ขอบเขตงาน (Terms of Reference : TOR)

โครงการจ้างที่ปรึกษาเพื่อวิเคราะห์ ประเมินช่องโหว่

และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team

เลขที่ 102-005/69

1. ความเป็นมา/เหตุผลและความจำเป็น

ด้วยศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ มีความประสงค์จะจัดจ้างที่ปรึกษาเพื่อวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team กับระบบสารสนเทศของธนาคาร ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล โดยมีวงเงินงบประมาณ 2,000,000.- บาท (สองล้านบาทถ้วน) เพื่อสร้างความน่าเชื่อถือ ด้านความมั่นคงปลอดภัยระบบสารสนเทศจากลูกค้าธนาคาร ปฏิบัติตามพระราชบัญญัติการรักษาความปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรการและแนวทางในการยกระดับทักษะความรู้ความเชี่ยวชาญ ในการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567 ประกาศธนาคารแห่งประเทศไทย เรื่องกรอบการประเมินความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience Assessment Framework) ประจำปี 2564 และสอดคล้องตามแนวปฏิบัติของธนาคารแห่งประเทศไทย เรื่องการทดสอบเจาะระบบแบบ Intelligence-led Penetration Testing (iPentest)

2. วัตถุประสงค์

ธนาคารอาคารสงเคราะห์ ซึ่งต่อไปนี้เรียกว่า "ธนาคาร" มีความประสงค์จะจัดจ้างที่ปรึกษาเพื่อวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team กับระบบสารสนเทศของธนาคาร ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล ดังนี้

2.1 สร้างความน่าเชื่อถือด้านความมั่นคงปลอดภัยทางไซเบอร์ในบริการให้แก่ลูกค้าธนาคารได้

2.2 เพิ่มประสิทธิภาพในการบริหารจัดการความเสี่ยงและบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีดิจิทัลของธนาคาร

2.3 ได้ระบบที่มีความปลอดภัยที่ดีตามมาตรฐานสากล

2.4 มีกระบวนการในการรวบรวม วิเคราะห์ และเฝ้าระวังข้อมูลเชิงลึกด้านภัยคุกคามทางไซเบอร์

3. คุณสมบัติของผู้เสนอราคา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวเนื่องจากเป็นผู้ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบที่รัฐมนตรีว่าการกระทรวงการคลังกำหนดตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพตามที่จ้าง

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ธนาคาร ณ วันประกาศจัดจ้าง หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกาศจัดจ้างครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น*

3.10 ผู้เสนอราคาต้องมีบุคลากรภายในทีมงานที่จะเข้ามาดำเนินการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล ไม่น้อยกว่า 2 ท่าน ที่มีประกาศนียบัตรที่เกี่ยวข้องด้านความมั่นคงปลอดภัย OSCP หรือ GPEN อย่างใดอย่างหนึ่ง หรือมีทั้ง 2 Certificate

3.11 ผู้เสนอราคาต้องมีประสบการณ์วิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Teaming หรือ iPentest หรือ Penetration Testing ให้กับองค์กรหรือหน่วยงานอย่างน้อย 1 หน่วยงาน และผู้เสนอราคาต้องแจ้งชื่อองค์กรหรือหน่วยงานดังกล่าวนั้น พร้อมสถานที่ตั้ง หมายเลขโทรศัพท์ ผู้ติดต่อ ให้ธนาคารทราบ เพื่อให้สามารถติดต่อได้

3.12 ผู้เสนอราคาต้องมีความรู้ความสามารถด้านเทคนิคและความชำนาญพิเศษเฉพาะด้านและขึ้นทะเบียนที่ปรึกษาของสำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง

3.13 ผู้เสนอราคาจะต้องเก็บรักษาข้อมูลที่เกี่ยวข้องทั้งหมดของธนาคารไว้เป็นความลับ จะไปเผยแพร่ที่อื่นมิได้

4. หลักฐานการเสนอราคา

ผู้เสนอราคาจะต้องเสนอเอกสารหลักฐานยื่นมาพร้อมกับซองใบเสนอราคา โดยแยกไว้นอกซองใบเสนอราคาเป็น 2 ส่วน คือ

4.1 ส่วนที่ 1 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) ในกรณีผู้เสนอราคาเป็นนิติบุคคล

(ก) ห้างหุ้นส่วนสามัญหรือห้างหุ้นส่วนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล บัญชีรายชื่อหุ้นส่วนผู้จัดการ ผู้มีอำนาจควบคุม พร้อมรับรองสำเนาถูกต้อง

