การประเมินความเสี่ยงการทุจริต ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

๑. การกำหนดเกณฑ์การประเมินความเสี่ยงการทุจริต

๑.๑ โอกาสเกิดการทุจริต (Likelihood)

โอกาสเกิดการทุจริต (Likelihood)	
๕	มีโอกาสในการเกิดขึ้นสูงมาก
๔	มีโอกาสในการเกิดขึ้นมาก
๓	มีโอกาสในการเกิดขึ้นปานกลาง
๒	มีโอกาสในการเกิดขึ้นน้อยมาก
๑	ไม่มีโอกาสเกิดขึ้นเลย

๑.๒ เกณฑ์ผลกระทบ (Impact)

เกณฑ์ผลกระทบ (Impact)	
๕	ส่งผลกระทบไปยังภายนอกกรม
๔	ส่งผลกระทบระดับกรม
๓	ส่งผลกระทบระดับหน่วยงาน (กอง สถาบัน ศูนย์ กลุ่ม สำนักงานเลขานุการกรม สำนักงานคลังเขต)
๒	ส่งผลกระทบในระดับหน่วยงานภายใต้กอง สถาบัน ศูนย์ กลุ่ม สำนักงานเลขานุการกรม สำนักงานคลังเขต
๑	ไม่ส่งผลเลย หรือส่งผลกระทบระดับบุคคล

๑.๓ เกณฑ์การวัดระดับความรุนแรงของความเสี่ยงการทุจริต

Risk Score					
โอกาสเกิด (Likelihood)	ผลกระทบ (Impact)				
	๑	๒	๓	๔	๕
๕	ปานกลาง	สูง	สูง	สูงมาก	สูงมาก
๔	ปานกลาง	ปานกลาง	สูง	สูง	สูงมาก
๓	ต่ำ	ปานกลาง	ปานกลาง	สูง	สูง
๒	ต่ำ	ต่ำ	ปานกลาง	ปานกลาง	สูง
๑	ต่ำ	ต่ำ	ต่ำ	ปานกลาง	ปานกลาง

ระดับความรุนแรงของความเสี่ยงการทุจริต

	ค่าความเสี่ยงรวม	ระดับความเสี่ยงการทุจริต
สีเขียว	๑ – ๓	ความเสี่ยงระดับต่ำ
สีเหลือง	๔ – ๙	ความเสี่ยงระดับปานกลาง
สีส้ม	๑๐ – ๑๖	ความเสี่ยงระดับสูง
สีแดง	๑๗ – ๒๕	ความเสี่ยงระดับสูงมาก

*** สามารถปรับเกณฑ์ประเมินความเสี่ยงการทุจริตได้ตามความเหมาะสมของหน่วยงาน**

๒. การประเมินความเสี่ยงการทุจริต

การประเมินความเสี่ยงการทุจริต					
ลำดับที่	ขั้นตอนการดำเนินงาน	ประเด็นความเสี่ยงการทุจริต	Risk Score (L x I)		
			Likelihood	Impact	Rise Score
๑. ๒. ๓. ๔. ๕. ๖. ๗.	จัดทำและทบทวนนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ควบคุมและดูแลให้มีการปฏิบัติตามนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง ตรวจสอบและติดตามภัยคุกคามทางด้านสารสนเทศ ศึกษาและวิเคราะห์เกี่ยวกับพฤติกรรมภัยคุกคามทางด้านสารสนเทศ วางแผนและประสานงานเรื่องงบประมาณเพื่อจัดหาอุปกรณ์ทางด้านการรักษาความปลอดภัยสารสนเทศ ประสานงานและตรวจสอบแผนสำรองฉุกเฉินระบบคอมพิวเตอร์ (Disaster Recovery Plan) ให้มีประสิทธิภาพและทันสมัย วางแผนและจัดให้มี IT Awareness Training	การละเมิดข้อมูล (Data breaches) หรือผู้ไม่มีสิทธิเข้าถึง แก้ไข ลบ หรือเปิดเผยข้อมูลที่เป็นความลับ	๔	๕	๒๐

