แบบรายงานเสนอความเสี่ยงการทุจริตของหน่วยงาน

กระบวนงาน/โครงการ	ชื่อความเสี่ยง	ศปท. กระทรวง	ชื่อหน่วยงาน	ประเภทหน่วยงาน	ด้านประเภทความเสี่ยง
โครงการ	ปรับปรุงประสิทธิภาพระบบเครือข่ายสื่อสาร ศูนย์คอมพิวเตอร์สำรอง (ระยะเวลา ๓ ปี)	ศปท. กระทรวงการคลัง	ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย (ธพว.)	รัฐวิสาหกิจ	ด้านที่ 3 โครงการจัดซื้อจัดจ้าง

โปรดจัดทำแบบประมาณการงบประมาณ

การกำหนดเกณฑ์การประเมินความเสี่ยงการทุจริต

โอกาส/ผลกระทบ	ประเภท	๑	๒	๓	๔	๕
โอกาส (Likelihood)	L1: ปริมาณของโอกาสที่จะเกิด (ครั้ง/ปี)	เกิดขึ้นได้ยากมาก หรืออาจเกิดขึ้น ๑ ครั้ง/ปี	มีโอกาสเกิดขึ้นน้อยมาก หรืออาจเกิดขึ้น ๒ ครั้ง/ปี	มีโอกาสเกิดขึ้นได้ในบางครั้ง หรืออาจเกิดขึ้น ๓ ครั้ง/ปี	มีโอกาสเกิดขึ้นค่อนข้างสูง หรืออาจเกิดขึ้น ๔ ครั้ง/ปี	มีโอกาสเกิดขึ้นสูง หรืออาจเกิดขึ้นมากกว่า ๕ ครั้ง/ปี
ผลกระทบ (Impact)	I2: ด้านการเงิน	ระดับผลกระทบทางการเงิน มูลค่าความเสียหาย 0 ถึง 10,000 บาท	ระดับผลกระทบทางการเงิน มูลค่าความเสียหาย ๑๐,๐๐๑ ถึง ๒๐๐,๐๐๐ บาท	ระดับผลกระทบทางการเงิน มูลค่าความเสียหาย ๒๐๐,๐๐๑ ถึง ๕๐๐,๐๐๐ บาท	ระดับผลกระทบทางการเงิน มูลค่าความเสียหาย ๕๐๐,๐๐๑ ถึง ๑,๐๐๐,๐๐๐ บาท	ระดับผลกระทบทางการเงิน มูลค่าความเสียหาย มากกว่า ๑,๐๐๐,๐๐๐ บาท
ผลกระทบ (Impact)	I1: ด้านชื่อเสียงและภาพลักษณ์	แทบจะไม่มี	ปรากฏข่าวลือที่อาจพาดพิงคนภายใน หน่วยงาน มีคนร้องเรียน แจ้งเบาะแส	หน่วยตรวจสอบของหน่วยงาน หรือ หน่วยตรวจสอบจากภายนอกเข้า ตรวจสอบข้อเท็จจริง	ภาพลักษณ์ของหน่วยงานติดลบเรื่อง ความโปร่งใส สื่อมวลชน สื่อสังคม ออนไลน์ลงข่าวอย่างต่อเนื่อง และสังคมให้ความสนใจ	เกิดความเสียหายต่อรัฐเจ้าหน้าที่ถูกลงโทษชี้มูลความผิดเข้าสู่กระบวนการทางยุติธรรม ปฏิบัติตามกฎระเบียบฯ ไม่ถูกต้อง และถูกฟ้องร้องดำเนินคดี
ผลกระทบ (Impact)	I3: ด้านกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง	ปฏิบัติตามกฎหมายหรือกฎระเบียบหรือข้อบังคับหรือสัญญาหรือข้อตกลง	ปฏิบัติตามกฎระเบียบฯ ไม่ถูกต้อง และไม่มีคำสั่งแก้ไขจากหน่วยงานกำกับดูแล	ปฏิบัติตามกฎระเบียบฯ ไม่ถูกต้อง และมีคำสั่งแก้ไขปรับปรุงจากหน่วยงานกำกับดูแล	ปฏิบัติตามกฎระเบียบฯ ไม่ถูกต้อง และ ถูกเปรียบเทียบปรับ	ปฏิบัติตามกฎระเบียบฯ ไม่ถูกต้อง และ ถูกฟ้องร้องดำเนินคดี

Risk Score					
โอกาสเกิด (Likelihood)	ผลกระทบ (Impact)				
	1	2	3	4	5
5	ปานกลาง	สูง	สูงมาก	สูงมาก	สูงมาก
4	ปานกลาง	สูง	สูง	สูงมาก	สูงมาก
3	ต่ำ	ปานกลาง	สูง	สูง	สูงมาก
2	ต่ำ	ปานกลาง	ปานกลาง	สูง	สูง
1	ต่ำ	ต่ำ	ต่ำ	ปานกลาง	ปานกลาง

ระดับความรุนแรงของความเสี่ยงการทุจริต

- **สีเขียว หมายถึง ความเสี่ยงระดับต่ำ (ดูแลติดตามความเสี่ยงอย่างต่อเนื่อง)**
- **สีเหลือง หมายถึง ความเสี่ยงระดับปานกลาง (จัดทำแผนและมาตรการควบคุมความเสี่ยง)**
- **สีส้ม หมายถึง ความเสี่ยงระดับสูง (จัดทำแผนและมาตรการควบคุมความเสี่ยง เพิ่มเติม)**
- **สีแดง หมายถึง ความเสี่ยงระดับสูงมาก (จัดทำแผนและมาตรการควบคุมความเสี่ยง อย่างเร่งด่วน)**

หมายเหตุ ธนาคารได้นำหลักเกณฑ์ประเมินความเสี่ยงของธนาคาร มาปรับใช้ร่วมกับเกณฑ์การประเมิน
ความเสี่ยงด้านการทุจริตของ ป.ป.ท. เพื่อให้สอดคล้องและเหมาะสมตามประเด็นความเสี่ยง
การทุจริตที่อาจจะเกิดขึ้น

แบบรายงานการระบุประเด็นความเสี่ยงการทุจริต

ศปท. กระทรวงการคลัง **ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย (ธพว.)**

ชื่อความเสี่ยง	ลำดับขั้นตอน	ขั้นตอนการดำเนินงาน	ประเด็นความเสี่ยงการทุจริต	Risk Score (L x I)			ระดับความเสี่ยง
				Likelihood	Impact	Risk Score	
โครงการ ปรับปรุงประสิทธิภาพระบบเครือข่ายสื่อสาร ศูนย์คอมพิวเตอร์สำรอง (ระยะเวลา ๓ ปี)	๑	จัดทำแผนการจัดซื้อจัดจ้าง	เจ้าหน้าที่พิจารณาเหตุลผความจำเป็นของงาน การจัดทำเอกสารประกอบทุกอย่างเพียงบุคคลเดียว อาจทำให้เหตุผลของงานไม่ตรงตามความต้องการหรือเป็นการเอื้อประโยชน์กับผู้ประกอบการบางรายและใช้เป็นช่องทางการเรียกรับผลประโยชน์หรือสินบน	๑	๒	๒	ต่ำ
	๒	การจัดทำร่างขอบเขตของงาน (TOR) และการกำหนดราคากลาง	- การจัดทำร่างขอบเขตของงาน (TOR) ในลักษณะการเฉพาะเจาะจง หรือเอื้อประโยชน์ให้กับผู้เสนอรายใดรายหนึ่ง เช่น เรียกรับผลประโยชน์จากผู้รับจ้าง มีการให้สินน้ำใจ มีการใช้ดุลยพินิจของคณะกรรมการอย่างไม่เหมาะสม ไม่สอดคล้องกับความต้องการมีการล็อกสเปคทำให้ไม่เกิดการแข่งขัน - เจ้าหน้าที่ ที่พนักงานที่ได้รับมอบหมายไม่ได้มีการสืบราคากลางที่แท้จริง	๒	๓	๖	ปานกลาง
	๓	จัดทำรายงานขอซื้อขอจ้างฯ เสนอต่อผู้มีอำนาจอนุมัติตามวงเงิน	- คณะกรรมการซื้อหรือจ้างอาจมีการเอื้อประโยชน์ให้กับผู้รับจ้าง หรือเรียกรับผลประโยชน์จากผู้รับจ้างมีการให้สินน้ำใจ มีการใช้ดุลยพินิจของคณะกรรมการอย่างไม่หมาะสม กรรมการที่มีลำดับชั้นบังคับบัญชาที่สูงกว่าใช้อำนาจหน้าที่โน้มน้าวจูงใจกรรมการคนอื่น ๆ เพื่อให้การจัดซื้อจัดจ้างเป็นไปอย่างไม่สุจริต	๑	๒	๒	ต่ำ
	๔	คณะกรรมการซื้อหรือจ้างโดยวิธีคัดเลือก จัดทำหนังสือเชิญชวนไปยังผู้ประกอบการ เพื่อยื่นเอกสารข้อเสนอราคา	คณะกรรมการซื้อหรือจ้างฯ ลักลอบให้ข้อมูลสำคัญเกี่ยวกับการยื่นเอกสารเสนอราคาแก่ผู้ประกอบการ เฉพาะรายที่ต้องการเพื่อใช้เป็นเงื่อนไขในการเจรจาต่อรองเรียกรับสินบน	๑	๒	๒	ต่ำ

ชื่อความเสี่ยง	ลำดับขั้นตอน	ขั้นตอนการดำเนินงาน	ประเด็นความเสี่ยงการทุจริต	Risk Score (L x I)			ระดับความเสี่ยง
				Likelihood	Impact	Risk Score	
	๕	ผู้ประกอบการที่ได้รับหนังสือเชิญชวนยื่นข้อเสนอตามวัน เวลา ที่กำหนด	คณะกรรมการฯ มีส่วนได้เสียหรือเอื้อประโยชน์ให้กับผู้ประกอบการที่ยื่นข้อเสนอ เพื่อใช้เจรจาต่อรองเรียกรับสินบนหรือผลประโยชน์	๑	๒	๒	ต่ำ
	๖	คณะกรรมการฯ เปิดซองข้อเสนอดำเนินการพิจารณาผลฯ ทำหน้าที่ตราวจเอกสาร และเจรจาต่อรองราคาและเรียกผู้เสนอราคาต่ำสุดหรือผู้ได้รับการคัดเลือกต่อรองราคา	๖.๑ คณะกรรมการฯ มีส่วนได้เสียหรือเอื้อประโยชน์ให้กับผู้ประกอบการที่ยื่นข้อเสนอ เพื่อใช้เจรจาต่อรองเรียกรับสินบนหรือผลประโยชน์	๓	๕	๑๕	สูงมาก
			๖.๒ ผู้บังคับบัญชาของกรรมการฯ หรือกรรมการผู้พิจารณาผลฯ ที่มีลำดับชั้นบังคับบัญชาที่สูงกว่าใช้อำนาจที่โน้มน้าวใจกรรมการคนอื่น ๆ เพื่อให้มีการจัดซื้อจัดจ้างเป็นไปอย่างไม่สุจริต	๒	๕	๑๐	สูง
			๖.๓ คณะกรรมการพิจารณาผลฯ ได้รับของขวัญจากผู้เสนอราคา เพื่อจูงใจให้คัดเลือกตน หรือคณะกรรมการพิจารณาผลฯ ได้เรียกหรือรับของแถม จากการต่อรองราคากับผู้เสนอราคาต่ำสุดหรือผู้ได้รับการคัดเลือก	๒	๕	๑๐	สูง
	๗	คณะกรรมการฯ รายงานผลการพิจารณาและเสนอความเห็นต่อผู้มีอำนาจอนุมัติ	ผู้มีอำนาจอนุมัติ มีส่วนได้เสียหรือเอื้อประโยชน์ให้กับผู้ประกอบการที่จะซื้อหรือจ้าง	๑	๒	๒	ต่ำ
	๘	หัวหน้าหน่วยงานและผู้มีอำนาจอนุมัติซื้อหรือจ้างเห็นชอบผลการพิจารณา	๘.๑ ผู้มีอำนาจอนุมัติ มีส่วนได้เสียหรือเอื้อประโยชน์กับผู้ประกอบการที่จะซื้อหรือจ้าง	๑	๒	๒	ต่ำ
			๘.๒ ผู้มีอำนาจอนุมัติตามวงเงิน ได้รับของขวัญจากผู้เสนอราคาเพื่อเป็นการจูงใจ	๑	๒	๒	ต่ำ
	๙	ประกาศผู้ชนะการเสนอราคาในเว็บไซต์กรมบัญชีกลาง เว็บไซต์ธนาคาร และปิดประกาศอย่างเปิดเผย	ไม่มีประเด็นความเสี่ยงด้านทุจริต	๑	๑	๑	ต่ำ
	๑๐	จัดทำสัญญา และลงนามสัญญา	เจ้าหน้าที่ส่วนสัญญา ทำสัญญาที่เอื้อประโยชน์ให้ผู้ประกอบการและทำให้ธนาคารเสียผลประโยชน์	๑	๒	๒	ต่ำ

