ข้อมูลประกอบการขออนุญาตจัดตั้งธนาคารพาณิชย์ไร้สาขา

หมวด 4 แผนการดำเนินงานด้านระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ของธนาคารพาณิชย์ไร้สาขา

ข้อ	คำถาม	คำตอบ / เอกสารแนบ
1. ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ (IT governance) ของธนาคารพาณิชย์ไร้สาขา		
1.1	**โปรดอธิบายกลยุทธ์และแผนการดำเนินงานด้านเทคโนโลยีสารสนเทศ**ที่สอดคล้องกับรูปแบบและแผนการประกอบธุรกิจของธนาคารพาณิชย์ไร้สาขา รวมถึงอธิบายเหตุผลสนับสนุนอย่างเป็นรูปธรรมว่าผู้ที่จะดำรงตำแหน่งกรรมการและผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์ไร้สาขาจะผลักดันการดำเนินงานด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์ไร้สาขาให้ประสบความสำเร็จได้อย่างไร	โปรดแนบไฟล์ IT01) กลยุทธ์และแผนการดำเนินงานด้านเทคโนโลยีสารสนเทศ
1.2	**โปรดอธิบายการกำกับดูแลการดำเนินงานและการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ**	โปรดแนบไฟล์ IT02) การกำกับดูแลด้านเทคโนโลยีสารสนเทศ
1.3	**โปรดระบุระดับความเสี่ยงที่ยอมรับได้ (IT risk appetite) ของเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ พร้อมทั้งระบุกรอบนโยบายและแนวทางการบริหารจัดการความเสี่ยงดังกล่าว** เพื่อให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยครอบคลุมเป้าหมายการกู้คืนระบบ เป้าหมายการสำรองข้อมูล และเป้าหมายอื่น ๆ ที่เกี่ยวข้อง	โปรดแนบไฟล์ IT03) ระดับความเสี่ยงที่ยอมรับได้ และกรอบนโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2. แนวทางการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและไซเบอร์ (IT/cyber security) และแนวทางการให้บริการที่ยืดหยุ่นและต่อเนื่อง (resiliency/availability)		
2.1	**โปรดระบุ Service Level Agreement (SLA) ในการให้บริการผ่านช่องทางดิจิทัล (mobile banking/internet banking) พร้อมอธิบายแนวทางการออกแบบระบบ (architecture design)** เพื่อให้รองรับแผนการประกอบธุรกิจของธนาคารพาณิชย์ไร้สาขาและเป็นไปตาม SLA ที่กำหนด	โปรดแนบไฟล์ IT04) แผนภาพ IT infrastructure diagram ที่แสดงการเชื่อมโยงแบบ end-to-end ทั้งศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง หรือ cloud computing availability zones รวมทั้งการเชื่อมต่อกับบุคคลภายนอก (third party) เช่น แผนภาพ API และมาตรฐานที่ใช้ในการเชื่อมต่อ

