ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจ้างผู้ให้บริการเช่าใช้ระบบคอมพิวเตอร์และเครือข่ายเพื่อให้บริการลูกค้า**

   (Managed Service for ECI Online and TBP and EXIM1)

2. หน่วยงานเจ้าของโครงการ **ฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ**

3. วงเงินงบประมาณที่ได้รับจัดสรร **15,000,000.00 บาท (สิบห้าล้านบาทถ้วน)**

4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) **9 พฤษภาคม** 2566

   เป็นเงิน **14,468,875.98 บาท (สิบสี่ล้านสี่แสนหกหมื่นแปดพันแปดร้อยเจ็ดสิบห้าบาทเก้าสิบแปดสตางค์)**

5. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)

   บริษัท อินเทอร์เนตประเทศไทย จำกัด (มหาชน)

6. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

6.1 นายประสิทธิ์	แซ่เบ๊	ผู้ช่วยผู้บริหารฝ่ายปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่ายปส.
6.2 นายนินาท	มรุตัณฑ์	ผู้ช่วยผู้บริหารส่วนพัฒนากระบวนการด้านเทคโนโลยีสารสนเทศ / ฝ่ายพส.
6.3 นายกิตติ์ธเนศ	วงศ์ประสิทธิ์	ผู้ช่วยผู้บริหารส่วนบริการและปฏิบัติการเทคโนโลยีสารสนเทศ / ฝ่ายปส.

ผนวก 1

คุณลักษณะด้านเทคนิคขั้นต่ำและขอบเขตการดำเนินงาน

การจ้างผู้ให้บริการเช่าใช้ระบบคอมพิวเตอร์และเครือข่ายเพื่อให้บริการลูกค้า

(Managed Service for ECI Online and TBP and EXIM1)

ผู้ยื่นข้อเสนอต้องดำเนินการให้บริการ Managed Service for ECI Online and TBP and EXIM1 โดยมีคุณลักษณะด้านเทคนิคขั้นต่ำอย่างน้อยดังนี้

1. ความต้องการเฉพาะด้านระบบคอมพิวเตอร์และเครือข่าย

1.1. บริการเช่าใช้ระบบคอมพิวเตอร์และเครือข่าย ที่นำเสนอต้องสามารถให้บริการดังนี้

1.1.1. สามารถให้บริการได้อย่างต่อเนื่อง โดยมีระดับของการให้บริการ (Service Level Agreement) ไม่ต่ำกว่า 99.90% ต่อเดือน

1.1.2. ต้องไม่มีเครื่องคอมพิวเตอร์แม่ข่าย หรือระบบงานของบุคคล/นิติบุคคลอื่นที่ไม่ใช่ของธนาคารติดตั้งหรือใช้บริการร่วมอยู่ในตู้จัดเก็บอุปกรณ์คอมพิวเตอร์ (Rack) เดียวกัน และ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการกับธนาคาร (ต้อง Dedicated Hardware ให้ใช้งานเฉพาะธนาคารแต่เพียงรายเดียว)

1.1.3. ต้องมีระบบการป้องกันไวรัส (Antivirus) และระบบการป้องกันมัลแวร์ (Anti-Malware) ติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายเสมือน

1.1.4. สามารถควบคุมการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายเสมือน ผ่านช่องทาง Web Portal

1.1.5. มีช่องทางการสื่อสารกับภายนอก ซึ่งมีคุณลักษณะดังนี้

1.1.5.1. มีช่องทางการเชื่อมต่อกับระบบอินเตอร์เน็ต แบบ Domestic ที่มีขนาด 1 Gbps และต้องมีการเชื่อมต่อไปยังผู้ให้บริการโทรคมนาคม (Communication Provider) ไม่น้อยกว่า 2 ราย (Separated Media Provider) เพื่อให้ระบบงานของธนาคารสามารถให้บริการได้ตามปกติเมื่อมีเหตุขัดข้องจากผู้ให้บริการรายใดรายหนึ่ง

1.1.5.2. การเชื่อมต่อโครงข่ายเฉพาะ (Private Link) ดังนี้

1.1.5.2.1. มีช่องทางเชื่อมต่อโครงข่ายศูนย์ข้อมูลหลักกับระบบของธนาคาร ต้องมีขนาด Bandwidth ไม่น้อยกว่า 30 Mbps จำนวนไม่น้อยกว่า 2 Links รวมถึงอุปกรณ์ Router ที่ใช้สำหรับเชื่อมต่อ

1.1.5.2.2. มีช่องทางเชื่อมต่อโครงข่ายศูนย์ข้อมูลสำรองกับระบบของธนาคาร ต้องมีขนาด Bandwidth ไม่น้อยกว่า 30 Mbps จำนวนไม่น้อยกว่า 2 Links รวมถึงอุปกรณ์ Router ที่ใช้สำหรับเชื่อมต่อ

1.1.5.3. หากมีความจำเป็นต้องขยาย Bandwidth เพิ่ม ทั้ง Internet หรือ Private Link เป็นการชั่วคราว ผู้ให้บริการต้องจัดหา Bandwidth เพิ่มตามที่ธนาคารร้องขอ โดยมีอัตราค่าใช้จ่ายตามที่ได้ตกลงไว้แล้ว

1.1.6. อุปกรณ์และ/หรือระบบที่นำเสนอ ต้องมีการทำงานแบบ HA (High Availability) ที่ศูนย์ข้อมูลหลัก (Data Center)

