เอกสารแนบ

ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและราคากลาง (ราคาอ้างอิง)

ในการจัดซื้อจัดจ้างที่มิใช่งานก่อสร้าง

1. ชื่อโครงการ **การจัดหาผู้ให้บริการ Cloud Service สำหรับระบบประกันการส่งออกผ่านช่องทาง Online**
/หน่วยงานเจ้าของโครงการ **ฝ่ายพัฒนาองค์กร**

2. วงเงินงบประมาณที่ได้รับจัดสรร 10,000,000.- **บาท (สิบล้านบาทถ้วน)**

3. วันที่กำหนดราคากลาง (ราคาอ้างอิง) ..... 21 ส.ค. 2560 .....
เป็นเงิน 9,999,792.- **บาท (เก้าล้านเก้าแสนเก้าหมื่นเก้าพันเจ็ดร้อยเก้าสิบสองบาทถ้วน)**
ราคา/หน่วย (ถ้ามี) - บาท

4. แหล่งที่มาของราคากลาง (ราคาอ้างอิง)
บริษัท อินเทอร์เน็ต ประเทศไทย จำกัด (มหาชน)

5. รายชื่อเจ้าหน้าที่ผู้กำหนดราคากลาง (ราคาอ้างอิง) ทุกคน

5.1 นายอภิรัฐ	แสงธงทอง	ผู้ช่วยผู้บริหารฝ่ายรับประกันการส่งออก
5.2 นางสาวเจียมใจ	ประทุมมา	ผู้จัดการส่วน ทีมปรับปรุงพัฒนาและออกแบบกระบวนการทำงานและทีมเทคโนโลยีสารสนเทศ / คณะทำงานขับเคลื่อนการเปลี่ยนแปลง
5.3 นายสวัสดิ์	โชติรสานนท์	ผู้จัดการส่วน ทีมปรับปรุงพัฒนาและออกแบบกระบวนการทำงานและทีมเทคโนโลยีสารสนเทศ / คณะทำงานขับเคลื่อนการเปลี่ยนแปลง

ผนวก 1

คุณลักษณะด้านเทคนิคขั้นต่ำและขอบเขตการดำเนินงาน

การจัดหาผู้ให้บริการ Cloud Service Authentication Service และ Data Encryption

---

1. **ความต้องการเฉพาะด้าน Cloud Service**

ผู้เสนอราคาต้องดำเนินการให้บริการ Cloud Service สำหรับระบบประกันการส่งออกผ่านช่องทาง Online ได้อย่างมีประสิทธิภาพ มีความคล่องตัว รวดเร็ว ทันสมัย และเป็นไปตามมาตรฐานสากล อย่างน้อยดังนี้

1.1. บริการ Cloud Service ที่นำเสนอต้องสามารถให้บริการดังนี้

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

1.1.2. ต้องไม่มีเครื่องคอมพิวเตอร์แม่ข่าย หรือระบบงานของบุคคล/นิติบุคคลอื่นที่ไม่ใช่ของธนาคาร ติดตั้งหรือใช้บริการร่วมอยู่ใน Cloud Service ของธนาคาร (ต้อง Dedicated Hardware ให้ใช้งานเฉพาะธนาคารแต่เพียงรายเดียว)

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

1.1.4. สามารถควบคุมการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายเสมือน ผ่านช่องทาง Web Portal และมีช่องทางการสื่อสารกับภายนอก ดังนี้

1.1.4.1. มีช่องทางการเชื่อมต่อกับระบบอินเตอร์เน็ต แบบ Domestic ที่มีขนาด Bandwidth ไม่น้อยกว่า 1 Gbps และต้องมีการเชื่อมต่อไปยังผู้ให้บริการโทรคมนาคม (Communication Provider) ไม่น้อยกว่า 2 ราย (Separated Media Provider) เพื่อให้ระบบงานของธนาคารสามารถให้บริการได้ตามปกติ เมื่อมีเหตุขัดข้องจากผู้ให้บริการรายใดรายหนึ่ง

