แบบ บก.๐๔

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่ายการจ้างที่ปรึกษา

๑. ชื่อโครงการ แผนงานจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร

๒. หน่วยงานเจ้าของโครงการ ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่

๓. วงเงินงบประมาณที่ได้รับจัดสรร ๑,๕๐๐,๐๐๐.- บาท (หนึ่งล้านห้าแสนบาทถ้วน)

๔. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ ...- 1 เมษ. 2567

เป็นเงิน ๑,๔๖๗,๐๓๔.๒๐ บาท (หนึ่งล้านสี่แสนหกหมื่นเจ็ดพันสามสิบสี่บาทยี่สิบสตางค์) (รวมภาษีมูลค่าเพิ่มแล้ว)

๕. ค่าตอบแทนบุคลากร ๑,๔๖๗,๐๓๔.๒๐ บาท (หนึ่งล้านสี่แสนหกหมื่นเจ็ดพันสามสิบสี่บาทยี่สิบสตางค์)

๕.๑ ประเภทที่ปรึกษากลุ่มวิชาชีพเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)

๕.๒ คุณสมบัติที่ปรึกษาต้องประกอบธุรกิจด้านการให้คำปรึกษา ต้องเป็นผู้ที่มีความรู้ ความชำนาญและประสบการณ์ด้านมาตรฐานความปลอดภัยสารสนเทศ

๕.๓ จำนวนที่ปรึกษาไม่น้อยกว่า ๔ คน

๖. ค่าวัสดุอุปกรณ์ .....-..... บาท

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

๘. ค่าใช้จ่ายอื่นๆ .....-.....บาท

๙. รายชื่อผู้รับผิดชอบในการกำหนดค่าใช้จ่าย/ดำเนินการ/ขอบเขตดำเนินการ (TOR) (ตามบันทึกข้อความที่ ศม.๐๓๒/๒๕๖๗ ลว.๑๕ ก.พ. ๒๕๖๗)

๙.๑ นายพัลลภ ม่วงไหมทอง	ประธานกรรมการ	
๙.๒ นายธีระชัย วิสุทธิพันธ์	กรรมการ	
๙.๓ นางสาวฐิมาพร โชติวินิจฉัย	กรรมการ	
๙.๔ นายวรวิทย์ วงศ์รัตนวัฒน์	กรรมการ	
๙.๕ นางสาวธนาภรณ์ พูลเลิศ	กรรมการและเลขานุการ	

๑๐. ที่มาของการกำหนดราคากลาง (ราคาอ้างอิง) .....

๑๐.๑ หนังสือเลขที่ กค(กวจ)๐๔๐๕.๓/ว๑๒๐๓ ของกรมบัญชีกลาง เรื่อง แนวทางการจ้างที่ปรึกษา ลว. ๒๗ กันยายน ๒๕๖๕

ขอบเขตงาน (Terms of Reference : TOR)

<u>จัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร ประจำปี 2567</u>

เลขที่ 102-063/67

1. ความเป็นมา/เหตุผลและความจำเป็น

ด้วยธนาคารอาคารสงเคราะห์มีความประสงค์จะดำเนินการจัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร ประจำปี 2567 เพื่อค้นหาและประเมินความเสี่ยงของช่องโหว่ ที่มีอยู่ในระบบสารสนเทศของธนาคาร และหาแนวทางป้องกัน ลดผลกระทบที่อาจจะเกิดขึ้นกับธนาคารได้ โดยมีวงเงินงบประมาณ 1,500,000.00 บาท (หนึ่งล้านห้าแสนบาทถ้วน) ตามแผนงานงบประมาณรายจ่ายประจำปี 2567 และสอดคล้องตามมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 และประกาศธนาคารแห่งประเทศไทย ที่ สนส.21/2562 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงิน

2. วัตถุประสงค์

ธนาคารอาคารสงเคราะห์ ซึ่งต่อไปนี้เรียกว่า "ธนาคาร" มีความประสงค์จะจัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร โดยวัตถุประสงค์ของการสำรวจประเมินช่องโหว่เพื่อช่วยตอบคำถามว่า "ระบบสารสนเทศในธนาคารฯมีความปลอดภัยเพียงใด" หลักการของ การสำรวจประเมินช่องโหว่ มีดังนี้

- สำรวจและวิเคราะห์ช่องโหว่ระบบสารสนเทศ (Vulnerability Assessment)
- ทดสอบการเจาะระบบ (Penetration Test)
- ให้คำปรึกษาในการปิดช่องโหว่ (Hardening)

