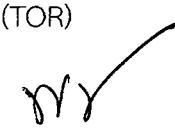
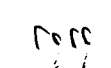
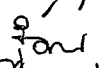
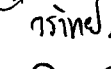
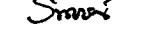


ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่ายการจ้างที่ปรึกษา

๑. ชื่อโครงการ แผนงานจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร ประจำปี ๒๕๖๘
๒. หน่วยงานเจ้าของโครงการ ศูนย์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
ธนาคารอาคารสงเคราะห์ สำนักงานใหญ่
๓. วงเงินงบประมาณที่ได้รับจัดสรร ๑,๕๐๐,๐๐๐.- บาท (หนึ่งล้านห้าแสนบาทถ้วน)
๔. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ณ วันที่ **10 มี.ค. 2568**
เป็นเงิน ๑,๔๙๗,๕๙๗.๔๑ บาท (หนึ่งล้านสี่แสนเก้าหมื่นเจ็ดพันห้าร้อยเก้าสิบเจ็ดบาทสี่สิบเอ็ดสตางค์)
(รวมภาษีมูลค่าเพิ่มแล้ว)
๕. ค่าตอบแทนบุคลากร ๑,๔๙๗,๕๙๗.๔๑ บาท (หนึ่งล้านสี่แสนเก้าหมื่นเจ็ดพันห้าร้อยเก้าสิบเจ็ดบาทสี่สิบเอ็ดสตางค์)
 - ๕.๑ ประเภทที่ปรึกษากลุ่มวิชาชีพเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)
 - ๕.๒ คุณสมบัติที่ปรึกษาต้องประกอบธุรกิจด้านการให้คำปรึกษา ต้องเป็นผู้ที่มีความรู้ ความชำนาญ และประสบการณ์ด้านมาตรฐานความปลอดภัยสารสนเทศ
 - ๕.๓ จำนวนที่ปรึกษาไม่น้อยกว่า ๔ คน
๖. ค่าวัสดุอุปกรณ์ บาท
๗. ค่าใช้จ่ายในการเดินทางไปต่างประเทศ (ถ้ามี)บาท
๘. ค่าใช้จ่ายอื่นๆบาท
๙. รายชื่อผู้รับผิดชอบในการกำหนดค่าใช้จ่าย/ดำเนินการ/ขอบเขตดำเนินการ (TOR)
(ตามบันทึกข้อความที่ ศม.๐๒๐/๒๕๖๘ ลว.๑๕ ม.ค. ๒๕๖๘)

๙.๑ นายพัลลภ ม่วงไหมทอง	ประธานกรรมการ	    
๙.๒ นายณัฐรัฐ รุจิรรัตน์	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)
จัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญ
ของธนาคาร ประจำปี 2568
เลขที่ 103-042/68

1. ความเป็นมา/เหตุผลและความจำเป็น

ด้วยธนาคารอาคารสงเคราะห์มีความประสงค์จะดำเนินการจัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร ประจำปี 2568 เพื่อค้นหาและประเมินความเสี่ยงของช่องโหว่ ที่มีอยู่ในระบบสารสนเทศของธนาคาร และหาแนวทางป้องกัน ลดผลกระทบที่อาจเกิดขึ้นกับธนาคารได้ โดยมีวงเงินงบประมาณ 1,500,000.00 บาท (หนึ่งล้านห้าแสนบาทถ้วน) ตามแผนงานงบประมาณรายจ่ายประจำปี 2568 และสอดคล้องตามมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001:2022 และประกาศธนาคารแห่งประเทศไทย ที่ สกข.5/2566 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

2. วัตถุประสงค์

ธนาคารอาคารสงเคราะห์ ซึ่งต่อไปนี้จะเรียกว่า “ธนาคาร” มีความประสงค์จะจัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร โดยวัตถุประสงค์ของการสำรวจประเมินช่องโหว่เพื่อช่วยตอบคำถามว่า “ระบบสารสนเทศในธนาคารมีความปลอดภัยเพียงใด” หลักการของการสำรวจประเมินช่องโหว่ มีดังนี้

- 1) สำรวจและวิเคราะห์ช่องโหว่ระบบสารสนเทศ (Vulnerability Assessment)
- 2) ทดสอบการเจาะระบบ (Penetration Test)
- 3) ให้คำปรึกษาในการปิดช่องโหว่ (Hardening)

