**คำถาม-คำตอบ**

**เรื่อง การรายงานข้อมูล (Data Set) เพื่อการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ**

**วันที่ 22 มกราคม 2563 สถานที่: ห้องประชุมป่วย อึ๊งภากรณ์**

| ข้อ | ประเด็นคำถาม | คำตอบ |
|---|---|---|
| **1.ชุดข้อมูลการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit)** | | |
| 1.1 | ขอบเขตการรายงานข้อสังเกตจากการตรวจสอบต้องรายงานในกรณีใดบ้าง | ข้อสังเกตที่เข้าข่ายต้องรายงาน ครอบคลุมดังนี้<br>● เป็นข้อสังเกตที่เกิดจากการกำกับดูแลและการดำเนินงานด้าน IT การบริหารจัดการความเสี่ยงด้าน IT (IT Risk) การกำกับดูแลตามกฎเกณฑ์และกฎหมายที่เกี่ยวข้องด้าน IT (IT Compliance) และการตรวจสอบด้าน IT (IT Audit)<br>● เป็นข้อสังเกตจากการตรวจสอบของหน่วยงานตรวจสอบภายใน หน่วยงานภายนอก และหน่วยงานกำกับดูแล<br>● เป็นข้อสังเกตที่มีระดับความเสี่ยงตั้งแต่ระดับปานกลางขึ้นไป |
| 1.2 | กรณีสาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศมีขอบเขตการรายงานข้อมูลอย่างไร | ขอบเขตการรายงานเป็นไปตามข้อ 1.1 โดยพิจารณาเพิ่มเติมว่าเป็นข้อสังเกตที่สาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศต้องรับทราบหรือดำเนินการแก้ไข |
| 1.3 | การรายงานข้อสังเกตตามหลักเกณฑ์นี้ มีขอบเขตในการรายงานข้อมูลตั้งต้นอย่างไร | ให้สถาบันการเงินรายงานข้อสังเกตที่มีความเสี่ยงระดับปานกลางขึ้นไป โดยรายงานที่ออกก่อนไตรมาส 2 ปี 2563 ให้รายงานเฉพาะข้อสังเกตที่ยังคงค้าง และรายงานที่ออกในไตรมาส 2 ปี 2563 ให้รายงานข้อสังเกตทั้งหมด |
| 1.4 | กรณีสถาบันการเงินมีข้อสังเกตที่ตรวจพบและแก้ไขแล้วเสร็จในช่วงไตรมาสเดียวกัน เข้าข่ายต้องรายงานหรือไม่ | เข้าข่ายต้องรายงาน โดยให้รายงานสถานะ (Audit Status) ของข้อสังเกตดังกล่าว เป็น “Completed” และไม่ต้องรายงานต่อในไตรมาสถัดไป |
| 1.5 | กรณีสถาบันการเงินมีข้อสังเกตที่ตรวจพบจากหน่วยงานภายนอกที่ไม่มีการระบุความเสี่ยง ถือว่าเข้าข่ายต้องรายงานหรือไม่ | ให้สถาบันการเงินพิจารณาระดับความเสี่ยงตามเกณฑ์ของสถาบันการเงิน หากข้อสังเกตดังกล่าวอยู่ในระดับปานกลางขึ้นไป เข้าข่ายต้องรายงานตามหลักเกณฑ์นี้ |

<table>
<tr><th>ข้อ</th><th>ประเด็นคำถาม</th><th>คำตอบ</th></tr>
<tr><td>1.6</td><td>กรณีสถาบันการเงินกำหนดระดับความเสี่ยงของข้อสังเกต (Audit Rating) ต่างจากระดับความเสี่ยงที่ ธปท. กำหนดไว้ (แบ่งเป็น 3 ระดับ ต่ำ, ปานกลาง, สูง) ต้องรายงานอย่างไร</td><td>ให้สถาบันการเงินพิจารณาเทียบเคียงระดับความเสี่ยงของข้อสังเกต (Audit Rating) ของสถาบันการเงิน เช่น หากจัดระดับเป็น 5 ระดับจากความเสี่ยงน้อยไปมาก ให้รายงานระดับ 3-5 มายัง ธปท. เป็นต้น</td></tr>
<tr><td>1.7</td><td>กรณีที่เป็นข้อสังเกตที่ตรวจพบ โดย ธปท. สถาบันการเงินสามารถพิจารณาปรับ Audit Status: Completed ได้หรือไม่</td><td>ให้สถาบันการเงินประสานงานกับ ธปท. เพื่อพิจารณาปิดข้อสังเกตก่อนรายงาน Audit Status: Completed</td></tr>
<tr><td colspan="3">2. ชุดข้อมูลความสามารถระบบเทคโนโลยีสารสนเทศ (IT Capacity)</td></tr>
<tr><td>2.1</td><td>ขอบเขตการรายงานชุดข้อมูล IT Capacity รายงานอย่างไร ครอบคลุมระบบอะไรบ้าง</td><td>ให้สถาบันการเงินรายงานความสามารถของระบบสำคัญ ได้แก่ ระบบ Mobile Banking Internet Banking ATM EAI และ Core Bank ผ่านการวัดค่า TPS และ/หรือ Concurrent User และ/หรือ End-to-end Response Time (PromptPay) ทุกกรณีที่สถาบันการเงินใช้ในการติดตาม ตามตารางนี้<br><br>
<table>
<tr><th>การวัด / ระบบ</th><th>TPS</th><th>Concurrent User</th><th>End-to-end Response Time</th></tr>
<tr><td>MB</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>IB</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>ATM</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>EAI</td><td>✓</td><td>-</td><td>-</td></tr>
<tr><td>CBS</td><td>✓</td><td>-</td><td>-</td></tr>
</table>
<br>ทั้งนี้ กรณีสถาบันการเงินใดไม่สามารถวัดความสามารถระบบงานผ่านการวัดค่า TPS, Concurrent User และ End-to-end Response Time (PromptPay) หรือมีระบบงานอยู่ที่บริษัทแม่ในต่างประเทศโดยไม่สามารถแยกวัดความสามารถระบบสำหรับการให้บริการในไทยได้ ให้ระบุ Capacity Type: None</td></tr>
</table>