1.1.7. ซอฟต์แวร์ Virtualization ที่ใช้งาน ต้องอยู่ใน Leader ของ Magic Quadrant Report on x86 Server Virtualization Infrastructure For 2020 เป็นอย่างน้อย

1.1.8. มีระบบการ Monitor และแจ้งเตือนสำหรับเหตุขัดข้องหรือเมื่อเกิดปัญหา (Incident) ด้วยวิธี SMS อย่างน้อยดังนี้

1.1.8.1. Network VM usage default alarm to monitor virtual machine network usage หรือ

1.1.8.2. Virtual machine memory usage Default alarm to monitor virtual machine memory usage หรือ

1.1.8.3. Virtual machine cpu usage Default alarm to monitor virtual machine cpu usage หรือ

1.1.8.4. VM State Suspend Default alarm to monitor virtual machine state suspend หรือ

1.1.8.5. VM State power off default alarm to monitor virtual machine state power off หรือ

1.1.8.6. Network VM ping status (Public IP)

1.1.9. มีระบบสำหรับการเข้าดู Performance ในส่วนของ vCPU , Memory , Storage เป็นราย VM แบบ Online (Web base) ได้

1.1.10. สามารถเก็บ Log (Event Viewer) ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เช่น Transaction Log, Access Log, Activity Log เป็นต้น โดยเพิ่มเติมจากโครงการ Managed Service for ECI Online and TBP อย่างน้อย 1 GB/Day และสามารถรองรับการขยายในอนาคตตามที่ธนาคารกำหนด

1.1.11. ต้องมีระบบสำรองและกู้คืนข้อมูลในศูนย์ข้อมูลหลัก (Data Center) โดยมีรายละเอียดดังต่อไปนี้

1.1.11.1. มีการสำรองข้อมูลที่ศูนย์ข้อมูลหลักทุกวัน โดยเก็บข้อมูลไว้ระยะเวลาไม่น้อยกว่า 7 วัน

1.1.11.2. มีการสำรองข้อมูลที่ศูนย์ข้อมูลสำรองทุกวัน โดยเก็บข้อมูลไว้ระยะเวลาไม่น้อยกว่า 7 วัน

1.1.12. กำหนดให้ระยะเวลาในการกู้คืนข้อมูล RTO (Recovery Time Objective) ต้องไม่มากกว่า 60 นาที

1.2. ความต้องการด้านคุณลักษณะเฉพาะของเครื่องคอมพิวเตอร์แม่ข่าย

1.2.1. เครื่องคอมพิวเตอร์แม่ข่ายที่นำเสนอต้องมีคุณลักษณะเฉพาะดังนี้

1.2.1.1. มีหน่วยประมวลผลกลาง (CPU) แบบ 64-bit โดยมีคุณสมบัติขั้นต่ำ CPU 2.2 GHz x 10 Core

1.2.1.2. มีหน่วยความจำหลัก (RAM) ชนิด ECC DDR4 หรือดีกว่า ขนาดรวมไม่น้อยกว่า 256 GB

1.2.1.3. มีหน่วยเก็บข้อมูล (Hard Drive) ชนิด SAS ที่มีความเร็วรอบไม่น้อยกว่า 10,000 RPM หรือ ชนิด Solid State Drive หรือดีกว่า ที่มีขนาดความจุไม่น้อยกว่า 300 GB

1.2.1.4. รองรับการทำงานในแบบ RAID level 0,1,5,6 และ 10

1.2.1.5. ต้องมีเครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่เป็น HOST มากกว่า 1 เครื่องเพื่อสามารถทำ HA ของเครื่องคอมพิวเตอร์แม่ข่าย กรณี HOST ใด HOST หนึ่งเกิดปัญหา

1.2.1.6. ใช้ VMware Hypervisor ESXi version 6.0 ขึ้นไป

1.2.1.7. สามารถทำงานแบบ Mirror Disk ได้

1.2.1.8. มีช่องเชื่อมต่อระบบเครือข่ายไม่น้อยกว่าแบบ 10/100/1000 Base-T

1.2.2. อุปกรณ์จัดเก็บข้อมูลแบบภายนอก (External Storage) ที่นำเสนอต้องมีคุณลักษณะเฉพาะดังนี้

1.2.2.1. เป็นอุปกรณ์ที่ทำหน้าที่จัดเก็บข้อมูลภายนอกแบบ SAN (Storage Area Network)

1.2.2.2. สามารถเชื่อมต่อแบบ Fiber Channel

1.2.2.3. มีช่องสัญญาณ Host Interface แบบ FC ความเร็วไม่น้อยกว่า 8 Gbps จำนวนไม่น้อยกว่า 2 ช่อง ต่อ 1 หน่วย Controller

1.2.2.4. รองรับการทำงานในแบบ RAID level 0, 1, 5, 6,(หรือเทียบเท่า 6) และ 10

1.2.2.5. สามารถเปลี่ยน Hard Drive ที่เสียได้ โดยไม่ต้องหยุดการทำงานของระบบ (Hot Plug)

1.2.2.6. มีหน่วยจัดเก็บข้อมูล (Hard Drive) ขนาดความจุไม่น้อยกว่า 10 TB (หลังการทำ RAID 5)

1.2.2.7. มีหน่วยจัดเก็บข้อมูล (Hard Drive) ชนิด SAS ที่มีความเร็วรอบไม่น้อยกว่า 10,000 RPM หรือชนิด Solid State Drive หรือดีกว่า