ชื่อความเสี่ยง	ลำดับขั้นตอน	ขั้นตอนการดำเนินงาน	ประเด็นความเสี่ยงการทุจริต	Risk Score (L x I)			ระดับความเสี่ยง
				Likelihood	Impact	Risk Score	
	๑๑	บริหารสัญญา ประกอบด้วย - การส่งมอบ - การตรวจรับ - การจ่ายเงิน	๑๑.๑ คณะกรรมการตรวจรับพัสดุ ตรวจรับงานไม่ตรงตาม TOR หรือตรวจรับงานในขณะที่งานยังไม่แล้วเสร็จหรือตรวจรับงานโดยที่คู่สัญญายังไม่ส่งมอบงาน	๑	๒	๒	ต่ำ
			๑๑.๒ คณะกรรมการตรวจรับพัสดุรับงานล่าช้า เพื่อใช้เจรจาต่อรองเรียกรับสินบน หรือผลประโยชน์	๑	๒	๒	ต่ำ
			๑๑.๓ เจ้าหน้าที่ ดำเนินการเบิกจ่ายล่าช้า เพื่อใช้เป็นเงื่อนไขในการเจรจาต่อรองเรียกรับสินบนกับคู่สัญญา	๑	๒	๒	ต่ำ

แบบรายงานแผนบริหารจัดการความเสี่ยงการทุจริต

ศปท. กระทรวงการคลัง	ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย (ธพว.)

การอนุมัติของผู้บริหาร		การเผยแพร่ในเว็บไซต์หน่วยงาน	Link เผยแพร่
ผ่านการอนุมัติแล้ว		ดำเนินการแล้ว	**https://www.smebank.co.th/**

ขั้นตอน	ประเด็นความเสี่ยงการทุจริต	ระดับความเสี่ยง	มาตรการควบคุมความเสี่ยงการทุจริต	วิธีดำเนินการ	ระยะเวลาดำเนินการ	งบประมาณ (บาท)	ผู้รับผิดชอบ
ขั้นตอนที่ ๒ การจัดทำร่างขอบเขตของงาน (TOR) และการกำหนดราคากลาง					๔๕ วัน	๕๐,๐๐๐,๐๐๐.๐๐	ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย
	- การจัดทำร่างขอบเขตของงาน (TOR) ในลักษณะการเฉพาะเจาะจง หรือเอื้อประโยชน์ให้กับผู้เสนอรายใดรายหนึ่ง เช่น เรียกรับผลประโยชน์จากผู้รับจ้าง มีการให้สินน้ำใจ มีการใช้ดุลยพินิจของคณะกรรมการอย่างไม่เหมาะสมไม่สอดคล้องกับความต้องการมีการล็อกสเปคทำให้ไม่เกิดการแข่งขัน - เจ้าหน้าที่ ที่พนักงานที่ได้รับมอบหมายไม่ได้มีการสืบราคากลางที่แท้จริง	**ปานกลาง**	๑. มีการทบทวนคู่มือการปฏิบัติงาน/แบบฟอร์มที่ใช้ดำเนินการจัดซื้อจัดจ้าง เพื่อยกระดับความโปร่งใส ในกระบวนการจัดซื้อจัดจ้าง	๑. ฝ่ายการบริหารพัสดุทบทวนคู่มือการปฏิบัติงาน/แบบฟอร์มที่ใช้ดำเนินการจัดซื้อจัดจ้าง เพื่อยกระดับความโปร่งใส ในกระบวนการจัดซื้อจัดจ้าง			
			๒. กำหนดมาตรการการป้องกันการรับสินบนของ ธพว.	๒.ธนาคาร ประกาศนโยบายไม่รับของขวัญและของกำนัลทุกชนิดจากการปฏิบัติหน้าที่ (No Gift Policy) ปี ๒๕๖๗ เพื่อให้ผู้บริหารและพนักงานถือปฏิบัติอย่างเคร่งครัด			
			๓. จัดทำแบบฟอร์มเปิดเผยความขัดแย้งทางผลประโยชน์ และไม่เรียกรับสินบน ของกำนัลหรือประโยชน์ใด ๆ ในกระบวนการจัดซื้อ จัดจ้าง โดยให้คณะกรรมการพิจารณาผลฯ ลงนามรับทราบทุกท่าน	๓. ให้คณะกรรมการกำหนดร่างขอบเขตของงาน (TOR) ทุกคนลงนามรับทราบข้อตกลงในการที่จะไม่เรียกรับสินบน หรือผลประโยชน์ใดๆ จากผู้มีส่วนได้ส่วนเสียกับธนาคาร			
			๔. มีการทบทวนคู่มือจรรยาบรรณคู่ค้าทางธุรกิจทาง ธพว.	๔. ฝ่ายการบริหารพัสดุทบทวนคู่มือจรรยาบรรณคู่ค้าทางธุรกิจทาง ธพว.			
			๕. มีการเพิ่มช่องทางในการแจ้งข้อร้องเรียนการทุจริตและประพฤติมิชอบ ถึงฝ่ายป้องกันการทุจริตและส่งเสริมธรรมาภิบาล โดยตรง เพื่อเพิ่มความเชื่อมั่นให้กับผู้แจ้งข้อร้องเรียน	๕. ธนาคารมีการเพิ่มช่องทางในการแจ้งเรียนการทุจริตและประพฤติมิชอบ ถึงฝ่ายป้องกันการทุจริตและส่งเสริมธรรมาภิบาล โดยตรง เพื่อเพิ่มความเชื่อมั่นให้กับผู้แจ้งข้อร้องเรียน			
			๖. เสริมสร้างความตระหนักในการปฏิบัติตามกฎเกณฑ์และกฎระเบียบอย่างเคร่งครัด	๖. จัดอบรมและเสริมสร้างความตระหนักรู้ ผ่าน website ธนาคาร Outlook และE-leaning ของธนาคาร			
			๗. หน่วยงานตรวจสอบภายในเข้าดำเนินการตรวจสอบกระบวนการจัดซื้อจัดจ้าง	๗. กำหนดแผนการตรวจสอบภายในประจำปี			

ขั้นตอน	ประเด็นความเสี่ยงการทุจริต	ระดับความเสี่ยง	มาตรการควบคุมความเสี่ยงการทุจริต	วิธีดำเนินการ	ระยะเวลาดำเนินการ	งบประมาณ (บาท)	ผู้รับผิดชอบ
<u>ขั้นตอนที่ ๖</u> คณะกรรมการพิจารณาผลฯ ทำหน้าที่ตรวจเอกสาร และเจรจาต่อรองราคา และเรียกผู้เสนอราคาต่ำสุดหรือผู้ได้รับการคัดเลือก ต่อรองราคา					**๔๕ วัน**	**๕๐,๐๐๐,๐๐๐.๐๐**	**ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย**
	ขั้นตอนที่ ๖.๑ คณะกรรมการฯ มีส่วนได้เสียหรือเอื้อประโยชน์ให้กับผู้ประกอบการที่ยื่นข้อเสนอ เพื่อใช้เจรจาต่อรองเรียกรับสินบน หรือผลประโยชน์	**สูงมาก**	๑. แต่งตั้งคณะกรรมการพิจารณาผลฯ	๑. ธนาคารแต่งตั้งคณะกรรมการพิจารณาผลฯ			
			๒. กำหนดมาตรการการป้องกันการรับสินบนของ ธพว.	๒.ธนาคาร ประกาศนโยบายไม่รับของขวัญและของกำนัลทุกชนิดจากการปฏิบัติหน้าที่ (No Gift Policy) ปี ๒๕๖๗ เพื่อให้ผู้บริหารและพนักงานถือปฏิบัติอย่างเคร่งครัด			
			๓. คณะกรรมการพิจารณาผลฯ เจ้าหน้าที่ และผู้มีอำนาจตามวงเงิน ต้องรับรองตนเอง ว่าเป็นผู้ไม่มีส่วนได้เสีย และไม่มีผลประโยชน์ทับซ้อนกับบริษัทหรือผู้ประกอบการ	๓.๑. ลงนามรับรองในเอกสารการจัดซื้อจัดจ้างเกี่ยวกับการทำหน้าที่ของคณะกรรมการพิจารณาผลฯ ๓.๒. ให้กรรมการที่มีความสัมพันธ์กับผู้ประกอบการเช่น พี่น้อง เครือญาติ ต้องแจ้งผู้บังคับบัญชา เพื่อถอนตัวจากการเป็นกรรมการ			
			๔. มีการทบทวนคู่มือการปฏิบัติงาน/แบบฟอร์มที่ใช้ดำเนินการจัดซื้อจัดจ้าง เพื่อยกระดับความโปร่งใส ในกระบวนการจัดซื้อจัดจ้าง	๔. ฝ่ายการบริหารพัสดุทบทวนคู่มือการปฏิบัติงาน/แบบฟอร์มที่ใช้ดำเนินการจัดซื้อจัดจ้าง เพื่อยกระดับความโปร่งใส ในกระบวนการจัดซื้อจัดจ้าง			
			๕. จัดทำแบบฟอร์มเปิดเผยความขัดแย้งทางผลประโยชน์ และไม่เรียกรับสินบน ของกำนัลหรือประโยชน์ใด ๆ ในกระบวนการจัดซื้อ จัดจ้าง โดยให้คณะกรรมการพิจารณาผลฯ ลงนามรับทราบทุกท่าน	๕. ให้คณะกรรมการพิจารณาผลฯ ทุกคนลงนามรับทราบข้อตกลงในการที่จะไม่เรียกรับสินบน หรือผลประโยชน์ใดๆ จากผู้มีส่วนได้ส่วนเสียกับธนาคาร			
			๖. มีการทบทวนคู่มือจรรยาบรรณคู่ค้าทางธุรกิจทาง ธพว.	๖. ฝ่ายการบริหารพัสดุทบทวนคู่มือจรรยาบรรณคู่ค้าทางธุรกิจทาง ธพว.			
			๗. มีการเพิ่มช่องทางในการแจ้งข้อร้องเรียนการทุจริตและประพฤติมิชอบ ถึงฝ่ายป้องกันการทุจริตและส่งเสริมธรรมาภิบาลโดยตรง เพื่อเพิ่มความเชื่อมั่นให้กับผู้แจ้งข้อร้องเรียน	๗. ธนาคารมีการเพิ่มช่องทางในการแจ้งเรียนการทุจริตและประพฤติมิชอบ ถึงฝ่ายป้องกันการทุจริตและส่งเสริมธรรมาภิบาลโดยตรง เพื่อเพิ่มความเชื่อมั่นให้กับผู้แจ้งข้อร้องเรียน			
			๘. จัดทำข้อตกลงคุณธรรม (Integrity Pact) ความร่วมมือป้องกันและต่อต้านการทุจริต	๘. ให้คณะกรรมการพิจารณาผลฯ ทุกคนลงนามรับทราบข้อตกลงคุณธรรม (Integrity Pact) ความร่วมมือป้องกันและต่อต้านการทุจริต			
			๙. เสริมสร้างความตระหนักในการปฏิบัติตามกฎเกณฑ์และกฎระเบียบอย่างเคร่งครัด	๙. จัดอบรมและเสริมสร้างความตระหนักรู้ ผ่าน website ธนาคาร Outlook และE-leaning ของธนาคาร			
			๑๐. หน่วยงานตรวจสอบภายในเข้าดำเนินการตรวจสอบกระบวนการจัดซื้อจัดจ้าง	๑๐. กำหนดแผนการตรวจสอบภายในประจำปี			

