คู่มือบริหารความเสี่ยง สวทช.

ตามกรอบมาตรฐานบริหารความเสี่ยง ISO 31000:2009

เวอร์ชั่น 5.2 (2561)

NSTDA Risk Management Manual

ISO 31000:2009

Version 5.2 (2561)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

คู่มือบริหารความเสี่ยง สวทช.

ตามกรอบมาตรฐานบริหารความเสี่ยง ISO 31000:2009

เวอร์ชั่น 5.2 (2561)

NSTDA Risk Management Manual

ISO 31000:2009

Version 5.2 (2561)

ผ่านการเห็นชอบจาก กวทช. เมื่อวันที่ 22 ม.ค. 2561

Disclaimer: เอกสารนี้ใช้เป็นแนวทางบริหารความเสี่ยงภายใน สวทช. และมีวัตถุประสงค์เพื่อสร้างความเข้าใจในหลักการ และบริบทที่เกี่ยวข้องของ สวทช. เนื้อหาในคู่มือจะมีการพัฒนาและปรับปรุงให้สมบูรณ์และทันสมัยตามแนวทางการพัฒนาระบบบริหารความเสี่ยงของ สวทช. แบบวิวัฒนาการ (Evolutionary approach) เอกสารฉบับนี้เป็นการปรับปรุงเพิ่มเติมจากคู่มือบริหารความเสี่ยง version 5.1

คำนำ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) เป็นหน่วยงานในกำกับของกระทรวงวิทยาศาสตร์และเทคโนโลยี จัดตั้งขึ้นเมื่อปี พ.ศ. 2534 ตาม พ.ร.บ.พัฒนาวิทยาศาสตร์และเทคโนโลยี เพื่อนำวิทยาศาสตร์และเทคโนโลยีมาใช้ในการพัฒนาประเทศอย่างมีประสิทธิผลและประสิทธิภาพ โดยเป็นองค์กรที่มีความเป็นอิสระและความคล่องตัวสูง ไม่ผูกพันไว้กับกฎ ระเบียบ การปฏิบัติ และข้อบังคับปกติของราชการและรัฐวิสาหกิจ

ด้วยภารกิจของ สวทช. ที่ต้องดำเนินการนำวิทยาศาสตร์และเทคโนโลยีไปใช้ในการพัฒนาประเทศ ซึ่งมีความเสี่ยงสูงในการดำเนินงาน คณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (กวทช.) จึงเห็นความสำคัญของการนำระบบบริหารความเสี่ยงมาใช้เป็นเครื่องมือในการบริหารจัดการ เพราะระบบบริหารความเสี่ยงที่มีประสิทธิภาพและประสิทธิผลเป็นปัจจัยสำคัญที่จะลดความเสี่ยงอันจะส่งผลกระทบต่อการบรรลุวัตถุประสงค์การดำเนินงานของ สวทช.

ดังนั้นเพื่อให้การดำเนินงานบริหารความเสี่ยงของ สวทช. เป็นไปตามนโยบายที่ กวทช. กำหนด สวทช. ได้นำกระบวนการบริหารจัดการความเสี่ยงมาผนวกกับกระบวนการบริหารจัดการภายใน เพื่อขับเคลื่อนการบริหารความเสี่ยงให้เป็นส่วนหนึ่งของการบริหาร รวมถึงเพื่อให้สอดคล้องกับเกณฑ์การประเมินผลการดำเนินงานของกรมบัญชีกลาง คณะกรรมการจัดการความเสี่ยงของ สวทช. จึงได้ปรับปรุงคู่มือบริหารความเสี่ยงของ สวทช. เป็นฉบับที่ 5.2 (2561)

คู่มือบริหารความเสี่ยงฉบับนี้จัดทำขึ้นเพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจในการบริหารความเสี่ยงแก่ผู้บริหาร พนักงานและผู้เกี่ยวข้องของ สวทช.

คณะผู้จัดทำหวังเป็นอย่างยิ่งว่าคู่มือนี้จะเป็นส่วนหนึ่งในการสนับสนุนให้มีการนำระบบบริหารความเสี่ยงไปปฏิบัติจนเป็นส่วนหนึ่งของการดำเนินงานตามภารกิจปกติจนเกิดเป็นวัฒนธรรมองค์กรในที่สุด

คณะกรรมการจัดการความเสี่ยงของ สวทช.
วันที่ 17 ตุลาคม 2560

บทสรุปผู้บริหาร

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) กำหนดแนวทางการบริหารความเสี่ยงให้สอดคล้องกับกรอบการบริหารความเสี่ยง (Framework) ตามมาตรฐาน ISO 31000:2009 และเริ่มดำเนินการรอบแรกในปีงบประมาณ 2555 โดยมีขอบเขตการดำเนินงานเริ่มจากความเสี่ยงระดับองค์กร (ERM) ในปีที่ 1 และขยายไปสู่ระดับศูนย์แห่งชาติ/หน่วยงานหลักในปีที่ 2 โปรแกรมหลัก/โครงการที่สำคัญในปีที่ 3 โดยมีเป้าหมาย เพื่อให้มีการนำระบบบริหารความเสี่ยงไปปฏิบัติจนเป็นส่วนหนึ่งของการดำเนินงานตามภารกิจปกติจนเกิดเป็นวัฒนธรรมองค์กรในที่สุด

ในการดำเนินงานมีคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. ภายใต้คณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (กวทช.) รับผิดชอบในการเสนอแนะนโยบาย กำกับดูแลการบริหารความเสี่ยงทั่วทั้งองค์กร รวมถึงรายงานผลการบริหารจัดการความเสี่ยง ต่อ กวทช. อย่างต่อเนื่อง โดยในช่วงก่อตั้งระบบบริหารความเสี่ยงคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. ได้แต่งตั้งคณะทำงานพัฒนาระบบบริหารความเสี่ยงของ สวทช. ขึ้นเพื่อทำหน้าที่พัฒนานโยบาย แผนงาน และรายงานผลการบริหารจัดการความเสี่ยงของ สวทช. ต่อคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. อย่างสม่ำเสมอ นอกจากนี้ ได้มีการจัดตั้งคณะกรรมการจัดการความเสี่ยงของ สวทช. ซึ่งมีผู้อำนวยการ สวทช. เป็นประธาน รับผิดชอบในการกำหนดนโยบาย จัดการให้ความเสี่ยงต่างๆ อยู่ในวิสัย และขอบเขตที่พึงประสงค์ โดยจัดให้มีการประเมินและทบทวนความเสี่ยงด้วยความถี่ที่เหมาะสม ประมวลวิเคราะห์ความก้าวหน้าในการดำเนินงาน และจัดทำรายงานการติดตามประเมินผลการบริหารความเสี่ยง รวมทั้งส่งเสริม สื่อสาร พัฒนาความรู้ความเข้าใจในเรื่องการบริหารความเสี่ยงให้กับบุคลากรทุกระดับ

ในการประเมิน วิเคราะห์ และจัดการความเสี่ยง สวทช. ได้ศึกษาแนวทางการบริหารความเสี่ยงขององค์กรวิจัย และพัฒนาทางด้านวิทยาศาสตร์และเทคโนโลยีทั้งในประเทศและต่างประเทศ ที่มีลักษณะและพันธกิจใกล้เคียงกับ สวทช. พบว่า ในการบริหารจัดการความเสี่ยงจะต้องมี Framework ในการวิเคราะห์สาเหตุ ผลกระทบ เพื่อพิจารณาสิ่งที่พึงกระทำและจุดอ่อนที่ต้องดำเนินการแก้ไขเพื่อประเมินโอกาสที่จะเกิดความเสี่ยง และผลกระทบทั้งก่อน และหลังดำเนินการ และได้พบว่า CSIRO (Commonwealth Scientific and Industrial Research Organization) ซึ่งเป็นหนึ่งในองค์กรวิจัยที่ใหญ่ที่สุด ในประเทศออสเตรเลีย และเป็นองค์กรที่มีพันธกิจใกล้เคียงกับ สวทช. รวมถึง CSIRO ยังเป็นองค์กรสำคัญที่มีส่วนร่วมในการออกแบบมาตรฐาน ISO 31000:2009 ซึ่งได้ใช้แผนภาพแสดงความเชื่อมโยงองค์ประกอบสำคัญในการบริหารจัดการความเสี่ยงหรือ Bow Tie Diagram เป็นเครื่องมือในการจัดการความเสี่ยงขององค์กร ซึ่งแผนภาพนี้สามารถสรุปสาเหตุ ผลกระทบ และมาตรการในการควบคุม/ลดความเสี่ยงที่ใช้สื่อสารทำความเข้าใจได้ง่ายและมีประสิทธิภาพ

ระบบบริหารความเสี่ยงตามคู่มือนี้จัดทำขึ้นเพื่อประยุกต์ใช้ในการวิเคราะห์สาเหตุ ผลกระทบ พิจารณาทางเลือก และกำหนดแนวทางตอบสนองความเสี่ยง รวมถึงใช้ในการประชุม รายงานผล ปรึกษา สื่อสาร ร่วมกับคณะกรรมการจัดการความเสี่ยง และผู้มีส่วนได้ส่วนเสียอื่นๆ ด้วย

สารบัญ

หน้า

[ ] : เลขในวงเล็บใหญ่ [ ] คือ เลขที่ของข้อกำหนด ISO 31000 : 2009 ระบุเพื่อความสะดวกในการอ้างอิง

สารบัญแผนภาพ

หน้า

สารบัญตาราง

หน้า

บทนำ

สภาพการเปลี่ยนแปลงทางด้านวิทยาศาสตร์และเทคโนโลยี ด้านเศรษฐกิจ สังคม การเมืองตลอดจนนวัตกรรมที่เกิดขึ้นมากมาย ส่งผลให้องค์กรต่างๆ ไม่ว่าจะเป็นองค์กรของรัฐ เอกชน ต้องเผชิญกับความไม่แน่นอนกับการเปลี่ยนแปลงที่เกิดขึ้น ทำให้องค์กรส่วนใหญ่ต้องมีการปรับตัวรับมือกับการเปลี่ยนแปลงอยู่เสมอและตลอดเวลาเพื่อที่จะทำให้องค์กรดำเนินการตามวิสัยทัศน์ นโยบาย แผนยุทธศาสตร์ กลยุทธ์ ได้ตามวัตถุประสงค์ที่กำหนดไว้

การบริหารจัดการความเสี่ยงเป็นกระบวนการบริหารจัดการที่ทำให้องค์กรมีการวางแผนป้องกันและรองรับผลกระทบที่อาจเกิดขึ้นในอนาคต เพื่อลดความเสียหายที่อาจเกิดขึ้น คณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (กวทช.) ซึ่งมีหน้าที่กำกับดูแลการดำเนินงานของ สวทช. จึงเห็นความสำคัญของการนำระบบการบริหารจัดการความเสี่ยงมาใช้เป็นเครื่องมือในการบริหารจัดการ เพื่อให้ สวทช. สามารถดำเนินงานได้ตามวัตถุประสงค์ที่กำหนดไว้ และมีภูมิต้านทานต่อสภาพแวดล้อมทั้งภายใน และภายนอกที่อาจมีการเปลี่ยนแปลงได้อย่างเหมาะสม เพราะระบบการบริหารจัดการความเสี่ยงจะช่วยในเรื่องของการวิเคราะห์และคาดการณ์สิ่งที่จะเกิดขึ้นในอนาคต ทำให้สามารถจัดลำดับความสำคัญของการดำเนินงาน การวางแผนป้องกัน ตลอดจนหาแนวทางในการบริหารจัดการ เพื่อเพิ่มประสิทธิภาพกระบวนการตัดสินใจ ซึ่งส่งผลให้ผลลัพธ์ในการปฏิบัติงานดีขึ้น

1. นโยบายการบริหารจัดการความเสี่ยงของ สวทช.

โดยความเห็นชอบของ กวทช.ทาง สวทช. ได้กำหนดนโยบายการบริหารจัดการความเสี่ยง โดยสำนักงานฯ จะดำเนินการ ดังต่อไปนี้ (ตามประกาศสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยี เรื่อง นโยบายการบริหารจัดการความเสี่ยง ประกาศ ณ วันที่ 30 พฤศจิกายน พ.ศ. 2559)

1. การบริหารจัดการความเสี่ยงจะใช้กรอบแนวทางตามมาตรฐาน ISO 31000:2009 โดยการดำเนินงานบริหารความเสี่ยงจะต้องดำเนินการในทุกระดับชั้นตามโครงสร้างองค์กรของสำนักงานฯ และครอบคลุมความเสี่ยงที่อาจเกิดขึ้นทั้งจากปัจจัยภายในและภายนอกองค์กร เพื่อให้สำนักงานฯ สามารถดำเนินงานตามวัตถุประสงค์และอำนาจหน้าที่ได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล
2. กำหนดให้มีการจัดระบบและกระบวนการบริหารจัดการความเสี่ยงโดยมีคู่มือการดำเนินงานตัวอย่างในการวิเคราะห์ และการบริหารจัดการความเสี่ยง เพื่อเผยแพร่ให้ทุกหน่วยงานได้รับทราบและปฏิบัติในแนวทางเดียวกัน โดยให้นำระบบบริหารความเสี่ยงไปปฏิบัติเป็นส่วนหนึ่งของการดำเนินงานตามภารกิจจนเกิดเป็นวัฒนธรรมองค์กรในที่สุด

3. กำหนดให้มีคณะทำงานพัฒนาระบบบริหารความเสี่ยงของสำนักงานฯ เพื่อทำหน้าที่เป็นผู้พัฒนานโยบาย แผนงาน ระบบบริหารจัดการความเสี่ยง และรายงานความก้าวหน้าในการดำเนินการบริหารจัดการความเสี่ยงของสำนักงานฯ ต่อคณะอนุกรรมการบริหารความเสี่ยงของ สวทช.ของสำนักงานฯ รวมทั้งปฏิบัติงานอื่นใดตามที่คณะอนุกรรมการบริหารความเสี่ยงของ สวทช.ของสำนักงานฯ มอบหมาย โดยมีฝ่ายติดตามประเมินผลองค์กร สำนักงานกลาง ทำหน้าที่เป็นฝ่ายเลขานุการของคณะทำงานพัฒนาระบบบริหารความเสี่ยงของสำนักงานฯ และเป็นหน่วยงานประสานงานกลางในเรื่องการบริหารจัดการความเสี่ยงของสำนักงานฯ
4. กำหนดให้มีคณะกรรมการจัดการความเสี่ยงของสำนักงานฯ เพื่อทำหน้าที่เป็นผู้ดูแลรับผิดชอบจัดการความเสี่ยง การป้องกัน และการแก้ไขข้อขัดแย้งที่อาจเกิดจากความเสี่ยงเหล่านั้น รวมถึงจัดให้มีการประเมินและทบทวนความเสี่ยงด้วยความถี่ที่เหมาะสมตามความจำเป็น โดยมีฝ่ายติดตามประเมินผลองค์กร สำนักงานกลาง ทำหน้าที่เป็นฝ่ายเลขานุการของคณะกรรมการจัดการความเสี่ยงของสำนักงานฯ และเป็นหน่วยงานประสานงานกลางในเรื่องการบริหารจัดการความเสี่ยงของสำนักงานฯ
5. คณะกรรมการจัดการความเสี่ยงของสำนักงานฯ จะประมวลวิเคราะห์ความก้าวหน้าในการดำเนินงานของคณะทำงานพัฒนาระบบบริหารความเสี่ยงของสำนักงานฯ และจัดทำรายงานการติดตามประเมินผลการบริหารจัดการความเสี่ยงนำเสนอต่อคณะอนุกรรมการบริหารความเสี่ยงของสำนักงานฯ และคณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติตามลำดับ ในทุก 6 เดือน เพื่อทราบ และ/หรือพิจารณาทบทวนและปรับปรุงแผนการบริหารจัดการความเสี่ยงของสำนักงานฯ ให้มีความเหมาะสม
6. กำหนดให้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการความเสี่ยงอย่างเหมาะสม เพื่อให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ
7. ดำเนินการจัดสรรทรัพยากรอย่างเพียงพอเพื่อบริหารจัดการความเสี่ยงให้มีประสิทธิภาพพร้อมทั้งส่งเสริม สื่อสาร และพัฒนาความรู้และความเข้าใจในเรื่องการบริหารจัดการความเสี่ยงให้แก่บุคลากรในทุกระดับ รวมทั้งการเสริมสร้างความตระหนักถึงประโยชน์และความสำคัญในการบริหารจัดการความเสี่ยงขององค์กร (เอกสารประกาศสำนักงานฯ เรื่องนโยบายบริหารจัดการความเสี่ยงของ สวทช. ปรากฏในภาคผนวก ก)

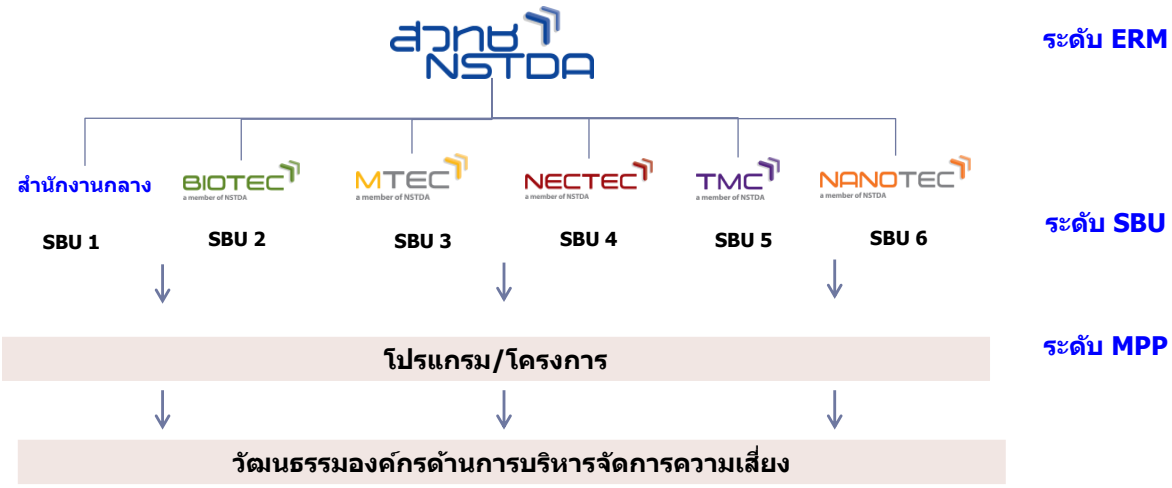
2. แนวทางการบริหารจัดการความเสี่ยงของ สวทช.

สวทช. ได้ศึกษาแนวทางการพัฒนา และจัดตั้งระบบบริหารความเสี่ยงขององค์กรวิจัยและพัฒนาทางด้านวิทยาศาสตร์และเทคโนโลยี ทั้งในประเทศและต่างประเทศที่มีลักษณะและพันธกิจใกล้เคียงกับ สวทช. รวมทั้งศึกษามาตรฐานระดับสากลที่ใช้ในการบริหารจัดการความเสี่ยง ผลจากการศึกษา พบว่า มาตรฐาน ISO 31000:2009 ซึ่งเป็นมาตรฐานการบริหารจัดการความเสี่ยงสากลระดับนานาชาติ (International Organization of Standard: ISO) มีชื่อเต็มว่า Risk Management-Guidelines on Principles and Implementation of Risk Management เป็นระบบบริหารความเสี่ยงองค์กรที่มีแนวปฏิบัติในการบริหารจัดการความเสี่ยงที่มีหลักการ และกรอบแนวทางการดำเนินงานที่ชัดเจน และหลายองค์กรได้ยึดถือเป็นกรอบในการดำเนินงานด้านการบริหารจัดการความเสี่ยงในองค์กรทาง สวทช. จึงได้ใช้มาตรฐาน ISO 31000:2009 เป็นกรอบในการดำเนินงานด้านบริหารความเสี่ยงทั่วทั้งองค์กรของ สวทช.

ในการประเมิน วิเคราะห์ และจัดการความเสี่ยง สวทช. ได้ศึกษาแนวทางการบริหารจัดการความเสี่ยงขององค์กรวิจัย และพัฒนาทางด้านวิทยาศาสตร์และเทคโนโลยีทั้งในประเทศและต่างประเทศที่มีลักษณะและพันธกิจใกล้เคียงกับ สวทช. พบว่า ในการบริหารจัดการความเสี่ยงจะต้องมี Framework ในการวิเคราะห์สาเหตุ ผลกระทบ เพื่อพิจารณาสิ่งที่พึงกระทำและจุดอ่อนที่ต้องดำเนินการแก้ไขเพื่อประเมินโอกาสที่จะเกิดความเสี่ยง และผลกระทบทั้งก่อน และหลังดำเนินการ และได้พบว่า CSIRO (Commonwealth Scientific and Industrial Research Organization) ซึ่งเป็นหนึ่งในองค์กรวิจัยที่ใหญ่ที่สุดในประเทศออสเตรเลีย และเป็นองค์กรที่มีพันธกิจใกล้เคียงกับ สวทช. ได้ใช้แผนภาพแสดงความเชื่อมโยงองค์ประกอบสำคัญในการบริหารจัดการความเสี่ยงที่เรียกว่า Bow Tie Diagram เป็นเครื่องมือในการจัดการความเสี่ยงขององค์กร ซึ่งแผนภาพนี้สามารถสรุปสาเหตุ ผลกระทบ และมาตรการในการควบคุม/ลดความเสี่ยงที่ใช้สื่อสารทำความเข้าใจได้ง่ายและมีประสิทธิภาพ สวทช. จึงได้นำ Bow Tie Diagram มาปรับปรุงดัดแปลงใช้เป็นเครื่องมือในการวิเคราะห์และบริหารจัดการความเสี่ยงของ สวทช.

2.1 โครงสร้างองค์กรและขอบเขตการดำเนินงานด้านการบริหารความเสี่ยงของ สวทช.

สวทช. บริหารความเสี่ยง โดยแบ่งแผนและแนวทางการบริหารเป็น 4 ระดับ ประกอบด้วย (1) ระดับองค์กร (Enterprise Risk Management) (2) ระดับศูนย์แห่งชาติ/หน่วยงานหลัก (Strategic Business Units) (3) ระดับโปรแกรมหลัก/โครงการ (Major Programs and Projects) และ (4) วัฒนธรรมองค์กรด้านการบริหารจัดการความเสี่ยงโดย 3 ระดับแรกดำเนินการตามกรอบกระบวนการบริหารจัดการความเสี่ยงของ สวทช. แต่จะมีขอบเขตการดำเนินงานที่แตกต่างกันตามบทบาทหน้าที่ โดยมีรายละเอียด ดังนี้



แผนภาพที่ 2.1 ขอบเขตการดำเนินงานบริหารความเสี่ยงของ สวทช. 4 ระดับ

ระดับองค์กร (Enterprise Risk Management: ERM) การบริหารจัดการความเสี่ยงในระดับนี้เป็นการบริหารความเสี่ยงขององค์กร (ดำเนินงานทั่วทั้งองค์กร) โดยมีคณะกรรมการจัดการความเสี่ยงของ สวทช. ซึ่งผู้อำนวยการ สวทช. เป็นประธาน และมีรองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (รอง ผพว.) ผู้อำนวยการศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ (ผศว.) ผู้อำนวยการศูนย์พันธุวิศวกรรมและเทคโนโลยีชีวภาพแห่งชาติ (ผศช.) ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (ผศอ.) ผู้อำนวยการศูนย์นาโนเทคโนโลยีแห่งชาติ (ผศน.) และผู้อำนวยการศูนย์บริหารจัดการเทคโนโลยี (ผศจ.) เป็นกรรมการ

โดยคณะกรรมการฯ ชุดนี้ทำหน้าที่เป็นผู้ดูแลรับผิดชอบบริหารจัดการความเสี่ยงระดับองค์กร จัดการให้ความเสี่ยงต่างๆ อยู่ในวิสัยและขอบเขตที่พึงประสงค์ โดยจัดให้มีการทบทวนและประเมินความเสี่ยงด้วยความถี่ที่เหมาะสม ประมวลวิเคราะห์ความก้าวหน้าในการดำเนินงานและจัดทำรายงานการติดตามประเมินผลการบริหารจัดการความเสี่ยงของระดับองค์กร ระดับศูนย์แห่งชาติ/หน่วยงานหลัก และระดับโปรแกรมหลัก/โครงการ รวมทั้งส่งเสริม สื่อสาร พัฒนาความรู้ความเข้าใจในเรื่องการบริหารจัดการความเสี่ยงให้กับบุคลากรทุกระดับ

ระดับศูนย์แห่งชาติ/หน่วยงานหลัก (Strategic Business Unit: SBU) การบริหารจัดการความเสี่ยงในระดับนี้เป็นบทบาทของศูนย์แห่งชาติ/หน่วยงานหลักซึ่งตามโครงสร้างการบริหารงานของ สวทช. ประกอบด้วย สำนักงานกลาง 1 หน่วย และศูนย์ 5 ศูนย์แห่งชาติ ประกอบด้วย (1) SBU 1 สำนักงานกลาง (2) SBU 2 ศูนย์พันธุวิศวกรรมและเทคโนโลยีชีวภาพแห่งชาติ (ศช.) (3) SBU 3 ศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ (ศว.) (4) SBU 4 ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (ศอ.) (5) SBU 5 ศูนย์บริหารจัดการเทคโนโลยี (ศจ.) (6) SBU 6 ศูนย์นาโนเทคโนโลยีแห่งชาติ (ศน.)

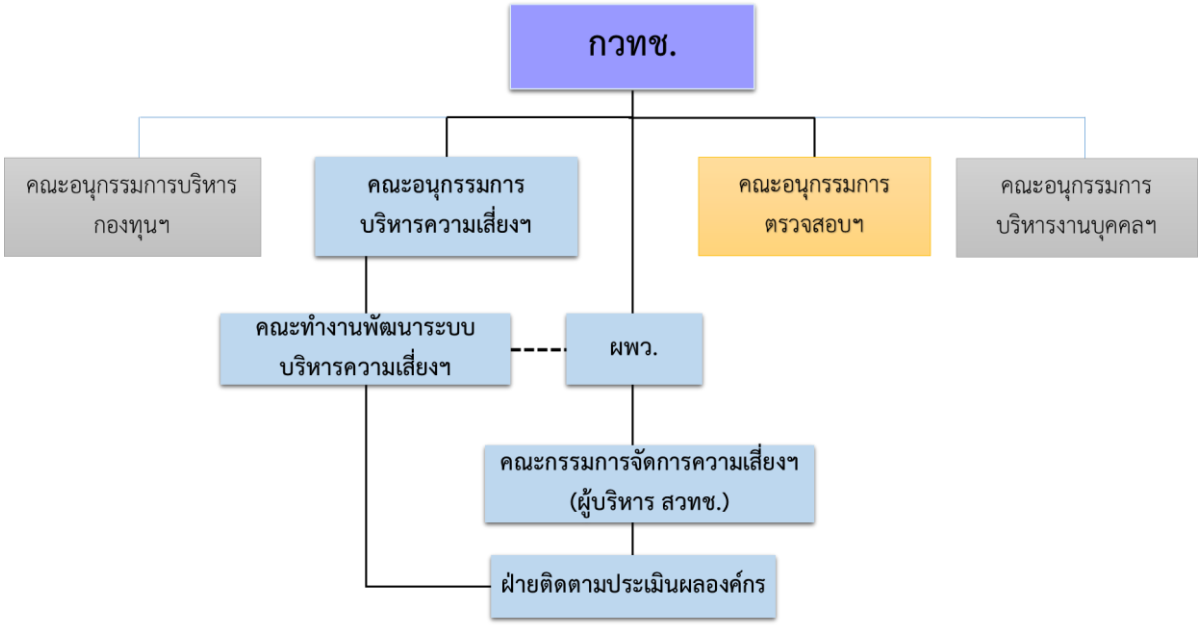
โดยแต่ละ SBU จะมีการแต่งตั้งคณะกรรมการจัดการความเสี่ยงของ SBU มีรองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (รอง ผพว.) และผู้อำนวยการศูนย์ฯ เป็นประธาน โดยคณะกรรมการฯ ทำหน้าที่เป็นผู้ดูแลรับผิดชอบบริหารจัดการความเสี่ยง ระดับ SBU ตามกรอบกระบวนการบริหารจัดการความเสี่ยงของ สวทช.

