

การประเมินความเสี่ยง โอกาสและผลกระทบและการจัดลำดับความเสี่ยง

การจัดลำดับความเสี่ยง ได้แก่

1. ความมั่นคงปลอดภัยทางด้านไซเบอร์
2. การขาดแคลนบุคลากรทักษะสูงด้านไอที
3. ความสำเร็จของการนำระบบไอทีไปใช้งานจริง

ความเสี่ยง	ประเภทของความเสี่ยง (ด้าน)	ปัจจัยเสี่ยง	การวิเคราะห์ความเสี่ยง					
			การประเมินความเสี่ยง		การควบคุม/การแก้ปัญหาที่มีอยู่เดิม	รายละเอียด/ผลการประเมินการควบคุมเดิมที่มีอยู่ก่อนได้ผลหรือไม่		
			โอกาส	ผลกระทบ			ระดับความเสี่ยง	ลำดับความเสี่ยง
(1)	(2)	(3)	(4)		(5)	(6)		
1.ความมั่นคงปลอดภัยทางด้านไซเบอร์	ความเสี่ยงด้านทรัพยากร	1.ขาดเครื่องมือที่จะใช้ในการรับมือภัยคุกคามภายนอก	5	4	สูงมาก	1 -มีนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่าย	-มีการกำหนดนโยบายความมั่นคงปลอดภัยรูปแบบภัยคุกคามมีการปรับเปลี่ยนอยู่เสมอ	
		2. ทรัพยากรที่มีอยู่ในปัจจุบันอาจไม่สามารถป้องกันภัยไซเบอร์ได้อย่างเพียงพอ				- ทรัพยากรที่มีอยู่สามารถรับมือและแก้ปัญหาได้บางส่วน	- มีการอัปเดตและปรับปรุงระบบให้พร้อมรับมือภัยไซเบอร์ได้บางส่วน	
		3. การสำรองข้อมูล (Bacup) ยังไม่ดีพอ						
		4. บุคลากรขาดความรู้ความเชี่ยวชาญด้าน Cyber Security						
2.การขาดแคลนบุคลากรทักษะสูงด้านไอที	ความเสี่ยงด้านบุคลากร	1.บุคลากรไม่เพียงพอเนื่องจากมีการลาออกของบุคลากรที่พัฒนาระบบงานและยังขาดแคลนบุคลากร จากกรณีที่จำนวนระบบสารสนเทศเพิ่มขึ้นตามความต้องการของผู้ใช้งาน ส่งผลต่อประสิทธิภาพในการพัฒนาระบบงาน	5	3	สูงมาก	2	- เปิดรับสมัครบุคลากรด้านไอทีเพิ่มเติม	-มีการเปิดรับสมัครนักวิชาการคอมพิวเตอร์ แต่ยังไม่มีความสมัคร

ความเสี่ยง	ประเภท ของ ความเสี่ยง (ด้าน)	ปัจจัยเสี่ยง	การวิเคราะห์ความเสี่ยง			
(1)	(2)	(3)	(4)		(5)	(6)
		2. บุคลากรที่มีอยู่บางส่วนยังขาดทักษะ ความรู้และความเชี่ยวชาญเฉพาะทาง			-ส่งเสริมให้บุคลากรเข้ารับการฝึกอบรม หรือเพิ่มทักษะโดยการศึกษา ค้นคว้าหาความรู้ด้วยตนเอง เพื่อให้การปฏิบัติงานลุล่วงตามวัตถุประสงค์	- บุคลากรมีการเข้ารับการฝึกอบรมกับหน่วยงานภายนอก และสามารถแก้ปัญหาได้บางกรณี