(ข) บริษัทจำกัดหรือบริษัทมหาชนจำกัด ให้ยื่นสำเนาหนังสือรับรองการจดทะเบียนนิติบุคคล หนังสือบริคณห์สนธิบัญชีรายชื่อกรรมการผู้จัดการ ผู้มีอำนาจควบคุม และบัญชีผู้ถือหุ้นรายใหญ่ พร้อมรับรองสำเนาถูกต้อง

(2) ในกรณีผู้เสนอราคาเป็นบุคคลธรรมดาหรือคณะบุคคลที่มิใช่นิติบุคคล ให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้นั้น สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน พร้อมทั้งรับรองสำเนาถูกต้อง

(3) ในกรณีผู้เสนอราคาเป็นผู้เสนอราคาร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า สำเนาบัตรประจำตัวประชาชนของผู้ร่วมค้า และในกรณีที่ผู้เข้าร่วมค้าฝ่ายใดเป็นบุคคลธรรมดาที่มิใช่สัญชาติไทย ก็ให้ยื่นสำเนาหนังสือเดินทาง หรือผู้ร่วมค้าฝ่ายใดเป็นนิติบุคคลให้ยื่นเอกสารตามที่ระบุไว้ใน (1)

(4) บัญชีเอกสารส่วนที่ 1 ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

4.2 ส่วนที่ 2 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) แค็ตตาล็อกและหรือแบบรูปรายการละเอียดคุณลักษณะเฉพาะ

(2) หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ผู้เสนอราคามอบอำนาจให้บุคคลอื่นลงนามในใบเสนอราคาแทน

(3) บัญชีเอกสารส่วนที่ 2 ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

5. คุณลักษณะเฉพาะ / รายละเอียดของงานจ้าง

5.1 ผู้เสนอราคาจะต้องเสนอรายละเอียดของวิธีการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team หรือ iPentest หรือ Penetration Testing แก่ธนาคาร

(1) แผนการดำเนินการ วิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team หรือ iPentest หรือ Penetration Testing

(2) รายละเอียดมาตรฐานสากลที่เกี่ยวข้องที่นำมาใช้ในการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงาน

5.2 รายละเอียดของ Proposal ควรประกอบด้วยหัวข้อ ดังต่อไปนี้

(1) ตารางเปรียบเทียบคุณลักษณะเฉพาะของการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากลตามที่ธนาคารกำหนด (ตามภาคผนวก 1)

(2) แผนการดำเนินงานทั้งหมด โดยต้องแบ่งแยกแผนการทำงานแต่ละงาน รายละเอียดงาน ช่วงเวลาและผู้รับผิดชอบในการเข้าปฏิบัติงาน และเบอร์ติดต่อ (ตามภาคผนวก 1)

(3) เอกสารอื่นๆ (ถ้ามี) ที่ผู้เสนอราคาเห็นว่าจะเป็นประโยชน์ต่อการพิจารณาของธนาคาร

6. ระยะเวลาดำเนินการ/ส่งมอบงาน และการตรวจรับ

การดำเนินงานโครงการจ้างที่ปรึกษาเพื่อวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล **มีระยะเวลาดำเนินงานทั้งสิ้น 365 วัน** ตลอดระยะเวลาโครงการ นับถัดจากวันที่ลงนามในสัญญา (**ตามภาคผนวก 1 : ระยะเวลาของโครงการ**)

เมื่อธนาคารได้ตรวจรับมอบการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากลถูกต้องครบถ้วนตามสัญญาจ้างแล้ว ธนาคารจะออกหลักฐานการรับมอบไว้เป็นหนังสือ เพื่อผู้ยื่นข้อเสนอนำมาใช้เป็นหลักฐานประกอบการขอรับเงินค่าจ้างโครงการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล

7. การทำสัญญา

ผู้ได้รับการคัดเลือกจะต้องติดต่อธนาคารเพื่อทำสัญญาภายใน 7 วัน นับถัดจากวันที่ได้รับแจ้ง และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ 5 ของมูลค่าสัญญา และให้ธนาคารยึดถือไว้ในขณะทำสัญญา โดยใช้หลักประกันอย่างหนึ่งอย่างใด ดังต่อไปนี้