ระดับโปรแกรมหลัก/โครงการ (Major Program and Project: MPP) การบริหารจัดการความเสี่ยงในระดับ MPP จะดำเนินการเฉพาะโครงการขนาดใหญ่ที่มีขอบเขตการดำเนินงาน วัตถุประสงค์ งบประมาณ บทบาทหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องอย่างชัดเจน หรือในการดำเนินงานบริหารความเสี่ยงจะต้องสามารถดำเนินการได้ตามขั้นตอนการบริหารความเสี่ยงตั้งแต่ การกำหนดรายการความเสี่ยง (Risk Identification) กำหนดผู้รับผิดชอบความเสี่ยง (Risk Owner) วิเคราะห์ความเสี่ยงด้วย Bow Tie Diagram ประเมินระดับความเสี่ยงและจัดทำแผนบริหารจัดการความเสี่ยง โดยการกำกับดูแลการบริหารจัดการความเสี่ยงระดับนี้ ดำเนินการโดยคณะกรรมการจัดการความเสี่ยงของระดับ SBU เช่นเดียวกับระดับศูนย์แห่งชาติ/หน่วยงานหลัก คณะกรรมการฯ ชุดนี้จะทำหน้าที่คัดเลือกและกำหนดโปรแกรม/โครงการหลักมาดำเนินการทบทวน ประเมินและวิเคราะห์บริหารจัดการความเสี่ยงตามกรอบกระบวนการบริหารจัดการความเสี่ยงของ สวทช.

ระดับวัฒนธรรมองค์กรด้านการบริหารจัดการความเสี่ยง (Risk Cuture) สวทช. กำหนดแผนการสร้างวัฒนธรรมองค์กรด้านการบริหารจัดการความเสี่ยง โดยมีวัตถุประสงค์เพื่อบูรณาการเรื่องการบริหารจัดการความเสี่ยงเข้ากับกระบวนการหลัก รวมถึงเพื่อดำเนินการให้ทุกส่วนในองค์กรตระหนักและนำหลักการบริหารความเสี่ยงไปใช้ในการดำเนินงานตามพันธกิจของ สวทช. จนเกิดเป็นวัฒนธรรมองค์กรในที่สุด โดยมีคณะกรรมการจัดการความเสี่ยงของ สวทช. ทำหน้าที่เป็นผู้ดูแลรับผิดชอบมีแนวทางการดำเนินงานประกอบด้วย (1) การวางแผนกลยุทธ์ที่ครอบคลุมการบริหารจัดการความเสี่ยง (Risk and Strategic Plan) (2) การสอบทานผลการดำเนินงานตามแนวทางการบริหารจัดการความเสี่ยง (Risk and Internal Audit) และ (3) การสื่อสารแนวทางการบริหารจัดการความเสี่ยง (Risk Communication) รายละเอียดตามหัวข้อ 3.2

2.2 โครงสร้างการบริหารจัดการความเสี่ยงของ สวทช.

กวทช. ได้กำหนดบทบาทหน้าที่และความรับผิดชอบของคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. คณะกรรมการจัดการความเสี่ยงของ สวทช. และคณะทำงานพัฒนาระบบบริหารความเสี่ยงต่างๆ ในการกำกับดูแลการบริหารจัดการความเสี่ยงของ สวทช. ไว้ดังแผนภาพที่ 2.2



แผนภาพที่ 2.2 โครงสร้างการกำกับดูแลการบริหารจัดการความเสี่ยงของ สวทช.

โดยกำหนดขอบเขตและหน้าที่รับผิดชอบของคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. คณะกรรมการจัดการความเสี่ยงของ สวทช. และคณะทำงานพัฒนาระบบบริหารความเสี่ยงของ สวทช. ไว้ ดังนี้

คณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (กวทช.) มีบทบาทในการกำหนดนโยบายบริหารความเสี่ยง และกำกับทิศทางของ สวทช. ผ่านการดำเนินงานของคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. เพื่อให้มั่นใจว่ามีการดำเนินการอย่างเหมาะสม เพื่อจัดการกับความเสี่ยงที่กำหนดในแผนบริหารความเสี่ยง

คณะอนุกรรมการบริหารความเสี่ยงของ สวทช. มีหน้าที่เสนอแนะนโยบายการบริหารความเสี่ยง พร้อมทั้งกำกับดูแลการบริหารความเสี่ยงทั่วทั้งองค์กรของ สวทช. ตามนโยบาย และรายงานผลการบริหารความเสี่ยง สวทช. ต่อ กวทช. ทั้งนี้สามารถแต่งตั้งคณะทำงานเพื่อปฏิบัติงานได้ตามความเหมาะสมและสามารถปฏิบัติงานอื่นตาม กวทช. มอบหมาย รายละเอียดตามภาคผนวก ข

คณะอนุกรรมการตรวจสอบและประเมินผลการดำเนินงานของ สวทช. มีหน้าที่สอบทานการประเมินการบริหารความเสี่ยง ด้วยการสอบทานกระบวนการบริหารความเสี่ยงตามมาตรฐาน ISO31000:2009, สอบทานและประเมินผลการบริหารความเสี่ยงที่สำคัญ (Key Risk) สอบทานการดำเนินการตามกระบวนการควบคุมเพื่อลดระดับความเสี่ยงที่กำหนดไว้ และให้คำปรึกษาและข้อแนะนำเพื่อพัฒนาระบบบริหารความเสี่ยง

คณะทำงานพัฒนาระบบบริหารความเสี่ยงของ สวทช. มีหน้าที่พัฒนานโยบาย แผนงาน ระบบบริหารจัดการความเสี่ยง และรายงานความก้าวหน้าในการดำเนินการบริหารจัดการความเสี่ยงของ สวทช. ต่อคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. รวมทั้งปฏิบัติงานอื่นตามที่คณะอนุกรรมการบริหารความ

เสี่ยงของ สวทช. มอบหมาย แต่งตั้งขึ้นโดยคำสั่งคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. ที่ 1/2559 รายละเอียดตามภาคผนวก ง

คณะกรรมการจัดการความเสี่ยงของ สวทช. มีทำหน้าที่จัดการให้รายการความเสี่ยงต่างๆ อยู่ในวิสัยและขอบเขตที่พึงประสงค์ โดยจัดให้มีการประเมิน ทบทวนความเสี่ยงด้วยความถี่ที่เหมาะสมและตามความจำเป็น ประมวลวิเคราะห์ความก้าวหน้าในการดำเนินงาน และจัดทำรายงานการติดตามประเมินผลการบริหารจัดการความเสี่ยง นำเสนอต่อคณะอนุกรรมการบริหารความเสี่ยงของ สวทช.

คณะกรรมการจัดการความเสี่ยงของ สวทช. ประกอบด้วย ผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (ผพว.) รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (รองผพว.) ผู้อำนวยการศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ (ผศว.) ผู้อำนวยการศูนย์พันธุวิศวกรรมและเทคโนโลยีชีวภาพแห่งชาติ (ผศช.) ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (ผศอ.) ผู้อำนวยการศูนย์นาโนเทคโนโลยีแห่งชาติ (ผศน.) และผู้อำนวยการศูนย์บริหารจัดการเทคโนโลยี (ผศจ.) โดยมีฝ่ายติดตามประเมินผลองค์กร สำนักงานกลาง ทำหน้าที่เลขานุการ รายละเอียดตามภาคผนวก ค

ฝ่ายติดตามประเมินผลองค์กร สำนักงานกลาง มีหน้าที่เป็นฝ่ายเลขานุการของคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. คณะกรรมการจัดการความเสี่ยงของ สวทช. คณะทำงานพัฒนาระบบบริหารความเสี่ยงของ สวทช. และเป็นหน่วยประสานงานกลางในเรื่องการบริหารจัดการความเสี่ยงของ สวทช. ตามนโยบาย สวทช. รายละเอียดตามภาคผนวก ก

2.3 การบูรณาการงานบริหารความเสี่ยงเข้ากับกระบวนการหลักของ สวทช.

กวทช. คาดหวังให้ สวทช. บูรณาการเรื่องการบริหารจัดการความเสี่ยงเข้ากับกระบวนการหลักซึ่ง สวทช. ได้นำกระบวนการบริหารจัดการความเสี่ยงมาผนวกเข้ากับกระบวนการวางแผนกลยุทธ์ โดยการดำเนินการบริหารความเสี่ยงจะต้องสอดคล้องกับนโยบาย กลยุทธ์ เป้าหมาย แผนงาน โครงการต่างๆ รวมทั้งต้องสอดคล้องกับมาตรฐาน ข้อกำหนดกฎหมาย ระเบียบ ประกาศ หลักเกณฑ์ และแนวทางปฏิบัติที่ดี ซึ่งต้องทบทวนกลยุทธ์การบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้ง ตามแผนประจำปี หรือทบทวนทันทีที่มีเหตุการณ์เปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้ทราบถึงปัญหา อุปสรรค ที่ส่งผลต่อการบรรลุเป้าหมายของ สวทช. ทั้งนี้เพื่อให้การดำเนินงานบริหารความเสี่ยงสามารถดำเนินงานควบคู่ไปกับกระบวนการหลักได้อย่างมีประสิทธิภาพ

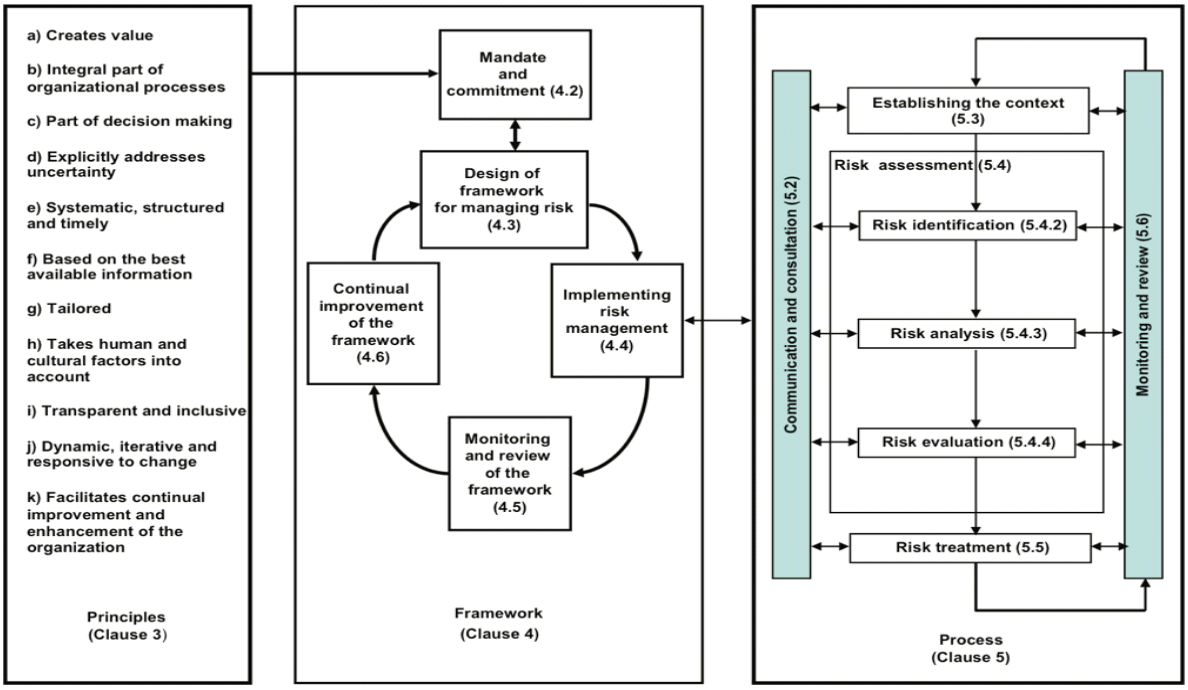
2.4 การสร้างวัฒนธรรมองค์กรด้านการบริหารจัดการความเสี่ยง (Risk Culture) ของ สวทช.

นอกจากขอบเขตการดำเนินงานทั้ง 3 ระดับแล้ว สวทช. ได้กำหนดแนวทางการสร้างวัฒนธรรมองค์กรด้านการบริหารจัดการความเสี่ยง (Risk Culture) ขึ้นเพื่อสนับสนุนและส่งเสริมให้การดำเนินงานในทุกส่วนของ สวทช. นำหลักการบริหารจัดการความเสี่ยงไปใช้เป็นเครื่องมือในการบริหารจัดการ เพราะการบริหารจัดการความเสี่ยงจะช่วยในเรื่องของการวิเคราะห์และคาดการณ์สิ่งที่จะเกิดขึ้นในอนาคต ช่วยในการจัดลำดับ

ความสำคัญของการดำเนินงาน การวางแผนป้องกัน ตลอดจนหาแนวทางในการบริหารจัดการ เพื่อเพิ่มประสิทธิภาพกระบวนการตัดสินใจ โดยแนวทางการสร้างวัฒนธรรมการบริหารจัดการความเสี่ยงของ สวทช. จะดำเนินการด้วยการผนวกหลักการบริหารจัดการความเสี่ยงเข้าไปในกระบวนการทำงานหลัก ควบคู่ไปกับการส่งเสริมและสื่อสารให้ความรู้เพื่อกระตุ้นให้เกิดความตระหนักและนำไปสู่การปฏิบัติจนเกิดเป็นวัฒนธรรมองค์กรในที่สุด

3. ระบบบริหารความเสี่ยงของ สวทช.(NSTDA Risk Management System: NRMS)

ในการประชุม กวทช. ครั้งที่ 2/2554 เมื่อวันที่ 9 มีนาคม 2554 กวทช. ได้พิจารณาหลักการและแนวทางตามมาตรฐาน ISO 31000:2009 ตามแผนภาพที่ 3.1 เป็นกรอบการบริหารจัดการความเสี่ยงของ สวทช.



แผนภาพที่ 3.1 ระบบการบริหารจัดการความเสี่ยงตามมาตรฐาน ISO 31000:2009

3.1 ระบบการบริหารจัดการความเสี่ยงตามมาตรฐาน ISO 31000:2009

จากแผนภาพที่ 3.1 แสดงความสัมพันธ์ระหว่างองค์ประกอบของการบริหารจัดการความเสี่ยง โดยระบุแนวทางการบริหารจัดการความเสี่ยงของมาตรฐาน ISO 31000:2009 แบ่งออกเป็น 3 ส่วนหลักๆ ประกอบด้วย (3.1) หลักการพื้นฐานในการบริหารจัดการความเสี่ยง (Principles) (3.2) กรอบการบริหารจัดการความเสี่ยง (Framework) และ (3.3) กระบวนการในการบริหารจัดการความเสี่ยง (Process) โดยสวทช. ได้นำหลักการทั้ง 3 ส่วน มาประยุกต์ใช้ให้มีความเหมาะสมกับกระบวนการบริหารจัดการ

ซึ่งมีรายละเอียดการดำเนินงานแต่ละส่วนตามลำดับที่จะกล่าวต่อไปนี้ และเพื่อความสะดวกในการอ้างอิงถึงระบบบริหารความเสี่ยง ISO31000:2009 ในคู่มือฉบับนี้จะใช้หัวข้อเรียงตามตัวเลขข้อกำหนด โดยตัวเลขดังกล่าวจะระบุในเครื่องหมายวงเล็บเหลี่ยม [...]

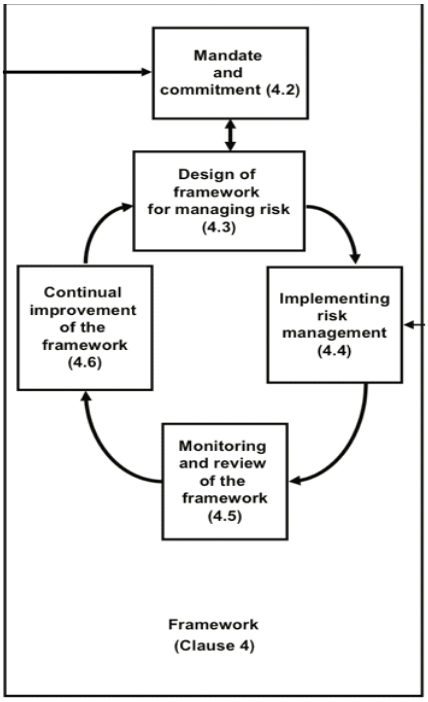
3.1.1 หลักการพื้นฐานในการบริหารจัดการความเสี่ยง (Principles) [3]

สวทช. ได้ทบทวนหลักการพื้นฐานในการบริหารจัดการความเสี่ยง (Risk Management Principles) ของสวทช. และเห็นสอดคล้องกับแนวทางและหลักการพื้นฐานตามมาตรฐาน ISO 31000 : 2009 พร้อมได้นำหลักการพื้นฐานดังกล่าวมาใช้ และเรียบเรียงจัดทำมาตรฐานเป็นภาษาไทย เพื่อให้การบริหารความเสี่ยงมีประสิทธิผลทุกระดับขององค์กร จะดำเนินการให้เป็นไปตามหลักการต่างๆ ดังต่อไปนี้

1. การบริหารความเสี่ยงช่วยสร้างและปกป้องคุณค่าขององค์กร (Creates Value)
2. การบริหารความเสี่ยงเป็นส่วนหนึ่งของกระบวนการดำเนินการทั้งหมดขององค์กร (Integral Part of Organizational Processes)
3. การบริหารความเสี่ยงเป็นส่วนหนึ่งของการตัดสินใจ (Part of Decision Making)
4. การบริหารความเสี่ยงใช้ในการจัดการกับความไม่แน่นอนอย่างชัดแจ้ง (Explicitly Addresses Uncertainty)
5. การบริหารความเสี่ยงเป็นระบบ มีรูปแบบที่ชัดเจน และทันต่อสถานการณ์ (Systematic, Structured and Timely)
6. การบริหารความเสี่ยงควรอยู่บนพื้นฐานสารสนเทศที่ดีที่สุดที่สามารถหาได้ (Based on the Best Available Information)
7. การบริหารความเสี่ยงควรออกแบบจัดทำขึ้นสำหรับองค์กรโดยเฉพาะ (Tailored)
8. การบริหารความเสี่ยงควรคำนึงถึงปัจจัยด้านบุคลากรและวัฒนธรรมขององค์กร (Takes Human and Cultural Factors into Account)
9. การบริหารความเสี่ยงควรมีความโปร่งใสและมีส่วนร่วม (Transparent and Inclusive)
10. การบริหารความเสี่ยงควรมีการดำเนินงานอย่างคล่องตัว ทบทวนทำซ้ำ และตอบสนองต่อการเปลี่ยนแปลงขององค์กร (Dynamic. Iterative and Responsive to Change)
11. การบริหารความเสี่ยงควรเอื้อต่อการพัฒนาปรับปรุงและเสริมสร้างองค์กรอย่างต่อเนื่อง (Facilitates Continual Inprovement of the Organization)

3.1.2 กรอบการบริหารความเสี่ยง (Framework for Managing Risk) [4]

สวทช. กำหนดกรอบการบริหารจัดการความเสี่ยง (Framework for Managing Risk) ตามมาตรฐานการบริหารจัดการความเสี่ยงสากล ISO 31000:2009 ซึ่งแบ่งออกเป็น 4 ส่วน โดยขับเคลื่อนผ่านวงจร PDCA ประกอบด้วย 1). การวางแผน (Plan) 2). การลงมือทำ (Do) 3). การตรวจสอบ (Check) 4). การปรับปรุงแก้ไข (Act) ในแต่ละรอบปีของการดำเนินงาน โดยมีสาระสำคัญของสิ่งที่ต้องดำเนินการตามมาตรฐาน ISO 31000:2009 ในแต่ละหัวข้อมี ดังนี้



แผนภาพที่ 3.2 กรอบการบริหารจัดการความเสี่ยง (อ้างอิงจากเอกสาร ISO 31000:2009)

(1) ความมุ่งมั่นของผู้บริหาร (Mandate and Commitment) [4.2]

การบริหารจัดการความเสี่ยงอย่างมีประสิทธิผลต้องการความมุ่งมั่นและการสนับสนุนจากผู้บริหารระดับสูงขององค์กร โดยสิ่งที่ผู้บริหารจะต้องให้ความสำคัญ ประกอบด้วย

- ประกาศ และให้การรับรองต่อนโยบายการบริหารจัดการความเสี่ยง (Risk Management Policy)
- สื่อสารถึงประโยชน์ที่จะได้จากการบริหารจัดการความเสี่ยงไปยังผู้มีส่วนได้ส่วนเสียทั้งหมด
- กำหนดโครงสร้างองค์กรที่จำเป็น บทบาทและหน้าที่ความรับผิดชอบ (Accountability) ที่เหมาะสม
- กำหนดดัชนีวัดผลการดำเนินงานบริหารความเสี่ยง ที่สอดคล้องกับผลการดำเนินงาน

- ดูแลให้วัตถุประสงค์การบริหารจัดการความเสี่ยงสอดคล้องกับวัตถุประสงค์และกลยุทธ์ขององค์กร
- ดูแลความสอดคล้องตามข้อกฎหมาย และระเบียบข้อบังคับ
- ดูแลให้มีการจัดสรรทรัพยากรที่จำเป็นเพื่อการบริหารจัดการความเสี่ยงอย่างเพียงพอ
- ดูแลความเหมาะสมของกรอบการบริหารจัดการความเสี่ยงอย่างต่อเนื่อง
- ติดตามการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงขององค์กรอย่างต่อเนื่อง
- รายงานความก้าวหน้าของระบบบริหารความเสี่ยง และผลของการบริหารความเสี่ยงต่อ กวทช. เป็นประจำในรอบปี

สวทช. มีการประกาศนโยบายการบริหารจัดการความเสี่ยงและดำเนินการสื่อสารไปยังบุคลากรภายในองค์กร ตลอดจนกำหนดวัตถุประสงค์การบริหารจัดการความเสี่ยงที่สอดคล้องกับวัตถุประสงค์และกลยุทธ์องค์กร มีการแต่งตั้งคณะทำงานพัฒนาระบบการบริหารจัดการความเสี่ยง คณะกรรมการจัดการความเสี่ยง กำหนดผู้รับผิดชอบความเสี่ยง (Risk Owner) เพื่อให้มีการบริหารจัดการความเสี่ยงอย่างเหมาะสม และสอดคล้องกับการบริหารงานโดยรวมขององค์กร

(2) การออกแบบกรอบเพื่อการบริหารจัดการความเสี่ยง (Design of Framework for Managing Risk) [4.3]

ในขั้นตอนของการวางแผน (Plan) หรือการออกแบบกรอบการบริหารจัดการความเสี่ยงขององค์กร จะต้องเริ่มจากการทำความเข้าใจในสภาพแวดล้อมทั้งภายในและภายนอกขององค์กร การกำหนดนโยบายการบริหารจัดการความเสี่ยง การบูรณาการระบบบริหารความเสี่ยงเข้ากับกระบวนการทำงานขององค์กร การกำหนดหน้าที่ความรับผิดชอบ การกำหนดกลไกในการสื่อสารและรายงานทั้งภายในและภายนอกองค์กร

การทำความเข้าใจในสภาพแวดล้อมทั้งภายในและภายนอกขององค์กร มีสาระสำคัญของสิ่งที่ต้องดำเนินการตามแนวทางมาตรฐาน ISO 31000:2009 ดังนี้

สภาพแวดล้อมภายนอกขององค์กรที่ต้องได้รับการพิจารณา ประกอบด้วย

- วัฒนธรรม การเมือง กฎหมาย ข้อบังคับ การเงิน เศรษฐกิจ และสภาพแวดล้อมในการแข่งขันทั้งในระดับประเทศ และต่างประเทศ
- ปัจจัยขับเคลื่อนที่สำคัญ และแนวโน้มที่ส่งผลกระทบต่อวัตถุประสงค์ขององค์กร การรับรู้และการให้ความสำคัญของผู้มีส่วนได้ส่วนเสียภายนอกองค์กร

สภาพแวดล้อมภายในองค์กรที่ต้องได้รับการพิจารณา ประกอบด้วย

- โครงสร้าง เช่น การควบคุม บทบาทหน้าที่ และความรับผิดชอบ
- ขีดความสามารถ ความเข้าใจในรูปของทรัพยากรและความรู้ เช่น งบประมาณ บุคลากร ความสามารถ กระบวนการทำงาน และเทคโนโลยี

- การไหลของข้อมูล และกระบวนการตัดสินใจ
- ผู้มีส่วนได้เสียภายในองค์กร
- นโยบาย วัตถุประสงค์ และกลยุทธ์ เพื่อให้ประสบความสำเร็จ
- การรับรู้ การให้ความสำคัญ และวัฒนธรรมองค์กร
- มาตรฐาน หรือรูปแบบที่ใช้ในการอ้างอิง

สวทช. ดำเนินการทบทวนสภาพแวดล้อมทั้งภายในและภายนอกผ่านกระบวนการจัดทำแผนกลยุทธ์ 5 ปี และแผนกลยุทธ์ประจำปี ซึ่งเริ่มจากการศึกษาและวิเคราะห์สภาพแวดล้อมทั้งภายในและภายนอกที่คาดว่าจะมีผลกระทบต่อการดำเนินงานในกระบวนการทบทวนวิสัยทัศน์ พันธกิจ ค่านิยม และเป้าประสงค์ขององค์กร โดยจะนำผลการทบทวนดังกล่าวมาประกอบการพิจารณา/ปรับปรุงนโยบาย แนวทางการดำเนินงาน รวมถึงแผนการบริหารจัดการความเสี่ยงประจำปี ทั้งนี้เพื่อให้การดำเนินงานบริหารความเสี่ยงสอดคล้องกับกระบวนการบริหารจัดการของ สวทช.