ขั้นตอน	ประเด็นความเสี่ยงการทุจริต	ระดับความเสี่ยง	มาตรการควบคุมความเสี่ยงการทุจริต	วิธีดำเนินการ	ระยะเวลาดำเนินการ	งบประมาณ (บาท)	ผู้รับผิดชอบ
			๑๑.จัดทำ Check List เอกสารประกอบการพิจาณาผลฯ ตามที่คณะกรรมการ TOR กำหนด	๑๑. กำหนดให้คณะกรรมการพิจารณาผลฯ ต้องตรวจสอบเอกสารหลักฐานว่ามีครบถ้วนตาม Check List เอกสารประกอบการขออนุมัติจัดซื้อจัดจ้าง			
			๑๒. จัดทำบันทึกข้อตกลงปฏิบัติตามจรรยาบรรณคู่ค้าทางธุรกิจของ ธพว.	๑๒. กำหนดให้คู่ค้าลงนามรับทราบและยินยอมปฏิบัติตามจรรยาบรรณคู่ค้าทางธุรกิจของ ธพว.			
			๑๓.จัดทำ Check List เอกสารประกอบการพิจาณาผลฯ ตามที่คณะกรรมการ TOR กำหนด	๑๓. กำหนดให้คณะกรรมการพิจารณาผลฯ ต้องตรวจสอบเอกสารหลักฐานว่ามีครบถ้วนตาม Check List เอกสารประกอบการขออนุมัติจัดซื้อจัดจ้าง			
			๑๔. จัดทำบันทึกข้อตกลงปฏิบัติตามจรรยาบรรณคู่ค้าทางธุรกิจของ ธพว.	๑๔. กำหนดให้คู่ค้าลงนามรับทราบและยินยอมปฏิบัติตามจรรยาบรรณคู่ค้าทางธุรกิจของ ธพว.			
			๑๕. กำหนดบทลงโทษอย่างเคร่งครัดต่อเจ้าหน้าที่ที่มีพฤติกรรมการทุจริต	๑๕. ผู้ที่กระทำความผิดจะได้รับการลงโทษทางวินัย ตามระเบียบข้อบังคับว่าด้วยการบริหารงานบุคคล เงินตอบแทน และค่าใช้จ่าย **อื่นของธนาคาร พ.ศ. ๒๕๖๒ (ฉบับใหม่) บทที่ ๘ วินัย การ** ดำเนินการทางวินัย และการลงโทษ และการดำเนินคดีต่างๆ ตามที่กฎหมายกำหนด			
<u>ขั้นตอนที่ ๖</u> คณะกรรมการพิจารณาผลฯ ทำหน้าที่ตรวจเอกสาร และเจรจาต่อรองราคา และเรียกผู้เสนอราคาต่ำสุดหรือผู้ได้รับการคัดเลือก ต่อรองราคา					**๔๕ วัน**	**๕๐,๐๐๐,๐๐๐.๐๐**	**ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย**
	ขั้นตอนที่ ๖.๒ ผู้บังคับบัญชาของกรรมการพิจารณาผลฯ หรือกรรมการผู้พิจารณาผลฯ ที่มีลำดับชั้นบังคับบัญชาที่สูงกว่าใช้อำนาจที่ไม่มีชอบธรรมแทรกแซงการปฏิบัติงานของกรรมการพิจารณาผลฯ เพื่อให้มีการจัดซื้อจัดจ้างเป็นไปอย่างไม่สุจริต	**สูง**	๑. คณะกรรมการพิจารณาผลฯ เจ้าหน้าที่ และผู้มีอำนาจตามวงเงิน ต้องรับรองตนเอง ว่าเป็นผู้ไม่มีส่วนได้เสีย และไม่มีผลประโยชน์ทับซ้อนกับบริษัทหรือผู้ประกอบการ	๑.๑ ลงนามรับรองในเอกสารการจัดซื้อจัดจ้างเกี่ยวกับการทำหน้าที่ของคณะกรรมการพิจารณาผลฯ ๑.๒ ให้กรรมการที่มีความสัมพันธ์กับผู้ประกอบการเช่น พี่น้อง เครือญาติ ต้องแจ้งผู้บังคับบัญชา เพื่อถอนตัวจากการเป็นกรรมการ			
			๒. กำหนดมาตรการการป้องกันการรับสินบนของ ธพว.	๒.ธนาคาร ประกาศนโยบายไม่รับของขวัญและของกำนัลทุกชนิดจากการปฏิบัติหน้าที่ (No Gift Policy) ปี ๒๕๖๗ เพื่อให้ผู้บริหารและพนักงานถือปฏิบัติอย่างเคร่งครัด			
	ขั้นตอนที่ ๖.๓ คณะกรรมการพิจารณาผลฯ ได้รับของขวัญจากผู้เสนอราคา เพื่อจูงใจให้คัดเลือกตน หรือคณะกรรมการพิจารณาผลฯ ได้เรียกหรือรับของแถม จากการต่อรองราคากับผู้เสนอราคาต่ำสุดหรือผู้ได้รับการคัดเลือก		๓. มีการทบทวนคู่มือการปฏิบัติงาน/แบบฟอร์มที่ใช้ดำเนินการจัดซื้อจัดจ้าง เพื่อยกระดับความโปร่งใส ในกระบวนการจัดซื้อจัดจ้าง	๓. ฝ่ายการบริหารพัสดุทบทวนคู่มือการปฏิบัติงาน/แบบฟอร์มที่ใช้ดำเนินการจัดซื้อจัดจ้าง เพื่อยกระดับความโปร่งใส ในกระบวนการจัดซื้อจัดจ้าง			
		สูง	๔. จัดทำแบบฟอร์มเปิดเผยความขัดแย้งทางผลประโยชน์ และไม่เรียกรับสินบน ของกำนัลหรือประโยชน์ใด ๆ ในกระบวนการจัดซื้อ จัดจ้าง โดยให้คณะกรรมการพิจารณาผลฯ ลงนามรับทราบทุกท่าน	๔. ให้คณะกรรมการพิจารณาผลฯ ทุกคนลงนามรับทราบข้อตกลงในการที่จะไม่เรียกรับสินบน หรือผลประโยชน์ใดๆ จากผู้มีส่วนได้ส่วนเสียกับธนาคาร			

ขั้นตอน	ประเด็นความเสี่ยงการทุจริต	ระดับความเสี่ยง	มาตรการควบคุมความเสี่ยงการทุจริต	วิธีดำเนินการ	ระยะเวลาดำเนินการ	งบประมาณ (บาท)	ผู้รับผิดชอบ
			๕. มีการทบทวนคู่มือจรรยาบรรณคู่ค้าทางธุรกิจทาง ธพว.	๕. ฝ่ายการบริหารพัสดุทบทวนคู่มือจรรยาบรรณคู่ค้าทางธุรกิจทาง ธพว.			
			๖. มีการเพิ่มช่องทางในการแจ้งข้อร้องเรียนการทุจริตและประพฤติมิชอบ ถึงฝ่ายป้องกันการทุจริตและส่งเสริมธรรมาภิบาลโดยตรง เพื่อเพิ่มความเชื่อมั่นให้กับผู้แจ้งข้อร้องเรียน	๖. ธนาคารมีการเพิ่มช่องทางในการแจ้งเรียนการทุจริตและประพฤติมิชอบ ถึงฝ่ายป้องกันการทุจริตและส่งเสริมธรรมาภิบาลโดยตรง เพื่อเพิ่มความเชื่อมั่นให้กับผู้แจ้งข้อร้องเรียน			
			๗. จัดทำข้อตกลงคุณธรรม (Integrity Pact) ความร่วมมือป้องกันและต่อต้านการทุจริต	๗. ให้คณะกรรมการพิจารณาผลฯ ทุกคนลงนามรับทราบข้อตกลงคุณธรรม (Integrity Pact) ความร่วมมือป้องกันและต่อต้านการทุจริต			
			๘. เสริมสร้างความตระหนักในการปฏิบัติตามกฎเกณฑ์และกฎระเบียบอย่างเคร่งครัด	๘. จัดอบรมและเสริมสร้างความตระหนักรู้ ผ่าน website ธนาคาร Outlook และE-leaning ของธนาคาร			
			๙. หน่วยงานตรวจสอบภายในเข้าดำเนินการตรวจสอบกระบวนการจัดซื้อจัดจ้าง	๙. กำหนดแผนการตรวจสอบภายในประจำปี			
			๑๐.จัดทำ Check List เอกสารประกอบการพิจาณาผลฯ ตามที่ คณะกรรมการ TOR กำหนด	**๑๐. กำหนดให้คณะกรรมการพิจารณาผลฯ ต้องตรวจสอบเอกสาร** หลักฐานว่ามีครบถ้วนตาม Check List เอกสารประกอบการขออนุมัติจัดซื้อจัดจ้าง			
			๑๑. จัดทำบันทึกข้อตกลงปฏิบัติตามจรรยาบรรณคู่ค้าทางธุรกิจของ ธพว.	๑๑. กำหนดให้คู่ค้าลงนามรับทราบและยินยอมปฏิบัติตามจรรยาบรรณคู่ค้าทางธุรกิจของ ธพว.			
			๑๒.จัดทำ Check List เอกสารประกอบการพิจาณาผลฯ ตามที่คณะกรรมการ TOR กำหนด	๑๒. กำหนดให้คณะกรรมการพิจารณาผลฯ ต้องตรวจสอบเอกสารหลักฐานว่ามีครบถ้วนตาม Check List เอกสารประกอบการขออนุมัติจัดซื้อจัดจ้าง			
			๑๓. กำหนดบทลงโทษอย่างเคร่งครัดต่อเจ้าหน้าที่ที่มีพฤติกรรมการทุจริต	๑๓. ผู้ที่กระทำความผิดจะได้รับการลงโทษทางวินัย ตามระเบียบข้อบังคับว่าด้วยการบริหารงานบุคคล เงินตอบแทน และค่าใช้จ่ายอื่นของธนาคาร พ.ศ. ๒๕๖๒ (ฉบับใหม่) บทที่ ๘ วินัย การดำเนินการทางวินัย และการลงโทษ และการดำเนินคดีต่างๆ ตามที่กฎหมายกำหนด			

ลงชื่อ .....