| ข้อ | ประเด็นคำถาม | คำตอบ |
|---|---|---|
| | | |
| 2.2 | การวัดค่า TPS, Concurrent Users และ Response Time ในแต่ละ Capacity Type มีแนวทางการวัดอย่างไร | ให้อ้างอิงตามเอกสารแนบ ข้อ 1 |
| 2.3 | วิธีการวัดค่า Max, Peak, Forecast Peak, Daily Average, Monthly Average, %Trigger มีแนวทางและวิธีการวัดอย่างไร | ให้อ้างอิงตามเอกสารแนบ ข้อ 2 |
| 2.4 | วิธีการนับ Number of Active Customer จะนับอย่างไร | ค่า Number of Active Customer จะให้นับจากจำนวนผู้ใช้งานที่มีการ Login เข้าใช้งานระบบภายในงวดเดือนที่รายงาน |
| **3. ชุดข้อมูลศูนย์คอมพิวเตอร์หลักและคอมพิวเตอร์สำรอง (IT DC-DR)** | | |
| 3.1 | กรณีสถาบันการเงินมีศูนย์คอมพิวเตอร์หลายแห่ง และไม่สามารถระบุศูนย์คอมพิวเตอร์หลักได้ จะรายงานอย่างไร | กรณีไม่สามารถระบุศูนย์คอมพิวเตอร์หลักได้ ให้ถือว่าศูนย์คอมพิวเตอร์ที่มีระบบงาน Core Banking System ที่ใช้งานอยู่เป็นศูนย์คอมพิวเตอร์หลัก |
| 3.2 | การวัดระยะทางระหว่าง DC และ DR (Distance Between DC & DR) จะดำเนินการอย่างไร | การวัดระยะทางใน Column “Distance Between DC & DR” ให้ดำเนินการดังนี้:<br>• กรณีเป็นศูนย์คอมพิวเตอร์หลัก ระยะทางให้ระบุเป็น 0<br>• กรณีศูนย์คอมพิวเตอร์หลักและสำรองมีหลายแห่ง ให้วัดจากศูนย์คอมพิวเตอร์ใด ๆ ไปยังศูนย์คอมพิวเตอร์หลักที่ประมวลผลระบบงาน Core Banking System<br>• หากไม่สามารถวัดระยะจริงของสาย Fiber ให้ใช้วิธีวัดแบบเส้นตรงระหว่างศูนย์คอมพิวเตอร์ทั้งสองแห่ง (ระยะกระจัด) |
| 3.3 | กรณีสาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศใช้ศูนย์คอมพิวเตอร์ของบริษัทแม่ หรือบริษัทแม่ว่าจ้างต่อ (Sub-contract) ผู้ให้บริการภายนอก ต้องรายงานอย่างไร | กรณีใช้ศูนย์คอมพิวเตอร์ของบริษัทแม่ หรือบริษัทแม่ว่าจ้างต่อ (Sub-contract) ผู้ให้บริการภายนอก ให้ถือว่าเป็นการใช้ศูนย์คอมพิวเตอร์จากผู้ให้บริการภายนอก (Data Center Operation Type: Outsource Staff and Data Center) และระบุ Vendor เป็นบริษัทแม่ |