ภารกิจหลักคือ การทบทวน ปรับปรุงเพิ่มเติมรายละเอียดของระบบบริหารความเสี่ยงในรอบปี เมื่อได้ดำเนินการบริหารความเสี่ยงครบปี โดยพัฒนาจากผลของการบริหารความเสี่ยงทั้งปี เหตุการณ์และสถานการณ์ที่เกิดขึ้นใหม่ในรอบปีและข้อเสนอแนะ ข้อสังเกตจากผู้ปฏิบัติงานและผู้เกี่ยวข้อง เพื่อให้ระบบการบริหารความเสี่ยงมีประสิทธิภาพ และประสิทธิผลที่ดีขึ้น สำหรับการบริหารจัดการความเสี่ยงในรอบถัดไป

(3) การดำเนินการบริหารจัดการความเสี่ยง (Implementing Risk Management) [4.4]

ในขั้นตอนของการดำเนินการ (Do) การบริหารจัดการความเสี่ยงองค์กรตามกระบวนการทำงาน (Process) ที่ระบุไว้ในหัวข้อ 3.1.3 มีแนวทางการทำงานดังนี้

- กำหนดช่วงเวลาและกลยุทธ์ที่เหมาะสมสำหรับการดำเนินการตามกรอบการบริหารจัดการความเสี่ยง
- กำหนดนโยบายและนำกระบวนการบริหารจัดการความเสี่ยงมาใช้กับกระบวนการต่างๆ ขององค์กร
- ดำเนินการให้สอดคล้องกับข้อกฎหมาย และระเบียบข้อบังคับต่างๆ
- จัดทำเอกสารอธิบายถึงการตัดสินใจ รวมถึงการจัดทำวัตถุประสงค์
- จัดให้มีข้อมูลสารสนเทศ และการฝึกอบรม
- สื่อสารและให้คำปรึกษากับผู้มีส่วนได้เสีย เพื่อให้มั่นใจว่ากระบวนการบริหารจัดการความเสี่ยงต่างๆ ได้รับการนำไปปฏิบัติในทุกระดับและหน้าที่งานที่เกี่ยวข้องในองค์กร โดยเป็นส่วนหนึ่งของการปฏิบัติงานขององค์กร และกระบวนการทางธุรกิจ

สวทช. ดำเนินการตามกรอบการบริหารจัดการความเสี่ยงควบคู่ไปกับการทบทวนกลยุทธ์ประจำทุกปี (Rolling Strategic Plan) โดยกำหนดปฏิทินการบริหารจัดการความเสี่ยงให้สอดคล้องกับการบริหารภายใน สวทช.

เริ่มจากคณะกรรมการจัดการความเสี่ยงของ สวทช. จะดำเนินการทบทวนรายการความเสี่ยงด้วยการวิเคราะห์ความเสี่ยงที่อาจมีผลกระทบต่อการบรรลุวัตถุประสงค์ตามแผนกลยุทธ์ขององค์กรควบคู่ไปกับกระบวนการทบทวนกลยุทธ์ประจำปี โดยกำหนดให้ดำเนินการจัดทำแผนบริหารจัดการความเสี่ยง ระดับองค์กร ให้แล้วเสร็จภายในเดือน ตุลาคม-พฤศจิกายน ของทุกปี ทั้งนี้ เพื่อให้การดำเนินงานบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพ

(4) การติดตามและรายงานผล (Monitoring and Review of the Framework) [4.5]

เมื่อมีการบริหารความเสี่ยงตามข้อ 3.1.3 แล้ว ในแต่ละรอบปี ระบบบริหารความเสี่ยงจัดให้มีการติดตาม ทบทวน ประเมินผลการดำเนินงานของระบบซึ่งตรงกับขั้นตอนการตรวจสอบ (Check) สิ่งที่ต้องดำเนินการเพื่อให้ระบบบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิผลอย่างต่อเนื่อง ดังนี้

- กำหนดการวัดผลการดำเนินงาน
- วัดความก้าวหน้าเทียบกับแผนการบริหารจัดการความเสี่ยงเป็นระยะๆ
- ทบทวนกรอบการบริหารจัดการความเสี่ยง นโยบาย และแผนงานอย่างสม่ำเสมอ
- จัดทำรายงานความเสี่ยง ความก้าวหน้าของแผนการบริหารจัดการความเสี่ยง และการดำเนินการสอดคล้องกับนโยบายการบริหารจัดการความเสี่ยง
- ทบทวนถึงความมีประสิทธิผลของกระบวนการบริหารจัดการความเสี่ยง

สวทช. กำหนดให้คณะกรรมการจัดการความเสี่ยงของ สวทช. มีการประชุมเพื่อพิจารณาผลการดำเนินงานเป็นประจำทุก 3 เดือน โดยจะมีการรายงานผลการดำเนินงานตามแผนบริหารจัดการความเสี่ยง ประเมินระดับโอกาสและผลกระทบ พร้อมกับทบทวนและปรับปรุงแผนบริหารจัดการความเสี่ยงอย่างสม่ำเสมอ

เมื่อคณะกรรมการจัดการความเสี่ยงของ สวทช. พิจารณาผลการดำเนินงานและให้ข้อเสนอแนะแล้ว สวทช. จะนำผลสรุปดังกล่าวรายงานต่อคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. และ กวทช. อย่างน้อยทุก 6 เดือน ในช่วงกลางปี และช่วงปลายปีงบประมาณต่อเนื่องกับต้นปีงบประมาณถัดไป เพื่อให้พิจารณาอนุมัติประกาศใช้

(5) การปรับปรุงกรอบการบริหารงานอย่างต่อเนื่อง (Continual Improvement of the Framework) [4.6]

เมื่อองค์กรได้ทบทวนระบบแล้ว ผลของการทบทวนจะนำไปสู่การตัดสินใจถึงแนวทางในการปรับปรุงกรอบการบริหารจัดการความเสี่ยง นโยบาย และแผนงาน ซึ่งการตัดสินใจนี้จะช่วยในการปรับปรุงการบริหารจัดการความเสี่ยง และวัฒนธรรมการบริหารงานขององค์กร รวมถึงช่วยปรับปรุงความคล่องตัว การควบคุม และความรับผิดชอบที่มีต่อเป้าหมายองค์กรด้วย

สวทช. กำหนดให้มีการทบทวนปรับปรุงกรอบการบริหารจัดการความเสี่ยง นโยบายและแผนการดำเนินงานเป็นประจำทุกปี ทั้งนี้เพื่อให้สอดคล้องกับการบริหารจัดการภายใน/นอกองค์กร โดยจะนำผลการดำเนินงานดังกล่าวมารายงานต่อคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. และระบุในคู่มือบริหารจัดการความเสี่ยงของ สวทช. และสื่อสารให้ผู้เกี่ยวข้องเพื่อนำไปเป็นแนวทางปฏิบัติต่อไป

3.1.3 กระบวนการบริหารจัดการความเสี่ยง (Process) [5]

กระบวนการบริหารจัดการความเสี่ยง (Process) ตามมาตรฐาน ISO 31000:2009 มีขั้นตอนที่สำคัญ ดังนี้

(1) การสื่อสารและการให้คำปรึกษา (Communication and Consultation) [5.2]

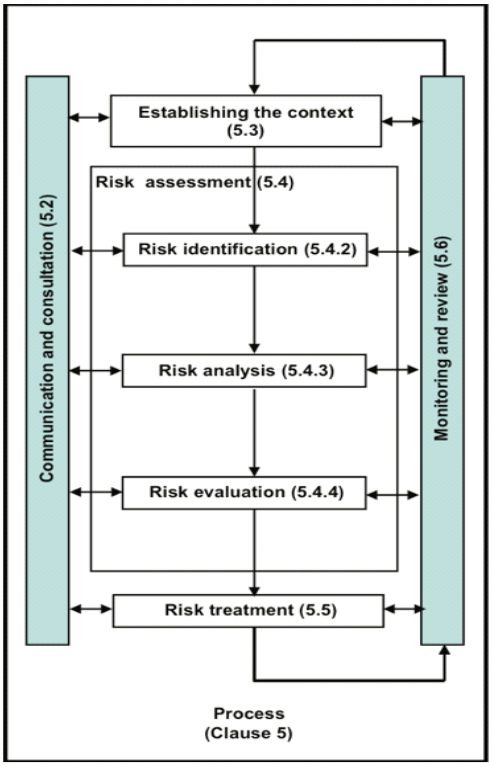
(2) การกำหนดวัตถุประสงค์ ขอบเขต และสภาพแวดล้อม (Establish the Context) [5.3]

(3) การประเมินความเสี่ยง (Risk Assessment) [5.4]

- การระบุความเสี่ยง (Risk Identification) [5.4.2]
- การวิเคราะห์ความเสี่ยง (Risk Analysis) [5.4.3]
- การประเมินความเสี่ยง (Risk Evaluation) [5.4.4]

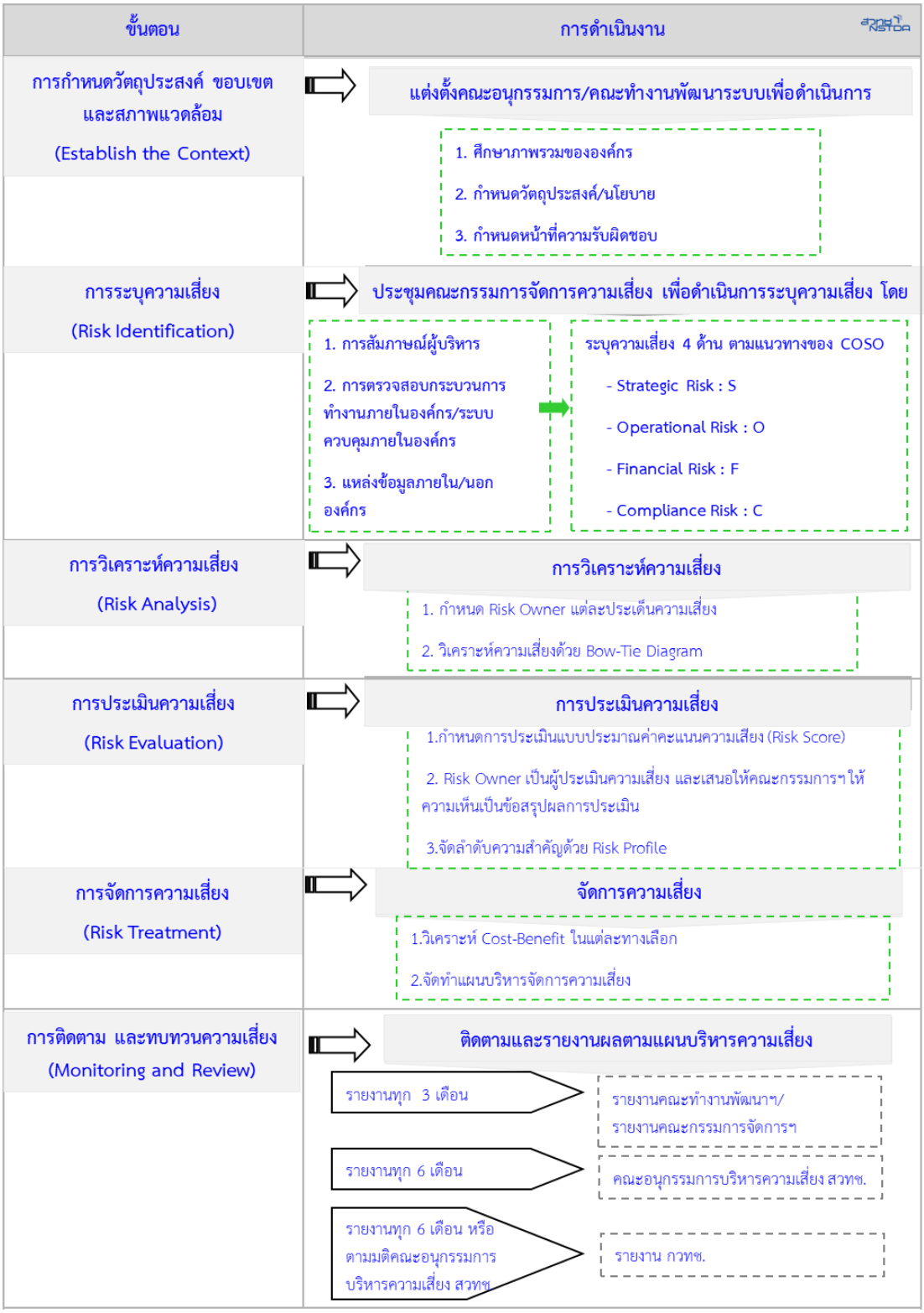
(4) การจัดการความเสี่ยง (Risk Treatment) [5.5]

(5) การติดตามตรวจสอบและการทบทวนความเสี่ยง (Monitoring and Review) [5.6]



แผนภาพที่ 3.3 กระบวนการบริหารจัดการความเสี่ยง ตามมาตรฐาน ISO 31000:2009

สวทช. กำหนดขั้นตอนและกระบวนการในการบริหารจัดการความเสี่ยงตามแนวทางมาตรฐาน ISO 31000:2009 โดยมีขั้นตอน ดังนี้



แผนภาพที่ 3.4 แนวทางการบริหารจัดการความเสี่ยงของ สวทช.

(1) การสื่อสารและการให้คำปรึกษา (Communication and Consultation) [5.2]

การสื่อสารและการให้คำปรึกษาเกี่ยวกับการบริหารจัดการความเสี่ยงเป็นการบอกกล่าวให้แก่ผู้ที่มีส่วนเกี่ยวข้องทั้งภายในและภายนอกองค์กร รวมถึงการให้คำแนะนำเกี่ยวกับขั้นตอนและวิธีการบริหารจัดการความเสี่ยง เพื่อให้เกิดความเข้าใจในการตัดสินใจดำเนินการบริหารจัดการความเสี่ยง ทราบถึงความจำเป็นขอบเขตการดำเนินงาน โดยมีการสื่อสารแลกเปลี่ยนข้อมูลระหว่างผู้ที่เกี่ยวข้องเพื่อให้เกิดความเข้าใจในแนวคิด หลักการและวิธีปฏิบัติที่ตรงกันเพื่อให้สามารถวิเคราะห์และจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ

สวทช. นำนโยบายการบริหารจัดการความเสี่ยงที่ผ่านความเห็นชอบจากคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. และ กวทช. จัดทำเป็นประกาศของ สวทช. เพื่อสื่อสารเกี่ยวกับการบริหารจัดการความเสี่ยงให้พนักงานทั่วทั้งองค์กรได้รับทราบ มีการสื่อสารและหารือร่วมกันเกี่ยวกับขั้นตอนและกระบวนการบริหารจัดการความเสี่ยงระหว่างผู้เกี่ยวข้อง เพื่อให้เกิดความเข้าใจในการตัดสินใจดำเนินการบริหารจัดการความเสี่ยง ทราบถึงความจำเป็นในการดำเนินการบริหารจัดการความเสี่ยง ตลอดจนทราบขอบเขตการดำเนินงาน โดยตลอดการดำเนินงานจะมีการสื่อสารแลกเปลี่ยนข้อมูลเพื่อให้เกิดความเข้าใจในแนวคิดหลักการและวิธีปฏิบัติเพื่อให้เกิดความเข้าใจที่ตรงกันในทุกขั้นตอน

(2) การกำหนดบริบทของการบริหารความเสี่ยง รวมถึงวัตถุประสงค์ ขอบเขตและสภาพแวดล้อม (Establish the Context) [5.3]

การกำหนดสภาพแวดล้อมขององค์กร เป็นการระบุสภาพแวดล้อมทั้งภายนอกและภายในขององค์กรที่มีความสัมพันธ์และเกี่ยวข้องกับองค์กร ทำให้เกิดผลกระทบต่อองค์กร จึงนำไปสู่กระบวนการบริหารจัดการความเสี่ยง

การกำหนดสภาพแวดล้อมภายนอก หมายถึง องค์ประกอบต่างๆ ที่อยู่ภายนอกองค์กรที่มีอิทธิพลต่อความสำเร็จในวัตถุประสงค์ขององค์กร ซึ่งการทำความเข้าใจในสภาพแวดล้อมภายนอกองค์กรจะช่วยสร้างความมั่นใจได้ว่าผู้มีส่วนได้ส่วนเสียขององค์กร รวมถึงวัตถุประสงค์ของผู้ที่มีส่วนได้ส่วนเสียนั้นๆ ได้รับการนำมาพิจารณาเพื่อกำหนดเกณฑ์ความเสี่ยง สภาพแวดล้อมภายนอกองค์กร ประกอบด้วยเศรษฐกิจ การเมือง วัฒนธรรม กฎหมาย ข้อบังคับ การเงิน สภาพแวดล้อมในการแข่งขันทั้งภายในประเทศและต่างประเทศ รวมถึงการยอมรับของผู้มีส่วนได้ส่วนเสียภายนอก

การกำหนดสภาพแวดล้อมภายใน หมายถึง สิ่งที่อยู่ภายในองค์กรซึ่งมีอิทธิพลต่อความสำเร็จในการบรรลุวัตถุประสงค์ขององค์กร โดยกระบวนการบริหารจัดการความเสี่ยง จะต้องสอดคล้องในทิศทางเดียวกันกับวัฒนธรรมกระบวนการ และโครงสร้างขององค์กร โดยสภาพแวดล้อมภายในองค์กร ประกอบด้วย นโยบาย

วัตถุประสงค์ วิสัยทัศน์ พันธกิจ และกลยุทธ์ที่จะนำไปสู่ความสำเร็จ ขีดความสามารถขององค์กรในรูปของทรัพยากร ความรู้ ความสามารถ ระบบสารสนเทศ ผู้มีส่วนได้ส่วนเสียภายในองค์กร วัฒนธรรมองค์กร โครงสร้าง ระบบการจัดการบทบาทหน้าที่ และความรับผิดชอบ

สวทช. ทำการระบุปัจจัยความเสี่ยงโดยพิจารณาทั้งปัจจัยภายนอกและปัจจัยภายในที่มีความสัมพันธ์ต่อองค์กร ซึ่งจะนำไปสู่การบริหารจัดการความเสี่ยง การกำหนดขอบเขตความเสี่ยง (Risk Scope) กำหนดเกณฑ์ประเมินความเสี่ยง (Risk Criteria) และปัจจัยเสี่ยงที่อาจเป็นอุปสรรคในการดำเนินธุรกิจให้บรรลุเป้าหมาย

ปัจจัยเสี่ยงภายนอก ประกอบด้วย การเปลี่ยนแปลงทางด้านสังคม เศรษฐกิจ ข้อบังคับ กฎหมาย การเงิน การเมือง วัฒนธรรม สิ่งแวดล้อม และภัยพิบัติต่างๆ

ปัจจัยเสี่ยงภายใน ประกอบด้วย งบประมาณแผ่นดิน แผนกลยุทธ์การวิจัยพัฒนา การบริหารจัดการภายใน การบริหารบุคลากร การบริหารจัดการงานวิจัย โครงสร้างพื้นฐานด้าน ว&ท กฎ ระเบียบ ข้อบังคับ คำสั่ง และประกาศต่างๆ ที่เกี่ยวข้อง

(3) การประเมินความเสี่ยง (Risk Assessment) [5.4]

การประเมินความเสี่ยงประกอบด้วยกระบวนการหลัก 3 กระบวนการ ดังต่อไปนี้

(3.1) การระบุความเสี่ยง (Risk Identification) [5.4.2]

องค์กรจะต้องทำการระบุถึงแหล่งที่มาของความเสี่ยง และระบุปัจจัยความเสี่ยง ตลอดจนพื้นที่ที่ได้รับผลกระทบ เหตุการณ์ และสาเหตุรวมถึงผลที่จะตามมา เป้าหมายของขั้นตอนนี้จะเป็นการจัดทำรายการความเสี่ยงจากเหตุการณ์ที่อาจทำให้ความสำเร็จของวัตถุประสงค์เปลี่ยนไป เช่น เกิดความล้มเหลวหรือลดระดับความสำเร็จลง หรือทำให้ความสำเร็จเกิดล่าช้า

การระบุความเสี่ยง และปัจจัยหรือสาเหตุของความเสี่ยง ต้องอาศัยผู้ปฏิบัติงาน และผู้บริหารทุกระดับพิจารณา/ทบทวนปัจจัยภายในและภายนอกให้ครอบคลุมในทุกประเภทของความเสี่ยงที่อาจจะส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร ซึ่งต้องอาศัยความร่วมมือของบุคลากรภายในหน่วยงานร่วมกันค้นหาความเสี่ยงที่อาจจะเกิดขึ้น โดยการประชุมปรึกษาหารือร่วมกันของคณะกรรมการ/คณะทำงาน หรือการระดมสมองของผู้ปฏิบัติงานที่เกี่ยวข้อง เพื่อการวิเคราะห์สภาพแวดล้อม (SWOT: Strength, Weakness, Threat, Opportunity) ที่ส่งผลกระทบต่อการดำเนินงาน หรืออาจจะใช้การวิเคราะห์กระบวนการทำงาน การวิเคราะห์ผลการปฏิบัติงานที่ผ่านมา การประชุมเชิงปฏิบัติการ การระดมสมอง การสัมภาษณ์ แบบสอบถาม หรือการศึกษาข้อมูลในอดีต ทั้งนี้การจะเลือกวิธีการในการระบุความเสี่ยงขึ้นอยู่กับความเหมาะสมขององค์กร

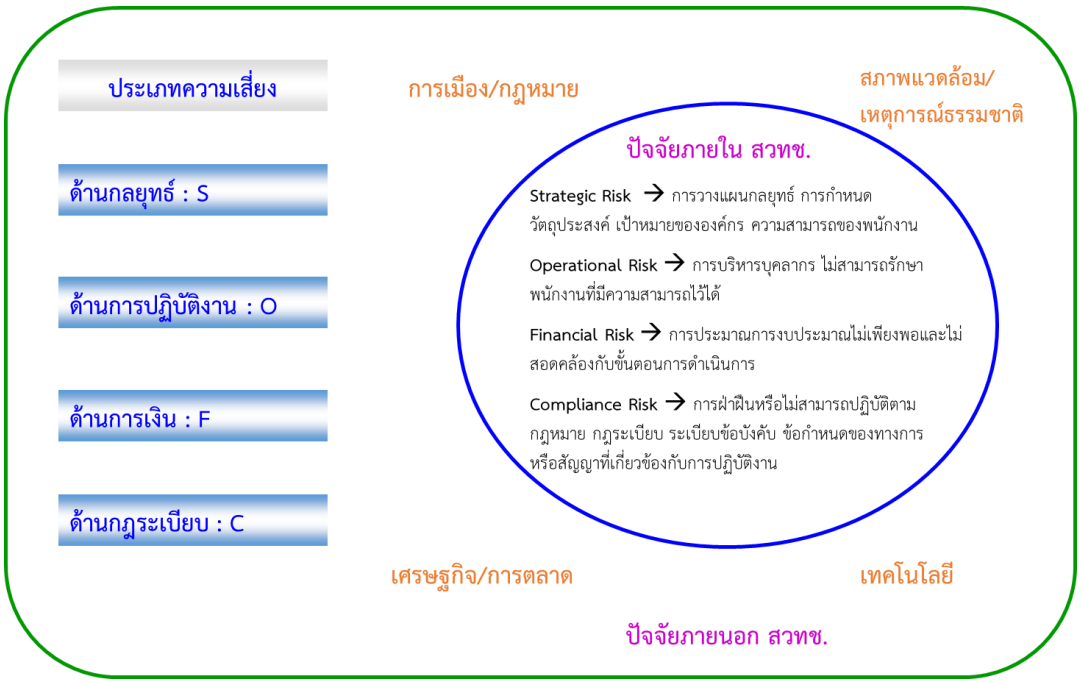
สำหรับการบริหารจัดการความเสี่ยงของ สวทช. จะใช้วิธีการสัมภาษณ์ผู้บริหาร พิจารณาแหล่งข้อมูลภายใน/นอกองค์กร ข้อมูลการตรวจสอบกระบวนการทำงานภายในองค์กรและระบบควบคุมของหน่วยงาน โดยการระบุความเสี่ยงจะครอบคลุมความเสี่ยง 4 ประเภท คือ

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) คือ ความเสี่ยงที่มีผลกระทบต่อทิศทาง หรือ ภารกิจหลักขององค์กร หรือมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร อันเนื่องมาจาก การเมือง เศรษฐกิจ ความเปลี่ยนแปลงของสถานการณ์ เหตุการณ์ภายนอก ผู้ใช้บริการ ฯลฯ หรือความเสี่ยงที่เกิดจากการตัดสินใจผิดพลาดหรือนำการตัดสินใจนั้นมาใช้อย่างไม่ถูกต้อง

2. ความเสี่ยงด้านปฏิบัติการ (Operational Risk) คือ ความเสี่ยงเนื่องจากการปฏิบัติงานภายในองค์กร อันเกิดจากกระบวนการ บุคลากร ความเพียงพอของข้อมูล ส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินธุรกิจ เช่น ความเสี่ยงของกระบวนการบริหารโครงการ การบริหารงานวิจัย ระบบงานต่างๆ ที่สนับสนุนการดำเนินงาน

3. ความเสี่ยงทางด้านการเงิน (Financial Risk) คือ ความเสี่ยงเนื่องจากสถานะและการดำเนินการทางการเงิน หรือ งบประมาณเกิดความขัดข้องจนกระทบการดำเนินงานขององค์กรในการบรรลุเป้าหมายตามพันธกิจ อันเนื่องมาจากขาดการจัดหาข้อมูล การวิเคราะห์ การวางแผน การควบคุม และการจัดทำรายงานเพื่อนำมาใช้ในการบริหารการเงินได้อย่างถูกต้อง เหมาะสม ทำให้ขาดประสิทธิภาพ และไม่ทันต่อสถาณการณ์ ซึ่งส่งผลต่อการตัดสินใจทางการเงิน หรือการบริหารงบประมาณที่ผิดพลาด ส่งผลกระทบต่อสถานะการเงินขององค์กร หรือเป็นความเสี่ยงที่เกี่ยวข้องกับการเงินขององค์กร เช่น การประมาณงบประมาณไม่เพียงพอและไม่สอดคล้องกับการดำเนินการ เนื่องจากขาดการจัดหาข้อมูล การวิเคราะห์ การวางแผน การควบคุม และการจัดทำรายงานเพื่อนำไปใช้ในการบริหารงบประมาณ ความผันผวนทางการเงิน สภาพคล่อง อัตราดอกเบี้ย ข้อมูลเอกสารหลักฐานทางการเงิน และการรายงานทางการเงิน/บัญชี

4. ความเสี่ยงทางด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk) คือ ความเสี่ยงเนื่องจากการฝ่าฝืนหรือไม่สามารถปฏิบัติตามกฎหมาย กฎระเบียบ ระเบียบข้อบังคับ ข้อกำหนดของทางการ หรือสัญญาที่เกี่ยวข้องกับการปฏิบัติงาน โดยความเสี่ยงลักษณะนี้อาจเกิดขึ้นจากความไม่ชัดเจน ความไม่ทันสมัย หรือความไม่ครอบคลุมของกฎหมาย กฎระเบียบ ข้อบังคับ ต่างๆ รวมถึงการทำนิติกรรมสัญญา การร่างสัญญาที่ไม่ครอบคลุมการดำเนินงาน การตกเป็นข่าว เสียชื่อเสียง (Reputation Risk) การเกิดคดี การถูกตรวจสอบ ฯลฯ



แผนภาพที่ 3.5 แหล่งที่มาของความเสี่ยงจากปัจจัยภายในและปัจจัยภายนอก สวทช.

กระบวนการระบุความเสี่ยงของ สวทช.