1.2.3. อุปกรณ์ Switch Layer 2 ที่นำเสนอต้องมีคุณสมบัติดังนี้

มีช่องเชื่อมต่อระบบเครือข่าย (Network Interface) แบบ 10/100/1000 Base-T จำนวนไม่น้อยกว่า 24 ช่อง

1.2.4. Firewall ที่นำเสนอต้องมีคุณลักษณะเฉพาะดังนี้

1.2.4.1. มีช่องทางการเชื่อมต่อระบบเครือข่าย (Network Interface) รองรับขนาดไม่น้อยกว่า 1 Gbps จำนวนไม่น้อยกว่า 8 ช่องทาง

1.2.4.2. เป็น Firewall แบบ Stateful Inspection Firewall

1.2.4.3. รองรับ Layer 7 (User – Identity) Firewall

1.2.4.4. มี Throughput (UDP) ไม่น้อยกว่า 8,000 Mbps

1.2.4.5. มี Throughput (TCP) ไม่น้อยกว่า 5,000 Mbps

1.2.4.6. Concurrent Sessions ไม่น้อยกว่า 3,000,000 sessions

1.2.5. Web Application Firewall ที่นำเสนอต้องมีคุณลักษณะเฉพาะดังนี้

1.2.5.1. ทำการวิเคราะห์และป้องกันภัยคุกคาม Web Application

1.2.5.2. มี Feature การป้องกันที่มีขนาด Throughput ไม่น้อยกว่า 700 Mbps

1.2.5.3. รองรับการใช้งานโปรโตคอล HTTP และ HTTPS ได้เป็นอย่างน้อย

1.2.5.4. สามารถป้องกันการโจมตีเหล่านี้ได้เป็นอย่างน้อย Cross Site Scripting (XSS) , SQL Injection , Session Hijacking , Buffer Overflow , Cookie Poisoning , Malicious and Illegal Encoding , Directory Traversal, Sensitive data exposure, Insecure Direct Object References, Missing Function Level Access Control

1.2.5.5. สามารถทำการ Updates Signature ได้ทั้งแบบ Manual หรือแบบ Automatic

1.2.6. ระบบป้องกันการบุกรุกด้านเครือข่าย (Intrusion Prevention System : IPS) ที่นำเสนอต้องมีคุณลักษณะเฉพาะดังนี้

1.2.6.1. มี IPS Throughput ไม่น้อยกว่า 500 Mbps

1.2.6.2. Concurrent Connection ไม่น้อยกว่า 50,000 Concurrent

1.2.6.3. สามารถป้องกันการบุกรุก เช่น Worm Trojan Phishing Spyware Botnet DOS DDOS Backdoor เป็นต้น

1.2.6.4. สามารถป้องกันการโจมตีแบบ Zeroday

1.2.6.5. สามารถตรวจสอบและป้องกันการโจมตีที่มีการเข้ารหัสด้วย SSL decryption ได้ โดยรองรับ SSL Throughput ได้ไม่น้อยกว่า 500 Mbps หรือสามารถเสนออุปกรณ์ภายนอกในการทำ SSL Decryption เพิ่มเติมได้

1.2.6.6. สามารถกำหนดรูปแบบการป้องกันการโจมตีแบบอัตโนมัติหรือ Manual ได้

1.2.7. DataBase Firewall ที่นำเสนอต้องมีคุณลักษณะเฉพาะดังนี้

1.2.7.1. สามารถใช้งานร่วมกับฐานข้อมูลชนิด RDBMS, Data Warehouses, Big Data Platforms และ Mainframe Databases ได้เป็นอย่างน้อย

1.2.7.2. สามารถป้องกันการโจมตีเหล่านี้ได้เป็นอย่างน้อย SQL injection, DoS

1.2.7.3. สามารถระบุพฤติกรรมที่น่าสงสัย และระงับการทำงานของพฤติกรรมที่ตรวจพบได้

1.2.7.4. สามารถป้องกัน และแจ้งเตือนการโจมตีฐานข้อมูล หรือการเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาต แบบ Real-Time

1.2.7.5. มี IPS Throughput อย่างน้อย 500 Mbps

1.3. ความต้องการด้านสถานที่ตั้ง และอุปกรณ์ ของศูนย์ข้อมูลหลัก (Data Center)

1.3.1. ต้องมีระยะห่างจากศูนย์ข้อมูลสำรองฉุกเฉิน ไม่น้อยกว่า 30 กิโลเมตร

1.3.2. ต้องมีเครื่องกำเนิดไฟฟ้า (Generator) ที่สามารถทำงานได้โดยอัตโนมัติ มีระบบป้องกันไฟฟ้ากระชาก (Surge Protection) ก่อนการเข้าถึงระบบไฟฟ้าของ Data Center และเครื่องกำเนิดไฟฟ้าต้องมีแหล่งจ่ายไฟฟ้าฉุกเฉิน (Emergency Power Supply) รวมทั้งต้องสามารถจ่ายไฟฟ้าสำรองได้ต่อเนื่องไม่ต่ำกว่า 2 ชั่วโมง

1.3.3. ต้องมีระบบสำรองไฟฟ้าแบบต่อเนื่อง (UPS) สำหรับ Backup Time Full Load ไม่ต่ำกว่า 10 นาที

1.3.4. ต้องได้รับการรับรองมาตรฐาน ระดับสากล มี Certificate มาตรฐาน ISO : 27001: 2013

1.3.5. ต้องมีระบบการป้องกันและตรวจสอบสิทธิ์ผู้ไม่เกี่ยวข้องเข้าไปในสถานที่ที่ให้บริการ Manage Hosting ของธนาคาร ซึ่งอาจก่อให้เกิดความเสียหายกับธนาคาร