| ข้อ | ประเด็นคำถาม | คำตอบ |
|---|---|---|
| 3.4 | กรณีสาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศที่มีศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองอยู่หลายแห่ง ทั้งในประเทศไทยและต่างประเทศ ต้องรายงานอย่างไร | การรายงานศูนย์คอมพิวเตอร์ ให้ดำเนินการดังนี้<br>• ศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองที่อยู่ในประเทศไทย ให้รายงานทุกแห่ง<br>• ศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองในต่างประเทศ ให้รายงานเฉพาะ ศูนย์คอมพิวเตอร์ที่มีการประมวลผลระบบงานสำคัญที่ให้บริการในประเทศไทย |
| **4. ชุดข้อมูลโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT Infrastructure)** | | |
| 4.1 | ขอทราบแนวทางการพิจารณาว่ากรณีใดบ้างที่เข้าข่ายเป็น Unpatched Server | กรณีที่มี Server ที่ติดตั้ง Security Patch ยังไม่แล้วเสร็จ และเกินระยะเวลาที่กำหนดไว้ในนโยบายของสถาบันการเงินให้นับเป็น Unpatched Server ทั้งนี้ หากมีการขอยกเว้น (Exception) โดยได้รับการอนุมัติจากผู้มีอำนาจตามนโยบายของสถาบันการเงินและบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Mitigation) แล้ว ไม่นับเป็น Unpatched Server |
| 4.2 | กรณีสถาบันการเงินมีการใช้เทคโนโลยี Virtualization เพื่อปรับเพิ่ม/ลดจำนวน Server ตามลักษณะการใช้งาน จะรายงาน Total Server อย่างไร | กรณีสถาบันการเงินมี Logical Server ที่สามารถปรับเพิ่ม/ลดตามการใช้งานได้ เช่น การใช้เทคโนโลยี Virtualization มาบริหารจัดการ ให้นับจำนวนสูงสุด ที่สามารถใช้ได้จริงในไตรมาสที่รายงาน |
| **5. ชุดข้อมูลโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ (IT Project)** | | |
| 5.1 | การรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญตามประกาศ ธปท. ที่ สนส. 21/2562 เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงเทคโนโลยีสารสนเทศ แตกต่างจากการรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญตามหนังสือเวียนฉบับนี้หรือไม่ อย่างไร | รายงานดังกล่าวเป็นชุดเดียวกัน ซึ่งการรายงานตามหนังสือเวียนฉบับนี้เป็นการปรับเปลี่ยนวิธีการรายงาน โดยให้สถาบันการเงินดำเนินการดังนี้<br>● การรายงานประจำปี 2563 (31 ม.ค. 63) และไตรมาส 1 ปี 2563 (15 เม.ย. 63) ให้สถาบันการเงินรายงานโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญผ่าน E-Application ตามคู่มือประชาชน<br>● ตั้งแต่ไตรมาส 2 ปี 2563 เป็นต้นไป ให้รายงานข้อมูลดังกล่าวผ่านระบบ DMS Data Acquisition ภายใน 15 วันหลังสิ้นไตรมาส ทั้งนี้ หากสถาบันการเงินมีความ |

| ข้อ | ประเด็นคำถาม | คำตอบ |
|---|---|---|
| | | ประสงค์จะนำส่งการรายงานงวดไตรมาสที่ 4 และการรายงานประจำปีในคราวเดียวกัน สามารถทำได้ |
| 5.2 | กรณีสถาบันการเงินรายงานแผนการทดสอบนวัตกรรม FinTech ใน Own Sandbox ประจำปีต่อ ธปท. แล้ว ยังคงต้องรายงานรายงานโครงการที่มีนัยสำคัญและรายงานการนำเทคโนโลยีมาใช้งานตามหนังสือเวียนนี้ด้วยหรือไม่ | สถาบันการเงินต้องรายงานข้อมูลโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ และรายงานการนำเทคโนโลยีมาใช้งานแยกจากการรายงานแผนการทดสอบนวัตกรรม FinTech ใน Own Sandbox ตามหนังสือเวียน ธปท.ฝทง. ว.311/2562 เนื่องจากขอบเขตและวัตถุประสงค์การรายงานแตกต่างกัน การรายงานตามแผนการทดสอบฯ เป็นการแจ้ง ธปท. ล่วงหน้าก่อนดำเนินการ ส่วนการรายงานโครงการที่มีนัยสำคัญและรายงานการนำเทคโนโลยีมาใช้เป็นการติดตามความคืบหน้าการดำเนินการ |
| 5.3 | กรณีสาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศให้บริษัทแม่ดำเนินโครงการด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ เข้าข่ายต้องรายงานหรือไม่ | เข้าข่ายต้องรายงาน กรณีโครงการดังกล่าวเป็นโครงการที่มีนัยสำคัญที่ส่งผลกระทบต่อสาขาธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศ ในประเทศไทย |
| **6. ชุดข้อมูลบุคลากรด้านเทคโนโลยีสารสนเทศ (IT Staff)** | | |
| **6.1** | กรณีสถาบันการเงินมีพนักงานรับผิดชอบงานมากกว่า 1 หน้าที่งาน (Job Function) มีวิธีรายงานอย่างไร | กรณีพนักงานรับผิดชอบงานมากกว่า 1 หน้าที่ ให้สถาบันการเงินพิจารณานับจำนวนพนักงาน (Number of Employees (Actual)) เฉพาะหน้าที่ที่เป็นงานหลัก 1 ประเภทเท่านั้น |
| **6.2** | การนับข้อมูลจำนวนพนักงาน ได้แก่ Number of Employees (Manpower), Number of Employees (Actual), Number of Employees with Certificate ให้นับจำนวนบุคลากรระดับใดบ้าง | ให้นับจำนวนบุคลากรตั้งแต่ระดับหัวหน้าฝ่ายงานลงมา (ระดับหัวหน้าฝ่ายงานจนถึงผู้ปฏิบัติงาน) ตามหน้าที่งาน (Job Function) |

