แบบ บก.04

ตารางแสดงวงเงินงบประมาณที่ได้รับจัดสรรและรายละเอียดค่าใช้จ่ายการจ้างที่ปรึกษา

1. ชื่อโครงการ จ้างที่ปรึกษาตรวจสอบระบบเทคโนโลยีสารสนเทศ ปี 2568
2. หน่วยงานเจ้าของโครงการ ฝ่ายตรวจสอบภายใน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
3. วงเงินงบประมาณที่ได้รับจัดสรร 2,500,000.00 บาท
4. วันที่กำหนดราคากลาง (ราคาอ้างอิง) 8 พฤศจิกายน พ.ศ. 2567

   เป็นเงิน 2,499,425.25 บาท
5. ค่าตอบแทนบุคลากร 2,499,425.25 บาท

   5.1 ประเภทที่ปรึกษา กลุ่มวิชาชีพเทคโนโลยีสารสนเทศและการสื่อสาร (ICT)

   5.2 คุณสมบัติที่ปรึกษา 1. ปริญญาโท ประสบการณ์ไม่น้อยกว่า 11 ปี จำนวน 3 คน

   2. ปริญญาตรี ประสบการณ์ไม่น้อยกว่า 5 ปี จำนวน 2 คน

   3. ปริญญาตรี ประสบการณ์ไม่น้อยกว่า 2 ปี จำนวน 1 คน

   5.3 จำนวนที่ปรึกษา 6 คน
6. ค่าวัสดุอุปกรณ์ ..... บาท
7. ค่าใช้จ่ายในการเดินทางไปต่างประเทศ (ถ้ามี) .....บาท
8. ค่าใช้จ่ายอื่น ๆ 0.00 บาท
9. รายชื่อผู้รับผิดชอบในการกำหนดค่าใช้จ่าย/ดำเนินการ/ขอบเขตดำเนินการ (TOR)

   9.1 นางสาวประวิตรี ศรีวิเชียร

   9.2 นางสาวสมฤทัย รอสูงเนิน

   9.3 นางสาวพิมพ์ชนก เกสพานิช

   9.4 นางสาวจรินทร์ วงศ์สุวรรณวารี

   9.5 นางสาวสุฉายพิมพ์ ศิริวัฒน์
10. ที่มาของการกำหนดราคากลาง (ราคาอ้างอิง) หลักเกณฑ์ราคากลางการจ้างที่ปรึกษา

    สำนักงานบริหารหนี้สาธารณะ

    สำนักบริหารการระดมทุนโครงการลงทุนภาครัฐ

คุณวุฒิ	กลุ่มวิชาชีพ	ประสบการณ์ (ปี)	จำนวน (คน)	อัตราเงินเดือนพื้นฐาน (บาท)	ระยะเวลาจ้าง (วัน)	รวมอัตราค่าบุคลากร (บาท)
ป. โท	ICT	11	1	76,980	60	381,051.00
ป. โท	ICT	11	2	76,980	105	1,333,678.50
ป. ตรี	ICT	5	2	41,310	105	715,695.75
ป. ตรี		2	1	18,000	115	69,000.00
					ค่าใช้จ่ายอื่น ๆ	0.00
					รวมทั้งสิ้น	**2,499,425.25**

ค่าใช้จ่ายงาน : โครงการจ้างที่ปรึกษาตรวจสอบระบบเทคโนโลยีสารสนเทศ ปี 2568									
ที่	รายการ	ค่าใช้จ่ายต่อรายการ (บาท)	จน.คน	จน.ชม	จน.วัน	จน. ครั้ง/ชิ้นงาน	จำนวนเดือน	ตัวคูณ	จำนวนเงิน
1	**ค่าที่ปรึกษา**								
1.1	**หัวหน้าโครงการด้าน ICT** วุฒิการศึกษาระดับปริญญาโท มีประสบการณ์เกี่ยวกับตรวจสอบระบบเทคโนโลยีสารสนเทศให้กับองค์กรภาครัฐ รัฐวิสาหกิจ หรือภาคเอกชน หรือวิเคราะห์สำรวจ หรือด้านที่เกี่ยวข้อง ไม่น้อยกว่า 11 ปี จำนวน 1 คน	76,980.00	1		60			2.475	381,051.00
1.2	**ผู้เชี่ยวชาญด้าน ICT** วุฒิการศึกษาระดับปริญญาโท มีประสบการณ์เกี่ยวกับตรวจสอบระบบเทคโนโลยีสารสนเทศให้กับองค์กรภาครัฐ รัฐวิสาหกิจ หรือภาคเอกชน หรือวิเคราะห์สำรวจ หรือด้านที่เกี่ยวข้อง ไม่น้อยกว่า 11 ปี จำนวน 2 คน	76,980.00	2		105			2.475	1,333,678.50
1.3	**ผู้เชี่ยวชาญด้าน ICT** วุฒิการศึกษาระดับปริญญาตรี มีประสบการณ์ด้านประสบการณ์ทำงานหรือผลงาน ด้านการพัฒนาหลักสูตร การเรียนรู้ เศรษฐศาสตร์ สังคมศาสตร์ บริหารธุรกิจ เทคโนโลยีดิจิทัล การวิจัย วิเคราะห์สำรวจ หรือด้านที่เกี่ยวข้อง ไม่น้อยกว่า 5 ปี จำนวน 2 คน	41,310.00	2		105			2.475	715,695.75
1.4	**เจ้าหน้าที่ประสานงาน** วุฒิการศึกษาไม่ต่ำกว่าระดับปริญญาตรี และมีประสบการณ์การทำงาน การบริหารจัดการงบประมาณ การดำเนินงานด้านเอกสาร หรือการประสานงานติดต่อหน่วยงานและบุคลากรที่เกี่ยวข้องในการตรวจสอบระบบเทคโนโลยีสารสนเทศ หรือด้านที่เกี่ยวข้อง ไม่น้อยกว่า 2 ปี จำนวน 1 คน	18,000.00	1		115				69,000.00
2	ค่าใช้จ่ายดำเนินงาน 10%								-
3	ค่าใช้จ่ายอื่นๆ								-
สรุปรายการ									
1. ค่าที่ปรึกษา (ข้อ 1.1-1.4)									2,499,425.25
2. ค่าใช้จ่ายอื่น ๆ (ข้อ 2, 3)									-
รวม									**2,499,425.25**