ในการสำรวจประเมินช่องโหว่ต้องอาศัยผู้เชี่ยวชาญที่มีความชำนาญเฉพาะด้านในการวิเคราะห์ช่องโหว่ที่มีความเสี่ยง รวมถึงเทคโนโลยีที่ก้าวทันต่อช่องโหว่ที่เหล่าบรรดาแฮกเกอร์นั้นพยายามเจาะเข้าสู่ระบบสารสนเทศอยู่ตลอดเวลา ดังนั้นศูนย์ความมั่นคงด้านเทคโนโลยีสารสนเทศ ได้กำหนดแผนงานตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคารฯ ทั้งนี้การดำเนินการตามแผนงานดังกล่าว มีความสอดคล้องกับ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 , พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

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 วันประกาศประกวดราคา หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรม ในการประกวดราคาครั้งนี้*

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น*

3.10 ผู้เสนอราคาต้องมีบุคลากรภายในทีมงานที่จะเข้ามาสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร ไม่น้อยกว่า 2 ท่าน ที่มีประกาศนียบัตรที่เกี่ยวข้องด้านความมั่นคงปลอดภัย OSCP หรือ GPEN อย่างใดอย่างหนึ่ง หรือมีทั้ง 2 Certificate

3.11 ผู้เสนอราคาต้องมีประสบการณ์ทดสอบช่องโหว่ให้กับองค์กรหรือหน่วยงาน ไม่น้อยกว่า 1 หน่วยงาน และผู้เสนอราคาต้องแจ้งชื่อองค์กรหรือหน่วยงานดังกล่าวนั้น พร้อมสถานที่ติดตั้ง หมายเลขโทรศัพท์ ผู้ติดต่อ ให้ธนาคารทราบ เพื่อให้สามารถติดต่อได้

3.12 ผู้เสนอราคาต้องมีความรู้ความสามารถด้านเทคนิคและความชำนาญพิเศษเฉพาะด้านและขึ้นทะเบียนที่ปรึกษาของสำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง

3.13 ผู้เสนอราคาจะต้องเก็บรักษาข้อมูลที่เกี่ยวข้องทั้งหมดของธนาคารไว้เป็นความลับจะไปเผยแพร่ที่อื่นมิได้

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 ผู้เสนอราคาจะต้องเสนอรูปแบบการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร โดยต้องนำเสนอมาตรฐานที่ใช้ในการดำเนินการทดสอบ เช่น

- มีกระบวนการขั้นตอนในการทดสอบ
- มีมาตรฐานอ้างอิงในการทดสอบ เช่น SANS หรือ OSCP หรือมาตรฐานสากลอื่นๆ ที่เกี่ยวข้อง

5.2 ผู้เสนอราคาต้องเสนอ Proposal โดยมีรายละเอียดของ Proposal ประกอบด้วยหัวข้อ ดังต่อไปนี้

- ตารางเปรียบเทียบคุณลักษณะเฉพาะของการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร ที่เสนอกับคุณลักษณะเฉพาะที่ธนาคารกำหนด (ตามภาคผนวก 1)
- แผนการดำเนินงานทั้งหมด โดยต้องแบ่งแยกแผนการทำงานแต่ละงาน รายละเอียดงาน ช่วงเวลาและผู้รับผิดชอบในการเข้าปฏิบัติงาน และเบอร์ติดต่อ (ตามภาคผนวก 1)
- เอกสารอื่นๆ (ถ้ามี) ที่ผู้เสนอราคาเห็นว่าจะเป็นประโยชน์ต่อการพิจารณาของธนาคาร

6. **ระยะเวลาดำเนินการ/ส่งมอบงาน และการตรวจรับ**

ระยะเวลาดำเนินการ/ส่งมอบงานทั้งสิ้น 220 วัน นับถัดจากวันลงนามในสัญญา (ตามภาคผนวก 1) โดยการส่งมอบงานจะแบ่งเป็น 2 งวดผู้เสนอราคาจะต้องส่งมอบ ดังนี้

<u>งวดที่ 1: ส่งมอบงานภายใน 70 วัน</u>

- เอกสารผลการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคารครั้งที่ 1 ที่เป็นเอกสารกระดาษและ Soft Copy จำนวน 1 ชุด โดยเอกสารทุกชุดต้องรวมเล่มมาในแฟ้ม และทำ Index ของเอกสาร **(ตามภาคผนวก 1: ขอบเขตการดำเนินงานข้อ** 3.1 -3.4)

<u>งวดที่ 2 : ส่งมอบงานภายใน 220 วัน</u>

- เอกสารผลการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร ครั้งที่ 2 ที่เป็นเอกสารกระดาษและ Soft Copy จำนวน 1 ชุด โดยเอกสารทุกชุดต้องรวมเล่มมาในแฟ้ม และทำ Index ของเอกสาร **(ตามภาคผนวก 1: ขอบเขตการดำเนินงานข้อ** 3.1 -3.4)
- สิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่มี Lab ให้ลงมือทำเชิงปฏิบัติได้จริงบนเครื่องจำลอง โดย Platform ดังกล่าวต้องมี Lab ที่ครอบคลุมตามมาตรฐาน OWASP top