สวทช. จะดำเนินการทบทวนและระบุรายการความเสี่ยงทุกปี โดยการระบุความเสี่ยง จะเริ่มดำเนินการหลังจากทบทวนวัตถุประสงค์เชิงกลยุทธ์/ตัวชี้วัด แล้วเสร็จ ซึ่งมีวิธีการดำเนินงาน ดังนี้

1) นำรายการความเสี่ยงของปีงบประมาณก่อนหน้า, ปีงบประมาณปัจจุบัน และเหตุการณ์/สถานการณ์ที่มีการเปลี่ยนแปลงกำหนดเป็นรายการความเสี่ยง
2) ตรวจสอบ Strategic Objectives : SO , SWOT, แผนกลยุทธ์ฉบับปัจจุบัน และเหตุการณ์/สถานการณ์ เกี่ยวข้องกับรายการความเสี่ยง
3) ทบทวนรายการความเสี่ยงของปีปัจจุบันร่วมกับผู้บริหารหรือผู้เกี่ยวข้องที่ทำหน้าที่ผู้รับผิดชอบความเสี่ยง (Risk Owner) โดยพิจารณาจากผลการบริหารจัดการความเสี่ยง ณ ไตรมาส ปัจจุบันเป็นหลัก เพื่อพิจารณาความคืบหน้าและทบทวนผลสัมฤทธิ์ของมาตรการในแผนบริหารจัดการความเสี่ยง
4) ตรวจสอบรายงานผลการประเมิน รายงานผลการสอบทานหน่วยงาน/กระบวนการทั้งภายในและภายนอก ฯลฯ ที่เกิดขึ้นในช่วงปีที่ผ่านมา
5) สัมภาษณ์ผู้บริหารเกี่ยวกับผลการดำเนินงานปัจจัยภายใน/ภายนอกที่อาจจะส่งผลกระทบต่อการดำเนินงานของ สวทช.

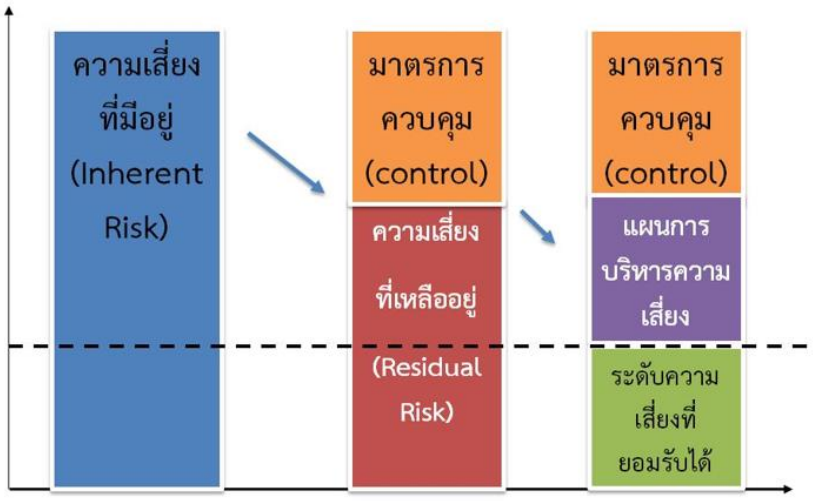
6) ประชุมหารือร่วมกับผู้บริหารและผู้เกี่ยวข้องเพื่อพิจารณาผลของการบริหารจัดการความเสี่ยงที่ผ่านมา รวมทั้งเหตุการณ์ที่คาดว่าจะเกิดและจะมีผลกระทบต่อการบรรลุวัตถุประสงค์ของ สวทช. รวมทั้งพิจารณาผลกระทบทั้งในเชิงบวกและเชิงลบจากเหตุการณ์ที่อาจจะเกิดขึ้น

7) นำผลการดำเนินงานข้อ 1-6 ระบุในตารางการทบทวนรายการความเสี่ยง ประจำปี (รายละเอียดตามภาคผนวก จ) ซึ่งสาระสำคัญของข้อมูลที่ต้องนำมาระบุในตาราง ประกอบด้วย

- เหตุการณ์/สถานการณ์ประกอบการพิจารณา
- ตัวชี้วัดของ สวทช. ในปีงบประมาณที่ดำเนินการระบุรายการความเสี่ยง
- วัตถุประสงค์เชิงกลยุทธ์ (SO : Strategic Objectives) ที่เกี่ยวข้อง
- ข้อเสนอเพื่อพิจารณา
- อื่นๆ ตามความเหมาะสม

8) เสนอที่ประชุมคณะกรรมการจัดการความเสี่ยงพิจารณานำรายการความเสี่ยงที่ผ่านการพิจารณามากำหนดเป็นรายการความเสี่ยงประจำปี

* กรณีดำเนินการระบุความเสี่ยงระดับองค์กร (ERM) ต้องแสดงผลการวิเคราะห์ประสิทธิผลการควบคุมที่มีอยู่ด้วย



แผนภาพที่ 3.6 Inherent Risk VS Residual Risk

เกณฑ์การประเมินประสิทธิผลการควบคุมที่มีอยู่ จะพิจารณาจาก 3 มุมมอง ประกอบด้วย (1) ผลการดำเนินงานเมื่อเทียบกับเป้าหมาย (2) กระบวนการควบคุม และ (3) การติดตามผลการดำเนินงาน โดยแบ่งเป็น 3 ระดับ ดังนี้

Risk ID :			
ระดับ	ผลการดำเนินงานเมื่อเทียบกับเป้าหมาย	กระบวนการควบคุม	การติดตามผลการดำเนินงาน
ต่ำ (Low)	● ผลการดำเนินงานต่ำกว่าเป้าหมาย	● มีการควบคุม แต่ยังไม่สอดคล้องกับบริบทที่เปลี่ยนไป	● มีการติดตามผลและรายงานให้ผู้เกี่ยวข้องทราบตามคำร้องขอ
กลาง (Medium)	● ผลการดำเนินงานเป็นไปตามเป้าหมาย	● มีการควบคุมที่สอดคล้องกับบริบทที่เปลี่ยนไป แต่ยังไม่กำหนดเป็นมาตรฐาน	● มีการติดตามและรายงานผลให้ผู้เกี่ยวข้องทราบตามระยะเวลาที่กำหนด
สูง (High)	● ผลการดำเนินงานดีกว่าเป้าหมายมาก	● มีการกำหนดกระบวนการควบคุมเป็นมาตรฐาน	● มีการกำหนดกระบวนการติดตามเป็นมาตรฐาน

ตารางที่ 3.1 เกณฑ์การประเมินประสิทธิผลการควบคุมที่มีอยู่

การพิจารณาประสิทธิผลการควบคุม หากมีมุมมองใด ที่มีการควบคุมอยู่ที่ “ต่ำ” จะถือว่าประสิทธิภาพการควบคุมไม่เพียงพอ

(3.2) การวิเคราะห์ความเสี่ยง (Risk Analysis) [5.4.3]

การวิเคราะห์ความเสี่ยงจะเป็นข้อมูลเพื่อใช้ในการตัดสินใจในการจัดการกับความเสี่ยง โดยการพิจารณาถึงโอกาสในการเกิด (Likelihood) และผลกระทบ (Impact) การวิเคราะห์อาจจะเป็นได้ทั้งการวิเคราะห์เชิงคุณภาพ (Qualitative) กึ่งปริมาณ (Semi-Quantitative) หรือเชิงปริมาณ (Quantitative) หรือผสมผสานกันไป

การวิเคราะห์ความเสี่ยง

เมื่อระบุรายการความเสี่ยงแล้ว ผู้บริหารจะกำหนดผู้รับผิดชอบความเสี่ยง (Risk Owner) โดยยึดบทบาท หน้าที่ ความรับผิดชอบที่มีอยู่ในภารกิจปกติเป็นหลักหรือพิจารณาตามความเหมาะสมจากมติที่ประชุมคณะกรรมการจัดการความเสี่ยง ทั้งนี้เพราะต้องการให้ระบบบริหารความเสี่ยงเป็นส่วนหนึ่งของการดำเนินงานตามภารกิจปกติจนเกิดเป็นวัฒนธรรมองค์กรในที่สุด

เมื่อกำหนดผู้รับผิดชอบความเสี่ยง (Risk Owner) แล้ว ผู้รับผิดชอบความเสี่ยงจะใช้ผังสรุปการวิเคราะห์และประเมินความเสี่ยงหรือ Bow Tie Diagram (เป็นข้อมูลที่ สวทช. ได้รับจาก CSIRO) ซึ่งเป็นองค์กรวิจัยขนาดใหญ่ในประเทศออสเตรเลีย ที่มีพันธกิจใกล้เคียงกับ สวทช. เห็นว่าเครื่องมือดังกล่าวมีความเหมาะสมและมีประสิทธิภาพในการบริหารจัดการความเสี่ยงในองค์กร) จึงได้นำมาปรับปรุงดัดแปลงใช้งานในการวิเคราะห์สาเหตุและผลกระทบของความเสี่ยง เพื่อให้ผู้รับผิดชอบความเสี่ยงใช้เป็นข้อมูลในการประเมินความเสี่ยง พิจารณาทางเลือกและกำหนดแนวทางตอบสนองความเสี่ยง เพราะแนวทางในการตอบสนองความเสี่ยงมีหลายวิธีและสามารถปรับเปลี่ยนให้เหมาะสมกับสถานการณ์ได้ ขึ้นอยู่กับดุลยพินิจของผู้รับผิดชอบความเสี่ยง (Risk Owner) โดยทางเลือกในการจัดการความเสี่ยงไม่จำเป็นต้องเฉพาะเจาะจงและอาจจะแปรเปลี่ยนไปได้ตามความเหมาะสมของสถานการณ์

การใช้ผังสรุปการวิเคราะห์และประเมินความเสี่ยงหรือ Bow Tie Diagram (BTD)

เพื่อให้กระบวนการบริหารจัดการความเสี่ยง มีประสิทธิภาพสูง คล่องตัว สวทช. ได้พิจารณาใช้ Bow Tie Diagram เป็นเอกสารหลักในการดำเนินการ การติดตามความก้าวหน้า ทั้งนี้เพราะกลไกสำคัญของการบริหารจัดการความเสี่ยง คือ การได้หารือและทำความเข้าใจร่วมกันระหว่างผู้มีส่วนได้ส่วนเสียที่สำคัญ เอกสารเป็นส่วนประกอบของการดำเนินงาน

ผู้รับผิดชอบความเสี่ยง (Risk Owner) เป็นผู้รับผิดชอบผังสรุปการวิเคราะห์และประเมินความเสี่ยงหรือ Bow Tie Diagram และใช้แผนภาพนี้ในการประชุม รายงานผล ปรึกษา สื่อสาร ร่วมกับคณะกรรมการจัดการความเสี่ยง และผู้มีส่วนได้ส่วนเสียอื่นๆ

ผู้ที่ทำหน้าที่เลขาฯ ของผู้รับผิดชอบความเสี่ยง มีหน้าที่บันทึกประเด็นต่างๆ ใน Bow Tie Diagram นี้ และจัดทำข้อมูลใน Bow Tie Diagram ให้เป็นปัจจุบัน (up-to-date) ฝ่ายเลขาฯ มีหน้าที่ในการบันทึกรายละเอียดอื่นๆ ที่เกี่ยวข้องกับ Bow Tie Diagram เพื่อเป็นข้อมูลในการอธิบายประกอบ และประมวลข้อมูลทั้งจาก Bow Tie Diagram และรายละเอียดอื่นๆ เพื่อจัดทำแผนบริหารจัดการความเสี่ยง รายงานความก้าวหน้า และรายงานสรุปการบริหาร/จัดการความเสี่ยง

การใช้ผังสรุปการวิเคราะห์และประเมินความเสี่ยงหรือ Bow Tie Diagram มีวัตถุประสงค์เพื่อสื่อสารประเด็นต่างๆ ที่เกี่ยวข้องกับความเสี่ยง ทั้งสาเหตุ ผลกระทบ กลไกการควบคุมต่างๆ แผนการดำเนินงานเพื่อจัดการความเสี่ยงโดยแสดงแยกให้เห็นทั้งกลไกควบคุมเดิมที่มีอยู่แล้ว (Exitsting Control) และแผนใหม่ (New Tasks) ในการจัดการความเสี่ยงให้ครอบคลุมรอบด้าน รวมทั้งระดับคะแนนของความเสี่ยงนั้น ทั้งนี้องค์ประกอบของ Bow Tie Diagram ปรากฏในแผนภาพที่ 3.8

BTD สำหรับ Risk ..... วันที่.....

7. Risk Rating "Before" Mitigation	
Likelihood	
Impact	
Residual Risk Rating	
วันที่	

1.Risk ID :	
Owner	
ผู้ช่วย Owner	

8. Risk Rating "After" Mitigation		
	แผน	ผล
Likelihood		
Impact		
Residual Risk Rating		
วันที่		

2. Causes	

3. Impacts	

4. Existing Controls (Preventative)		
Existing Preventative controls	Link to Cause #	Control Owner

5. Existing Controls (Mitigating)		
Existing Mitigating Controls	Link to Impact #	Control Owner

6. Risk Mitigating (Tasks)				
Risk Control Area	Link to Cause#	Link to Impact#	Due date	Task Owner

จัดทำโดย.....
วันที่.....

อนุมัติโดย.....
วันที่.....

แผนภาพที่ 3.7 แผนภาพแสดงสรุปการวิเคราะห์และประเมินความเสี่ยง หรือ Bow Tie Diagram

คำอธิบายผังสรุปการวิเคราะห์และประเมินความเสี่ยง **หรือ Bow Tie Diagram**

1. รหัส ชื่อ และคำอธิบาย ความเสี่ยง ผู้รับผิดชอบความเสี่ยง (Risk Identification)

กล่องหมายเลข 1 อยู่ตรงกลางของแผนภาพ

แผนภาพที่ 3.8 Bow Tie Diagram กล่องหมายเลข 1 รหัส ชื่อ และคำอธิบายความเสี่ยง

ช่องบนสุดของกล่องหมายเลข 1 คือ รหัส โดยแต่ละความเสี่ยงของสำนักงานฯ จะได้รับการกำหนดรหัสชื่อเรียก (Code) เพื่อให้เข้าใจตรงกันอย่างชัดเจนว่า รายการความเสี่ยงที่จัดการอยู่นี้เกี่ยวข้องกับความเสี่ยงเรื่องใด โดยรายการความเสี่ยงระดับองค์กร (Enterprise-level Risk) ประกอบด้วย ตัวอักษร 4 ตัว ประกอบด้วย

ตัวที่ 1 แทนด้วยตัวอักษร R = Risk เพื่อแสดง ว่าเป็นรหัสในระบบบริหารความเสี่ยง

ตัวที่ 2 แทนระดับองค์กร E = Enterprise เพื่อแสดงว่าเป็นระบบบริหารความเสี่ยงระดับองค์กร

ตัวที่ 3 แทนประเภทของความเสี่ยง S-O-F-C

ตัวที่ 4 แทนลำดับที่ของรายการความเสี่ยงแต่ละประเภท (ระบุหมายเลข 1,2,3.....ตามลำดับที่ได้รับไม่ได้หมายถึงระดับความสำคัญของความเสี่ยง)

ช่องที่ 2 ของกล่องที่ 1 คือ ชื่อของความเสี่ยง โดยแต่ละความเสี่ยงจะได้รับการเสนอและหารือกันในคณะกรรมการจัดการความเสี่ยง เพื่อให้ได้ใจความสำคัญ และ ความเข้าใจที่ตรงกันสำหรับความเสี่ยงเรื่องนั้นๆ

ช่องที่ 3 ของกล่องที่ 1 คือ คำอธิบายโดยย่อของความเสี่ยงนั้นๆ (Short Description) เพื่ออธิบาย ขยายความจาก “ชื่อของความเสี่ยง”

ช่องที่ 4 ของกล่องที่ 1 คือ ชื่อและตำแหน่งของผู้รับผิดชอบความเสี่ยงนั้นๆ (Risk Owner) เพื่อให้มีการมอบหมายความรับผิดชอบที่ชัดเจนในการบริหารจัดการความเสี่ยง คณะกรรมการจัดการความเสี่ยง จะพิจารณามอบหมายผู้บริหารหรือผู้ที่มีส่วนเกี่ยวข้อง ให้เป็นผู้ที่รับผิดชอบในการกำหนดแผนจัดการความเสี่ยงย่อยๆ รวมถึงการติดตามผลการจัดการความเสี่ยง เพื่อนำเสนอต่อคณะกรรมการจัดการความเสี่ยง

ช่องสุดท้ายของกล่องที่ 1 คือ ชื่อของผู้ช่วยผู้รับผิดชอบความเสี่ยงนั้นๆ เพื่อช่วยผู้รับผิดชอบความเสี่ยง (Risk Owner) จัดเตรียมข้อมูลสำหรับการวิเคราะห์ ประเมิน จัดทำแผนบริหารจัดการความเสี่ยง และติดตามผลการดำเนินงาน ร่วมทั้งประสานงานผู้เกี่ยวข้องในการจัดประชุม/หารือตามความเหมาะสม

2. สาเหตุของความเสี่ยง (Causes)

2.Causes	3.Impacts
แสดงถึงสาเหตุต่างๆ ที่สามารถจะส่งผลให้เกิดความเสี่ยงในกล่องหมายเลข 1 ได้	

แผนภาพที่ 3.9 Bow Tie Diagram กล่องหมายเลข 2 สาเหตุของความเสี่ยง (Causes)

กล่องหมายเลข 2 แสดงถึงสาเหตุต่างๆ ที่สามารถจะส่งผลให้เกิดความเสี่ยงในกล่องหมายเลข 1 ได้ การกรอกข้อมูลในกล่องหมายเลข 2 นี้ ดำเนินการโดยใส่ชื่อรายการสาเหตุ โดยอาจจะเรียงลำดับจากสาเหตุที่สำคัญที่สุดก่อนก็ได้ แต่ทุกสาเหตุที่ใส่ในกล่องหมายเลข 2 นี้ จะต้องใส่หมายเลขกำกับที่คอลัมน์แรกไว้ด้วย เพื่อวิเคราะห์การเชื่อมโยงต่อไป

3. ผลกระทบที่เกิดขึ้นหากเกิดความเสี่ยงนั้น (Impact)

2.Causes	3.Impacts
	แสดงถึงผลกระทบหรือเหตุการณ์ต่างๆ ที่จะเกิดขึ้นพร้อมกับ/หลังจากเกิดความเสี่ยงในกล่องหมายเลข 1 แล้ว

แผนภาพที่ 3.10 Bow Tie Diagram กล่องหมายเลข 3 ผลกระทบที่เกิดขึ้นหากเกิดความเสี่ยงนั้น

กล่องหมายเลข 3 แสดงถึงผลกระทบหรือเหตุการณ์ต่างๆ ที่จะเกิดขึ้นหลังจากเกิดความเสี่ยงในกล่องหมายเลข 1 แล้ว การกรอกข้อมูลในกล่องหมายเลข 3 นี้ ดำเนินการโดยใส่ชื่อรายการผลกระทบ โดยอาจจะเรียงลำดับจากผลกระทบที่สำคัญที่สุดก่อนก็ได้ แต่ทุกผลกระทบที่ใส่ในกล่องหมายเลข 3 นี้ จะต้องใส่หมายเลขกำกับที่คอลัมน์แรกไว้ด้วย เพื่อวิเคราะห์การเชื่อมโยงต่อไป

4. กลไกการควบคุมเชิงป้องกันที่มีอยู่แล้ว (Existing Controls - Preventative)

4. Existing Controls (Preventative)		
Existing Preventative Controls	**Link to Cause #**	**Control Owner**
แสดงรายชื่อกลไกที่องค์กรมีอยู่แล้ว ที่ใช้ในการป้องกันมิให้เกิดสาเหตุในกล่องที่ 2		

แผนภาพที่ 3.11 Bow Tie Diagram กล่องหมายเลข 4 กลไกการควบคุมเชิงป้องกันที่มีอยู่แล้ว

กล่องหมายเลข 4 แสดงรายชื่อกลไกที่องค์กรมีอยู่แล้ว ที่ใช้ในการควบคุม/ป้องกันมิให้เกิดสาเหตุในกล่องหมายเลข 2 (Existing Preventative Controls) โดยแต่ละกลไกที่แสดงนั้น จะต้องใส่หมายเลขกำกับว่ากลไกนั้นๆ สามารถช่วยป้องกัน/มีส่วนช่วยป้องกันสาเหตุเรื่องใด (Link to Causes #) พร้อมทั้งระบุผู้ที่รับผิดชอบ/หน่วยงานที่รับผิดชอบกลไกนั้นๆ (Control Owner) เพื่อวิเคราะห์การเชื่อมโยงต่อไป

5. กลไกการควบคุมเชิงแก้ไขที่มีอยู่แล้ว (Existing Controls - Mitigating)

5. Existing Controls (Mitigating)		
Existing Mitigating Controls	**Link to Impact #**	**Control Owner**
แสดงรายชื่อกลไกที่องค์กรมีอยู่แล้ว ที่ใช้ในการแก้ไขผลกระทบ/ดำเนินการมิให้เกิดผลกระทบที่รุนแรงในกล่องหมายเลข 3		

แผนภาพที่ 3.12 Bow Tie Diagram กล่องหมายเลข 5 กลไกการควบคุมเชิงแก้ไขที่มีอยู่แล้ว

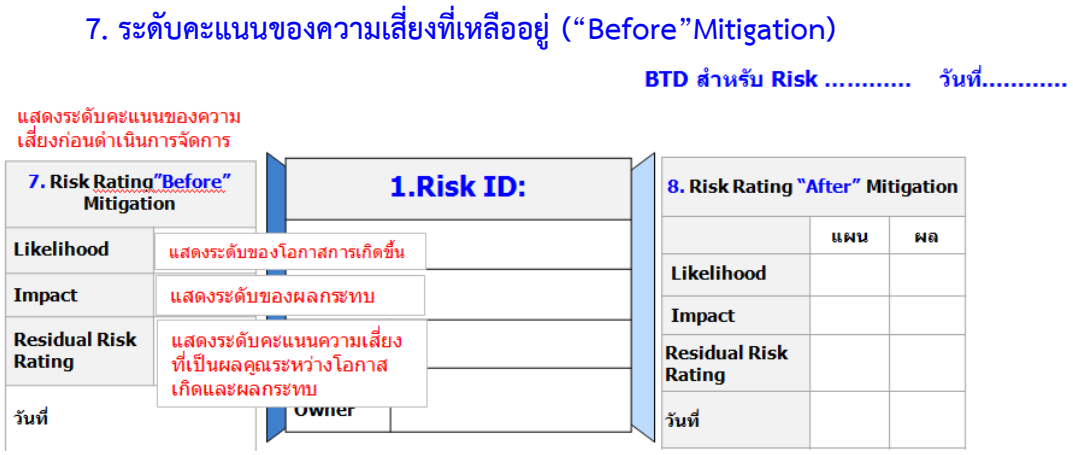
กล่องหมายเลข 5 แสดงรายชื่อกลไกที่องค์กรมีอยู่แล้ว ที่ใช้ในการแก้ไขผลกระทบ/ดำเนินการมิให้เกิดผลกระทบที่รุนแรงในกล่องหมายเลข 3 (Existing Controls) โดยแต่ละกลไกที่แสดงนั้น จะต้องใส่หมายเลขกำกับว่า กลไกนั้นๆ สามารถช่วยแก้ไข/มีส่วนช่วยแก้ไขผลกระทบเรื่องใด (Link to Impact #) พร้อมทั้งระบุผู้ที่รับผิดชอบ/หน่วยงานที่รับผิดชอบกลไกนั้นๆ (Control Owner) เพื่อวิเคราะห์เชื่อมโยงต่อไป

6. กิจกรรมเพื่อปรับปรุงแก้ไข (Risk Mitigation Tasks)

6.Risk Mitigation Tasks				
Risk Control Area	**Link to Cause #**	**Link to Impact#**	**Due Date**	**Task Owner**
แสดงรายชื่อกิจกรรมที่ Risk owner ประสงค์จะให้มีการดำเนินการเพิ่มเติม (รวมทั้งการปรับปรุงกลไกที่มีอยู่เดิม) เพื่อใช้ในการป้องกันสาเหตุ และแก้ไขผลกระทบ/ดำเนินการมิให้เกิดผลกระทบที่รุนแรง				

แผนภาพที่ 3.13 Bow Tie Diagram กล่องหมายเลข 6 กิจกรรมเพิ่มเติมเพื่อปรับปรุงแก้ไข

กล่องหมายเลข 6 แสดงรายชื่อกิจกรรมที่ผู้รับผิดชอบความเสี่ยง (Risk Owner) ประสงค์ให้ดำเนินการเพิ่มเติม หรือการปรับปรุงกลไกที่มีอยู่เดิม เพื่อป้องกันสาเหตุ และ/หรือดำเนินการมิให้เกิดผลกระทบที่รุนแรง โดยแต่ละกิจกรรมที่แสดงนั้น จะต้องใส่หมายเลขกำกับว่า กิจกรรมนั้นๆ สามารถช่วยแก้ไข/มีส่วนช่วยป้องกันสาเหตุ/แก้ไขผลกระทบเรื่องใด พร้อมทั้งระบุผู้ที่รับผิดชอบ/หน่วยงานที่รับผิดชอบกิจกรรมนั้นๆ (Task Owner) เพื่อดำเนินการ และติดตามผลการดำเนินงานต่อไป



แผนภาพที่ 3.14 Bow Tie Diagram กล่องหมายเลข 7 ระดับคะแนนของความเสี่ยงก่อนมีมาตรการใหม่

กล่องหมายเลข 7 แสดงระดับคะแนนของความเสี่ยงที่เหลืออยู่ภายใต้กลไกเดิมที่มีอยู่ก่อนการดำเนินการตามมาตรการใหม่ โดยแสดงระดับของผลกระทบ (Impact) เป็นตัวเลข (1-8) ระดับโอกาสการเกิดขึ้น (1-8) ระดับคะแนนความเสี่ยงที่เป็นผลคูณระหว่างผลกระทบและโอกาสการเกิดขึ้น ซึ่งเป็นระดับคะแนนที่ผ่านการพิจารณาของคณะกรรมการจัดการความเสี่ยง การระบุระดับคะแนนนี้มีวัตถุประสงค์เพื่อประกอบการพิจารณา การวิเคราะห์และเชื่อมโยงในส่วนของการกำหนดเป้าหมาย/แผนงานในส่วนที่เกี่ยวข้องต่อไป

8. ระดับคะแนนของความเสี่ยงหลังจากได้ดำเนินการจัดการความเสี่ยงตามมาตรการที่กำหนด “After”Mitigation)

แผนภาพที่ 3.15 Bow Tie Diagram กล่องหมายเลข 8 ระดับคะแนนของความเสี่ยงหลังจากได้ดำเนินการตามมาตรการที่กำหนด

