# แนวทางการจัดทำแผนเตรียมความพร้อมด้าน IT QAB สัญชาติมาเลเซีย

เอกสารแนบ 3

*(ข้อ 1-17 สำหรับคำขอทุกกรณี)*

**แผนเตรียมความพร้อมด้าน IT โดยควรมีรายละเอียดอย่างน้อย** ดังนี้

1. โครงสร้างการกำกับดูแลด้าน IT (IT Governance Structure) ครอบคลุมทั้ง 3 Lines of Defense
2. รายชื่อและคุณสมบัติของผู้บริหารทั้ง 3 Lines of Defense
3. รายชื่อและประวัติกรรมการสถาบันการเงินที่มีประวัติด้านการบริหารจัดการ IT
4. นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security Policy)
5. นโยบายบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Policy)
6. จำนวนบุคลากรด้าน IT ที่อยู่ที่ประเทศไทย และ Job Description (JD)
7. ข้อมูลศูนย์คอมพิวเตอร์ (Data Center) ทั้งศูนย์คอมพิวเตอร์หลักและสำรอง เช่น สถานที่ตั้ง การรักษาความมั่นคงปลอดภัย ความพร้อมระบบไฟฟ้า ระบบไฟฟ้าสำรอง ระบบดับเพลิง ระบบทำความเย็น เป็นต้น
8. แผนภาพระบบงานด้าน IT (IT System Diagram) ทั้งที่ศูนย์คอมพิวเตอร์หลักและสำรอง
9. รายละเอียดระบบงานที่ใช้ในการให้บริการในประเทศไทย ทั้งที่ศูนย์คอมพิวเตอร์หลักและสำรอง เช่น ชื่อระบบงาน ระบบปฏิบัติการ เป็นต้น
10. แผนภาพระบบเครือข่าย (Network Diagram) และอุปกรณ์รักษาความปลอดภัยเครือข่ายทั้งที่ศูนย์คอมพิวเตอร์หลักและสำรอง
11. มาตรฐาน/กระบวนการรักษาความปลอดภัยข้อมูล (Information Security)
12. มาตรฐานการจัดชั้นความลับข้อมูลและการรักษาความมั่นคงปลอดภัยตามระดับชั้นความลับ
13. มาตรฐานการเข้ารหัสและการบริหารจัดการการเข้ารหัส
14. กระบวนการควบคุมการเข้าถึงระบบงาน (Access Control) เช่น แนวทางการกำหนดสิทธิ (ทั้งระดับบัญชีผู้ใช้งานทั่วไปและบัญชีผู้ใช้งานสิทธิสูง) กระบวนการพิสูจน์ตัวตน (Authentication) กระบวนการบริหารจัดการสิทธิสูง เป็นต้น
15. กระบวนการตั้งค่าความปลอดภัย (Security Baseline Standard) เช่น การกำหนดการรักษาความมั่นคงปลอดภัยขั้นต่ำ (Minimum Security Baseline) กระบวนการบริหารจัดการการตั้งค่าระบบ (การตั้งค่า การสอบทานการตั้งค่า) เป็นต้น
16. กระบวนการสำรองข้อมูล (Back up) ของระบบงานสำคัญ เช่น วิธีการ เทคโนโลยีและรอบระยะเวลาที่ใช้ในการสำรองข้อมูลในแต่ละประเภท การทดสอบความพร้อมของข้อมูลสำรองและความถี่ในการทดสอบ เป็นต้น
17. แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT DRP) รวมทั้งการกำหนดระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) และ ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD) ของระบบงานสำคัญ
18. ผลการประเมินช่องโหว่ (vulnerability testing) และผลการทดสอบเจาะระบบ (penetration testing) ของระบบงานสำคัญ

สำหรับคำขอกรณี A : ให้นำส่งผลการประเมินฯ และผลการทดสอบฯ ก่อนให้บริการ

สำหรับคำขอกรณี B และ C : ให้นำส่งผลการประเมินฯ และผลการทดสอบฯ เมื่อยื่นใบสมัคร