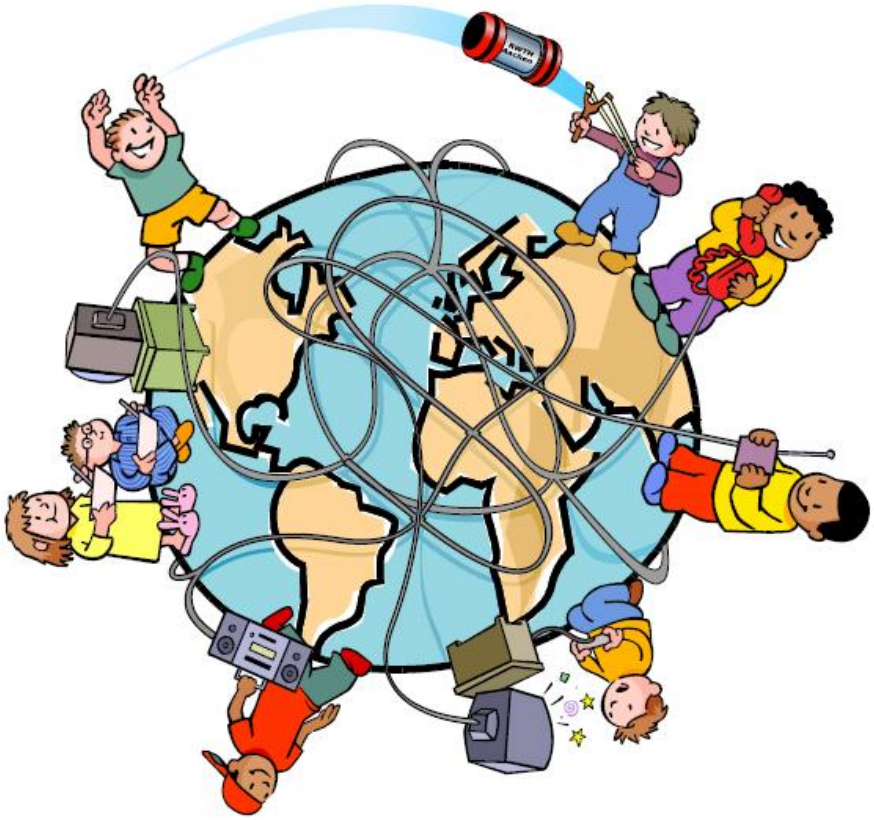
ประเมินความเสี่ยงด้านสารสนเทศ

และ

แผนด้านเทคโนโลยีสารสนเทศ



ประจำปี ๒๕๖๔

ของกลุ่มตรวจสอบภายใน

การบริหารความเสี่ยง

ด้านเทคโนโลยีสารสนเทศ กลุ่มตรวจสอบภายใน

กรมสนับสนุนบริการสุขภาพ

การประเมินความเสี่ยง หมายถึง การคาดคะเนหรือคำนวณโอกาสที่จะเกิดมูลเหตุที่นำไปสู่ความเสียหาย เพื่อให้ทราบถึงความสำคัญของความเสี่ยงที่แตกต่างกัน และใช้ในการพิจารณากำหนดจุดควบคุมความเสี่ยงที่มีนัยสำคัญ

การประเมินความเสี่ยงเป็นกระบวนการที่ประกอบด้วย การวิเคราะห์ การประเมิน และการจัดระดับความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานขององค์กร ดังนี้

(๑) การกำหนดเกณฑ์การประเมินความเสี่ยง ได้แก่ ระดับโอกาสที่จะเกิดความเสียหาย (Likelihood) ระดับความรุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) โดยคณะทำงานบริหารความเสี่ยงระดับกรมได้กำหนดเกณฑ์การประเมินความเสี่ยงของกรมสนับสนุนบริการสุขภาพ ดังแสดงในตารางที่ ๑

