ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการทดสอบเจาะระบบงาน MY EXIM (EXIM TBP Phase 2)**

2. หน่วยงานเจ้าของโครงการ **ฝ่ายพัฒนากระบวนการและนวัตกรรม**

3. วงเงินงบประมาณที่ได้รับจัดสรร **1,500,000.- บาท (หนึ่งล้านห้าแสนบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 29 ก.ย. 2563
   เป็นเงิน 1,500,000.- บาท (หนึ่งล้านห้าแสนบาทถ้วน)

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
   5.1 บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด
   5.2 บริษัท ดีลอยท์ ทู้ช โธมัทสุ ไชยยศ จำกัด
   5.3 บริษัท ดาต้าฟาร์ม จำกัด
   5.4 บริษัท เอซีอินโฟเทค จำกัด

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายสมชาย	พันธ์นาค	ผู้เชี่ยวชาญพิเศษ ฝ่ายธุรกิจธนาคาร
6.2 นายภาคิน	โพธิคุณ	ผู้ช่วยผู้จัดการส่วนพัฒนาระบบสารสนเทศบริการ 1 ฝ่ายบริหารและพัฒนาเทคโนโลยีสารสนเทศ
6.3 นายวรอรรถ	วัฒนาพรินทร	ผู้ช่วยผู้บริหารส่วนพัฒนากระบวนการด้านเทคโนโลยีสารสนเทศ ฝ่ายพัฒนากระบวนการและนวัตกรรม

ผนวก 1

ขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการทดสอบเจาะระบบงาน MY EXIM (EXIM TBP Phase 2)

---

1. ขอบเขตการดำเนินงาน

ผู้ยื่นข้อเสนอต้องดำเนินการตามเงื่อนไขและขอบเขตความต้องการของธนาคารฯ อย่างน้อยดังนี้

1.1 จัดทำแผนดำเนินงานอย่างละเอียด โดยต้องเสนอแผนดำเนินงานดังกล่าวให้ ธนาคารฯ เห็นชอบก่อนดำเนินงาน

1.2 ระบบงานเป้าหมาย คือ ระบบ EXIM Transactional Banking Portal (EXIM TBP)

1.3 ในการทดสอบ ผู้ยื่นข้อเสนอต้องดำเนินการโดยใช้โปรแกรมหรือซอฟท์แวร์ที่เป็นแบบ Commercial ที่มีความน่าเชื่อถือ และเป็นโปรแกรมที่ผู้ยื่นข้อเสนอมีลิขสิทธิ์ถูกต้อง

1.4 ดำเนินการทดสอบเจาะระบบ MY EXIM (EXIM TBP Phase 2) ตามระยะเวลาการ Go live ของเว็บแอพพลิเคชั่น (Web Application) และโมบายล์แอพพลิเคชั่น (Mobile Application) ทั้ง Front end และ Back end โดยแบ่งออกเป็น 2 ระยะ ซึ่งแต่ละระยะต้องะดำเนินการทดสอบ จำนวน 2 ครั้ง เพื่อเปรียบเทียบผลการดำเนินการปิดช่องโหว่ ดังนี้

1.4.1 ดำเนินการทดสอบเจาะระบบในรูปแบบ Grey-Box Penetration Testing โดยธนาคารฯ จะจัดเตรียม USERNAME และ PASSWORD ในการเข้าถึง พร้อมจัดเตรียมชุดข้อมูลในการทดสอบ ผู้ยื่นข้อเสนอต้องดำเนินการค้นหาช่องโหว่ในทุกหน้าและทุกฟังก์ชัน ของ EXIM TBP Web Application/ Mobile Application โดยจะต้องค้นหาช่องโหว่ทั้งทางด้านเทคนิค เช่น OWASP Top 10 Application Risk และ ช่องโหว่ทาง Business Logic