ในการสำรวจประเมินช่องโหว่ต้องอาศัยผู้เชี่ยวชาญที่มีความชำนาญเฉพาะด้านในการวิเคราะห์ช่องโหว่ที่มีความเสี่ยง รวมถึงเทคโนโลยีที่ก้าวทันต่อช่องโหว่ที่เหล่าบรรดาแฮกเกอร์นั้นพยายามเจาะเข้าสู่ระบบสารสนเทศอยู่ตลอดเวลา ดังนั้นศูนย์ความมั่นคงด้านเทคโนโลยีสารสนเทศ ได้กำหนดแผนงานการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร 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 ไม่เป็นบุคคลซึ่งถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย
- 3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา
- 3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพตามที่จ้าง
- 3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่ธนาคาร ณ วันประกาศประกวดราคา หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการประกวดราคารั้งนี้
- 3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น
- 3.10 ผู้เสนอราคาต้องมีบุคลากรภายในทีมงานที่จะเข้ามาสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร ไม่น้อยกว่า 2 ท่าน โดยแต่ละท่านต้องมีประกาศนียบัตรที่เกี่ยวข้องด้านความมั่นคงปลอดภัย OSCP หรือ GPEN หรือ eWPT อย่างใดอย่างหนึ่ง
- 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) ในกรณีผู้เสนอราคาเป็นบุคคลธรรมดาหรือคณะบุคคลที่มีชื่อนิติบุคคล ให้ยื่นสำเนาบัตรประจำตัวประชาชนของผู้ยื่น สำเนาข้อตกลงที่แสดงถึงการเข้าเป็นหุ้นส่วน (ถ้ามี) สำเนาบัตรประจำตัวประชาชนของผู้เป็นหุ้นส่วน พร้อมทั้งรับรองสำเนาถูกต้อง

(3) ในกรณีผู้เสนอราคาเป็นผู้เสนอการร่วมกันในฐานะเป็นผู้ร่วมค้า ให้ยื่นสำเนาสัญญาของการเข้าร่วมค้า สำเนาบัตรประจำตัวประชาชนของผู้ร่วมค้า และในกรณีที่ผู้เข้าร่วมค้าฝ่ายใดเป็นบุคคลธรรมดาที่มีชื่อสัญชาติไทย ก็ให้ยื่นสำเนาหนังสือเดินทาง หรือผู้ร่วมค้าฝ่ายใดเป็นนิติบุคคลให้ยื่นเอกสารตามที่ระบุไว้ใน (1)

(4) บัญชีเอกสารส่วนที่ 1 ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

4.2 ส่วนที่ 2 อย่างน้อยต้องมีเอกสารดังต่อไปนี้

(1) แค็ตตาล็อกและหรือแบบรูปรายการละเอียดคุณลักษณะเฉพาะ

(2) หนังสือมอบอำนาจซึ่งปิดอากรแสตมป์ตามกฎหมายในกรณีที่ผู้เสนอราคามอบอำนาจให้บุคคลอื่นลงนามในใบเสนอราคาแทน

(3) บัญชีเอกสารส่วนที่ 2 ทั้งหมดที่ได้ยื่นพร้อมกับซองใบเสนอราคา

5. หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ

ธนาคารจะพิจารณาคัดสินโดยใช้เกณฑ์ราคา

6. การทำสัญญา

ผู้ได้รับการคัดเลือกจะต้องติดต่อธนาคารเพื่อทำสัญญาภายใน 7 วัน นับถัดจากวันที่ได้รับแจ้ง และจะต้องวางหลักประกันสัญญาเป็นจำนวนเงินเท่ากับร้อยละ 5 ของมูลค่าสัญญา และให้ธนาคารยึดถือไว้ในขณะทำสัญญา โดยให้หลักประกันอย่างหนึ่งอย่างใด ดังต่อไปนี้



6.1 เงินสด

6.2 เช็คหรือตราพดที่ธนาคารเซ็นสั่งจ่าย ซึ่งเป็นเช็คหรือตราพดลงวันที่ที่ใช้เช็คหรือตราพดนั้นชำระต่อเจ้าหน้าที่ หรือก่อนหน้านั้นไม่เกิน 3 วัน ทำการ

6.3 หนังสือค้ำประกันของธนาคารภายในประเทศตามตัวอย่างที่คณะกรรมการนโยบายกำหนด โดยอาจเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนดก็ได้

6.4 หนังสือค้ำประกันของบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบ โดยอนุมัติให้ใช้ตามตัวอย่างหนังสือค้ำประกันของธนาคารที่คณะกรรมการนโยบายกำหนด