สำเนาเอกสารเผยแพร่ผ่านเว็บไซต์

ETDA	ขอบเขตของงาน (Terms of Reference : TOR)		จำนวน	11 หน้า
	เรื่อง	โครงการจ้างที่ปรึกษาตรวจสอบระบบเทคโนโลยีสารสนเทศ ปี 2568		
	จัดทำโดย	ฝ่ายตรวจสอบภายใน	วันที่จัดทำ	17 ก.ย. 67

1. ความเป็นมา

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ สพธอ. เป็นองค์กรที่ออกแบบมาให้ส่งเสริมและขับเคลื่อนเศรษฐกิจและสังคมไทย ไปสู่เศรษฐกิจและสังคมดิจิทัล ที่ทุกภาคส่วนสามารถทำธุรกรรมที่น่าเชื่อถือ ผ่านทางออนไลน์ ได้อย่างมั่นใจและมั่นคงปลอดภัย เพื่อให้การดำเนินการขององค์กรบรรลุตามวัตถุประสงค์และมีประสิทธิภาพ และเพื่อให้เกิดความมั่นใจและความมั่นคงปลอดภัย จึงต้องมีการตรวจสอบระบบเทคโนโลยีสารสนเทศที่เป็นไปตามมาตรฐานสากล สพธอ. จึงมีความประสงค์ที่จะจัดหาที่ปรึกษาที่มีความรู้ ความชำนาญ และมีประสบการณ์ในการตรวจสอบระบบเทคโนโลยีสารสนเทศมาศึกษาวิเคราะห์ ตรวจสอบ ประเมินความเสี่ยง และกำกับดูแลการปฏิบัติงานระบบเทคโนโลยีสารสนเทศของ สพธอ. โดยการตรวจสอบภายในและการทดสอบช่องโหว่ของระบบเทคโนโลยีสารสนเทศ พร้อมทั้งให้ข้อเสนอแนะในการปรับปรุงแก้ไข และเป็นแนวทางในการสร้างกรอบการดำเนินงานของ สพธอ. ในการควบคุมกำกับดูแลความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้เป็นมาตรฐานสากลที่มีความเหมาะสมเพียงพอกับการประกอบดำเนินงานของ สพธอ.

2. วัตถุประสงค์

เพื่อดำเนินการตรวจสอบเทคโนโลยีสารสนเทศของ สพธอ. ให้เป็นไปตามมาตรฐานสากล โดยจะต้อง ครอบคลุมวัตถุประสงค์ ดังนี้

2.1 เพื่อให้มีแนวทาง/ข้อมูลที่เป็นประโยชน์ ที่จะนำไปใช้ในการพัฒนาระบบการตรวจสอบด้านเทคโนโลยีสารสนเทศในอนาคต

2.2 เพื่อให้ข้อสังเกต ข้อเสนอแนะและให้คำปรึกษาแก่ผู้บริหาร โดยใช้ผลที่ได้จากการตรวจสอบ ระบบเทคโนโลยีสารสนเทศของ สพธอ.

2.3 เพื่อพัฒนาศักยภาพบุคลากร ความรู้ ทักษะ เทคนิควิธีการตรวจสอบเทคโนโลยีสารสนเทศ จากการมีส่วนร่วมในการปฏิบัติงานตรวจสอบและการรายงานผลการตรวจสอบในทุกขั้นตอน

3. คุณสมบัติของที่ปรึกษา

3.1 มีความสามารถตามกฎหมาย

3.2 ไม่เป็นบุคคลล้มละลาย

3.3 ไม่อยู่ระหว่างเลิกกิจการ

3.4 ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราวตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง

เอกสารเผยแพร่ภายนอก

3.5 ไม่เป็นบุคคลซึ่งถูกระบุชื่อไว้ในบัญชีรายชื่อผู้ทิ้งงานและได้แจ้งเวียนชื่อให้เป็นผู้ทิ้งงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทิ้งงานเป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย

3.6 มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา

3.7 เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพรับจ้างงานดังกล่าว

3.8 ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับที่ปรึกษารายอื่นที่เข้ายื่นข้อเสนอให้แก่ สพธอ. ณ วันที่ได้รับประกาศเชิญชวนหรือหนังสือเชิญชวนให้เข้ามายื่นข้อเสนอจากหน่วยงานของรัฐ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวางการแข่งขันอย่างเป็นธรรมในการยื่นข้อเสนอในครั้งนี้

3.9 ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาลของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นว่านั้น

3.10 ผู้ยื่นข้อเสนอที่ยื่นข้อเสนอในรูปแบบของ “กิจการร่วมค้า” ต้องมีคุณสมบัติ ดังนี้

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลัก ข้อตกลงฯ จะต้องมีการกำหนดสัดส่วนหน้าที่ และความรับผิดชอบในปริมาณงาน สิ่งของ หรือมูลค่าตามสัญญาของผู้เข้าร่วมค้าหลักมากกว่าผู้เข้าร่วมค้ารายอื่นทุกราย