| ข้อ | ประเด็นคำถาม | คำตอบ |
|---|---|---|
| **6.3** | กรณีสถาบันการเงินไม่สามารถนับข้อมูลจำนวนพนักงานหรือจำนวนบุคลากรจากผู้ให้บริการภายนอกได้ จะรายงานข้อมูลอย่างไร | ให้กรอกข้อมูลจำนวนพนักงานเป็น 0 เฉพาะกรณีต่อไปนี้<br>1. กรณีสถาบันการเงินใช้บุคลากรจากผู้ให้บริการภายนอกประเภทบริษัทนอกกลุ่มธุรกิจ (Non-consolidated Company) และไม่สามารถนับจำนวนบุคลากรได้<br>2. กรณีสาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศที่ใช้บุคลากรจากบริษัทแม่ และไม่สามารถนับจำนวนบุคลากรได้ |
| **6.4** | ข้อมูลจำนวนพนักงานที่ได้รับการรับรองมาตรฐานสากลเฉพาะที่เกี่ยวข้องกับงาน IT มีวิธีการรายงานอย่างไร | ให้รายงานจำนวนพนักงานที่มาตรฐานที่รับรองทั่วไป (Certificate) เฉพาะด้านที่เกี่ยวข้องกับงานด้านเทคโนโลยีสนเทศ ได้แก่<br>• ISACA: CISA, CISM, CRISC<br>• CompTIA: CASP, CSA+, Security+<br>• (ISC)²: CISSP, SSCP, CAP, CSSLP, CCFP, CCSP<br>• EC-Council: CEH, ECSA, LPT, CHFI, ECIH, ENSA, CCISO<br>• Cisco: CCNA Security, CCNP Security, CCIE Security, CCNA CyberOps<br>• Mile2: C)PTE, C)PTC, C)DFE, C)IHE, C)ISSO, C)PEH, C)ISSM, C)ISSA<br>• GIAC: GISF, GSEC, GISP, GCFE<br><br>สำหรับรายชื่อ Certificate ที่ไม่อยู่ในข้างต้น หากสถาบันการเงินพิจารณาแล้วว่าเป็นรายชื่อ Certificate ที่อยู่ภายใต้ข้อกำหนดของสถาบันการเงินที่เพิ่มผลตอบแทนแก่พนักงาน สามารถนับเพิ่มเติมได้ |
| **7. ชุดข้อมูลภาพรวมระบบเทคโนโลยีสารสนเทศ (IT System Profile)** | | |

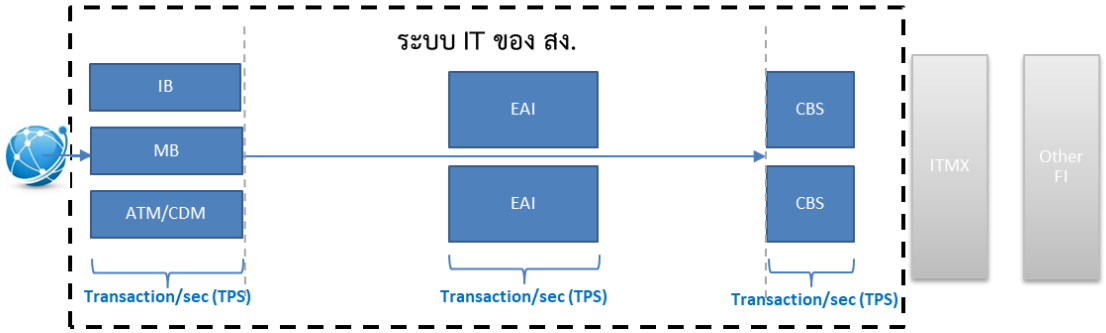
| ข้อ | ประเด็นคำถาม | คำตอบ |
|---|---|---|
| 7.1 | ขอบเขตการรายงานต้องรายงานทุกระบบโดยแจกแจงตามแต่ละช่อง หรือรายงานเฉพาะระบบงานที่มีนัยสำคัญ | ขอบเขตการรายงาน ให้รายงานทุกระบบ ตาม Classification Name: System โดยรายงานให้ครบถ้วนตามแต่ละ System และ Server Tier (สามารถดูตัวอย่างการกรอกข้อมูลที่ตาราง Excel) |
| 7.2 | กรณีสาขาของธนาคารพาณิชย์ต่างประเทศหรือธนาคารพาณิชย์ที่เป็นบริษัทลูกของธนาคารพาณิชย์ต่างประเทศที่มีระบบงานอยู่ที่บริษัทแม่หรือบริษัทในเครือที่อยู่ต่างประเทศ จะรายงานอย่างไร | ขอบเขตการรายงาน ให้รายงานเฉพาะระบบงานตาม Classification Name: System ทั้งหมดที่เกี่ยวข้องกับการบริการในประเทศไทย |
| **8. ชุดข้อมูลการนำเทคโนโลยีมาใช้งาน (Technology Implementation)** | | |
| 8.1 | ขอทราบขอบเขตและแนวทางการรายงานข้อมูลการนำเทคโนโลยีมาใช้งาน | ขอบเขตและแนวทางการรายงานชุดข้อมูลการนำเทคโนโลยีมาใช้งาน มีดังนี้<br>1. การรายงานครอบคลุมถึงการนำเทคโนโลยีตามประเภทที่กำหนด (Technology Category) มาใช้ในปัจจุบันทั้งหมด หรือการใช้เทคโนโลยีใหม่ที่สถาบันการเงินนำมาใช้เป็นครั้งแรก เพื่อสนับสนุนการให้บริการลูกค้า หรือเพิ่มประสิทธิภาพการดำเนินธุรกิจของสถาบันการเงิน<br>2. การรายงานงวดไตรมาสให้รายงานตั้งแต่เมื่อเริ่มศึกษาการนำเทคโนโลยีที่คาดว่าจะต้องทดลองใช้ใน Own Sandbox หรือ Regulatory Sandbox ในอนาคต (POC) หรือเมื่อเริ่มโครงการ (Initiatives) และรายงานจนกว่าจะยกเลิกโครงการ (Cancelled) หรือยกเลิกการให้บริการ (End of Service) |
| **9. ชุดข้อมูลการใช้บริการ การเชื่อมต่อระบบ IT และการเข้าถึงข้อมูลจากบุคคลภายนอก (IT Third Party)** | | |
| 9.1 | ขอทราบขอบเขตและแนวทางการรายงานชุดข้อมูล IT Third Party | ขอบเขตและแนวทางการรายงานชุดดังกล่าว มีดังนี้<br>(1) ผู้ให้บริการ IT Outsource ทั้งประเภทที่มีความสำคัญอย่างยิ่ง ที่อาจก่อให้เกิดความเสี่ยงและผลกระทบต่อสถาบัน |