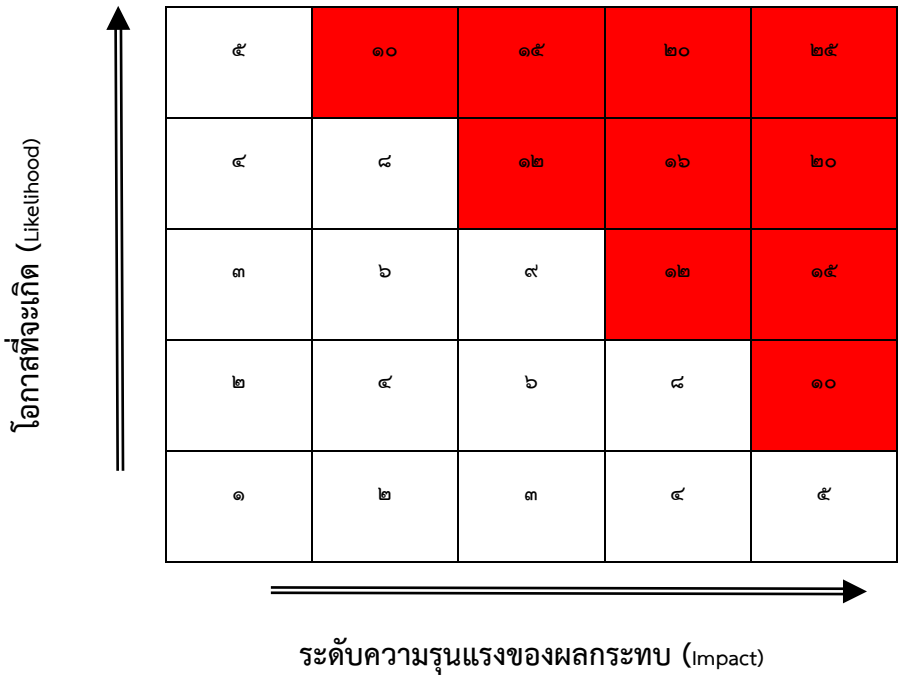
ตารางที่ ๑ แสดงเกณฑ์การประเมินความเสี่ยงของกรมสนับสนุนบริการสุขภาพ

ประเด็นในการพิจารณา		ระดับคะแนน				
		๑=น้อยมาก	๒=น้อย	๓=ปานกลาง	๔=สูง	๕=สูงมาก
โอกาสที่จะเกิดความเสียหาย (Likelihood : L)						
- ระเบียบและคู่มือปฏิบัติ	L๑	มีทั้ง๒อย่างและมีการปฏิบัติ	มีอย่างใดอย่างหนึ่งและมีการปฏิบัติ	มีทั้ง๒อย่างแต่ปฏิบัติตามอย่างใดอย่างหนึ่ง	มีอย่างใดอย่างหนึ่งแต่ไม่ถือปฏิบัติ	ไม่มีทั้ง๒อย่างและไม่ถือปฏิบัติ
- การควบคุม ติดตาม และตรวจสอบของผู้บังคับบัญชาหรือหน่วยงานอื่น	L๒	๒ สัปดาห์	๑ เดือน	๓ เดือน	๖ เดือน	>/เท่ากับ ๑ ปี
- การอบรม/สอนงาน/ทบทวนการปฏิบัติงาน	L๓	ทุกเดือน	ทุก ๓ เดือน	ทุก ๖ เดือน	ทุก ๑ ปี	มากกว่า ๑ ปี
- ความถี่ในการเกิด	L๔	๕ ปี/ครั้ง	๒-๓ ปี/ครั้ง	๑ ปี/ครั้ง	๑-๖ เดือน/ครั้ง ไม่เกิน ๕ ครั้ง/ปี	๑ เดือน/ครั้งหรือมากกว่าเกิดขึ้นแน่นอนตั้งแต่ ๒ ครั้ง/ปีขึ้นไป