กรณีที่ข้อตกลงฯ กำหนดให้ผู้เข้าร่วมค้ารายใดรายหนึ่งเป็นผู้เข้าร่วมค้าหลักกิจการร่วมค้านั้นต้องใช้ผลงานของผู้เข้าร่วมค้าหลักรายเดียวเป็นผลงานของกิจการร่วมค้าที่ยื่นข้อเสนอ

สำหรับข้อตกลงฯ ที่ไม่ได้กำหนดให้ผู้เข้าร่วมค้ารายใดเป็นผู้เข้าร่วมค้าหลักผู้เข้าร่วมค้าทุกรายจะต้องมีคุณสมบัติครบถ้วนตามเงื่อนไขที่กำหนดไว้ในเอกสารเชิญชวน

3.11 ที่ปรึกษาที่จะเข้าร่วมการเสนองานกับหน่วยงานของรัฐ ต้องเป็นที่ปรึกษาที่ได้ขึ้นทะเบียนไว้กับศูนย์ข้อมูลที่ปรึกษา กระทรวงการคลัง

3.12 ที่ปรึกษาต้องเสนอทีมงานที่มีความรู้และประสบการณ์ การตรวจสอบระบบเทคโนโลยี สารสนเทศ พร้อมข้อมูลประวัติและประสบการณ์ของทีมงานรายบุคคล รวมทั้งผลงานและหน้าที่ความรับผิดชอบของแต่ละบุคคล (Profile) โดยทีมงานที่เสนอจะต้องมีคุณสมบัติดังนี้

3.12.1 ต้องเป็นผู้ตรวจ/ผู้นำการตรวจ (Lead Auditor) ตามมาตรฐาน ISO/IEC 27001:2013 ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ อย่างน้อย 1 ท่าน หรือได้รับประกาศนียบัตร Certified Information Systems Auditor (CISA) จากสถาบัน ISACA อย่างน้อย 1 ท่าน

3.12.2 ต้องเป็นผู้พัฒนา/ผู้นำการพัฒนา (Lead Implementer) ตามมาตรฐาน ISO/IEC 27001:2013 ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ อย่างน้อย 1 ท่าน

3.12.3 ต้องเป็นผู้ตรวจ/ผู้นำการตรวจ หรือผ่านการอบรมผู้ตรวจ/ผู้นำการตรวจ (Lead Auditor) ตามมาตรฐาน ISO/IEC 27032:2012 การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์

เอกสารเพื่อประกอบการเสนอราคา

อย่างน้อย 1 ท่าน หรือได้รับประกาศนียบัตรการอบรม Cybersecurity จากสถาบัน ISACA อย่างน้อย 1 ท่าน

3.13 ต้องจัดให้มีบุคลากรตำแหน่งต่าง ๆ เพื่อเป็นทีมผู้ปฏิบัติงาน ดังนี้

3.13.1 หัวหน้าโครงการ จำนวน 1 (หนึ่ง) คน จบการศึกษาไม่ต่ำกว่าระดับปริญญาโท ด้านเทคโนโลยีสารสนเทศหรือสาขาที่เกี่ยวข้อง และมีประสบการณ์ทำงานและผลงานในงานที่รับจ้างไม่น้อยกว่า 11 (สิบเอ็ด) ปี

3.13.2 ที่ปรึกษาด้านการตรวจสอบเทคโนโลยีสารสนเทศ หรือด้านความมั่นคงปลอดภัย จำนวน 2 (สอง) คน จบการศึกษาไม่ต่ำกว่าระดับปริญญาโท และมีประสบการณ์ทำงานและผลงานในงานที่รับจ้างไม่น้อยกว่า 11 (สิบเอ็ด) ปี

3.13.3 ที่ปรึกษาด้านการตรวจสอบเทคโนโลยีสารสนเทศ หรือด้านความมั่นคงปลอดภัย จำนวน 2 (สอง) คน จบการศึกษาไม่ต่ำกว่าระดับปริญญาตรี และมีประสบการณ์ทำงานและผลงานในงานที่รับจ้างไม่น้อยกว่า 5 (ห้า) ปี

3.13.4 เจ้าหน้าที่รับผิดชอบในการประสานงานและสนับสนุนการดำเนินงานให้เป็นไปตามแผนงานที่กำหนดไว้ จำนวน 1 (หนึ่ง) คน จบการศึกษาไม่ต่ำกว่าระดับปริญญาตรี และมีประสบการณ์ทำงานและผลงานในงานที่รับจ้างไม่น้อยกว่า 2 (สอง) ปี

ทั้งนี้ ผู้ยื่นข้อเสนอต้องแนบเอกสารรายละเอียดคุณสมบัติและประสบการณ์ของบุคลากรแต่ละตำแหน่งข้างต้น ให้เหมาะสมกับปริมาณงานในการจ้างในครั้งนี้ พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของบุคลากรแต่ละตำแหน่งที่ปฏิบัติงาน เพื่อเสนอให้ สพธอ. พิจารณาด้วย

4. <u>ขอบเขตการดำเนินงาน</u>

ที่ปรึกษาจะต้องส่งทีมงานที่ปรึกษาที่มีความรู้ ความชำนาญและมีประสบการณ์การตรวจสอบระบบเทคโนโลยีสารสนเทศมาดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศของ สพธอ. โดยมีหัวข้อดังนี้