| ข้อ | ประเด็นคำถาม | คำตอบ |
|---|---|---|
| | | การเงิน หรือระบบสถาบันการเงินในวงกว้าง (Critical IT Outsourcing) และประเภทอื่น (Other IT Outsourcing)<br>(2) Partnership ที่มีนัยสำคัญที่มีการเชื่อมต่อระบบสารสนเทศร่วมกับสถาบันการเงินโดยตรง หรือเชื่อมต่อผ่าน API<br>(3) บริษัทผู้ให้บริการ Switching เพื่อให้บริการทางธุรกรรมที่เกี่ยวข้องกับธุรกิจสถาบันการเงิน<br>(4) ผู้ให้บริการเครือข่าย (Internet Service Provider: ISP)<br><br>ทั้งนี้ ขอบเขตการรายงานข้างต้นครอบคลุมข้อมูล Third Party เพียงส่วนหนึ่งตามแนวปฏิบัติ เรื่องการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ดังนั้น Third Party ที่นอกเหนือจากการรายงานตามหนังสือเวียนฉบับนี้ ยังต้องดำเนินการตามแนวปฏิบัติดังกล่าว โดยสามารถอ้างอิงข้อมูลเพิ่มเติมในเอกสารแนบข้อ 3 และข้อ 4 |
| 9.2 | กรณีที่สถาบันการเงินใช้บริการจากบริษัทแม่ และไม่สามารถระบุ Service Risk Level ได้ ต้องรายงานอย่างไร | ในกรณีที่สถาบันการเงินใช้บริการจากบริษัทแม่ และไม่สามารถระบุ Service Risk Level ได้ ให้ระบุ Service Risk Level เป็น “Not Applicable” |
| 9.3 | กรณีใดบ้างที่ต้องระบุที่ตั้งศูนย์คอมพิวเตอร์หลัก (DC Country) และที่ตั้งศูนย์คอมพิวเตอร์สำรอง (DR Country) | กรณีที่สถาบันการเงินใช้บริการ Cloud Computing จากผู้ให้บริการภายนอก และกรณีที่บุคคลภายนอกมีการจัดเก็บหรือประมวลผลข้อมูลของสถาบันการเงิน |
| 9.4 | กรณีที่สถาบันการเงินใช้บริการ Cloud Computing จากผู้ให้บริการภายนอก หรือผู้ให้บริการ Cloud Computing (Service Provider) แต่ทำสัญญากับตัวกลาง (Dealer) จะต้องรายงานอย่างไร | กรณีที่มีการใช้บริการจากผู้ให้บริการภายนอก รวมถึงการใช้บริการ Cloud Computing โดยทำสัญญากับตัวกลาง (Dealer) ให้รายงานตามคู่สัญญา ทั้งนี้ ให้สถาบันการเงินระบุผู้ให้บริการภายนอก หรือผู้ให้บริการ Cloud Computing เพิ่มเติมในช่อง Third Party Name ในรูปแบบ “ชื่อคู่สัญญา [ผู้ให้บริการภายนอก หรือผู้ให้บริการ Cloud Computing]" พร้อมระบุที่ตั้งศูนย์คอมพิวเตอร์หลัก (DC Country) และที่ตั้งศูนย์คอมพิวเตอร์สำรอง (DR Country) (ถ้ามี) |
| 9.5 | ขอบเขตการรายงานชุดข้อมูล IT Third Party ครอบคลุมถึง สาขาของธนาคารใน | ระยะแรก ให้รายงานข้อมูลกรณีที่ธนาคารใช้บริการ IT Third Party เฉพาะส่วนของธนาคารเอง ไม่รวมถึงกรณีสาขาของ |

| ข้อ | ประเด็นคำถาม | คำตอบ |
| --- | --- | --- |
| | ต่างประเทศและบริษัทลูกของธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยที่อยู่ในกลุ่ม Solo Consolidation หรือไม่ | ธนาคารในต่างประเทศหรือบริษัทลูกของธนาคารที่จดทะเบียนในประเทศไทยที่อยู่ในกลุ่ม Solo Consolidation ใช้บริการ IT Third Party โดยตรง<br><br>ทั้งนี้ สาขาของธนาคารในต่างประเทศและบริษัทลูกของธนาคารพาณิชย์ที่จดทะเบียนในประเทศไทยที่อยู่ในกลุ่ม Solo Consolidation ยังต้องดำเนินการตามแนวปฏิบัติ เรื่องการบริหารจัดการความเสี่ยงจากบุคคลภายนอก |