10 ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ Enterprise จำนวน 3 ผู้ใช้งาน (**ตามภาคผนวก 1: ขอบเขตการดำเนินงานข้อ 3.5**)

- สิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่สามารถทดสอบโจมตีด้วยช่องโหว่ต่างๆ ได้จริง โดยสามารถทดสอบโจมตีได้หลากหลายรูปแบบและไม่ผิดกฎหมาย รวมถึงต้องมีเอกสาร Official Write-Up ให้ธนาคารใช้เป็นแนวทางในการทดสอบโจมตีได้ ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ VIP Plus จำนวน 3 ผู้ใช้งาน (**ตามภาคผนวก 1: ขอบเขตการดำเนินงานข้อ 3.6**)
- เครื่องคอมพิวเตอร์แบบพกพา (Notebook) รวมถึง License ของระบบปฏิบัติการ โดยธนาคารไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม และดำเนินการติดตั้ง Software License แบบ 1 ปี ของเครื่องมือที่ใช้ในการทดสอบบุกรุกระบบ (Burp Suite Professional) จำนวน 1 License เพื่อให้ธนาคารสามารถในการศึกษา Cyber Security Platform และใช้สอบทานผลการตรวจสอบช่องโหว่ได้ภายหลัง (**ตามภาคผนวก 1: ขอบเขตการดำเนินงานข้อ 3.7**)

เมื่อธนาคารได้รับมอบผลการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร ถูกต้องครบถ้วนตามสัญญาจ้าง แล้ว ธนาคารจะออกหลักฐานการรับมอบไว้เป็นหนังสือเพื่อผู้เสนอราคานำมาใช้เป็นหลักฐานประกอบการขอรับเงินค่าจ้าง

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***

โครงการจัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร จะแบ่งการชำระออกเป็น 2 งวด โดยมีรายละเอียดดังนี้

งวดที่ 1: ชำระเงินเป็นจำนวน 50% ของมูลค่าโครงการจัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร เป็นจำนวนเงินทั้งสิ้น (.....) บาท (.....) (รวมภาษีมูลค่าเพิ่มแล้ว) เมื่อผู้เสนอราคาได้ทำการส่งมอบงานงวดที่ 1 (**ตามภาคผนวก 1: ขอบเขตการดำเนินงานข้อ** 3.1 – 3.4) ภายในระยะเวลา 70 วัน ให้แก่ธนาคาร และคณะกรรมการตรวจรับ ได้ตรวจสอบคุณสมบัติถูกต้องครบถ้วนตามที่ระบุไว้ในสัญญาจ้าง และกรรมการตรวจรับเห็นว่าถูกต้องตรงตามเงื่อนไขของสัญญาจ้าง

งวดที่ 2: ชำระเงินเป็นจำนวน 50% ของมูลค่าจัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร เป็นจำนวนเงินทั้งสิ้น (.....) บาท (.....) (รวมภาษีมูลค่าเพิ่มแล้ว) เมื่อผู้เสนอราคาได้ทำการส่งมอบงานงวดที่ 2 (**ตามภาคผนวก 1: ขอบเขตการดำเนินงานข้อ** 3.1 – 3.7) ภายในระยะเวลา 220 วัน ให้แก่ธนาคาร และคณะกรรมการตรวจรับ ได้ตรวจสอบคุณสมบัติถูกต้องครบถ้วนตามที่ระบุไว้ในสัญญาจ้าง และกรรมการตรวจรับเห็นว่าถูกต้องตรงตามเงื่อนไขของสัญญาจ้าง

การชำระเงิน ดังกล่าวข้างต้น ต้องรับจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การรับจ่ายเงินแต่ละครั้งซึ่งมีมูลค่าไม่เกิน 30,000 บาท อาจรับจ่ายเป็นเงินสดได้

9. **วงเงินในการจัดหา**

วงเงินงบประมาณ 1,500,000.00 บาท (หนึ่งล้านห้าแสนบาทถ้วน)

10. **หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ**

ธนาคารจะพิจารณาตัดสินโดยใช้เกณฑ์ราคา

11. **อัตราค่าปรับ***

ค่าปรับตามแบบสัญญาจ้าง ให้คิดเป็นรายวันในอัตราร้อยละ 0.10 ของราคางานจ้าง แต่จะต้องไม่ต่ำกว่าวันละ 100.- บาท