1.1.4.2. การเชื่อมต่อโครงข่ายเฉพาะ (Private Link)

1.1.4.2.1. มีช่องทางเชื่อมต่อโครงข่ายศูนย์ข้อมูลหลักกับระบบของธนาคาร ต้องมีขนาด Bandwidth ไม่น้อยกว่า 10 Mbps จำนวนไม่น้อยกว่า 2 Links รวมถึงเสนอ Router ที่ใช้สำหรับเชื่อมต่อ

1.1.4.2.2. มีช่องทางเชื่อมต่อโครงข่ายศูนย์ข้อมูลสำรองกับระบบของธนาคาร ต้องมีขนาด Bandwidth ไม่น้อยกว่า 10 Mbps จำนวนไม่น้อยกว่า 2 Links รวมถึงเสนอ Router ที่ใช้สำหรับเชื่อมต่อ

1.1.5. อุปกรณ์หรือระบบที่นำเสนอ ต้องมีการทำงานแบบ HA (High Availability) ที่ศูนย์ข้อมูลหลัก (Data Center)

1.1.6. ซอฟต์แวร์ Virtualize ที่ใช้งานต้องอยู่ใน Leader ของ Magic Quadrant Report on x86 Server Virtualization Infrastructure For 2016 เป็นอย่างน้อย

1.1.7. มีระบบการ Monitor และแจ้งเตือนสำหรับเหตุขัดข้องหรือเมื่อเกิดปัญหา (Incident) ด้วยวิธี SMS อย่างน้อยดังนี้

1.1.7.1. Network VM usage default alarm to monitor virtual machine network uasge

1.1.7.2. Virtual machine memory usage Default alarm to monitor virtual machine memory usage

1.1.7.3. Virtual machine cpu usage Default alarm to monitor virtual machine cpu usage

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

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

1.1.7.6. Network VM ping status (Public IP)

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

1.1.9. สามารถเก็บ Log (Event Viewer) ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย เช่น Transaction Log, Access Log, Activity Log เป็นต้น

1.1.10. ต้องมีระบบสำรองและกู้คืนข้อมูลในศูนย์ข้อมูลหลัก (Data Center) โดยมีรายละเอียดดังต่อไปนี้

1.1.10.1. มีการสำรองข้อมูลที่ศูนย์ข้อมูลหลักทุกวัน โดยเก็บข้อมูลไว้ระยะเวลาไม่น้อยกว่า 4 วัน

1.1.10.2. มีการสำรองข้อมูลที่ศูนย์ข้อมูลสำรองทุกวัน โดยเก็บข้อมูลไว้ระยะเวลาไม่น้อยกว่า 7 วัน

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

1.2. ความต้องการด้านคุณสมบัติเฉพาะของ Cloud Service

1.2.1. เครื่องคอมพิวเตอร์แม่ข่ายที่นำเสนอต้องมีคุณสมบัติดังนี้

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. ใช้ VMware Hypervisor ESXi version 6.0 ขึ้นไป

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

1.2.1.7. สามารถทำงานแบบ Mirror Disk ได้

1.2.1.8. มีช่องเชื่อมต่อระบบเครือข่ายไม่น้อยกว่าแบบ 10/100/1000 Base-T

1.2.2. อุปกรณ์จัดเก็บข้อมูลแบบภายนอก (External Storage) ที่นำเสนอต้องมีคุณสมบัติดังนี้

1.2.2.1. เป็นอุปกรณ์ที่ทำหน้าที่จัดเก็บข้อมูลภายนอกแบบ SAN (Storage Area Network)

1.2.2.2. สามารถเชื่อมต่อแบบ Fiber Channel

1.2.2.3. มีช่องสัญญาน 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. มีหน่วยเก็บข้อมูล (Hard Drive) ชนิด SAS ที่มีความเร็วรอบไม่น้อยกว่า 10,000 RPM หรือ ชนิด Solid State Drive หรือดีกว่า