1.4.2 ดำเนินการเจาะระบบจากเครือข่ายภายนอกธนาคารฯ External Penetration Testing (Black-Box) เพื่อนำเอาข้อมูลสำคัญ เช่น บัญชีผู้ดูแลระบบพร้อมทั้งรหัสผ่าน หรือบัญชีผู้ใช้พร้อมรหัสผ่าน หรือข้อมูลอื่นๆ ที่มีความสำคัญ รวมถึงการกระทำใดๆ ที่อาจทำให้ธนาคารฯ ได้ทราบถึงความเสี่ยงจากการถูกเจาะระบบ ในการทดสอบจะดำเนินการเหมือนกับการเจาะระบบโดยไวรัสหรือแฮกเกอร์ที่ปฏิบัติการจริง โดยดำเนินการทดสอบเพื่อหาช่องทางในการเข้าถึงระบบ (Exploit) เป็นการเข้าถึงระบบโดยผ่านช่องโหว่ต่างๆ เพื่อมุ่งเจาะระบบแม่ข่ายและเครือข่าย โดยครอบคลุมระบบงานเป้าหมายตามข้อ 1.2

1.4.3 ในการทดสอบ Grey-Box Penetration Testing ต้องครอบคลุม Open Web Application Security Project (OWASP) TOP 10 ปี 2017 หรือใหม่กว่า

1.4.4 การดำเนินการทดสอบการเจาะระบบจากเครือข่ายภายนอกธนาคารฯ External Penetration Testing (Black-Box) นี้ จะต้องใช้วิธีการที่เป็นไปตามมาตรฐานดังต่อไปนี้เป็นอย่างน้อย 1 ข้อ (Version ล่าสุดที่มีการประกาศในการใช้งาน ณ วันที่ลงนามในสัญญา)

1.4.4.1 Open Source Security Testing Methodology (OSSTM) และ/หรือ

1.4.4.2 NIST SP800-115 Guideline on Network Security Testing

1.4.5 ดำเนินการทดสอบเจาะระบบในรูปแบบผสมผสาน คือการทดสอบโดยใช้โปรแกรมเจาะระบบแบบอัตโนมัติ (Automate Tool) ทั้งที่เป็น Commercial Tool และ ที่เป็น Open Source Tool ผสมผสานกับความเชี่ยวชาญของบุคลากร (Human Skill) พร้อมเก็บหลักฐานจากการทดสอบ (ผู้ยื่นข้อเสนอต้องใช้การทดสอบและวิเคราะห์ด้วยตัวบุคคลเอง (Manual Test) มิให้ใช้เครื่องมืออัตโนมัติ (Automatic Test Tool) เพียงอย่างเดียว)

1.5 ดำเนินการจัดทำรายงานผลการทดสอบการเจาะระบบแต่ละระยะ และนำเสนอเอกสารการประเมินและวิเคราะห์ความปลอดภัย ผลการประเมิน จุดอ่อน ระดับความเสี่ยง และคำแนะนำการปรับปรุงแก้ไขข้อบกพร่อง รวมถึงผลกระทบที่อาจเกิดขึ้นอย่างละเอียดพร้อมแนวทางการแก้ไข รวมถึง เวลาโดยประมาณในการแก้ไขต่อธนาคารฯ ต่าง ๆ ดังนี้

1.5.1 จัดทำรายงานอย่างละเอียด โดยมีเนื้อหาครอบคลุมถึง วิธีการทดสอบ ผลการประเมินต่าง ๆ (ตามข้อ 1.4) พร้อมผลการวิเคราะห์ผลกระทบจากความเสี่ยง และคำแนะนำในการแก้ไขปัญหาที่ค้นพบเพื่อปรับปรุงความมั่นคง ปลอดภัย

1.5.2 จัดทำรายงานสรุปผลการประเมิน และคำแนะนำสำหรับผู้บริหาร (Executive Summary)

1.5.3 นำเสนอผลการประเมินต่างๆ (ตามข้อ 1.4) พร้อมคำแนะนำและวิธีดำเนินการในการแก้ปัญหาเพื่อปรับปรุงความมั่นคงปลอดภัย ให้แก่ เจ้าหน้าที่ของธนาคาร หลังจากนั้น ธนาคารฯ จะดำเนินการปรับปรุงระบบ โดยมีระยะเวลาไม่เกิน 1 เดือน นับจากผู้ยื่นข้อเสนอที่ได้รับการคัดเลือกส่งมอบข้อ 1.5.3 และแจ้งให้บริษัทฯ ดำเนินการต่อในข้อ 1.5.4

1.5.4 ประเมินความเสี่ยงเพื่อหาช่องโหว่ และการทดสอบเจาะระบบ (Penetration Testing) ซ้ำและจัดทำรายงานการทดสอบ

