การประเมินความเสี่ยง
ระบบเทคโนโลยีสารสนเทศ
สถาบันมาตรวิทยาแห่งชาติ

สารบัญ

โดย นายมาณพ ติณสิริสุข
ผู้ตรวจสอบภายใน

บทนำ

* นิยาม

ความเสี่ยง (Risk) หมายถึง เหตุการณ์ที่ไม่มีความแน่นอนที่อาจเกิดขึ้นได้ในอนาคต และอาจส่งผลกระทบเชิงลบ สร้างความสูญเสีย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือลดโอกาสที่จะบรรลุเป้าหมายที่สถาบันกำหนดไว้ ซึ่งครอบคลุมทั้งด้านการปฏิบัติงาน การสอบเทียบ งานด้านวิชาการ และการบริหารจัดการ

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ปัจจัยหรือสาเหตุที่ไม่พึงประสงค์อันส่งผลกระทบเชิงลบหรือลดโอกาสที่จะบรรลุเป้าหมายที่สถาบันกำหนดไว้

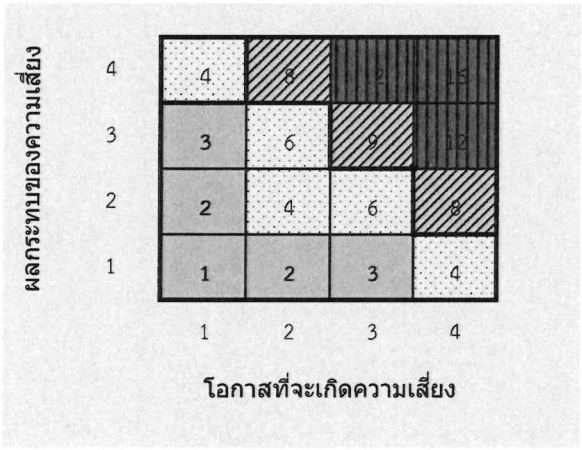
การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุเหตุการณ์เสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินระดับความเสี่ยง (Risk Evaluation) โดยประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) ของความเสี่ยงนั้นๆ ต่อสถาบันฯ หรือความคืบหน้าของแผน

โอกาส (Likelihood : L) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง

ผลกระทบ (Impact : I) หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง

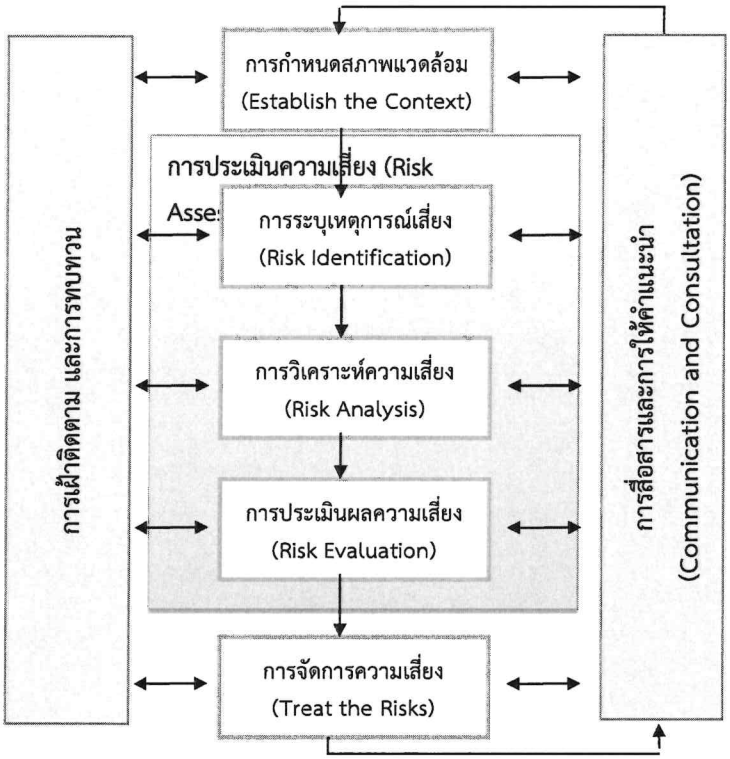
ระดับของความเสี่ยง (Degree of Risk : D) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาส และผลกระทบของแต่ละปัจจัยเสี่ยง มีค่าเป็นเชิงปริมาณ

* การจัดระดับความเสี่ยง (Degree of Risk)



1-3	เสี่ยงต่ำ	ระดับที่ยอมรับความเสี่ยงได้ ภายใต้วิธีการจัดการความเสี่ยงที่มีอยู่เดิม ไม่ต้องมีการจัดการเพิ่มเติม
4-6	เสี่ยงปานกลาง	ไม่สามารถยอมรับได้
8-9	เสี่ยงสูง	ระดับที่ไม่สามารถยอมรับความเสี่ยงได้ จำเป็นต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับได้ต่อไป
12-16	เสี่ยงสูงมาก	ระดับที่ไม่สามารถยอมรับความเสี่ยงได้ จำเป็นต้องเร่งจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับได้ทันที