4.1 ที่ปรึกษาต้องดำเนินการร่วมประชุมเปิดการตรวจกับทีมตรวจสอบของ สพธอ. เพื่อชี้แจง ขอบเขตการตรวจสอบ ระยะเวลา และวิธีการตรวจสอบต่อหน่วยรับตรวจที่เกี่ยวข้อง

4.2 ดำเนินการตรวจสอบเทคโนโลยีสารสนเทศ ด้านการตรวจสอบการควบคุมทั่วไปเทคโนโลยีสารสนเทศ (IT General Controls) ในภาพรวมของสำนักงาน โดยมีหัวข้อการตรวจสอบอย่างน้อย ดังนี้

4.2.1 การกำกับดูแลด้านเทคโนโลยีสารสนเทศขององค์กร (IT Governance)

4.2.1.1 การประเมิน และการสั่งการ

4.2.1.2 การจัดวางแนวทาง และแผนงาน

4.2.1.3 การพัฒนา การจัดหา และการนำไปใช้งาน

4.2.1.4 การส่งมอบ การให้บริการและสนับสนุนงาน

4.2.1.5 การเฝ้าติดตาม วัดผลและประเมินการดำเนินการ

เอกสารเผยแพร่ทางอิเล็กทรอนิกส์

4.2.2 การบริหารจัดการผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (IT Outsourcing Management)

4.2.2.1 บริบทขององค์กร

4.2.2.2 ภาวะผู้นำ

4.2.2.3 การวางแผน

4.2.2.4 การสนับสนุนสำหรับระบบบริหารงานบริการ

4.2.2.5 การปฏิบัติการของระบบบริหารงานบริการ

4.2.2.6 การประเมินผลการปฏิบัติงาน

4.2.2.7 การปรับปรุง

4.2.3 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Security Management System)

4.2.3.1 มาตรการขององค์กร

4.2.3.2 มาตรการด้านบุคลากร

4.2.3.3 มาตรการทางกายภาพ

4.2.3.4 มาตรการทางเทคโนโลยี

4.2.4 การบริหารจัดการบริการคลาวด์ (Cloud Services Management)

4.2.4.1 การกำหนดความรับผิดชอบบริการคลาวด์

4.2.4.2 การถอนหรือคืนทรัพย์สินเมื่อสิ้นสุดสัญญาบริการคลาวด์

4.2.4.3 การป้องกันและการแยกสภาพแวดล้อมบริการคลาวด์

4.2.4.4 การกำหนดค่าบริการคลาวด์

4.2.4.5 การดำเนินการดูแลระบบและขั้นตอนจัดการบริการคลาวด์

4.2.4.6 การติดตามกิจกรรมของบริการคลาวด์

4.2.4.7 การจัดตำแหน่งสภาพแวดล้อมเครือข่ายและบริการคลาวด์

4.3 ดำเนินการทดสอบช่องโหว่ระบบเทคโนโลยีสารสนเทศ (System Testing) โดยมีหัวข้อการตรวจสอบอย่างน้อย ดังนี้

4.3.1 จัดทำการตรวจสอบช่องโหว่ซอฟต์แวร์ (Vulnerability Assessment) และ ช่องโหว่ของระบบ Web Application (Vulnerability Scan)

4.3.1.1 สามารถตรวจสอบช่องโหว่โดยใช้ซอฟต์แวร์ที่ถูกออกแบบมาสำหรับการบริหารจัดการความเสี่ยงของตรวจสอบช่องโหว่ซอฟต์แวร์ (Vulnerability Assessment)

4.3.1.2 สามารถระบุประเภทของการตรวจสอบได้ เช่น ระบบปฏิบัติการ (OS) ซอฟต์แวร์ (Software) เน็ตเวิร์ก (Network) และ โปรโตคอล (Protocol) เป็นต้น

เอกสารเผยแพร่ผ่านเว็บไซต์

4.3.1.3 สามารถตรวจสอบช่องโหว่ซอฟต์แวร์ทั้งภายในองค์กร (IP Address) และภายนอกองค์กร (Domain)

4.3.1.4 สามารถตรวจสอบช่องโหว่โดยใช้ซอฟต์แวร์ที่ถูกออกแบบมาสำหรับการบริหารจัดการความเสี่ยงของระบบ Web Application (Vulnerability Scan)

4.3.1.5 สามารถตรวจสอบช่องโหว่ของ Web Application รูปแบบ Web Spidering หรือ Crawling

4.3.1.6 สามารถตรวจสอบช่องโหว่ของ Web Application ทั้งแบบ Non- Credential และ Credential Scan

4.3.1.7 สามารถตรวจสอบช่องโหว่ของ Web Application ตาม Signature หรือ ฐานข้อมูล Security Vulnerability อย่างน้อยตาม TOP 10 Web Application Hacking หรือ OWASP

4.3.1.8 สามารถสแกนช่องโหว่ Web Server ที่มีการใช้งานอยู่ทั่วไป เช่น Apache, Tomcat, IIS และ NGINX เป็นต้น

4.3.1.9 สามารถตรวจสอบหาช่องโหว่ CMS หรือเว็บไซต์สำเร็จรูปได้ เช่น WordPress, Drupal และ Joomla เป็นต้น

4.3.1.10 สามารถจัดทำรายงานการตรวจสอบช่องโหว่รูปแบบ CVSS 3.0 (Common Vulnerability Scoring System) ตามมาตรฐาน NIST พร้อมการนำเสนอ รวมทั้งการให้คำปรึกษา และตอบปัญหาหรือข้อหารือต่าง ๆ

4.3.2 จัดทำการทดสอบการเจาะระบบ Web Application (Penetration Testing)