6.5 พันธบัตรรัฐบาลไทย

หลักประกันนี้จะคืนให้โดยไม่มีดอกเบี้ย ภายใน 15 วัน นับถัดจากวันที่คู่สัญญาพ้นจากข้อผูกพันตามสัญญาแล้ว

ทั้งนี้ หากผู้ได้รับการคัดเลือกไม่ดำเนินการภายในระยะเวลาดังกล่าวข้างต้น ธนาคารสงวนสิทธิ์ที่จะยกเลิกการจ้าง และพิจารณาแจ้งเป็นผู้ทำงาน

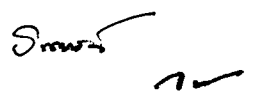
7. คุณสมบัติเฉพาะ / รายละเอียดของงานจ้าง

7.1 ผู้ยื่นข้อเสนอจะต้องเสนอรูปแบบการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร โดยต้องนำเสนอมาตรฐานที่ใช้ในการดำเนินการทดสอบ เช่น

- มีกระบวนการขั้นตอนในการทดสอบ
- มีมาตรฐานอ้างอิงในการทดสอบ เช่น OSSTMM , PTES , OWASP หรือมาตรฐานสากลอื่นๆ ที่เกี่ยวข้อง

7.2 ผู้ยื่นข้อเสนอต้องเสนอ Proposal โดยมีรายละเอียดของ Proposal ประกอบด้วยหัวข้อดังต่อไปนี้

- ตารางเปรียบเทียบคุณลักษณะเฉพาะของการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร ที่เสนอกับคุณลักษณะเฉพาะที่ธนาคารกำหนด (ตามผนวก 1)
- แผนการดำเนินงานทั้งหมด โดยต้องแบ่งแยกแผนการทำงานแต่ละงาน รายละเอียดงานช่วงเวลาและผู้รับผิดชอบในการเข้าปฏิบัติงาน และเบอร์ดิตต่อ (ตามผนวก 1)
- เอกสารอื่น ๆ (ถ้ามี) ที่ผู้ยื่นข้อเสนอเห็นว่าจะเป็นประโยชน์ต่อการพิจารณาของธนาคาร



8. ระยะเวลาดำเนินการ/ส่งมอบงาน และการตรวจรับ

ผู้ได้รับการคัดเลือกต้องส่งมอบงานภายใน 220 วัน นับถัดจากวันลงนามในสัญญา มีเงื่อนไขการส่งมอบพัสดุตามผนวก 1.

9. วงเงินในการจัดหา

วงเงินงบประมาณ 1,500,000.00 บาท (หนึ่งล้านห้าแสนบาทถ้วน)

10. เงื่อนไขการชำระเงิน

ธนาคารจะแบ่งชำระเงินค่าจ้างบริการ โดยแบ่งการชำระออกเป็น 2 งวด มีรายละเอียด ดังนี้

- 1) งวดที่ 1: ชำระเงินเป็นจำนวน 50% ของมูลค่าโครงการ ฯ เมื่อผู้ได้รับการคัดเลือกได้ส่งมอบงานงวดที่ 1 ภายในระยะเวลา 70 วัน นับถัดจากวันลงนามในสัญญา และเมื่อคณะกรรมการตรวจรับ ตรวจรับงานถูกต้องครบถ้วนตรงตามเงื่อนไขของสัญญาจ้าง ตามที่ระบุไว้ในผนวก 1.
- 2) งวดที่ 2: ชำระเงินเป็นจำนวน 50% ของมูลค่าโครงการ ฯ เมื่อผู้ได้รับการคัดเลือกได้ส่งมอบงานงวดที่ 2 ภายในระยะเวลา 220 วัน นับถัดจากวันลงนามในสัญญา และเมื่อคณะกรรมการตรวจรับ ตรวจรับงานถูกต้องครบถ้วนตรงตามเงื่อนไขของสัญญาจ้าง ตามที่ระบุไว้ในผนวก 1.