แผนภูมิแสดงกระบวนการบริหารความเสี่ยง



ที่มา : ขนิษฐา ชัยรัตนาวรรณ. Standard Risk Management ISO 3100 and Thailand Education System

กระบวนการบริหารความเสี่ยงในส่วนของการควบคุมภายในของสถาบัน/ มีขั้นตอนการดำเนินงานและหลักเกณฑ์ในการวิเคราะห์อย่างเหมาะสม ประกอบด้วย 4 ขั้นตอน คือ

1) การระบุเหตุการณ์เสี่ยง (Risk Identification) : การค้นหาความเสี่ยง สำรวจเหตุการณ์ที่เป็นความเสี่ยง ปัจจัยหรือสาเหตุของความเสี่ยง รวมทั้งความเสียหายหรือผลกระทบที่อาจเกิดขึ้น ซึ่งสามารถหาได้จากคำร้องเรียนจากผู้ใช้บริการ การสัมภาษณ์ผู้ปฏิบัติงาน การออกแบบสอบถาม การศึกษาเอกสารและตำราวิชาการต่างๆ เป็นต้น

2) การวิเคราะห์ความเสี่ยง (Risk Analysis) : การพิจารณาถึงความถี่ ความรุนแรง และความสำคัญของเหตุการณ์แต่ละเหตุการณ์ว่ามีความถี่และความรุนแรงมากน้อยเพียงใด ซึ่งต้องอาศัยประสบการณ์ ข้อมูลในอดีต และความมีวิสัยทัศน์ เพื่อให้สามารถประเมินผลกระทบได้อย่างค่อนข้างแม่นยำ

3) การประเมินผลความเสี่ยง (Risk Evaluation) : การประเมินผลการจัดการความเสี่ยงจะบ่งบอกถึงความสามารถที่จะทำให้ความเสี่ยงที่ได้ดำเนินการบริหารความเสี่ยงนั้นลดลง โดยศึกษาถึงเหตุการณ์ที่เกิดขึ้นย้อนหลังเพื่อดูความสำเร็จของการบริหารความเสี่ยง

4) การจัดการความเสี่ยง (Risk Treatment) : การหาวิธีการเพื่อนำมาใช้ในการจัดการกับความเสี่ยงที่เกิดขึ้น โดยวิธีการที่นำมาใช้นั้นต้องสอดคล้องกับนโยบายและเป้าหมายของหน่วยงานหรือองค์กร

สถาบันมาตรวิทยาแห่งชาติ

แบบประเมินความเสี่ยง การตรวจสอบระบบเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ. 2568

กระบวนการปฏิบัติงาน/โครงการ/กิจกรรม : ประเมินผลการตรวจสอบภายในระบบเทคโนโลยีสารสนเทศ ที่มีความเสี่ยงเกิดขึ้น

วัตถุประสงค์ : เพื่อทำการประเมินความเสี่ยงที่เกิดขึ้นจากระบบเทคโนโลยีสารสนเทศเพื่อวิเคราะห์ ความเสี่ยง ปัจจัยเสี่ยง ผลกระทบ

ความเสี่ยง	ประเภทความเสี่ยง*	ปัจจัยเสี่ยง/สาเหตุของความเสี่ยง 	ความสูญเสีย/ผลกระทบที่อาจเกิดขึ้น 	เกณฑ์ประเมินความเสี่ยง				กิจกรรมควบคุม	การจัดการความเสี่ยง			หมายเหตุฝ่ายงาน/กลุ่มงานผู้รับผิดชอบ
				โอกาสที่จะเกิด (L)	ผลกระทบ (I)	คะแนนความเสี่ยง (L)X(I)	ระดับความเสี่ยง		วิธีการจัดการความเสี่ยง	สถานะดำเนินการ**	กำหนดเสร็จ/ผู้รับผิดชอบ	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)
1. การถูกโจมตีทางไซเบอร์	IT (3.6)	ขาดความพร้อมในการรับมือการโจมตีจากภายนอก	ทำให้ระบบสารสนเทศของสถาบันไม่สามารถดำเนินการได้ ส่งผลให้การทำงานของระบบงานทั้งหมดของสถาบันหยุดชะงัก ไม่สามารถให้การบริการแก่ลูกค้าได้	3	4	12	สูงมาก	1.จัดซื้ออุปกรณ์ป้องกันการโจมตีทางไซเบอร์ (Firewall) ให้ครอบคลุมทุกฟังก์ชัน 2.สร้างกระบวนการสำรองข้อมูลจากระบบงานต่าง ๆ ของสถาบัน	การลด/การควบคุมความเสี่ยง Treat		30-Sep-68	ฝ่ายนโยบายและยุทธศาสตร์/กลุ่มงานเทคโนโลยีสารสนเทศ
2. การไม่ปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	O (3)	พนักงานกลุ่มงานเทคโนโลยีสารสนเทศไม่ดำเนินงานตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	ถูกโจมตีทางไซเบอร์ ทำให้ระบบงานต่าง ๆ ของสถาบันหยุดชะงัก	3	4	12	สูงมาก	ตรวจสอบ/สอบทานการดำเนินงานของกลุ่มงานเทคโนโลยีสารสนเทศ เพื่อให้มีการปฏิบัติงานตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	การลด/การควบคุมความเสี่ยง Treat		30-Sep-68	กลุ่มงานเทคโนโลยีสารสนเทศ /ผู้ตรวจสอบภายใน