1.2.3. อุปกรณ์ Switch Layer 2 ที่นำเสนอต้องมีคุณสมบัติดังนี้

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

1.2.4. Firewall ที่นำเสนอต้องมีคุณสมบัติดังนี้

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 8 (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 ที่นำเสนอต้องมีคุณสมบัติดังนี้

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

1.2.5.5. สามารถทำการ Updates Signature ได้ทั้งแบบ Manual หรือแบบ Automatic

1.2.6. ระบบป้องกันการบุกรุกด้านเครือข่าย (Intrusion Prevention System : IPS) ที่นำเสนอต้องมีคุณสมบัติดังนี้

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. สามารถป้องการการโจมตีแบบ 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 ที่นำเสนอต้องมีคุณสมบัติดังนี้

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 หรือการเข้าถึงฐานข้อมูลโดยไม่ได้รับอนุญาติ แบบ Real-Time

1.2.7.5. มี IPS Throughput อย่างน้อย 500 Mbps

1.3. ความต้องการ Cloud Service ด้าน VM (Virtual Machine) ต้องสร้าง VM ให้ธนาคารดังนี้

1.3.1. Development Environment Zone ต้องมีรายละเอียดดังนี้

1.3.1.1. Web&Application Server จำนวน 1 หน่วย

1.3.1.1.1. CPU: 4 Core

1.3.1.1.2. RAM: 8 GB

1.3.1.1.3. Usage disk: 150GB (Drive C: 100GB, Drive D: 50GB)

1.3.1.1.4. OS: Windows Server 2016

1.3.1.2. Database Server จำนวน 1 หน่วย

1.3.1.2.1. CPU: 4 Core

1.3.1.2.2. RAM: 8 GB

1.3.1.2.3. Usage disk: 200GB (Drive C: 100GB, Drive D: 50GB, Drive E: 50GB)

1.3.1.2.4. OS: Windows Server 2016

1.3.1.2.5. Database: MSSQL 2016

1.3.1.3. Data Authentication and Data Encryption Server จำนวน 1 หน่วย

1.3.1.3.1. CPU: 4 Core

1.3.1.3.2. RAM: 8 GB

1.3.1.3.3. Usage disk: 150GB (Drive C: 100GB, Drive D: 50GB)

1.3.1.3.4. OS: Windows Server 2016

1.3.2. User Acceptance Test Environment Zone ต้องมีรายละเอียดดังนี้

1.3.2.1. Web Server จำนวน 1 หน่วย

1.3.2.1.1. CPU: 4 Core

1.3.2.1.2. RAM: 8 GB

1.3.2.1.3. Usage disk: 150GB (Drive C: 100GB, Drive D: 50GB)

1.3.2.1.4. OS: Windows Server 2016

1.3.2.2. Application Server จำนวน 1 หน่วย

1.3.2.2.1. CPU: 4 Core

1.3.2.2.2. RAM: 8 GB

1.3.2.2.3. Usage disk: 150GB (Drive C: 100GB, Drive D: 50GB)

1.3.2.2.4. OS: Windows Server 2016

1.3.2.3. Database Server จำนวน 1 หน่วย

1.3.2.3.1. CPU: 4 Core

1.3.2.3.2. RAM: 8 GB

1.3.2.3.3. Usage disk: 200GB (Drive C: 100GB, Drive D: 50GB, Drive E: 50GB)

1.3.2.3.4. OS: Windows Server 2016

1.3.2.3.5. Database: MSSQL 2016

1.3.2.4. Data Authentication and Data Encryption Server จำนวน 1 หน่วย

1.3.2.4.1. CPU: 4 Core

1.3.2.4.2. RAM: 8 GB

1.3.2.4.3. Usage disk: 150GB (Drive C: 100GB, Drive D: 50GB)

1.3.2.4.4. OS: Windows Server 2016

1.3.3. Production Environment Zone ต้องมีรายละเอียดดังนี้

1.3.3.1. Web Server (Failover Cluster: Active-Standby) จำนวน 2 หน่วย

1.3.3.1.1. CPU: 4 Core

1.3.3.1.2. RAM: 8 GB

1.3.3.1.3. Usage disk: 150GB (Drive C: 100GB, Drive D: 50GB)