ประเด็นในการพิจารณา		ระดับคะแนน				
		๑=น้อยมาก	๒=น้อย	๓=ปานกลาง	๔=สูง	๕=สูงมาก
- โอกาสที่จะเกิดเหตุการณ์	L๕	น้อยที่สุด	น้อย	ปานกลาง	สูง	เกิดขึ้นแน่นอน
- ความถี่ในการเปลี่ยนแปลง	L๖	๔ ปี/ครั้ง	๓ ปี/ครั้ง	๒ ปี/ครั้ง	๑ ปี/ครั้ง	ตั้งแต่ ๒ ครั้ง/ปี ขึ้นไป
ความรุนแรงของผลกระทบ (Consequent : C)						
- มูลค่าความเสียหาย	C๑	>๑ หมื่นบาท	๑-๕ หมื่นบาท	๕ หมื่น-๒.๕ แสนบาท	๒.๕ แสน-๑๐ ล้านบาท	>๑๐ ล้านบาท
- อันตรายต่อชีวิต	C๒.๑	เดือนร้อน	บาดเจ็บเล็กน้อย	บาดเจ็บต้องรักษาแพทย์	บาดเจ็บสาหัส	อันตรายถึงชีวิต
- ระดับความปลอดภัย	C๒.๒	น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
- ผลกระทบต่อภาพลักษณ์	C๓.๑	น้อยมาก	น้อย	ปานกลาง	สูง	สูงมาก
- ความพึงพอใจ	C๓.๒	พึงพอใจ >๘๐%	>๖๐-๘๐%	>๔๐-๖๐%	>๒๐-๔๐%	</เท่ากับ ๒๐%
- ข่าวสารจากสื่อในทางลบ	C๓.๓	๑ ข่าว/เดือน	๒ ข่าว/เดือน	๓ ข่าว/เดือน	๔ ข่าว/เดือน	>/เท่ากับ ๕ ข่าว/เดือน
- ผู้รับบริการได้รับความเสียหาย หรือผู้ได้รับผลกระทบ	C๔	กระทบเฉพาะกลุ่มผู้เกี่ยวข้องโดยตรงบางราย	กระทบเฉพาะกลุ่มผู้เกี่ยวข้องโดยตรงเป็นส่วนใหญ่	กระทบเฉพาะกลุ่มผู้เกี่ยวข้องโดยตรงทั้งหมด	กระทบกลุ่มผู้เกี่ยวข้องโดยตรงทั้งหมดและผู้อื่นบางส่วน	กระทบกลุ่มผู้เกี่ยวข้องโดยตรงทั้งหมดและผู้อื่นมากราย
- จำนวนผู้ร้องเรียน	C๕	น้อยกว่า ๑ราย (ต่อเดือน)	๑-๒ ราย (ต่อเดือน)	๓-๕ ราย (ต่อเดือน)	๕-๖ ราย (ต่อเดือน)	๗ รายขึ้นไป (ต่อเดือน)

และได้กำหนดเกณฑ์ระดับความเสี่ยงไว้ ๔ ระดับ ได้แก่ ต่ำ ปานกลาง สูง และสูงมาก ดังนี้

- ระดับความเสี่ยงต่ำ หมายถึง ปัจจัยเสี่ยงที่มีระดับคะแนนความเสี่ยง ๑-๓ คะแนน
- ระดับความเสี่ยงปานกลาง หมายถึง ปัจจัยเสี่ยงที่มีระดับคะแนนความเสี่ยง ๔-๙ คะแนน
- ระดับความเสี่ยงสูง หมายถึง ปัจจัยเสี่ยงที่มีระดับคะแนนความเสี่ยง ๑๐-๑๖ คะแนน
- ระดับความเสี่ยงสูงมาก หมายถึง ปัจจัยเสี่ยงที่มีระดับคะแนนความเสี่ยง ๑๗-๒๕ คะแนน



(๒) การประเมินโอกาสและผลกระทบของความเสี่ยง วิเคราะห์ระดับความเสี่ยง

เป็นการนำความเสี่ยงและปัจจัยเสี่ยงที่ระบุไว้มาประเมินโอกาสที่จะเกิดความเสียหาย(Likelihood) และประเมินระดับความรุนแรงของผลกระทบ (Impact) ตามเกณฑ์การประเมินความเสี่ยงของกรมสนับสนุนบริการสุขภาพ เพื่อให้เห็นถึงระดับของความเสี่ยง (Degree of Risk) ที่แตกต่างกัน