3.ความไม่สมบูรณ์ ไม่ถูกต้องของข้อมูลจากการประมวลผลของ Application ระบบงานต่าง ๆ ของสถาบัน	IT (3.6)	ความผิดพลาดในการประมวลผลของ Application ระบบงานต่าง ๆ ของสถาบัน	1.ข้อมูลที่ประมวลผลออกมาไม่ถูกต้อง อาทิ ข้อมูลทางการเงิน ข้อมูลสถิติ จะนำไปสู่ความผิดพลาดในการจัดการ การบริหารงาน ของสถาบันที่คลาดเคลื่อนตามไปด้วย 2.กรณี เป็นข้อมูลตัวเลขทางการเงิน อาจนำไปสู่การฟ้องร้องเป็นคดีความได้	2	4	8	สูง	ดำเนินการตรวจสอบ Application Control ระบบงานต่าง ๆ ของสถาบันตามแผนปฏิบัติงานตรวจสอบภายใน ของผู้ตรวจสอบภายใน เพื่อให้ความเชื่อมั่นในการทำงานของ Application ระบบงานต่าง ๆ ของสถาบัน	การลด/การควบคุมความเสี่ยง Treat		30-Sep-68	ผู้ตรวจสอบภายใน / กลุ่มงานเทคโนโลยีสารสนเทศ

สถาบันมาตรวิทยาแห่งชาติ

การประเมินความเสี่ยงหลังดำเนินการกิจกรรมจัดการความเสี่ยง ประจำปี 2568

กระบวนการปฏิบัติงาน/โครงการ/กิจกรรม : ความเสี่ยงที่เกิดขึ้น จากการประเมินผลการตรวจสอบระบบงานเทคโนโลยีสารสนเทศ ของสถาบัน

วัตถุประสงค์ : เพื่อประเมินผลวิเคราะห์กิจกรรมจัดการความเสี่ยงด้านระบบการควบคุมภายในของระบบงานเทคโนโลยีสารสนเทศ

ความเสี่ยง	ประเภทความเสี่ยง*	ระดับความเสี่ยงก่อนมีกิจกรรม/มาตรการจัดการ				การจัดการความเสี่ยง		สถานะดำเนินการ**	ระดับความเสี่ยงหลังกิจกรรม/มาตรการจัดการ (ณ สิงหาคม 2568)				คำชี้แจงผลการดำเนินงาน/ข้อเสนอแนะ
		โอกาสที่จะเกิด (L)	ผลกระทบ (I)	คะแนนความเสี่ยง (L)X(I)	ระดับความเสี่ยง	กิจกรรม	ประเมิน ณ วันที่ 18/8/68 ผู้รับผิดชอบ		โอกาสที่จะเกิด (L)	ผลกระทบ (I)	คะแนนความเสี่ยง (L)X(I)	ระดับความเสี่ยง	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
1. การถูกโจมตีทางไซเบอร์	IT (3.6)	3	4	12	สูงมาก	1.จัดซื้ออุปกรณ์ป้องกันการโจมตีทางไซเบอร์ (Firewall) ให้ครอบคลุมทุกฟังก์ชัน 2.สร้างกระบวนการสำรองข้อมูลจากระบบงานต่าง ๆ ของสถาบัน	ฝ่ายนโยบายและยุทธศาสตร์/กลุ่มงานเทคโนโลยีสารสนเทศ	◕	2	4	8	สูง	เนื่องจากกิจกรรมปิดความเสี่ยงอยู่ระหว่างดำเนินการระหว่างปีงบประมาณ เพื่อดำเนินการจัดซื้อ Firewall ให้ครบทุกฟังก์ชัน
2. การไม่ปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	O (3)	3	4	12	สูงมาก	ตรวจสอบ/สอบทานการดำเนินงานของกลุ่มงานเทคโนโลยีสารสนเทศ เพื่อให้มีการปฏิบัติงานตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	กลุ่มงานเทคโนโลยีสารสนเทศ /ผู้ตรวจสอบภายใน	●	1	3	3	ต่ำ	กิจกรรมปิดความเสี่ยงสามารถลดความเสี่ยงลงมาที่ระดับ ต่ำ เรียบร้อยแล้ว

