ	✗ สิ่งที่ไม่ควรทำ
✓ กำหนดความคาดหวังเชิงนโยบายให้ระบบใหม่ สามารถเปลี่ยนอัลกอริทึมรหัสลับได้ และให้ฝ่ายบริหารยืนยันว่าได้บรรจุข้อกำหนดดังกล่าวไว้ในกระบวนการออกแบบและการจัดซื้อ	✗ ยอมรับการออกแบบที่ทำให้ระบบ เปลี่ยนอัลกอริทึมหรือขนาดกุญแจได้ยาก จนการปรับเปลี่ยนแต่ละครั้งส่งผลกระทบต่อหลายระบบหรือจำเป็นต้องปรับรื้อระบบทั้งหมด
✓ ขอหลักฐานยืนยันว่า จุดควบคุมการตั้งค่ารหัสลับมีการแบ่งแยกสิทธิ์ การอนุมัติ การบันทึกเหตุการณ์ และแผนสำรองที่รัดกุมอย่างเพียงพอ	✗ รวมศูนย์การควบคุมโดยปราศจาก มาตรการควบคุมที่รัดกุม จนอาจกลายเป็นเป้าหมายการโจมตีที่สำคัญ
✓ ขอผลการทดสอบที่ ครอบคลุมปริมาณงานจริง เกณฑ์การผ่าน และแผนถอยกลับ ก่อนพิจารณาอนุมัติการขยายผล	✗ ทดสอบเพียง ความสามารถในการเชื่อมต่อ โดยไม่ประเมินความเร็ว ปริมาณข้อมูล ความเสถียร และผลกระทบต่อลูกค้า
✓ อนุมัติการใช้แนวทาง Hybrid เฉพาะกรณีที่สอดคล้องกับมาตรฐานและมีเหตุผลรองรับ โดยกำหนดให้ฝ่ายบริหารระบุวิธีการผสมผสานและเงื่อนไขการยกเลิกใช้งานอย่างชัดเจน	✗ เข้าใจว่า การใช้สองอัลกอริทึมจะทำให้ปลอดภัยมากขึ้นเสมอ ทั้งที่การผสมผสานอย่างไม่ถูกต้องอาจเพิ่มความซับซ้อนและช่องโหว่
✓ กำหนดให้ แผนครอบคลุมผู้ให้บริการภายนอก อุปกรณ์ในรับรอง และระบบเดิม พร้อมระบุข้อจำกัดสำคัญที่อาจทำให้การเปลี่ยนผ่านไม่แล้วเสร็จตามกำหนด	✗ ประเมินเฉพาะ แอปพลิเคชันที่องค์กรพัฒนาขึ้นเอง โดยละเลยผลิตภัณฑ์หรือผู้ให้บริการภายนอกที่องค์กรไม่สามารถแก้ไขได้เอง

คำถามเพื่อการกำกับดูแล

1. ในกรณีที่จำเป็นต้องเปลี่ยนหรือยกเลิกการใช้อัลกอริทึมอย่างเร่งด่วน องค์กรทราบหรือไม่ว่าระบบใดได้รับผลกระทบ ผู้ใดเป็นผู้มีอำนาจอนุมัติ และต้องใช้ระยะเวลาดำเนินการจริงเท่าใด?
2. ระบบที่มีความสำคัญใดยังคงกำหนดอัลกอริทึมหรือใบรับรองไว้อย่างตายตัวภายในระบบ และได้กำหนดแผนดำเนินการผู้รับผิดชอบ งบประมาณ และกรอบเวลาในการแก้ไขไว้แล้วหรือไม่?
3. ผลการทดสอบ PQC ครอบคลุมปริมาณงานจริง ความเร็วในการทำธุรกรรม เครือข่าย อุปกรณ์ปลายทาง ใบรับรอง และการเชื่อมต่อกับผู้ให้บริการภายนอกครบถ้วนแล้วหรือไม่?
4. จุดควบคุมการตั้งค่ารหัสลับมีการแบ่งแยกสิทธิ์ การอนุมัติ การบันทึกเหตุการณ์ แผนสำรอง และการทดสอบแผนถอยกลับอย่างเพียงพอหรือไม่?
5. ผู้ให้บริการภายนอก ผลิตภัณฑ์ หรือระบบเดิมใดเป็นข้อจำกัดสำคัญที่ทำให้องค์กรไม่สามารถเปลี่ยนอัลกอริทึมได้ตามกำหนด และฝ่ายบริหารได้เตรียมทางเลือกไว้ล่วงหน้าหรือไม่ ในกรณีที่ผู้ให้บริการดังกล่าวไม่สามารถดำเนินการได้ตามแผน?

บทที่ 7

ความเสี่ยงจากห่วงโซ่อุปทาน: ความพร้อมของคู่ค้าและผู้ให้บริการภายนอกต่อการเปลี่ยนผ่านไปสู่ PQC

การเปลี่ยนผ่านไปสู่ PQC ขององค์กรมีได้ขึ้นอยู่กับระบบภายในเพียงประการเดียว ระบบคลาวด์ ซอฟต์แวร์ สำเร็จรูป ระบบซื้อขาย ระบบชำระเงิน อุปกรณ์รักษาความปลอดภัย ใบรับรอง และการเชื่อมต่อกับหน่วยงานอื่น ล้วนมีการใช้อัลกอริทึมรหัสลับของผู้ให้บริการภายนอกอยู่เบื้องหลัง ในกรณีที่ผู้ให้บริการรายสำคัญไม่สามารถดำเนินการเปลี่ยนผ่านได้ทันตามกำหนด องค์กรอาจยังคงมีจุดเสี่ยงคงค้างหรือไม่สามารถให้บริการได้ แม้ระบบภายในขององค์กรจะมีความพร้อมแล้วก็ตาม

องค์กรไม่จำเป็นต้องประเมินผู้ให้บริการภายนอกทุกรายด้วยระดับความเข้มข้นที่เท่าเทียมกัน หากแต่ควรเริ่มจากผู้ให้บริการที่หากไม่สามารถให้บริการอย่างต่อเนื่องหรือเปลี่ยนผ่านระบบได้ทันตามกำหนด แล้วจะส่งผลกระทบต่อธุรกิจในระดับสูง เช่น ผู้ให้บริการคลาวด์ ระบบแกนหลัก ระบบซื้อขายและชำระเงิน ผู้ให้บริการใบรับรอง อุปกรณ์รักษาความปลอดภัย และผู้เชื่อมต่อผ่าน API ทั้งนี้ การจัดลำดับควรพิจารณาทั้งความสำคัญของบริการ ข้อมูลที่ผู้ให้บริการเข้าถึง การใช้ลายมือชื่อดิจิทัลหรือการยืนยันตัวตน ความยากในการเปลี่ยนผู้ให้บริการ และระยะเวลาที่ผู้ให้บริการต้องใช้ในการปรับปรุงผลิตภัณฑ์

การประเมินจำเป็นต้องขอ **หลักฐานประกอบ** มากกว่าการรับคำยืนยันเพียงว่า “รองรับ PQC แล้ว” โดยอย่างน้อยควรทราบว่าผลิตภัณฑ์รุ่นใดรองรับมาตรฐานใด ต้องปรับปรุงซอฟต์แวร์ เฟิร์มแวร์ หรืออุปกรณ์หรือไม่ ผ่านการทดสอบกับระบบใด มีข้อจำกัดด้านประสิทธิภาพและความเข้ากันได้อย่างไร รวมถึงกำหนดเวลาที่ลูกค้าจะใช้งานได้จริง ในกรณีที่ผู้ให้บริการภายนอกไม่สามารถให้คำตอบที่ชัดเจนได้ องค์กรควรบันทึกเป็นความเสี่ยงและกำหนดวันที่ติดตาม โดยองค์กรยังคงต้องรับผิดชอบในการบริหารจัดการความเสี่ยงดังกล่าว ไม่ควรถือว่าความเสี่ยงได้ถูกส่งต่อให้ผู้ให้บริการภายนอกแล้ว

คณะกรรมการควรกำหนดนโยบายให้ฝ่ายบริหารบรรลุความพร้อมด้าน PQC และ Crypto Agility ไว้ในเกณฑ์การจัดซื้อจัดจ้างใหม่ทุกรายการตั้งแต่ขั้นตอนการกำหนดความต้องการ โดยมอบหมายให้ฝ่ายจัดซื้อ ฝ่ายกฎหมาย และหน่วยงานเจ้าของระบบร่วมกันรับผิดชอบ พร้อมกำกับให้มีการรายงานผลการปฏิบัติตามนโยบายดังกล่าวต่อคณะกรรมการเป็นระยะ

สำหรับบริการที่มีความสำคัญ เจือจางในเอกสารกำหนดขอบเขตของงาน (Terms of Reference: TOR) หรือสัญญาควรครอบคลุมอย่างน้อย 6 ประการ ได้แก่ (1) มาตรฐานและผลิตภัณฑ์ที่ผู้ขายต้องรองรับ (2) กำหนดส่งมอบและแผนการปรับปรุงผลิตภัณฑ์ (3) การแจ้งให้องค์กรทราบล่วงหน้าเมื่อผู้ขายมีการเปลี่ยนแปลงแผน (4) การร่วม