1. รูปแสดงแนวทางการวัดประสิทธิภาพระบบงาน สำหรับรายงานชุดข้อมูล IT Capacity

- **แนวทางการวัดค่า TPS ของระบบงาน ให้วัดแยกรายระบบงาน ครอบคลุมระบบ Channel (IB, MB, ATM), EAI และ CBS ดังรูป**




Definition

**Transaction/second (TPS) การวัดจำนวนธุรกรรมต่อวินาที**

**Peak:** ค่า TPS สูงสุดที่เกิดขึ้นจริงภายในงวดข้อมูล

**Daily Average:** ค่า TPS เฉลี่ยที่เกิดขึ้นในช่วงเวลา 06.00 น. ถึง 22.00 น.ของวันที่มีธุรกรรมสูงสุดในงวดข้อมูล

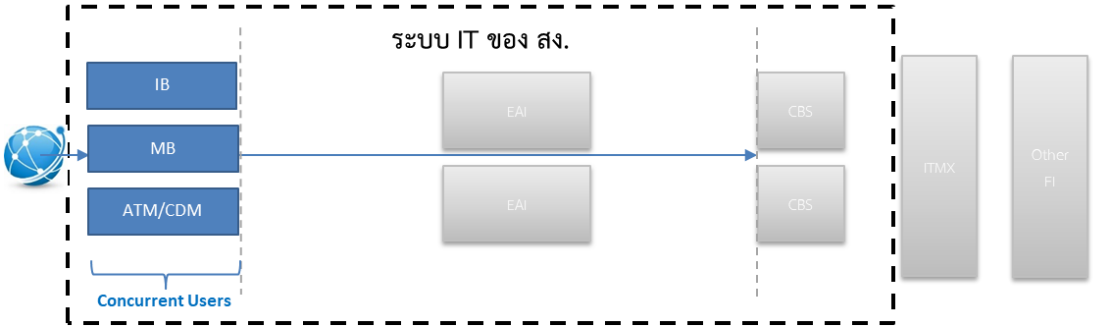
**Monthly Average:** ค่า TPS เฉลี่ยที่เกิดขึ้นในช่วงเวลา 06.00 น. ถึง 22.00 น. ในงวดข้อมูล

**Max:** ค่า TPS สูงสุดที่ระบบรองรับได้ ภายในงวดข้อมูล

**Forecast Peak:** ค่า TPS สูงสุดที่คาดว่าจะเกิดขึ้น ในช่วงเวลา 6 เดือนนับจากงวดข้อมูล ตามแนวทางการบริหารจัดการของ สง.

**%Trigger:** ค่าระดับการแจ้งเตือนที่มีนัยสำคัญ เพื่อใช้ในการบริหารจัดการความสามารถระบบงานให้สามารถรองรับบริการได้อย่างต่อเนื่อง

- **แนวทางการวัดค่า Concurrent Users ให้วัดแยกรายระบบงาน ครอบคลุมระบบ Channel (IB, MB, ATM) ดังรูป**




Definition

**Concurrent Users การวัดปริมาณผู้ใช้งานที่เข้าใช้งานพร้อมกัน ณ ขณะใดขณะหนึ่ง**

**Peak:** ค่า Concurrent Users สูงสุดที่เกิดขึ้นจริงภายในงวดข้อมูล

**Daily Average:** ค่า Concurrent Users เฉลี่ยที่เกิดขึ้นในช่วงเวลา 06.00 น. ถึง 22.00 น. ของวันที่มีธุรกรรมสูงสุดในงวดข้อมูล

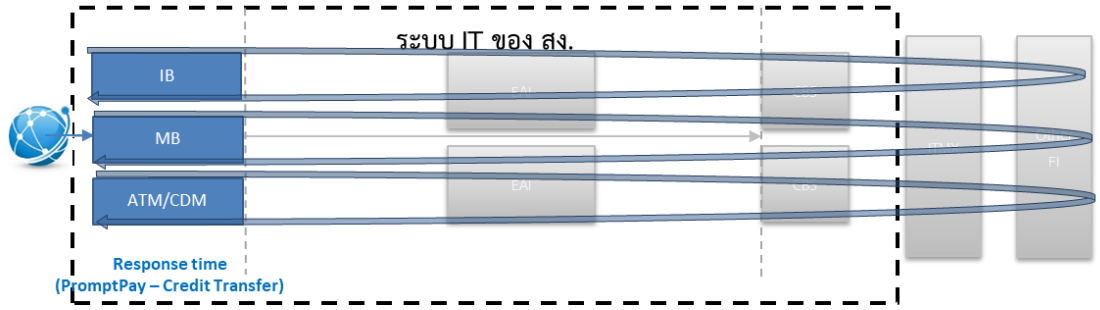
**Monthly Average:** ค่า Concurrent Users เฉลี่ยที่เกิดขึ้นในช่วงเวลา 06.00 น. ถึง 22.00 น. ในงวดข้อมูล

**Max:** ค่า Concurrent Users สูงสุดที่ระบบรองรับได้ ภายในงวดข้อมูล

**Forecast Peak:** ค่า Concurrent Users สูงสุดที่คาดว่าจะเกิดขึ้นในช่วงเวลา 6 เดือนนับจากงวดข้อมูล ตามแนวทางการบริหารจัดการของ สง.