(นายณัฐพล นภาพรชนะ)

ตำแหน่ง ผู้อำนวยการฝ่ายป้องกันการทุจริตและส่งเสริมธรรมาภิบาล

วันที่ ๒๙ เมษายน ๒๕๖๗

แบบรายงานที่ ๔ แบบรายงานประมาณการงบประมาณโครงการจัดซื้อจัดจ้าง

แบบแสดงรายละเอียดประมาณการงบประมาณโครงการจัดซื้อจัดจ้าง ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

ศปท. กระทรวง	ชื่อหน่วยงาน	ส่วนราชการที่ดำเนินการจัดซื้อจัดจ้าง	ชื่อโครงการ	งบประมาณ (บาท)	ประเภทงบประมาณ	วิธีจัดซื้อจัดจ้าง	ระยะเวลาดำเนินการ	โครงการ IP	โครงการ CoST
กระทรวงการคลัง/กระทรวงอุตสาหกรรม	ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย	ฝ่ายการบริหารพัสดุ ดำเนินการโดยคณะกรรมการซื้อหรือจ้าง **โดยวิธีคัดเลือก**	โครงการปรับปรุงประสิทธิภาพระบบเครือข่ายสื่อสารศูนย์คอมพิวเตอร์สำรอง **(ระยะเวลา 3 ปี)**	๕๐,๐๐๐,๐๐๐	เงินงบประมาณ	วิธีคัดเลือก	๔๕ วัน	-	-

ที่	รายการ	รายละเอียด (ประเภท จำนวน คุณลักษณะ(Spec) อื่นๆ)	ประมาณการงบประมาณ (Cost breakdown)	รวมงบประมาณ (บาท)
๑	อุปกรณ์ค้นหาเส้นทาง จำนวน ๓ ชุด (ติดตั้งสำนักงานใหญ่ ๒ ชุด / ติดตั้งศูนย์คอมพิวเตอร์สำรอง ๑ ชุด)	๑.๑ มี CPU Architecture แบบ x๘๖ ขนาดไม่น้อยกว่า ๑๒ Core หรือดีกว่าหรือเทียบเท่า และมี IPv๔ Forwarding Throughput ไม่ต่ำกว่า ๒๐ Gbps หรือมี Forwarding performance ไม่ต่ำกว่า ๑๒๐ Mpps **๑.๒ มี IPsec Throughput ได้ไม่ต่ำกว่า ๑๙ Gbps** ๑.๓ มีหน่วยความจำแบบ Ram หรือ DRAM ขนาดไม่น้อยกว่า ๑๖ GB และ มี Flash Memory หรือ Flash Storage ขนาดไม่น้อยกว่า ๑ GB ๑.๔ มีWANพอร์ต แบบ๑GbpsชนิดRJ๔๕ จำนวนไม่น้อยกว่า๘พอร์ต และมี WAN พอร์ต แบบ๑๐ Gbps ชนิด SFP+ จำนวนไม่น้อยกว่า ๔ พอร์ต เสนอ Transceiver Module ชนิด ๑๐G Base-SR จำนวน ๔ โมดูล **๑.๕ รองรับการทำ IPSec SVTI Tunnels ได้ไม่น้อยกว่า ๔,๐๐๐ Tunnels** ๑.๖ รองรับ Routes IPV๔ หรือ IPv๖ ได้ไม่น้อยกว่า ๒,๐๐๐,๐๐๐ Routes ๑.๗ สามารถทำ IPv๔ และ IPv๖ แบบ Static Route ได้ ๑.๘ สามารถทำ IPv๔ Routing Protocol ได้แก่ RIPv๒, OSPF และ BGP ได้เป็นอย่างน้อย **๑.๙ สามารถทำ IPv๖ Routing Protocol ได้แก่ BGP ได้เป็นอย่างน้อย** ๑.๑๐ สามารถกำหนด Traffic Management Quality of Service (QoS) ตามมาตรฐาน Class-Based Weighted Fair Queuing (CBWFQ) หรือ Weighted Random Early Detection (WRED) หรือ เทียบเท่าได้ ๑.๑๑ การทำ CBWFQ QoS จะต้องสามารถทำที่ WAN port แต่ละ WAN Port และ Tunnel แต่ละ Tunnel แยกจากกันได้ หรือ Protocol อื่นที่เทียบเท่าได้ ๑.๑๒ สามารถส่งข้อมูลสถิติการใช้งานเครือข่าย (IP Flow Usage Statistic) ในรูปแบบ Netflowหรือ Cflowได้ ๑.๑๓ รองรับการทำงานร่วมกับระบบบริหารและจัดการ Network Infrastructure แบบ Software-Defined WAN (SD-WAN) และรองรับการทำ Programmable APIs ๑.๑๔ สามารถทำงานตามมาตรฐาน SSH, NTP, SNMPv๓ ได้ ๑.๑๕ มีพอร์ต Console อย่างน้อย ๑ พอร์ต ๑.๑๖ ผ่านการรับรองตามมาตรฐานความปลอดภัย UL หรือ EN หรือ IEC หรือ เทียบเท่า ได้ ๑.๑๗ อุปกรณ์ที่นำเสนอ ต้องมี Rack Mount สามารถติดตั้งบน Rack ๑๙" ได้ ๑.๑๘ มีRedundant Power Supply ในตัวอุปกรณ์โดยสามารถใช้กับระบบไฟฟ้าในประเทศไทยแบบ ๒๒๐VAC ๕๐Hz ได้ และแหล่งจ่ายไฟนี้จะต้องทำงานได้ในลักษณะ Hot-Swappable ได้ ๑.๑๙ อุปกรณ์ที่นำเสนอ ต้องสามารถทำงานร่วมกันได้กับ ระบบบริหารและจัดการเครือข่าย Network Access Control ที่ทางธนาคารฯใช้อยู่ ยี่ห้อ Cisco Identity Service Engine (ISE) ผ่าน Protocol TACACS+ ได้ ๑.๒๐ อุปกรณ์ที่นำเสนอ ต้องสามารถ ส่ง Log ไปยัง SIEM ของธนาคารฯได้ ๑.๒๑ อุปกรณ์ที่นำเสนอต้องเป็นยี่ห้อเดียวกันกับ Router สาขาที่ทางธนาคารฯใช้งานอยู่ในปัจจุบัน ซึ่งสามารถเชื่อมต่อและรับส่งข้อมูลกับRouter สาขา จำนวน๙๕สาขา ต่างๆของธนาคารฯได้ อย่างไม่ มีปัญหา เช่น การเชื่อมต่อกับ MPLS ของ NT เป็นต้น ๑.๒๒ อุปกรณ์ที่นำเสนอ ต้องเป็นรุ่นที่ยังอยู่ในสายการผลิตในปัจจุบัน โดยต้องได้รับการแต่งตั้งจากเจ้าของผลิตภัณฑ์ หรือ สาขาเจ้าของผลิตภัณฑ์ในประเทศไทย		