1.3.3.1.4. OS: Windows Server 2016

1.3.3.2. Application Server (Failover Cluster: Active-Standby) จำนวน 2 หน่วย

1.3.3.2.1. CPU: 4 Core

1.3.3.2.2. RAM: 8 GB

1.3.3.2.3. Usage disk: 150GB (Drive C: 100GB, Drive D: 50GB)

1.3.3.2.4. OS: Windows Server 2016

1.3.3.3. Database Server (Failover Cluster: Active-Standby) จำนวน 2 หน่วย

1.3.3.3.1. CPU: 6 Core

1.3.3.3.2. RAM: 12 GB

1.3.3.3.3. Usage disk: 200GB (Drive C: 100GB, Drive D: 50GB)

1.3.3.3.4. OS: Windows Server 2016

1.3.3.3.5. Database: MSSQL 2016

1.3.3.4. Data Storage Disk for Database Server (Failover Cluster: Active-Standby)

1.3.3.4.1. Usage disk: 500GB

1.3.3.5. Data Authentication and Data Encryption Server จำนวน 2 หน่วย

1.3.3.5.1. CPU: 4 Core

1.3.3.5.2. RAM: 8 GB

1.3.3.5.3. Usage disk: 150GB (Drive C: 100GB, Drive D: 50GB)

1.3.3.5.4. OS: Windows Server 2016

1.4. ความต้องการ Cloud Service ด้านศูนย์ข้อมูลหลัก (Data Center)

1.4.1. ต้องมีระยะห่างจากศูนย์ข้อมูลสำรองฉุกเฉิน ไม่น้อยกว่า 30 กิโลเมตร

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

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

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

1.4.5. ต้องมีระบบการป้องกันและตรวจสอบสิทธิ์ผู้ไม่เกี่ยวข้องเข้าไปในสถานที่ที่ให้บริการ Private Cloud ของธนาคาร ซึ่งอาจก่อให้เกิดความเสียหายกับธนาคาร

1.5. ความต้องการ Cloud Service ด้านศูนย์ข้อมูลสำรองฉุกเฉิน (Backup Data Center)

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

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

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

1.5.4. ต้องมีระบบการป้องกันและตรวจสอบสิทธิ์ผู้ไม่เกี่ยวข้องเข้าไปในสถานที่ที่ให้บริการ Private Cloud ของธนาคาร ซึ่งอาจก่อให้เกิดความเสียหายกับธนาคาร

1.6. โปรแกรมอื่น ๆ ที่เกี่ยวข้องกับการให้บริการ จะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย โดยไม่ละเมิดสิทธิ์ของผู้อื่น รวมทั้งรับผิดชอบในกรณีที่มีการกล่าวหา ฟ้องร้อง หรือเรียกค่าเสียหายใดๆ จากเจ้าของลิขสิทธิ์หรือผู้เรียกร้องอื่นใด

2. **ความต้องการเฉพาะด้านการพิสูจน์ตัวตน** (Authentication Service) **และบริการเพื่อบริหารจัดการเข้ารหัสข้อมูล** (Data Encryption)

2.1. คุณลักษณะของซอฟแวร์ด้านการพิสูจน์ตัวตน (Authentication)

2.1.1. สามารถทำ Two-Factor Authentication อย่างน้อย 1 ระบบ ดังนี้

2.1.1.1. RADIUS

2.1.1.2. SAML

2.1.1.3. Agent

2.1.1.4. API

2.1.2. สามารถบริหารจัดการอุปกรณ์ Two-Factor Authenticator อย่างน้อยดังนี้

2.1.2.1. Hardware Token OTP (One-Time Password) แบบ Time-based และ Event-based

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

2.1.2.3. Mobile Token สำหรับ iOS และ Android

2.1.2.4. SMS Token

2.1.2.5. e-Mail Token

2.1.2.6. สามารถทำงานกับ Hardware Token OTP ของยี่ห้ออื่นได้

2.1.3. สามารถใช้ Soft Token ที่ได้รับมาตรฐานความปลอดภัย FIPS 104-2 ขึ้นไป โดยต้องมีจำนวนไม่ต่ำกว่า 500 Username