1.4. ความต้องการด้านสถานที่ตั้ง และอุปกรณ์ ของศูนย์ข้อมูลสำรองฉุกเฉิน (Backup Data Center)

1.4.1. ต้องมีเครื่องกำเนิดไฟฟ้า (Generator) ที่สามารถทำงานได้โดยอัตโนมัติ มีระบบป้องกันไฟฟ้ากระชาก (Surge Protection) ก่อนการเข้าถึงระบบไฟฟ้าของ Backup Data Center และเครื่องกำเนิดไฟฟ้าต้องมีแหล่งจ่ายไฟฟ้าฉุกเฉิน (Emergency Power Supply) รวมทั้งต้องสามารถจ่ายไฟฟ้าสำรองได้ต่อเนื่องไม่ต่ำกว่า 2 ชั่วโมง

1.4.2. ต้องมีระบบสำรองไฟฟ้าแบบต่อเนื่อง (UPS) สำหรับ Backup Time Full Load ไม่ต่ำกว่า 10 นาที

1.4.3. ต้องได้รับการรับรองมาตรฐาน ระดับสากล มี Certificate มาตรฐาน ISO : 27001:2013

1.4.4. ต้องมีระบบการป้องกันและตรวจสอบสิทธิ์ผู้ไม่เกี่ยวข้องเข้าไปในสถานที่ที่ให้บริการเช่าใช้ระบบคอมพิวเตอร์ และเครือข่ายของธนาคาร ซึ่งอาจก่อให้เกิดความเสียหายกับธนาคาร

1.5. โปรแกรม (Software) ที่เกี่ยวข้องกับการให้บริการ จะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย โดยไม่ละเมิดสิทธิ์ของผู้อื่น รวมทั้งรับผิดชอบในกรณีที่มีการกล่าวหา ฟ้องร้อง หรือเรียกค่าเสียหายใดๆ จากเจ้าของลิขสิทธิ์หรือผู้เรียกร้องอื่นใด

1.6. จัดให้มีบริการ Backup as a services โดยคิดค่าบริการตามจำนวนขนาดพื้นที่ ของ Disk ที่มีการจัดเก็บต่อ Server เริ่มต้นที่ 50 GB จำนวน 1 Server และสามารถเพิ่มจำนวน Server และหรือขนาดพื้นที่ในการจัดเก็บได้ตามที่ธนาคารร้องขอ เมื่อธนาคารมีความต้องการใช้งานเพิ่มขึ้น

1.7. ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ตั้งอยู่ในประเทศไทย อย่างน้อย 3 ศูนย์ข้อมูล มีระยะทางห่างกันอย่างน้อย 100 กิโลเมตร จำนวน 1 ศูนย์ข้อมูล และ Data Center ทุกแห่ง ต้องมีระบบเครือข่ายสื่อสารหลัก ที่เชื่อมเป็นเครือข่ายเดียวกันด้วยเทคโนโลยีบริหารจัดการระบบเครือข่าย (Software Define Infrastructure: SDI) เพื่อรองรับแผนการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Planning: BCP)

1.8. มีวงจรเชื่อมโยงกับศูนย์แลกเปลี่ยนข้อมูลอินเทอร์เน็ตภายในประเทศ (National Internet Exchange: NIX) ไม่น้อยกว่าน้อย 5 แห่ง และวงจรเชื่อมโยงกับศูนย์แลกเปลี่ยนข้อมูลอินเทอร์เน็ตเพื่อออกต่างประเทศ (International Internet Gateway : IIG) ไม่น้อยกว่าน้อย 3 แห่ง ในกรณีที่ Gateway ใด Gateway หนึ่งขัดข้องก็สามารถใช้งานอีก Gateway ได้โดยอัตโนมัติ

1.9. ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center หรือบริการระบบคลาวด์ (Cloud Computing) ได้รับการรับรองมาตรฐาน ดังต่อไปนี้

1) มาตรฐานการบริหารการรักษาความความปลอดภัย ISO/IEC 27001
2) มาตรฐานการจัดการบริการด้านไอที ISO/IEC 20000-1
3) มาตรฐานการบริหารความต่อเนื่องทางธุรกิจ ISO 22301
4) มาตรฐานความปลอดภัยสำหรับระบบคลาวด์ CSA-STAR Cloud Security (CSA STAR)
5) มาตรฐานการบริการศูนย์คอมพิวเตอร์ในระดับ Tier3 โดยแสดงเอกสารได้รับการรับรอง TIA-942 หรือ Uptime institute

1.10. ที่ตั้งของศูนย์ข้อมูลคอมพิวเตอร์และระบบสนับสนุนต่างๆ (Data Center & Facilities) จะต้องมีความมั่นคงปลอดภัย อย่างน้อยดังนี้

1) ไม่มีความเสี่ยงจากภัยธรรมชาติ อันได้แก่ ภัยจากอุทกภัย โดยต้องเป็นพื้นที่อยู่สูงกว่าระดับน้ำทะเลอย่างน้อย 40 เมตร
2) ตั้งห่างจากสิ่งปลูกสร้างที่มีความเสี่ยงจากภัยคุกคามทางกายภาพ อันได้แก่ สนามบิน โรงกลั่นน้ำมันหรือสถานีน้ำมัน โรงงานเคมี และโรงกำจัดขยะมีพิษไม่น้อยกว่า 2 กิโลเมตร