12. **การรับประกันความชำรุดบกพร่อง**

ผู้ได้รับการคัดเลือกซึ่งได้ทำสัญญากับธนาคาร จะต้องรับประกันความชำรุดบกพร่องของสิ่งของงานจ้างที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า 60 วัน นับถัดจากวันที่ธนาคารได้รับมอบงาน

13. **หน่วยงานที่รับผิดชอบ**

ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ธนาคารอาคารสงเคราะห์ (สำนักงานใหญ่) 63 ถนนพระราม 9 ห้วยขวาง กรุงเทพฯ 10310 โทร. 022021735

นายพัลลภ ม่วงไหมทอง	นายธีระชัย วิสุทธิพันธ์
หัวหน้าส่วนดูแลมาตรฐานความมั่นคงปลอดภัย กฎข้อบังคับและประเมินความเสี่ยงระบบสารสนเทศ	ผู้ช่วยหัวหน้าส่วนฯ
ประธานกรรมการ	กรรมการ
นางสาวฐิมาพร โชติวินิจฉัย	นายวรวิทย์ วงศ์รัตนวัฒน์
พนักงานคอมพิวเตอร์อาวุโส	พนักงานคอมพิวเตอร์อาวุโส
กรรมการ	กรรมการ

นางสาวธนาภรณ์ พูลเลิศ
พนักงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
กรรมการและเลขานุการ

ผนวก 1.

รายละเอียดและคุณลักษณะเฉพาะของการจัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร

---

1. วัตถุประสงค์ของโครงการ

1) เพื่อทำการตรวจสอบและค้นหาจุดอ่อนที่สำคัญของระบบการรักษาความมั่นคงปลอดภัยของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM, ระบบที่ให้บริการ Electronic Channel และระบบงานสนับสนุนระบบสารสนเทศของธนาคารที่ธนาคารกำหนด
2) เพื่อให้ธนาคารทราบถึงข้อบกพร่อง และข้อเสนอแนะ ในการปรับปรุงแก้ไขระบบให้มีประสิทธิภาพและความปลอดภัยที่ดีตามมาตรฐานสากล
3) เพื่อเพิ่มประสิทธิภาพการทำงาน ให้ธนาคารมีแนวทางการปฏิบัติงานตามเกณฑ์มาตรฐานสากลเป็นที่ยอมรับจากสถาบันที่มีหน้าที่กำกับและตรวจสอบธนาคาร ตลอดจนพัฒนาบุคลากรให้ได้รับความรู้ความเข้าใจเกี่ยวกับการปฏิบัติงาน และการป้องกันระบบงานสารสนเทศ และสามารถนำความรู้ที่ได้รับไปประยุกต์ใช้ในการปฏิบัติและการป้องกันความปลอดภัยระบบสารสนเทศ และระบบเครือข่ายสื่อสารต่อไป

2. เป้าหมายของโครงการ

1) เพื่อให้ธนาคารทราบข้อมูลจุดอ่อนที่สำคัญของระบบการรักษาความมั่นคงปลอดภัยของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM, ระบบที่ให้บริการ Electronic Channel และระบบงานสนับสนุนระบบสารสนเทศของธนาคารที่ธนาคารกำหนด
2) เพื่อให้ธนาคารทราบถึงข้อบกพร่อง และข้อเสนอแนะ ในการปรับปรุงแก้ไขระบบให้มีประสิทธิภาพและความปลอดภัยที่ดีตามมาตรฐานสากล
3) ธนาคารมีกระบวนการจัดการด้านเทคโนโลยีสารนเทศที่มีประสิทธิภาพ จะสามารถช่วยทีม IT ของธนาคารเพิ่มประสิทธิภาพในการให้บริการและการดำเนินงาน ลดปัญหาของการเกิดการละเมิดความมั่นคงปลอดภัยสารสนเทศและการเกิด Incident ได้
4) เพิ่มพูนความรู้ด้านเทคนิคการรักษาความมั่นคงปลอดภัยสารสนเทศ

3. ขอบเขตการดำเนินงาน

ขอบเขตของการทำ Vulnerability Assessment และ Penetration Test ของโครงการ จะทำการทดสอบเป้าหมาย เป็นจำนวน 300 ไอพี ตามที่ธนาคารกำหนด ประกอบด้วยงานดังต่อไปนี้

3.1 ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด โดยจะต้องดำเนินการดังต่อไปนี้