2.1.4. สามารถจัดการข้อมูลผู้ใช้งานของธนาคารอย่างน้อยดังนี้

2.1.4.1. Microsoft Active Directory (AD)

2.1.4.2. Open Database Connectivity (ODBC)

2.1.4.3. Microsoft SQL Server (SQL)

2.1.4.4. Lightweight Directory Access Protocol (LDAP)

2.1.5. เป็นสถาปัตยกรรมแบบ Multi-Tier, Multi-Tenant และรองรับการทำงานกับ Multi-Domain ได้ รวมทั้งต้องไม่จำกัดจำนวน Token ที่ให้กับผู้ใช้งานแต่ละราย

2.1.6. รองรับการทำงานสำหรับอุปกรณ์ Token ดังนี้

2.1.6.1. การจัดเตรียมอุปกรณ์ Token ให้กับผู้ใช้งาน (Provisioning)

2.1.6.2. การจัดการอุปกรณ์ Token ให้กับผู้ใช้งาน (Management)

2.1.6.3. การยกเลิกการใช้งานอุปกรณ์ Token ให้กับผู้ใช้งาน (De-Provisioning)

2.1.6.4. การจัดทำรายงานสำหรับอุปกรณ์ Token ของผู้ใช้งาน (Reporting)

2.1.6.5. การเตือนภัยสำหรับอุปกรณ์ Token ของผู้ใช้งาน (Alert)

2.1.6.6. การจัดการอุปกรณ์ Token กรณีสูญหาย (Lost Token)

2.1.7. มีหน้าเว็บไซต์บริการตนเองสำหรับผู้ใช้งาน (User Self-Service Portal) เพื่อใช้งาน ดังนี้

2.1.7.1. การลงทะเบียนด้วยตนเอง (Self-Registration)

2.1.7.2. การเปลี่ยนรหัส (Change Password)

2.1.7.3. การปลดล็อค (Unlock Token)

2.1.7.4. การซิงค์อีกครั้ง (Resync Token)

2.1.8. มี Integrations Guide อย่างน้อยดังนี้

2.1.8.1. ระบบ 2 Factor Authentication กับ VPN

2.1.8.2. ระบบ 2 Factor Authentication กับ Cloud

2.1.8.3. ระบบ 2 Factor Authentication กับ ระบบเครือข่าย

2.1.8.4. ระบบ 2 Factor Authentication กับ VM

2.1.8.5. ระบบ 2 Factor Authentication กับ Web Portal

2.2. คุณลักษณะด้าน Data Encryption

ต้องจัดเตรียมอุปกรณ์ Centralized Cryptographic Key Management (CCKM) ให้ธนาคาร จำนวน 2 ชุด โดยมีรายละเอียดของอุปกรณ์และความต้องการใช้งาน ดังนี้

2.2.1. มีมาตรฐาน Key Management Interoperability Protocol (KMIP)

2.2.2. มี API ต่อไปนี้ KMIP, PKCS #11, Java และ .NET เป็นอย่างน้อย

2.2.3. มี Algorithms ต่อไปนี้ AES, ARIA, DES, DESede, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, RC4 และ RSA เป็นอย่างน้อย

2.2.4. สามารถจัดเก็บ Symmetric และ Asymmetric Keys ได้

2.2.5. สามารถบริหารจัดการ Key ดังนี้

2.2.5.1. การสร้าง Key

2.2.5.2. การจัดเก็บ Key

2.2.5.3. การสำรอง Key

2.2.5.4. การกระจาย Key

2.2.5.5. การยกเลิกการใช้งาน Key

2.2.5.6. การทำลาย Key

2.2.6. สามารถทำ Authentication กับ LDAP และ Active Directory เป็นอย่างน้อย

2.2.7. สามารถบริหารจัดการผ่านหน้าเว็บไซต์ และการจัดการผ่าน Command Line Interface ได้