4.3.2.1 การทดสอบการเจาะระบบจากภายนอกองค์กร (Black-Box) และภายในองค์กร (Grey-Box)

4.3.2.2 จัดทำแผนประเมินความเสี่ยง พร้อมทั้งหาวิธีรับมือกับความเสี่ยงหรือผลกระทบนั้น ๆ ก่อนการดำเนินการทดสอบเจาะระบบ หรือการค้นหาจุดอ่อนหรือช่องโหว่ โดยร่าง Scenario แบบการทดสอบการเจาะระบบโดยใช้รูปแบบ (Manual Test) โดยให้ครอบคลุมกับระบบของ Web Application

4.3.2.3 การทดสอบการเจาะระบบโดยการนำข้อมูลการตรวจสอบช่องโหว่ของ Web Application (Vulnerability Scan) มาอ้างอิงหรือประเมินความเสี่ยง

4.3.2.4 การทดสอบการเจาะระบบจะต้องใช้วิธีการที่เป็นตามมาตรฐาน OWASP TOP 10 หรือ SANS TOP 20 หรือ NIST 800-115 ได้เป็นอย่างน้อย

4.3.2.5 จัดทำรายงานสรุปผลพร้อมการนำเสนอ รวมทั้งการให้คำปรึกษา และตอบปัญหาหรือข้อหารือต่าง ๆ

เอกสารเผยแพร่ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

4.4 ศึกษาระบบงานเทคโนโลยีสารสนเทศที่ใช้งานอยู่ในปัจจุบันของ สพธอ. และประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อการวางแผนการตรวจสอบให้ครอบคลุมความเสี่ยงที่ได้จากการประเมินความเสี่ยงตามมาตรฐานสากลที่ยอมรับได้ เช่น COSO-ERM, ISO, และ COBIT5 เป็นต้น

4.5 จัดทำแผนการตรวจสอบประจำปีที่ได้จากการวิเคราะห์ประเมินความเสี่ยงบนพื้นฐานความเสี่ยงด้านระบบสารสนเทศให้เป็นไปตามมาตรฐานวิชาชีพระดับสากล อย่างน้อยต้องเป็นไปตาม COSO-ERM หรือที่ใหม่กว่า ทั้งนี้ ผู้รับจ้างจะต้องจัดทำแผนการตรวจสอบประจำปีตามที่ได้ระบุไว้ข้างต้น เพื่อให้ทีมงาน ตรวจสอบ สพธอ. สามารถใช้เป็นแนวทางในการจัดทำแผนการตรวจสอบได้ด้วยตนเองในปีถัด ๆ ไป

4.6 ร่วมประชุมปิดการตรวจและสรุปผลการตรวจสอบกับเจ้าหน้าที่และฝ่ายบริหารของ สพธอ. พร้อมจัดทำรายงานผลการตรวจสอบที่แสดงข้อตรวจพบ ผลกระทบ และข้อเสนอแนะในการปรับปรุงแก้ไขที่สามารถนำไปปฏิบัติได้

4.7 จัดทำรายงานการตรวจสอบระบบเทคโนโลยีสารสนเทศฉบับสมบูรณ์ พร้อมการนำเสนอต่อคณะกรรมการตรวจสอบ รวมทั้งการให้คำปรึกษา และตอบปัญหาหรือข้อหารือต่าง ๆ

4.8 จัดฝึกอบรมเชิงปฏิบัติการ จำนวน 2 หลักสูตร โดยให้มีผู้เข้าร่วมอบรมอย่างน้อย หลักสูตรละ 4 คน ดังนี้

4.8.1 ผู้ตรวจ/ผู้นำการตรวจประเมินมาตรฐาน ISO/IEC 27001:2022 ระบบบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ โดยต้อง

4.8.2 ผู้ตรวจประเมินภายในมาตรฐาน ISO/IEC 27701:2019 การจัดการข้อมูลส่วนบุคคล

5. <u>สถานที่ส่งมอบงาน</u>

ณ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือทางไปรษณีย์อิเล็กทรอนิกส์ saraban@etda.or.th

6. <u>วงเงินในการจัดหา</u>

วงเงินงบประมาณ 2,500,000 บาท (สองล้านห้าแสนบาทถ้วน) และราคากลางเป็นจำนวนเงิน 2,499,425.25 บาท (สองล้านสี่แสนเก้าหมื่นเก้าพันสี่ร้อยยี่สิบห้าบาทยี่สิบห้าสตางค์)

7. <u>ระยะเวลาดำเนินการ</u>

กำหนดระยะเวลาดำเนินการให้แล้วเสร็จภายใน 320 (สามร้อยยี่สิบ) วัน นับถัดจากวันที่ลงนามในสัญญา หรือวันที่สำนักงานมีหนังสือแจ้งให้เริ่มดำเนินการ แล้วแต่กรณี

8. <u>เงื่อนไขการทำหน้าที่ของที่ปรึกษา</u>

ตลอดระยะเวลาที่เข้าดำเนินการตามสัญญาจ้าง ต้องให้ผู้ตรวจสอบภายในของ สพธอ. มีส่วนร่วมในการปฏิบัติงานตรวจสอบและการรายงานผลการตรวจสอบในทุกขั้นตอน เพื่อพัฒนาความรู้ ทักษะ เทคนิค วิธีการตรวจสอบเทคโนโลยีสารสนเทศ