ข้อ	คำถาม	คำตอบ / เอกสารแนบ
		IT05) แผนภาพระบบงานที่ให้บริการ (application architecture diagram) IT06) แผนภาพระบบเครือข่ายสื่อสาร (network diagram) พร้อมแนวทางการรักษาความมั่นคงปลอดภัยเครือข่ายสื่อสาร
2.2	**โปรดระบุแผนการใช้บริการระบบงานหรือบริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ (IT outsourcing)** พร้อมทั้งอธิบายแนวทางคัดเลือกและการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (third party risk management) โดยครอบคลุมการใช้บริการ IT outsourcing การเชื่อมต่อระบบ และการเข้าถึงข้อมูลสำคัญ	โปรดแนบไฟล์ IT07) แผนการใช้บริการจากผู้ให้บริการภายนอกด้านงานเทคโนโลยีสารสนเทศ IT08) แนวทางคัดเลือกและการบริหารจัดการความเสี่ยงจากบุคคลภายนอก
2.3	**โปรดอธิบายแนวทางและเทคโนโลยีในการออกแบบการให้บริการผ่านช่องทางดิจิทัล (mobile banking/internet banking)** เพื่อการรักษาความมั่นคงปลอดภัยและป้องกันภัยทุจริต	โปรดแนบไฟล์ IT09) แนวทางและเทคโนโลยีในการออกแบบการให้บริการผ่านช่องทางดิจิทัล (mobile banking/ internet banking)
2.4	**โปรดอธิบายแนวทางในการเตรียมการทั้งด้านบุคลากร กระบวนการ และเทคโนโลยี ที่รองรับทั้งในเชิงป้องกัน ติดตาม ตอบสนอง และรับมือ**ต่อเหตุการณ์ที่นำมาซึ่งความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจส่งผลกระทบต่อการให้บริการของธนาคารพาณิชย์ไร้สาขา เพื่อให้ระบบมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ รวมทั้งสามารถให้บริการที่ยืดหยุ่นและต่อเนื่อง โดยระบุอย่างน้อย 5 เหตุการณ์	โปรดแนบไฟล์ IT10) แนวทางในการเตรียมการในด้านต่าง ๆ เพื่อให้ระบบมีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ รวมทั้งสามารถให้บริการที่ยืดหยุ่นและต่อเนื่อง
3. การประเมินจากผู้เชี่ยวชาญภายนอกของธนาคารพาณิชย์ไร้สาขา		
3.1	**โปรดส่งรายงานผลการประเมินแผนการดำเนินงานด้านระบบเทคโนโลยีสารสนเทศและความเห็นของผู้เชี่ยวชาญภายนอกด้านเทคโนโลยีสารสนเทศที่มีคุณสมบัติตามที่กำหนดในข้อ 3.2** โดยอย่างน้อยต้องครอบคลุมประเด็นดังต่อไปนี้ (1) ความครอบคลุมและความสอดคล้องของการออกแบบระบบเทคโนโลยีสารสนเทศซึ่งสอดคล้องกับรูปแบบและแผนการประกอบธุรกิจของธนาคารพาณิชย์ไร้สาขา	โปรดกรอกข้อมูลในแบบฟอร์มที่กำหนด IT11) รายงานผลการประเมินแผนการดำเนินงานด้านระบบเทคโนโลยีสารสนเทศและความเห็นของผู้เชี่ยวชาญภายนอกด้านเทคโนโลยีสารสนเทศ (link)

ข้อ	คำถาม	คำตอบ / เอกสารแนบ
	(2) ความเพียงพอเหมาะสมของการกำกับดูแลและการบริหารจัดการด้านเทคโนโลยีสารสนเทศและไซเบอร์ ซึ่งครอบคลุมประเด็นดังต่อไปนี้ (ก) การกำกับดูแล โครงสร้างองค์กร และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (governance) (ข) การให้บริการที่ยืดหยุ่นและต่อเนื่อง (resiliency/availability) (ค) การรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและไซเบอร์ (IT/cyber security) (3) แผนการดำเนินงานด้านระบบเทคโนโลยีสารสนเทศซึ่งมีความสอดคล้องกับหลักเกณฑ์และแนวนโยบายที่ ธปท. กำหนด ได้แก่ ประกาศธนาคารแห่งประเทศไทยว่าด้วยการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน และแนวนโยบายของธนาคารแห่งประเทศไทยว่าด้วยการรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) สำหรับสถาบันการเงิน	
3.2	**โปรดส่งหนังสือรับรองคุณสมบัติพร้อมรายละเอียดของผู้เชี่ยวชาญภายนอกด้านเทคโนโลยีสารสนเทศที่ดำเนินการประเมินและให้ความเห็นตามข้อ 3.1 รวมถึงสมาชิกในทีมงาน**[1] ซึ่งต้องมีคุณสมบัติดังต่อไปนี้ (1) มีใบรับรอง (certificate) โดยอย่างน้อยครอบคลุมเรื่องที่เกี่ยวกับเทคโนโลยีสารสนเทศและไซเบอร์ เช่น CISM CISSP (2) มีความรู้และประสบการณ์ในการประเมินหรือตรวจสอบด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์ไร้สาขาในต่างประเทศ หรือธนาคารพาณิชย์แห่งอื่นในส่วนที่ให้บริการ digital banking เช่น mobile banking หรือ internet banking	โปรดกรอกข้อมูลในแบบฟอร์มที่กำหนด IT12) หนังสือรับรองคุณสมบัติของผู้เชี่ยวชาญภายนอกด้านเทคโนโลยีสารสนเทศและสมาชิกในทีมงาน (link) โปรดแนบไฟล์ IT13) ข้อมูลเกี่ยวกับความรู้และประสบการณ์ในการประเมินหรือตรวจสอบด้านเทคโนโลยีสารสนเทศของธนาคารพาณิชย์ไร้สาขาในต่างประเทศ หรือธนาคารพาณิชย์แห่งอื่นในส่วน