ประเมินความเสี่ยงด้านสารสนเทศ

กลุ่มตรวจสอบภายใน กรมสนับสนุนบริการสุขภาพ ประจำปี ๒๕๖๔

กระบวนงาน/วัตถุประสงค์	ความเสี่ยง	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	รวม
<u>กระบวนงานการวางนโยบาย</u>					
วัตถุประสงค์: เพื่อให้การรักษาความมั่นคงปลอดภัยมีกรอกทิศทางและแนวทางปฏิบัติที่มีประสิทธิภาพ	การรักษาความมั่นคงปลอดภัยไม่มีกรอบทิศทางหรือแนวทางปฏิบัติ	-ขาดการจัดทำข้อปฏิบัติรองรับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ	๑	๔	๔
	กรอบและทิศทางหรือแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไม่มีประสิทธิภาพ	-ขาดการสื่อสารข้อปฏิบัติรองรับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศหรือสื่อสารไม่ชัดเจน	๑	๔	๔
		-ไม่มีการทบทวนข้อปฏิบัติรองรับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นปัจจุบันอย่างน้อยปีละครั้ง	๑	๔	๔
		-ไม่มีกระบวนการประเมินผลติดตามการปฏิบัติให้เป็นไปตามนโยบายหรือข้อปฏิบัติที่หน่วยงานกำหนด	๔	๔	๑๖
<u>กระบวนงานการวางแผนงานด้านเทคโนโลยีสารสนเทศ</u>					
วัตถุประสงค์: เพื่อมีแนวทางการดำเนินงานด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ ประสิทธิผล	ไม่มีแนวทางการดำเนินงานด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ ประสิทธิผล	-ไม่มีการจัดทำแผนงานด้านเทคโนโลยีสารสนเทศ	๔	๔	๑๖
		-ขาดการสื่อสารแผนงานด้านเทคโนโลยีสารสนเทศ	๔	๔	๑๖
		-ไม่มีกระบวนการติดตามประเมินผลแผนงานด้านเทคโนโลยีสารสนเทศ	๔	๔	๑๖

กระบวนงาน/วัตถุประสงค์	ความเสี่ยง	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	รวม
<u>กระบวนงานด้านพัฒนาระบบสารสนเทศและการดูแลระบบสารสนเทศ</u>					
วัตถุประสงค์: ๑.เพื่อให้การพัฒนาระบบสารสนเทศสอดคล้องกับการใช้งานของผู้ใช้งาน	การพัฒนาระบบสารสนเทศไม่สอดคล้องกับการใช้งานของผู้ใช้งาน	-ผู้ใช้งานไม่มีส่วนร่วมในการพัฒนาระบบสารสนเทศ	๒	๔	๘
		-ไม่มีการรวบรวมความต้องการในการใช้งานระบบจากผู้ใช้งาน	๒	๔	๘
๒.เพื่อให้การพัฒนาระบบประสบความสำเร็จตามแผนงานที่กำหนด	การพัฒนาระบบไม่ประสบความสำเร็จตามแผนงานที่กำหนด	-ไม่มีแผนการดำเนินงานในการพัฒนาระบบ	๒	๒	๔
		-ไม่มีระบบการติดตามประเมินผลการดำเนินงานในการพัฒนาระบบ	๒	๒	๔
๓.เพื่อให้ระบบสารสนเทศมีความพร้อมใช้งานตลอด ๒๔ ชั่วโมง	ระบบสารสนเทศไม่พร้อมใช้งาน ตลอด ๒๔ ชั่วโมง	-มีการโจมตีจากผู้บุกรุกภายนอกทำให้ระบบสารสนเทศไม่พร้อมใช้งาน	๒	๕	๑๐
		-เครื่องแม่ข่ายล่มเนื่องจากไฟฟ้าดับ	๓	๕	๑๕
		-เครื่องแม่ข่ายล่มเนื่องจากซอฟแวร์ปฏิบัติการไม่มีลิขสิทธิ์ทำให้ไม่ได้ update โปรแกรมปฏิบัติการ	๓	๕	๑๕
		-เครื่องแม่ข่ายล่มเนื่องจากบุคลากรผู้ดูแลระบบดึงสายสัญญาณผิด	๒	๕	๑๐
		-เครื่องแม่ข่ายล่มเนื่องจากหนูกัดสายสัญญาณ	๒	๕	๑๐
		-เครื่องแม่ข่ายล่มเนื่องจากเกินขีดสมรรถนะของเครื่องที่จะรับไหว	๓	๕	๑๕
		-ระบบสารสนเทศมีการเขียนโปรแกรมที่มีการทำงานผิดพลาด(Error/Bug)	๒	๕	๑๐