เอกสารเผยแพร่ผ่านระบบจัดซื้อจัดจ้างภาครัฐ

9. <u>สิ่งส่งมอบ กำหนดเวลาการส่งมอบและเงื่อนไขการจ่ายเงิน</u>

ที่ปรึกษาต้องดำเนินการและส่งมอบงานตามขอบเขตของงาน ข้อ 4 โดยแบ่งกำหนดระยะเวลาการส่งมอบเป็นจำนวน 4 (สี่) งวด โดยการส่งมอบงานในแต่ละงวดต้องส่งมอบ Hard Copy และ Flash Drive อย่างละ 2 ชุด ดังนี้

งวดที่ 1 อัตราร้อยละ 25 (ยี่สิบห้า) ของค่าจ้าง เมื่อได้ดำเนินการและส่งมอบงานตามขอบเขตการดำเนินงานข้อ 4.1 และข้อ 4.2.1 ภายใน 80 (แปดสิบ) วัน นับถัดจากวันที่ลงนามในสัญญา หรือวันที่สำนักงานมีหนังสือแจ้งให้เริ่มดำเนินการ และคณะกรรมการตรวจรับได้ตรวจรับงานจ้างครบถ้วนถูกต้องแล้ว

งวดที่ 2 อัตราร้อยละ 25 (ยี่สิบห้า) ของค่าจ้าง เมื่อได้ดำเนินการและส่งมอบงานตามขอบเขตการดำเนินงานข้อ 4.2.2 และข้อ 4.3.1 และข้อ 4.8.1 ภายใน 160 (หนึ่งร้อยหกสิบ) วัน นับถัดจากวันที่ลงนามในสัญญา หรือวันที่สำนักงานมีหนังสือแจ้งให้เริ่มดำเนินการ และคณะกรรมการตรวจรับได้ตรวจรับงานจ้างครบถ้วนถูกต้องแล้ว

งวดที่ 3 อัตราร้อยละ 25 (ยี่สิบห้า) ของค่าจ้าง เมื่อได้ดำเนินการและส่งมอบงานตามขอบเขตการดำเนินงานข้อ 4.2.3 และข้อ 4.8.2 ภายใน 240 (สองร้อยสี่สิบ) วัน นับถัดจากวันที่ลงนามในสัญญา หรือวันที่สำนักงานมีหนังสือแจ้งให้เริ่มดำเนินการ และคณะกรรมการตรวจรับได้ตรวจรับงานจ้างครบถ้วนถูกต้องแล้ว

งวดที่ 4 อัตราร้อยละ 25 (ยี่สิบห้า) ของค่าจ้าง เมื่อได้ดำเนินการและส่งมอบงานตามขอบเขตการดำเนินงานข้อ 4.2.4 และข้อ 4.3.2 และข้อ 4.4 และข้อ 4.5 และข้อ 4.6 และข้อ 4.7 ภายใน 320 (สามร้อยยี่สิบ) วัน นับถัดจากวันที่ลงนามในสัญญา หรือวันที่สำนักงานมีหนังสือแจ้งให้เริ่มดำเนินการ และคณะกรรมการตรวจรับได้ตรวจรับงานจ้างครบถ้วนถูกต้องแล้ว

10. <u>อัตราค่าปรับ</u>

เมื่อครบกำหนดส่งมอบงานตามที่กำหนด ถ้าที่ที่ปรึกษาไม่ส่งมอบงานตามที่ตกลงจ้างให้แก่ สพธอ. ส่งมอบล่าช้าหรือส่งมอบไม่ถูกต้อง หรือไม่ครบจำนวน ที่ปรึกษาจะต้องชำระค่าปรับให้แก่ สพธอ. เป็นรายวันเป็นจำนวนเงินตายตัวในอัตราร้อยละ 0.10 (ศูนย์จุดหนึ่งศูนย์) ของราคางานจ้าง แต่ต้องไม่ต่ำกว่าวันละ 100 บาท (หนึ่งร้อยบาทถ้วน) นับถัดจากวันที่ครบกำหนดตามสัญญาจนถึงวันที่ที่ปรึกษาได้ส่งมอบงานให้แก่ สพธอ. จนถูกต้องครบถ้วน

11. <u>การจัดทำข้อเสนอโครงการ</u>

ต้องจัดทำข้อเสนอโครงการโดยแยกเป็น ข้อเสนอด้านเทคนิค และข้อเสนอด้านราคา ตามรายละเอียดข้อ 4 เสนอต่อ “ประธานคณะกรรมการดำเนินการจ้าง โครงการจ้างที่ปรึกษาตรวจสอบระบบเทคโนโลยีสารสนเทศ ปี 2568” นำส่งไฟล์อิเล็กทรอนิกส์ ทางไปรษณีย์อิเล็กทรอนิกส์ procure@etda.or.th

11.1 ต้องนำเสนอแนวคิดและวิธีการในการดำเนินงานตามรายละเอียดในข้อเสนอด้านเทคนิค ต่อคณะกรรมการดำเนินการจ้างที่ปรึกษาสำหรับโครงการจ้างที่ปรึกษาตรวจสอบระบบเทคโนโลยีสารสนเทศ ปี 2568 โดยใช้เวลาไม่เกิน 30 (สามสิบ) นาที ตามวัน เวลา และสถานที่ สพธอ. กำหนด

เอกสารใช้เพื่อการประกวดราคาเท่านั้น

11.2 ข้อเสนอโครงการ ต้องแสดงรายละเอียด ดังต่อไปนี้

1) ข้อเสนอด้านเทคนิค จะต้องมีรายละเอียดครอบคลุมประเด็นสำคัญ ดังนี้

1.1 วิธีการของการดำเนินงาน แผนการดำเนินงาน ผลงานส่งมอบ และข้อเสนอที่จะทำให้บรรลุวัตถุประสงค์ และขอบเขตการดำเนินงาน โดยให้มีรายละเอียดครอบคลุมเนื้อหาทั้งหมดตามที่ระบุไว้ใน ข้อ 4 ของเอกสารขอบเขตการดำเนินงาน (TOR) ฉบับนี้