3.ความไม่สมบูรณ์ ไม่ถูกต้องของข้อมูลจากการประมวลผลของ Application ระบบงานต่าง ๆ ของสถาบัน	IT (3.6)	2	4	8	สูง	ดำเนินการตรวจสอบ Application Control ระบบงานต่าง ๆ ของสถาบันตามแผนปฏิบัติงานตรวจสอบภายใน ของผู้ตรวจสอบภายในเพื่อให้ความเชื่อมั่นในการทำงานของ Application ระบบงานต่าง ๆ ของสถาบัน	ผู้ตรวจสอบภายใน / กลุ่มงานเทคโนโลยีสารสนเทศ		2	4	8	สูง	กิจกรรมปิดความเสี่ยงอยู่ระหว่างดำเนินการ ตามแผนปฏิบัติงานตรวจสอบประจำปี 2568 ของผู้ตรวจสอบภายใน

สถาบันมาตรวิทยาแห่งชาติ

การตรวจสอบระบบเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ พ.ศ.2568

กระบวนการปฏิบัติงาน/โครงการ/กิจกรรม : ความเสี่ยงที่เกิดขึ้น จากการประเมินผลการตรวจสอบระบบงานเทคโนโลยีสารสนเทศ ของสถาบัน

วัตถุประสงค์ : เพื่อติดตามประเมินผลวิเคราะห์ความเสี่ยงด้านระบบการควบคุมภายใน อันนำไปสู่การจัดลำดับความเสี่ยงของสถาบัน และนำไปสู่การกำหนดมาตรการ/กิจกรรมในการจัดการกับความเสี่ยงที่เกิดขึ้น อันจะกระทบต่อวัตถุประสงค์/เป้าหมายของสถาบัน

ความเสี่ยง	ประเภทความเสี่ยง*	ระดับความเสี่ยงประจำปีงบประมาณ (พ.ศ.2568) ก่อนมีกิจกรรม/มาตรการจัดการ				การจัดการความเสี่ยง		สถานะดำเนินการ**	ระดับความเสี่ยง (ณ กันยายน 2568)				คำชี้แจงผลการดำเนินงาน/ข้อเสนอแนะ
		โอกาสที่จะเกิด (L)	ผลกระทบ (I)	คะแนนความเสี่ยง (L)X(I)	ระดับความเสี่ยง	กิจกรรม	กำหนดเสร็จ 30/9/68 ผู้รับผิดชอบ		โอกาสที่จะเกิด (L)	ผลกระทบ (I)	คะแนนความเสี่ยง (L)X(I)	ระดับความเสี่ยง	
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
1. การถูกโจมตีทางไซเบอร์	IT (3.6)	3	4	12	สูงมาก	1.จัดซื้ออุปกรณ์ป้องกันการโจมตีทางไซเบอร์ (Firewall) ให้ครอบคลุมทุกฟังก์ชัน 2.สร้างกระบวนการสำรองข้อมูลจากระบบงานต่าง ๆ ของสถาบัน	ฝ่ายนโยบายและยุทธศาสตร์/กลุ่มงานเทคโนโลยีสารสนเทศ	◕	1	4	4	ปานกลาง	เนื่องจากกิจกรรมปิดความเสี่ยงได้ดำเนินการจัดซื้อ Firewall ครบทุกฟังก์ชันเรียบร้อยแล้ว ทำให้โอกาสที่เกิดลดลง แต่หากเกิดผลกระทบยังคงมีมากทำให้ควมเสี่ยงอยู่ในระดับปานกลาง
2. การไม่ปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	O (3)	3	4	12	สูงมาก	ตรวจสอบ/สอบทานการดำเนินงานของกลุ่มงานเทคโนโลยีสารสนเทศ เพื่อให้มีการปฏิบัติงานตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	กลุ่มงานเทคโนโลยีสารสนเทศ /ผู้ตรวจสอบภายใน	●	1	2	2	ต่ำ	กิจกรรมปิดความเสี่ยงสามารถลดความเสี่ยงลงมาที่ระดับ ต่ำ เรียบร้อยแล้ว

3.ความไม่สมบูรณ์ ไม่ถูกต้องของข้อมูลจากการประมวลผลของ Application ระบบงานต่าง ๆ ของสถาบัน	IT (3.6)	2	4	8	สูง	ดำเนินการตรวจสอบ Application Control ระบบงานต่าง ๆ ของสถาบันตามแผนปฏิบัติงานตรวจสอบภายใน ของผู้ตรวจสอบภายในเพื่อให้ความเชื่อมั่นในการทำงานของ Application ระบบงานต่าง ๆ ของสถาบัน	ผู้ตรวจสอบภายใน / กลุ่มงานเทคโนโลยีสารสนเทศ		2	3	6	ปานกลาง	กิจกรรมปิดความเสี่ยงสามารถลดความเสี่ยงลงมาที่ระดับปานกลางได้ แต่ยังมีความเสี่ยงอยู่จึงจำเป็นต้องเพิ่มความเข้างวดของมาตรการปิดความเสี่ยงขึ้นไป