เมื่อธนาคารได้ตรวจรับมอบการสอบทานการตรวจสอบข้อเท็จจริงและทดสอบนுகฎระบบสารสนเทศสำคัญของธนาคาร ถูกต้องครบถ้วนตามสัญญาจ้าง แล้ว ธนาคารจะออกหลักฐานการรับมอบไว้เป็นหนังสือ เพื่อผู้ยื่นข้อเสนอนำมาใช้เป็นหลักฐานประกอบการขอรับเงินค่าจ้างการสอบทานการตรวจสอบข้อเท็จจริงและทดสอบนுகฎระบบสารสนเทศสำคัญของธนาคาร

11. อัตราค่าปรับ

ค่าปรับตามแบบสัญญาจ้าง ให้คิดเป็นรายวันในอัตราร้อยละ 0.10 ของราคางานจ้าง แต่จะต้องไม่ต่ำกว่าวันละ 100.- บาท

12. การรับประกันความชำรุดบกพร่อง

ผู้ได้รับการคัดเลือกซึ่งได้ทำสัญญากับธนาคาร จะต้องรับประกันความชำรุดบกพร่องของสิ่งของงานจ้างที่เกิดขึ้นภายในระยะเวลาไม่น้อยกว่า 60 วัน นับถัดจากวันที่ธนาคารได้รับมอบงาน



13. การปฏิบัติตามกฎหมายและระเบียบ

ผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกต้องปฏิบัติตามหลักเกณฑ์ที่กฎหมายและระเบียบได้กำหนดไว้
โดยเคร่งครัด

14. หน่วยงานที่รับผิดชอบ

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

นายพัลลภ ม่วงไหมทอง

หัวหน้าส่วนดูแลมาตรฐานความมั่นคงปลอดภัย
กฎข้อบังคับและประเมินความเสี่ยงระบบสารสนเทศ
ประธานกรรมการ

นายณัฐรัฐ รุจิรรัตน์

พนักงานด้านความมั่นคงปลอดภัย
ด้านเทคโนโลยีสารสนเทศอาวุโส
กรรมการ

นางสาวฐิมาพร ไชติวินิจชัย
พนักงานคอมพิวเตอร์อาวุโส
กรรมการ

นายวรวิทย์ วงศ์รัตนวัฒน์
พนักงานคอมพิวเตอร์อาวุโส
กรรมการ

นางสาวธนาภรณ์ พูลเลิศ
พนักงานด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
กรรมการและเลขานุการ

ผนวก 1.

รายละเอียดและคุณลักษณะเฉพาะของการจัดจ้างที่ปรึกษาเพื่อสอบทานการตรวจสอบช่องโหว่ และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร

1. ขอบเขตการดำเนินงาน

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

1.1 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 , 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

1.2 ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในอาคาร ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคาร กำหนด โดยจะต้องดำเนินการดังต่อไปนี้

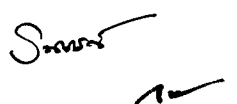
- ใช้เครื่องมือตรวจสอบช่องโหว่ (Scanning Tool) จำนวน 1 ชนิด ซึ่งต้องเป็นเครื่องมือ ที่เป็น Commercial มีการใช้งานแพร่หลาย เช่น Nessus หรือ Nexpose
- จัดทำผลสรุปภาพรวมการทดสอบสำหรับผู้บริหาร (Executive Summary) รวมถึงเสนอแผนในการแก้ไขระยะสั้น และระยะยาว
- วิเคราะห์ผลสำหรับผู้ดูแลระบบ โดยมีรายละเอียดดังนี้
 - จัดลำดับความเสี่ยงที่ต้องเร่งดำเนินการแก้ไข แยกตามประเภทอุปกรณ์ เครือข่าย/เครื่องแม่ข่าย และเรียงตามลำดับหมายเลขไอพี ที่ตรวจพบความเสี่ยงมากที่สุดไปน้อยที่สุด
 - รายละเอียดช่องโหว่ที่ตรวจพบในแต่ละอุปกรณ์เครือข่าย/เครื่องแม่ข่าย พร้อมทั้งให้คำแนะนำการปรับปรุงระบบหรือการแก้ไขช่องโหว่ที่ตรวจพบหรือ แนวทางในการลดความเสี่ยงที่เกิดขึ้น
 - รายละเอียดช่องโหว่ที่ตรวจพบ แบ่งตามประเภทช่องโหว่และระดับความรุนแรง (Critical, High) โดยอธิบายรายละเอียดช่องโหว่, ระดับความรุนแรง, CVSS Score Detail, แนวทางการแก้ไข และอุปกรณ์เครือข่าย/เครื่องแม่ข่าย ที่ได้รับผลกระทบ

1.3 ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด โดยจะต้อง ดำเนินการดังต่อไปนี้