กระบวนงาน/วัตถุประสงค์	ความเสี่ยง	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	รวม
		-ระบบสารสนเทศไม่พร้อมใช้งาน เนื่องจากอัคคีภัย อุทกภัย แผ่นดินไหว และจลาจล/ประท้วง	๑	๕	๕
<u>กระบวนการบริหารจัดการฐานข้อมูล</u>					
วัตถุประสงค์: ๑.เพื่อให้ข้อมูลมีสภาพความคงอยู่ไม่สูญหาย/ไม่เสียหาย/ไม่ถูกแก้ไขอย่างไม่ถูกต้องโดยผู้ไม่ได้รับอนุญาต	ข้อมูลไม่คงสภาพหรือสูญหาย/เสียหาย/ถูกแก้ไขอย่างไม่ถูกต้อง โดยผู้ไม่ได้รับอนุญาต	-ข้อมูลสูญหาย/เสียหายเนื่องจากบุคลากรนำทัมที่ติดไวรัสเข้ามาแพร่ระบาดในองค์กร	๓	๕	๑๕
		-ข้อมูลสูญหาย/เสียหายเนื่องจากระบบเครือข่ายล่มแล้วฮารดิสเสียหาย	๓	๕	๑๕
		-ข้อมูลสูญหาย/เสียหายเนื่องจากอัคคีภัย อุทกภัย แผ่นดินไหวและจลาจล/ประท้วง	๑	๕	๕
		-ข้อมูลถูกแก้ไขโดยผู้ไม่ได้รับอนุญาต เนื่องจากมีคนลักลอบเข้าUsername & Password ของผู้ดูแลระบบ	๑	๕	๕
		-ข้อมูลถูกแก้ไขโดยผู้ไม่ได้รับอนุญาต เนื่องจากมีการสวมรอยกรณีไม่มีการตัด Time Out ของสัญญาณอินเทอร์เน็ต	๑	๕	๕
		-ข้อมูลถูกแก้ไขโดยผู้ไม่ได้รับอนุญาต เนื่องจากไม่มีการเปลี่ยนรหัสบ่อยๆ	๒	๕	๑๐
		-ข้อมูลถูกแก้ไขโดยผู้ไม่ได้รับอนุญาต เนื่องจากไม่มีการทบทวนสิทธิการเข้าใช้งานอย่างน้อยปีละ๑ครั้ง	๑	๕	๕

กระบวนงาน/วัตถุประสงค์	ความเสี่ยง	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	รวม
๒.เพื่อข้อมูลที่มีคุณภาพ(ครบถ้วน ถูกต้อง ทันสมัย)	ข้อมูลไม่ได้คุณภาพ (ครบถ้วน ถูกต้อง ทันสมัย)	-ข้อมูลไม่ได้คุณภาพเนื่องจากไม่มีระบบการตรวจสอบคุณภาพข้อมูล	๑	๕	๕
		-ข้อมูลไม่ได้คุณภาพเนื่องจากไม่มีผู้รับผิดชอบดูแลและนำเข้าข้อมูล	๑	๕	๕
<u>กระบวนงานบริหารจัดการระบบเครือข่าย</u>					
วัตถุประสงค์: ระบบเครื่องข่ายมีความพร้อมใช้งานตลอด ๒๔ ชั่วโมง	ระบบเครือข่ายไม่พร้อมใช้งาน ตลอด ๒๔ ชั่วโมง	-ระบบเครือข่ายไม่พร้อมใช้งานเนื่องจากมีผู้บุกรุกโจมตีระบบเครือข่าย	๑	๕	๕
		-ไม่มีนโยบายและขั้นตอนการปฏิบัติงานอย่างเป็นระบบทำให้ผู้ปฏิบัติงานไม่ทราบว่าต้องปฏิบัติอย่างไรบ้าง	๑	๕	๕
		-ไม่มีการupdateโปรแกรมปฏิบัติการหรืออุปกรณ์ที่สำคัญในการป้องกันการโจมตีทางเครือข่าย	๒	๕	๑๐
		-บุคลากรผู้ดูแลเครือข่ายไม่มีความรู้ทักษะความชำนาญในการดูแลระบบเครือข่าย	๒	๕	๑๐
		-มีการใช้พื้นที่ของแบนด์วิชมากเกินความจำเป็น ทำให้ระบบเครือข่ายหนาแน่น	๒	๔	๘
<u>การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศขององค์กร</u>					
วัตถุประสงค์: เพื่อป้องกันทรัพย์สินด้านเทคโนโลยีสารสนเทศขององค์กรไม่ให้สูญหายหรือเสียหายหรือใช้งานอย่างเหมาะสม	ทรัพย์สินด้านเทคโนโลยีสารสนเทศขององค์กรสูญหายหรือเสียหาย	-ไม่มีระบบการยืม-คืนทรัพย์สินด้านเทคโนโลยีสารสนเทศ	๑	๔	๔