1.2 รายละเอียดของบุคลากรของที่ปรึกษาทั้งหมด โดยระบุรายชื่อ ความเชี่ยวชาญ คุณสมบัติพิเศษของบุคลากรหรือที่ปรึกษา ประสบการณ์การทำงานในอดีตและปัจจุบัน รวมทั้งหน้าที่ความรับผิดชอบของบุคลากรแต่ละคน

2) ข้อเสนอด้านราคา จะต้องมีรายละเอียดค่าใช้จ่ายทั้งหมดที่ต้องใช้ในการดำเนินงาน โดยแยกตามประเภทรายการ คือ

2.1 ค่าใช้จ่ายบุคลากร เช่น ค่าตอบแทนบุคลากรของที่ปรึกษา โดยแสดงรายละเอียดจำนวนบุคลากรและระยะเวลาการทำงาน

2.2 ค่าใช้จ่ายดำเนินงาน เช่น ค่าจัดประชุม ค่าเดินทาง ค่าจัดพิมพ์ และค่าสำเนาเอกสาร หรือค่าใช้จ่ายอื่น ๆ เช่น ค่าโทรศัพท์ ค่าโทรสาร

2.3 ค่าใช้จ่ายอื่น เช่น ค่าธรรมเนียม และค่าภาษี

ทั้งนี้ เอกสารทุกฉบับให้ประทับตราสถาบันหรือตราบริษัท และกรณีที่เป็นสำเนา ต้องให้ผู้มีอำนาจลงนามรับรองสำเนาถูกต้อง

12. <u>การรักษาความลับ</u>

12.1 ที่ปรึกษาจะต้องจัดเก็บรักษาข้อมูลต่าง ๆ ที่เกี่ยวกับการดำเนินงานที่ที่ปรึกษาได้รับจาก สพธอ. และข้อมูลต่าง ๆ ที่ที่ปรึกษาได้จัดทำขึ้นเนื่องจากการดำเนินงานตามสัญญานี้อย่างเป็นความลับของ สพธอ. ซึ่งต่อไปในสัญญานี้เรียกว่า “ข้อมูลที่เป็นความลับ” โดยที่ปรึกษาต้องหามาตรการในการจัดเก็บข้อมูลที่เป็นความลับให้มิดชิด รวมทั้งไม่เปิดเผย หรือเผยแพร่ หรือกระทำด้วยวิธีการใดให้บุคคลอื่นใดที่มิใช่คู่สัญญาภายใต้สัญญานี้ หรือมิใช่บุคคลที่ สพธอ. ได้อนุญาตเป็นลายลักษณ์อักษรให้มีส่วนเกี่ยวข้องที่จะรับทราบข้อมูลที่เป็นความลับภายใต้สัญญานี้ ได้ทราบถึงข้อมูลที่เป็นความลับดังกล่าว เว้นแต่จะเป็นการเปิดเผยข้อมูลดังกล่าวให้แก่เจ้าหน้าที่ผู้ปฏิบัติงานของที่ปรึกษาที่ต้องเกี่ยวข้องโดยตรงกับข้อมูลดังกล่าวเท่านั้น และที่ปรึกษาจะต้องจัดให้เจ้าหน้าที่ผู้ปฏิบัติงานดังกล่าวได้ผูกพันและปฏิบัติตามเงื่อนไขในการรักษาข้อมูลที่เป็นความลับเช่นว่านั้นด้วย

12.2 หากที่ปรึกษามิได้ปฏิบัติตามข้อ 12.1 ที่ปรึกษาจะต้องรับผิดชอบต่อ สพธอ. หรือบุคคลอื่นที่เป็นเจ้าของข้อมูลที่เป็นความลับนั้นในความเสียหายใด ๆ ที่เกิดขึ้นเนื่องจากการที่ข้อมูลที่เป็นความลับดังกล่าว ได้ถูกเปิดเผยไม่ว่าทั้งหมดหรือแต่บางส่วน และ สพธอ. มีสิทธิบอกเลิกสัญญาได้ทันที

เอกสารนี้เผยแพร่เพื่อการศึกษาเท่านั้น

12.3 ที่ปรึกษาจะยังคงต้องผูกพันตามข้อกำหนดเกี่ยวกับการรักษาข้อมูลที่เป็นความลับตามข้อ 12.1 ต่อไป ตราบที่ข้อมูลที่เป็นความลับดังกล่าวยังคงเป็นความลับอยู่ แม้ว่าการจ้างตามสัญญานี้ได้สิ้นสุดลงแล้วไม่ว่าด้วยเหตุใดก็ตาม

13. <u>หลักเกณฑ์ในการพิจารณา</u>

พิจารณาโดยใช้เกณฑ์เกณฑ์คุณภาพและราคาต่ำสุด

การพิจารณาข้อเสนอตามขอบเขตงาน ผู้ที่ผ่านการพิจารณาตามเกณฑ์ต้องได้รับคะแนนไม่น้อยกว่า 80 (แปดสิบ) คะแนน จากคะแนนรวม 100 (หนึ่งร้อย) คะแนน และหากไม่ผ่านคะแนนขั้นต่ำด้านคุณภาพจะไม่พิจารณาข้อเสนอด้านราคา หลักเกณฑ์การพิจารณา ดังนี้