7.1 เงินสด

7.2 เช็คหรือดราฟท์ที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือดราฟท์ลงวันที่ที่ใช้เช็คหรือดราฟท์นั้นชำระต่อเจ้าหน้าที่ หรือก่อนหน้านั้นไม่เกิน 3 วัน ทำการ

7.3 หนังสือค้ำประกันของธนาคารภายในประเทศตามตัวอย่างที่คณะกรรมการนโยบายกำหนด โดยอาจเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนดก็ได้

7.4 หนังสือค้ำประกันของบรรษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุโลมให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

7.5 พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้โดยไม่มีดอกเบี้ย ภายใน 15 วัน นับถัดจากวันที่คู่สัญญาพ้นจากข้อผูกพันตามสัญญาแล้ว

ทั้งนี้ หากผู้ได้รับการคัดเลือกไม่ดำเนินการภายในระยะเวลาดังกล่าวข้างต้น ธนาคารสงวนสิทธิ์ที่จะยกเลิกการจ้าง และพิจารณาแจ้งเป็นผู้ทิ้งงาน

8. **เงื่อนไขการชำระเงิน**

โครงการจ้างที่ปรึกษาเพื่อวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล จะแบ่งการชำระออกเป็น 2 งวด โดยมีรายละเอียดดังนี้

งวดที่ 1: ชำระเงินเป็นจำนวน 50% ของมูลค่าโครงการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล เมื่อผู้เสนอราคาได้ทำการส่งมอบงานงวดที่ 1 (**ตามภาคผนวก 1: ระยะเวลาของโครงการ ข้อ 5.1**) ภายในระยะเวลา 180 วัน ให้แก่ธนาคาร และคณะกรรมการตรวจรับ ได้ตรวจสอบคุณสมบัติถูกต้องครบถ้วนตามที่ระบุไว้ในสัญญาจ้าง และกรรมการตรวจรับเห็นว่าถูกต้องตรงตามเงื่อนไขของสัญญาจ้าง

งวดที่ 2: ชำระเงินเป็นจำนวน 50% ของมูลค่าโครงการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล เมื่อผู้เสนอราคาได้ทำการส่งมอบงานงวดที่ 2 (**ตามภาคผนวก 1: ระยะเวลาของโครงการ ข้อ 5.2**) ภายในระยะเวลา 365 วัน ให้แก่ธนาคาร และคณะกรรมการตรวจรับ ได้ตรวจสอบคุณสมบัติถูกต้องครบถ้วนตามที่ระบุไว้ในสัญญาจ้าง และกรรมการตรวจรับเห็นว่าถูกต้องตรงตามเงื่อนไขของสัญญาจ้าง

9. **วงเงินในการจัดหา**

วงเงินงบประมาณ 2,000,000.- บาท (สองล้านบาทถ้วน) (เฉพาะที่ใช้ในการจัดซื้อ จัดจ้างครั้งนี้)

10. **หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ**

ธนาคารจะพิจารณาตัดสินโดยใช้เกณฑ์ราคา

11. **อัตราค่าปรับ**

ค่าปรับตามแบบสัญญาจ้าง ให้คิดเป็นรายวันในอัตราร้อยละ 0.10 ของราคางานจ้าง เศษของวันให้คิดเป็นรายชั่วโมง โดย 1 วัน เท่ากับ 24 ชั่วโมง แต่จะต้องไม่ต่ำกว่าวันละ 100.- บาท

12. **ข้อสงวนสิทธิ์ในการยื่นข้อเสนอและอื่น ๆ**

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกยินยอมให้ธนาคารอาคารสงเคราะห์ ธนาคารแห่งประเทศไทย และ/หรือหน่วยงานอื่นที่กำกับดูแลธนาคารอาคารสงเคราะห์ตามกฎหมาย รวมทั้ง ผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก ที่ได้รับการแต่งตั้งจากธนาคารแห่งประเทศไทย ธนาคารอาคารสงเคราะห์ หรือหน่วยงานอื่นที่กำกับดูแลธนาคารอาคารสงเคราะห์ตามกฎหมาย มีสิทธิเข้าตรวจสอบการดำเนินงาน และ/หรือการควบคุมภายในของผู้ยื่นข้อเสนอที่ได้รับการคัดเลือก และ/หรือบุคคลภายนอกที่เกี่ยวข้องกับผลิตภัณฑ์