กล่องหมายเลข 8 แสดงระดับคะแนนของความเสี่ยงหลังจากที่ได้ดำเนินการตามมาตรการใหม่ในการลด/ควบคุมความเสี่ยงไปช่วงระยะเวลาหนึ่งแล้ว โดยแสดงระดับของผลกระทบ (Impact) เป็นตัวเลข (1-8) ระดับโอกาสการเกิดขึ้น (1-8) ระดับคะแนนความเสี่ยงที่เป็นผลคูณระหว่างผลกระทบและโอกาสการเกิดขึ้น ซึ่งเป็นระดับคะแนนที่ผ่านการพิจารณาของคณะกรรมการจัดการความเสี่ยง (ความถี่ในการประเมิน เป็นไปตามที่คณะกรรมการจัดการความเสี่ยงกำหนด) มีวัตถุประสงค์เพื่อประกอบการพิจารณา การวิเคราะห์และเชื่อมโยงต่อไป

(3.3) การประเมินความเสี่ยง (Risk Evaluation) [5.4.4]

เป้าหมายของการประเมินความเสี่ยงจะบ่งบอกถึงระดับความเสี่ยง (Degree of Risk) ซึ่งเป็นสถานะของความเสี่ยงที่ได้จากการวิเคราะห์ผลกระทบและโอกาสของแต่ละปัจจัยเสี่ยง ซึ่งแบ่งเป็นระดับ เช่น ต่ำ-กลาง-สูง-สูงมาก องค์กรจะเป็นผู้พิจารณาระดับความสำคัญของความเสี่ยงเพื่อนำมาดำเนินการจัดการความเสี่ยง

การประเมินความเสี่ยงระดับองค์กรของ สวทช. จะใช้กลุ่มผู้บริหารระดับสูงทำหน้าที่ในการประเมินและพิจารณาถึงเหตุการณ์ที่อาจจะเกิดขึ้น ที่อาจจะมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กรที่ตั้งไว้ ผู้บริหารจะเป็นผู้ประเมินโดยพิจารณาเป็น 2 มิติ คือ ประเมินว่าแต่ละปัจจัยเสี่ยงนั้นมีโอกาสที่จะเกิดมากน้อยเพียงใด และหากเกิดขึ้นแล้วจะส่งผลกระทบต่อองค์กรรุนแรงเพียงใด และนำมาจัดลำดับว่า ปัจจัยเสี่ยงมีความสำคัญมากน้อยกว่ากัน เพื่อจะได้กำหนดมาตรการจัดการกับปัจจัยเสี่ยงเหล่านั้นได้อย่างเหมาะสม

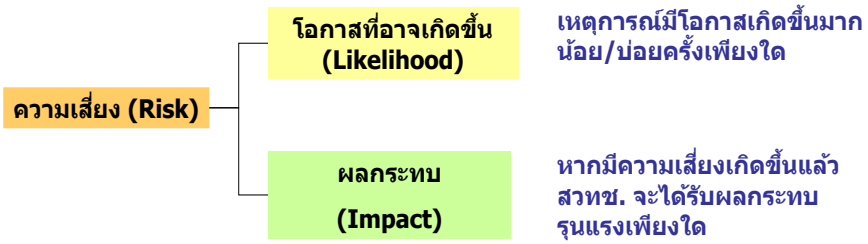
กระบวนการประเมินความเสี่ยงของ สวทช. จะทำการวิเคราะห์โอกาสที่จะเกิดเหตุการณ์ความเสี่ยง (Likelihood) และผลกระทบ (Impact) อันเนื่องมาจากความเสี่ยง

โอกาสที่จะเกิด (Likelihood) หมายถึง การประเมินโอกาส ของการที่แต่ละเหตุการณ์จะเกิดขึ้น โดยการพิจารณาจากสถิติการเกิดเหตุการณ์ในอดีต ปัจจุบัน หรือ การคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต

ผลกระทบ (Impact) หมายถึง ความเสียหายที่จะเกิดขึ้น หากความเสี่ยงนั้นเกิดขึ้น เป็นการพิจารณาระดับความรุนแรงและมูลค่าความเสียหายจากความเสี่ยงที่คาดว่าจะได้รับ

ระดับความเสี่ยง (Risk Level) กำหนดค่าเท่ากับผลคูณของระดับโอกาสที่ความเสี่ยงอาจเกิดขึ้น (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) อันเนื่องมาจากความเสี่ยง อ้างอิง ISO31000:2009

ระดับความเสี่ยง (Risk Level) = ระดับโอกาสที่จะเกิด (Likelihood) × ระดับผลกระทบ (Impact)



แผนภาพที่ 3.16 การวิเคราะห์และประเมินความเสี่ยงพิจารณาจากโอกาสที่จะเกิดและผลกระทบ

แนวทางในการประเมินความเสี่ยง

1. ในการประเมินความเสี่ยง ผู้บริหารจะพิจารณาทั้งเหตุการณ์ที่คาดว่าจะเกิดและจะมีผลกระทบต่อการบรรลุวัตถุประสงค์ รวมทั้งพิจารณาผลกระทบทั้งในเชิงบวกและเชิงลบจากเหตุการณ์ที่อาจจะเกิดขึ้น

2. เทคนิคการประเมินความเสี่ยงมีทั้งวิธีการเชิงคุณภาพและวิธีการเชิงปริมาณ ผู้บริหารจะใช้การประเมินเชิงปริมาณเป็นหลักเพราะมีความชัดเจนและสามารถจับต้องได้มากกว่า กรณีที่รายการความเสี่ยงนั้นไม่สามารถเก็บข้อมูลเชิงปริมาณเพื่อประกอบการประเมินได้ จะใช้การประเมินเชิงคุณภาพประกอบการพิจารณา

3. การประเมินความเสี่ยงควรเริ่มต้น และสิ้นสุด ด้วยวัตถุประสงค์ที่เฉพาะเจาะจงขององค์กร หรือหน่วยงาน วัตถุประสงค์เหล่านี้จะใช้เป็นพื้นฐานในการประเมินโอกาส (Likelihood) และผลกระทบ (Impact) ของความเสี่ยง

4. การประเมินความเสี่ยงสามารถทำได้ในหลายระดับขององค์กร ศูนย์แห่งชาติ ฝ่าย/งาน หน่วยวิจัย โปรแกรมวิจัย จึงควรพิจารณาว่าการประเมินความเสี่ยงประเภทใดตรงกับวัตถุประสงค์ขององค์กร (Objectives) และลำดับความสำคัญ (Priorities) ความเสี่ยงที่มีโอกาสจะเกิดขึ้นสูง และส่งผลกระทบต่อองค์กรอย่างมาก จำเป็นต้องได้รับการพิจารณาบริหารจัดการความเสี่ยงนั้นๆ เป็นลำดับแรก และลดหลั่นลงมาตามลำดับ

การประเมินความเสี่ยง (Risk Assessment)

การประเมินระดับโอกาสที่ความเสี่ยงอาจเกิดขึ้น (Likelihood) และประเมินระดับความรุนแรงของผลกระทบ (Impact) ที่เกิดจากความเสี่ยง มีแนวทาง ดังนี้

1. การประเมินโอกาสการเกิด (Likelihood) ในการประเมินโอกาสของเหตุการณ์ที่อาจจะเกิดขึ้นจะพิจารณาจากสถิติการเกิดเหตุการณ์ในอดีต ปัจจุบัน หรือ การคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต โดยทั่วไปการหาข้อมูลมาทำการสนับสนุนการประมาณโอกาสการเกิดที่ถูกต้องเป็นไปได้ยาก ในกรณีที่สามารถหาข้อมูลที่เกี่ยวกับเหตุการณ์ความล้มเหลวหรือความถี่ที่เกิดขึ้นในอดีต ต้องมีความมั่นใจในฐานข้อมูลดังกล่าวว่าสามารถบ่งชี้ถึงความเป็นไปได้ของเหตุการณ์ในอนาคตได้

การประเมินระดับโอกาส สามารถกำหนดจากสถิติเกิดเหตุการณ์ในอดีต ปัจจุบัน หรือ การคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต เช่น จำนวนการเกิดขึ้นของสาเหตตาม Bow Tie Diagram , ความถี่ในการเกิดขึ้นของปัจจัยเสี่ยงนั้นๆ ฯลฯ การประเมินระดับโอกาสขึ้นอยู่กับระยะเวลาที่นำมาพิจารณา ดังนั้นผู้บริหารต้องมีความชัดเจนในการกำหนดระยะเวลาที่จะใช้ในการพิจารณา โดยไม่ควรละเลยความเสี่ยงที่อาจจะเกิดขึ้นในระยะยาว

2. การประเมินผลกระทบ (Impact) พิจารณาตามประเภทความเสี่ยง คือ ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ความเสี่ยงด้านปฏิบัติการ (Operational Risk) ความเสี่ยงทางด้านการเงิน (Financial Risk) และความเสี่ยงทางด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk) ซึ่งการพิจารณาผลกระทบนั้นจะพิจารณ์ตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI) ที่สอดคล้องกับประเภทของรายการความเสี่ยง

(3.4) ตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI)

คือ มาตรวัดหรือจุดเตือนภัย (Trigger Point) ของความเสี่ยง โดยเบื้องต้นมีตัวอย่างมุมมองและตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI) เพื่อเป็นทางเลือก สำหรับการประเมินแต่ละประเภทไว้ดังนี้

ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

ประเด็นความเสี่ยง	ตัวอย่างตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI)
1). การบรรลุผลสำเร็จตามเป้าหมายในวัตถุประสงค์เชิงยุทธศาสตร์	ความสามารถในการปฏิบัติตามแผน
2). การบรรลุผลสำเร็จตามเป้าหมายในภาพรวม หรือตาม KPI ที่เกี่ยวข้อง หรือวัดผลการดำเนินงานตาม Bow Tie Diagram	ผลการดำเนินงานตามเป้าหมายตัวชี้วัด
3). ความพึงพอใจของผู้ใช้บริการ	ระดับความพึงพอใจของผู้ใช้บริการ
4).ความน่าเชื่อถือ และไว้วางจากจากหน่วยงานอื่น ผู้ใช้ ลูกค้า (รายยุทธศาสตร์)	จำนวนลูกค้าที่กลับมาใช้

ตารางที่ 3.2 แสดงตัวอย่างตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)

ความเสี่ยงด้านปฏิบัติการ (Operational Risk)

ประเด็นความเสี่ยง	ตัวอย่างตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI)
1) ขีดความสามารถของพนักงาน	ความสอดคล้องของผลประเมินขีดความสามารถกับมาตรฐานตำแหน่ง
2) อัตรากำลังเทียบกับตำแหน่งงาน	อัตรากำลังที่เทียบกับตำแหน่งงานที่มีอยู่ในปัจจุบัน
3) ผลการดำเนินงานเป็นไปตามเป้าหมาย (รายโครงการ/ตาม Gantt chart)	ผลการดำเนินงานตามแผนงาน/โครงการ
4) ความพึงพอใจของผู้ใช้บริการ	ระดับความพึงพอใจของผู้ใช้บริการ
5) ผลการดำเนินงานตาม SLA โดยกำหนด	ผลการดำเนินงานตาม SLA
6) การส่งรายงาน Final report	การส่ง Final Report ได้ตามระยะเวลา
7) ความปลอดภัยในการปฏิบัติงาน	การเกิดอุบัติเหตุจากการปฏิบัติงาน
8) ความเพียงพอของบุคลากร	Turnover rate ของบุคลากร
9) จำนวนชั่วโมงที่ระบบไม่สามารถให้บริการได้เนื่องจากระบบถูกละเมิดหรือโจมตีสำเร็จและเกิดความเสียหายต่อองค์กร (ครอบคลุม	จำนวนชั่วโมง/ปีที่ไม่สามารถให้บริการได้ (Downtime)

ประเด็นความเสี่ยง	ตัวอย่างตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI)
ระบบและทุก Public web ที่ hosting อยู่ที่ สวทช.)	
10) ความมั่นคงปลอดภัยของข้อมูลสำคัญ	ระยะเวลาการกู้คืนข้อมูล

ตารางที่ 3.3 แสดงตัวอย่างตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI) ความเสี่ยงด้านปฏิบัติการ (Operational Risk)

ความเสี่ยงด้านการเงิน (Financial Risk)

ประเด็นความเสี่ยง	ตัวอย่างตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI)
1) รายได้ไม่น้อยกว่าค่าใช้จ่าย	สัดส่วนรายได้รวมต่อค่าใช้จ่ายรวม
2) รายได้ไม่เป็นไปตามเป้าหมายที่กำหนด	รายได้อุดหนุนวิจัย รับจ้างวิจัย ร่วมวิจัย และรายได้จากผลงานวิจัยและองค์ความรู้

ตารางที่ 3.4 แสดงตัวอย่างตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI) ความเสี่ยงด้านการเงิน (Financial Risk)

ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk)

ประเด็นความเสี่ยง	ตัวอย่างตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI)
1) การจ่ายค่าเสียหาย / ค่าปรับจากการผิดสัญญา	ค่าเสียหายที่ต้องจ่าย
2) ด้านชื่อเสียง ภาพลักษณ์องค์กร โดยกำหนดข่าวเชิงลบ การปรากฏในสื่อมวลชนและสื่อสังคม (FB, Social Network etc.)	ระยะเวลาการแก้ไข
3) จำนวนครั้งที่ไม่ปฏิบัติตามกฎระเบียบทั้งภายในและภายนอก	จำนวนครั้งที่พบการไม่ปฏิบัติตามกฎระเบียบทั้งภายในและภายนอก
4) การปฏิบัติตามกฎหมาย กฎ ระเบียบข้อบังคับ (ภายใน และภายนอก)	ระดับความเสียหายจากการไม่ปฏิบัติตามกฎหมาย กฎ ระเบียบข้อบังคับ (ภายในและภายนอก)
5) ความพึงพอใจของผู้ใช้บริการ	ระดับความพึงพอใจของผู้ใช้บริการ

ตารางที่ 3.5 แสดงตัวอย่างตัวชี้วัดระดับความเสี่ยง Key Risk Indicator (KRI) ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk)

แนวทางการกำหนดตัวชี้วัดระดับความเสี่ยง (Key risk indicator : KRI)

1. ทำความเข้าใจกับสาเหตุของการเกิดความเสี่ยงด้วยการตรวจสอบและวิเคราะห์ข้อมูลในอดีตที่เกี่ยวข้องกับความเสี่ยงเพื่อค้นหากระบวนการ กิจกรรม ที่ก่อให้เกิดเหตุ

2. ตรวจสอบแผนกลยุทธ์ วัตถุประสงค์การดำเนินงาน ดัชนีชี้วัดของผลการดำเนินงาน (Key Performance indicator : KPI) เพราะ KPI สามารถทำหน้าที่เป็น KRI เพราะจะชี้วัดความเสี่ยงที่สะท้อนการดำเนินงานทางลบ

3. ตรวจสอบนโยบาย กฎระเบียบ ข้อบังคับที่เกี่ยวข้อง ธุรกรรมทั้งหมดที่เกี่ยวข้องกับกฎเกณฑ์ได้ดำเนินการอยู่ภายใต้การปฏิบัติครบถ้วนหรือไม่

4. ตรวจสอบความต้องการ ข้อกำหนดของผู้มีส่วนได้ส่วนเสียที่นอกเหนือไปจากกฎระเบียบ ข้อบังคับ โดยอาจจะหมายถึงลูกค้า นำข้อมูลส่วนนี้มาใช้ประกอบการพัฒนา/กำหนด KRI

5. การกำหนดตัวชี้วัดความเสี่ยง KRI (Key Risk Indicator) กำหนดได้ตามความเหมาะสมของแต่ละรายการความเสี่ยง ทั้งนี้ขึ้นอยู่กับดุลยพินิจของผู้รับผิดชอบความเสี่ยง (Risk Owner)

(3.5) แนวทางการกำหนดระดับความเสี่ยงที่รับได้ (Acceptable Risk Level)

การประเมินความเสี่ยง (Risk assessment) เป็นเครื่องมือที่สำคัญสำหรับผู้บริหาร เพราะช่วยในการพิจารณากลยุทธ์และนโยบายขององค์กรว่าจัดอยู่ในทิศทางใด กลยุทธ์และนโยบายดังกล่าวยอมรับความเสี่ยงที่อาจจะเกิดขึ้นได้มากน้อยเพียงใด รวมถึงความเสี่ยงที่ระบุนั้นมีความสอดคล้องกับกลยุทธ์และนโยบายขององค์กรอย่างไร โดยองค์กรสามารถกำหนดค่าระดับความเสี่ยงที่องค์กรต้องการ Risk Appetite (RA) และค่าระดับความเสี่ยงที่ยังคงอยู่ในระดับที่องค์กรยังสามารถรับได้ Risk Tolerance (RT) จากข้อมูลประกอบการประเมิน ซึ่งค่าดังกล่าวจะช่วยในการคัดเลือกและจัดลำดับการดำเนินการที่เหมาะสมในการลดและควบคุมความเสี่ยง

ค่าระดับความเสี่ยงที่องค์กรต้องการ Risk Appetite (RA)

คือ ค่าระดับความเสี่ยงในเชิงปริมาณหรือเชิงคุณภาพที่องค์กรสามารถยอมรับความเสียหาย/สูญเสียจากความเสี่ยง โดยกำหนดให้สอดคล้องกับเป้าหมายกลยุทธ์ประจำปี ซึ่งสามารถระบุเป็นค่าเป้าหมายค่าเดียวหรือระบุเป็นช่วงก็ได้ ขึ้นอยู่กับความเหมาะสม โดยคณะกรรมการจัดการความเสี่ยงยอมรับได้ในการดำเนินการเพื่อให้บรรลุวัตถุประสงค์หรือนโยบายขององค์กร

ค่าระดับความเสี่ยงที่องค์กรยอมรับได้ Risk Tolerance (RT)

คือ ค่าเบี่ยงเบนสูงสุด/ต่ำสุดของระดับความเสี่ยงที่องค์กร/SBU/โปรแกรมหลัก โครงการ/ส่วนงานยอมรับได้จากเป้าหมายหรือวัตถุประสงค์ที่กำหนดไว้ ในกรณีเหตุการณ์ที่ไม่สามารถคาดการณ์ล่วงหน้า/เป็นเหตุการณ์ฉุกเฉิน ซึ่งการกำหนดระดับค่าเบี่ยงเบนจะต้องกำหนดโดยคณะกรรมการจัดการความเสี่ยง

หลักการของการกำหนด Risk Appetite และ Risk Tolerance

1. การระบุ Risk Appetite และ Risk Tolerance ต้องแสดงให้เห็นถึงความเชื่อมโยง/ความสอดคล้องกับเป้าหมาย/วัตถุประสงค์ขององค์กรได้อย่างชัดเจน (Business Objective)

2. ควรมีวิธีการเก็บรวบรวมข้อมูลและเป้าหมายของการวัดความเสี่ยงที่ชัดเจน ไม่ควรนำปัญหาในการปฏิบัติงานประจำวัน ปัญหาที่เกิดจากโครงการหรือกิจกรรมที่เกิดขึ้นแบบฉุกเฉินหรือสั่งการตามนโยบายแบบโครงการชั่วคราว เพราะสิ่งนี้จะหมดไปตามนโยบาย แต่ควรเก็บข้อมูลปัจจัยที่ส่งผลกระทบความสำเร็จขององค์กร หรือโครงการขนาดใหญ่ที่ส่งผลกระทบกับองค์กรถ้าโครงการนี้ไม่ประสบความสำเร็จตามระยะเวลาที่กำหนด เป็นต้น

3. ต้องคำนึงถึงมุมมองที่แตกต่างของกลยุทธ์และยุทธวิธีในระดับปฏิบัติงาน เพราะการกำหนดเกณฑ์ระดับความเสี่ยงที่ยอมรับได้ โดยเกณฑ์นี้จะต้องสามารถปฏิบัติได้จริง และมีความชัดเจนในเชิงปริมาณ และที่สำคัญสามารถปรับเปลี่ยนได้ตามระยะเวลา และเงื่อนไขที่เปลี่ยนแปลงได้โดยคณะกรรมการจัดการความเสี่ยง

4. ต้องบูรณาการกับวัฒนธรรมการควบคุมขององค์กร รวมทั้งคุณลักษณะและวิธีการที่ใช้ควบคุมความเสี่ยงขององค์กร ดังนั้นผู้มีหน้าที่รวบรวมข้อมูลปัจจัยเสี่ยง จะต้องมีการศึกษาเกี่ยวกับกฎ ระเบียบองค์กร เพื่อไม่ให้เกิดการขัดแย้งขึ้น หรือซ้ำซ้อนกัน เป็นต้น

(3.6) เกณฑ์การประเมินค่าความเสี่ยง (Risk Assessment Criteria)

สวทช. กำหนดระดับเกณฑ์การประเมิน [ระดับโอกาสที่ความเสี่ยงอาจเกิดขึ้น (Likelihood) × ระดับความรุนแรงของผลกระทบ (Impact)] เป็น 8×8 โดยมีแนวทางการกำหนดเกณฑ์การประเมินทั้ง 2 มิติ ดังนี้

1. เกณฑ์การประเมินโอกาสการเกิด (Likelihood) จะพิจารณาจากสถิติการเกิดเหตุการณ์ในอดีต ปัจจุบัน หรือ การคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต แล้วนำมากำหนดเป็นค่าและคำอธิบายของระดับคะแนน 1-8 ตามรายละเอียดใน แผนภาพที่ 3.17 เกณฑ์ประเมินโอกาสการเกิด (Likelihood)

มุมมอง/ตัวชี้วัด	ความถี่ในการเกิดขึ้น
คะแนน	• ..... • .....
8 โอกาสเกิดเป็นความเสี่ยงแน่นอน	
7 โอกาสเกิดเป็นความเสี่ยงสูงมาก	
6 โอกาสเกิดเป็นความเสี่ยงสูง	
5 โอกาสเกิดเป็นความเสี่ยงปานกลาง	
4 ค่าเบี่ยงเบนจากเป้าหมายที่องค์กรยอมรับได้	
3 ค่าเป้าหมายที่องค์กรกำหนด	
2 โอกาสเกิดเป็นความเสี่ยงน้อย	
1 โอกาสเกิดเป็นความเสี่ยงน้อยมาก	

แผนภาพที่ 3.17 เกณฑ์ประเมินโอกาสการเกิด (Likelihood)

2. เกณฑ์การประเมินผลกระทบ (Impact) ของความเสี่ยงแบ่งการพิจารณาตามประเภทความเสี่ยง คือ ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ความเสี่ยงด้านปฏิบัติการ (Operational Risk) ความเสี่ยงทางด้านการเงิน (Financial Risk) และความเสี่ยงทางด้านการปฏิบัติตามกฎระเบียบ (Compliance Risk) จะพิจารณาเงื่อนไขตามมุมมอง เช่น ความสามารถในการบรรลุวัตถุประสงค์, Turnover rate ของบุคลากร, จำนวนชั่วโมงที่ระบบไม่สามารถให้บริการได้เนื่องจากระบบถูกละเมิดหรือโจมตีสำเร็จ และเกิดความเสียหายต่อองค์กร เป็นต้น แล้วนำมากำหนดเป็นค่าและคำอธิบายของระดับคะแนน 1-8 ตามรายละเอียดในแผนภาพที่ 3. 18 เกณฑ์ประเมินผลกระทบ (Impact)

SOFC	Strategic Risk	Operational Risk	Financial Risk	Compliance Risk
มุมมอง/ตัวชี้วัด คะแนน	•	•	•	• .....
8 วิกฤต				
7 เสียหายรุนแรง/สูงมาก				
6 เสียหายสูง				
5 เสียหายปานกลาง				
4 ค่าเบี่ยงเบนจากเป้าหมายที่องค์กรยอมรับได้				
3 ค่าเป้าหมายที่องค์กรกำหนด				
2 ดีกว่าเป้าหมายอย่างมีนัยสำคัญ				
1 ดีกว่าเป้าหมายเป็นอย่างมาก				

แผนภาพที่ 3.18 เกณฑ์ประเมินผลกระทบ (Impact)

คณะกรรมการจัดการความเสี่ยงจะพิจารณาค่าและคำอธิบายของระดับโอกาสการเกิด (Likelihood) และระดับผลกระทบ (Impact) ของระดับคะแนน 1-8 โดยอาจมีการเปลี่ยนแปลงได้ ขึ้นอยู่กับความเหมาะสมของสถานการณ์ในขณะนั้น

แนวทางการประเมินความเสี่ยง

เมื่อผู้รับผิดชอบความเสี่ยง (Risk owner) ดำเนินการวิเคราะห์ความเสี่ยงด้วย Bow Tie Diagram แล้ว จะต้องดำเนินการประเมินระดับคะแนนของโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) ตามเกณฑ์การประเมินที่กำหนด โดยสามารถประเมินความเสี่ยงตามแนวทางการประเมิน ดังนี้

แผนภาพที่ 3.19 แนวทางการประเมินความเสี่ยง

จากแผนภาพที่ 3.19 แนวทางการประเมินความเสี่ยง ในขั้นตอนที่ 2 เมื่อผู้รับผิดชอบความเสี่ยง (Risk owner) วิเคราะห์ความเสี่ยงแล้วบันทึกข้อมูลลงใน Bow Tie Diagram กล่อง 2-5 แล้ว ขั้นตอนที่ 3 ผู้รับผิดชอบความเสี่ยง (Risk owner) จะต้องกำหนดตัวชี้วัดระดับความเสี่ยง (Key risk indicator) ที่เหมาะสม เพื่อประเมินระดับโอกาส (likelihood) และระดับผลกระทบ (Impact), กำหนด Risk Appetite , Risk Tolerance และระบุ Mitigation Action ใน Bow Tie Diagram กล่อง 6 โดยจะต้องพิจารณาระดับโอกาสการเกิด (Likelihood) และระดับผลกระทบ (Impact) ดังนี้

1. การพิจารณาระดับโอกาสการเกิด (Likelihood) กำหนดให้พิจารณาระดับโอกาสการเกิด (Likelihood) ในมุมมองความถี่ในการเกิดขึ้นของสาเหตุตามที่ระบุใน Bow Tie Diagram กล่อง 2 ทั้งนี้ความถี่ที่เกิดขึ้นดังกล่าว ควรจะสามารถบ่งชี้ความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้นในอนาคตได้

2. การพิจารณาระดับผลกระทบ (Impact) จะพิจารณาผลกระทบที่คาดว่าจะเกิดขึ้น ในมุมมองของผลกระทบตามที่ระบุใน Bow Tie Diagram กล่อง 3 เปรียบเทียบกับเกณฑ์ระดับคะแนน 1-8 ตามคำอธิบายที่กำหนด

3. นำระดับคะแนนโอกาสการเกิด (Likelihood) × ระดับคะแนนผลกระทบ (Impact) = ระดับคะแนนความเสี่ยง (สูงมาก, สูง, กลาง, ต่ำ)

4. การประเมินระดับความเสี่ยงทั้งก่อนการจัดการความเสี่ยง (Before mitigation) การกำหนดเป้าหมาย และผลหลังการจัดการความเสี่ยง (After mitigation) จะใช้วิธีการเดียวกันแตกต่างกันที่ระยะเวลาที่ทำการประเมิน