ทดสอบ (5) สิทธิในการขอข้อมูลหรือเข้าสอบทาน และ (6) แนวทางดำเนินการในกรณีที่ผู้ขายไม่สามารถส่งมอบได้ตามกำหนด ทั้งนี้ ควรกำหนดระดับความเข้มข้นของเงื่อนไขให้เหมาะสมกับสำคัญของบริการ

สำหรับผู้ให้บริการภายนอกรายเดิม คณะกรรมการควรให้ฝ่ายบริหารเชื่อมโยงผลการประเมินความพร้อมของผู้ให้บริการเข้ากับ CBOM ขององค์กร เพื่อให้เห็นว่าผลิตภัณฑ์หรือบริการใดใช้อัลกอริทึมที่จำเป็นต้องเปลี่ยน รวมทั้งความสำคัญของผู้ให้บริการรายใดจะส่งผลกระทบต่อระบบใดขององค์กร และหน่วยงานใดเป็นผู้รับผิดชอบ ติดตามผู้ให้บริการแต่ละราย อย่างไรก็ตาม การขอ CBOM จากผู้ให้บริการภายนอกอาจดำเนินการได้เฉพาะบางราย เนื่องจากผู้ให้บริการบางรายยังมิได้จัดทำ CBOM หรือมีข้อจำกัดด้านความลับทางการค้า ฝ่ายบริหารจึงควรกำหนดข้อมูลขั้นต่ำที่จำเป็นต่อการประเมินความเสี่ยง อาทิ หน้าที่ของอัลกอริทึมรหัสลับที่ใช้ มาตรฐานที่รองรับรุ่นผลิตภัณฑ์ กำหนดการปรับปรุง และส่วนที่องค์กรต้องดำเนินการเอง แทนการเรียกขอเอกสารฉบับสมบูรณ์จากผู้ให้บริการทุกราย

คณะกรรมการควรขอหลักฐานยืนยันว่าฝ่ายบริหารได้จัดทำแผนสำรองสำหรับผู้ให้บริการภายนอกสำคัญและกำหนดจุดตัดสินใจล่วงหน้าแล้ว ในกรณีที่ผู้ให้บริการดังกล่าวไม่สามารถเปลี่ยนผ่านได้ตามกำหนด ทางเลือกอาจรวมถึงการจำกัดข้อมูลหรือบริการที่ใช้ การแยกการเชื่อมต่อ การใช้มาตรการชั่วคราว การเร่งเปลี่ยนรุ่นผลิตภัณฑ์ หรือการเตรียมผู้ให้บริการทางเลือก โดยฝ่ายบริหารควรประเมินผลกระทบ ต้นทุน ระยะเวลา และผู้มีอำนาจตัดสินใจของแต่ละทางเลือกไว้ก่อนเกิดเหตุ ทั้งนี้ ความร่วมมือระดับอุตสาหกรรมอาจช่วยลดการประเมินซ้ำซ้อนและทำให้ข้อกำหนดที่ส่งไปยังผู้ขายมีความสอดคล้องกันมากขึ้น

✓ สิ่งที่ต้องทำ	✗ สิ่งที่ไม่ควรทำ
✓ กำกับให้ฝ่ายบริหารจัดลำดับผู้ให้บริการภายนอกตามผลกระทบต่อธุรกิจ และกำหนดระดับการประเมินที่เข้มข้นยิ่งขึ้นสำหรับบริการที่มีความสำคัญ	✗ ใช้แบบประเมินชุดเดียวกับผู้ให้บริการภายนอกทุกราย โดยไม่ปรับระดับการประเมินให้สอดคล้องกับสำคัญของบริการและผลกระทบต่อธุรกิจ
✓ ขอแผนดำเนินการ รุ่นผลิตภัณฑ์ และผลการทดสอบ พร้อมกำหนดวันที่ลูกค้าจะสามารถใช้งานได้จริง	✗ ยอมรับเพียงคำยืนยันว่า “รองรับ PQC” โดยปราศจากหลักฐานประกอบ หรือมิได้ทราบว่าต้องปรับปรุงส่วนใดบ้าง
✓ กำหนดเงื่อนไขไว้ใน TOR และสัญญาตั้งแต่เริ่มต้น ครอบคลุมการปรับปรุง การทดสอบ การแจ้งเปลี่ยนแปลงแผน และแนวทางดำเนินการรองรับ	✗ คัดเลือกผู้ให้บริการก่อนแล้วจึงเจรจาเรื่อง PQC ในภายหลัง อาจทำให้อำนาจต่อรองขององค์กรลดลง
✓ เชื่อมโยงข้อมูลผู้ให้บริการภายนอกกับ CBOM ขององค์กร เพื่อให้ทราบว่าจะระบบใดมีความผูกพันกับผู้ให้บริการรายใด	✗ จัดเก็บผลการประเมินผู้ให้บริการภายนอกแยกจากแผนระบบ อาจทำให้ไม่เห็นผลกระทบต่อกำหนดการเปลี่ยนผ่านขององค์กร
✓ กำหนดจุดตัดสินใจและแผนสำรองล่วงหน้า ในกรณีที่ผู้ให้บริการภายนอกไม่มีความพร้อมตามกำหนด	✗ รอจนใกล้กำหนดเวลาสิ้นสุดแล้วจึงแสวงหาทางเลือก ทั้งที่การเปลี่ยนระบบหรือผู้ให้บริการต้องใช้ระยะเวลาดำเนินการนาน

คำถามเพื่อการกำกับดูแล

1. ผู้ให้บริการภายนอกหรือผลิตภัณฑ์ใดเป็นข้อจำกัดสำคัญของการเปลี่ยนผ่าน และฝ่ายบริหารได้จัดลำดับตามผลกระทบทางธุรกิจ ข้อมูลที่เข้าถึง และความยากในการเปลี่ยนผู้ให้บริการไว้แล้วหรือไม่?
2. หลักฐานความพร้อมของผู้ให้บริการภายนอกที่สำคัญได้ระบุผลิตภัณฑ์ มาตรฐานที่รองรับ ผลการทดสอบสิ่งที่ลูกค้าต้องดำเนินการปรับปรุง และวันที่สามารถใช้งานได้จริงไว้ครบถ้วนแล้วหรือไม่?
3. TOR และสัญญาใหม่ได้กำหนดเรื่องการปรับปรุง PQC การร่วมทดสอบ การแจ้งเมื่อมีการเปลี่ยนแปลงแผน สิทธิในการสอบทาน และแนวทางดำเนินการในกรณีที่ส่งมอบไม่ทันตามกำหนดไว้หรือไม่?
4. ผลการประเมินผู้ให้บริการภายนอกได้เชื่อมโยงกับ CBOM และแผนเปลี่ยนผ่านระบบขององค์กรแล้วหรือไม่ เพื่อแสดงให้เห็นว่าความล่าช้าของผู้ขายรายใดส่งผลกระทบต่อระบบใด?
5. ในกรณีที่ผู้ให้บริการภายนอกที่สำคัญไม่มีความพร้อมตามกำหนด องค์กรได้กำหนดจุดตัดสินใจ มาตรการชั่วคราว ผู้ให้บริการทางเลือก งบประมาณ และผู้มีอำนาจอนุมัติไว้ล่วงหน้าแล้วหรือไม่?

บทที่ 8

การเตรียมความพร้อมด้านบุคลากร

ความสำเร็จของการเปลี่ยนผ่านไปสู่การใช้วิทยาการรหัสลับที่ทนทานต่อควอนตัม (PQC) ขึ้นอยู่กับความพร้อมของบุคลากรควบคู่กับเทคโนโลยีใหม่ เนื่องจากผู้กำหนดนโยบายและทิศทาง ออกแบบระบบ จัดซื้อจัดจ้าง จัดทำสัญญา ทดสอบ และใช้งานจริง ต่างมีบทบาทสำคัญต่อผลลัพธ์ทั้งสิ้น ความพร้อมด้านบุคลากรจึงมีใช้การจัดอบรมเรื่องควอนตัมให้บุคลากรทุกคน หากแต่เป็นการพัฒนาให้**แต่ละบทบาทมีความรู้และทักษะเพียงพอต่องานที่อยู่ในความรับผิดชอบ** ซึ่งเป็นแนวทางที่ใช้ทรัพยากรได้อย่างคุ้มค่าและเห็นผลในทางปฏิบัติ

องค์กรควรมีการจัดทำ แผนทักษะตามบทบาท โดยเริ่มจากภารกิจที่ต้องดำเนินการใน 12–24 เดือน แล้วเทียบกับบุคลากรที่มีอยู่ เพื่อให้เห็นช่องว่างด้านจำนวน ความรู้ และประสบการณ์ จากนั้นจึงเลือกแนวทางที่เหมาะสม ทั้งการพัฒนาบุคลากรภายใน การสรรหาเพิ่มเติม การใช้ผู้เชี่ยวชาญภายนอก หรือความร่วมมือกับสถาบันการศึกษา การดำเนินการในลักษณะดังกล่าวจะช่วยให้องค์กรจัดสรรทรัพยากรได้ตรงกับทักษะที่จำเป็นต่อการเปลี่ยนผ่าน ทั้งนี้ แผนทักษะตามบทบาทยังใช้เป็นข้อมูลประกอบการพิจารณาของคณะกรรมการในการอนุมัติแผนกำลังคนและงบประมาณได้อีกทางหนึ่งด้วย