ที่	รายการ	รายละเอียด (ประเภท จำนวน คุณลักษณะ(Spec) อื่นๆ)	ประมาณการงบประมาณ (Cost breakdown)	รวมงบประมาณ (บาท)
๒	อุปกรณ์กระจายสัญญาณหลัก (Core Switch) จำนวน ๑ ชุด	๒.๑ เป็น Layer ๓ Switch ทีมีขนาด bandwidth ไม่น้อยกว่า ๓.๖ Tbps. ๒.๒ อุปกรณ์ทำงานแบบ Low Latency โดยมี Latency ไม่เกิน ๑ microsecond ๒.๓ มีพอร์ต ๑/๑๐/๒๕ Gigabit Ethernet จำนวนไม่น้อยกว่า ๔๘ พอร์ต พร้อมเสนอ Transceiver Modules แบบ ๑๐ Gbps. ชนิด **๑๐GBase-SR หรือเทียบเท่า จำนวนไม่น้อยกว่า ๕๔ โมดูล** ๒.๔ มีพอร์ต ๔๐/๑๐๐ Gigabit Ethernet จำนวนไม่น้อยกว่า ๖ พอร์ต ๒.๕ รองรับการทำงาน แบบ protocol มาตรฐานเช่น VXLAN ได้เป็นอย่างน้อย **๒.๖ สามารถทำการเชื่อมต่อกับNetworkภายนอกด้วยRouting Protocol แบบ BGP, OSPF, PBR, และ VRF** ๒.๗ สามารถทำงานตามมาตรฐาน SSH, NTP, SNMPv๓ ได้ ๒.๘ รองรับการทำ remote leaf หรือ leaf switch ได้ ๒.๙ รองรับการทำงานร่วมกับระบบบริหารและจัดการ Network Infrastructure แบบ Software-Defined Network (SDN) ได้ **๒.๑๐ มีพัดลมระบายความร้อนสามารถถอดเปลี่ยนได้** ๒.๑๑ อุปกรณ์ที่นำเสนอ ต้องมี Rack Mount สามารถติดตั้งบน Rack ๑๙" ได้ ๒.๑๒ ผ่านการรับรองตามมาตรฐานความปลอดภัย UL หรือ EN หรือ IEC หรือ เทียบเท่า ได้ ๒.๑๓ มีRedundant Power Supply ในตัวอุปกรณ์โดยสามารถใช้กับระบบไฟฟ้าในประเทศไทยแบบ ๒๒๐ VAC ๕๐Hz ได้ และ**แหล่งจ่ายไฟนี้จะต้องทำงานได้ในลักษณะ Hot-Swappable ได้** ๒.๑๔ อุปกรณ์ที่นำเสนอ ต้องสามารถทำงานร่วมกันได้กับ ระบบบริหารและจัดการเครือข่าย Network Access Control ที่ทางธนาคารใช้อยู่ ยี่ห้อ Cisco Identity Service Engine (ISE) ผ่าน Protocol TACACS+ ได้ ๒.๑๕ อุปกรณ์ที่นำเสนอ ต้องสามารถ ส่ง Log ไปยัง SIEM ของธนาคารฯได้ **๒.๑๖ อุปกรณ์ที่นำเสนอ ต้องเชื่อมต่อและรับส่งข้อมูลกับอุปกรณ์Network หรือ อุปกรณ์Server ต่างๆของ ธนาคารฯได้อย่างไม่มีปัญหา** ๒.๑๗ อุปกรณ์ที่นำเสนอ ต้องเป็นรุ่นที่ยังอยู่ในสายการผลิตในปัจจุบัน โดยต้องได้รับการแต่งตั้งจากเจ้าของ ผลิตภัณฑ์ หรือ สาขาเจ้าของผลิตภัณฑ์ในประเทศไทย		
๓	อุปกรณ์กระจายสัญญาณย่อย จำนวน ๒ ชุด	๓.๑ มี Switching Bandwidth ขนาดไม่น้อยกว่า ๑๒๘ Gbps. ๓.๒ มีประสิทธิภาพในการส่งผ่านข้อมูล Forwarding Rate ไม่น้อยกว่า ๔๐ Mpps. ๓.๓ มีพอร์ต Gigabit Ethernet แบบ ๑๐/๑๐๐/๑๐๐๐ จำนวนไม่น้อยกว่า ๒๔ พอร์ต ๓.๔ มีพอร์ตGigabit Ethernet แบบ SFP+ จำนวนไม่น้อยกว่า ๔ พอร์ต พร้อมเสนอ Transceiver Modules แบบ ๑๐ Gbps. ชนิด ๑๐GBase-SR หรือเทียบเท่า จำนวนไม่น้อยกว่า ๔ โมดูล ๓.๕ รองรับการทำStacking ได้ไม่น้อยกว่า ๘ อุปกรณ์ และ มี Stacking Throughput ไม่น้อยกว่า ๘๐ Gbps. ๓.๖ สามารถทำ MTU ได้ไม่น้อยกว่า ๙,๐๐๐ Bytes ๓.๗ สามารถทำ ตามมาตรฐาน IEEE๘๐๒.๑p และ IEEE๘๐๒.๑q ๓.๘ สามารถทำงาน ทั้ง IP Version ๔ และ IP Version ๖ ๓.๙ สามารถทำ Spanning tree ตามมาตรฐาน IEEE๘๐๒.๑D, IEEE๘๐๒.๑w และ IEEE๘๐๒.๑s ๓.๑๐ สามารถทำ Port Aggregation ตามมาตรฐาน IEEE๘๐๒.๓ad ได้ **๓.๑๑ รองรับการทำ VLAN ได้ไม่น้อยกว่า ๒๕๐ active VLANหรือ Switched Virtual Interfaces (SVIs)** ๓.๑๒ รองรับ MAC address ได้ไม่น้อยกว่า ๑๕,๐๐๐ MAC address ๓.๑๓ มี Console Port เพื่อกำหนดค่าการทำงานของอุปกรณ์ และสำหรับตรวจสอบระบบได้ ๓.๑๔ สามารถทำงานตามมาตรฐาน SSH, NTP, SNMPv๓ ได้ **๓.๑๕ อุปกรณ์ที่นำเสนอ ต้องมี Rack Mount สามารถติดตั้งบน Rack ๑๙" ได้** ๓.๑๖ ผ่านการรับรองตามมาตรฐานความปลอดภัย UL หรือ EN หรือ IEC หรือ เทียบเท่า ได้ ๓.๑๗ มีRedundant Power Supply ในตัวอุปกรณ์โดยสามารถใช้กับระบบไฟฟ้าในประเทศไทยแบบ ๒๒๐ VAC ๕๐Hz ได้ และแหล่งจ่ายไฟนี้จะต้องทำงานได้ในลักษณะ Hot-Swappable ได้ **๓.๑๘ อุปกรณ์ที่นำเสนอ ต้องสามารถทำงานร่วมกันได้กับระบบบริหารและจัดการเครือข่าย Network Access Control ที่ทางธนาคารฯใช้อยู่ ยี่ห้อ** Cisco Identity Service Engine (ISE) ผ่าน Protocol TACACS+ ได้ ๓.๑๙ อุปกรณ์ที่นำเสนอ ต้องสามารถส่ง Log ไปยัง SIEM ของธนาคารฯได้ ๓.๒๐ อุปกรณ์ที่นำเสนอ ต้องเชื่อมต่อและรับส่งข้อมูลกับอุปกรณ์Network หรือ อุปกรณ์Server ต่างๆ ของ ธนาคารฯได้อย่างไม่มีปัญหา **๓.๒๑ อุปกรณ์ที่นำเสนอ ต้องเป็นรุ่นที่ยังอยู่ในสายการผลิตในปัจจุบัน โดยต้องได้รับการแต่งตั้งจากเจ้าของ ผลิตภัณฑ์ หรือ สาขาเจ้าของผลิตภัณฑ์** ในประเทศไทย		

ที่	รายการ	รายละเอียด (ประเภท จำนวน คุณลักษณะ(Spec) อื่นๆ)	ประมาณการงบประมาณ (Cost breakdown)	รวมงบประมาณ (บาท)
๔	อุปกรณ์ป้องกันการบุกรุก แบบที่ ๑ จำนวน ๑ ชุด (Branch Zone)	๔.๑ มี Layer ๔Firewall Throughput ไม่น้อยกว่า ๗๐Gbps และ IPSec VPN ได้ ๕๕Gbps ๔.๒ มี Layer ๗ Firewall Throughput (NGFW) ไม่น้อยกว่า ๑๑ Gbps และ Threat prevention หรือ IPS Throughput ไม่น้อยกว่า ๑๔ Gbps ในแบบ Appmixหรือ Enterprise testing condition หรือ Enterprise traffic mix และจำนวน Max Sessions หรือ Max Concurrentsได้ไม่**น้อยกว่า ๘,๐๐๐,๐๐๐ sessions และ New Sessions หรือ New Connections ไม่น้อยกว่า ๕๕๐,๐๐๐ ต่อวินาที** ๔.๓ มีพอร์ต GE RJ๔๕ จำนวนไม่น้อยกว่า ๑๖ ช่อง มีช่องเสียบ module GE SFP หรือดีกว่า จำนวนไม่น้อยกว่า ๘ ช่อง และมีช่องเสียบ module ๑๐GE SFP+ จำนวนไม่น้อยกว่า ๔ ช่อง พร้อมเสนอ Transceiver Module ๑๐ GE SFP+ ชนิด SR จำนวน ๔โมดูล ๔.๔ รองรับการทำงานในลักษณะของไฟล์วอลล์เสมือน (Logical System หรือ Virtual System หรือ Virtual Domain หรือ Security Context หรือ **Multi-Instanceหรือ เทียบเท่า ได้)** ๔.๕ สามารถบริหารจัดการอุปกรณ์แบบ Web-based หรือ CLI (Command Line Interface) หรือ GUI (Graphic User Interface) ได้ ๔.๖ รองรับการทำงานแบบ High Availability แบบ Active/Active หรือ Active/Passive หรือ แบบ Active-Stand by ได้ ๔.๗ สามารถป้องกันภัยคุกคามประเภท Virus หรือ Vulnerability หรือ Spyware(หรือ Anti-Bot) ได้ โดยสามารถมีการอัพเดท Signature ใหม่แบบ **อัตโนมัติได้** ๔.๘ อุปกรณ์ที่นำเสนอ ต้องสามารถส่ง Log ไปยัง SIEM ของธนาคารฯได้ ๔.๙ มีRedundant Power Supply ในตัวอุปกรณ์โดยสามารถใช้กับระบบไฟฟ้าในประเทศไทยแบบ ๒๒๐ VAC ๕๐Hz ได้ และแหล่งจ่ายไฟนี้จะต้องทำงานได้ในลักษณะ Hot-Swappable ได้ **๔.๑๐ อุปกรณ์ที่นำเสนอจะต้องไม่เป็นยี่ห้อเดียวกันกับอุปกรณ์ป้องกันการบุกรุก(Firewall)ในแบบที่๒ และ๓** ๔.๑๑ อุปกรณ์ที่นำเสนอต้องเป็นยี่ห้อเดียวกัน อุปกรณ์ป้องกันการบุกรุก(Firewall-Branch) ที่ติดตั้งสำนักงาน ใหญ่จำนวน ๒ชุด และเชื่อมต่อกับหน่วยงานต่างๆ หรือ สาขา จำนวน ๙๕ สาขา อย่างไม่มีปัญหา ๔.๑๒ เป็นผลิตภัณฑ์หรืออยู่ในกลุ่มผลิตภัณฑ์ยี่ห้อที่ได้รับอยู่ใน Leader Gartner Magic Quadrant for Network Firewall ปี ๒๐๒๒ เป็นอย่าง**น้อย**		
๕	**อุปกรณ์ป้องกันการบุกรุก แบบที่ ๒ จำนวน ๑ ชุด** (Internet)	**๕.๑ มี Layer ๔ Firewall Throughput ไม่น้อยกว่า ๑๔ Gbps** ๕.๒ มี Layer ๗ Firewall Throughput (NGFW) ไม่น้อยกว่า ๑๑ Gbps และ Threat prevention หรือ IPS Throughput ไม่น้อยกว่า ๕.๖ Gbps ในแบบ Appmixหรือ Enterprise testing condition หรือ Enterprise traffic mix และจำนวน Max Sessions หรือ Max Concurrentsได้ไม่น้อยกว่า ๑,๔๐๐,๐๐๐ sessions และ New Sessions หรือ New Connections ไม่น้อยกว่า ๑๔๕,๐๐๐ ต่อวินาที **๕.๓ มี Network Interface แบบ ๑G/๒.๕G/๕G/๑๐G (RJ๔๕) หรือดีกว่า ไม่ต่ำกว่า ๑๒ พอร์ต, ช่องเชื่อมต่อ แบบ ๑/๑๐G SFP+ ไม่ต่ำ**กว่า ๑๐ พอร์ต และช่องเชื่อมต่อแบบ ๒๕G SFP๒๘ ไม่ต่ำกว่า ๔ พอร์ต พร้อม เสนอ module SFP+ แบบ ๑๐GBASE-SR จำนวน ๔ modules ๕.๔ มี Interface แบบ ๑G ไม่ต่ำกว่า ๑ พอร์ต สำหรับ Management และ Interface แบบ ๑G หรือ ๑๐G ไม่ต่ำกว่า ๑ พอร์ต สำหรับ **การทำ High Availability (HA) โดย Interface ดังกล่าวแยกออกมาจาก Network Interface** ๕.๕ อุปกรณ์ต้องมี SSD สำหรับเก็บข้อมูลระบบไม่ต่ำกว่า ๔๘๐GB หรือเสนออุปกรณ์เก็บ log เพิ่มเติมที่มี ขนาด disk ขนาด ๔๘๐GB เพิ่มเติม ๕.๖ ระบบต้องสามารถทำการตรวจสอบเครื่องที่จะสามารถ Connect VPNเข้ามาในระบบเพื่อความ ปลอดภัยในการใช้งานทรัพยากร **ภายในองค์กร โดยสามารถตรวจสอบและกำหนดนโยบายควบคุม Connected VPNได้ดังต่อไปนี้** (๑) Operating system and patch level หรือเทียบเท่า (๒) Host anti-malware version หรือเทียบเท่า (๓) Customized host conditions (e.g., registry entries) หรือเทียบเท่า ๕.๗ สามารถใช้กับระบบเครือข่ายแบบ VLAN ผ่าน Protocol ๘๐๒.๑Q ได้ ๕.๘ สามารถทำ Dynamic Routing Protocol ได้แก่ OSPF และ BGP เป็นอย่างน้อย ๕.๙ สามารถทำ NAT (Network Address Translation) และ PAT (Port Address Translation) หรือ Port Translation ได้ **๕.๑๐ สามารถบริหารจัดการอุปกรณ์แบบ Web-based หรือ CLI (Command Line Interface) หรือ GUI (Graphic User Interface) ได้**		