2. ความต้องการด้าน VM (Virtual Machine) ต้องรองรับการสร้าง VM ตามที่ธนาคารกำหนด และรองรับการขยาย Capaicity ของ VM Guest ในอนาคต ด้วย Growth Rate 20% ต่อปี ดังนี้

ระบบ ECI Online

No.	Environment	Server Type	VM	CPU	Memory	Total Harddisk	Software requirement
1	ECI_APP1WEB1_DEV	Web1 Server	1	4	8	150 GB	Windows Server 2016
2	ECI_DB1_DEV	DB1 Server	1	4	8	200 GB	Windows Server 2016
3	ECI_AD1_DEV	AD1 Server	1	2	4	150 GB	Windows Server 2016
4	ECI_DB1_DEV	DB1 Server	1	6	12	150 GB	Windows Server 2016
5	ECI_DB2_PRD	DB2 Server	1	6	12	700 GB	Windows Server 2016
6	EXIM_APP1_PRD	APP1 Server	1	4	8	150 GB	Windows Server 2016
7	EXIM_APP2_PRD	APP2 Server	1	4	8	200 GB	Windows Server 2016
8	EXIM_WEB1_PRD	WEB1 Server	1	4	8	200 GB	Windows Server 2016

ระบบ EXIM_APP1_UAT

No.	Environment	Server Type	VM	CPU	Memory	Total Harddisk	Software requirement
1	EXIM_TBP_APP1	Web1 Server	1	4	8	150 GB	Windows Server 2016
2	EXIM_TBP_WEB1	DB1 Server	1	4	8	200 GB	Windows Server 2016
3	TBP_FS01_DEV	AD1 Server	1	2	4	150 GB	Windows Server 2016
4	TBP_APP01_PRD	DB1 Server	1	6	12	150 GB	Windows Server 2016

ระบบ TBP

No.	Environment	Server Type	VM	CPU	Memory	Total Harddisk	Software requirement
1	EXIM_TBP_APP1	APP1 Server	1	4	8	150 GB	Windows Server 2016
2	EXIM_TBP_WEB1	WEB1 Server	1	4	8	150 GB	Windows Server 2016
3	TBP_FS01_DEV	FS1 Server	1	4	8	150 GB	Windows Server 2016
4	TBP_APP01_PRD	APP1 Server	1	4	16	40 GB	Windows Server 2016
5	TBP_APP02_PRD	APP2 Server	1	4	16	40 GB	Windows Server 2016
6	EXIM-DFS-01	DFS1 Server	1	2	4	300 GB	Windows Server 2016
7	EXIM-DFS-02	DFS2 Server	1	2	4	300 GB	Windows Server 2016
8	TBP_WEB01_PRD	WEB1 Server	1	2	4	40 GB	Windows Server 2016
9	TBP_WEB02_PRD	WEB2 Server	1	2	4	40 GB	Windows Server 2016

ระบบ I-Sprint Server

No.	Environment	Server Type	VM	CPU	Memory	Total Harddisk	Software requirement
1	UAS_DEV	UAS_DEV Server	1	4	8	40 GB	Windows Server 2016
2	DB_DEV	DB_DEV Server	1	4	4	40 GB	Windows Server 2016, MS SQL Server 2016
3	UAS_PRD	UAS Server	1	4	8	40 GB	Windows Server 2016
4	DB_PRD	DB Server	1	4	8	40 GB	Windows Server 2016
5	SIT_UAT	SIT_UAT Server	1	4	8	40 GB	Windows Server 2016
6	DB_UAT	DB Server	1	4	4	40 GB	Windows Server 2016, MS SQL Server 2016

ระบบจัดเก็บข้อมูล (Data Storage)

No.	Environment	Type	Total Space
1	PRD	Data Storage	1000 GB
2	PRD	Data Storage	200 GB

ระบบ EXIM1

No.	Environment	Server Type	VM	CPU	Memory	Total Harddisk	Software requirement
1	EXIM1Web01UAT	UAS_DEV Server	1	4	8	100 GB	Windows Server 2019
2	EXIM1Web02UAT	DB_DEV Server	1	4	8	100 GB	Windows Server 2019
3	EXIM1App01UAT	UAS Server	1	4	8	50 GB	Windows Server 2019
4	EXIM1App02UAT	DB Server	1	4	8	50 GB	Windows Server 2019
5	EXIM1Auth1UAT	SIT_UAT Server	1	4	8	50 GB	Windows Server 2019
6	EXIM1Auth2UAT	DB Server	1	4	4	50 GB	Windows Server 2019
7	EXIM1FS01DEVUAT	FS1 Server	1	2	4	203 GB	Windows Server 2019
8	EXIM1FS02DEVUAT	FS2 Server	1	2	4	203 GB	Windows Server 2019
9	EXIM1Web01PRD	Web1 Server	1	4	16	100 GB	Windows Server 2019
10	EXIM1Web02PRD	Web2 Server	1	4	16	100 GB	Windows Server 2019
11	EXIM1App01PRD	APP1 Server	1	4	16	100 GB	Windows Server 2019
12	EXIM1App02PRD	APP2 Server	1	4	16	100 GB	Windows Server 2019
13	EXIM1Auth1PRD	Auth1 Server	1	4	16	100 GB	Windows Server 2019
14	EXIM1Auth2PRD	Auth1 Server	1	4	16	100 GB	Windows Server 2019

2.1 สามารถรองรับการใช้งานผ่านระบบเครือข่ายแบบ IP Address : 1 IP/VM

3. ความต้องการเฉพาะด้านการพิสูจน์ตัวตน (Authentication Service)