ลำดับ	รายละเอียด	น้ำหนัก (ร้อยละ)	คะแนนต่อข้อ (100)	คะแนนรวม (100)
1	ผลงานและประสบการณ์ของผู้เสนอราคารวมถึงบุคลากรที่ร่วมงาน	<u>40</u>		
	1.1) ที่ปรึกษามีประวัติหรือผลงานที่เกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศให้กับองค์กรภาครัฐ รัฐวิสาหกิจ หรือภาคเอกชน ในประเทศไทย โดยแสดงประวัติและผลงานที่ทำสำเร็จแล้ว ภายในระยะเวลา 5 ปี <u>เกณฑ์การให้คะแนน</u> - 10 หน่วยงานหรือมากกว่า จะได้คะแนน 20 คะแนน - 7 หน่วยงานหรือมากกว่า จะได้คะแนน 18 คะแนน - 5 หน่วยงานหรือมากกว่า จะได้คะแนน 16 คะแนน - มีผลงานน้อยกว่า 5 หน่วยงาน หรือไม่มีผลงาน จะได้ 0 คะแนน	20		
	1.2) พิจารณาคุณวุฒิ และประสบการณ์ของบุคลากรที่จะร่วมในโครงการ <u>เกณฑ์การให้คะแนน</u> - มีประวัติการศึกษามากกว่าที่กำหนดใน TOR หรือมีผลงานหรือประสบการณ์ที่เกี่ยวข้องกับโครงการ หรือมีประกาศนียบัตรมากกว่าที่กำหนด อย่างน้อย 2 รายการ ได้คะแนน 20 คะแนน	20		

เอกสารเผยแพร่ในเว็บไซต์

ลำดับ	รายละเอียด	น้ำหนัก (ร้อยละ)	คะแนนต่อข้อ (100)	คะแนนรวม (100)
	- มีประวัติการศึกษาตรงตามที่กำหนดใน TOR และมีผลงานและประสบการณ์ที่เกี่ยวข้องกับโครงการ และมีประกาศนียบัตร ตามที่กำหนด ได้คะแนน 15 คะแนน - มีประวัติการศึกษาไม่ตรงตามที่กำหนดใน TOR หรือไม่มีผลงานหรือประสบการณ์ที่เกี่ยวข้องกับโครงการ หรือไม่มีประกาศนียบัตรตามที่กำหนด ได้คะแนน 0 คะแนน			
2	แนวคิด วิธีการ เครื่องมือที่ใช้ แผนการดำเนินการ ความสมบูรณ์ของเนื้อหา ความสอดคล้องกับ TOR	60		
	2.1) แนวคิด วิธีการ และเครื่องมือที่ใช้ รูปแบบของวิธีการดำเนินงานที่นำเสนอ ตัวอย่างเนื้อหา สะท้อนให้เห็นถึงความรู้ ความเข้าใจในงาน และแสดงให้เห็นถึงผลลัพธ์ตามวัตถุประสงค์ตามขอบเขตงาน <u>เกณฑ์การให้คะแนน</u> - แนวคิด วิธีการ และเครื่องมือที่ใช้ เป็นไปตามมาตรฐานแนวทางปฏิบัติ และกรอบวิธีปฏิบัติสากล รูปแบบของวิธีการดำเนินงานมีความน่าสนใจ แสดงให้เห็นถึงความรู้และเข้าใจในงาน และเห็นถึงความสอดคล้องกับผลลัพธ์ตามวัตถุประสงค์ตามขอบเขตงาน เท่ากับ 30 คะแนน - แนวคิด วิธีการ และเครื่องมือที่ใช้ เป็นไปตามมาตรฐานแนวทางปฏิบัติ และกรอบวิธีปฏิบัติสากล มีการนำเสนอรูปแบบของวิธีการดำเนินงาน และเห็นถึงความสอดคล้องกับผลลัพธ์ตามวัตถุประสงค์ตามขอบเขตงาน เท่ากับ 25 คะแนน - แนวคิด วิธีการ และเครื่องมือที่ใช้ ไม่เป็นไปตามมาตรฐานแนวทางปฏิบัติ และกรอบวิธีปฏิบัติสากล หรือมีการนำเสนอรูปแบบของวิธีการดำเนินงาน ไม่สอดคล้องกับวัตถุประสงค์ของขอบเขตงานตามที่กำหนด ได้คะแนน 0 คะแนน	30		

เอกสารใช้ประกอบการพิจารณาเว็บไซต์

ลำดับ	รายละเอียด	น้ำหนัก (ร้อยละ)	คะแนนต่อข้อ (100)	คะแนนรวม (100)
	2.2) แผนการดำเนินการ สอดคล้องตามขอบเขตของงาน พร้อมระยะเวลาดำเนินงาน โดยให้ความสำคัญกับการแสดงรายละเอียดที่ชัดเจน แนวโน้มสามารถดำเนินการได้จริงภายในระยะเวลาที่กำหนด พร้อมวิธีการควบคุมติดตาม <u>เกณฑ์การให้คะแนน</u> - แผนการปฏิบัติงาน มีรายละเอียดสอดคล้องตามขอบเขตงาน และมีแผนสำรองกรณีเหตุขัดข้องไม่สามารถดำเนินการได้ตามแผนที่ตั้งไว้ จะได้คะแนน 30 คะแนน - แผนการปฏิบัติงาน มีรายละเอียดสอดคล้องตามขอบเขตงาน จะได้คะแนน 25 คะแนน - แผนการปฏิบัติงานมีรายละเอียดที่ไม่ครบถ้วนหรือไม่สอดคล้องตามขอบเขตงาน จะได้คะแนน 0 คะแนน	30		
	คะแนนรวมทั้งหมด	<u>100</u>		

เอกสารเผยแพร่ผ่านเว็บไซต์