ที่	รายการ	รายละเอียด (ประเภท จำนวน คุณลักษณะ(Spec) อื่นๆ)	ประมาณการงบประมาณ (Cost breakdown)	รวมงบประมาณ (บาท)
		๕.๑๑ รองรับการทำ High Availability (HA) แบบ Active/Passive หรือ Active/Active ได้ ๕.๑๒ มีระบบป้องกันภัยคุกคาม (Threat Prevention) หรือนำเสนออุปกรณ์เพิ่มเติม โดยเมื่อเปิดการใช้งาน Intrusion Prevention (IPS), Command-and-Control protection (Antispyware) และ Malware protection **๕.๑๓ สามารถป้องกันภัยคุกคามประเภท Virus หรือ Vulnerability หรือ Spyware(หรือ Anti-Bot) ได้ โดย สามารถมีการอัพเดท** Signature ใหม่แบบอัตโนมัติได้ ๕.๑๔ สามารถกำหนดนโยบายการเข้าถึง website (URL Filtering หรือ Web Filtering), สามารถติดตาม และควบคุมการเข้าถึงเว็บได้ตาม Category รวมทั้งสามารถปรับแต่ง Custom Category ได้ตาม ต้องการ **๕.๑๕ สามารถกำหนดนโยบาย Domain ที่มีความเสี่ยง เช่น Newly Seen Domains หรือ Newly registered domain ได้** ๕.๑๖ สามารถ Customize Block Page หรือ Redirect ไปยัง URLได้ตามความต้องการของธนาคารฯ ๕.๑๗ มีระบบป้องกัน DNS (DNS Security) ที่สามารถป้องกันระบบ DNS จากการโจมตีของ Command- and-Control และการจารกรรมข้อมูล (Data Theft) หรือสามารถนำเสนอระบบอื่นเพิ่มเติมเพื่อให้ ทำงานตามที่กำหนด ๕.๑๘ มีระบบเรียกดูสรุปข้อมูลรายงานของ Data ในรูปแบบของกราฟฟิคได้ โดยสามารถ ปรับแต่งรายงาน ตามความต้องการ (Custom Report) และส่งออก (Export) ให้อยู่ในรูปแบบ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้ และสามารถทำรายงานต่างๆได้เป็นอย่าง น้อยดังนี้ **(๑) Top Application หรือ Application Category หรือ เทียบเท่า** (๒) Threat Report หรือ MITRE ATT&CK report หรือ เทียบเท่า (๓) User activity report หรือ User Security Analysis หรือ เทียบเท่า หรือสามารถนำเสนอระบบอื่น เพิ่มเติมเพื่อให้ทำงานตามที่กำหนด ในกรณีที่เสนออุปกรณ์ภายนอกจะต้องเสนอระบบที่มียี่ห้อ เดียวกันกับ Firewall ที่นำเสนอ **๕.๑๙ อุปกรณ์ที่นำเสนอ ต้องสามารถส่ง Log ไปยัง SIEM ของธนาคารฯได้** ๕.๒๐ มีRedundant Power Supply ในตัวอุปกรณ์โดยสามารถใช้กับระบบไฟฟ้าในประเทศไทยแบบ ๒๒๐ VAC ๕๐Hz ได้ และแหล่งจ่ายไฟนี้จะต้องทำงานได้ในลักษณะ Hot-Swappable ได้ ๕.๒๑ อุปกรณ์ที่นำเสนอต้องเป็นยี่ห้อเดียวกันกับอุปกรณ์ป้องกันการบุกรุก (FirewallInternet) ที่ติดตั้ง สำนักงานใหญ่ และ เชื่อมต่อกับ **Cloud Provider หรือ Internet (ISP) ต่างๆ ได้อย่างไม่มีปัญหา** ๕.๒๒ เป็นผลิตภัณฑ์หรืออยู่ในกลุ่มผลิตภัณฑ์ยี่ห้อที่ได้รับอยู่ใน Leader Gartner Magic Quadrant for Network Firewall ปี ๒๐๒๒ เป็นอย่างน้อย		
๖	**อุปกรณ์ป้องกันการบุกรุก แบบที่ ๓ จำนวน ๑ ชุด** (Server Zone)	**๖.๑ มี Layer ๔ Firewall Throughput ไม่น้อยกว่า ๒๐Gbps** ๖.๒ มี Layer ๗ Firewall Throughput (NGFW) ไม่น้อยกว่า ๑๖ Gbps และ Threat prevention หรือ IPS Throughput ไม่น้อยกว่า ๘.๗ Gbps ในแบบ Appmixหรือ Enterprise testing condition หรือ Enterprise traffic mix และจำนวน Max Sessions หรือ Max Concurrentsได้ไม่น้อยกว่า ๒,๐๐๐,๐๐๐ sessions และ New Sessions หรือ New Connections ไม่น้อยกว่า ๒๐๕,๐๐๐ ต่อวินาที **๖.๓ มี Network Interface แบบ ๑G/๒.๕G/๕G/๑๐G (RJ๔๕) หรือดีกว่า ไม่ต่ำกว่า ๑๒ พอร์ต, ช่องเชื่อมต่อ แบบ ๑/๑๐G SFP+ ไม่ต่ำ** กว่า ๑๐ พอร์ต และช่องเชื่อมต่อแบบ ๒๕G SFP๒๘ ไม่ต่ำกว่า ๔ พอร์ต พร้อม เสนอ module SFP+ แบบ ๑๐GBASE-SR จำนวน ๑๐ modules ๖.๔ มี Interface แบบ ๑G ไม่ต่ำกว่า ๑ พอร์ต สำหรับ Management และ Interface แบบ ๑G หรือ ๑๐G ไม่ต่ำกว่า ๑ พอร์ต สำหรับการทำ High Availability (HA) โดย Interface ดังกล่าวแยกออกมาจาก Network Interface ๖.๕ อุปกรณ์ต้องมี SSD สำหรับเก็บข้อมูลระบบไม่ต่ำกว่า ๔๘๐GB หรือเสนออุปกรณ์เก็บ log เพิ่มเติมที่มี ขนาด disk ขนาด ๔๘๐GB เพิ่มเติม **๖.๖ สามารถใช้กับระบบเครือข่ายแบบ VLAN ผ่าน Protocol ๘๐๒.๑Q ได้** ๖.๗ สามารถทำ Dynamic Routing Protocol ได้แก่ OSPF และ BGP เป็นอย่างน้อย ๖.๘ สามารถบริหารจัดการอุปกรณ์แบบ Web-based หรือ CLI (Command Line Interface) หรือ GUI (Graphic User Interface) ได้ ๖.๙ สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication System) ได้แก่ Active Directory หรือ LDAP หรือ RADIUS เพื่อ **ทำการติดตามผู้ใช้ได้เป็นอย่างน้อย** ๖.๑๐ รองรับการทำ High Availability (HA) แบบ Active/Passive หรือ Active/Active ได้ ๖.๑๑ มีระบบป้องกันภัยคุกคาม (Threat Prevention) หรือนำเสนออุปกรณ์เพิ่มเติม โดยเมื่อเปิดการใช้งาน Intrusion Prevention (IPS), Command-and-Control protection (Antispyware) และ Malware protection **๖.๑๒ สามารถป้องกันภัยคุกคามประเภท Virus หรือ Vulnerability หรือ Spyware(หรือ Anti-Bot) ได้ โดย สามารถมีการอัพเดท** Signature ใหม่แบบอัตโนมัติได้		