✓ สิ่งที่ต้องทำ	✗ สิ่งที่ไม่ควรทำ
✓ กำหนดความรู้และทักษะตามบทบาท ให้สอดคล้องกับภารกิจที่แต่ละหน่วยงานต้องรับผิดชอบ	✗ บุคลากรทุกคนเข้ารับการอบรมหลักสูตรเดียวกัน โดยไม่ได้พิจารณาหน้าที่และระดับความรู้ที่จำเป็นต้องใช้
✓ วัดผลจากการปฏิบัติงานจริงและผลการทดสอบ อาทิ การสำรวจ CBOM การทดสอบระบบ หรือการจัดทำเงื่อนไขกับผู้ให้บริการภายนอก	✗ พิจารณาเพียงจำนวนบุคลากรหรือชั่วโมงการอบรม อาจยังไม่สะท้อนความพร้อมที่แท้จริงในการปฏิบัติงานขององค์กร
✓ จัดอบรมหน่วยธุรกิจ กฎหมาย ความเสี่ยง และจัดซื้อ ให้สามารถปฏิบัติหน้าที่ของตนได้	✗ พัฒนากลุ่มเฉพาะฝ่ายเทคโนโลยีสารสนเทศ โดยไม่ให้ความสำคัญกับฝ่ายงานสำคัญอื่น ๆ ที่เกี่ยวข้อง
✓ วางแผนพัฒนาบุคลากรและใช้ผู้เชี่ยวชาญภายนอกอย่างเหมาะสม พร้อมถ่ายทอดความรู้กลับสู่องค์กร	✗ พึ่งพาที่ปรึกษาหรือผู้ให้บริการจนองค์กรไม่สามารถดำเนินการได้ด้วยตนเอง และมีได้มีกระบวนการในการถ่ายทอดองค์ความรู้
✓ เชื่อมโยงแผนทักษะกับแผนงานและงบประมาณ พร้อมรายงานช่องว่างที่อาจส่งผลให้การดำเนินงานล่าช้า	✗ การจัดอบรมแยกส่วนจากแผนเปลี่ยนผ่าน อาจทำให้ความรู้ที่ได้รับมิได้ถูกนำไปใช้กับการปฏิบัติงานจริง

คำถามเพื่อการกำกับดูแล

1. บทบาทใดจำเป็นต้องแผนเปลี่ยนผ่านใน 12–24 เดือน และบุคลากรมีความรู้หรือสามารถเพียงพอต่อการปฏิบัติงานในบทบาทดังกล่าวหรือไม่?
2. ช่องว่างสำคัญอยู่ที่จำนวนบุคลากร ความรู้ หรือประสบการณ์ด้านใด และช่องว่างใดที่อาจส่งผลให้ขั้นตอนการเปลี่ยนผ่าน เช่น CBOM การทดสอบ ระบบ หรือสัญญากับผู้ให้บริการภายนอกล่าช้า?
3. องค์กรได้วัดผลการพัฒนากทักษะจากผลงานจริงหรือไม่ (อาทิ การสำรวจ การทดสอบ การปรับแก้ระบบ และการกำหนดเงื่อนไขกับผู้ให้บริการภายนอก เป็นต้น) ?
4. ในกรณีที่จำเป็นต้องใช้ที่ปรึกษาหรือผู้ให้บริการภายนอก องค์กรได้จัดทำแผนถ่ายทอดความรู้ ลดการพึ่งพา และรักษาความสามารถสำคัญไว้ภายในองค์กรแล้วหรือไม่?
5. คณะกรรมการได้รับรายงานเรื่องช่องว่างทักษะ แผนกำลังคน งบประมาณ ความคืบหน้า และความเสี่ยงในกรณีที่บุคลากรไม่มีความพร้อม ควบคู่กับแผนในเรื่องระบบหรือไม่?

บทที่ 9

จากแผนสู่การปฏิบัติ: แผนการเปลี่ยนผ่าน 5 ระยะ

แผนเปลี่ยนผ่าน 5 ระยะต่อไปนี้เป็นกรอบสำหรับการดำเนินงาน มิใช่แนวทางตายตัว บางระยะอาจดำเนินการคู่ขนานกันได้ และระยะเวลาที่ใช้จริงย่อมขึ้นอยู่กับขนาดองค์กร ลักษณะและความซับซ้อนของระบบเดิม ผู้ให้บริการภายนอก และอายุการรักษาความลับของข้อมูล โดยแต่ละระยะควรมี **ผลลัพธ์ที่ตรวจสอบได้ ผู้รับผิดชอบ กำหนดเวลา และเงื่อนไขก่อนเข้าสู่ระยะถัดไป** ทั้งนี้ อาจพิจารณาใช้กรอบปี 2026–2035 ของ สกมช. และใช้หมวดหมายสากลเป็นกรอบอ้างอิงในการกำหนดทิศทางและวางแผนการเตรียมความพร้อม

ระยะที่ 1 — ตั้งต้นและกำหนดความรับผิดชอบ องค์กรมีการแต่งตั้งผู้บริหาร / ฝ่ายงานที่รับผิดชอบหลัก กำหนดโครงสร้าง ขอบเขต และแผนงานการดำเนินงาน

ผลลัพธ์ก่อนผ่านระยะ: มีผู้บริหารที่รับผิดชอบหลักและโครงสร้างการกำกับดูแลที่ชัดเจน มีการกำหนดขอบเขต การดำเนินการ และแผนการดำเนินงาน 12 เดือนแรก

ระยะที่ 2 — สำรวจและจัดลำดับความสำคัญ จัดทำ CBOM ให้ครอบคลุมระบบที่มีความสำคัญ เชื่อมโยงข้อมูลกับผลกระทบทางธุรกิจ และจัดลำดับความสำคัญโดยพิจารณาจากอายุของความลับ การยืนยันตัวตน ระบบเดิม การพึ่งพาคุณค่าและผู้ให้บริการภายนอก พร้อมจัดทำงบประมาณและแผนรองรับ

ผลลัพธ์ก่อนผ่านระยะ: มีรายการงานเรียงตามความเสี่ยง ผู้รับผิดชอบ กำหนดเวลา งบประมาณ และแผนรองรับ ค่าและผู้ให้บริการภายนอกรายสำคัญ

ระยะที่ 3 — ทดลองและพิสูจน์ว่าใช้ได้จริง คัดเลือกระบบนำร่องที่ก่อให้เกิดการเรียนรู้ แต่สามารถควบคุมผลกระทบได้ ทดสอบมาตรฐาน PQC กับปริมาณงานจริง ความเข้ากันได้ ใบรับรอง อุปกรณ์ คู่ค้าและผู้ให้บริการภายนอก ในกรณีที่เลือกใช้แนวทางแบบผสมผสาน ควรระบุเหตุผล วิธีการ และเงื่อนไขที่ชัดเจน

ผลลัพธ์ก่อนผ่านระยะ: มีผลการทดสอบ เกณฑ์การผ่าน ข้อจำกัด แผนถอยกลับ และเงื่อนไขในการขยายผล ปรับแก้ หรือยุติ

ระยะที่ 4 — การเปลี่ยนผ่านระบบที่มีความสำคัญตามลำดับ เริ่มจากข้อมูลและระบบที่มีความเสี่ยงสูง โดยแบ่งรอบการเปลี่ยนผ่านให้อยู่ในระดับที่ควบคุมได้ ประสานงานกับผู้ให้บริการภายนอก ปรับปรุงใบรับรอง ระบบบริหารจัดการกฎ และแผนรองรับเหตุขัดข้อง พร้อมติดตามผลกระทบต่อการให้บริการและลูกค้า

ผลลัพธ์ก่อนผ่านระยะ: ระบบเป้าหมายสามารถใช้งานได้ตามเกณฑ์ที่กำหนด ความเสี่ยงคงเหลือได้รับการพิจารณา หรือมีแผนแก้ไขรองรับ และไม่ปรากฏข้อบกพร่องสำคัญที่ยังไม่มีผู้รับผิดชอบ

ระยะที่ 5 – ทำให้เป็นงานประจำและปรับปรุงต่อเนื่อง ผนวก Crypto Agility และการดำเนินการข้างต้น เข้ากับวงจรการพัฒนา ระบบ การจัดซื้อจัดจ้าง และการตรวจสอบ พร้อมทบทวนมาตรฐาน ความเสี่ยง และแผน อย่างสม่ำเสมอ

ผลลัพธ์: องค์กรสามารถคงการมองเห็นการใช้อัลกอริทึมรหัสลับได้อย่างต่อเนื่อง ไม่ย้อนกลับสู่สภาวะที่ขาด การมองเห็นอีก และสามารถปรับเปลี่ยนได้เมื่อมาตรฐานหรือภัยคุกคามเปลี่ยนแปลง โดยไม่จำเป็นต้องเริ่มโครงการ ใหม่ทั้งหมด