หมายเหตุ ตารางรายงานผลการติดตาม สถาบันจะทำการวิเคราะห์ประเมินติดตามการบริหารจัดการความเสี่ยงด้านการตรวจสอบภายใน ณ 30 กันยายน หรือ ณ วันที่กำหนดแล้วเสร็จ หากประเด็นใดที่มีความเสี่ยงในระดับสูงขึ้นไป ได้มีมาตรการปรับปรุงแก้ไขอยู่ในระดับที่ยอมรับได้ ก็จะถูกพิจารณาปิดความเสี่ยงในประเด็นนั้นๆ ต่อไป

ตารางที่ 1 ประเภทความเสี่ยง

ประเภทความเสี่ยง (ตามเกณฑ์ ด้านต่างๆ)	สัญลักษณ์	รายละเอียด
1. ความเสี่ยงจากเหตุการณ์ภายนอก	E:External	ความเสี่ยงที่ไม่ได้เกิดประจำ แต่ส่งผลกระทบต่อสัมฤทธิ์ผลตามแผนกลยุทธ์ และไม่สามารถคาดการณ์การเกิดความสูญเสียได้อย่างแม่นยำ รวมไปถึงเหตุการณ์ที่เกิดจากปัจจัยภายนอกที่อยู่นอกเหนือการควบคุม เช่น ความเสี่ยงจากผลกระทบการเป็นประชาคมอาเซียนของประเทศไทย และความเสี่ยงที่กระทบต่อเป้าหมาย ความเสี่ยงทางการเมือง การโยกย้ายผู้บริหาร เป็นต้น
2.ความเสี่ยงเชิงนโยบายและยุทธศาสตร์	S:Strategic Risk	ความเสี่ยงที่เกี่ยวข้องกับนโยบายและแผนกลยุทธ์รวมไปถึงการตัดสินใจด้านบริหารที่ส่งผลต่อทิศทางของสถาบันในทางที่ไม่ส่งเสริมหรือเป็นอุปสรรคต่อการปฏิบัติงานตามแผนกลยุทธ์
2.1 ความเสี่ยงด้านยุทธศาสตร์	S:Strategic Risk	ความเสี่ยงที่เกี่ยวข้องกับวัตถุประสงค์เชิงกลยุทธ์ ซึ่งได้รับผลกระทบจากสภาพแวดล้อม นโยบายของผู้บริหาร เช่น การเมือง เศรษฐกิจ กฎหมาย ตลาด ภาพลักษณ์ ผู้นำ ชื่อเสียง ลูกค้า เป็นต้น
2.2 ความเสี่ยงด้านธรรมาภิบาล	G:Governance Risk	ความเสี่ยงที่เกี่ยวข้องกับเรื่องธรรมาภิบาลที่อาจเกิดขึ้นจากการดำเนินแผนงาน/โครงการ เพื่อให้เป็นไปตามหลักธรรมาภิบาล (Good Governance) โดยเฉพาะจรรยาบรรณของบุคลากร
3. ความเสี่ยงด้านปฏิบัติงาน	O:Operational Risk	ความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงานประจำวัน กระบวนการทำงานที่ช่วยให้สถาบันบรรลุเป้าประสงค์ เช่น ความเสี่ยงของกระบวนการสอบเทียบ การบริหารงานระบบงาน กระบวนการ เทคโนโลยี ระบบสารสนเทศและคน
3.1 ความเสี่ยงด้านปฏิบัติงานสนับสนุน/หรือด้านวิชาการ	O:Operational Risk	ความเสี่ยงเกี่ยวกับ การผิดพลาดในการปฏิบัติงาน จากวิธีการทำงาน เช่น ความเสี่ยงของกระบวนการบริหารจัดการด้านการปฏิบัติงาน การบริหารงานวิจัย ระบบประกันคุณภาพ

3.2 ความเสี่ยงด้านการเงิน	F:Financial Risk	ความเสี่ยงที่เกี่ยวกับการเงินและทรัพย์สินซึ่งมีผลทำให้สถาบันต้องมีรายได้ลดน้อยลงหรือค่าใช้จ่ายเพิ่มขึ้น หรือความเสียหายต่อทรัพย์สินของสถาบัน เช่น การผันผวนทางการเงินสภาพคล่องอัตราดอกเบี้ย ข้อมูลเอกสารหลักฐานทางการเงิน การรายงานทางการเงินบัญชีการเงินและงบประมาณ เป็นต้น
3.3 ความเสี่ยงกฎหมาย ระเบียบ ข้อบังคับ	C:Compliance Risk	ความเสี่ยงที่เกี่ยวข้องกับประเด็นข้อกฎหมาย ระเบียบการปกป้องคุ้มครองผู้มีส่วนได้เสีย การป้องกันข้อมูลรวมถึงประเด็นทางด้านกฎระเบียบอื่นๆ
3.4 ความเสี่ยงด้านความปลอดภัยจากอันตรายต่อชีวิตและทรัพย์สิน	H:Hazard Risk	ความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยของบุคลากรความปลอดภัยของอาคาร สถานที่ ระบบสาธารณูปโภครวมถึงการสูญเสียทางชีวิตและทรัพย์สินจากเหตุการณ์ไม่คาดคิด ภัยพิบัติทางธรรมชาติ และการก่อการร้าย เป็นต้น
3.5 ความเสี่ยงด้านทรัพยากรบุคคล	Human Resource Risk	ความเสี่ยงเกี่ยวกับ พนักงาน และผู้บริหารระดับสูง ขาดความรู้หรือประสบการณ์ หรือมีพฤติกรรมที่ไม่เหมาะสม ความเสี่ยงเกี่ยวกับการที่บุคลากรและระบบงาน ไม่สามารถดำเนินงาน หรือเหตุการณ์อื่นๆ ที่มีผลต่อการ
3.6 ความเสี่ยงด้านเทคโนโลยีและสารสนเทศ	IT:Information and Technology Risk	คือ ความเสี่ยงเกี่ยวกับความผิดพลาดของระบบเทคโนโลยีและสารสนเทศ ส่งผลให้ในการปฏิบัติงานเกิดความผิดพลาดหรือหยุดชะงัก