2.2.8. สามารถเข้ารหัสระบบได้ ในระดับต่างๆ ดังนี้

2.2.8.1. การเข้ารหัสฐานข้อมูล (DataBase Encryption)

2.2.8.2. การเข้ารหัสแอพพลิเคชันเซิร์ฟเวอร์ (Application Encryption)

2.2.8.3. การเข้ารหัสไฟล์เซิร์ฟเวอร์ (File and Folder Encryption)

2.2.8.4. การเข้ารหัสเครื่องเสมือน (Virtual Machine Encryption)

2.2.8.5. การเข้ารหัสระบบจัดเก็บข้อมูล (Storage Encryption)

2.2.9. สามารถจัดเก็บ Key ในอุปกรณ์ได้ ไม่น้อยกว่า 25,000 key

2.2.10. มี Concurrent Client ได้ไม่น้อยกว่า 100 Client

2.2.11. สามารถทำงานในลักษณะ High Availability (HA) แบบ Active-Active ได้

2.2.12. สามารถส่ง Log ไปที่ Syslog และ SIEM (Security Information and Event Management) ได้

2.2.13. ผ่านการรับรองมาตรฐาน FIPS 140-2 Level 1

2.2.14. สามารถเข้ารหัสไฟล์เซิร์ฟเวอร์ไม่น้อยกว่า 4 เครื่อง และการเข้ารหัสเครื่องคอมพิวเตอร์แม่ข่ายเสมือนไม่น้อยกว่า 25 ระบบ

2.3. โปรแกรมอื่นๆ ที่เกี่ยวข้องกับการให้บริการ จะต้องมีลิขสิทธิ์ถูกต้องตามกฎหมาย โดยไม่ละเมิดสิทธิ์ของผู้อื่น รวมทั้งรับผิดชอบในกรณีที่มีการกล่าวหา ฟ้องร้อง หรือเรียกค่าเสียหายใดๆ จากเจ้าของลิขสิทธิ์หรือผู้เรียกร้องอื่นใด

3. **การให้บริการสนับสนุนของบริการตลอดระยะเวลาการใช้บริการ (Support)**

ผู้เสนอราคาที่ได้รับคัดเลือกจะต้องให้บริการสนับสนุน เป็นระยะเวลา 1 ปี (ตามข้อ 3. ผนวก 2) อย่างน้อยดังนี้

3.1. ต้องจัดให้มีเจ้าหน้าที่ประสานงานที่มีความเชี่ยวชาญพร้อมเบอร์โทรศัพท์ รวมถึงช่องทางอื่น เพื่อบริการให้คำปรึกษา ตอบข้อซักถาม และให้ความช่วยเหลือในการแก้ไขปัญหาต่างๆ ได้ทุกวันตลอด 24 ชั่วโมง โดยผู้ให้บริการต้องแก้ไขระบบในส่วนของบริการ Cloud Service Authentication Service และ Data Encryption ให้สามารถใช้งานได้เป็นปกติภายใน 60 นาที หลังจากได้รับแจ้งเหตุขัดข้อง หรือความชำรุดบกพร่องจากธนาคาร

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

3.3. กรณีมีการปรับปรุงเปลี่ยนแปลงอุปกรณ์ ผู้ให้บริการต้องจัดหาอุปกรณ์ที่มีคุณลักษณะเทียบเท่าหรือดีกว่าอุปกรณ์ที่ชำรุดบกพร่องให้ธนาคารใช้งาน โดยไม่คิดค่าใช้จ่ายใดๆ โดยจะต้องแจ้งให้ธนาคารทราบล่วงหน้าไม่น้อยกว่า 10 วัน ก่อนดำเนินการเปลี่ยนแปลงอุปกรณ์