✓ สิ่งที่ต้องทำ	✗ สิ่งที่ไม่ควรทำ
✓ กำหนดผลลัพธ์และเงื่อนไขการผ่านของแต่ละระยะ พร้อมหลักฐานประกอบที่คณะกรรมการใช้ประกอบการตัดสินใจ	✗ เข้าสู่ระยะถัดไปเพียงเพราะครบกำหนดเวลา ทั้งที่ภารกิจสำคัญหรือหลักฐานยังไม่ครบถ้วน
✓ ให้ระบบที่มีความเสี่ยงสูงดำเนินการก่อนและสามารถ ดำเนินการหลายระยะคู่ขนานได้ เมื่อมีมาตรการควบคุมอย่างเพียงพอ	✗ รอให้การสำรวจแล้วเสร็จครบทุกระบบก่อนจึงเริ่มทดลอง จนระบบที่มีความเร่งด่วนต้องล่าช้าไปด้วย
✓ เชื่อมโยงแผนเปลี่ยนผ่านกับงบลงทุนและแผนปรับเปลี่ยน ระบบ เพื่อกระจายต้นทุนและลดความซ้ำซ้อนของงาน	✗ จัดทำแผนเปลี่ยนผ่านแยกจากแผนธุรกิจและงบประมาณ อาจทำให้มีแผนแต่ขาดทรัพยากรในการดำเนินการ
✓ ทดสอบก่อนการขยายผลและจัดให้มีแผนถอยกลับ รวมถึงเกณฑ์การยุติเมื่อผลไม่เป็นไปตามที่คาดการณ์	✗ ขยายผลโครงการนำร่องเพียงเพราะดำเนินการแล้วเสร็จ โดยไม่ได้ทบทวนผลกระทบและข้อจำกัด
✓ ทบทวนแผนเมื่อมาตรฐาน ระบบ หรือผู้ให้บริการภายนอก เปลี่ยนแปลง และรายงานผลกระทบต่อความเสี่ยงและ งบประมาณ	✗ ยึดตามแผนเปลี่ยนผ่านที่ได้รับอนุมัติครั้งแรกโดยไม่มี การทบทวน แม้สมมติฐานหรือความพร้อมจะเปลี่ยนแปลงไป

คำถามเพื่อการกำกับดูแล

1. คณะกรรมการจะใช้ผลลัพธ์และหลักฐานใดเป็นเงื่อนไขในการอนุมัติให้เข้าสู่ระยะถัดไป และผู้ใดเป็นผู้รับรองว่าหลักฐาน ดังกล่าวครบถ้วนเพียงพอ?

2. แผนเปลี่ยนผ่านถูกเชื่อมกับรอบงบประมาณ แผนปรับเปลี่ยนระบบ และรอบการต่ออายุสัญญากับผู้ค้าและผู้ให้บริการ หรือไม่ หรือยังคงเป็นแผนเฉพาะกิจที่ไม่มีทรัพยากรรองรับ?

3. มีระบบหรือความเสี่ยงใดที่ควรเร่งดำเนินการคู่ขนาน โดยไม่รอให้ระยะก่อนหน้าแล้วเสร็จทั้งหมด และองค์กรมีมาตรการ ควบคุมความเสี่ยงจากการดำเนินการหลายระยะพร้อมกันอย่างไร?

4. ในกรณีที่แผนล่าช้า งบประมาณไม่เพียงพอ ผู้ค้าหรือผู้ให้บริการรายสำคัญไม่มีความพร้อม จุดใดเป็นเกณฑ์ให้ฝ่ายบริหาร ต้องเสนอทางเลือกใหม่ ยกระดับความเสี่ยง หรือเสนอขอมติจากคณะกรรมการ?

5. แผนได้กำหนดรอบการทบทวนเมื่อมาตรฐาน ภัยคุกคาม สมมติฐาน ระบบ หรือความพร้อมของผู้ค้าหรือผู้ให้บริการ เปลี่ยนแปลงไว้หรือไม่ และการเปลี่ยนแผนจะแสดงผลต่อความเสี่ยง งบประมาณ และกรอบเวลาให้คณะกรรมการ เห็นอย่างไร?

ภาคผนวก ก — ชุดเครื่องมือสำหรับคณะกรรมการ

เครื่องมือที่ 1 — ชุดคำถามเพื่อการกำกับดูแล

วิธีใช้

คณะกรรมการไม่จำเป็นต้องใช้คำถามทุกข้อในการประชุมคราวเดียวกัน แต่อาจเลือกเฉพาะคำถาม หลักฐาน และประเด็นพิจารณาที่สอดคล้องกับระยะการเปลี่ยนผ่านขององค์กร วาระการประชุม และระดับความเสี่ยง ณ ขณะนั้น ทั้งนี้ คำถามส่วนที่เหลือสามารถนำไปใช้ประกอบการพิจารณาในการประชุมคราวถัดไปได้ตามความเหมาะสม

ระยะที่ 1 — ตั้งต้นและกำหนดความรับผิดชอบ

ใช้เมื่อองค์กรเริ่มนำความเสี่ยงด้านควอนตัมเข้าสู่การกำกับดูแล กำหนดผู้รับผิดชอบ และวางขอบเขตงานระยะแรก

คำถามที่คณะกรรมการควรถาม	หลักฐานที่ควรได้รับ	เรื่องที่ต้องพิจารณา
1. ความเสี่ยงด้านควอนตัมถูกจัดทำเข้าสู่ทะเบียนความเสี่ยงองค์กรแล้วหรือไม่?	☐ ทะเบียนความเสี่ยงและผลกระทบทางธุรกิจ	☐ รับรองให้เป็นความเสี่ยงเชิงยุทธศาสตร์
2. ใครคือผู้บริหารที่รับผิดชอบผลลัพธ์โดยรวม และมีอำนาจเพียงพอหรือไม่?	☐ คำสั่งแต่งตั้งผู้บริหารที่รับผิดชอบหลัก	☐ กำหนดผู้รับผิดชอบหลัก
3. เจ้าของความเสี่ยง ผู้ปฏิบัติงาน ผู้ติดตาม และผู้ตรวจสอบแยกจากกันชัดเจนหรือไม่?	☐ บทบาทตามหลักการ Three Lines Model	☐ กำหนดขอบเขตและกรอบเวลา
4. ข้อมูล ระบบ ธุรกรรม และคู่ค้า / ผู้ให้บริการกลุ่มใดอยู่ในขอบเขตเริ่มต้น?	☐ ขอบเขตและแผนงาน 12 เดือนแรก	☐ อนุมัติทรัพยากรเริ่มต้น
5. ฝ่ายบริหารประเมินกรณีที่ภัยจาก Quantum Computing ภัยนี้ มาเร็ว เป็นไปตามคาด และมาช้าแล้วหรือยัง?	☐ รูปแบบและรอบการรายงาน	☐ ขอกการสอบทานอิสระ
6. องค์กรต้องการผลลัพธ์ใดภายใน 12 เดือน และอะไรคือเงื่อนไขความสำเร็จ?	☐ รายการข้อมูลที่ยังไม่เพียงพอ	☐ กำหนดวันที่รายงานกลับ
7. คณะกรรมการจะได้รับรายงานผ่านช่องทางและความถี่ใด?		
8. ข้อมูลใดยังไม่เพียงพอ และฝ่ายบริหารจะปิดช่องว่างเมื่อใด?		

ข้อสรุปของคณะกรรมการ

มติ / ทิศทาง _____ ผู้บริหารที่รับผิดชอบหลัก _____

หลักฐานที่ต้องได้รับ _____ กำหนดรายงานกลับ _____

ระยะที่ 2 – สำรวจและจัดลำดับความสำคัญ		
คำถามที่คณะกรรมการควรถาม	หลักฐานที่ควรได้รับ	เรื่องที่อาจพิจารณา
1. CBOM ครอบคลุมระบบสำคัญ คลาวด์ API ไบรรับรอง และคู่ค้า / ผู้ให้บริการหลักแล้วเพียงใด? 2. ส่วนใดยังไม่ได้จัดทำ และมีผลต่อการตัดสินใจเพียงใด? 3. ฝ่ายบริหารพิสูจน์ความครบถ้วนของ CBOM ด้วยวิธีใด? 4. ข้อมูลใดต้องเก็บเป็นความลับ และต้องคุ้มครองถึงเมื่อใด? 5. ระบบใดเสี่ยงต่อการปลอมลายมือชื่อ ไบรรับรอง หรือการสวมรอย? 6. ระบบใดสำคัญต่อธุรกิจและต้องเปลี่ยนก่อน แม้ข้อมูลไม่ได้เก็บไว้นาน? 7. ลำดับความสำคัญพิจารณาระบบเดิม คู่ค้า / ผู้ให้บริการ และเวลาที่ต้องใช้จริงแล้วหรือไม่? 8. คู่ค้า / ผู้ให้บริการรายใดอาจทำให้องค์กรเปลี่ยนผ่านไม่ทัน และมีหลักฐานใดรองรับ? 9. รายการที่ต้องทำก่อนมีผู้รับผิดชอบ งบประมาณ และกำหนดแล้วเสร็จหรือยัง? 10. ระบบใหม่และสัญญาใหม่ถูกกันไม่ให้เพิ่มภาระที่ต้องแก้ไขในอนาคตหรือไม่?	☐ ขอบเขตและความครอบคลุมของ CBOM ☐ วิธีพิสูจน์ความครบถ้วนและความถูกต้อง ☐ รายการความเสี่ยงสำคัญพร้อมเหตุผล ☐ อายุความลับและผลกระทบทางธุรกิจ ☐ ความเสี่ยงด้านลายมือชื่อและตัวตน ☐ แผนและหลักฐานจากคู่ค้า / ผู้ให้บริการรายสำคัญ ☐ งบประมาณและแผนหลายปี	☐ รับรองลำดับความสำคัญ ☐ ขอบขยายขอบเขตสำรวจ ☐ กำหนดกรอบเวลาคู่ค้า / ผู้ให้บริการ ☐ อนุมัติงบประมาณ ☐ พิจารณายอมรับความเสี่ยง ☐ ขอบทางเลือกหรือแผนสำรอง
ข้อเสนอของคณะกรรมการ ลำดับที่รับรอง _____ มติ / เจื่อนไข _____ กำหนดรายงานกลับ _____		