**%Trigger:** ค่าระดับการแจ้งเตือนที่มีนัยสำคัญ เพื่อใช้ในการบริหารจัดการความสามารถระบบงานให้สามารถรองรับบริการได้อย่างต่อเนื่อง

- **แนวทางการวัดค่า Response Time ของธุรกรรม Prompt Pay ให้วัดแยกรายระบบงาน ครอบคลุมระบบ Channel ตั้งแต่เริ่มส่ง Request จนกระทั่งได้รับ Response กลับมา ดังรูป (หน่วย: millisecond)**




Definition

**End-to-end Response Time (PromptPay) ระยะเวลาที่ระบบทำธุรกรรม Promptpay ตั้งแต่เริ่มส่งคำสั่งธุรกรรมจนกระทั่งธุรกรรมสำเร็จ**

**Peak:** ค่า Response time สูงสุดที่เกิดขึ้นจริงภายในงวดข้อมูล

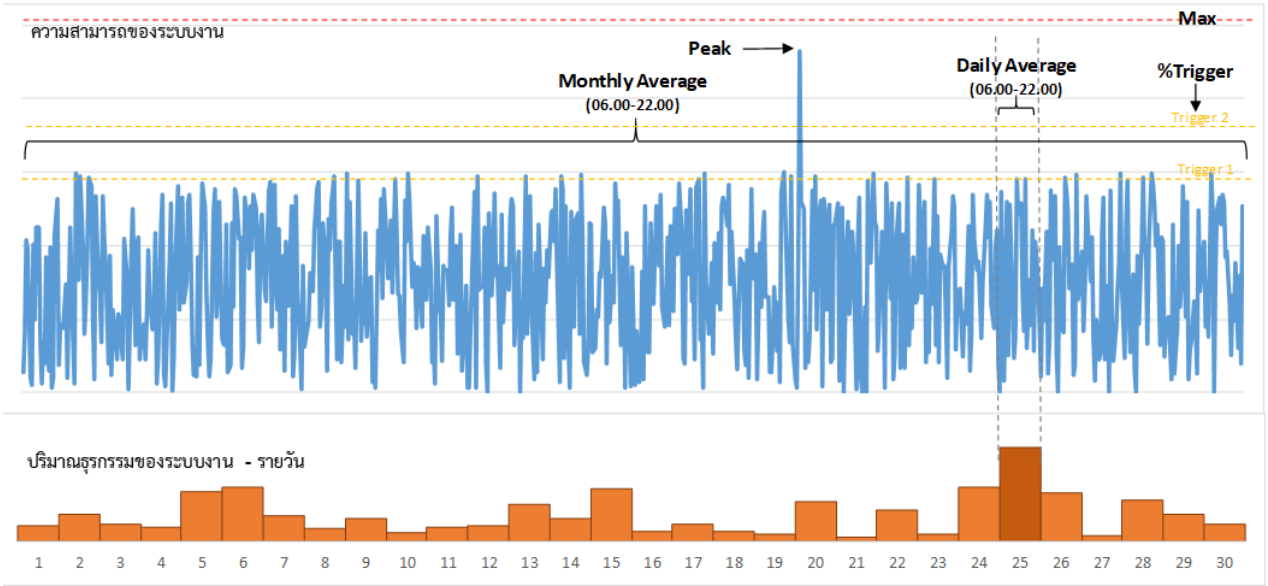
**Daily Average:** ค่า Response time เฉลี่ยที่เกิดขึ้นในช่วงเวลา 06.00 น. ถึง 22.00 น. ของวันที่มีธุรกรรมสูงสุดในงวดข้อมูล

**Monthly Average:** ค่า Response time เฉลี่ยที่เกิดขึ้นในช่วงเวลา 06.00 น. ถึง 22.00 น. ในงวดข้อมูล

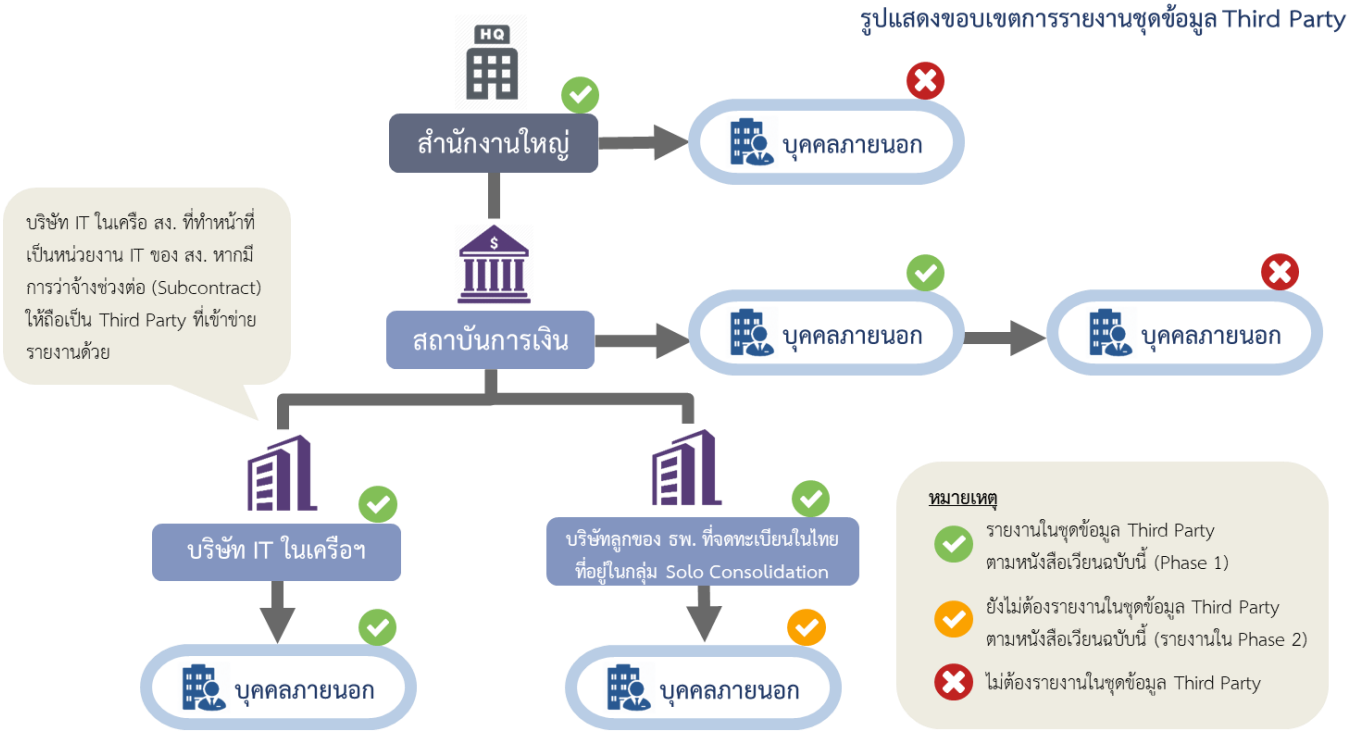
**Max:** ค่า Response time สูงสุดที่ระบบรองรับได้ ภายในงวดข้อมูล (Time out)