กระบวนงาน/วัตถุประสงค์	ความเสี่ยง	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	รวม
		-ไม่มีผู้รับผิดชอบในการดูแลทรัพย์สินด้านเทคโนโลยีสารสนเทศ	๑	๔	๔
		-ไม่มีทะเบียนคุมทรัพย์สินด้านเทคโนโลยีสารสนเทศถึงคุณลักษณะอุปกรณ์ที่สำคัญ	๑	๔	๔
		-ไม่มีการตรวจนับทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ๑ครั้ง	๑	๔	๔
		ไม่มีการขึ้นทะเบียนทรัพย์สินที่ได้รับการจัดสรรใหม่ทุกครั้ง	๑	๔	๔
		ไม่มีการกำหนดแนวทางปฏิบัติ/ข้อปฏิบัติเมื่อสิ้นสุดการจ้างหรือโอน-ย้าย ลาออก หรือเกษียณอายุ แล้วต้องคืนทรัพย์สิน	๑	๔	๔
	ใช้งานทรัพย์สินด้านเทคโนโลยีสารสนเทศไม่เหมาะสม	ไม่มีการจัดทำกฎ ระเบียบ หลักเกณฑ์การจัดสรรอุปกรณ์คอมพิวเตอร์ให้เหมาะสมกับภารกิจของบุคลากร (เพิ่มแนวทางการจัดสรรในข้อปฏิบัติ)	๑	๔	๔
		ไม่มีการจัดทำ/ประกาศใช้ คู่มือการใช้งานอุปกรณ์คอมพิวเตอร์ เครือข่ายและ softwareรวมทั้งขั้นตอนการดูแลรักษาเป็นรายอุปกรณ์	๒	๔	๘
		ไม่มีการตรวจสอบ บำรุงรักษาคอมพิวเตอร์ เครือข่ายและ softwareให้มีความพร้อมใช้งานอย่างน้อยปีละ๑ครั้ง	๑	๔	๔

การประเมินมาตรการควบคุม

ระบบบริหารความเสี่ยง หมายถึง ระบบการบริหารปัจจัยและควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่างๆ โดยลดมูลเหตุแต่ละโอกาสที่จะทำให้เกิดความเสียหายเพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถรับได้ ประเมินได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบโดยคำนึงถึงการบรรลุวัตถุประสงค์หรือเป้าหมายตามแผนปฏิบัติราชการประจำปีงบประมาณ ๒๕๕๑ ของหน่วยงานราชการเป็นสำคัญ

กิจกรรมควบคุม หมายถึง กระบวนการปฏิบัติที่ทุกคนในองค์กรร่วมกันพิจารณากำหนดขึ้นเพื่อสร้างความมั่นใจในระดับสมเหตุสมผลในการบรรลุวัตถุประสงค์ของหน่วยงาน

ทั้งนี้ได้กำหนดวิธีการตอบสนองความเสี่ยง แบ่งเป็น ๔ วิธี ดังนี้

๑. Take (การยอมรับ) คือ ยอมรับความเสี่ยงที่เกิดจากการปฏิบัติงาน (สามารถรับได้)
๒. Treat (การควบคุม) คือ การดำเนินการเพิ่มเติมเพื่อลดโอกาส หรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
๓. Terminate (การหลีกเลี่ยง) คือ การดำเนินการเพื่อยกเลิกหรือหลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง ทั้งนี้หากทำการใช้กลยุทธ์นี้อาจต้องทำการพิจารณาวัตถุประสงค์ว่าสามารถบรรลุได้หรือเพื่อทำการปรับเปลี่ยนต่อไป
๔. Transfer (การถ่ายโอน) คือ การแบ่งความเสี่ยงบางส่วนให้กับบุคคลหรือองค์กรอื่น

คณะทำงานบริหารความเสี่ยงระดับกรมได้ร่วมกันพิจารณามาตรการการบริหารความเสี่ยงของกรมสนับสนุนบริการสุขภาพทั่วทั้งองค์กร โดยตรวจสอบมาตรการการบริหารความเสี่ยงที่ใช้ในปัจจุบัน หรือที่เรียกว่า กระบวนการควบคุมภายใน สำหรับกลุ่มความเสี่ยงและปัจจัยเสี่ยงที่มีคะแนนความเสี่ยงอยู่ในระดับต่ำและปานกลาง (๑-๙ คะแนน) ทั้งนี้หลังจากได้มีกระบวนการควบคุมภายในไว้แล้วให้ถือว่าความเสี่ยงนี้เป็นความเสี่ยงที่สามารถยอมรับได้ ส่วนกลุ่มความเสี่ยงและปัจจัยเสี่ยงที่มีระดับคะแนนสูงและสูงมาก (๑๐ คะแนนขึ้นไป) ให้จัดทำมาตรการการบริหารความเสี่ยงและกำหนดไว้ในแผนบริหารความเสี่ยง ดังแสดงในตารางที่ ๓