3.4. ต้องจัดทำรายงานสรุปรายละเอียดโปรแกรมและอุปกรณ์ที่ปรับปรุงเปลี่ยนแปลงทั้งหมดส่งให้ธนาคารภายใน 15 วัน นับจากวันที่มีการเปลี่ยนแปลง

3.5. ต้องส่งรายงานผลการทดสอบระบบการกู้คืนข้อมูลในศูนย์ข้อมูลหลักของผู้ให้บริการให้ธนาคารภายใน 30 วัน หลังจากทำการทดสอบเสร็จสิ้น อย่างน้อยปีละ 1 ครั้ง

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

3.7. ต้องจัดทำรายงาน Performance Report ในส่วนของ vCPU, Memory, Storage เป็นราย VM ทุกสิ้นเดือนให้กับธนาคาร ภายใน 10 วัน นับจากวันสิ้นเดือน

3.8. ต้องจัดทำรายงานความพร้อมใช้ระบบ (Service Availability Report) ทุกสิ้นเดือนให้กับธนาคาร ภายใน 10 วัน นับจากวันสิ้นเดือน

3.9. ต้องจัดทำรายงานผลภัยคุกคามทุกสิ้นเดือนให้กับธนาคาร ภายใน 10 วัน นับจากวันสิ้นเดือน

3.10. ต้องจัดทำรายงานการวิเคราะห์ Log เช่น Traffic Log, Access Log, Audit Log เป็นต้น เป็นรายไตรมาส ให้กับธนาคาร ภายใน 10 วัน นับจากวันสิ้นสุดไตรมาส

3.11. ต้องทำ Preventive Maintenance (PM) เป็นรายไตรมาส และจัดทำรายงานแจ้งผลให้ธนาคาร ภายใน 10 วัน นับจากวันสิ้นสุดไตรมาส

3.12. กรณีต้องการปิดปรับปรุงระบบจะต้องแจ้งให้ธนาคารทราบล่วงหน้าไม่น้อยกว่า 15 วัน ก่อนดำเนินการ

3.13. กรณีธนาคารพบช่องโหว่ของระบบเครือข่ายการสื่อสารและระบบคอมพิวเตอร์ ผู้เสนอราคาที่ได้รับการคัดเลือกต้องดำเนินการแก้ไขเพื่อปิดช่องโหว่ดังกล่าวและจัดส่งรายงานการแก้ไขให้ธนาคาร ภายในระยะเวลาที่กำหนดตามระดับความรุนแรง ดังนี้

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

หมายเหตุ : ระดับความรุนแรงจะอ้างอิงตามรายงานการประเมินช่องโหว่ที่ธนาคารได้รับจากผู้ให้บริการประเมินช่องโหว่ฯ

4. การ Upgrade ระบบ

ในระหว่างดำเนินการให้บริการ Cloud Service และ Authentication Service & Data Encryption หาก Application Software มีการออก Service Pack หรือ Version ใหม่ ผู้เสนอราคาที่ได้รับการคัดเลือกต้องแจ้งรายละเอียดการเปลี่ยนแปลงและผลกระทบที่มีความต้องการใช้งาน เพื่อใช้เป็นข้อมูลประกอบการตัดสินใจ ทั้งนี้ หากธนาคารประสงค์จะทำการ Upgrade Application Software ผู้เสนอราคาที่ได้รับการคัดเลือกจะต้องดำเนินการให้โดยไม่คิดค่าใช้จ่ายใดๆ เพิ่มเติมจากธนาคาร

5. ขอบเขตงาน

ผู้เสนอราคาที่ได้รับการคัดเลือกต้องดำเนินการตามขอบเขตงานที่กำหนดอย่างน้อยดังต่อไปนี้