3.1. คุณลักษณะของซอฟแวร์ด้านการพิสูจน์ตัวตน (Authentication)

3.1.1. สามารถทำ Two-Factor Authentication อย่างน้อย 1 ระบบ ดังนี้

3.1.1.1. RADIUS หรือ

3.1.1.2. SMAL หรือ

3.1.1.3. Agent หรือ

3.1.1.4. API

3.1.2. สามารถบริหารจัดการอุปกรณ์ Two-Factor Authenticator อย่างน้อยดังนี้

3.1.1.1. Hardware Token OTP (One-Time Password) แบบ Time-based และ Event-Based หรือ

3.1.2.2. Hardware Token OTP (One-Time Password) แบบ Challenge-Reponses หรือ

3.1.2.3. Moblie Token สำหรับ IOS และ Android หรือ

3.1.2.4. SMS Token หรือ

3.1.2.5. e-Mail Token หรือ

3.1.2.6. สามารถทำงานกับ Hardware Token OTP ของยี่ห้ออื่นได้

3.1.3. มีระบบ SMS Gateway เพื่อจัดส่ง OTP (ONE-Time Password) แบบ SMS ให้กับผู้ใช้งานเพื่อทำ Two-Factor Authenticator

3.1.4 สามารถรองรับการใช้ Soft Token ที่ได้รับมาตรฐานความปลอดภัย FIPS 140-2 ขึ้นไป โดยต้องจำนวนไม่ต่ำกว่า 1500 Username

3.1.5. สามารถจัดการข้อมูลผู้ใช้งานของธนาคารอย่างน้อยดังนี้

3.1.5.1. Microsoft Active Directory (AD) หรือ

3.1.5.2. Open Database Connectivity (ODBC) หรือ

3.1.5.3. Microsoft SQL Server (SQL) หรือ

3.1.5.4. Lightweight Directory Access Protocol (LDAP)

3.1.6. เป็นสถาปัตยกรรมแบบ Multi-Tier หรือ Multi-Tenant และรองรับการทำงานกับ Multi-Domain ได้ รวมทั้งต้องไม่จำกัดจำนวน Token

3.1.7. รองรับการทำงานสำหรับอุปกรณ์ Token ดังนี้

3.1.7.1. การจัดเตรียมอุปกรณ์ Token ให้กับผู้ใช้งาน (Provisioning)

3.1.7.2. การจัดการอุปกรณ์ Token ให้กับผู้ใช้งาน (Management)

3.1.7.3. การยกเลิกการใช้งานอุปกรณ์ Token ให้กับผู้ใช้งาน (De-Reporting)

3.1.7.4. การจัดทำรายงานสำหรับอุปกรณ์ Token ของผู้ใช้งาน (Reporting)

3.1.7.5 การเตือนภัยสำหรับอุปกรณ์ Token ของผู้ใช้งาน (Alert)

3.1.7.6 การจัดการอุปกรณ์ Token กรณีสูญหาย (Lost Token)

3.1.8. มีหน้าเว็บไซต์บริการตนเองสำหรับผู้ใช้งาน (Admin Self-Service Portal) เพื่อใช้งาน ดังนี้

3.1.8.1. การลงทะเบียนด้วยต้นเอง (Self-Registration)

3.1.8.2. การเปลี่ยนรหัส (Change Password)

3.1.8.3. การปลดล็อก (Unlock Token)

3.1.8.4. การซิงค์อีกครั้ง (Resync Token)

3.1.9. มี intergrations Guide อย่างน้อยดังนี้

3.1.9.1. ระบบ 2 Factor Authentications กับ VPN หรือ

3.1.9.2. ระบบ 2 Factor Authentications กับ Manage Hosting หรือ

3.1.9.3. ระบบ 2 Factor Authentications กับ ระบบเครือข่าย หรือ

3.1.9.4. ระบบ 2 Factor Authentications กับ Web Portal

3.2 โปรแกรมอื่นๆ ที่เกี่ยวข้องกับการให้บริการ จะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย โดยไม่ละเมิดสิทธิ์ของผู้อื่น รวมทั้งรับผิดชอบในกรณีที่มีการกล่าวหา ฟ้องร้อง หรือเรียกค่าเสียหายใดๆ จากเจ้าของลิขสิทธิ์หรือผู้เรียกร้องอื่นใด

4. ขอบเขตงาน

ผู้ยื่นข้อเสนอต้องดำเนินการตามขอบเขตงานที่กำหนดอย่างน้อยดังต่อไปนี้

4.1. ด้านการติดตั้ง การทดสอบ และการดำเนินการอื่นๆ

4.1.1. ต้องดำเนินการติดตั้ง ปรับตั้งค่าต่างๆ และทดสอบความถูกต้องของการให้บริการ ร่วมกับธนาคารให้เรียบร้อยก่อนการใช้งาน

4.1.2. ต้องให้คำแนะนำในการประยุกต์ใช้ และการดำเนินงานอื่น ๆ ที่จำเป็นเพื่อให้ธนาคารสามารถใช้บริการได้อย่างมีประสิทธิภาพ

4.1.3. ต้องจัดให้มีบุคลากรที่จะให้การสนับสนุนธนาคารในระหว่างดำเนินโครงการ จนแล้วเสร็จตามระยะเวลาที่กำหนด

4.1.4. ต้องติดตั้งระบบและทดสอบความถูกต้องของระบบงาน รวมทั้งสนับสนุนให้ธนาคารสามารถใช้งานระบบได้อย่างมีประสิทธิภาพ