ระยะที่ 3 — ทดลองและพิสูจน์ว่าใช้ได้จริง

คำถามที่คณะกรรมการควรถาม	หลักฐานที่ควรได้รับ	เรื่องที่อาจพิจารณา
- เหตุใดจึงเลือกระบบนี้เป็นโครงการนำร่อง และต้องการเรียนรู้อะไร? - เกณฑ์ผ่าน เกณฑ์หยุด และแผนถอยกลับชัดเจนหรือไม่? - ผลทดสอบครอบคลุมปริมาณงานจริง ความเร็ว ความจุ เครือข่าย ใบบรรอง และอุปกรณ์หรือยัง? - ทดสอบการเชื่อมต่อกับลูกค้า / ผู้ให้บริการและผลต่อลูกค้าหรือไม่? - หากใช้ Hybrid, QKD หรือ QRNG มีเหตุผลและมาตรฐานรองรับหรือไม่? - ก่อนขยายผล ยังมีข้อจำกัดและความเสี่ยงใดเหลืออยู่? - ใครมีอำนาจตัดสินใจว่าจะขยายผล ปรับแก้ หรือยุติ?	☐ เหตุผลและขอบเขตการนำร่อง ☐ เกณฑ์ผ่านและแผนถอยกลับ ☐ ผลทดสอบกับระบบจริง ☐ ผลต่อบริการและลูกค้า / ผู้ให้บริการ ☐ ข้อจำกัดและความเสี่ยงที่ยังเหลือ ☐ ความเห็นจากผู้สอบทานอิสระ	☐ อนุมัตินำร่อง ☐ ปรับขอบเขตหรือเกณฑ์ทดสอบ ☐ ขอข้อมูลเพิ่มเติม ☐ ขยายผลแบบมีเงื่อนไข ☐ ให้ทดสอบซ้ำ ☐ ยุติโครงการนำร่อง
ข้อสรุปของคณะกรรมการ มติ ☐ ขยายผล ☐ มีเงื่อนไข ☐ ทดสอบซ้ำ ☐ ยุติ เงื่อนไข _____ กำหนดรายงานกลับ _____		

ระยะที่ 4 — การเปลี่ยนผ่านระบบที่มีความสำคัญตามลำดับ

คำถามที่คณะกรรมการควรถาม	หลักฐานที่ควรได้รับ	เรื่องที่อาจพิจารณา
- ระบบและข้อมูลใดอยู่ในรอบการเปลี่ยนผ่านนี้ และเหตุใดจึงต้องเริ่มก่อน? - งบประมาณและกำลังคนเพียงพอหรือไม่? - ลูกค้า / ผู้ให้บริการรายสำคัญพร้อมตามกำหนดและมีหลักฐานเพียงพอหรือยัง? - ใบบรรอง ระบบบริหารกฎแฉ และการเชื่อมต่อถูกประสานงานครบแล้วหรือไม่? - แผนถอยกลับและแผนรับเหตุขัดข้อง ผ่านการทดสอบหรือยัง? - มีข้อยกเว้นใดเกินกำหนดหรือไม่ผู้รับผิดชอบ? - ความเสี่ยงที่ยังเหลืออยู่ในระดับที่องค์กรยอมรับได้หรือไม่? - หากลูกค้า / ผู้ให้บริการไม่พร้อม ทางเลือกสำรองคืออะไร?	☐ แผนเปลี่ยนผ่านตามความเสี่ยง ☐ งบประมาณ กำลังคน และลูกค้า / ผู้ให้บริการ ☐ ผลทดสอบก่อนใช้งานจริง ☐ แผนถอยกลับ ☐ ผลกระทบต่อลูกค้าและบริการ ☐ ข้อยกเว้นและความเสี่ยงที่ยังเหลือ	☐ อนุมัติงบหรือทรัพยากรเพิ่ม ☐ กำหนดกรอบเวลา ☐ อนุมัติข้อยกเว้น ☐ พิจารณาความเสี่ยงที่ยังเหลือ ☐ เปลี่ยนลูกค้า / ผู้ให้บริการหรือผลิตภัณฑ์ ☐ ชะลอหรือปรับลำดับ
ข้อสรุปของคณะกรรมการ มติ / เงื่อนไข _____ ความเสี่ยงที่รับทราบ _____ กำหนดรายงานกลับ _____		

ระยะที่ 5 — ทำให้เป็นงานประจำและปรับปรุงต่อเนื่อง		
คำถามที่คณะกรรมการควรถาม	หลักฐานที่ควรได้รับ	เรื่องที่อาจพิจารณา
1. CBOM ถูกปรับเมื่อมีระบบใหม่ อัปเดต เปลี่ยนใบรับรอง หรือต่อสัญญาหรือไม่? 2. ระบบใหม่เปลี่ยนรหัสได้โดยไม่ต้องรีเซ็ตระบบครั้งใหญ่หรือไม่? 3. TOR และสัญญาใหม่ครอบคลุม PQC การทดสอบ การอัปเดต และทางออกหรือยัง? 4. หากต้องเปลี่ยนหรือถอนอัลกอริทึมเร่งด่วน องค์กรทำได้ภายในเวลาเท่าใด? 5. คนที่มีบทบาทสำคัญทำงานได้จริงและมีการถ่ายทอดความรู้หรือไม่? 6. หน่วยงานกำกับความเสี่ยงและตรวจสอบภายในให้ความเชื่อมั่นเรื่องใดแล้วบ้าง? 7. มาตรฐาน ภัย หรือความพร้อมของคู่ค้า / ผู้ให้บริการเปลี่ยนจนต้องปรับ Roadmap หรือไม่? 8. รายงานต่อคณะกรรมการยังสะท้อนความเสี่ยงที่เหลือและเรื่องที่ต้องตัดสินใจหรือไม่?	☐ หลักฐานการปรับ CBOM ☐ มาตรฐาน Crypto Agility ☐ ข้อกำหนดใน TOR และสัญญา ☐ ผลการซ้อมเปลี่ยนรหัสเร่งด่วน ☐ แผนทักษะและการถ่ายทอดความรู้ ☐ ผลการสอบทานจากหน่วยงาน Second Line และ Third Line ☐ สรุปมาตรฐานและสมมติฐานที่เปลี่ยน	☐ ปรับนโยบายหรือมาตรฐานองค์กร ☐ กำหนดความถี่การสอบทาน ☐ อนุมัติการลงทุนต่อเนื่อง ☐ ขอรทดสอบเพิ่มเติม ☐ ปิดข้อบกพร่องที่ค้าง ☐ ปรับ Roadmap
ข้อสรุปของคณะกรรมการ เรื่องที่ต้องปรับปรุง _____ มติ / เจอนไข _____ กำหนดทบทวนครั้งถัดไป _____		

เครื่องมือที่ 2 – ตารางกลั่นกรองความเสี่ยงและลำดับงาน

ใช้เป็นเครื่องมือช่วยกลั่นกรองประเด็นสำคัญที่คณะกรรมการควรติดตามเป็นลำดับแรก เพื่อประโยชน์ในการจัดลำดับความสำคัญ