การจัดทำแผนบริหารความเสี่ยง

แผนงานที่ ๑ แผนงานบริหารความเสี่ยงด้วยการกำหนดนโยบาย ระเบียบปฏิบัติ และวิธีปฏิบัติ คู่มือแนวทางการปฏิบัติงาน ของระบบเทคโนโลยีสารสนเทศ กรมสนับสนุนบริการสุขภาพ

แผนด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ ๒๕๖๔

ความเสี่ยง	ปัจจัยเสี่ยง	คะแนนความเสี่ยง	มาตรการการบริหารความเสี่ยง	วิธีการจัดการความเสี่ยง				ระยะเวลาที่ปฏิบัติ	ผู้รับผิดชอบ
				ยอมรับ	ควบคุม	หลีกเลี่ยง	ถ่ายโอน		
<u>กระบวนงานการวางแผนงานด้านเทคโนโลยีสารสนเทศ</u>									
๑.กรอบและทิศทางหรือแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไม่มีประสิทธิภาพ	-ไม่มีกระบวนการประเมินผลติดตามการปฏิบัติให้เป็นไปตามนโยบายหรือข้อปฏิบัติที่หน่วยงานกำหน	๑๖	มีการระบบการติดตามประเมินผลตามข้อปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศ		✓			กย.๖๔	ณัฐณิชา
๒.ไม่มีแนวทางการดำเนินงานด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ ประสิทธิผล	-ไม่มีการจัดทำแผนงานด้านเทคโนโลยีสารสนเทศ	๑๖	จัดทำแผนงานด้านเทคโนโลยีสารสนเทศ		✓			ตค.๖๓	ณัฐณิชา
	-ขาดการสื่อสารแผนงานด้านเทคโนโลยีสารสนเทศ	๑๖	แจ้งเวียนในกลุ่มและสื่อสารผ่านเว็ป และไลน์กลุ่ม		✓			ตค.๖๓	ณัฐณิชา

แผนด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ ๒๕๖๔

ความเสี่ยง	ปัจจัยเสี่ยง	คะแนนความเสี่ยง	มาตรการการบริหารความเสี่ยง	วิธีการจัดการความเสี่ยง				ระยะเวลาที่ปฏิบัติ	ผู้รับผิดชอบ
				ยอมรับ	ควบคุม	หลีกเลี่ยง	ถ่ายโอน		
๒.ไม่มีแนวทางการดำเนินงานด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ ประสิทธิผล	-ไม่มีกระบวนการติดตามประเมินผลแผนงานด้านเทคโนโลยีสารสนเทศ	๑๖	จัดระบบกระบวนการติดตามประเมินผลแผนงานด้านเทคโนโลยีสารสนเทศ		✓			กย.๖๔	ณัฐณิชา
<u>กระบวนงานด้านพัฒนาระบบสารสนเทศและการดูแลระบบสารสนเทศ</u>									
๓.ระบบสารสนเทศไม่พร้อมใช้งาน ตลอด ๒๔ ชั่วโมง	-เครื่องแม่ข่ายล่มเนื่องจากไฟฟ้าดับ	๑๕	สำรองข้อมูลทุกเดือน		✓			ตค.๖๓-กย.๖๔	ณัฐพล
	-เครื่องแม่ข่ายล่มเนื่องจากซอฟแวร์ปฏิบัติการไม่มีลิขสิทธิ์ทำให้ไม่ได้ update โปรแกรมปฏิบัติการ	๑๕	นำระบบงานสารสนเทศขึ้น server ตัวใหม่ที่ไม่ติดลิขสิทธิ์		✓			พย.๖๓	ณัฐณิชา