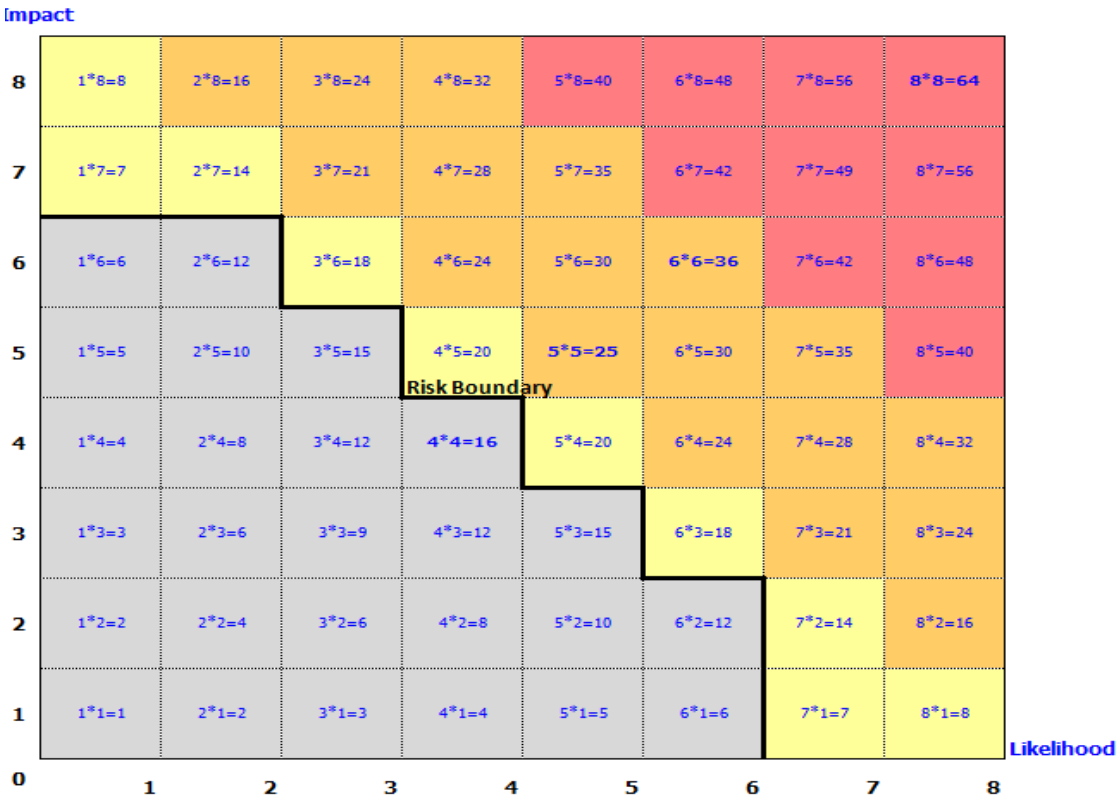
- ก่อนการจัดการความเสี่ยง (Before mitigation)
- การกำหนดเป้าหมาย
- หลังการจัดการความเสี่ยง (After mitigation)

5. เมื่อประเมินระดับความเสี่ยงเรียบร้อยแล้ว ผู้รับผิดชอบความเสี่ยง (Risk owner) จะต้องเสนอผลการประเมินให้คณะกรรมการจัดการความเสี่ยงพิจารณาให้ข้อคิดเห็น

6. ดำเนินการจัดการความเสี่ยงตามแนวทางการตอบสนองความเสี่ยงแต่ละระดับ

(3.7) การแสดงผลการประเมินความเสี่ยงด้วยผังภูมิความเสี่ยง (Risk Profile)

เมื่อประเมินโอกาสการเกิดและผลกระทบเสร็จแล้วจะคำนวณคะแนนรวมความเสี่ยงจากผลคูณของระดับโอกาส และระดับผลกระทบ แล้วนำมาจัดลำดับความเสี่ยงโดยใช้แผนภูมิแสดงความเสี่ยง (Risk Profile) ในการแสดงผล เพื่อให้เห็นระดับของความเสี่ยง (Level of Risk) หรือขนาดความสูญเสียที่ต้องเผชิญ เพื่อให้ทราบว่าความเสี่ยงแต่ละรายการจัดอยู่ในประเภทความเสี่ยงระดับสูงมาก (สีแดง) ระดับสูง (สีส้ม) ระดับปานกลาง (สีเหลือง) หรือระดับต่ำ (สีเทา) ซึ่งจะช่วยในการตัดสินใจว่าจะกำหนดแนวทางในการบริหาร ควบคุม ป้องกัน หรือลดความเสี่ยงอย่างไร ตลอดจนใช้เพื่อพิจารณาว่าความเสี่ยงใดที่ต้องได้รับการจัดการในลำดับแรกๆ เมื่อเทียบกับเกณฑ์หรือดัชนีความเสี่ยงของกิจกรรมหรือวัตถุประสงค์ที่กำหนดไว้



แผนภาพที่ 3.20 ผังภูมิความเสี่ยง (Risk Profile: RP)

ผังภูมิความเสี่ยง (Risk Profile: RP) จะช่วยให้มองเห็นความสัมพันธ์ของระดับโอกาสการเกิดกับระดับผลกระทบ (ภาคผนวก ช)

ในผังภูมิความเสี่ยง (Risk Profile: RP) ของ สวทช. ได้กำหนดระดับความเสี่ยง ไว้ดังนี้

- ระดับสูงมาก (Very high) - สีแดง
- ระดับสูง (High) - สีส้ม
- ระดับปานกลาง (Medium) - สีเหลือง
- ระดับต่ำ (Low) - สีเทา

ผลการประเมินความเสี่ยงที่นำมาจัดลำดับความเสี่ยงและนำเสนอในรูปของแผนภูมิผังภูมิความเสี่ยง (Risk Profile: RP) จะช่วยให้เห็นภาพรวมของความเสี่ยง (Portfolio view of risk) ของทั้งองค์กร ที่พร้อมจะนำมาใช้วิเคราะห์ต่อและยังช่วยในการกำหนดว่า Risk area ใดที่มีความเสี่ยงสูงอย่างมีนัยสำคัญ และคณะกรรมการจัดการความเสี่ยงของ สวทช. ติดตามผลการบริหารจัดการความเสี่ยงทุกไตรมาส รวมทั้งการพิจารณาทางเลือกในการบริหารจัดการความเสี่ยงดังกล่าวต่อไป

ขอบเขตของคะแนนระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Boundary)

คือ ขอบเขตของคะแนนระดับความเสี่ยงที่องค์กรยอมรับได้ ซึ่งองค์กรกำหนดให้มีเส้นแบ่งระหว่างระดับปานกลาง (Medium) สีเหลือง กับระดับต่ำ (Low) สีเทา แสดงตามแผนภาพที่ 3. 20 ผังภูมิความเสี่ยง (Risk Profile: RP)

(4) การจัดการความเสี่ยง (Risk Treatment/Risk Mitigation) [5.5]

แนวทางการจัดการความเสี่ยง

การกำหนดแนวทางการจัดการความเสี่ยงเป็นการระบุทางเลือกที่เหมาะสมและนำไปปฏิบัติเป็นส่วนหนึ่งของแผนการบริหารจัดการความเสี่ยงขององค์กรได้ ซึ่งต้องประเมินผลต่อการลดโอกาสหรือผลกระทบของความเสี่ยง รวมทั้งต้นทุนและประโยชน์ที่ได้รับ เพื่อให้ความเสี่ยงที่เหลืออยู่ภายในช่วงเบี่ยงเบนจากเป้าหมายที่องค์กรยอมรับได้ Risk Tolerance ทั้งนี้องค์กรได้กำหนดแนวทางในการตอบสนองต่อความเสี่ยง (Risk Mitigation Options) ดังนี้

- **การยอมรับ (Accept / Take)** ยอมรับความเสี่ยงที่เกิดจากการปฏิบัติงานและภายใต้ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้

- **การลด (Reduce / Treat)** การดำเนินการเพิ่มเติมเพื่อลดโอกาสเกิด หรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เป็นการลดความถี่หรือโอกาสที่จะเกิด (Likelihood) ความเสี่ยง หรือการลดผลกระทบ (Impact) หรือความเสียหายที่จะเกิดขึ้น โดยการควบคุมภายใน หรือปรับปรุงเปลี่ยนแปลงการดำเนินงานเพื่อช่วยลดโอกาสที่จะเกิดความเสียหาย ลดความเสียหายหรือทั้งสองอย่าง เช่น การฝึกอบรมให้กับพนักงาน การจัดทำคู่มือการปฏิบัติงาน การจัดทำแผนสำรองเพื่อรับมือไว้ล่วงหน้าก่อนที่ความสูญเสียจะเกิดขึ้นจริง ซึ่งจะช่วยให้เกิดการตระหนักถึงความเสี่ยงและช่วยให้ลดระดับความรุนแรงของความสูญเสียลง

- **การหลีกเลี่ยง (Avoid / Terminate)** การดำเนินการเพื่อยกเลิกหรือหลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง ทั้งนี้หากทำการใช้กลยุทธ์นี้อาจต้องทำการพิจารณาวัตถุประสงค์ว่าสามารถบรรลุได้หรือไม่ เพื่อทำการปรับเปลี่ยนต่อไป

- **การร่วมจัดการ (Share / Transfer)** การร่วมจัดการโดยแบ่งความเสี่ยงบางส่วนกับบุคคลหรือองค์กรอื่น

(4.1) ขั้นตอนการจัดการความเสี่ยงของ สวทช.

เมื่อผู้รับผิดชอบความเสี่ยง (Risk owner) ใช้ Bow Tie Diagram ในการวิเคราะห์ความเสี่ยงและประเมินระดับความเสี่ยงตามเกณฑ์การประเมินที่กำหนดแล้ว ผู้รับผิดชอบความเสี่ยง (Risk owner) จะต้องพิจารณาหาแนวทาง วิธีการหรือมาตรการเพิ่มเติมที่เหมาะสมสำหรับใช้จัดการความเสี่ยงโดยการจัดทำแผนบริหารจัดการความเสี่ยง (Risk Mitigation Plan) สามารถดำเนินการตามแนวทางตอบสนองความเสี่ยงแต่ละระดับ ดังนี้

ความเสี่ยงระดับสูงมาก (Very high)

ผู้รับผิดชอบความเสี่ยง (Risk owner) จะต้องกำหนดแผนลดความเสี่ยง โดยจัดสรรทรัพยากรและกำหนดมาตรการให้มีความสมเหตุสมผล (validity) และมีความเพียงพอ (sufficience) เพื่อลดความเสี่ยงอย่างเร่งด่วนและดำเนินการให้สามารถลดระดับความเสี่ยงได้ภายในเวลาที่กำหนด หรืออาจจะต้องถ่ายโอนความเสี่ยง

การโอนย้าย/แบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น การจ้างบุคคลภายนอกมาดำเนินการแทน การทำประกันภัย

การลดความเสี่ยง ผู้รับผิดชอบความเสี่ยง (Risk Owner) จะต้องจัดทำแผนลดความเสี่ยงโดยกำหนดวิธีการดำเนินงาน (ขั้นตอน, กระบวนการ) กำหนดหน่วยงานหรือบุคคลที่จะเป็นผู้รับผิดชอบ กำหนดระยะเวลาแล้วเสร็จ และสามารถวัดและประเมินระดับของความเสี่ยงที่ลดลงภายหลังการดำเนินการตามแผนแล้วได้

ความเสี่ยงระดับสูง (High)

จะต้องมีแผนลดความเสี่ยง โดยจัดสรรทรัพยากรและกำหนดมาตรการให้มีความสมเหตุสมผลและเพียงพอ เพื่อลดความเสี่ยง เพื่อให้ความเสี่ยงลดลงให้อยู่ในระดับที่ยอมรับได้

ความเสี่ยงระดับปานกลาง (Medium)

จะต้องมีแผนควบคุมความเสี่ยง เพื่อให้มีมาตรการควบคุมเพียงพอและเหมาะสม เช่น การปรับปรุงกระบวนการดำเนินงาน การจัดทำมาตรฐานควบคุมเพื่อให้ความเสี่ยงกลับมาอยู่ในระดับที่ยอมรับได้ โดยวิเคราะห์จากกลไกการปฏิบัติงานปกติเป็นหลักเพื่อหาแนวทางการปรับปรุงกลไกที่มีอยู่เดิมหรือแนวทางที่ต้องการดำเนินการเพิ่มเติมเพื่อควบคุมความเสี่ยงระดับนี้

การควบคุมความเสี่ยง ผู้รับผิดชอบความเสี่ยง (Risk owner) จะใช้ Bow-Tie Diagram เป็นกลไกในการควบคุมความรุนแรงและโอกาสในการเกิดของความเสี่ยงนั้นๆ โดยผู้รับผิดชอบความเสี่ยง (Risk owner) สามารถตัดสินใจใช้กลไกการปฏิบัติงานปกติที่มีอยู่เป็นกลไกในการควบคุมความเสี่ยงระดับนี้ได้ หรือจะจัดทำ

แผนควบคุมความเสี่ยงเพิ่มเติม ทั้งนี้ขึ้นอยู่กับการหารือร่วมกันระหว่างผู้รับผิดชอบความเสี่ยง (Risk owner) และผู้ที่ได้รับมอบหมายให้ทำหน้าที่เป็นผู้รับผิดชอบ (Task owner) ในมาตรการลดความเสี่ยงนั้นๆ

ความเสี่ยงระดับต่ำ (Low)

ยอมรับความเสี่ยงภายใต้การควบคุมที่มีอยู่ในปัจจุบัน ซึ่งความเสี่ยงในระดับนี้จะถือว่ากลไกปฏิบัติงานปกติที่มีอยู่ในปัจจุบันสามารถดูแลระดับความเสี่ยงนี้ได้โดยให้เพิ่มความระมัดระวังในการดำเนินงานตามกลไกปฏิบัติงานปกติ แต่ต้องมีการติดตาม KRI และผลการดำเนินงานตามตัวชี้วัดที่เกี่ยวข้อง อย่างสม่ำเสมอตามกรอบเวลาที่กำหนด

แนวทางบริหารจัดการความเสี่ยงตามระดับความรุนแรง

Very high	จะต้องมี**แผนลด**ความเสี่ยง โดยจัดสรรทรัพยากรและมาตรการให้เพียงพอเพื่อลดความเสี่ยงทันทีและดำเนินการให้สามารถลดระดับความเสี่ยงภายในเวลาที่กำหนด หรืออาจจะต้องถ่ายโอนความเสี่ยง * การโอนย้าย/แบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น การจ้างบุคคลภายนอกมาดำเนินการแทน การทำประกันภัย *
High	จะต้องมี**แผนลด**ความเสี่ยง โดยจัดสรรทรัพยากรและมาตรการให้เพียงพอเพื่อลดความเสี่ยง เพื่อให้ความเสี่ยงลดลงให้อยู่ในระดับที่ยอมรับได้
Moderate	จะต้องมี**แผนควบคุม**ความเสี่ยง เพื่อให้มีการควบคุมเพียงพอและเหมาะสม เช่น การปรับปรุงกระบวนการดำเนินงาน การจัดทำมาตรฐานควบคุม
Low	ยอมรับความเสี่ยงภายใต้การควบคุมที่มีอยู่ในปัจจุบัน ซึ่งความเสี่ยงในระดับนี้จะถือว่ากลไกปฏิบัติงานปกติที่มีอยู่ในปัจจุบันสามารถดูแลระดับความเสี่ยงนี้ได้โดยให้เพิ่มความระมัดระวังในการดำเนินงานตามกลไกปฏิบัติงานปกติ แต่ต้องมีการติดตามผลการดำเนินงานตามตัวชี้วัดที่กำหนด = area of appetite

แผนภาพที่ 3.21 ภาพแสดงแนวทางการบริหารจัดการความเสี่ยงตามระดับความรุนแรง

ดังนั้นในการจัดทำแผนบริหารจัดการความเสี่ยง (Risk Mitigation Plan) อาจจะมีการดำเนินการทั้งแผนลดและแผนควบคุม ความเสี่ยง หรือจะมีเพียงแผนลดความเสี่ยงอย่างเดียวก็ได้ ทั้งนี้ขึ้นอยู่กับการพิจารณาของผู้รับผิดชอบความเสี่ยง (Risk Owner) แต่การเรียกชื่อจะรวมเรียกว่า “แผนบริหารจัดการความเสี่ยง”

(4.2) การวิเคราะห์ Cost-Benefit ในแต่ละทางเลือก

ในการจัดการความเสี่ยงระดับองค์กร (ERM) เมื่อผู้รับผิดชอบความเสี่ยง (Risk owner) กำหนดมาตรการ/กิจกรรมที่ใช้ในการจัดการความเสี่ยงแล้ว จะต้องวิเคราะห์ Cost-Benefit ของแต่ละทางเลือกโดยมีรายละเอียดการวิเคราะห์ตามแผนภาพที่ 3.22 การวิเคราะห์ Cost-Benefit ของแต่ละทางเลือก

การวิเคราะห์ Cost-Benefit ในแต่ละทางเลือก

วัตถุประสงค์ เพื่อระบุแนวทางในการตอบสนองต่อความเสี่ยง (Risk Mitigation Option)

RISK ID : .....

แนวทางในการตอบสนองต่อความเสี่ยง	Mitigation Action Plan	ต้นทุน (Cost)	ประโยชน์ที่ได้รับ (Benefit)	ทางเลือกที่เหมาะสม
Take				
Treat				
Transfer				
Terminate				

ผู้วิเคราะห์ _____

วันที่ _____

แผนภาพที่ 3.22 การวิเคราะห์ Cost-Benefit ของแต่ละทางเลือก

การวิเคราะห์ผลได้ผลเสียของแต่ทางเลือกมีสิ่งที่จะต้องพิจารณาในการวิเคราะห์ คือ

- ผลเสีย (Cost) ได้แก่ ต้นทุน เวลาหรือความสะดวกที่มีโอกาสสูญเสียไปกับความเสี่ยง หรือความเสี่ยงที่จะเกิดขึ้นได้อีกในอนาคต เป็นต้น
- ผลได้ (Benefit) ได้แก่ ผลลัพธ์ในทางบวกที่เกิดขึ้นทันทีที่นำมาตรการนั้นไปลดความเสี่ยง หรือผลประโยชน์ในระยะยาว รวมไปถึงโอกาสดีๆ ในอนาคต เป็นต้น

ดังนั้นในวิเคราะห์ทางเลือกในการจัดการความเสี่ยงจะต้องพิจารณาถึงค่าใช้จ่ายหรือต้นทุนในการจัดการความเสี่ยงกับประโยชน์ที่จะได้ว่าคุ้มค่าหรือไม่ เพราะเป้าหมายของการจัดทำแผนบริหารจัดการความเสี่ยงคือ ลดโอกาสที่จะเกิดความเสี่ยงนั้นๆ ลดความรุนแรงของผลกระทบจากความเสี่ยงนั้นในกรณีที่ความเสี่ยงนั้นเกิดขึ้น และเปลี่ยนลักษณะของผลลัพธ์ที่จะเกิดขึ้นของความเสี่ยงให้เป็นไปในรูปแบบที่องค์กรหรือหน่วยงานต้องการ

ผู้รับผิดชอบความเสี่ยง (Risk Owner) จะต้องวิเคราะห์ Cost-Benefit ของแต่ละทางเลือกโดยมีแนวทางการวิเคราะห์ ดังนี้

1. **การวิเคราะห์ต้นทุน (Cost)** จะพิจารณาจากงบประมาณ และแรงงานที่ต้องใช้ในการดำเนินงานตามมาตรการนั้นๆ (Man-month) โดยมีรายละเอียด ดังนี้

งบประมาณ แบ่งการพิจารณาเป็น 3 ระดับ คือ Low, Medium และ High ซึ่งแต่ละระดับ มีคำอธิบาย ดังนี้

ระดับ	งบประมาณ
Low	ใช้งบประมาณบริหารจัดการปกติ ไม่ต้องจัดหางบประมาณเพิ่ม
Medium	ต้องใช้งบประมาณเพื่อจัดการกับความเสี่ยงเพิ่มเติม < 10% ของงบประมาณที่ตั้งไว้เดิม
High	ต้องใช้งบประมาณเพื่อจัดการกับความเสี่ยงเพิ่มเติม > 10% ของงบประมาณที่ตั้งไว้เดิม

ตารางที่ 3.6 การพิจารณางบประมาณ 3 ระดับ

แรงงาน (Man-month) แบ่งการพิจารณาเป็น 3 ระดับ คือ Low, Medium และ High ซึ่งแต่ละระดับ มีคำอธิบาย ดังนี้

ระดับ	แรงงาน (Man-month)
Low	• ไม่ต้องมีบุคลากรเพิ่มเติม • เป็นงานที่อยู่ในภาระหน้าที่ของหน่วยงาน • มีการแต่งตั้งคณะทำงานที่ต้องดูแลเรื่องการควบคุมหรือลดความเสี่ยงในกิจกรรมนั้นๆ เป็นตัวแทนภายในศูนย์แห่งชาติ/สก./ศจ.
Medium	• มีการสรรหาบุคลากรเพิ่มเติมหรือมีการประสานงานกับหน่วยงานภายใน สวทช. เพื่อจัดให้มีบุคลากรที่ปฏิบัติหน้าที่ในการควบคุมหรือลดความเสี่ยงในกิจกรรมนั้นๆ เพิ่ม • มีการมอบหมายภารกิจในการควบคุมหรือลดความเสี่ยงเพิ่มโดยกำหนดเป็นภาระงานที่ชัดเจนของหน่วยงานภายใน สวทช.ที่เกี่ยวข้อง 2 หน่วยงาน • มีการแต่งตั้งคณะทำงานที่ต้องดูแลเรื่องการควบคุมหรือลดความเสี่ยงในกิจกรรมนั้นๆ เป็นตัวแทนร่วมกันระหว่างศูนย์แห่งชาติ/สก./ศจ.
High	• มีการสรรหาบุคลากรเพิ่มเติมหรือมีการประสานงานกับหน่วยงานภายนอก สวทช. เพื่อจัดให้มีบุคลากรที่ปฏิบัติหน้าที่ในการควบคุมหรือลดความเสี่ยงในกิจกรรมนั้นๆ เพิ่ม • มีการมอบหมายภารกิจในการควบคุมหรือลดความเสี่ยงในกิจกรรมเพิ่มโดยกำหนดเป็นภาระงานที่ชัดเจนของหน่วยงานภายใน สวทช.ที่เกี่ยวข้องตั้งแต่ 3 หน่วยงานขึ้นไป • มีการแต่งตั้งคณะทำงานที่ต้องดูแลเรื่องการควบคุมหรือลดความเสี่ยงในกิจกรรมนั้นๆ เป็นตัวแทนร่วมกันระหว่างศูนย์แห่งชาติ/สก./ศจ.และมีตัวแทนจากหน่วยงานภายนอก สวทช.
หมายเหตุ การพิจารณาระดับ Man-month สามารถเลือกประเด็นที่สอดคล้องหรือใกล้เคียงโดยไม่จำเป็นต้องครบทุกประเด็นในแต่ละระดับ	

ตารางที่ 3.7 การพิจารณาแรงงานที่ต้องใช้ (Man-month) 3 ระดับ

การวิเคราะห์ต้นทุนโดยรวม (Cost Level) พิจารณาจากระดับของงบประมาณกับแรงงาน (Man-Month) โดยมีรายละเอียดตามตารางนี้

การวิเคราะห์ต้นทุน (Cost)		
Cost Level	งบประมาณ	Man-month
High	High	High
High	High	Medium
Medium	High	Low
High	Medium	High
Medium	Medium	Medium
Low	Medium	Low
Medium	Low	High
Low	Low	Medium
Low	Low	Low

ตารางที่ 3.8 การวิเคราะห์ต้นทุน (Cost Level) ของมาตรการที่กำหนดเพื่อจัดการความเสี่ยง

2. การวิเคราะห์ประโยชน์ที่ได้รับ (Benefit Level) จะพิจารณาว่ามาตรการ/กิจกรรมจะช่วยลดโอกาสที่จะเกิดความเสี่ยงและ/หรือลดความรุนแรงของผลกระทบจากความเสี่ยงนั้นระดับใดโดยแบ่งการพิจารณาเป็น 3 ระดับ เช่นกัน คือ Low, Medium และ High โดยแต่ละระดับ พิจารณาจากรายละเอียดที่ระบุในตาราง ดังนี้

การวิเคราะห์ประโยชน์ที่ได้รับ (Benefit Level)	
Benefit Level	ลดระดับคะแนน Impact / Likelihood
High	เป็นกิจกรรมที่เป็นปัจจัยสำคัญ (Critical Factor) ในการลดความเสี่ยง**มาก**
Medium	เป็นกิจกรรมที่เป็นปัจจัยสำคัญ (Critical Factor) ในการลดความเสี่ยง**ปานกลาง**
Low	เป็นกิจกรรมที่เป็นปัจจัยสำคัญ (Critical Factor) ในการลดความเสี่ยง**น้อย**

ตารางที่ 3.9 การวิเคราะห์ประโยชน์ที่ได้รับ (Benefit Level)

(4.3) การจัดทำแผนบริหารจัดการความเสี่ยง (Risk Mitigation Plan)

ผู้รับผิดชอบความเสี่ยง (Risk Owner) จะต้องคำนึงเสมอว่ามาตรการ/กิจกรรมที่คัดเลือกจะส่งผลให้ลดความรุนแรงของผลกระทบและ/หรือโอกาสในการเกิดอย่างไร รวมถึงสามารถช่วยควบคุม/ลดสาเหตุและผลกระทบในเรื่องใดบ้าง ซึ่งการดำเนินการดังกล่าวจะใช้ Bow Tie Diagram เป็นเครื่องมือหลัก ทั้งนี้เพราะกลไกสำคัญของการบริหารจัดการความเสี่ยง คือ การได้ปรึกษาหารือ และทำความเข้าใจร่วมกันระหว่างผู้มีส่วนได้ส่วนเสีย

ในการจัดทำแผนบริหารจัดการความเสี่ยง จะใช้เกณฑ์การจัดลำดับความสำคัญเหมือนการวิเคราะห์ Cost Level และ Benefit Level แล้วนำมาพิจารณาจัดลำดับความสำคัญของมาตรการ/กิจกรรมที่ใช้ในการจัดการความเสี่ยง (Mitigation Action) โดยมีเกณฑ์การจัดลำดับความสำคัญ ดังนี้

การพิจารณา Mitigation Action Level		
Benefit Level	**Cost Level**	**Priority for Mitigation Action**
High	High	Risk Owner พิจารณาร่วมกับ Task Owner อีกครั้ง
High	Medium	2
High	Low	1
Medium	High	3
Medium	Medium	2
Medium	Low	1
Low	High	4
Low	Medium	3
Low	Low	2

ตารางที่ 3.10 การพิจารณาเพื่อจัดลำดับความสำคัญของมาตรการที่กำหนดเพื่อจัดการความเสี่ยง (Mitigation Action Level)

คำอธิบาย

1) การพิจารณาลำดับความสำคัญของมาตรการ/กิจกรรมถ้าต้นทุนอยู่ที่ Low Level และมี Benefit Level อยู่ในระดับ High และ Medium จะมีลำดับความสำคัญของการดำเนินการอยู่ในลำดับที่ 1 เพราะสามารถช่วยลดความเสี่ยงได้โดยใช้งบประมาณบริหารจัดการปกติ ไม่ต้องจัดหางบประมาณเพิ่ม และเป็นงานที่อยู่ในภาระหน้าที่ของหน่วยงาน ส่วนมาตรการ/กิจกรรมที่มีต้นทุนอยู่ Medium Level และ High Level ให้จัดลำดับความสำคัญของการดำเนินงานในระดับรองลงมา (2, 3 และ 4) ตามลำดับ