ตารางที่ 2 เกณฑ์การประเมินระดับความเสี่ยง

ระดับ ความเสี่ยง	ระดับคะแนน	ความหมาย
ระดับความเสี่ยงต่ำ	1-3	ระดับที่ยอมรับความเสี่ยงได้ ภายใต้วิธีการจัดการความเสี่ยงที่มีอยู่เดิม ไม่ต้องมีการจัดการเพิ่มเติม
ระดับความเสี่ยงปานกลาง	4-6	ระดับที่พอยอมรับความเสี่ยงได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ไม่สามารถยอมรับได้
ระดับความเสี่ยงสูง	8-9	ระดับที่ไม่สามารถยอมรับความเสี่ยงได้ จำเป็นต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับได้ต่อไป
ระดับความเสี่ยงสูงมาก	12-16	ระดับที่ไม่สามารถยอมรับความเสี่ยงได้ จำเป็นต้องเร่งจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่สามารถยอมรับได้ทันที

ตารางที่ 3 สถานะดำเนินการ (Degree of Acceptance)

สถานะดำเนินการ	สัญลักษ	ค่า	รายละเอียด
การวิเคราะห์ระดับความยอมรับหรือความพอใจในมาตรการที่ได้ดำเนินการอยู่แล้วเปรียบเทียบกับระดับความเสี่ยงและทรัพยากรที่มีอยู่ โดยใช้หลักเกณฑ์ ดังนี้	◔	1	ยังไม่มีมาตรการรองรับ (Unaccepted Risk)
	◑	2	มาตรการที่มีอยู่ไม่เพียงพอ จำเป็นต้องหามาตรการใหม่รองรับและ/หรือเปลี่ยนผู้รับผิดชอบ (Volatile Risk)
	◕	3	ทำมาตรการเดิม แต่ต้องเพิ่มความเข้มข้นในการดำเนินงาน (Mitigating Risk)
	●	4	มาตรการดีอยู่แล้วไม่ต้องทำอะไรเพิ่มเติม (Accepted Risk)

การบริหารความเสี่ยง (Risk Management) คือ การบริหารจัดการเพื่อควบคุมกิจกรรม รวมทั้งกระบวนการดำเนินงานต่างๆ เพื่อลดโอกาสและมูลเหตุที่สถาบันมาตรวิทยาแห่งชาติจะเกิดความเสียหายอันเป็นผลจากปัจจัยเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ ทั้งนี้เพื่อให้องค์กรสามารถบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น การจัดการความเสี่ยงมีหลายวิธี ดังนี้

การจัดการความเสี่ยง (Treat the Risks) เป็นการกำหนดนโยบาย (Policies) มาตรการและวิธีปฏิบัติ (Procedures) เพื่อตามตอบสนองต่อความเสี่ยง (Risk Response) ซึ่งสถาบันมาตรวิทยาแห่งชาติได้กำหนดแนวทางในการจัดการความเสี่ยงให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ โดยใช้วิธีดังต่อไปนี้