5.1. ด้านการติดตั้ง การทดสอบ และการดำเนินการอื่นๆ

5.1.1. ต้องดำเนินการติดตั้ง ปรับตั้งค่าต่างๆ และทดสอบความถูกต้องของการให้บริการ ร่วมกับธนาคารให้เรียบร้อยก่อนการใช้งาน

5.1.2. ต้องให้คำแนะนำในการประยุกต์ใช้ และการดำเนินงานอื่น ๆ ที่จำเป็นเพื่อให้ธนาคารสามารถใช้บริการได้อย่างมีประสิทธิภาพ

5.1.3. ต้องจัดให้มีบุคลากรที่จะให้การสนับสนุนธนาคารในระหว่างดำเนินโครงการ จนแล้วเสร็จตามระยะเวลาที่กำหนด

5.1.4. ต้องติดตั้งระบบและทดสอบความถูกต้องของระบบงาน รวมทั้งสนับสนุนให้ธนาคารสามารถนำระบบขึ้นใช้งาน (Go-live)

5.2. ด้านเอกสาร

ต้องจัดทำเอกสารส่งมอบเป็นภาษาไทย รวมทั้งจัดทำข้อมูลในรูปแบบอิเล็กทรอนิกส์ (Soft File) และบันทึกลงอุปกรณ์จัดเก็บข้อมูลอิเล็กทรอนิกส์ จำนวนอย่างละ 2 ชุด ดังนี้

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

5.2.2. จัดทำรายงานสรุปรายละเอียดและจำนวนโปรแกรมพร้อมอุปกรณ์ที่ใช้ใน Cloud Service ทั้งหมด พร้อมเอกสารแสดงสิทธิการใช้งานที่ถูกต้องตามกฎหมาย

5.2.3. จัดทำหนังสือยืนยันการให้บริการแบบ Private Cloud

5.2.4. จัดทำเอกสารแสดงรายละเอียดสถานที่ติดตั้ง Data center พร้อมเบอร์ติดต่อ Call Center

5.2.5. จัดทำ Diagram สำหรับระบบ Cloud Service ที่ให้บริการสำหรับธนาคาร โดยระบุรายละเอียดแต่ละ VM

5.2.6. จัดทำเอกสารแสดงกระบวนการจัดการ (Incident Work Flow) ตั้งแต่ได้รับแจ้งปัญหา ตรวจสอบปัญหา แก้ไขปัญหา และสรุปผลที่เป็นลำดับขั้นตอนที่ชัดเจน โดยต้องจัดทำรายละเอียดและขั้นตอนการแก้ไขปัญหา หรือเหตุขัดข้อง หรือความชำรุดบกพร่องของบริการ Cloud Service โดยละเอียดให้แก่ธนาคาร

5.2.7. จัดทำหนังสือยืนยันสิทธิการเข้ารหัสไฟล์เซิร์ฟเวอร์และการเข้ารหัสเครื่องคอมพิวเตอร์แม่ข่ายเสมือน (ข้อ 2.2.14 ผนวก 1)

5.2.8. จัดทำรายงานความก้าวหน้าให้ธนาคารทราบ ทุก 2 สัปดาห์ จนกว่างานจะแล้วเสร็จ พร้อมจัดให้มีการประชุมร่วมกับคณะทำงานโครงการของธนาคารเป็นระยะ

5.2.9. จัดทำคู่มืออย่างน้อยดังนี้

5.2.9.1. คู่มือการกำหนดค่าในระบบ (System Configuration)

5.2.9.2. คู่มือการใช้งานสำหรับผู้ดูแลระบบ (Admin Manual)

5.2.9.3. คู่มือการใช้งานระบบ (User Manual)

5.3. ด้านการฝึกอบรม

ต้องจัดทำเอกสารพร้อมจัดฝึกอบรมให้แก่พนักงานของธนาคาร จำนวนไม่น้อยกว่า 5 คน โดยครอบคลุมเนื้อหาดังนี้

5.3.1. การบริหารจัดการบริการ Cloud Service

5.3.2. การบริหารจัดการและการใช้งานระบบการพิสูจน์ตัวตน