13. **การรับประกันความชำรุดบกพร่อง**

ผู้ได้รับการคัดเลือกซึ่งได้ทำสัญญากับธนาคาร จะต้องรับประกันความชำรุดบกพร่องของสิ่งของงานจ้างที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า 120 วัน นับถัดจากวันที่ธนาคารได้รับมอบงาน

14. **หน่วยงานที่รับผิดชอบ**

ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์ (สำนักงานใหญ่) 63 ถนนพระราม 9 ห้วยขวาง กรุงเทพฯ 10310 โทร. 02-2021735

ลงชื่อ.....ประธานกรรมการ
(นายพัลลภ ม่วงไหมทอง)
หัวหน้าส่วนดูแลมาตรฐานความมั่นคงปลอดภัย
กฎข้อบังคับและประเมินความเสี่ยงระบบสารสนเทศ

ลงชื่อ.....กรรมการ
(นายฉนานนท์ ตันสกุล)
ผู้ช่วยหัวหน้าส่วน
ส่วนจัดการระบบเครือข่ายและความมั่นคงฯ

ลงชื่อ.....กรรมการ
(นายเอกณัฏฐ์ อเนกเจริญวณิช)
ผู้ช่วยหัวหน้าส่วน
ส่วนดูแลมาตรฐานความมั่นคงปลอดภัยฯ

ลงชื่อ.....กรรมการ
(นายณัฐรัฐ รุจิวรารัตน์)
พนักงานด้านความมั่นคงปลอดภัยเทคโนโลยี
สารสนเทศอาวุโส

ลงชื่อ.....กรรมการและเลขานุการ
(นายธีระชัย วิสุทธิพันธ์)
ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ

ภาคผนวก 1.
รายละเอียดและคุณลักษณะเฉพาะของ โครงการ วิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team

1. เป้าหมายของโครงการ

1.1 เพื่อให้ธนาคารได้ทราบถึงช่องโหว่ แนวทางในการโจมตี และวิธีการแฝงตัวในระบบงานของธนาคารในระยะยาว ด้วยรูปแบบการทดสอบบุกรุก ในลักษณะ Red Teams หรือ Intelligence-led Penetration Testing (iPentest) หรือ ตามรูปแบบของการทำ Penetration Testing และนำมาวิเคราะห์ Technic, Tactic และ Procedure (TTP) นำมาปรับปรุงการตรวจจับของธนาคาร

1.2 เพื่อให้ธนาคารทราบถึงข้อบกพร่อง และข้อเสนอแนะ ในการปรับปรุงแก้ไข ระบบสารสนเทศของธนาคาร ให้มีประสิทธิภาพและความปลอดภัยที่ดีตามมาตรฐานสากล

1.3 เพื่อให้ธนาคารมีกระบวนการจัดการด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ จะสามารถช่วยทีม IT ของธนาคารเพิ่มประสิทธิภาพในการให้บริการและการดำเนินงาน ลดปัญหาของการเกิดการละเมิดความมั่นคงปลอดภัยสารสนเทศและการเกิด Incident ได้

1.4 เพื่อให้เจ้าหน้าที่ของธนาคาร สามารถนำความรู้ที่ได้จากกระบวนการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team มาปรับใช้ในธนาคารได้

2. ขอบเขตการดำเนินงาน

ขอบเขตของการดำเนินงานโครงการจ้างที่ปรึกษาเพื่อวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล ประกอบด้วย

2.1 การวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team หรือ iPentest หรือ Penetration Testing เป็นการทดสอบระยะยาวตลอดโครงการ โดยมีเป้าหมายการทดสอบ ตามระบบงาน และช่วงระยะเวลาที่ธนาคารกำหนดเท่านั้น โดยจะต้องทดสอบจำนวนทั้งสิ้น 6 ระบบงาน และ 1 สถานการณ์ (1 Objective)

2.2 เป้าหมายการทดสอบจะเป็น เครื่องแม่ข่ายระบบงาน , Mobile Application หรือระบบสารสนเทศที่สำคัญ ตามที่ธนาคารกำหนด ภายในระยะเวลา 365 วัน นับถัดจากวันที่ลงนามในสัญญาและอยู่ในขอบเขตระยะเวลาของโครงการ

2.3 เป้าหมายการดำเนินงานทั้งหมดจะเป็นระบบงานของธนาคารเท่านั้น โดยอุปกรณ์คอมพิวเตอร์หรือ Software ที่นำมาใช้ในการดำเนินงานตามขอบเขตงาน บริษัทผู้รับงานจะต้องเป็นผู้จัดหามาทั้งสิ้น