ตารางที่ 4 วิธีการจัดการความเสี่ยง

4T's Strategies	ศัพท์ที่นิยมใช้ (กรมบัญชีกลาง)	รายละเอียด
การยอมรับความเสี่ยง Take	Risk Acceptance (Accept)	การยอมรับให้มีความเสี่ยงปรากฏอยู่ เป็นความเสี่ยงที่หน่วยงานสามารถยอมรับได้เนื่องจากมีกิจกรรมการควบคุมภายในที่ดีอยู่แล้ว เนื่องจากการดำเนินการในการจัดการกับความเสี่ยง ไม่มีความคุ้มค่าเพียงพอ หรือทรัพยากรมีไม่เพียงพอต่อการดำเนินการในปีงบประมาณ
การลด/การควบคุมความเสี่ยง Treat	Risk Reduction (Control)	การลดโอกาสในการเกิดความเสี่ยง และ/ หรือความรุนแรงของผลกระทบที่เกิดขึ้นโดยหาวิธีการเพิ่มเติมเพื่อจัดการความเสี่ยง เช่น การออกแบบระบบการควบคุมภายใน ปรับปรุงแก้ไขกระบวนการ การตรวจติดตาม การจัดทำแผนฉุกเฉิน การจัดทำมาตรฐานความปลอดภัย การฝึกอบรมเพื่อพัฒนาทักษะ เป็นต้น
การกระจายความเสี่ยง Transfer	Risk Sharing (Transfer)	การกระจาย หรือโอนความเสี่ยงทั้งหมดหรือเพียงบางส่วนไปยังผู้อื่นที่มั่นใจว่าสามารถควบคุมความเสี่ยงนั้นได้เป็นอย่างดี ทั้งนี้เพื่อลดความสูญเสียที่อาจเกิดขึ้น เช่น การทำประกันภัย การจ้างบุคคลภายนอกดำเนินการแทน เป็นต้น
การหลีกเลี่ยงความเสี่ยง Terminate	Risk Avoidance (Avoid)	การหลีกเลี่ยงเหตุการณ์ที่ก่อให้เกิดความเสี่ยง เช่น การหยุดดำเนินกิจกรรมการเปลี่ยนแปลงวัตถุประสงค์หรือเปลี่ยนแปลงกิจกรรมที่เป็นความเสี่ยง การปรับเปลี่ยนรูปแบบการทำงาน การลดขนาดของงานหรือกิจกรรมที่จะดำเนินการลง หรือเลือกกิจกรรมอื่นที่สามารถยอมรับได้มากกว่า เป็นต้น

กิจกรรมการควบคุม (Control Activity) หมายถึง นโยบาย แนวทาง หรือขั้นตอนปฏิบัติต่างๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินงานบรรลุวัตถุประสงค์ที่กำหนดอย่างมีประสิทธิภาพ การควบคุมความเสี่ยงมีหลายวิธี ดังนี้

ตารางที่ 5 วิธีการควบคุม

วิธีการควบคุม	รายละเอียด
การควบคุมเพื่อป้องกัน (Preventive Control)	การควบคุมล่วงหน้าเพื่อป้องกันมิให้ความเสี่ยงและข้อผิดพลาดเกิดขึ้น เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อป้องกันไม่ให้เกิดความเสี่ยงและข้อผิดพลาด
การควบคุมเพื่อให้ตรวจพบ (Detective Control)	การควบคุมโดยการค้นหาข้อผิดพลาดที่เกิดขึ้น เช่น การทวนสอบ การวิเคราะห์ การตรวจนับ การรายงานข้อบกพร่อง เป็นต้น จัดเป็นวิธีการควบคุมที่กำหนด
การควบคุมโดยการชี้แนะ (Directive Control)	การควบคุมโดยการชี้แนะที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การให้รางวัลแก่ผู้มีผลงานดี เป็นต้น ซึ่งเป็นวิธีการ
การควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง (Corrective Control)	การควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือเพื่อหาวิธีการแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

ตารางที่ 6 เกณฑ์การประเมินระดับของโอกาสที่จะเกิดและผลกระทบของความเสี่ยงระบบการควบคุมภายใน

	1=ต่ำ	2=ปานกลาง	3=สูง	4=สูงมาก
<u>โอกาสที่จะเกิด (Likelihood : L)</u>				
โอกาสเกิดเชิงปริมาณ	5 ปีต่อครั้ง	2-3 ปีต่อครั้ง	1 ปีต่อครั้ง	1 เดือนต่อครั้ง หรือมากกว่า
	มีโอกาสเกิดน้อยกว่า 5%	มีโอกาสเกิด 5% - 10%	มีโอกาสเกิด 11% - 20%	มีโอกาสเกิดมากกว่า 20%
โอกาสเกิดเชิงคุณภาพ	ยากที่จะเกิดขึ้น	ไม่น่าจะเกิดขึ้นหรือเกิดได้น้อย	มีโอกาสเกิดแต่นานๆ ครั้ง	มีโอกาสเกิดเกือบทุกครั้ง
<u>ผลกระทบของความเสี่ยง (Impact : I)</u>				
· ด้านการเงิน	น้อยกว่า 1,000 บาท	1,001- 10,000 บาท	10,001- 30,000 บาท	เกิน 30,000 บาท
· ด้านเวลา	ทำให้เกิดความล่าช้าของโครงการไม่เกิน 1 เดือน	ทำให้เกิดความล่าช้าของโครงการมากกว่า 1-2 เดือน	ทำให้เกิดความล่าช้าของโครงการมากกว่า 2-6 เดือน	ทำให้เกิดความล่าช้าของโครงการมากกว่า 6 เดือน
· ด้านชื่อเสียงขององค์กร	ไม่มีการเผยแพร่ข่าว	มีการลงข่าวในสื่อต่างๆ เช่นหนังสือพิมพ์ในประเทศบางฉบับ 1 วัน	มีการลงข่าวในสื่อต่างๆ เช่นหนังสือพิมพ์ในประเทศหลายฉบับ 2-3วัน	มีการเผยแพร่ข่าวเป็นวงกว้างในประเทศและมีการเผยแพร่ข่าวในต่างประเทศ
· ด้านความปลอดภัย	เดือดร้อน รำคาญ	บาดเจ็บเล็กน้อยหรือไม่มีผลต่อสุขภาพ	บาดเจ็บต้องรักษา	บาดเจ็บสาหัส/อันตรายถึงชีวิต