- ทดสอบเจาะระบบจากภายนอกแบบ Black-Box Penetration Testing และทำการ ทดสอบเจาะระบบจากภายในอาคารแบบ Gray-Box Penetration Testing การดำเนินงานจะต้องครอบคลุมการทดสอบหาเป้าหมายทั้งแบบทางตรงและทางอ้อม
- จัดทำรายงาน ที่แสดงขั้นตอน/วิธีการในการบุกรุก เปรียบเทียบภาพรวมและผลกระทบ ของช่องโหว่ที่ตรวจพบ จากการทำ Black-Box และ Gray-Box Penetration Testing พร้อมทั้งดำเนินการวิเคราะห์และสรุปผลการดำเนินงาน แนวทางในการปรับปรุงแก้ไข ประเมินและจัดลำดับความเสี่ยง แยกตามประเภทของอุปกรณ์เครือข่าย

และเครื่องแม่ข่าย โดยวิเคราะห์ผลจะต้องสอดคล้องหรือต้องอ้างอิงตาม OWASP หรือมาตรฐานสากลอ้างอิงอื่นๆ ขึ้นอยู่กับประเภทของช่องโหว่ที่ตรวจพบ

- 1.4 ดำเนินการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงาน สลับส่นระบบสารสนเทศของธนาคาร 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
- 1.5 ดำเนินการส่งมอบเครื่องคอมพิวเตอร์แบบพกพา (Notebook) รวมถึง License ของระบบปฏิบัติการ โดยธนาคารไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม 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)
- 1.6 ดำเนินการจัดหาสิทธิ์การใช้งาน Platform ทางด้าน Cyber Security ที่มี Lab ให้ลงมือทำเชิงปฏิบัติได้จริงบนเครื่องจำลอง โดย Platform ดังกล่าวต้องมี Lab ที่ครอบคลุมตามมาตรฐาน OWASP ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ Enterprise จำนวน 3 สิทธิ์การใช้งาน
- 1.7 ดำเนินการจัดหาสิทธิ์การใช้งาน Platform ทางด้าน Cyber Security ที่สามารถทดสอบโจมตีด้วยช่องโหว่ต่างๆ ได้จริง โดยสามารถทดสอบโจมตีได้หลากหลายรูปแบบ และไม่ผิดกฎหมาย รวมถึงต้องมีเอกสาร Official Write-Up ให้ธนาคารใช้เป็นแนวทางในการ



ทดสอบโจมตีได้ ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ VIP Plus จำนวน 4 สิทธิการใช้งาน

- 1.8 ดำเนินการจัดหาสิทธิการใช้งานเครื่องมือที่ใช้ในการทดสอบบุกรุกระบบ (Burp Suite Professional) ที่ใช้ในการดำเนินวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงาน ระยะเวลา 1 ปี จำนวน 3 สิทธิการใช้งาน

2. วิธีการดำเนินงาน

- 2.1 จัดทำโครงสร้างการบริหารโครงการ พร้อมแต่งตั้งผู้บริหารโครงการ (Project Manager) จำนวน 1 คน โดยต้องมีความชำนาญและมีประสบการณ์ในการควบคุมและบริหารโครงการด้าน IT เพื่อรับผิดชอบดำเนินงานตามข้อกำหนด และประสานการดำเนินงานกับธนาคาร เพื่อให้โครงการสำเร็จได้ด้วยดี
- 2.2 จัดทำแผนงานรายละเอียดโครงสร้างของทีมงาน ตำแหน่ง คุณสมบัติ/ประกาศนียบัตร หน้าที่ความรับผิดชอบปฏิบัติงานในแต่ละช่วงเวลา หรือแต่ละขั้นตอนของกิจกรรมของแต่ละท่านที่จะเข้ามาปฏิบัติงานให้แก่ธนาคาร
- 2.3 เป้าหมายการดำเนินงานทั้งหมดจะเป็นระบบงานของธนาคารเท่านั้น โดยอุปกรณ์คอมพิวเตอร์ หรือ Software ที่นำมาใช้ในการดำเนินงานตรวจสอบช่องโหว่ และทดสอบบุกรุกระบบตามขอบเขตงาน ที่ปรึกษาจะต้องเป็นผู้จัดหาทุกสิ่ง
- 2.4 ในการดำเนินงานโครงการสอบทานการตรวจสอบช่องโหว่และทดสอบบุกรุกระบบสารสนเทศสำคัญของธนาคาร สรุปได้ดังนี้
 - 1) ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด (ตามขอบเขตการดำเนินงานข้อ 1.1)
 - 2) ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด (ตามขอบเขตการดำเนินงานข้อ 1.2)
 - 3) ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย



(Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด (ตามขอบเขตการดำเนินงานข้อ 1.3)

- 4) ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด (ตามขอบเขตการดำเนินงานข้อ 1.4)
- 5) ดำเนินการส่งมอบเครื่องคอมพิวเตอร์แบบพกพา (Notebook) รวมถึง License ของระบบปฏิบัติการ Windows 11 Pro ที่จำเป็นต้องใช้งาน โดยธนาคารไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม เพื่อให้ธนาคารสามารถใช้งานสอบทานตรวจสอบผลการดำเนินงานได้ภายหลัง (ตามขอบเขตการดำเนินงานข้อ 1.5)
- 6) ดำเนินการจัดหาสิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่มี Lab ให้ลงมือทำเชิงปฏิบัติได้จริงบนเครื่องจำลอง โดย Platform ดังกล่าวต้องมี Lab ที่ครอบคลุมตามมาตรฐาน OWASP ให้เป็นกรรมสิทธิ์ของธนาคาร เข้าใช้งานเป็นระยะเวลา 1 ปี แบบ Enterprise จำนวน 3 สิทธิ์การใช้งาน (ตามขอบเขตการดำเนินงานข้อ 1.6)
- 7) ดำเนินการจัดหาสิทธิ์การเข้าใช้งาน Platform ทางด้าน Cyber Security ที่สามารถทดสอบโจมตีด้วยช่องโหว่ต่างๆ ได้จริง โดยสามารถทดสอบโจมตีได้หลากหลายรูปแบบและไม่ผิดกฎหมาย รวมถึงต้องมีเอกสาร Official Write-Up ให้ธนาคารใช้เป็นแนวทางในการทดสอบโจมตีได้ ให้เป็นกรรมสิทธิ์ของธนาคาร เข้าใช้งานเป็นระยะเวลา 1 ปี แบบ VIP Plus จำนวน 4 สิทธิ์การใช้งาน (ตามขอบเขตการดำเนินงานข้อ 1.7)
- 8) ดำเนินการจัดหาสิทธิ์การเข้าใช้งานเครื่องมือที่ใช้ในการทดสอบบุกรุกระบบ (Burp Suite Professional) ที่สามารถทดสอบโจมตีด้วยช่องโหว่ต่างๆ ได้จริง ระยะเวลา 1 ปี จำนวน 3 สิทธิ์การใช้งาน (ตามขอบเขตการดำเนินงานข้อ 1.8)

3. 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

3.1 ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด (ตามขอบเขตการดำเนินงานข้อ 1.1)

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

3.2 ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) จากวงเครือข่ายภายในธนาคาร ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด (ตามขอบเขตการดำเนินงานข้อ 1.2)

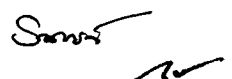
- ครั้งที่ 1 : ส่งมอบงานภายใน 50 วัน นับถัดจากวันที่ลงนามในสัญญา
- ครั้งที่ 2 : ส่งมอบงานภายใน 190 วัน นับถัดจากวันที่ลงนามในสัญญา

3.3 ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด (ตามขอบเขตการดำเนินงานข้อ 1.3)

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

3.4 ดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด (ตามขอบเขตการดำเนินงานข้อ 1.4)

- ครั้งที่ 1 : ส่งมอบงานภายใน 70 วัน นับถัดจากวันที่ลงนามในสัญญา



- ครั้งที่ 2 : ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

3.5 ดำเนินการดำเนินการส่งมอบเครื่องคอมพิวเตอร์แบบพกพา (Notebook) รวมถึง License ของระบบปฏิบัติการ Windows 11 Pro ที่จำเป็นต้องใช้งาน โดยธนาคารไม่ต้องเสียค่าใช้จ่ายเพิ่มเติม เพื่อให้ธนาคารสามารถใช้งานสอบทานตรวจสอบผลการดำเนินงานได้ภายหลัง (ตามขอบเขตการดำเนินงานข้อ 1.5)

- ส่งมอบงานภายใน 70 วัน นับถัดจากวันที่ลงนามในสัญญา

3.6 ดำเนินการจัดหาสิทธิการใช้งาน Platform ทางด้าน Cyber Security ที่มี Lab ให้ลงมือทำเชิงปฏิบัติได้จริงบนเครื่องจำลอง โดย Platform ดังกล่าวต้องมี Lab ที่ครอบคลุมตามมาตรฐาน OWASP ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ Enterprise จำนวน 3 สิทธิการใช้งาน (ตามขอบเขตการดำเนินงานข้อ 1.6)

- ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

3.7 ดำเนินการจัดหาสิทธิการใช้งาน Platform ทางด้าน Cyber Security ที่สามารถทดสอบโจมตีด้วยช่องโหว่ต่างๆ ได้จริง โดยสามารถทดสอบโจมตีได้หลากหลายรูปแบบและไม่ผิดกฎหมาย รวมถึงต้องมีเอกสาร Official Write-Up ให้ธนาคารใช้เป็นแนวทางในการทดสอบโจมตีได้ ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ VIP Plus จำนวน 4 สิทธิการใช้งาน (ตามขอบเขตการดำเนินงานข้อ 1.7)

- ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

3.8 ดำเนินการจัดหาสิทธิดำเนินการจัดหาสิทธิการใช้งานเครื่องมือที่ใช้ในการทดสอบบุกรุกระบบ (Burp Suite Professional) ที่ใช้ในการดำเนินวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงาน ระยะเวลา 1 ปี จำนวน 3 สิทธิการใช้งาน (ตามขอบเขตการดำเนินงานข้อ 1.8)

- ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา

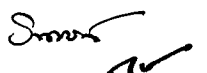
4. งานที่ต้องส่งมอบ

เอกสารส่งมอบต้องส่งมอบในลักษณะของแฟ้มงาน และจัดทำ Index ของเอกสาร แบ่งแยกเอกสารแต่ละชุดอย่างชัดเจน โดยมีรายละเอียด ดังนี้

4.1 สิ่งที่ต้องส่งมอบตามขอบเขตการดำเนินงานข้อ 1.1

- ครั้งที่ 1 : ส่งมอบงานภายใน 50 วัน นับถัดจากวันที่ลงนามในสัญญา

รายงานผลการดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) ของอุปกรณ์ระบบเครือข่าย (Network)



เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด (ฉบับภาษาไทย) (Initial Scan)

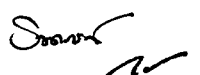
- ครั้งที่ 2 : ส่งมอบงานภายใน 190 วัน นับถัดจากวันที่ลงนามในสัญญา
รายงานผลการทดสอบซ้ำของการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด (ฉบับภาษาไทย) (Revisit Scan)

4.2 สิ่งที่ต้องส่งมอบตามขอบเขตการดำเนินงานข้อ 1.2

- ครั้งที่ 1 : ส่งมอบงานภายใน 50 วัน นับถัดจากวันที่ลงนามในสัญญา
รายงานผลการดำเนินการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด (ฉบับภาษาไทย) (Initial Scan)
- ครั้งที่ 2 : ส่งมอบงานภายใน 190 วัน นับถัดจากวันที่ลงนามในสัญญา
รายงานผลการทดสอบซ้ำของการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) ของอุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด (ฉบับภาษาไทย) (Revisit Scan)

4.3 สิ่งที่ต้องส่งมอบตามขอบเขตการดำเนินงานข้อ 1.3

- ครั้งที่ 1 : ส่งมอบงานภายใน 70 วัน นับถัดจากวันที่ลงนามในสัญญา
รายงานผลการวิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด (ฉบับภาษาไทย) (Initial Pentest)
- ครั้งที่ 2 : ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา
รายงานผลการทดสอบซ้ำของการสอบทานการตรวจสอบ การวิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network)



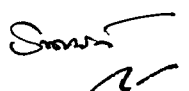
เครื่องแม่ข่าย (Servers) ของระบบหลัก GHB SYSTEM และระบบที่ให้บริการ Electronic Channel ที่ธนาคารกำหนด (ฉบับภาษาไทย) (Revisit Pentest)

4.4 สิ่งที่ต้องส่งมอบตามขอบเขตการดำเนินงานข้อ 1.4

- ครั้งที่ 1 : ส่งมอบงานภายใน 70 วัน นับถัดจากวันที่ลงนามในสัญญา
รายงานผลการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด (ฉบับภาษาไทย) (Initial Pentest)
- ครั้งที่ 2 : ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา
รายงานผลการทดสอบซ้ำการสอบทานการตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Penetration Testing) ของ อุปกรณ์ระบบเครือข่าย (Network) เครื่องแม่ข่าย (Servers) ของระบบงานสนับสนุนระบบสารสนเทศของธนาคาร ที่ธนาคารกำหนด (ฉบับภาษาไทย) (Revisit Pentest)