รอบรายงาน _____ ผู้บริหารที่รับผิดชอบหลัก _____ วันที่ทบทวนครั้งถัดไป _____				
เรื่องที่คณะกรรมการ ควรติดตาม	เหตุผลที่ควรให้ความสำคัญ	สถานะ	การดำเนินการ / ผู้รับผิดชอบ / กำหนดแล้วเสร็จ	เรื่องที่เสนอให้ คณะกรรมการ พิจารณา
ตัวอย่าง ระบบลงนามคำสั่งธุรกรรม เจ้าของความเสี่ยง: COO	☒ มีความเสี่ยงต่อการ ปลอมแปลงหรือสวมรอย ☒ กระทบระบบหรือบริการ สำคัญขององค์กร	☒ ต้องเร่ง พิจารณา คู่ค้า / ผู้ให้บริการ ยังไม่ยืนยันวันที่ พร้อมใช้งาน	การดำเนินการ: เสนอ ผลทดสอบและแผนสำรอง ผู้รับผิดชอบ: CIO กำหนดแล้วเสร็จ: ก่อนการ ประชุมครั้งถัดไป	☒ อนุมัติงบประมาณ ☒ กำหนดกรอบเวลา ให้คู่ค้า / ผู้ให้บริการ ☒ ขอให้เสนอ ทางเลือกสำรอง
1. _____ เจ้าของความเสี่ยง: _____	☐ ข้อมูลที่ต้องเก็บเป็น ความลับนาน ☐ มีความเสี่ยงต่อการ ปลอมแปลงหรือสวมรอย ☐ กระทบระบบหรือบริการ สำคัญขององค์กร ☐ ต้องรอความพร้อมจาก คู่ค้า / ผู้ให้บริการ	☐ ข้อมูลยังไม่ เพียงพอ ☐ ต้องเร่ง พิจารณา ☐ มีแผนและ ติดตามได้ ☐ เป็นไปตามแผน	การดำเนินการ: _____ ผู้รับผิดชอบ: _____ กำหนดแล้วเสร็จ: _____	☐ อนุมัติงบประมาณ ☐ กำหนดกรอบเวลา ☐ พิจารณายอมรับ ความเสี่ยง ☐ ขอข้อมูลหรือ ทางเลือกเพิ่มเติม
2. _____ เจ้าของความเสี่ยง: _____	☐ ข้อมูลที่ต้องเก็บเป็น ความลับนาน ☐ มีความเสี่ยงต่อการ ปลอมแปลงหรือสวมรอย ☐ กระทบระบบหรือบริการ สำคัญขององค์กร ☐ ต้องรอความพร้อมจาก คู่ค้า / ผู้ให้บริการ	☐ ข้อมูลยังไม่ เพียงพอ ☐ ต้องเร่ง พิจารณา ☐ มีแผนและ ติดตามได้ ☐ เป็นไปตามแผน	การดำเนินการ: _____ ผู้รับผิดชอบ: _____ กำหนดแล้วเสร็จ: _____	☐ อนุมัติงบประมาณ ☐ กำหนดกรอบเวลา ☐ พิจารณายอมรับ ความเสี่ยง ☐ ขอข้อมูลหรือ ทางเลือกเพิ่มเติม
ข้อสรุปของคณะกรรมการ มติ / ทิศทาง: _____ เงื่อนไขและหลักฐานที่ต้องได้รับ: _____ ผู้บริหารที่รับผิดชอบหลัก _____ กำหนดรายงานกลับ _____				

เครื่องมือที่ 3 – Dashboard สำหรับคณะกรรมการ

รายงานหน้าเดียวที่ตอบ 3 คำถามหลัก ได้แก่ ความเสี่ยงสำคัญอยู่ที่ใด สถานะเปลี่ยนไปอย่างไรจากครั้งก่อน และคณะกรรมการต้องตัดสินใจเรื่องใด โดยองค์กรกำหนดรอบการรายงานตามความเหมาะสม

หมายเหตุ: ตัวเลขสมมติ เกณฑ์ที่ยอมรับได้ และการกำหนดผู้รับผิดชอบ ในตารางนี้เป็นเพียงตัวอย่างเพื่อการอธิบาย มิใช่ข้อกำหนดหรือแนวทางตามความคาดหวังของสำนักงาน ก.ล.ต.



ตัวชี้วัดความเสี่ยงเทียบระดับที่คณะกรรมการยอมรับได้

ตัวชี้วัด	ครั้งนี้	ครั้งก่อน	เกณฑ์ที่ยอมรับได้	สถานะ
ระบบสำคัญที่ยังไม่ทราบว่าจะใช้รหัสใด	X%	Y%	ไม่เกิน Z %	ยังเกินเกณฑ์
ข้อมูลอายุยาวที่ยังไม่ได้รับการป้องกันเพิ่ม	X ชุด	Y ชุด	ควรเป็น Z	เกินเกณฑ์
คู่ค้า / ผู้ให้บริการรายสำคัญที่ยังไม่ยืนยันแผนและกำหนดเวลา	X ราย	Y ราย	ไม่เกิน Z ราย	เกินเกณฑ์
ข้อบกพร่องที่เกินกำหนดปิด	X รายการ	Y รายการ	ควรเป็น Z	แย่มาก
ระบบสำคัญที่เปลี่ยนผ่านและผ่านการทดสอบแล้ว	X / Y	X / Y	ตามแผนที่อนุมัติ	เป็นไปตามแผน
ระบบสำคัญที่ยังใช้รหัสซึ่งจะพ้นการรับรองตามมาตรฐานสากล	X ระบบ	Y ระบบ	ควรมีแผนรองรับทุกระบบ	เกินเกณฑ์
สัญญาหรือการจัดซื้อใหม่ที่ยังไม่มีข้อกำหนดด้านรหัสลับ	X ฉบับ	Y ฉบับ	ควรเป็น Z ฉบับ	ดีขึ้นแต่ยังไม่ถึงเกณฑ์
ระบบใหม่ที่ออกแบบให้เปลี่ยนวิธีเข้ารหัสได้โดยไม่ต้องรื้อระบบ	X%	Y%	ไม่น้อยกว่า Z%	อยู่ในเกณฑ์

ความเสี่ยงสำคัญที่ต้องติดตาม				งานสำคัญใน 90 วันข้างหน้า		
ความเสี่ยง	ผลกระทบ	โอกาสเกิด	ระดับ	สิ่งที่ควรดำเนินการ	ผู้รับผิดชอบ	กำหนด
ข้อมูลถูกดักเก็บวันนี้เพื่อถอดรหัสภายหลัง (HNDL)	สูง	สูง	สูง	จัดทำบัญชีรายการการใช้รหัสลับของระบบสำคัญให้ครบ	CIO	90 วัน
การปลอมลายมือชื่อหรือคำสั่งธุรกรรม	สูง	กลาง	สูง	ขอคำยืนยันแผนและวันที่พร้อมจากคู่ค้า / ผู้ให้บริการ	ฝ่ายจัดซื้อ	60 วัน
คู่ค้า / ผู้ให้บริการรายสำคัญยังไม่พร้อมตามกำหนด	สูง	สูง	สูง	ทดสอบความเข้ากันได้ของระบบนำร่อง	CTO	90 วัน
ขอบเขตบัญชีรายการการใช้รหัสลับยังไม่ครบถ้วน	กลาง	สูง	สูง	ซ้อมแผนถอยกลับและการรับมือเหตุขัดข้อง	COO	90 วัน
ระบบเดิมที่เปลี่ยนรหัสได้ยาก	กลาง	กลาง	กลาง	ปิดช่องกเว้นที่เกินกำหนดทั้งหมด	CIO	90 วัน

จุดที่ใช้รหัสลับและผลกระทบต่อธุรกิจ		
ข้อมูลลูกค้าและข้อมูลการเงิน	ต้องเก็บเป็นความลับระยะยาว กระทบความเชื่อมั่นและการกำกับดูแลหากรั่วไหล	
ลายมือชื่อดิจิทัลและการยืนยันตัวตน	คำสั่งปลอมอาจถูกยอมรับว่าเป็นของจริง กระทบธุรกรรมและความรับผิดชอบ	
ใบรับรองและระบบบริหารกุญแจ	การเปลี่ยนกระทบหลายระบบพร้อมกัน ต้องวางแผนล่วงหน้า	
โครงสร้างพื้นฐานและระบบเดิม	เปลี่ยนยากและใช้เวลานาน เป็นข้อจำกัดของกรอบเวลาโดยรวม	
การเชื่อมต่อภายนอกและคลาวด์	ทดสอบผ่านบางส่วน อยู่ระหว่างขยายขอบเขต	

■ ควรเร่งดำเนินการ ■ ควรติดตามใกล้ชิด ■ เป็นไปตามแผน

เรื่องที่ขอมติหรือกึ่งทางจากคณะกรรมการ		
เรื่องที่เสนอ	ผู้รับผิดชอบ	กำหนดรายงานกลับ
1. กำหนดให้คู่ค้า / ผู้ให้บริการระบบลงนามยืนยันแผนและวันที่พร้อมใช้งานภายใน 60 วัน และอนุมัติแนวทางสำรองหากส่งมอบไม่ทัน	CIO / COO	รอบถัดไป
2. ให้เสนอแผนงบประมาณ และกำหนดปิดช่องกเว้นที่ค้างอยู่	CFO / CIO	ภายใน 2 เดือน

☐ รับทราบ ☐ เห็นชอบตามข้อเสนอมติ ☐ เห็นชอบโดยมีเงื่อนไข ☐ ขอข้อมูลเพิ่มเติม ☐ รับทราบความเสี่ยงที่ยังเหลือ
มติและเงื่อนไข _____ ผู้รับผิดชอบ _____ หลักฐานที่ต้องได้รับ _____

เครื่องมือที่ 4 – สรุปภาพรวมคู่ค้า / ผู้ให้บริการรายสำคัญสำหรับคณะกรรมการ

รายงานหน้าเดียวที่แสดงคู่ค้า / ผู้ให้บริการซึ่งหากเปลี่ยนผ่านไม่ทันแล้วกระทบระบบหรือบริการสำคัญ เพื่อให้คณะกรรมการเห็นในคราวเดียวว่ารายใดเป็นข้อจำกัดของแผน และมีเรื่องใดที่ต้องตัดสินใจ