4.1.5. เมื่อสิ้นสุดการใช้บริการฯ หรือมีการยกเลิกการใช้บริการต้องส่งคืน และทำลายข้อมูล ผู้ใช้บริการของธนาคาร และข้อมูลของธนาคารทั้งหมด ที่ผู้ให้บริการถือครองอยู่

4.2. ด้านเอกสาร

ต้องจัดทำเอกสารส่งมอบเป็นภาษาไทย รวมทั้งจัดทำข้อมูลในรูปแบบอิเล็กทรอนิกส์ (Soft File) และจัดส่งทางจดหมายอิเล็กทรอนิกส์ จำนวนอย่างละ 1 ชุด ดังนี้

4.2.1. จัดทำแผนการดำเนินงานโดยละเอียดตั้งแต่เริ่มดำเนินการจนแล้วเสร็จประกอบด้วยตารางการปฏิบัติงาน ขั้นตอนในการดำเนินงาน/ปฏิบัติงาน ผู้รับผิดชอบงานแต่ละขั้นตอน ผลงานที่ส่งมอบ ระยะเวลาที่ใช้ในแต่ละขั้นตอน ในรูปแบบ Gantt chart เพื่อใช้ในการบริหารและติดตามผลการดำเนินงาน

4.2.2. จัดทำรายงานสรุปรายละเอียดและจำนวนโปรแกรมพร้อมอุปกรณ์ที่ใช้ในโครงการทั้งหมด

4.2.3. จัดทำหนังสือยืนยันการให้บริการเช่าใช้ระบบคอมพิวเตอร์และเครือข่ายเพื่อให้บริการลูกค้า (Managed Service for ECI Online and TBP and EXIM1)

4.2.4. จัดทำเอกสารแสดงรายละเอียดสถานที่ติดตั้ง Data center พร้อมเบอร์ติดต่อ Call Center

4.2.5. จัดทำ System Architecture Diagram ที่ให้บริการสำหรับธนาคาร

4.2.6. จัดทำเอกสารแสดงกระบวนการจัดการ (Incident Work Flow) ตั้งแต่ได้รับแจ้งปัญหา ตรวจสอบปัญหา แก้ไขปัญหา และสรุปผลที่เป็นลำดับขั้นตอนที่ชัดเจน โดยต้องจัดทำรายละเอียดและขั้นตอนการแก้ไขปัญหา หรือเหตุขัดข้อง หรือความชำรุดบกพร่องของบริการ โดยละเอียดให้แก่ธนาคาร

4.2.7. จัดทำคู่มืออย่างน้อยดังนี้

4.2.7.1. คู่มือการกำหนดค่าในระบบ (System Configuration)

4.2.7.2. คู่มือการใช้งานสำหรับผู้ดูแลระบบ (Admin Manual)

4.2.7.3. คู่มือการใช้งานระบบ (User Manual)

5. การให้บริการสนับสนุนของบริการตลอดระยะเวลาการใช้บริการ (Support)

ผู้ยื่นข้อเสนอที่ได้รับคัดเลือกจะต้องให้บริการสนับสนุนธนาคารตลอดระยะเวลาการใช้บริการ เป็นระยะเวลา 1 ปี ตั้งแต่วันที่ 1 มิถุนายน 2566 ถึงวันที่ 31 พฤษภาคม 2567 โดยมีรายละเอียดดังนี้

5.1. ต้องจัดให้มีเจ้าหน้าที่ประสานงานที่มีความเชี่ยวชาญพร้อมเบอร์โทรศัพท์ รวมถึงช่องทางอื่น เพื่อบริการให้คำปรึกษา ตอบข้อซักถาม และให้ความช่วยเหลือในการแก้ไขปัญหาต่างๆ ได้ทุกวันตลอด 24 ชั่วโมง โดยผู้ให้บริการต้องแก้ไขปัญหาในส่วนของการให้บริการ Managed Service for ECI Online and TBP

and EXIM1 ให้สามารถใช้งานได้เป็นปกติภายใน 1 ชั่วโมง นับจากได้รับแจ้งเหตุขัดข้อง หรือความชำรุดบกพร่องจากธนาคาร

5.2. ต้องจัดทำแผนบริหารจัดการเหตุการณ์ไม่ปกติ (Incident Management) เพื่อรับมือในกรณีที่เกิดเหตุการณ์ไม่ปกติกับระบบที่ให้บริการธนาคารอยู่

5.3. ต้องจัดให้มีเจ้าหน้าที่ที่มีความเชี่ยวชาญเพื่อดูแลรักษาระบบทั้งหมดที่เกี่ยวข้องในศูนย์ข้อมูลหลักให้พร้อมในการทำงานตลอดเวลา รวมทั้งคอยตรวจสอบการทำงานของระบบ Web Server, Application Server และ Database Server พร้อมแจ้งเตือนลูกค้าและแก้ไขปัญหาทุกวัน ตลอด 24 ชั่วโมง

5.4. ต้องจัดทำรายละเอียดและขั้นตอนการแก้ไขปัญหาเหตุขัดข้อง และ/หรือความชำรุดบกพร่องอย่างละเอียดให้แก่ธนาคารภายใน 5 วัน นับถัดจากวันที่ดำเนินการแก้ไขแล้วเสร็จ