1.6 ผู้ยื่นข้อเสนอจะต้องรวบรวมและจัดทำรายงานการดำเนินการ แผนการดำเนินการ ขั้นตอนการดำเนินการ รวมถึงรายงานผลการทดสอบทั้งหมด บทวิเคราะห์ คำแนะนำ การแก้ไข การตรวจสอบหลังการแก้ไข และบทสรุปผู้บริหารทั้งหมด โดยจัดทำเป็นเอกสารพร้อมส่งทั้งแบบ Hardcopy และ Softcopy ในรูปแบบ MS Word และ Portable Document Format (PDF) เพื่อนำเสนอธนาคารฯ จำนวน 2 ชุด

1.7 ผู้ยื่นข้อเสนอต้องแจ้งพนักงานธนาคารฯ ให้ทราบทุกครั้งก่อนเข้าดำเนินงานในแต่ละขั้นตอน ถึงแผนการเข้ามาดำเนินงาน รายละเอียดการดำเนินการ เครื่องมือที่ใช้ โปรแกรมที่เกี่ยวข้อง หรือเทคนิคที่ใช้ในการเจาะระบบ รวมถึงการประเมินผลกระทบที่อาจมีขึ้นเพื่อป้องกันไม่ให้เกิดความเสียหายต่อระบบที่ทดสอบนั้น ทั้งนี้ ผู้ยื่นข้อเสนอจะต้องแจ้งธนาคารฯ ทราบล่วงหน้าอย่างน้อย 3 วันทำการและจะดำเนินการได้หลังจากที่ได้รับความเห็นชอบทุกครั้ง

1.8 ผู้ยื่นข้อเสนอต้องรับผิดชอบในการแนะนำแนวทางการปิดช่องโหว่ ให้กับผู้ดูแลและผู้พัฒนาระบบของธนาคารฯ ที่อาจส่งผลกระทบต่อระดับความปลอดภัยของระบบเทคโนโลยีสารสนเทศของธนาคารฯ ภายหลังจากการทดสอบการเจาะระบบและการประเมินความเสี่ยง รวมถึงการปรับปรุงความมั่นคงปลอดภัยของระบบให้เป็นไปอย่างเหมาะสม หรือตามที่ธนาคารฯ กำหนด

1.9 ผู้ดูแลและผู้พัฒนาระบบของธนาคารฯ จะเป็นผู้ดำเนินการปิดช่องโหว่ที่พบตามคำแนะนำและวิธีการที่ผู้ยื่นข้อเสนอได้นำเสนอ โดยมีผู้ยื่นข้อเสนอให้คำปรึกษาจนดำเนินการแล้วเสร็จ

1.10 หลังจากที่ผู้ดูแลและผู้พัฒนาระบบของธนาคารฯ ดำเนินการปิดช่องโหว่ตามข้อ 1.8 แล้ว ผู้ยื่นข้อเสนอต้องดำเนินการตรวจสอบผลการปิดช่องโหว่หรือจุดอ่อน เพื่อยืนยันช่องโหว่ที่พบว่าได้รับการแก้ไขแล้วและหาช่องโหว่ที่อาจยังเหลืออยู่ (Re-visit)

1.11 หากในข้อ 1.10 ผู้ยื่นข้อเสนอตรวจสอบพบจุดอ่อนหรือช่องโหว่เดิมที่ได้รายงานและแก้ไขไปแล้วในข้อ 1.8 ให้ ถือเป็นความรับผิดชอบของผู้ดูแลและผู้พัฒนาระบบของธนาคารฯ ในการดำเนินการแก้ไข โดยมีผู้ยื่นข้อเสนอให้คำปรึกษาจนดำเนินการแล้วเสร็จ และระหว่างดำเนินการแก้ไขผู้ยื่นข้อเสนอสามารถระงับการทดสอบชั่วคราว จนกว่าผู้ดูแลและผู้พัฒนาระบบของธนาคารฯ จะดำเนินการแก้ไขเสร็จสิ้น จึงดำเนินการตรวจสอบเพื่อยืนยันผลการแก้ไขให้กับทางธนาคารฯ ได้รับทราบต่อไป

ร่วมมา