2) ในทางปฏิบัติระหว่างการดำเนินงานตามแผนบริหารจัดการความเสี่ยง ผู้รับผิดชอบความเสี่ยง (Risk Owner) สามารถปรับปรุงหรือแก้ไขมาตรการ/กิจกรรมในแผนฯ ได้ หากพบว่ามีมาตรการ/กิจกรรมบางอย่างที่ควรดำเนินการก่อนเพราะช่วยลดความเสี่ยง โดย Risk Owner สามารถพิจารณาสั่งการหรือมอบหมายให้ดำเนินการได้ทันทีโดยไม่จำเป็นต้องวิเคราะห์ผลได้ผลเสีย (Cost-Benefit Analysis) เพื่อจัดลำดับความสำคัญของมาตรการ/กิจกรรมนั้นๆ

การดำเนินการวิเคราะห์ต้นทุนโดยรวม (Cost Level) และประโยชน์ที่ได้รับ (Benefit Level) ให้ดำเนินการในผังวิเคราะห์ความคุ้มค่าของมาตรการจัดการความเสี่ยง (Cost benefit Analysis For RMR: CBA) รายละเอียดตามภาคผนวก ซ

เมื่อพิจารณาคัดเลือกมาตรการ/กิจกรรมแล้ว ผู้รับผิดชอบความเสี่ยง (Risk Owner) จะนำข้อมูลมาจัดทำแผนบริหารจัดการความเสี่ยง โดยระบุแผนปฏิบัติการ/กิจกรรมย่อย ตัวชี้วัด เป้าหมาย กิจกรรมที่มี/เพิ่มความถี่ในการรายงานผล กำหนดแล้วเสร็จ ผู้รับผิดชอบและแหล่งงบประมาณ ลงในแบบฟอร์มแผนบริหารจัดการความเสี่ยง (Mitigation Action Plan: MAP) (ภาคผนวก ฌ)

ผู้รับผิดชอบความเสี่ยง (Risk Owner) จะต้องนำเสนอแผนบริหารจัดการความเสี่ยงที่แล้วเสร็จให้คณะกรรมการจัดการความเสี่ยงพิจารณาอนุมัติ และรายงานให้คณะอนุกรรมการบริหารความเสี่ยงของ สวทช. และกวทช. เห็นชอบต่อไป

เมื่อคณะกรรมการจัดการความเสี่ยงมีมติเห็นชอบแผนบริหารจัดการความเสี่ยงแล้ว จะดำเนินการสื่อสารรายละเอียดของแผนการดำเนินงานดังกล่าวให้ผู้เกี่ยวข้องทราบและดำเนินการตามแผนที่กำหนด

(5) การติดตามตรวจสอบและการทบทวนผลการบริหารจัดการความเสี่ยง (Monitor and Review) [5.6]

องค์กรจะต้องจัดให้มีการเฝ้าติดตามตรวจสอบและทบทวนไว้เป็นหนึ่งในกระบวนการบริหารจัดการความเสี่ยง โดยจะต้องมีการกำหนดผู้รับผิดชอบและกรอบเวลาในการดำเนินการไว้อย่างชัดเจน ทั้งนี้การเฝ้าติดตามตรวจสอบและทบทวน จะต้องครอบคลุมในทุกๆ ส่วนของกระบวนการบริหารจัดการความเสี่ยง

(5.1) การติดตามตรวจสอบและทบทวนผลการบริหารจัดการความเสี่ยง (Monitor and Review)

การติดตามตรวจสอบและรายงานผลการดำเนินงานตามแผนบริหารจัดการความเสี่ยง ดำเนินการเพื่อสร้างความมั่นใจว่าการบริหารจัดการความเสี่ยงได้ถูกนำไปปฏิบัติและเป็นข้อมูลประกอบการตัดสินใจให้แก่ผู้รับผิดชอบความเสี่ยง (Risk Owner) ในการดำเนินการจัดการความเสี่ยง สวทช. ได้กำหนดขั้นตอนในการดำเนินการ ดังนี้

1.1. ผู้รับผิดชอบความเสี่ยง (Risk owner) สื่อสารผลการพิจารณาแผนบริหารจัดการความเสี่ยงต่อ Task owner เพื่อนำข้อเสนอแนะไปปรับปรุงแผนการดำเนินงานที่เกี่ยวข้อง พร้อมมอบหมายให้ Task

owner ดำเนินการวาง/ปรับปรุง/แก้ไข แผนการดำเนินงานรายไตรมาสในแบบรายงานผลการจัดการความเสี่ยง (Mitigation action report)

1.2. Task owner ดำเนินงานตามแผนรายไตรมาสและเมื่อครบไตรมาส (ทุก 3 เดือน) Task owner จะต้องรายงานผลการดำเนินงานลงในแบบรายงานผลการจัดการความเสี่ยง (Mitigation action report) รายละเอียดตามภาคผนวก ญ

1.3. ผู้รับผิดชอบความเสี่ยง (Risk owner) รวบรวมแบบรายงานผลการจัดการความเสี่ยง (Mitigation action report) ของทุกแผนปฏิบัติการ/กิจกรรมย่อย และสรุปผลการดำเนินงานภาพรวมของรายการความเสี่ยงลงในแบบรายงานการติดตามความเสี่ยง (Risk monitor report: RMR) รายละเอียดตามภาคผนวก ฎ

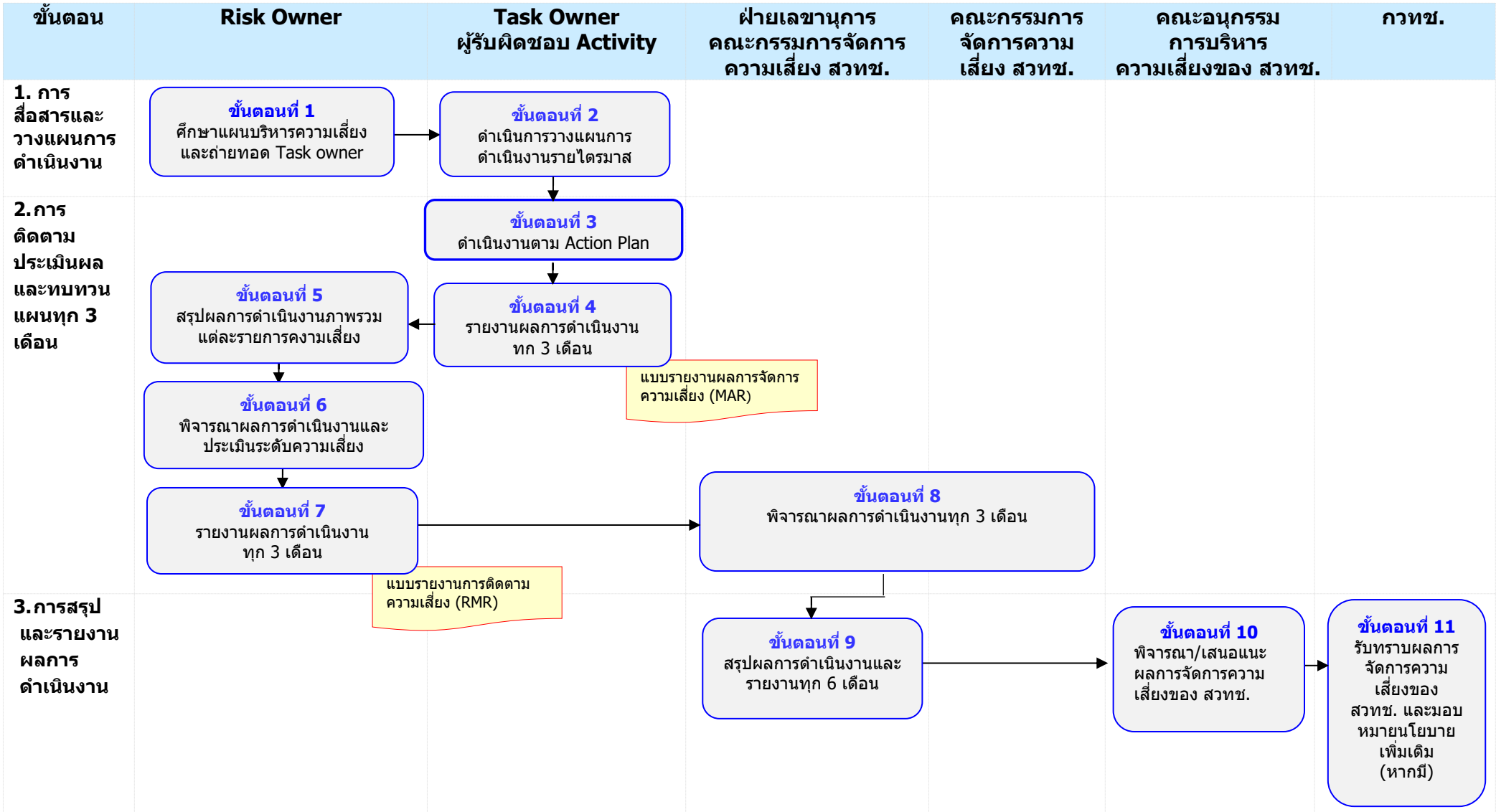
1.4. ผู้รับผิดชอบความเสี่ยง (Risk owner) พิจารณาผลการดำเนินงานและประเมินระดับความเสี่ยง (ระดับโอกาส ×ระดับผลกระทบ) พร้อมระบุข้อเสนอแนะการดำเนินการ ฯลฯ ตามหัวข้อที่ระบุในแบบรายงานการติดตามความเสี่ยง (Risk monitor report: RMR)

1.5. ผู้รับผิดชอบความเสี่ยง (Risk owner) เสนอผลการการติดตามและประเมินผลรายความเสี่ยง (Risk monitor report: RMR) ต่อคณะกรรมการจัดการความเสี่ยงของ สวทช.

1.6. ฝ่ายเลขานุการฯ นำมติที่การพิจารณาผลการประเมินระดับคะแนน (ระดับโอกาส ×ระดับผลกระทบ) ของทุกรายการความเสี่ยงไปแสดงในแผนภูมิแสดงความเสี่ยง (Risk Profile) เพื่อตรวจสอบว่าระดับของความเสี่ยง (Level of risk) มีการเปลี่ยนแปลงจากตำแหน่งเดิมหรือไม่ ทั้งนี้เพื่อแสดงให้เห็นว่าแนวทางในการลด/ควบคุมความเสี่ยงที่ระบุในแผนบริหารจัดการความเสี่ยงมีประสิทธิภาพ/เหมาะสมกับการลด/ควบคุมรายการความเสี่ยงแต่ละรายการหรือไม่ หากตรวจสอบแล้วพบว่ามาตรการที่ระบุในแผนบริหารจัดการความเสี่ยงไม่เหมาะสมหรือมีเหตุการณ์/สถานการณ์ที่กระทบต่อการดำเนินงาน คณะกรรมการจัดการความเสี่ยงของ สวทช. จะต้องพิจารณาปรับปรุงแผนบริหารจัดการความเสี่ยงตามความเหมาะสม

1.7. คณะกรรมการจัดการความเสี่ยงของ สวทช. จะนำผลการติดตามการดำเนินงานตามแผนบริหารจัดการความเสี่ยงในส่วนของผลการประเมินระดับคะแนน (ระดับโอกาส ×ระดับผลกระทบ) แผนภูมิแสดงความเสี่ยง (Risk Profile) และแผนการดำเนินงานในระยะต่อไปเสนอให้คณะอนุกรรมการบริหารความเสี่ยงของ สวทช. พิจารณาให้ข้อเสนอแนะทุก 6 เดือน และรวบรวมผลการดำเนินงานในภาพรวมรายงานต่อ กวทช. ต่อไป

การติดตามตรวจสอบและการทบทวน (Monitoring and review) [5.6]



(5.2) การรายงานผลการบริหารจัดการความเสี่ยง (Report)

Task owner ดำเนินงานและรายงานผลตามแผนบริหารจัดการความเสี่ยงรายไตรมาส (ทุก 3 เดือน) ให้ผู้รับผิดชอบความเสี่ยง (Risk owner) พิจารณาผลการดำเนินการ ก่อนรายงานคณะกรรมการจัดการความเสี่ยงของ สวทช. คณะอนุกรรมการบริหารความเสี่ยงของ สวทช. และ กวทช. ตามลำดับต่อไป

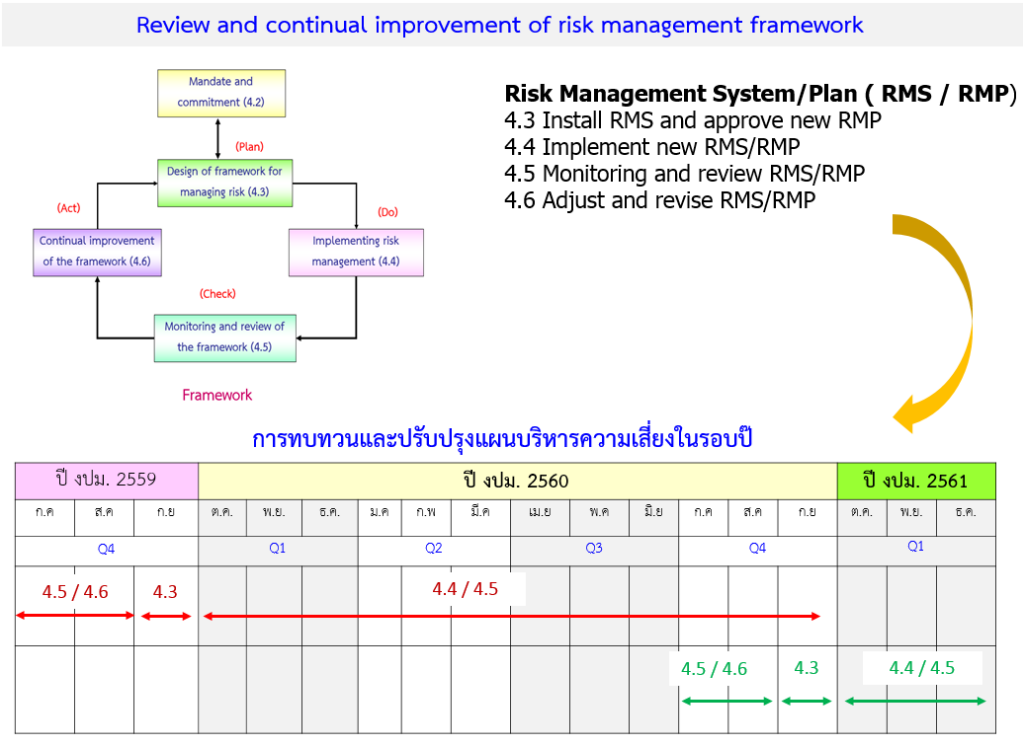
3.1.4 การติดตามและทบทวนกรอบการบริหารความเสี่ยง (Monitoring and review of the framework) [4.5]

เพื่อให้มั่นใจว่าการบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิผลและสนับสนุนการดำเนินงานขององค์กรอย่างต่อเนื่อง สวทช. จะดำเนินการวัดผลารดำเนินงานการบริหารความเสี่ยงเทียบกับตัวชี้วัด ซึ่งมีการทบทวนตั้งแต่ต้นปี รายไตรมาส และรายปี เพื่อวัดความก้าวหน้าและความเบี่ยงเบนในการดำเนินการเทียบกับแผนบริหารความเสี่ยง รวมทั้งทบทวนกรอบการบริหารความเสี่ยง นโยบาย และแผนบริหารความเสี่ยงยังคงมีความเหมาะสมและสอดคล้องกับบริบททั้งภายในและภายนอกองค์กร

3.1.5 การปรับปรุงกรอบการบริหารความเสี่ยงอย่างต่อเนื่อง (Continual Improvement of the Framework) [4.6]

การปรับปรุงกรอบการบริหารความเสี่ยงจะดำเนินการเป็นประจำทุกปีโดยคณะทำงานพัฒนาระบบบริหารความเสี่ยงจะดำเนินการทบทวนและปรับปรุงกระบวนการบริหารจัดการความเสี่ยงด้วยการพิจารณาปัญหา/อุปสรรค การดำเนินงานในรอบปีที่ผ่านมาแล้วสรุปผลเสนอ คณะกรรมการจัดการความเสี่ยง คณะอนุกรรมการบริหารความเสี่ยงของ สวทช. และ กวทช. พิจารณาปรับปรุงกรอบการบริหารงานอย่างต่อเนื่อง (Continual Improvement of the Framework) ซึ่งการดำเนินการดังกล่าวจะทำเป็นประจำทุกปี ทั้งนี้เพื่อให้สอดคล้องกับการบริหารจัดการภายใน/นอกองค์กร

การทบทวนและปรับปรุงกรอบการบริหารความเสี่ยง จะเริ่มดำเนินการช่วงไตรมาสที่ 3-4 ของปีงบประมาณปัจจุบัน เพื่อนำแนวทางการบริหารจัดการความเสี่ยงที่ผ่านการทบทวน/ปรับปรุงไปใช้ในการดำเนินงานในปีงบประมาณถัดไป โดยช่วงระยะเวลาการดำเนินงานแสดงตามแผนภาพที่ 3.23 แสดงการทบทวน/ปรับปรุงกรอบการบริหารงานอย่างต่อเนื่อง



แผนภาพที่ 3.23 การทบทวน/ปรับปรุงกรอบการบริหารงานอย่างต่อเนื่อง

3.2 การสร้างวัฒนธรรมองค์กรด้านการบริหารจัดการความเสี่ยง (Risk Culture)

สวทช. ได้ให้ความสำคัญกับการสร้างวัฒนธรรมการบริหารจัดการความเสี่ยง (Risk Culture) ตั้งแต่การกำหนดนโยบาย/บทบาทหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องทุกระดับในกระบวนการบริหารจัดการความเสี่ยง โดย กวทช. ได้จัดตั้งคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. ขึ้นเพื่อกำกับดูแลการดำเนินงานด้านการบริหารจัดการความเสี่ยงของ สวทช. และคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. ชุดนี้ได้แต่งตั้งคณะทำงานพัฒนาระบบบริหารความเสี่ยงของ สวทช. ขึ้นเพื่อทำหน้าที่พัฒนานโยบาย แผนงาน และรายงานผลการบริหารจัดการความเสี่ยงของ สวทช. ต่อคณะอนุกรรมการบริหารความเสี่ยงของ สวทช. อย่างสม่ำเสมอ นอกจากนี้ ได้มีการจัดตั้งคณะกรรมการจัดการความเสี่ยงของ สวทช. ซึ่งมีผู้อำนวยการ สวทช. เป็นประธานฯ รับผิดชอบในการกำหนดนโยบาย จัดการให้ความเสี่ยงต่างๆ อยู่ในวิสัย และขอบเขตที่พึงประสงค์

ในการดำเนินงาน สวทช. ได้บูรณาการกระบวนการบริหารจัดการความเสี่ยง (Process) ตามมาตรฐาน ISO 31000:2009 เข้ากับกระบวนการทำงานปกติโดยกำหนดขอบเขตการดำเนินงานทั้ง 3 ระดับ ประกอบด้วย (1) ระดับองค์กร (Enterprise Risk Management) (2) ระดับศูนย์แห่งชาติ/หน่วยงานหลัก (Strategic Business Unit) และ (3) ระดับโปรแกรม/กระบวนการหลัก (Major Program and Project) โดยกำหนดบทบาท/หน้าที่ให้ผู้บริหารและพนักงานผู้เกี่ยวข้องได้มีส่วนร่วมในการดำเนินงานบริหารความเสี่ยงในทุกขั้นตอนตั้งแต่ขั้นตอนการระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis)

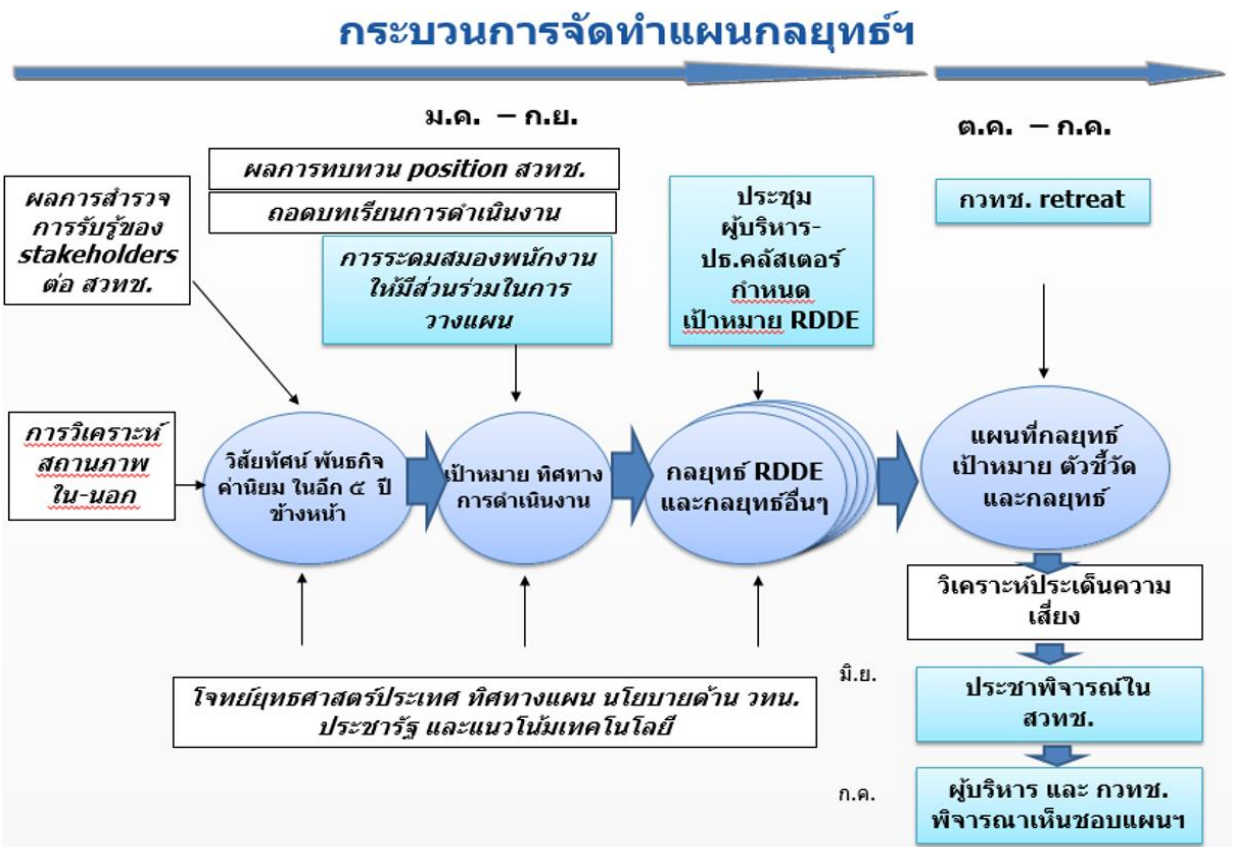
การประเมินความเสี่ยง (Risk Evaluation) การจัดการความเสี่ยง (Risk Treatment) และการติดตามตรวจสอบและการทบทวนความเสี่ยง (Monitoring and Review) และเพื่อให้การดำเนินงานในทุกส่วนขององค์กรตระหนักและนำหลักการบริหารจัดการความเสี่ยงไปใช้ในการดำเนินงานตามพันธกิจของ สวทช. จนเกิดเป็นวัฒนธรรมองค์กรในที่สุด

สวทช. ได้กำหนดแผนการสร้างวัฒนธรรมการบริหารจัดการความเสี่ยงโดยมีแนวทางการดำเนินงานแบ่งเป็น 3 หัวข้อ ประกอบด้วย (1) การวางแผนกลยุทธ์ที่ครอบคลุมการบริหารจัดการความเสี่ยง (Risk and Strategic Plan) (2) การสอบทานผลการดำเนินงานตามแนวทางการบริหารจัดการความเสี่ยง (Risk and Internal Audit) และ (3) การสื่อสารแนวทางการบริหารจัดการความเสี่ยง (Risk Communication) โดยแต่ละขั้นตอนมีสาระสำคัญของแนวทางการดำเนินงาน ดังนี้

3.2.1 การวางแผนกลยุทธ์ที่ครอบคลุมการบริหารจัดการความเสี่ยง (Risk and Strategic Planning)

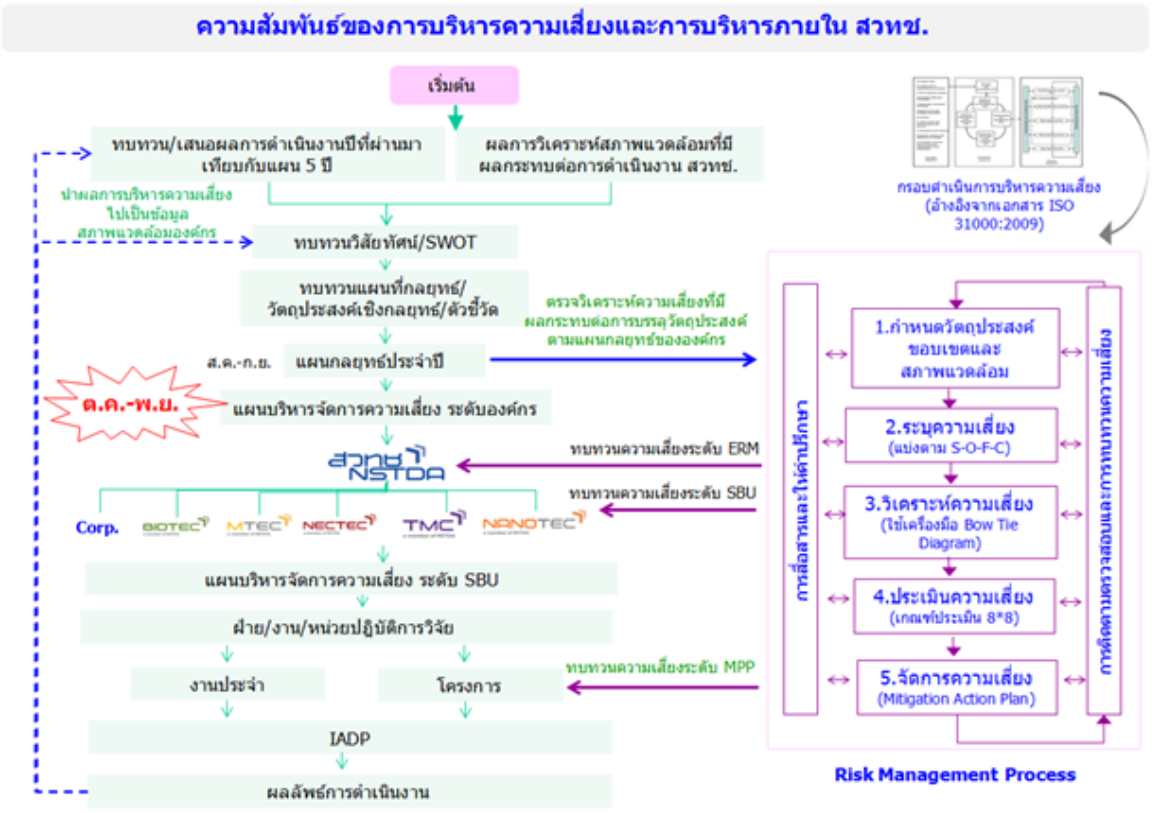
สวทช. มีการจัดทำแผนกลยุทธ์ 5 ปี และทบทวนกลยุทธ์เป็นประจำทุกปี (Rolling strategic plan) โดยให้ความสำคัญกับความสอดคล้องกับยุทธศาสตร์ประเทศ แผนพัฒนเศษฐกิจและสังคมแห่งชาติ และการวิเคราะห์บริบท สภาพแวดล้อมภายในและภายนอกที่เปลี่ยนไป เพื่อระบุโอกาส ความได้เปรียบเชิงกลยุทธ์ มุ่งสู่การกำหนดเป้าหมายองค์กร วัตถุประสงค์เชิงกลยุทธ์ และกลยุทธ์ในการดำเนินงาน เพื่อให้การดำเนินของ สวทช. เป็นไปตามแผนกลยุทธ์ที่กำหนดไว้ รายละเอียดตามแผนภาพที่ 3.24

สวทช. ได้นำกระบวนการบริหารจัดการความเสี่ยงมาผนวกกับกระบวนการวางแผนกลยุทธ์ โดยจะดำเนินการทบทวนและวิเคราะห์ความเสี่ยงหลังจากกำหนดแผนที่กลยุทธ์ เป้าหมาย ตัวชี้วัด เรียบร้อยแล้ว ซึ่งในการวิเคราะห์ความเสี่ยงจะพิจารณาข้อมูลจากทั้งภายในและภายนอก เช่น การสัมภาษณ์ผู้บริหาร การสอบทานกระบวนการทำงานภายในองค์กร/ระบบการควบคุมภายในของหน่วยงาน รายงานการประเมินผลการดำเนินงานของ สวทช. โดยที่ปรึกษาภายนอก ฯลฯ เพื่อคาดการณ์ว่าเหตุการณ์/สถานณการณ์ที่อาจจะเกิดขึ้นในอนาคตและส่งผลกระทบต่อการบรรลุวัตถุประสงค์ เป้าหมาย การดำเนินงานของ สวทช.