- ใช้เครื่องมือตรวจสอบช่องโหว่ (Scanning Tool) จำนวน 1 ชนิด ซึ่งต้องเป็นเครื่องมือที่เป็น Commercial มีการใช้งานแพร่หลาย เช่น Nessus หรือ Nexpose
- จัดทำผลสรุปภาพรวมการทดสอบสำหรับผู้บริหาร (Executive Summary) รวมถึงเสนอแผนในการแก้ไขระยะสั้น และระยะยาว
- วิเคราะห์ผลสำหรับผู้ดูแลระบบ โดยมีรายละเอียดดังนี้
  - จัดลำดับความเสี่ยงที่ต้องเร่งดำเนินการแก้ไข แยกตามประเภทอุปกรณ์เครือข่าย/เครื่องแม่ข่าย และเรียงตามลำดับหมายเลขไอพี ที่ตรวจพบความเสี่ยงมากที่สุดไปน้อยที่สุด
  - รายละเอียดช่องโหว่ที่ตรวจพบในแต่ละอุปกรณ์เครือข่าย/เครื่องแม่ข่าย พร้อมทั้งให้คำแนะนำการปรับปรุงระบบหรือการแก้ไขช่องโหว่ที่ตรวจพบหรือแนวทางในการลดความเสี่ยงที่เกิดขึ้น
  - รายละเอียดช่องโหว่ที่ตรวจพบ แบ่งตามประเภทช่องโหว่และระดับความรุนแรง (Critical, High) โดยอธิบายรายละเอียดช่องโหว่, ระดับความรุนแรง, CVSS Score Detail, แนวทางการแก้ไข และอุปกรณ์เครือข่าย/เครื่องแม่ข่ายที่ได้รับผลกระทบ

3.2 ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด โดยจะต้องดำเนินการดังต่อไปนี้

- ใช้เครื่องมือตรวจสอบช่องโหว่ (Scanning Tool) จำนวน 1 ชนิด ซึ่งต้องเป็นเครื่องมือที่เป็น Commercial มีการใช้งานแพร่หลาย เช่น Nessus หรือ Nexpose
- จัดทำผลสรุปภาพรวมการทดสอบสำหรับผู้บริหาร (Executive Summary) รวมถึงเสนอแผนในการแก้ไขระยะสั้น และระยะยาว
- วิเคราะห์ผลสำหรับผู้ดูแลระบบ โดยมีรายละเอียดดังนี้
  - จัดลำดับความเสี่ยงที่ต้องเร่งดำเนินการแก้ไข แยกตามประเภทอุปกรณ์เครือข่าย/เครื่องแม่ข่าย และเรียงตามลำดับหมายเลขไอพี ที่ตรวจพบความเสี่ยงมากที่สุดไปน้อยที่สุด
  - รายละเอียดช่องโหว่ที่ตรวจพบในแต่ละอุปกรณ์เครือข่าย/เครื่องแม่ข่าย พร้อมทั้งให้คำแนะนำการปรับปรุงระบบหรือการแก้ไขช่องโหว่ที่ตรวจพบหรือแนวทางในการลดความเสี่ยงที่เกิดขึ้น
  - รายละเอียดช่องโหว่ที่ตรวจพบ แบ่งตามประเภทช่องโหว่และระดับความรุนแรง (Critical, High) โดยอธิบายรายละเอียดช่องโหว่, ระดับความรุนแรง, CVSS Score Detail, แนวทางการแก้ไข และอุปกรณ์เครือข่าย/เครื่องแม่ข่ายที่ได้รับผลกระทบ

3.3 ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด โดยจะต้องดำเนินการดังต่อไปนี้

- ทดสอบเจาะระบบจากภายนอกแบบ Black-Box Penetration Testing และทำการทดสอบเจาะระบบจากภายในธนาคารแบบ Gray-Box Penetration Testing การดำเนินงานจะต้องครอบคลุมการทดสอบหาเป้าหมายทั้งแบบทางตรงและทางอ้อม
- จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก เปรียบเทียบภาพรวมและผลกระทบของช่องโหว่ที่ตรวจพบ จากการทำ Black-Box และ Gray-Box Penetration Testing พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง แยกตามประเภทของอุปกรณ์เครือข่าย และเครื่องแม่

ข่าย โดยวิเคราะห์ผลจะต้องสอดคล้องหรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ

3.4 ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด โดยจะต้องดำเนินการดังต่อไปนี้

- ทดสอบเจาะระบบจากภายนอกแบบ Black-Box Penetration Testing และทำการทดสอบเจาะระบบจากภายในธนาคารแบบ Gray-Box Penetration Testing การดำเนินงานจะต้องครอบคลุมการทดสอบหาเป้าหมายทั้งแบบทางตรงและทางอ้อม
- จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก เปรียบเทียบภาพรวมและผลกระทบของช่องโหว่ที่ตรวจพบ จากการทำ Black-Box และ Gray-Box Penetration Testing พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง แยกตามประเภทของอุปกรณ์เครือข่าย และเครื่องแม่ข่าย โดยวิเคราะห์ผลจะต้องสอดคล้องหรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ ณ วันลงนามในสัญญา

3.5 ดำเนินการจัดหาสิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่มี Lab ให้ลงมือทำเชิงปฏิบัติได้จริงบนเครื่องจำลอง โดย Platform ดังกล่าวต้องมี Lab ที่ครอบคลุมตามมาตรฐาน OWASP top 10 ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ Enterprise จำนวน 3 ผู้ใช้งาน

3.6 ดำเนินการจัดหาสิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่สามารถทดสอบโจมตีด้วยช่องโหว่ต่างๆ ได้จริง โดยสามารถทดสอบโจมตีได้หลากหลายรูปแบบและไม่ผิดกฎหมาย รวมถึงต้องมีเอกสาร Official Write-Up ให้ธนาคารใช้เป็นแนวทางในการทดสอบโจมตีได้ ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ VIP Plus จำนวน 3 ผู้ใช้งาน

3.7 ดำเนินการส่งมอบเครื่องคอมพิวเตอร์แบบพกพา (Notebook) รวมถึง License ของระบบปฏิบัติการ โดยธนาคารไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม และดำเนินการติดตั้ง Software License แบบ 1 ปี ของเครื่องมือที่ใช้ในการทดสอบบุกรุกระบบ (Burp Suite Professional) จำนวน 1 License เพื่อให้ธนาคารสามารถในการศึกษา Cyber Security Platform และใช้สอบทานผลการตรวจสอบช่องโหว่ได้ภายหลัง โดยมีคุณสมบัติขั้นพื้นฐาน ดังนี้

- CPU Core i-7 หรือสูงกว่า

- Memory 16 GB DDR4
- Hard disk SSD 500 GB หรือสูงกว่า
- ระบบปฏิบัติการ Windows 11 Pro (64 bit)

4. วิธีการดำเนินงาน

4.1 จัดทำโครงสร้างการบริหารโครงการ พร้อมแต่งตั้งผู้บริหารโครงการ (Project Manager) จำนวน 1 คน โดยต้องมีความชำนาญและมีประสบการณ์ในการควบคุมและบริหารโครงการด้าน IT เพื่อรับผิดชอบดำเนินงานตามข้อกำหนด และประสานการดำเนินงานกับธนาคารเพื่อให้โครงการสำเร็จได้ด้วยดี

4.2 จัดทำแผนงานรายละเอียดโครงสร้างของทีมงาน ตำแหน่ง คุณสมบัติ/ประกาศนียบัตร หน้าที่ความรับผิดชอบปฏิบัติงานในแต่ละช่วงเวลา หรือแต่ละขั้นตอนของกิจกรรมของแต่ละคนที่จะเข้ามาปฏิบัติงานให้แก่ธนาคาร

4.3 เป้าหมายการดำเนินงานทั้งหมดจะเป็นระบบงานของธนาคารเท่านั้น โดยอุปกรณ์คอมพิวเตอร์หรือ Software ที่นำมาใช้ในการดำเนินงานตรวจสอบช่องโหว่ และทดสอบบุกรุกระบบตามขอบเขตงาน ที่ปรึกษาจะต้องเป็นผู้จัดหามาทั้งสิ้น

4.4 ในการดำเนินงานโครงการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร สรุปได้ดังนี้

1) ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด **(ตามขอบเขตการดำเนินงานข้อ** 3.1)

2) ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด **(ตามขอบเขตการดำเนินงานข้อ** 3.2)

3) ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย

(Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด **(ตามขอบเขตการดำเนินงานข้อ** 3.3)

4) ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด **(ตามขอบเขตการดำเนินงานข้อ** 3.4)

5) ดำเนินการจัดหาสิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่มี Lab ให้ลงมือทำเชิงปฏิบัติได้จริงบนเครื่องจำลอง โดย Platform ดังกล่าวต้องมี Lab ที่ครอบคลุมตามมาตรฐาน OWASP top 10 ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ Enterprise จำนวน 3 ผู้ใช้งาน **(ตามขอบเขตการดำเนินงานข้อ** 3.5)

6) ดำเนินการจัดหาสิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่สามารถทดสอบโจมตีด้วยช่องโหว่ต่างๆ ได้จริง โดยสามารถทดสอบโจมตีได้หลากหลายรูปแบบและไม่ผิดกฎหมาย รวมถึงต้องมีเอกสาร Official Write-Up ให้ธนาคารใช้เป็นแนวทางในการทดสอบโจมตีได้ ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ VIP Plus จำนวน 2 ผู้ใช้งาน **(ตามขอบเขตการดำเนินงานข้อ** 3.6)