· ด้านการปฏิบัติงาน	ทำให้การปฏิบัติงานเกิดความล่าช้าเล็กน้อย ไม่ส่งผลกระทบต่อการปฏิบัติงาน	ทำให้การปฏิบัติงานเกิดความล่าช้า สามารถกลับสู่สภาวะการปฏิบัติงานปกติได้ในเวลาไม่นาน	ทำให้การปฏิบัติงานเกิดความล่าช้ามาก ส่งผลให้การปฏิบัติงานไม่ต่อเนื่อง	ทำให้ไม่สามารถปฏิบัติงานต่อไปได้อย่างสิ้นเชิง
· ด้านกลยุทธ์/การดำเนินงานตามแผน	ดำเนินงานสำเร็จตามแผนได้มากกว่า 90%	ดำเนินงานสำเร็จตามแผน 76-90%	ดำเนินงานสำเร็จตามแผน 50-75%	ดำเนินงานสำเร็จตามแผนน้อยกว่า50%
· ด้านกฎระเบียบ/ข้อบังคับ	การปฏิบัติงานไม่เคยเกิดข้อพลาด	การปฏิบัติงานเกิดข้อผิดพลาดบ้างแต่ไม่รุนแรงหรือกระทบต่อความเสียหายกับพนักงานหรือสถาบัน สามารถปรับปรุงแก้ไขได้	การปฏิบัติงานเกิดข้อผิดพลาดมาก ส่งกระทบต่อความเสียหายกับพนักงานหรือสถาบัน/ผู้มีส่วนได้ส่วนเสีย และมีผลต่อการข้อกฎหมายส่งผลต่อการดำเนินคดี	การปฏิบัติงานเกิดข้อผิดพลาดอย่างรุนแรง พนักงาน/สถาบันถูกดำเนินคดี
· ด้านบุคลากร	สร้างความไม่สะดวกต่อการปฏิบัติงานนาน ๆ ครั้ง	สร้างความไม่สะดวกต่อการปฏิบัติงานบ่อยครั้ง	ถูกทำทัณฑ์บน คุณภาพชีวิตและบรรยากาศการปฏิบัติงานไม่เหมาะสม/ถูกลงโทษทางวินัย ตัดเงินเดือน ไม่ได้ขึ้นเงินเดือน	ถูกเลิกจ้างออกจากงานและอันตรายต่อร่างกายและชีวิตโดยตรง

· ด้านประสิทธิผล	ต่ำกว่าเป้าหมายไม่เกิน 5%	ต่ำกว่าเป้าหมาย 5-15%	ต่ำกว่าเป้าหมาย 16-20%	ต่ำกว่าเป้าหมาย 20%
· ด้านความพึงพอใจ	ระดับความพึงพอใจมากกว่า 80 % ขึ้นไป	ระดับความพึงพอใจมากกว่า 71-79%	ระดับความพึงพอใจมากกว่า 60-70%	ระดับความพึงพอใจมากกว่า 50 %
· ด้านผลการสอบเทียบ	มีผลด้านสอบเทียบ/ดำเนินการสอบเทียบเพิ่มขึ้นตามเป้าหมาย	มีผลการสอบเทียบมากกว่าปีที่ผ่านมา	มีผลงานการสอบเทียบเท่ากับปีที่ผ่านมา	มีผลงานสอบเทียบน้อยกว่าปีที่ผ่านมา
· ด้านระบบเทคโนโลยีสารสนเทศ	เกิดเหตุเล็กน้อยที่ไม่มีความสำคัญ	ระบบมีปัญหาแต่มีความสูญเสียไม่มาก	เกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่าง ๆ
· ด้านเป้าหมายขององค์กร	แทบไม่มีมีผลกระทบต่อเป้าหมายและชื่อเสียงขององค์กรเลย	มีผลกระทบต่อเป้าหมายบางอย่างและชื่อเสียงขององค์กรบ้าง	มีผลกระทบต่อเป้าหมายและชื่อเสียงขององค์กรในระดับสูง	มีผลกระทบต่อเป้าหมายและชื่อเสียงขององค์กรในระดับสูงมาก

หมายเหตุ ผลกระทบ (Impact) ของความเสี่ยง ที่ปรากฏตามตารางข้อมูลข้างต้น สถาบันได้พิจารณาและกำหนดไว้หลายด้าน ทั้งนี้เพื่อรองรับการประเมินความเสี่ยง กรอบและเกณฑ์ในการประเมินความเสี่ยงที่อาจเกิดขึ้นในอนาคต จากการดำเนินงานของสถาบัน