ฝ่ายบริหารเป็นผู้รวบรวมและรับรองข้อมูล เสนอตามรอบเดียวกับเครื่องมือที่ 3 และก่อนต่อสัญญาที่มีนัยสำคัญ

สรุปภาพรวมคู่ค้า / ผู้ให้บริการรายสำคัญ				
รอบรายงาน _____ ผู้บริหารที่รับผิดชอบหลัก _____ วันที่ทบทวนครั้งถัดไป _____				
ข้อจำกัดสำคัญของแผน: _____				
สิ่งที่ขอลาจากคณะกรรมการ: _____				
ชื่อคู่ค้า / ผู้ให้บริการ	ระบบที่พึ่งพา และสัดส่วนการพึ่งพา	แผนรองรับ PQC และวันที่พร้อม	ผลกระทบหากไม่ทัน / ทางเลือกสำรอง / วันที่ต่อสัญญา	ความเร่งด่วน และเรื่องที่เสนอ
ตัวอย่าง บริษัท ก จำกัด (นามสมมติ) ผู้รับผิดชอบ: CIO	ระบบรับส่งคำสั่งซื้อขาย หลักกรรพย์ (OMS) สัดส่วนการพึ่งพา: ☒ สูง	☒ ยังไม่ยืนยัน	ผลกระทบ: การรับส่งคำสั่งซื้อขายอาจหยุดชะงัก ทางเลือกสำรอง: อยู่ระหว่างจัดทำ วันที่ต่อสัญญา: ไตรมาสถัดไป	☒ สูง ☒ กำหนดกรอบเวลา ☒ ทบทวนเงื่อนไขสัญญา ☒ พิจารณายอมรับความเสี่ยง
1. ชื่อ: _____ ผู้รับผิดชอบ: _____	ระบบที่พึ่งพา: _____ สัดส่วนการพึ่งพา: _____ ☐ สูง ☐ กลาง ☐ ต่ำ	☐ ยืนยันแล้ว ☐ ยืนยันบางส่วน ☐ ยังไม่ยืนยัน วันที่พร้อม: _____	ผลกระทบ: _____ ทางเลือกสำรอง: _____ วันที่ต่อสัญญา: _____	☐ สูง ☐ กลาง ☐ ต่ำ ☐ กำหนดกรอบเวลา ☐ อนุมัติทางเลือกสำรอง ☐ ทบทวนเงื่อนไขสัญญา ☐ พิจารณายอมรับความเสี่ยง
2. ชื่อ: _____ ผู้รับผิดชอบ: _____	ระบบที่พึ่งพา: _____ สัดส่วนการพึ่งพา: _____ ☐ สูง ☐ กลาง ☐ ต่ำ	☐ ยืนยันแล้ว ☐ ยืนยันบางส่วน ☐ ยังไม่ยืนยัน วันที่พร้อม: _____	ผลกระทบ: _____ ทางเลือกสำรอง: _____ วันที่ต่อสัญญา: _____	☐ สูง ☐ กลาง ☐ ต่ำ ☐ กำหนดกรอบเวลา ☐ อนุมัติทางเลือกสำรอง ☐ ทบทวนเงื่อนไขสัญญา ☐ พิจารณายอมรับความเสี่ยง
ข้อสรุปของคณะกรรมการ ☐ รับทราบ ☐ เห็นชอบตามข้อเสนอ ☐ เห็นชอบโดยมีเงื่อนไข ☐ ขอลข้อมูลเพิ่มเติม ☐ รับทราบความเสี่ยงที่ยังเหลือ มติและเงื่อนไข _____ ผู้รับผิดชอบ _____ กำหนดรายงานกลับ _____				

ภาคผนวก ข — อภิธานศัพท์

คำอธิบายแบบเข้าใจง่ายของศัพท์ที่ใช้ในเล่ม โดยนิยามบางคำปรับให้เหมาะกับบริบทการกำกับดูแลและควรอ่านร่วมกับแหล่งอ้างอิงท้ายเล่ม

กลุ่มที่ 1 — ความเสี่ยงและกรอบเวลา

คำศัพท์	ความหมายแบบเข้าใจง่าย
CRQC Cryptographically Relevant Quantum Computer	คอมพิวเตอร์ควอนตัมที่มีพลังมากพอที่จะถอดรหัสและทำให้การเข้ารหัสบางชนิดที่ใช้อยู่ในปัจจุบันไม่ปลอดภัย
HNDL Harvest Now, Decrypt Later	การดักเก็บข้อมูลที่ยังอ่านไม่ได้ในวันนี้ เพื่อรอถอดรหัสเมื่อเทคโนโลยีพร้อมในอนาคต
TNFL Trust Now, Forge Later	ความเสี่ยงที่ลายมือชื่อ ใบรับรอง ตัวตน หรือคำสั่งที่เชื่อถือในวันนี้อาจถูกปลอมได้ในอนาคต
กฎของมอสคา Mosca's Theorem (หรืออสมการของมอสคา / Mosca's Inequality)	กรอบคิดที่เปรียบเทียบอายุความลับของข้อมูล เวลาที่ใช้เปลี่ยนระบบ และเวลาที่คาดว่าเหลือก่อนภัยจะมีนัยสำคัญ
ความเสี่ยงที่ยังเหลือ Residual Risk	ความเสี่ยงส่วนที่ยังคงอยู่หลังจากที่องค์กรได้ดำเนินการมาตรการลดความเสี่ยงแล้ว

กลุ่มที่ 2 – เทคโนโลยีและมาตรฐาน

คำศัพท์	ความหมายแบบเข้าใจง่าย
PQC Post-Quantum Cryptography	วิทยาการรหัสลับรุ่นใหม่ที่จะออกแบบให้ทนต่อการโจมตีจากทั้งคอมพิวเตอร์ทั่วไปและคอมพิวเตอร์ควอนตัม
QKD Quantum Key Distribution	การใช้คุณสมบัติทางฟิสิกส์ควอนตัมเพื่อกระจายกุญแจและช่วยตรวจพบการดักฟังระหว่างส่งกุญแจ
QRNG Quantum Random Number Generator	อุปกรณ์หรือกลไกที่ใช้ปรากฏการณ์ควอนตัมสร้างเลขสุ่มสำหรับกุญแจและงานความมั่นคงปลอดภัย
แนวทางแบบผสมผสาน Hybrid Approach	การใช้รหัสแบบเดิมร่วมกับรหัสรุ่นใหม่ในช่วงเปลี่ยนผ่าน เพื่อลดการพึ่งพาเทคโนโลยีใหม่เพียงชั้นเดียว
FIPS 203–205	มาตรฐาน PQC ชุดแรกของ NIST สำหรับการสร้างความลับร่วมและลายมือชื่อดิจิทัล ซึ่งประกาศใช้ในปี 2024 ทั้งนี้ ยังมีมาตรฐานลายมือชื่อทางเลือกเพิ่มเติมที่อยู่ระหว่างจัดทำ
RSA Rivest–Shamir–Adleman	รหัสกุญแจสาธารณะที่ใช้แพร่หลายในการแลกเปลี่ยนกุญแจ ลายมือชื่อดิจิทัล และใบรับรองความปลอดภัยอาศัยความยากของการแยกตัวประกอบจำนวนขนาดใหญ่ ซึ่งเป็นโจทย์ที่คอมพิวเตอร์ควอนตัมที่ใหญ่พอจะแก้ได้
ECC Elliptic Curve Cryptography	รหัสกุญแจสาธารณะบนเส้นโค้งวงรี ให้ความแข็งแกร่งใกล้เคียงกับ RSA โดยใช้กุญแจสั้นกว่า จึงนิยมในอุปกรณ์และช่องทางสื่อสารที่มีทรัพยากรจำกัด แต่ถูกทำลายด้วยวิธีเดียวกับ RSA
อัลกอริทึมของชอร์ Shor’s Algorithm	วิธีคำนวณบนคอมพิวเตอร์ควอนตัมที่สามารถแก้ปัญหาคณิตศาสตร์การแยกตัวประกอบจำนวนเต็มและปัญหาลอการิทึมไม่ต่อเนื่อง (Discrete Logarithm Problem) ได้เร็วกว่าวิธีดั้งเดิมอย่างมีนัยสำคัญ จึงเป็นเหตุผลสำคัญที่ทำให้การเข้ารหัสแบบ RSA และ ECC ไม่ปลอดภัยในยุคควอนตัม
AES Advanced Encryption Standard	รหัสแบบสมมาตรที่ใช้กุญแจเดียวกันในการเข้ารหัสและถอดรหัส ใช้ปกป้องข้อมูลปริมาณมากทั้งขณะจัดเก็บและรับส่ง โดยทั่วไปยังใช้ได้ในยุคควอนตัมหากความยาวกุญแจเพียงพอ เช่น AES-256