5.5. กรณีมีการปรับปรุงเปลี่ยนแปลงอุปกรณ์ ผู้ให้บริการต้องจัดหาอุปกรณ์ที่มีคุณลักษณะเทียบเท่าหรือดีกว่าอุปกรณ์ที่ชำรุดบกพร่องให้ธนาคารใช้งาน โดยไม่คิดค่าใช้จ่ายใดๆ โดยจะต้องแจ้งให้ธนาคารทราบล่วงหน้าไม่น้อยกว่า 10 วัน ก่อนดำเนินการเปลี่ยนแปลงอุปกรณ์

5.6. กรณีมีการปรับปรุงเปลี่ยนแปลงแก้ไขระบบงานหรืออุปกรณ์ ผู้ให้บริการต้องมีกระบวนการควบคุมการเปลี่ยนแปลง (Change Management) โดยต้องแจ้งให้ธนาคารทราบเป็นลายลักษณ์ล่วงหน้าไม่น้อยกว่า 15 วัน ก่อนดำเนินการแก้ไขระบบงานหรืออุปกรณ์

5.7. ต้องจัดทำรายงานสรุปรายละเอียดระบบงานหรืออุปกรณ์ที่ปรับปรุงเปลี่ยนแปลงทั้งหมดส่งให้ธนาคารภายใน 15 วัน นับถัดจากวันที่ดำเนินการปรับปรุงเปลี่ยนแปลงแล้วเสร็จ

5.8. ต้องทำการทดสอบแผนการกู้คืนข้อมูลที่ศูนย์ข้อมูลสำรอง (DR) และจัดทำรายงานผลการทดสอบระบบการกู้คืนข้อมูลของผู้ให้บริการให้ธนาคารภายใน 30 วัน หลังจากทำการทดสอบเสร็จสิ้น อย่างน้อยปีละ 1 ครั้ง และให้มีเจ้าหน้าที่ของธนาคารเข้าไปร่วมการทดสอบการกู้คืนข้อมูล

5.9. ต้องนำส่ง File Backup (vmdk) ให้กับธนาคารภายใน 10 วัน นับจากวันที่ธนาคารร้องขอ

5.10. ต้องจัดทำรายงาน Performance Report ในส่วนของ vCPU, Memory, Storage เป็นราย VM ทุกสิ้นเดือนให้กับธนาคาร ภายใน 10 วัน นับถัดจากวันสิ้นเดือน

5.11. ต้องจัดทำรายงานความพร้อมใช้ระบบ (Service Availability Report) ทุกสิ้นเดือนให้กับธนาคาร ภายใน 10 วัน นับถัดจากวันสิ้นเดือน

5.12. ต้องจัดทำรายงานผลภัยคุกคามทุกสิ้นเดือนให้กับธนาคาร ภายใน 10 วัน นับถัดจากวันสิ้นเดือน

5.13. ต้องจัดทำรายงานการวิเคราะห์ Log ดังต่อไปนี้ Security Log,Traffic Log, Access Log, Audit Log เป็นรายเดือนให้กับธนาคาร ภายใน 10 วัน นับถัดจากวันสิ้นเดือน

5.14. ต้องทำ Preventive Maintenance (PM) เป็นรายไตรมาส และจัดทำรายงานแจ้งผลให้ธนาคาร ภายใน 10 วัน นับถัดจากวันที่เข้าให้บริการตรวจสอบและบำรุงรักษาดังนี้

- ครั้งที่ 1 ภายในเดือนสิงหาคม 2566
- ครั้งที่ 2 ภายในเดือนพฤษจิกายน 2566
- ครั้งที่ 3 ภายในเดือนกุมภาพันธ์ 2567
- ครั้งที่ 4 ภายในเดือนพฤษภาคม 2567

5.15. กรณีต้องการปิดปรับปรุงระบบจะต้องแจ้งให้ธนาคารทราบล่วงหน้าไม่น้อยกว่า 15 วัน ก่อนดำเนินการปิดปรับปรุง

5.16. กรณีธนาคารพบช่องโหว่ของระบบเครือข่ายการสื่อสารและระบบคอมพิวเตอร์ ผู้ยื่นข้อเสนอต้องดำเนินการแก้ไขเพื่อปิดช่องโหว่ดังกล่าวและจัดส่งรายงานการแก้ไขให้ธนาคารภายในระยะเวลาที่กำหนดตามระดับความรุนแรง ดังนี้

ระดับความรุนแรง	ระยะเวลาดำเนินการแก้ไขและจัดส่งรายงาน นับถัดจากวันที่ธนาคารแจ้งให้ดำเนินการแก้ไข
สูง (High)	7 วัน
ปานกลาง (Medium)	15 วัน
ต่ำ (Low)	45 วัน

หมายเหตุ : ระดับความรุนแรงจะอ้างอิงตามรายงานการประเมินช่องโหว่ที่ธนาคารได้รับจากผู้ให้บริการประเมินช่องโหว่ฯ

6. การ Upgrade ระบบ

ในระหว่างดำเนินการให้บริการ หากมีโปรแกรม (Software) ที่เกี่ยวข้องกับการให้บริการ มีการออก Patch หรือ Version ใหม่ ผู้ให้บริการต้องแจ้งรายละเอียดการเปลี่ยนแปลงและผลกระทบที่เกี่ยวข้อง ให้ธนาคารทราบเพื่อใช้เป็นข้อมูลการตัดสินใจ ทั้งนี้ หากธนาคารประสงค์จะทำการ Upgrade โปรแกรม (Software) ผู้ให้บริการจะต้องดำเนินการให้โดยไม่คิดค่าใช้จ่ายใดๆ เพิ่มเติมจากธนาคาร