3. วิธีการดำเนินงาน

3.1 ดำเนินการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานภายใต้สถานการณ์เสมือนจริง (Red Teaming) หรือ iPentest ให้สอดคล้องกับความเสี่ยงไซเบอร์ที่ธนาคารเผชิญหรือรูปแบบภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในปัจจุบัน โดยต้องดำเนินการทดสอบจำนวน 1 สถานการณ์ (1 Objective) ตามที่ธนาคารกำหนด ภายในระยะเวลา 180 วัน นับถัดจากวันที่ลงนามในสัญญา เพื่อให้ธนาคารรับทราบความเสี่ยง หรือช่องโหว่ในสภาพปัจจุบัน ภายใต้ขอบเขตวัตถุประสงค์ดังนี้

(1) ดำเนินการทดสอบบุกรุกระบบสำคัญที่ธนาคารกำหนดจากภายนอกธนาคาร (Access to Internal Network from External Network)

(2) ดำเนินการยึดครองหรือเข้าถึงข้อมูลบนเครื่อง Active Directory และใช้ประโยชน์จากสิ่งที่ตรวจพบ ในการเข้าถึงเป้าหมายสำคัญที่ธนาคารกำหนด (Compromise Active Directory)

(3) ดำเนินการยกระดับสิทธิ์ เป็นผู้ใช้งานสิทธิ์สูงสุดบนเครื่องแม่ข่ายที่เป็นเป้าหมายสำคัญที่ธนาคารกำหนด (Privilege Escalation)

(4) จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก ภาพรวมและผลกระทบ ของช่องโหว่ที่ตรวจพบ พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง โดยวิเคราะห์ผลจะต้องสอดคล้องหรือต้องอ้างอิงตามมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ และส่งมอบให้กับธนาคารเพื่อให้ธนาคารนำข้อมูลช่องโหว่ที่ตรวจพบไปดำเนินการแก้ไขปรับปรุงให้มีความปลอดภัย และรายงานผลให้ธนาคารรับทราบ

(5) ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไขในครั้งแรก เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ

(6) จัดส่งรายงานผลการทดสอบฉบับสมบูรณ์ให้กับธนาคาร

3.2 ดำเนินการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Penetration Testing ของเครื่องแม่ข่ายระบบงาน หรือ Mobile Application หรือระบบสารสนเทศที่สำคัญ ตามที่ธนาคารกำหนด ภายในระยะเวลา 365 วัน (จำนวน 6 ระบบงาน) นับ

ถัดจากวันที่ลงนามในสัญญา เพื่อให้ธนาคารรับทราบความเสี่ยง หรือช่องโหว่ในสภาพปัจจุบัน โดยมีรายละเอียดดังนี้

(1) ดำเนินการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงาน หรือเครื่องแม่ข่ายระบบงาน หรือ Mobile Application หรือ ระบบสารสนเทศที่สำคัญตามที่ธนาคารกำหนด

(2) จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก ภาพรวมและผลกระทบ ของช่องโหว่ที่ตรวจพบ พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง โดยวิเคราะห์ผลจะต้องสอดคล้องหรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ และส่งมอบให้กับธนาคารเพื่อให้ธนาคารนำข้อมูลช่องโหว่ที่ตรวจพบไปดำเนินการแก้ไขปรับปรุงให้มีความปลอดภัย และรายงานผลให้ธนาคารรับทราบ

(3) ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไขในครั้งแรก เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ

(4) จัดส่งรายงานผลการทดสอบฉบับสมบูรณ์ให้กับธนาคาร

4. ระยะเวลาของโครงการ

การดำเนินงานโครงการจ้างที่ปรึกษาเพื่อวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team ให้มีความมั่นคงปลอดภัยตามเกณฑ์มาตรฐานสากล มีระยะเวลาดำเนินงานทั้งสิ้น 365 วัน ตลอดระยะเวลาโครงการ นับถัดจากวันที่ลงนามในสัญญา โดยการดำเนินการจะแบ่งเป็น 2 ครั้ง ดังนี้

4.1 <u>ครั้งที่ 1 : เวลาดำเนินงานทั้งสิ้น 180 วัน (นับถัดจากวันที่ลงนามในสัญญา)</u>

ดำเนินการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานภายใต้สถานการณ์เสมือนจริง (Red Teaming) หรือ iPentest ให้สอดคล้องกับความเสี่ยงไซเบอร์ที่ธนาคารเผชิญหรือรูปแบบภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในปัจจุบัน โดยต้องดำเนินการทดสอบจำนวน 1 สถานการณ์ (1 Objective) ตามที่ธนาคารกำหนด ภายในระยะเวลา 180 วัน นับถัดจากวันที่ลงนามในสัญญา เพื่อให้ธนาคารรับทราบความเสี่ยง หรือช่องโหว่ในสภาพปัจจุบัน ภายใต้ขอบเขตวัตถุประสงค์ดังนี้

(1) ดำเนินการทดสอบบุกรุกระบบสำคัญที่ธนาคารกำหนดจากภายนอกธนาคาร (Access to Internal Network from External Network)

(2) ดำเนินการยึดครองหรือเข้าถึงข้อมูลบนเครื่อง Active Directory และใช้ประโยชน์จากสิ่งที่ตรวจพบ ในการเข้าถึงเป้าหมายสำคัญที่ธนาคารกำหนด (Compromise Active Directory)

(3) ดำเนินการยกระดับสิทธิ์ เป็นผู้ใช้งานสิทธิ์สูงสุดบนเครื่องแม่ข่ายที่เป็นเป้าหมายสำคัญที่ธนาคารกำหนด (Privilege Escalation)

(4) จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก ภาพรวมและผลกระทบ ของช่องโหว่ที่ตรวจพบ พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง โดยวิเคราะห์ผลจะต้องสอดคล้องหรือต้องอ้างอิงตามมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ และส่งมอบให้กับธนาคารเพื่อให้ธนาคารนำข้อมูลช่องโหว่ที่ตรวจพบไปดำเนินการแก้ไขปรับปรุงให้มีความปลอดภัย และรายงานผลให้ธนาคารรับทราบ

(5) ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไขในครั้งแรก เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ

(6) จัดส่งรายงานผลการทดสอบฉบับสมบูรณ์ให้กับธนาคาร

4.2 **<u>ครั้งที่ 2 : เวลาดำเนินงานทั้งสิ้น 365 วัน (นับถัดจากวันที่ลงนามในสัญญา)</u>**

ดำเนินการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Penetration Testing ของเครื่องแม่ข่ายระบบงาน หรือ Mobile Application หรือระบบสารสนเทศที่สำคัญ ตามที่ธนาคารกำหนด ภายในระยะเวลา 365 วัน (จำนวน 6 ระบบงาน) นับถัดจากวันที่ลงนามในสัญญา เพื่อให้ธนาคารรับทราบความเสี่ยง หรือช่องโหว่ในสภาพปัจจุบัน โดยมีรายละเอียดดังนี้

(1) ดำเนินการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงาน หรือเครื่องแม่ข่ายระบบงาน หรือ Mobile Application หรือ ระบบสารสนเทศที่สำคัญ ตามที่ธนาคารกำหนด

(2) จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก ภาพรวมและผลกระทบ ของช่องโหว่ที่ตรวจพบ พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง โดยวิเคราะห์ผลจะต้องสอดคล้องหรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ และส่งมอบให้กับธนาคารเพื่อให้ธนาคารนำข้อมูลช่องโหว่ที่ตรวจพบไปดำเนินการแก้ไขปรับปรุงให้มีความปลอดภัย และรายงานผลให้ธนาคารรับทราบ

(3) ดำเนินการตรวจสอบซ้ำ จากผลการแก้ไขในครั้งแรก เพื่อยืนยันความถูกต้องของการแก้ไข และรายงานผลให้ธนาคารรับทราบ

(4) จัดส่งรายงานผลการทดสอบฉบับสมบูรณ์ให้กับธนาคาร

5. สิ่งที่ต้องส่งมอบ

5.1 ครั้งที่ 1 : ส่งมอบงานภายใน 180 วัน นับถัดจากวันที่ลงนามในสัญญา ตามวิธีการดำเนินงาน ข้อ 3.1

- รายงานผลการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team หรือ iPentest ที่สอดคล้องกับความเสี่ยงไซเบอร์ที่ธนาคารเผชิญหรือในสถานการณ์การโจมตีจริง โดยนำเสนอเส้นทางการโจมตีที่สามารถนำไปสู่การเข้าถึงเป้าหมายสำคัญ พร้อมหลักฐานเชิงปฏิบัติ (Proof of Concept: POC) จำนวน 1 สถานการณ์ (ฉบับภาษาไทย)