๓. แผนบริหารจัดการความเสี่ยงการทุจริต

กระบวนการ/โครงการ การรักษาความปลอดภัยด้านสารสนเทศ หน่วยงาน กรมบัญชีกลาง		
ลำดับที่	**ขั้นตอนการดำเนินงาน/ประเด็นความเสี่ยงการทุจริต**	**มาตรการควบคุมความเสี่ยงการทุจริต**
๑.	การละเมิดข้อมูลหรือผู้ไม่มีสิทธิอาจเข้าถึง แก้ไข ลบ หรือเปิดเผยข้อมูลที่เป็นความลับ ความเสี่ยงในประเด็นดังกล่าว อาจเกิดขึ้นในกรณีที่เจ้าหน้าที่กรมบัญชีกลางในฐานะผู้ดูแลระบบทั้งเจ้าหน้าที่ผู้ดูแลระบบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และเจ้าหน้าที่ผู้ดูแลระบบปฏิบัติการต่าง ๆ ตามภารกิจของกรมบัญชีกลาง เป็นผู้ที่สามารถเข้าถึงข้อมูลส่วนบุคคล เช่น ข้อมูลของบุคลากรภาครัฐและบุคคลในครอบครัว ข้อมูลผู้ค้าภาครัฐ เป็นต้น และอาจใช้ตำแหน่งหน้าที่ของตนแก้ไข ลบหรือนำข้อมูลดังกล่าวไปเปิดเผยต่อผู้อื่นโดยปราศจากความยินยอมของเจ้าของข้อมูล	กรมบัญชีกลางมีมาตรการควบคุมความเสี่ยงการทุจริตในกระบวนงานการรักษาความปลอดภัยด้านสารสนเทศ ดังนี้ ๑. การบริหารจัดการสิทธิการเข้าถึงระบบ และข้อมูลที่มีความสำคัญ ๒. ฝึกอบรม ทบทวนนโยบายและซักซ้อมความเข้าใจเป็นระยะ ๓. ใช้อุปกรณ์ และเครื่องมือเข้ามาช่วยบริหารจัดการสิทธิในการเข้าถึง ๔. จัดเก็บ Log ในการทำงานต่าง ๆ เพื่อให้ตรวจสอบได้ ๕. มีขั้นตอนปฏิบัติ และทบทวนกระบวนการ และมีมาตรการควบคุมตามหลักการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC๒๗๐๐๑ ๖. ทบทวนสิทธิของผู้ดูแลระบบ ทั้งนี้ การตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC๒๗๐๐๑:๒๐๑๓ กรมได้ดำเนินโครงการจ้างที่ปรึกษาพัฒนานโยบายการกำกับดูแลระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และแผนบริหารความต่อเนื่อง โดยในโครงการจะมีการวางแผนพัฒนาระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑ หรือ Information Security Management System (ISMS) ซึ่งเป็นมาตรฐานสากลด้านการจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ซึ่งกำหนดขึ้นโดยองค์กร ISO (International Organization for Standardization) ร่วมมือกับองค์กร IEC (International Electro technical Commission) อย่างไรก็ดี มาตรการควบคุมความเสี่ยงการทุจริตที่มีอยู่สามารถลดความเสี่ยงได้ในระดับหนึ่ง แต่ยังไม่เพียงพอ ยังมีความเสี่ยงที่อาจก่อให้เกิดการทุจริตในกระบวนงานดังกล่าว ได้แก่ การละเมิดข้อมูลหรือผู้ไม่มีสิทธิอาจเข้าถึง แก้ไข ลบ หรือเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลส่วนบุคคลตามพระราชบัญญัติข้อมูลข่าวสารส่วนบุคคล พ.ศ. ๒๕๔๐ กรมบัญชีกลางจึงเห็นควรกำหนดมาตรการควบคุมความเสี่ยงการทุจริตเพิ่มเติม ดังนี้ ๑. การเพิ่มอุปกรณ์ช่วยในการตรวจสอบ ติดตาม และป้องกันการเกิดข้อมูลรั่วไหล (ดักจับการรั่วไหลข้อมูล) ๒. ปรับปรุงกระบวนการตรวจสอบ ติดตามให้ทันสมัย ทันต่อภัยคุกคาม

๔. แบบสรุปรายงานการประเมินความเสี่ยงการทุจริต

๔.๑ แบบสรุปรายงานการประเมินความเสี่ยงการทุจริต ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ (รอบที่ ๑)

แบบสรุปรายงานการประเมินความเสี่ยงการทุจริต ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ รอบที่ ๑ แผนบริหารจัดการความเสี่ยงการทุจริต			
ชื่อหน่วยงาน กรมบัญชีกลาง			
ด้านที่ ๒ การใช้อำนาจและตำแหน่งหน้าที่ ๑. ชื่องานตามภารกิจ กระบวนงานการรักษาความปลอดภัยด้านสารสนเทศ			
ที่	**ขั้นตอนที่มีความเสี่ยงและ รายละเอียดประเด็นความเสี่ยงการทุจริต**	**ระดับความเสี่ยง การทุจริต**	**รายละเอียดมาตรการ ควบคุมความเสี่ยงการทุจริต**
๑.	การละเมิดข้อมูลหรือผู้ไม่มีสิทธิอาจเข้าถึง แก้ไข ลบ หรือเปิดเผยข้อมูลที่เป็นความลับ ความเสี่ยงในประเด็นดังกล่าว อาจเกิดขึ้นในกรณีที่เจ้าหน้าที่กรมบัญชีกลางในฐานะผู้ดูแลระบบ ทั้งเจ้าหน้าที่ผู้ดูแลระบบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และเจ้าหน้าที่ผู้ดูแลระบบปฏิบัติการต่าง ๆ ตามภารกิจของกรมบัญชีกลาง เป็นผู้ที่สามารถเข้าถึงข้อมูลส่วนบุคคล เช่น ข้อมูลของบุคลากรภาครัฐและบุคคลในครอบครัว ข้อมูลผู้ค้าภาครัฐ เป็นต้น และอาจใช้ตำแหน่งหน้าที่ของตนแก้ไข ลบหรือนำข้อมูลดังกล่าวไปเปิดเผยต่อผู้อื่นโดยปราศจากความยินยอมของเจ้าของข้อมูล	สูงมาก	มาตรการควบคุมความเสี่ยงการทุจริต ดังนี้ ๑. การเพิ่มอุปกรณ์ช่วยในการตรวจสอบ ติดตามและป้องกันการเกิดข้อมูลรั่วไหล (ดักจับการรั่วไหลข้อมูล) ๒. ปรับปรุงกระบวนการตรวจสอบ ติดตามให้ทันสมัยทันต่อภัยคุกคาม