กลุ่มที่ 3 – การสำรวจและเปลี่ยนผ่าน

คำศัพท์	ความหมายแบบเข้าใจง่าย
CBOM Cryptographic Bill of Materials	บัญชีที่บอกว่ารหัสลับอยู่ในระบบใด ปกป้องข้อมูลหรือกระบวนการใด ใครเป็นเจ้าของ และพึ่งพาใครบ้าง
ความคล่องตัวทางวิทยาการรหัสลับ Crypto Agility	ความสามารถในการเปลี่ยนหรือถอนรหัสได้ทัน โดยบริการไม่หยุดและไม่ต้องรื้อระบบครั้งใหญ่ทุกครั้ง
ใบรับรองอิเล็กทรอนิกส์ Digital Certificate	ข้อมูลรับรองอิเล็กทรอนิกส์ที่ผูกตัวตนหรือระบบกับกุญแจสาธารณะ (Public Key) เพื่อช่วยให้อีกฝ่ายยืนยันได้ว่าข้อมูลดังกล่าวเป็นของจริง
ระบบบริหารกุญแจ Key Management System	ระบบที่ควบคุมวงจรชีวิตของกุญแจ ตั้งแต่สร้าง เก็บ แจก ใช้ หมุนเวียน เพิกถอน จนถึงทำลาย
ระบบเดิม Legacy System	ระบบเก่าที่ยังจำเป็นต่อธุรกิจ แต่อาจแก้ไขยาก ขาดผู้ดูแล หรือไม่รองรับมาตรฐานและผลิตภัณฑ์รุ่นใหม่
แผนถอยกลับ Rollback Plan	แผนกลับไปยังสถานะที่ปลอดภัยและให้บริการต่อได้ หากการเปลี่ยนแปลงใหม่ทำให้เกิดปัญหา และระบบอาจไม่สามารถใช้งานต่อได้
โครงการนำร่อง Pilot	การทดลองในขอบเขตที่ควบคุมได้ เพื่อเรียนรู้ผลต่อระบบจริงก่อนขยายผล
แผนเปลี่ยนผ่าน Transition Roadmap	แผนหลายปีที่เชื่อมความเสี่ยง ระบบ คู่ค้า บุคลากร งบประมาณ ผลลัพธ์ และเงื่อนไขก่อนขยับระยะถัดไป
Project Leap โครงการ Leap	โครงการของ BIS Innovation Hub ร่วมกับธนาคารกลางและผู้ให้บริการโครงสร้างพื้นฐาน เพื่อทดลองทำให้ระบบการเงินและระบบการชำระเงินทนต่อภัยควอนตัมด้วย PQC โดยระยะที่ 1 เผยแพร่ปี 2023 และระยะที่ 2 ปี 2025

กลุ่มที่ 4 – การกำกับดูแล

คำศัพท์	ความหมายแบบเข้าใจง่าย
Three Lines Model	หลักแบ่งบทบาทเพื่อให้การปฏิบัติงาน การกำกับดูแล และการตรวจสอบถ่วงดุลกัน โดยรายละเอียดต้องใช้ตามบริบทและหลักเกณฑ์ขององค์กร
ผู้บริหารที่รับผิดชอบหลัก	ผู้บริหารหนึ่งคนที่ได้รับผิดชอบผลลัพธ์โดยรวม มีอำนาจประสานหลายฝ่าย เข้าถึงทรัพยากร และยกระดับปัญหา
เจ้าของความเสี่ยง Risk Owner	บุคคลหรือหน่วยงานที่รับผิดชอบบริหารความเสี่ยงนั้น ตัดสินใจเลือกวิธีตอบสนอง และติดตามผล
เกณฑ์ผ่าน / เกณฑ์หยุด Go / Stop Criteria	เงื่อนไขที่กำหนดล่วงหน้าว่าผลแบบใดยอมรับได้ แบบใดต้องแก้ไข และแบบใดต้องหยุดหรือเปลี่ยนแนวทาง
การสอบทานอิสระ Independent Review	การประเมินโดยผู้ที่ไม่ได้รับผิดชอบลงมือทำงานนั้นโดยตรง เพื่อกำทายข้อมูล หลักฐาน และข้อสรุปอย่างเป็นกลาง

เอกสารอ้างอิง

1. **Bank for International Settlements Innovation Hub, Bank of Italy, Banque de France, Deutsche Bundesbank, Nexi-Colt, & Swift.** (2025). *Project Leap phase 2: Quantum-proofing payment systems*. Bank for International Settlements.
2. **Bank for International Settlements Innovation Hub, Banque de France, & Deutsche Bundesbank.** (2023). *Project Leap phase 1: Quantum-proofing the financial system*. Bank for International Settlements.
3. **Bernstein, D. J., Hülsing, A., & Lange, T.** (2022). *Post-quantum cryptography: Integration study*. European Union Agency for Cybersecurity.
4. **Beullens, W., D’Anvers, J.-P., Hülsing, A., Lange, T., Panny, L., de Saint Guilhem, C., & Smart, N. P.** (2021). *Post-quantum cryptography: Current state and quantum mitigation (Version 2)*. European Union Agency for Cybersecurity.
5. **Canadian Centre for Cyber Security.** (2025). *Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)*.
6. **CRYPTREC.** (2025). *CRYPTREC cryptographic technology guideline—Post-quantum cryptography—2024 edition (CRYPTREC GL-2007-2024)*.
7. **Cyber Security Agency of Singapore, Government Technology Agency of Singapore, & Infocomm Media Development Authority.** (2026). *Quantum-safe migration handbook and Quantum Readiness Index*.
8. **CyberSecurity Malaysia.** (2024). *Post-quantum cryptography migration framework (CD-4-RPT-2724-PQCMigration-V1)*.
9. **European Commission.** (2024). *Commission Recommendation (EU) 2024/1101 of 11 April 2024 on a coordinated implementation roadmap for the transition to post-quantum cryptography*.
10. **Mosca, M., & Piani, M.** (2026). *Quantum threat timeline report 2025*. Global Risk Institute in Financial Services.
11. **Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D.** (2024). *Transition to post-quantum cryptography standards (NIST IR 8547, Initial Public Draft)*. National Institute of Standards and Technology.
12. **National Association of Corporate Directors, & Internet Security Alliance.** (2023). *Director’s handbook on cyber-risk oversight*.
13. **National Cybersecurity Center of Excellence.** (n.d.). *Migration to post-quantum cryptography*. National Institute of Standards and Technology.
14. **National Cyber Security Centre.** (2023). *Cyber security toolkit for boards*.
15. **National Cyber Security Centre.** (2025). *Timelines for migration to post-quantum cryptography*.
16. **National Institute of Standards and Technology.** (2024a). *Module-lattice-based digital signature standard (FIPS 204)*.
17. **National Institute of Standards and Technology.** (2024b). *Module-lattice-based key-encapsulation mechanism standard (FIPS 203)*.
18. **National Institute of Standards and Technology.** (2024c). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29)*.
19. **National Institute of Standards and Technology.** (2024d). *NIST Cybersecurity Framework 2.0: Quick-start guide for creating and using organizational profiles (NIST SP 1301)*.

20. **National Institute of Standards and Technology.** (2024e). *Stateless hash-based digital signature standard* (FIPS 205).
21. **NIS Cooperation Group.** (2025). *A coordinated implementation roadmap for the transition to post-quantum cryptography*. European Commission.
22. **สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ.** (2568). *Post Quantum Cryptography*.
23. **สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ.** (2569ก). (ร่าง) กรอบการเตรียมความพร้อมเข้าสู่ยุคควอนตัม พ.ศ. 2569–2578.
24. **สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ.** (2569ข). *QUANTA Platform: แพลตฟอร์มควอนตัมเพื่อการเรียนรู้ ประเมิน และติดตามระดับชาติ*.
25. **สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ.** (2568ก). *คู่มือการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) สำหรับกรรมการบริษัทในภาคตลาดทุน*.
26. **สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ.** (2568ข). *Quantum Risk: ภัยคุกคามใหม่ในโลกดิจิทัล ที่ไม่ควรมองข้าม*.
27. **สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ.** (2569). *Quantum Risk: UNHOD การรักษาความลับที่ต้องแข่งกับเวลา*.

หมายเหตุการจัดทำ

คู่มือฉบับนี้จัดทำขึ้นเพื่อส่งเสริมความรู้และความตระหนักด้านความเสี่ยงจากเทคโนโลยีควอนตัมและการเตรียมความพร้อมขององค์กรในตลาดทุน ไม่ใช่ข้อกำหนด หรือหลักเกณฑ์ของสำนักงาน ก.ล.ต. ผู้อ่านควรตรวจสอบข้อมูลที่เป็นปัจจุบันและพิจารณาความเหมาะสมกับบริบทขององค์กรก่อนนำไปใช้

การจัดทำเนื้อหาบางส่วนและภาพประกอบมีการใช้เครื่องมือปัญญาประดิษฐ์ (AI) เป็นเครื่องมือสนับสนุน โดยภาพประกอบทั้งหมดสร้างขึ้นเพื่อสื่อความหมายเชิงแนวคิด ซึ่งเนื้อหาและภาพประกอบได้ผ่านการสอบทานโดยฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงาน ก.ล.ต. ทั้งนี้ การกล่าวถึงเทคโนโลยีมาตรฐาน ผลิตภัณฑ์ หรือบริการ มิได้หมายถึงการรับรองหรือสนับสนุนโดยสำนักงาน ก.ล.ต.