5.2 ครั้งที่ 2 : ส่งมอบงานภายใน 365 วัน นับถัดจากวันที่ลงนามในสัญญา ตามวิธีการดำเนินงาน ข้อ 3.2

- รายงานผลการวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Penetration Testing ของเครื่องแม่ข่ายระบบงาน หรือ Mobile Application หรือระบบสารสนเทศที่สำคัญ ตามที่ธนาคารกำหนด จำนวน 6 ระบบ (ฉบับภาษาไทย)

5.3 สิ่งที่ต้องส่งมอบทั้งหมดในโครงการ (ส่งมอบงานภายใน 365 วัน นับถัดจากวันที่ลงนามในสัญญา) ต้องส่งมอบ File เอกสารต่าง ๆ ฉบับสมบูรณ์ ต้องสามารถเปิดและแก้ไขด้วยชุดโปรแกรมจาก Microsoft office ตั้งแต่ Version 2019 ขึ้นไป บรรจุใน USB Drive อย่างละ 1 ชุด (ฉบับภาษาไทย) แนบมาในแฟ้มงาน

ธนาคารอาคารสงเคราะห์ให้ความสำคัญกับการปฏิบัติตามกฎหมายว่าด้วย
การคุ้มครองข้อมูลส่วนบุคคล ธนาคารจึงได้กำหนดนโยบายคุ้มครองข้อมูล
ส่วนบุคคล โดยสามารถศึกษารายละเอียดที่ QR Code นี้

แบบ บก.๐๔

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่ายการจ้างที่ปรึกษา

๑. ชื่อโครงการ จ้างที่ปรึกษาเพื่อวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงานในลักษณะ Red Team

๒. หน่วยงานเจ้าของโครงการ ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่

๓. วงเงินงบประมาณที่ได้รับจัดสรร ๒,๐๐๐,๐๐๐.- บาท (สองล้านบาทถ้วน)

๔. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ ...- 19 ธ.ค. 2568 .....

เป็นเงิน ๑,๙๙๕,๙๗๘.๘๐ บาท (หนึ่งล้านเก้าแสนเก้าหมื่นห้าพันเก้าร้อยเจ็ดสิบแปดบาทแปดสิบสตางค์) (รวมภาษีมูลค่าเพิ่มแล้ว)

๕. ค่าตอบแทนบุคลากร ๑,๙๙๕,๙๗๘.๘๐ บาท (หนึ่งล้านเก้าแสนเก้าหมื่นห้าพันเก้าร้อยเจ็ดสิบแปดบาทแปดสิบสตางค์) (รวมภาษีมูลค่าเพิ่มแล้ว)

๕.๑ ประเภทที่ปรึกษากลุ่มวิชาชีพเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)

๕.๒ คุณสมบัติที่ปรึกษาต้องประกอบธุรกิจด้านการให้คำปรึกษา ต้องเป็นผู้ที่มีความรู้ ความชำนาญและประสบการณ์ด้านมาตรฐานความปลอดภัยสารสนเทศ

๕.๓ จำนวนที่ปรึกษาไม่น้อยกว่า ๒ คน

๖. ค่าวัสดุอุปกรณ์ .....-..... บาท

๗. ค่าใช้จ่ายในการเดินทางไปต่างประเทศ (ถ้ามี) .....-..... บาท

๘. ค่าใช้จ่ายอื่นๆ .....-..... บาท

๙. รายชื่อผู้รับผิดชอบในการกำหนดค่าใช้จ่าย/ดำเนินการ/ขอบเขตดำเนินการ (TOR)

๙.๑ นายพัลลภ ม่วงไหมทอง ประธานกรรมการ

๙.๒ นายฉนานนท์ ตันสกุล กรรมการ

๙.๓ นายเอกณัฏฐ์ อเนกเจริญวณิช กรรมการ

๙.๔ นายณัฐรัฐ รุจิวรารัตน์ กรรมการ

๙.๕ นายธีระชัย วิสุทธิพันธ์ กรรมการและเลขานุการ

๑๐. ที่มาของการกำหนดราคากลาง (ราคาอ้างอิง) .....

๑๐.๑ หนังสือเลขที่ กค ๐๙๑๐/ว ๔๔ ของกระทรวงการคลัง

เรื่อง หลักเกณฑ์ราคากลางการจ้างที่ปรึกษาฉบับใหม่ ลว. ๒๒ สิงหาคม ๒๕๖๗