ที่	รายการ	รายละเอียด (ประเภท จำนวน คุณลักษณะ(Spec) อื่นๆ)	ประมาณการงบประมาณ (Cost breakdown)	รวมงบประมาณ (บาท)
		๖.๑๓ มีระบบตรวจจับ Malware, exploit แบบ Cloud-Based เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero- day Malware) ซึ่งไม่มีในฐานข้อมูลการบุกรุกโจมตีได้ รวมถึงสามารถสร้างรูปแบบการโจมตี (Signature) ดังกล่าวขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ และมีรายงานแสดงพฤติกรรม การทำงานของ Malware ดังกล่าว **๖.๑๔ มีระบบเรียกดูสรุปข้อมูลรายงานของ Data ในรูปแบบของกราฟฟิคได้ โดยสามารถ ปรับแต่งรายงาน ตามความต้องการ (Custom** Report) และส่งออก (Export) ให้อยู่ในรูปแบบ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลา ส่งรายงานผ่านทาง Email แบบอัตโนมัติได้ และสามารถทำรายงานต่างๆได้เป็นอย่าง น้อยดังนี้ **(๑) Top Application หรือ Application Category หรือ เทียบเท่า** (๒) Threat Report หรือ MITRE ATT&CK report หรือ เทียบเท่า (๓) User activity report หรือ User Security Analysis หรือ เทียบเท่า หรือสามารถนำเสนอระบบอื่น เพิ่มเติมเพื่อให้ทำงานตามที่กำหนด ในกรณีที่เสนออุปกรณ์ภายนอกจะต้องเสนอระบบที่มียี่ห้อ เดียวกันกับ Firewall ที่นำเสนอ **๖.๑๕ อุปกรณ์ที่นำเสนอ ต้องสามารถส่ง Log ไปยัง SIEM ของธนาคารฯได้** ๖.๑๖ มีRedundant Power Supply ในตัวอุปกรณ์โดยสามารถใช้กับระบบไฟฟ้าในประเทศไทยแบบ ๒๒๐ VAC ๕๐Hz ได้ และแหล่งจ่ายไฟนี้จะต้องทำงานได้ในลักษณะ Hot-Swappable ได้ ๖.๑๗ อุปกรณ์ที่เสนอจะต้องไม่เป็นยี่ห้อเดียวกันกับอุปกรณ์ป้องกันการบุกรุก (Firewall) ในแบบที่ ๑ **๖.๑๘ อุปกรณ์ที่นำเสนอต้องเป็นยี่ห้อเดียวกัน อุปกรณ์ป้องกันการบุกรุก (Firewall-Server) ที่ติดตั้งสำนักงาน ใหญ่ และ เชื่อมต่อกับ** Private Link และ Core Bank ได้ อย่างไม่มีปัญหา ๖.๑๙ เป็นผลิตภัณฑ์หรืออยู่ในกลุ่มผลิตภัณฑ์ยี่ห้อที่ได้รับอยู่ใน Leader Gartner Magic Quadrant for Network Firewall ปี ๒๐๒๒ เป็นอย่างน้อย		
๗	ระบบควบคุมการเข้าใช้งานเครือข่ายสื่อสาร	๗.๑ เป็น Software Virtual Appliances ที่สามารถติดตั้งบน Hypervisor VMware ESX/ESXi ๕.x ขึ้นไป ได้เป็นอย่างน้อย **๗.๒ รองรับการทำ Authentication, Authorization และ Accounting ตามมาตรฐานโพรโตคอล RADIUS ได้เป็นอย่างน้อย** ๗.๓ รองรับการตรวจสอบตัวตนด้วย Protocol PAP, MS-CHAP v๒, EAP-TLS, PEAP และ EAP-FAST ได้ เป็นอย่างน้อย ๗.๔ มีระบบที่สามารถบริหารจัดการผู้ใช้งานผ่าน Web Browser ได้ ๗.๕ มีคุณสมบัติที่ทำหน้าที่บริหารจัดการสิทธิ์แบบพิเศษ (Privilege User) ในการเข้าถึงอุปกรณ์เครือข่าย สื่อสาร ได้แก่ Router, Switch **เพื่อตรวจสอบรายชื่อ รหัสผ่าน สิทธิการใช้งาน และบันทึกการทำงาน ของผู้ดูแลระบบ TACACS+ ได้** ๗.๖ ผลิตภัณฑ์ที่นำเสนอจะต้องมีประสิทธิภาพในการทำงานเป็นอย่างดี โดยได้รับการจัดลำดับอยู่ใน Leaders Quadrant ของ Gartner Magic Quadrant ในเรื่องของ Wired and Wireless LAN Access Infrastructure ปี ๒๐๒๒ หรือใหม่กว่า ๗.๗ ระบบควบคุมการเข้าใช้งานเครือข่ายสื่อสารที่เสนอ ต้องสามารถทำงานร่วมกับอุปกรณ์ Cisco Identity Services Engine เดิมที่ **ติดตั้งที่ศูนย์คอมพิวเตอร์หลัก ของธนาคารฯที่ใช้งานในปัจจุบัน ในกรณีระบบที่ นำเสนอ ไม่สามารถทำร่วมกับระบบเดิมของธนาคารฯได้** ให้เสนอระบบบันทึกการทำงานของผู้ดูแล ระบบ TACACS+ เพิ่มได้		
๘	**อุปกรณ์สำหรับการเก็บบันทึกข้อมูลเหตุการณ์ของ** ระบบเครือข่าย (Log appliance) จำนวน ๑ ชุด	๘.๑ เป็นอุปกรณ์ Appliance หรือ อุปกรณ์คอมพิวเตอร์ที่ได้มาตรฐาน สามารถเก็บรวบรวมเหตุการณ์ (logs or Events) ที่เกิดขึ้นในอุปกรณ์ที่เป็น appliances และ non-appliances เช่น Firewall, Network Devices ต่างๆ ระบบปฏิบัติการ ระบบ appliances ระบบเครือข่าย และระบบฐานข้อมูล ๘.๒ ต้องสามารถจัดเก็บข้อมูลได้ตามหลักเกณฑ์ การจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ **๘.๓ เป็นระบบจัดเก็บข้อมูล Log ที่ได้ผ่านการตรวจสอบคุณสมบัติตามมาตรฐาน "ระบบเก็บรักษาข้อมูล จราจรทางคอมพิวเตอร์" ได้ตามมาตรฐาน** Standard NTS ๔๐๐๓.๑-๒๕๖๐ โดยต้องมีเอกสารรายงานผล การทดสอบ ๘.๔ เป็นอุปกรณ์ที่ได้รับการทดสอบและผ่านการรับรองมาตรฐานสินค้าภายใต้เครื่องหมายรับผลิตภัณฑ์ FCC หรือ CE หรือ RoHS หรือเทียบเท่า ๘.๕ มีความสามารถบริหารจัดการแบบ Web Base Administration ผ่าน HTTPS หรือ Command Line Interface (CLI) ผ่าน SSH เพื่อ **สามารถเข้าไปบริหารจัดการ ระบบ log ผ่านเครือข่ายได้** ๘.๖ ต้องรองรับการจัดเก็บ Log แบบ Syslog ที่เกิดขึ้นจากอุปกรณ์เครือข่ายได้ และ Non-Syslogที่เกิดจาก ระบบปฏิบัติการ ๘.๗ ระบบต้องสามารถทำการตั้งเวลา Backup Archive Log Data แยกออกไปยังอุปกรณ์ NAS Server ผ่าน NFS Protocol ได้ ๘.๘ ระบบมีส่วนของการรายงานผลกราฟและตารางข้อมูล โดยมีข้อมูลดังต่อไปนี้เป็นอย่างน้อย Total Events, Total Bandwidth, Total Log **Usage, Top ๑๐ Total Event, Top ๑๐ EPS, Top ๑๐ Total Log Usage** ๘.๙ ระบบมีส่วนของสรุปข้อมูลรายงาน รายการ Host หรือ อุปกรณ์ที่ส่ง Log เข้ามาจัดเก็บ โดยระบุข้อมูล ได้อย่างน้อย ดังนี้ ชื่อ Host, ระยะเวลาจัดเก็บมาแล้วทั้งสิ้น, ปริมาณเหตุการณ์, ปริมาณข้อมูล Log โดย สามารถส่งออกข้อมูลได้ทั้งแบบ Copy, CSV, JSON, PDF ๘.๑๐ ระบบที่นำเสนอรองรับการจัดเก็บ Log ตาม พ.ร.บ.คอมพิวเตอร์ ๒๕๖๐ ได้ไม่น้อยกว่า ๙๐ วัน และ รองรับการจัดเก็บ Log ๒ปีในกรณีจำเป็นที่ **เจ้าหน้าที่ต้องการสั่งให้เก็บ Log โดยระบุวันและเวลาที่ เจ้าหน้าที่ต้องการได้ ทั้งนี้ ระบบต้องรองรับการเข้ารหัสด้วย AES-๒๕๖ ในกรณีที่มีการดาวน์** โหลดไฟล์ ออกจากระบบเพื่อป้องกันการแก้ไขข้อมูล Log ได้ ๘.๑๑ ระบบมี Software ภายใต้เครื่องหมายการค้าเดียวกันที่เป็น Native Mobile Application ที่สามารถ ดาวน์โหลดได้จาก Google PlayStore เพื่อใช้สำหรับการแจ้งเตือนการทำงานของระบบได้		

ที่	รายการ	รายละเอียด (ประเภท จำนวน คุณลักษณะ(Spec) อื่นๆ)	ประมาณการงบประมาณ (Cost breakdown)	รวมงบประมาณ (บาท)
		๘.๑๒ รองรับการ Authentication ร่วมกับ AD หรือ LDAP และรองรับการ Authentication แบบ Two Factor Authentication ๘.๑๓ ระบบต้องมีเทคโนโลยีการค้นหาข้อมูล (Search) ได้จากทุกเนื้อความในข้อมูล Log ที่ส่งเข้ามาได้ทั้งแบบ Keyword, Field, Boolean Expression, Regular Expression ได้ **๘.๑๔ สามารถการวิเคราะห์ข้อมูลจากระบบ Web Application Firewall หรือ Next Generation Firewall** (NGFW) และ Authentication Log จาก Operating System ได้เป็นอย่างน้อย ๘.๑๕ ระบบสามารถวิเคราะห์และรายงานประเภทเหตุการณ์ข้อมูลส่วนบุคคลจาก Log PDPA **ของระบบจัดเก็บข้อมูลหลัก Centralized Raw Log ที่เกิดจากระบบ Database หรือ File Server** หรือ Storage Server หรือ อื่นๆที่ทำหน้าที่จัดเก็บข้อมูลส่วนบุคคล ๘.๑๖ เป็นเครื่องระดับ Server มีหน่วยประมวลผลกลาง (CPU) แบบ Quad Core หรือดีกว่า ๘.๑๗ มีหน่วยความจำ (RAM) ไม่น้อยกว่า ๓๒ GB **๘.๑๘ มีพอร์ต Gigabit Ethernet แบบ ๑๐๐๐ Base-T อย่างน้อย ๒ พอร์ต** ๘.๑๙ มีแหล่งจ่ายไฟ (Power Supply) แบบ Redundant Power สามารถถอดเปลี่ยนได้แบบ Hot Plug ไม่ต้องทำการหยุดระบบ		
๙	อุปกรณ์สลับสัญญาณ (Core Switch) สำหรับศูนย์คอมพิวเตอร์สำรอง จำนวน ๒ ชุด	๙.๑ เป็น Layer ๓ Switch ที่มีขนาด bandwidth ไม่น้อยกว่า ๒.๑๖Tbps. **๙.๒ อุปกรณ์ทำงานแบบ Low Latency โดยมี Latency ไม่เกิน ๒.๕ microsecond** ๙.๓ มีพอร์ต ๑/๒.๕/๕/๑๐G BASE-T จำนวนไม่น้อยกว่า ๔๘ พอร์ต พร้อมเสนอ Transceiver Modules แบบ ๑๐ Gbps. ชนิด ๑๐GBase-SR หรือเทียบเท่า จำนวนไม่น้อยกว่า ๔ โมดูล **๙.๔ มีพอร์ต ๔๐/๑๐๐ Gigabit Ethernet จำนวนไม่น้อยกว่า ๖ พอร์ต** ๙.๕ รองรับการทำงาน แบบ protocol มาตรฐานเช่น VXLAN ได้เป็นอย่างน้อย ๙.๖ สามารถทำการเชื่อมต่อกับ Network ภายนอกด้วย Routing Protocol แบบBGP, OSPF, PBR, และVRF ๙.๗ สามารถทำงานตามมาตรฐาน SSH, NTP, SNMPv๓ ได้ **๙.๘ รองรับกาทำ remote leafหรือ leaf switch ได้** ๙.๙ รองรับการทำงานร่วมกับระบบบริหารและจัดการ Network Infrastructure แบบ Software-Defined Network (SDN) ได้ ๙.๑๐ มีพัดลมระบายความร้อนสามารถถอดเปลี่ยนได้ ๙.๑๑ อุปกรณ์ที่นำเสนอ ต้องมี Rack Mount สามารถติดตั้งบน Rack ๑๙" ได้ **๙.๑๒ ผ่านการรับรองตามมาตรฐานความปลอดภัย UL หรือ EN หรือ IEC หรือ เทียบเท่า ได้** ๙.๑๓ มีRedundant Power Supply ในตัวอุปกรณ์โดยสามารถใช้กับระบบไฟฟ้าในประเทศไทยแบบ ๒๒๐ VAC ๕๐Hz ได้ และแหล่งจ่ายไฟนี้จะต้องทำงานได้ในลักษณะ Hot-Swappable ได้ ๙.๑๔ อุปกรณ์ที่นำเสนอ ต้องสามารถทำงานร่วมกันได้กับ ระบบบริหารและจัดการเครือข่าย Network Access Control ที่ทางธนาคารฯใช้อยู่ ยี่ห้อ Cisco Identity Service Engine (ISE) ผ่าน Protocol TACACS+ ได้ ๙.๑๕ อุปกรณ์ที่นำเสนอ ต้องสามารถส่ง Log ไปยัง SIEM ของธนาคารฯได้ ๙.๑๖ อุปกรณ์ที่นำเสนอ ต้องเชื่อมต่อและรับส่งข้อมูลกับอุปกรณ์ Network หรืออุปกรณ์ Server ต่างๆ ของธนาคารฯได้อย่างไม่มีปัญหา ๙.๑๗ อุปกรณ์ที่นำเสนอ ต้องเป็นรุ่นที่ยังอยู่ในสายการผลิตในปัจจุบัน โดยต้องได้รับการแต่งตั้งจากเจ้าของ ผลิตภัณฑ์		
๑๐	อุปกรณ์สลับสัญญาณ (Out-of-band management) สำหรับศูนย์คอมพิวเตอร์สำรอง จำนวน ๑ ชุด	๑๐.๑ มี Switching Bandwidth หรือรองรับ Switch capacity with Stacking ขนาดไม่น้อยกว่า ๒๕๖ Gbps. **๑๐.๒ มีประสิทธิภาพในการส่งผ่านข้อมูล Forwarding Rate ไม่น้อยกว่า ๑๒๕ Mpps.** ๑๐.๓ มีพอร์ต Gigabit Ethernet แบบ ๑๐/๑๐๐/๑๐๐๐ จำนวนไม่น้อยกว่า ๔๘ พอร์ต ๑๐.๔ มีพอร์ต Gigabit Ethernet แบบ SFP+ จำนวนไม่น้อยกว่า ๔ พอร์ต พร้อมเสนอ Transceiver Modules แบบ ๑๐ Gbps. ชนิด ๑๐GBase-SR หรือเทียบเท่า จำนวนไม่น้อยกว่า ๔ โมดูล **๑๐.๕ รองรับการทำStacking ได้ไม่น้อยกว่า ๘ อุปกรณ์ และ มีStacking Throughput ไม่น้อยกว่า ๘๐ Gbps.** ๑๐.๖ สามารถทำ ตามมาตรฐาน IEEE๘๐๒.๑p และ IEEE๘๐๒.๑q ๑๐.๗ สามารถทำงาน ทั้ง IP Version ๔ และ IP Version ๖ ๑๐.๘ สามารถทำ Spanning tree ตามมาตรฐาน IEEE๘๐๒.๑D, IEEE๘๐๒.๑w และ IEEE๘๐๒.๑s **๑๐.๙ สามารถทำ Port Aggregation ตามมาตรฐาน IEEE๘๐๒.๓ad ได้** ๑๐.๑๐ รองรับการทำVLANได้ไม่น้อยกว่า ๒๕๐ active VLANหรือ Switched Virtual Interfaces (SVIs) ๑๐.๑๑ รองรับ MAC address ได้ไม่น้อยกว่า ๑๕,๐๐๐ MAC address ๑๐.๑๒ มี Console Port เพื่อกำหนดค่าการทำงานของอุปกรณ์ และสำหรับตรวจสอบระบบได้ **๑๐.๑๓ สามารถทำงานตามมาตรฐาน SSH, NTP, SNMPv๓ ได้** ๑๐.๑๔ อุปกรณ์ที่นำเสนอ ต้องมี Rack Mount สามารถติดตั้งบน Rack ๑๙" ได้ ๑๐.๑๕ ผ่านการรับรองตามมาตรฐานความปลอดภัย UL หรือ EN หรือ IEC หรือ เทียบเท่า ได้ **๑๐.๑๖ มีRedundant Power Supply ในตัวอุปกรณ์โดยสามารถใช้กับระบบไฟฟ้าในประเทศไทยแบบ ๒๒๐ VAC ๕๐Hz ได้ และ** แหล่งจ่ายไฟนี้จะต้องทำงานได้ในลักษณะ Hot-Swappable ได้ ๑๐.๑๗ อุปกรณ์ที่นำเสนอ ต้องสามารถทำงานร่วมกันได้กับ ระบบบริหารและจัดการเครือข่าย Network Access Control ที่ทางธนาคารฯใช้อยู่ ยี่ห้อ Cisco Identity Service Engine (ISE) ผ่าน Protocol TACACS+ ได้ ๑๐.๑๘ อุปกรณ์ที่นำเสนอ ต้องสามารถส่ง Log ไปยัง SIEM ของธนาคารฯได้ ๑๐.๑๙ อุปกรณ์ที่นำเสนอ ต้องเชื่อมต่อและรับส่งข้อมูลกับอุปกรณ์Network หรือ อุปกรณ์Server ต่างๆ ของธนาคารฯได้อย่างไม่มีปัญหา		