แผนด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ ๒๕๖๔

ความเสี่ยง	ปัจจัยเสี่ยง	คะแนนความเสี่ยง	มาตรการการบริหารความเสี่ยง	วิธีการจัดการความเสี่ยง				ระยะเวลาที่ปฏิบัติ	ผู้รับผิดชอบ
				ยอมรับ	ควบคุม	หลีกเลี่ยง	ถ่ายโอน		
๓.ระบบสารสนเทศไม่พร้อมใช้งาน ตลอด ๒๔ ชั่วโมง	-เครื่องแม่ข่ายล่ม เนื่องจากเกินขีดสมรรถนะของเครื่องที่จะรับไหว	๑๕	สำรองข้อมูลทุกเดือน		✓			ตค.๖๓-กย.๖๔	ณัฐพล
	-เครื่องแม่ข่ายล่ม เนื่องจากบุคลากรผู้ดูแลระบบดึงสายสัญญาณผิด	๑๐	สำรองข้อมูลทุกเดือน		✓			ตค.๖๓-กย.๖๔	ณัฐพล
	-เครื่องแม่ข่ายล่ม เนื่องจากหนูกัดสายสัญญาณ	๑๐	สำรองข้อมูลทุกเดือน		✓			ตค.๖๓-กย.๖๔	ณัฐพล
	-ระบบสารสนเทศมีการเขียนโปรแกรมที่มีการทำงานผิดพลาด (Error/Bug)	๑๐	สำรองข้อมูลทุกเดือน		✓			ตค.๖๓-กย.๖๔	ณัฐพล

แผนด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ ๒๕๖๔

ความเสี่ยง	ปัจจัยเสี่ยง	คะแนนความเสี่ยง	มาตรการการบริหารความเสี่ยง	วิธีการจัดการความเสี่ยง				ระยะเวลาที่ปฏิบัติ	ผู้รับผิดชอบ
				ยอมรับ	ควบคุม	หลีกเลี่ยง	ถ่ายโอน		
๓.ระบบสารสนเทศไม่พร้อมใช้งาน ตลอด ๒๔ ชั่วโมง	-มีการโจมตีจากผู้บุกรุกภายนอกทำให้ระบบสารสนเทศไม่พร้อมใช้งาน	๑๐	สำรองข้อมูลทุกเดือน		✓			ตค.๖๓-กย.๖๔	ณัฐพล
<u>กระบวนการบริหารจัดการฐานข้อมูล</u>									
ข้อมูลไม่คงสภาพหรือสูญหาย/เสียหาย/ถูกแก้ไขอย่างไม่ถูกต้อง โดยผู้ไม่ได้รับอนุญาต	-ข้อมูลสูญหาย/เสียหายเนื่องจากบุคลากรนำทัมที่ติดไวรัสเข้ามาแพร่ระบาดในองค์กร	๑๕	กำหนดมาตรการในการสแกนทรัมไดร์ก่อนนำมาใช้ในหน่วยงาน แจ้งเวียนสื่อสารให้ปฏิบัติอย่างเคร่งครัด		✓			ตค.๖๓	ณัฐณิชา
	-ข้อมูลสูญหาย/เสียหายเนื่องจากระบบเครือข่ายล่มแล้วฮารดิสเสียหาย	๑๕	สำรองข้อมูล		✓			ตค.๖๓-กย.๖๔	ณัฐพล

แผนด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ ๒๕๖๔

ความเสี่ยง	ปัจจัยเสี่ยง	คะแนนความเสี่ยง	มาตรการการบริหารความเสี่ยง	วิธีการจัดการความเสี่ยง				ระยะเวลาที่ปฏิบัติ	ผู้รับผิดชอบ
				ยอมรับ	ควบคุม	หลีกเลี่ยง	ถ่ายโอน		
	-ข้อมูลถูกแก้ไขโดยผู้ไม่ได้รับอนุญาตเนื่องจากไม่มีการเปลี่ยนรหัสบ่อยๆ	๑๐	กำหนดมาตรการอย่างเคร่งครัดให้มีการเปลี่ยนแปลงรหัสตามข้อปฏิบัติที่กำหนด		✓			ตค.๖๓-กย.๖๔	ณัฐพล
<u>กระบวนงานบริหารจัดการระบบเครือข่าย</u>									
ระบบเครือข่ายไม่พร้อมใช้งาน ตลอด ๒๔ ชั่วโมง	-ไม่มีการupdate โปรแกรมปฏิบัติการหรืออุปกรณ์ที่สำคัญในการป้องกันการโจมตีทางเครือข่าย	๑๐	สำรองข้อมูล		✓			ตค.๖๓-กย.๖๔	ณัฐพล
	-บุคลากรผู้ดูแลเครือข่ายไม่มีความรู้ทักษะความชำนาญในการดูแลระบบเครือข่าย	๑๐	เรียนรู้ด้วยตัวเองสำหรับผู้ดูแลเครือข่าย					ตค.๖๓-กย.๖๔	ณัฐพล