[1] ผู้เชี่ยวชาญภายนอกด้านเทคโนโลยีสารสนเทศต้องมีคุณสมบัติครบทั้งตามข้อ 3.2 (1)-(3) และสมาชิกในทีมงานของผู้เชี่ยวชาญภายนอกด้านเทคโนโลยีสารสนเทศต้องมีคุณสมบัติตามข้อ 3.2 (3) เป็นอย่างน้อย

ข้อ	คำถาม	คำตอบ / เอกสารแนบ
	(3) มีความเป็นอิสระ โดยไม่มีความเกี่ยวข้องกับผู้ขออนุญาตดังนี้ (ก) ไม่มีส่วนเกี่ยวข้องกับการจัดทำแผนการดำเนินงานด้านระบบเทคโนโลยีสารสนเทศของธนาคารพาณิชย์ไร้สาขา[2] (ข) ไม่เป็นผู้ที่เกี่ยวข้องกับผู้ขออนุญาตที่จะเป็นผู้ถือหุ้นรายใหญ่ของธนาคารพาณิชย์ไร้สาขา[3]	ที่ให้บริการ digital banking เช่น mobile banking หรือ internet banking IT14) ใบรับรอง (certificate) โดยอย่างน้อยครอบคลุมเรื่องที่เกี่ยวกับเทคโนโลยีสารสนเทศและไซเบอร์ เช่น CISSP CISM (ทั้งนี้ กรณีผู้เชี่ยวชาญภายนอกด้านเทคโนโลยีสารสนเทศมีทีมงาน โปรดแนบไฟล์เป็นรายบุคคลตามรูปแบบที่ ธปท. กำหนดบนระบบ Microsoft Teams)

[2] ผู้เชี่ยวชาญภายนอกด้านเทคโนโลยีสารสนเทศและทีมงานอาจเป็นผู้ปฏิบัติหน้าที่ในนิติบุคคลเดียวกับผู้ที่ช่วยหรือมีส่วนในการจัดทำแผนการดำเนินงานด้านระบบเทคโนโลยีสารสนเทศของผู้ขออนุญาตได้ แต่ต้องไม่มีส่วนเกี่ยวข้องกับการจัดทำแผนดังกล่าว โดยต้องสามารถแยกผู้เชี่ยวชาญภายนอกด้านเทคโนโลยีสารสนเทศและทีมงานออกจากผู้ที่ช่วยหรือมีส่วนในการจัดทำแผนดังกล่าวได้อย่างชัดเจน

[3] คำว่า “ผู้ที่เกี่ยวข้อง” และ “ผู้ถือหุ้นรายใหญ่” เป็นไปตามนิยามในมาตรา 4 แห่ง พ.ร.บ. ธุรกิจสถาบันการเงิน พ.ศ. 2551