ที่	รายการ	รายละเอียด (ประเภท จำนวน คุณลักษณะ(Spec) อื่นๆ)	ประมาณการงบประมาณ (Cost breakdown)	รวมงบประมาณ (บาท)
๑๑	อุปกรณ์บริหารจัดการ Firewall (Services Zone) จำนวน ๑ ชุด	๑๑.๑ เป็นอุปกรณ์แบบ Virtual Appliance ทำหน้าที่บริหารจัดการแบบรวมศูนย์ (centralized management) ที่สามารถติดตั้งลงบน VMware ของธนาคารได้ และทำงานร่วมกับอุปกรณ์ป้องกันการ บุกรุก Firewall (Services Zone) ยี่ห้อ Check Point รุ่น CPAP-SG๖๒๐๐ ที่ติดตั้งไว้ ศูนย์คอมพิวเตอร์ สำรองได้ **๑๑.๒ สามารถส่ง Log ที่ได้ไปยังอุปกรณ์ภายนอกในรูปแบบของ UDP หรือ TCP หรือ SSL** ๑๑.๓ สามารถทำการ correlate ข้อมูลเพื่อตรวจจับหาเครื่องที่ถูก compromise ได้ หรือ สามารถทำ Event Correlation และทำการวิเคราะห์ข้อมูลเหตุการณ์ที่เกิดขึ้นได้ **๑๑.๔ สามารถกำหนดสิทธิที่ต่างกันให้กับผู้ดูแลระบบแต่ละคนได้** (Role-based Administration) ๑๑.๕ สามารถทำการ อัพเดท software, license และ contents ของ firewall ที่ควบคุมอยู่ได้ ๑๑.๖ สามารถแสดงหน้า Dashboardจากการประมวลผลจาก ข้อมูล ที่มาจาก firewall ได้ ๑๑.๗ สามารถสร้างรายงาน (Report) โดยสามารถทำการปรับแต่งรายงาน (Custom Report) และส่งออก (Export) ให้อยู่ในรูปแบบ PDF หรือ CSV ได้ ๑๑.๘ สามารถส่ง Log ไปยัง SIEM ของธนาคารฯได้		
๑๒	**อุปกรณ์บริหารจัดการ Intrusion Prevention** System(IPS) จำนวน ๑ ชุด	๑๒.๑ เป็นอุปกรณ์แบบ Virtual Appliance สามารถทำงานบน VMware ได้ และ ทำหน้าที่บริหารจัดการ แบบรวมศูนย์ (centralized management) ยี่ห้อเดียวกับอุปกรณ์ IPS ข้อ ๑๓. ๑๒.๒ มี Licensed บริหารจัดการอุปกรณ์ IPS จากศูนย์กลาง (Centralized Management) ได้ไม่น้อยกว่า๒อุปกรณ์ (Licensed) ๑๒.๓ สามารถทำการ correlate ข้อมูลเพื่อตรวจจับหาเครื่องที่ถูก compromise ได้ **๑๒.๔ สามารถกำหนดสิทธิที่ต่างกันให้กับผู้ดูแลระบบแต่ละคนได้** (Role-based Administration) ๑๒.๕ สามารถทำการอัพเดท software, license และ contents ของ IPS ที่ควบคุมอยู่ได้ ๑๒.๖ สามารถบริหารจัดการและปรับเปลี่ยนค่าต่าง ๆ จากส่วนกลาง เช่น Policies, Object และ Security Profile แล้วทำการส่งผ่านการตั้งค่าไปยังอุปกรณ์รักษาความปลอดภัยได้ **๑๒.๗ สามารถแสดงหน้า Dashboard จากการประมวลผลจาก log ที่มาจาก firewall ในรูปแบบ graphical เช่น data files, threats** และสามารถ customize เองได้ ๑๒.๘ มีระบบเรียกดูสรุปข้อมูลรายงานของ Data ในรูปแบบของกราฟฟิคได้ โดยสามารถ ปรับแต่งรายงาน ตามความต้องการ (Custom Report) และส่งออก (Export) ให้อยู่ในรูปแบบ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลา ส่งรายงานผ่านทาง Email แบบอัตโนมัติได้ และ**สามารถทำรายงานต่างๆได้** ๑๒.๙ สามารถส่ง Log ไปยัง SIEM ของธนาคารฯได้		
๑๓	**อุปกรณ์ตรวจจับการบุกรุก Intrusion Prevention** System (IPS) จำนวน ๑ชุด	**๑๓.๑ เป็นอุปกรณ์แบบ Hardware Appliance ที่ออกแบบมาเพื่อทำหน้าที่ IPS โดยเฉพาะ** ๑๓.๒ มีIPS Throughput หรือIPS Inspection Throughput หรือPerformance สูงสุดไม่น้อยกว่า ๑๐ Gbps ๑๓.๓ มี Network Interface แบบ RJ๔๕ จำนวนไม่น้อยกว่า ๘ พอร์ต ๑๓.๔ มี Network Interface แบบ SFP+ (๑/๑๐G) จำนวนไม่น้อยกว่า ๘ พอร์ต พร้อมเสนอ Transceiver ชนิด SFP-๑๐G-SR จำนวนไม่น้อยกว่า ๘ Transceiver ๑๓.๕ มี Hardware bypass แบบ ๑๐G SR multimode จำนวนไม่น้อยกว่า ๖ พอร์ต ๑๓.๗ สามารถทำ Decryption ทั้งแบบ Inbound Traffic เพื่อตรวจสอบการโจมตีบนเครื่องแม่ข่าย และ Outbound Traffic เพื่อตรวจสอบการเชื่อมต่อจากเครื่องลูกข่ายไปเครือข่ายภายนอกที่ไม่ปลอดภัย **๑๓.๘ มี Storage ขนาดไม่น้อยกว่า ๙๐๐ GB หรือ ในกรณีที่ Storage ภายใน IPS ไม่รับรองความจุขนาดไม่ น้อยกว่า ๙๐๐GB สามารถเสนอ** Storage เพิ่ม ที่รองรับการส่งข้อมูลจาก IPS ผ่าน Protocol FTP หรือ SFTP หรือดีกว่าได้ ๑๓.๙ สามารถกำหนดนโยบายการตรวจจับการโจมตีตามกลุ่ม IP address, Port, Application, User รวมถึง ประเทศต้นทาง (geolocation) ได้ ๑๓.๑๐ สามารถทำงานในรูปแบบของ Application Control และรองรับการควบคุม Application รูปแบบต่างๆ ไม่น้อยกว่า ๔,๐๐๐ applications **๑๓.๑๑ สามารถรับข้อมูลต้องสงสัย (security intelligence) ทั้งในรูปแบบ IP address, URL และ DNS จาก เจ้าของผลิตภัณฑ์ เพื่อนำมาใช้ป้อง** การเชื่อมต่อไปต้องสงสัย หรือไม่ปลอดภัยได้ ๑๓.๑๕ สามารถตรวจวิเคราะห์ Advance Malware หรือ Zero-Day Malware โดยใช้เทคนิค Dynamic Analysis แบบ File analysis (File Reputation) และ Sandboxing ได้ **๑๓.๑๖ สามารถทำงานตามมาตรฐาน SSH, NTP, SNMPv๓ ได้** ๑๓.๑๗ อุปกรณ์ที่นำเสนอ ต้องมี Rack Mount สามารถติดตั้งบน Rack ๑๙" ได้ ๑๓.๑๘ ผ่านการรับรองตามมาตรฐานความปลอดภัย UL หรือ EN หรือ IEC หรือ เทียบเท่า ได้ ๑๓.๑๙ มีRedundant Power Supplyในตัวอุปกรณ์โดยสามารถใช้กับระบบไฟฟ้าในประเทศไทยแบบ ๒๒๐ VAC ๕๐Hz ได้ และแหล่งจ่ายไฟนี้**จะต้องทำงานได้ในลักษณะ Hot-Swappable ได้**		