7) ดำเนินการส่งมอบเครื่องคอมพิวเตอร์แบบพกพา (Notebook) รวมถึง License ของระบบปฏิบัติการ Windows 11 Pro ที่จำเป็นต้องใช้งาน โดยธนาคารไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม และดำเนินการติดตั้ง Software License แบบ 1 ปี ของเครื่องมือที่ใช้ในการทดสอบบุกรุกระบบ (Burp Suite Professional) จำนวน 1 License เพื่อให้ธนาคารสามารถใช้งานสอบทานตรวจสอบผลการดำเนินงานได้ภายหลัง **(ตามขอบเขตการดำเนินงานข้อ** 3.7)

5. ระยะเวลาของโครงการ

งานจัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคารนี้ มีระยะเวลาดำเนินงานทั้งสิ้น 220 วัน ตลอดระยะเวลาโครงการ นับถัดจากวันที่ลงนามในสัญญา โดยการดำเนินการจะแบ่งเป็น 2 ครั้ง ดังนี้

- ครั้งที่ 1 : เวลาดำเนินงานทั้งสิ้น 70 วัน นับถัดจากวันที่ลงนามในสัญญา
- ครั้งที่ 2 : เวลาดำเนินงานทั้งสิ้น 220 วัน นับถัดจากวันที่ลงนามในสัญญา

ประกอบด้วยขั้นตอนการดำเนินงานหลักๆ คือ

5.1 ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด **(ตามขอบเขตการดำเนินงานข้อ 3.1)**

- ครั้งที่ 1 : ส่งมอบงานภายใน 50 วัน นับถัดจากวันที่ลงนามในสัญญา
- ครั้งที่ 2 : ส่งมอบงานภายใน 190 วัน นับถัดจากวันที่ลงนามในสัญญา

5.2 ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด **(ตามขอบเขตการดำเนินงานข้อ 3.2)**

- ครั้งที่ 1 : ส่งมอบงานภายใน 50 วัน นับถัดจากวันที่ลงนามในสัญญา
- ครั้งที่ 2 : ส่งมอบงานภายใน 190 วัน นับถัดจากวันที่ลงนามในสัญญา

5.3 ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด **(ตามขอบเขตการดำเนินงานข้อ 3.3)**

- ครั้งที่ 1 : ส่งมอบงานภายใน 70 วัน นับถัดจากวันที่ลงนามในสัญญา
- ครั้งที่ 2 : ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

5.4 ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด **(ตามขอบเขตการดำเนินงานข้อ 3.4)**

- ครั้งที่ 1 : ส่งมอบงานภายใน 70 วัน นับถัดจากวันที่ลงนามในสัญญา
- ครั้งที่ 2 : ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

5.5 ดำเนินการจัดหาสิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่มี Lab ให้ลงมือทำเชิงปฏิบัติได้จริงบนเครื่องจำลอง โดย Platform ดังกล่าวต้องมี Lab ที่ครอบคลุมตามมาตรฐาน OWASP top 10 ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ Enterprise จำนวน 3 ผู้ใช้งาน **(ตามขอบเขตการดำเนินงานข้อ** 3.5)

- ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

5.6 ดำเนินการจัดหาสิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่สามารถทดสอบโจมตีด้วยช่องโหว่ต่างๆ ได้จริง โดยสามารถทดสอบโจมตีได้หลากหลายรูปแบบและไม่ผิดกฎหมาย รวมถึงต้องมีเอกสาร Official Write-Up ให้ธนาคารใช้เป็นแนวทางในการทดสอบโจมตีได้ ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ VIP Plus จำนวน 3 ผู้ใช้งาน **(ตามขอบเขตการดำเนินงานข้อ** 3.6)

- ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

5.7 ดำเนินการส่งมอบเครื่องคอมพิวเตอร์แบบพกพา (Notebook) รวมถึง License ของระบบปฏิบัติการ โดยธนาคารไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม และดำเนินการติดตั้ง Software License แบบ 1 ปี ของเครื่องมือที่ใช้ในการทดสอบบุกรุกระบบ (Burp Suite Professional) จำนวน 1 License เพื่อให้ธนาคารสามารถในการศึกษา Cyber Security Platform และใช้สอบทานผลการตรวจสอบช่องโหว่ได้ภายหลัง **(ตามขอบเขตการดำเนินงานข้อ** 3.7)

- ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

5.8 จัดทำและส่งมอบงาน ฉบับสมบูรณ์ **(ตามขอบเขตการดำเนินงานข้อ** 3.1 -3.7) (ระยะเวลาดำเนินงาน 220 วัน นับถัดจากวันที่ลงนามในสัญญา)

6. งานที่ต้องส่งมอบ

สิ่งที่ต้องส่งมอบในการดำเนินงานตามข้อ 3.1

- ครั้งที่ 1 : ส่งมอบงานภายใน 50 วัน นับถัดจากวันที่ลงนามในสัญญา
- ครั้งที่ 2 : ส่งมอบงานภายใน 190 วัน นับถัดจากวันที่ลงนามในสัญญา

1. รายงานผลการดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด (ฉบับภาษาไทย)

สิ่งที่ต้องส่งมอบในการดำเนินงานตามข้อ 3.2

- ครั้งที่ 1 : ส่งมอบงานภายใน 50 วัน นับถัดจากวันที่ลงนามในสัญญา
- ครั้งที่ 2 : ส่งมอบงานภายใน 190 วัน นับถัดจากวันที่ลงนามในสัญญา

1. รายงานผลการดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด (ฉบับภาษาไทย)

สิ่งที่ต้องส่งมอบในการดำเนินงานตามข้อ 3.3

- ครั้งที่ 1 : ส่งมอบงานภายใน 70 วัน นับถัดจากวันที่ลงนามในสัญญา
- ครั้งที่ 2 : ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

1. รายงานผลการวิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด (ฉบับภาษาไทย)

สิ่งที่ต้องส่งมอบในการดำเนินงานตามข้อ 3.4

- ครั้งที่ 1 : ส่งมอบงานภายใน 70 วัน นับถัดจากวันที่ลงนามในสัญญา
- ครั้งที่ 2 : ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

1. รายงานผลการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด (ฉบับภาษาไทย)

สิ่งที่ต้องส่งมอบในการดำเนินงานตามข้อ 3.5

- ครั้งที่ 1 : ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

1. เอกสารแสดงสิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่มี Lab ให้ลงมือทำเชิงปฏิบัติได้จริงบนเครื่องจำลอง โดย Platform ดังกล่าวต้องมี Lab ที่ครอบคลุมตามมาตรฐาน OWASP top 10 ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ Enterprise จำนวน 3 ผู้ใช้งาน

สิ่งที่ต้องส่งมอบในการดำเนินงานตามข้อ 3.6 (ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา)

1. เอกสารแสดงสิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่สามารถทดสอบโจมตีด้วยช่องโหว่ต่างๆ ได้จริง โดยสามารถทดสอบโจมตีได้หลากหลายรูปแบบและไม่ผิดกฎหมาย รวมถึงต้องมีเอกสาร Official Write-Up ให้ธนาคารใช้เป็นแนวทางในการทดสอบโจมตีได้ ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ VIP Plus จำนวน 3 ผู้ใช้งาน

สิ่งที่ต้องส่งมอบในการดำเนินงานตามข้อ 3.7 (ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา)

1. เอกสารแสดง Software License แบบ 1 ปี ของเครื่องมือที่ใช้ในการทดสอบบุกรุกระบบ (Burp Suite Professional) จำนวน 1 License เพื่อให้ธนาคารสามารถใช้งานสอบทานตรวจสอบผลการดำเนินงานได้ภายหลัง
2. เอกสารแสดง Software License ของระบบปฏิบัติการ Windows 11 Pro ที่ติดตั้งในเครื่องคอมพิวเตอร์แบบพกพา (Notebook) ที่ส่งมอบมาในโครงการ
3. เครื่องคอมพิวเตอร์แบบพกพา (Notebook) เพื่อให้ธนาคารสามารถในการศึกษา Cyber Security Platform และใช้สอบทานผลการตรวจสอบช่องโหว่ได้ภายหลัง ที่มีคุณสมบัติขั้นต่ำดังนี้
    - CPU Core i-7 หรือสูงกว่า
    - Memory 16 GB DDR4
    - Hard disk SSD 500 GB หรือสูงกว่า
    - ระบบปฏิบัติการ Windows 11 Pro (64 bit)

สิ่งที่ต้องส่งมอบในการดำเนินงานตามข้อ 3.1- ข้อ 3.7 (ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา)

1. เอกสารต่างๆ ฉบับสมบูรณ์ ที่ต้องส่งมอบตามข้อ 3.1 – ข้อ 3.7 ต้องถูกรวบรวมและส่งมอบ ในลักษณะของแฟ้มงาน 1 แฟ้ม และจัดทำ Index ของเอกสาร แบ่งแยกเอกสารแต่ละชุดอย่างชัดเจน
2. File เอกสารต่าง ๆ ฉบับสมบูรณ์ ที่ส่งมอบตามข้อ 3.1 – ข้อ 3.7 ต้องสามารถเปิดและแก้ไขด้วยชุดโปรแกรมจาก Microsoft office ตั้งแต่ Version 2016 ขึ้นไป บรรจุใน USB Drive อย่างละ 1 ชุด (ฉบับภาษาไทย) แนบมาในแฟ้มงาน

ธนาคารอาคารสงเคราะห์ให้ความสำคัญกับการปฏิบัติตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ธนาคารจึงได้กำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคล โดยสามารถศึกษารายละเอียดที่ QR Code นี้