ทั้งนี้ ในกรณี Capacity Type: Response Time ไม่ต้องกรอกค่า Forecast Peak และ %Trigger

2. รูปแสดงตัวอย่างกราฟความสามารถของระบบงาน และข้อมูลที่ต้องบันทึกในชุดข้อมูล IT Capacity



3. รูปแสดงขอบเขตการรายงานชุดข้อมูล Third Party




4. ตัวอย่างแนวทางการเลือก Third Party Type

| IT Outsource | Partner | Switching | ISP | Out-of-scope |
|---|---|---|---|---|
| งาน IT ที่ใช้บริการจากบุคคลภายนอก ที่โดยปกติและสถาบันการเงินต้องดำเนินการเอง | การร่วมมือเป็นพันธมิตรทางธุรกิจที่มีนัยสำคัญกับองค์กรภายนอก ที่มีการเชื่อมต่อระบบงานระหว่างองค์กร ไม่ว่าจะเป็นการเชื่อมต่อโดยตรง (Direct link) หรือผ่าน API | ผู้ให้บริการระบบชำระเงินกลาง (เช่น VISA, MASTER, NITMX หรือ PCC เป็นต้น) | การใช้บริการระบบเครือข่ายภายนอก เช่น เครือข่าย Internet หรือการเช่าสายสื่อสาร fiber optic | การจัดซื้อ ติดตั้ง บำรุงรักษาโปรแกรมสำเร็จรูป ที่ไม่ต้องพัฒนา Software เพิ่มเติม |
| การจ้างทีมงานเพื่อพัฒนา Software หรือ Application | | | | การจัดซื้อ ติดตั้ง บำรุงรักษา Software Hardware แก่เครื่องคอมพิวเตอร์และอุปกรณ์สำนักงาน (End Point) |
| การบำรุงรักษา Software และ Hardware ยกเว้น เครื่องคอมพิวเตอร์และอุปกรณ์สำนักงาน (End Point) | | | | การใช้บริการข้อมูลการเงิน ข้อมูลตลาด ข้อมูลธุรกิจ เช่น Credit Bureau, BOL, Bloomberg, Moody's, Standard & Poors และ Fitch Rating เป็นต้น |

| IT Outsource | Partner | Switching | ISP | Out-of-scope |
|---|---|---|---|---|
| การเช่าพื้นที่เพื่อใช้เป็นศูนย์คอมพิวเตอร์ | | | | การส่งข้อมูลไปยังบริษัทแม่ เพื่อปฏิบัติตามข้อกำหนดของหลักเกณฑ์ในต่างประเทศ เช่น FATCA |
| การใช้บริการระบบเครือข่ายสื่อสารภายในที่มีการเชื่อมโยงอุปกรณ์ระบบงานและข้อมูลสำคัญเข้าไว้ด้วยกัน | | | | การจ้างบุคลากรภายนอกมาแก้ไขปัญหาระบบงานที่เกิดขึ้นแบบฉุกเฉินอย่างทันท่วงที ซึ่งสถาบันการเงินไม่สามารถแก้ไขปัญหาดังกล่าวได้ |
| | | | | การตรวจสอบเพื่อรับรองมาตรฐานหรือเอกสารการรับรองเกี่ยวข้องกับ IT (certificate) |
| | | | | การจ้างที่ปรึกษาด้านเทคโนโลยีสารสนเทศ |
| | | | | การเชื่อมต่อเพื่อเป็นการปฏิบัติตามกฎเกณฑ์ทางการ เช่น DOPA, NCB |
| | | | | การจ้างพิมพ์ใบแจ้งยอด, งานผลิต จัดทำ และจัดส่งบัตรเครดิต/เดบิต |