4.5 สิ่งที่ต้องส่งมอบตามขอบเขตการดำเนินงานข้อ 1.5 (ส่งมอบงานภายใน 70 วัน นับถัดจากวันที่ลงนามในสัญญา)

1. เอกสารแสดง Software License ของระบบปฏิบัติการ Windows 11 Pro ที่ติดตั้งในเครื่องคอมพิวเตอร์แบบพกพา (Notebook) ที่ส่งมอบมาในโครงการ
2. เครื่องคอมพิวเตอร์แบบพกพา (Notebook) เพื่อให้ธนาคารสามารถในการศึกษา Cyber Security Platform และใช้สอบทานผลการตรวจสอบช่องโหว่ได้ภายหลัง โดยมีคุณสมบัติขั้นต่ำ ดังนี้
 - CPU Core i-7 หรือสูงกว่า
 - Memory 16 GB DDR4
 - Hard disk SSD 500 GB หรือสูงกว่า
 - ระบบปฏิบัติการ Windows 11 Pro (64 bit)



4.6 สิ่งที่ต้องส่งมอบตามขอบเขตการดำเนินงานข้อ 1.6 (ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา)

- เอกสารแสดงสิทธิ์การใช้งาน Platform ทางด้าน Cyber Security ที่มี Lab ให้ลงมือทำเชิงปฏิบัติได้จริงบนเครื่องจำลอง โดย Platform ดังกล่าวต้องมี Lab ที่ครอบคลุมตามมาตรฐาน OWASP ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ Enterprise จำนวน 3 สิทธิ์การใช้งาน

4.7 สิ่งที่ต้องส่งมอบตามขอบเขตการดำเนินงานข้อ 1.7 (ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา)

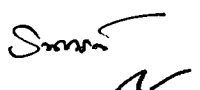
- เอกสารแสดงสิทธิ์การใช้งาน Platform ทางด้าน Cyber Security ที่สามารถทดสอบโจมตีด้วยช่องโหว่ต่างๆ ได้จริง โดยสามารถทดสอบโจมตีได้หลากหลายรูปแบบและไม่ผิดกฎหมาย รวมถึงต้องมีเอกสาร Official Write-Up ให้ธนาคารใช้เป็นแนวทางในการทดสอบโจมตีได้ ให้เป็นกรรมสิทธิ์ของธนาคารเข้าใช้งานเป็นระยะเวลา 1 ปี แบบ VIP Plus จำนวน 4 สิทธิ์การใช้งาน

4.8 สิ่งที่ต้องส่งมอบตามขอบเขตการดำเนินงานข้อ 1.8 (ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา)

- เอกสารแสดงสิทธิ์การใช้งานเครื่องมือที่ใช้ในการทดสอบบุกรุกระบบ (Burp Suite Professional) ที่ใช้ในการดำเนินวิเคราะห์ ประเมินช่องโหว่ และทดสอบความปลอดภัยของระบบงาน ระยะเวลา 1 ปี จำนวน 3 สิทธิ์การใช้งาน

4.9 สิ่งที่ต้องส่งมอบตามขอบเขตการดำเนินงานข้อ 1.1- ข้อ 1.8 (ส่งมอบงานภายใน 220 วัน นับถัดจากวันที่ลงนามในสัญญา) สามารถเปิดและแก้ไขด้วยชุดโปรแกรมจาก Microsoft office ตั้งแต่ Version 2016 ขึ้นไป บรรจุใน USB Drive อย่างละ 1 ชุด (ฉบับภาษาไทย) แนบมาในแฟ้มงาน โดยมีรายละเอียดดังนี้

1. ไฟล์เอกสารต่าง ๆ ฉบับสมบูรณ์ ที่ส่งมอบตามข้อ 4.1 – ข้อ 4.8
2. ไฟล์รายงานผลลัพธ์จากเครื่องมือที่ใช้ในการทดสอบ (Raw Data) ในหัวข้อขอบเขตการดำเนินงาน ข้อ 1.1 และข้อ 1.2 ครั้งที่ 1 และครั้งที่ 2 (นามสกุลไฟล์ .csv หรือ .xlsx)



ธนาคารอาคารสงเคราะห์ให้ความสำคัญกับการปฏิบัติตามกฎหมายว่าด้วย
การคุ้มครองข้อมูลส่วนบุคคล ธนาคารจึงได้กำหนดนโยบายคุ้มครองข้อมูล
ส่วนบุคคล โดยสามารถศึกษารายละเอียดที่ QR Code นี้