แผนภาพที่ 3.24 กระบวนการจัดทำแผนกลยุทธ์ฯ

สวทช. ได้กำหนดปฏิทินการบริหารจัดการความเสี่ยงให้สอดคล้องกับการบริหารภายใน โดยกำหนดให้ คณะกรรมการจัดการความเสี่ยงของ สวทช. ดำเนินการทบทวนวิเคราะห์ความเสี่ยงทุกปี หลังจากการกำหนดตัวชี้วัดเชิงกลยุทธ์ (Strategic KPIs) และถ่ายทอดตัวชี้วัดผ่านกระบวนการถ่ายทอดตัวชี้วัดประจำปี และกำหนดให้ดำเนินการจัดทำแผนบริหารจัดการความเสี่ยง ระดับองค์กร ให้แล้วเสร็จภายในเดือนตุลาคม-พฤศจิกายน ทั้งนี้ เพื่อให้การดำเนินงานบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพ รายละเอียดตามแผนภาพที่ 3.25 ความสัมพันธ์ของการบริหารจัดการความเสี่ยงและการบริหารภายใน สวทช.



แผนภาพที่ 3.25 ความสัมพันธ์ของการบริหารจัดการความเสี่ยงและการบริหารภายใน สวทช.

แผนภาพความสัมพันธ์ของการบริหารจัดการความเสี่ยงและการบริหารภายใน สวทช. ข้างต้นได้รับการเห็นชอบจากคณะกรรมการจัดการความเสี่ยง สวทช. ในการประชุมครั้งที่ 7/2557 เมื่อวันที่ 9 กันยายน พ.ศ. 2557

3.2.2 การสอบทานผลการดำเนินงานตามแนวทางการบริหารจัดการความเสี่ยง (Risk and Internal Audit)

1) กระบวนการสอบทานการดำเนินงาน สวทช. สำนักตรวจสอบภายใน ซึ่งเป็นหน่วยงานที่ทำหน้าที่หลัก จะดำเนินการวิเคราะห์ความเสี่ยงในขั้นตอนการจัดทำแผลกลยุทธ์การตรวจสอบ (Internal Audit Strategic) รวมทั้งกำหนดให้มีการใช้ Risk Control Review วิเคราะห์ความเสี่ยงและจุดควบคุมในขั้นตอนการดำเนินงานของแต่ละกระบวนการ) ในการตรวจสอบ/สอบทาน หน่วยงาน/โครงการ

2) ในกระบวนการประเมินผลการดำเนินงาน สวทช. กำหนดให้เพิ่มการบริหารจัดการความเสี่ยงเป็นส่วนหนึ่งในการประเมินผลการบริหารจัดการหน่วยงาน/โครงการ ในคู่มือการประเมินผล สวทช.

3) ผนวกการตรวจประเมินระบบบริหารความเสี่ยงเข้ากับการตรวจประเมินภายใน (Internal Audit) ระบบ ISO9001 อย่างเป็นทางการ โดยเริ่มดำเนินการตามข้อกำหนดระบบบริหารคุณภาพ ISO9001 Version 2015 ตั้งแต่ปีงบประมาณ 2559 ซึ่งสาระสำคัญข้อกำหนดนี้คือ มีการเพิ่มเรื่องการจัดการความเสี่ยงเป็น

เป็น ข้อกำหนดที่ 6.1 การดำเนินการเพื่อจัดการกับความเสี่ยงและโอกาส (Action to address risk and opportunities)

ดังนั้นตั้งแต่ปีงบประมาณ 2559 สวทช. ได้ผนวกเรื่องการบริหารความเสี่ยงเข้าไปเป็นส่วนหนึ่งของการบริหารจัดการระดับหน่วยงาน โดยกำหนดให้มีการตรวจประเมินระบบบริหารคุณภาพทั้งภายในและนอกตามข้อกำหนด ISO9001:2015 ซึ่งขอบเขตการตรวจประเมินครอบคลุมถึงกระบวนการทำงานตามพันธกิจ สวทช.

3.2.3 การสื่อสารแนวทางการบริหารจัดการความเสี่ยง (Risk communication)

สวทช. กำหนดแนวทางการสื่อสารแนวทางการสร้างวัฒนธรรมการบริหารจัดการความเสี่ยง (Risk Culture) นอกเหนือจากการดำเนินงานตามนโยบาย/บทบาทหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในทุกระดับ ด้วยการจัดทำแผนการดำเนินงานสื่อสารและให้คำปรึกษาเพื่อเป็นช่องทางการแลกเปลี่ยนเรียนรู้ให้กับพนักงานและผู้เกี่ยวข้องของ สวทช. ประกอบด้วย

1) การจัดการสื่อสารให้กับพนักงานและผู้เกี่ยวข้องทุกระดับให้มีความตระหนักและความเข้าใจเรื่องการบริหารจัดการความเสี่ยง ด้วยการใช้สื่อต่างๆ ที่เหมาะสมกับสถานการณ์/สถานที่ เช่น การจัดทำ info-graphic , e-book, VDO เป็นต้น

2) การจัดเสวนาโดยเชิญผู้มีชื่อเสียงมาบรรยายถึงประสบการณ์การจัดการความเสี่ยง โดยเน้นกลุ่มงานวิจัย

3) การเชิญนักวิจัยที่เคยนำเรื่องความเสี่ยงไปใช้เป็นเครื่องมือในการบริหารจัดการโครงการ/แผนงาน มาบรรยายถึงประโยชน์ของการจัดการความเสี่ยง

4) การนำความรู้ด้านการจัดการความเสี่ยงไปรวมอยู่ในกิจกรรมการฝึกอบรมผู้บริหารระดับกลาง MMRP

5) การเขียนบทความลงใน NSTDA Style โดยจัดให้มีคำถามและมีรางวัลให้ผู้ตอบ

ภาคผนวก

ประกาศสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
เรื่อง นโยบายการบริหารจัดการความเสี่ยง

โดยที่เป็นการสมควรปรับปรุงนโยบายการบริหารจัดการความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ให้มีความเหมาะสมและมีประสิทธิภาพยิ่งขึ้น จึงให้ยกเลิกประกาศสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ เรื่อง นโยบายการบริหารจัดการความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ลงวันที่ ๓๑ ตุลาคม พ.ศ. ๒๕๕๔ และกำหนดนโยบายการบริหารจัดการความเสี่ยง โดยสำนักงานฯ จะดำเนินการ ดังต่อไปนี้

๑. การบริหารจัดการความเสี่ยงจะใช้กรอบแนวทางตามมาตรฐาน ISO 31000:2009 โดยการดำเนินงานบริหารความเสี่ยงจะต้องดำเนินการในทุกระดับชั้นตามโครงสร้างองค์กรของสำนักงานฯ และครอบคลุมความเสี่ยงที่อาจเกิดขึ้นทั้งจากปัจจัยภายในและภายนอกองค์กร เพื่อให้สำนักงานฯ สามารถดำเนินงานตามวัตถุประสงค์และอำนาจหน้าที่ได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล

๒. กำหนดให้มีการจัดระบบและกระบวนการบริหารจัดการความเสี่ยงโดยมีคู่มือการดำเนินงานตัวอย่างในการวิเคราะห์ และการบริหารจัดการความเสี่ยง เพื่อเผยแพร่ให้ทุกหน่วยงานได้รับทราบและปฏิบัติในแนวทางเดียวกัน โดยให้นำระบบบริหารความเสี่ยงไปปฏิบัติเป็นส่วนหนึ่งของการดำเนินงานตามภารกิจจนเกิดเป็นวัฒนธรรมองค์กรในที่สุด

๓. กำหนดให้มีคณะทำงานพัฒนาระบบบริหารความเสี่ยงของสำนักงานฯ เพื่อทำหน้าที่เป็นผู้พัฒนานโยบาย แผนงาน ระบบบริหารจัดการความเสี่ยง และรายงานความก้าวหน้าในการดำเนินการบริหารจัดการความเสี่ยงของสำนักงานฯ ต่อคณะอนุกรรมการบริหารความเสี่ยงของสำนักงานฯ รวมทั้งปฏิบัติงานอื่นใดตามที่คณะอนุกรรมการบริหารความเสี่ยงของสำนักงานฯ มอบหมาย โดยมีฝ่ายติดตามประเมินผลองค์กร สำนักงานกลาง ทำหน้าที่เป็นฝ่ายเลขานุการของคณะทำงานพัฒนาระบบบริหารความเสี่ยงของสำนักงานฯ และเป็นหน่วยงานประสานงานกลางในเรื่องการบริหารจัดการความเสี่ยงของสำนักงานฯ

๔. กำหนดให้มีคณะกรรมการจัดการความเสี่ยงของสำนักงานฯ เพื่อทำหน้าที่เป็นผู้ดูแลรับผิดชอบจัดการความเสี่ยง การป้องกัน และการแก้ไขข้อขัดแย้งที่อาจเกิดจากความเสี่ยงเหล่านั้น รวมถึงจัดให้มีการประเมินและทบทวนความเสี่ยงด้วยความถี่ที่เหมาะสมตามความจำเป็น โดยมีฝ่ายติดตามประเมินผลองค์กร สำนักงานกลาง ทำหน้าที่เป็นฝ่ายเลขานุการของคณะกรรมการจัดการความเสี่ยงของสำนักงานฯ และเป็นหน่วยงานประสานงานกลางในเรื่องการบริหารจัดการความเสี่ยงของสำนักงานฯ

๕. คณะกรรมการจัดการความเสี่ยงของสำนักงานฯ จะประมวลวิเคราะห์ความก้าวหน้าในการดำเนินงานของคณะทำงานพัฒนาระบบบริหารความเสี่ยงของสำนักงานฯ และจัดทำรายงานการติดตามประเมินผลการบริหารจัดการความเสี่ยงนำเสนอต่อคณะอนุกรรมการบริหารความเสี่ยงของสำนักงานฯ และคณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติตามลำดับ ในทุก ๖ เดือน เพื่อทราบ และ/หรือพิจารณาทบทวนและปรับปรุงแผนการบริหารจัดการความเสี่ยงของสำนักงานฯ ให้มีความเหมาะสม

๖. กำหนดให้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการความเสี่ยงอย่างเหมาะสม เพื่อให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ

๗. ดำเนินการจัดสรรทรัพยากรอย่างเพียงพอเพื่อบริหารจัดการความเสี่ยงให้มีประสิทธิภาพ พร้อมทั้งส่งเสริม สื่อสาร และพัฒนาความรู้และความเข้าใจในเรื่องการบริหารจัดการความเสี่ยงให้แก่บุคลากรในทุกระดับ รวมทั้งการเสริมสร้างความตระหนักถึงประโยชน์และความสำคัญในการบริหารจัดการความเสี่ยงขององค์กร

จึงประกาศเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๓๐ พฤศจิกายน พ.ศ. ๒๕๕๙

(นายณรงค์ ศิริเลิศวรกุล)
ผู้อำนวยการ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

คำสั่งคณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
ที่ ๕ /๒๕๖๑
เรื่อง แต่งตั้งคณะอนุกรรมการบริหารความเสี่ยง
ของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

ตามที่คณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ได้มีคำสั่งคณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่ ๘/๒๕๕๘ เรื่อง แต่งตั้งคณะอนุกรรมการบริหารความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ลงวันที่ ๑๖ พฤศจิกายน พ.ศ. ๒๕๕๘ และคำสั่งคณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่ ๓/๒๕๕๙ เรื่อง แต่งตั้งคณะอนุกรรมการบริหารความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (แก้ไขเพิ่มเติม) ลงวันที่ ๙ ธันวาคม พ.ศ. ๒๕๕๙ และในการประชุมคณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ครั้งที่ ๙/๒๕๖๐ เมื่อวันที่ ๒๔ พฤศจิกายน ๒๕๖๐ ได้มีมติเห็นชอบให้แต่งตั้งคณะอนุกรรมการบริหารความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ แทนชุดเดิมที่ครบวาระไปแล้ว นั้น

ดังนั้น เพื่อให้เป็นไปตามมติคณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติดังกล่าวข้างต้น อาศัยอำนาจตามความในมาตรา ๑๐ แห่งพระราชบัญญัติพัฒนาวิทยาศาสตร์และเทคโนโลยี พ.ศ. ๒๕๓๔ จึงแต่งตั้งคณะอนุกรรมการบริหารความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ โดยให้มีองค์ประกอบและอำนาจหน้าที่ ดังนี้

๑. องค์ประกอบ

๑.๑ นายอาชว์ เตาลานนท์	เป็น ประธานอนุกรรมการ
๑.๒ ผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ	เป็น รองประธานอนุกรรมการ
๑.๓ นายยงยุทธ ยุทธวงศ์	เป็น อนุกรรมการ
๑.๔ นายกอปร กฤตยากีรณ	เป็น อนุกรรมการ
๑.๕ นายหริส สูตะบุตร	เป็น อนุกรรมการ
๑.๖ นายทวีศักดิ์ กออนันตกูล	เป็น อนุกรรมการ
๑.๗ รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่รับผิดชอบด้านบริหารความเสี่ยง สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ	เป็น อนุกรรมการและเลขานุการ

/ ๑.๘ ผู้อำนวยการ ...

๑.๘ ผู้อำนวยการฝ่ายติดตามประเมินผลองค์กร เป็น ผู้ช่วยเลขานุการ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

๒. อำนาจหน้าที่

๒.๑ เสนอแนะนโยบายการบริหารความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติต่อคณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ เพื่อพิจารณาอนุมัติ

๒.๒ กำกับดูแลการบริหารความเสี่ยงทั่วทั้งองค์กรของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

๒.๓ แต่งตั้งคณะทำงานเพื่อปฏิบัติงานตามความเหมาะสม

๒.๔ รายงานผลการบริหารความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติต่อคณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

๒.๕ ปฏิบัติงานอื่นตามที่คณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติมอบหมาย

ทั้งนี้ ตั้งแต่วันที่ ๒๕ พฤศจิกายน ๒๕๖๐ เป็นต้นไป โดยให้มีวาระในการดำรงตำแหน่ง ๒ ปี

สั่ง ณ วันที่ ๑๗ มกราคม พ.ศ. ๒๕๖๑

(นายสุวิทย์ เมษินทรีย์)
รัฐมนตรีว่าการกระทรวงวิทยาศาสตร์และเทคโนโลยี
ประธานกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

คำสั่งสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

ที่ ๒๒๑ /๒๕๕๙

เรื่อง แต่งตั้งคณะกรรมการจัดการความเสี่ยง

ของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

ตามที่ได้มีคำสั่งสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่ ๒๙๑/๒๕๕๖ ลงวันที่ ๑๙ พฤศจิกายน พ.ศ. ๒๕๕๖ ให้แต่งตั้งคณะกรรมการจัดการความเสี่ยง ของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ซึ่งได้ครบวาระลงแล้วเมื่อวันที่ ๑๘ พฤศจิกายน ๒๕๕๘ ดังนั้น เพื่อให้การดำเนินการดังกล่าวเป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ สอดคล้องกับการปรับปรุงโครงสร้างองค์กรใหม่

อาศัยอำนาจตามมาตรา ๑๕ แห่งพระราชบัญญัติพัฒนาวิทยาศาสตร์และเทคโนโลยี พ.ศ. ๒๕๓๔ จึงแต่งตั้งคณะกรรมการจัดการความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ โดยมีองค์ประกอบ ดังนี้

๑. นายกอปร กฤตยากีรณ เป็น ที่ปรึกษา
๒. นายหริส สูตะบุตร เป็น ที่ปรึกษา
๓. ผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ เป็น ประธานกรรมการ
๔. รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สายงานกลยุทธ์องค์กร เป็น กรรมการ
๕. รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สายงานพัฒนากำลังคนทางวิทยาศาสตร์และเทคโนโลยี เป็น กรรมการ
๖. รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สายงานบริหาร เป็น กรรมการ
๗. รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สายงานบริหารการวิจัยและพัฒนา เป็น กรรมการ
๘. รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สายงานออกแบบและวิศวกรรม เป็น กรรมการ
๙. รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สายงานกิจการพิเศษ เป็น กรรมการ
๑๐. รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สถาบันการจัดการเทคโนโลยีและนวัตกรรมเกษตร เป็น กรรมการ

/ ๑๑. รองผู้อำนวยการ ...

๑๑. รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ เป็น กรรมการ
ศูนย์บริหารจัดการเทคโนโลยี
๑๒. ผู้อำนวยการศูนย์พันธุวิศวกรรมและเทคโนโลยีชีวภาพแห่งชาติ เป็น กรรมการ
๑๓. ผู้อำนวยการศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ เป็น กรรมการ
๑๔. ผู้อำนวยการศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เป็น กรรมการ
๑๕. ผู้อำนวยการศูนย์นาโนเทคโนโลยีแห่งชาติ เป็น กรรมการ
๑๖. ผู้อำนวยการฝ่าย ฝ่ายติดตามประเมินผลองค์กร เป็น เลขานุการ

ให้คณะกรรมการดังกล่าวมีอำนาจหน้าที่ ดังต่อไปนี้

๑. ดูแลรับผิดชอบจัดการความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ เพื่อให้สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติสามารถดำเนินงานตามวัตถุประสงค์ได้อย่างมีประสิทธิภาพและประสิทธิผล ป้องกันและแก้ไขประเด็นที่อาจเกิดขึ้นจากความเสี่ยง ประเมินและทบทวนความเสี่ยงด้วยความถี่ที่เหมาะสมและตามความจำเป็น

๒. จัดให้มีระบบบริหารความเสี่ยงในสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ พร้อมทั้งทรัพยากรที่ใช้ในการดำเนินการจัดทำแผนบริหารความเสี่ยงและรายงานผลการบริหารความเสี่ยงและให้มีการรายงานความก้าวหน้าของการบริหารความเสี่ยงอย่างสม่ำเสมอ

๓. ส่งเสริม สื่อสาร พัฒนาความรู้ความเข้าใจในเรื่องการบริหารความเสี่ยงให้แก่บุคลากรในทุกระดับและเสริมสร้างความตระหนักถึงประโยชน์ในการบริหารจัดการความเสี่ยงทั่วทั้งองค์กร

ทั้งนี้ ตั้งแต่วันที่ ๑๒ ตุลาคม ๒๕๕๙ เป็นต้นไป โดยให้มีวาระในการดำรงตำแหน่ง ๒ ปี

สั่ง ณ วันที่ ๒๗ ตุลาคม พ.ศ. ๒๕๕๙

(นายณรงค์ ศิริเลิศวรกุล)
ผู้อำนวยการ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

คำสั่งคณะอนุกรรมการบริหารความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

ที่ ๑ /๒๕๕๙

เรื่อง แต่งตั้งคณะทำงานพัฒนาระบบบริหารความเสี่ยง

เพื่อให้การดำเนินงานด้านการบริหารความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ

อาศัยอำนาจตามคำสั่งคณะกรรมการพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่ ๘/๒๕๕๘ จึงแต่งตั้งคณะทำงานพัฒนาระบบบริหารความเสี่ยง โดยมีองค์ประกอบ ดังนี้

๑. นายกอปร กฤตยากีรณ เป็น ที่ปรึกษา
๒. นายหริส สูตะบุตร เป็น ที่ปรึกษา
๓. รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สายงานกลยุทธ์องค์กร เป็น ประธานคณะทำงาน
๔. รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สายงานพัฒนากำลังคนทางวิทยาศาสตร์และเทคโนโลยี เป็น ผู้ทำงาน
๕. รองผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สายงานบริหาร เป็น ผู้ทำงาน
๖. หัวหน้าสำนักตรวจสอบภายใน เป็น ผู้ทำงาน
๗. ผู้อำนวยการฝ่าย ฝ่ายติดตามประเมินผลองค์กร เป็น ผู้ทำงานและเลขานุการ

ให้คณะทำงานดังกล่าวมีอำนาจหน้าที่ ดังต่อไปนี้

๑. พัฒนานโยบาย แผนงาน และระบบบริหารจัดการความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ และเสนอต่อคณะอนุกรรมการบริหารความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

๒. รายงานความก้าวหน้าในการดำเนินการบริหารจัดการความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติต่อคณะอนุกรรมการบริหารความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

๓. ปฏิบัติงานอื่นตามที่คณะอนุกรรมการบริหารความเสี่ยงของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป โดยให้มีวาระในการดำรงตำแหน่ง ๒ ปี

สั่ง ณ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๕๙

(นายอาชว์ เตาลานนท์)
ประธานอนุกรรมการบริหารความเสี่ยง
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

ภาคผนวก จ

ผังทบทวนความเสี่ยง ประจำปี (Annual Risk Review : ARR)									
	A **New Risks/ Revised Statement**	B **คำอธิบายของความเสี่ยง**	C **Score**		D Risk Owner	E **เหตุการณ์/สถานการณ์ประกอบการพิจารณา**	F **ตัวชี้วัดของ สวทช. ปีงบประมาณ 2559**	G **วัตถุประสงค์เชิงกลยุทธ์** (SO : strategic objectives) **ที่เกี่ยวข้อง**	H **ข้อเสนอเพื่อพิจารณา**
				L × I					
Strategic Risk									
Operational Risk									
Financial Risk									
Compliance Risk									

ภาคผนวก ฉ

ผังสรุปการวิเคราะห์และประเมินความเสี่ยง (Risk Analysis and Evaluation Summary)

Bow Tie Diagram: BTD

BTD สำหรับ Risk ..... วันที่.....

7. Risk Rating "Before" Mitigation	
Likelihood	
Impact	
Residual Risk Rating	
วันที่	

1.Risk ID :	
Owner	
ผู้ช่วย Owner	

8. Risk Rating "After" Mitigation		
	แผน	ผล
Likelihood		
Impact		
Residual Risk Rating		
วันที่		

2. Causes	

3. Impacts	

4. Existing Controls (Preventative)		
Existing Preventative controls	Link to Cause #	Control Owner

5. Existing Controls (Mitigating)		
Existing Mitigating Controls	Link to Impact #	Control Owner

6. Risk Mitigating (Tasks)				
Risk Control Area	Link to Cause#	Link to Impact#	Due date	Task Owner

จัดทำโดย.....

วันที่.....

อนุมัติโดย.....

วันที่.....

ภาคผนวก ช

ผังภูมิความเสี่ยง (Risk Profile : RP)

Impact

8	1*8=8	2*8=16	3*8=24	4*8=32	5*8=40	6*8=48	7*8=56	**8*8=64**
7	1*7=7	2*7=14	3*7=21	4*7=28	5*7=35	6*7=42	7*7=49	8*7=56
6	1*6=6	2*6=12	3*6=18	4*6=24	5*6=30	**6*6=36**	7*6=42	8*6=48
5	1*5=5	2*5=10	3*5=15	4*5=20	**5*5=25**	6*5=30	7*5=35	8*5=40
4	1*4=4	2*4=8	3*4=12	**4*4=16**	5*4=20	6*4=24	7*4=28	8*4=32
3	1*3=3	2*3=6	3*3=9	4*3=12	5*3=15	6*3=18	7*3=21	8*3=24
2	1*2=2	2*2=4	3*2=6	4*2=8	5*2=10	6*2=12	7*2=14	8*2=16
1	1*1=1	2*1=2	3*1=3	4*1=4	5*1=5	6*1=6	7*1=7	8*1=8
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**

Risk Boundary

Likelihood

ภาคผนวก ซ

ผังวิเคราะห์ความคุ้มค่าของมาตรการจัดการความเสี่ยง (Cost benefit Analysis For RMA : CBA)

การวิเคราะห์ประโยชน์ที่จะได้รับเทียบกับค่าใช้จ่าย (Cost-Benefit Analysis)	"Before" Mitigation	
	Consequence	
ประเด็นความเสี่ยง	Likelihood	
Risk Owner	Residual Risk Rating	

	Risk Mitigation Tasks	Task Owner	Cost Level (L, M, H)			② Benefit Level	Priority for Mitigation Action (1, 2, 3, 4)
			งบประมาณ	Man-month	① Cost Level		
1							
2							
3							
4							
5							
6							

ผู้วิเคราะห์ _____

วันที่ _____

ภาคผนวก ฌ

แผนบริหารจัดการความเสี่ยง (Mitigation Action Plan : MAP)

ความเสี่ยง (Risk Identification)	ผู้รับผิดชอบ (Risk Owner)	กลยุทธ์/แผนงาน	Task Owner	แผนปฏิบัติการ/กิจกรรมย่อย	ตัวชี้วัด	เป้าหมาย	กิจกรรมที่มี	กิจกรรมที่เพิ่ม	เริ่มเก็บข้อมูล/ดำเนินการ	(f) ความถี่การติดตามผล	กำหนดแล้วเสร็จ	ผู้รับผิดชอบ (ระบุชื่อบุคคล)	แหล่งงบประมาณของกิจกรรม

รายงานการติดตามความเสี่ยง (Risk Monitoring Report)			RMR
ความเสี่ยง (Risk ID)			
Risk Owner		ผู้ช่วย Risk Owner	
ระยะติดตามผล		วันที่รายงาน	

1. สรุปสาระสำคัญการดำเนินการตามแผนบริหารจัดการความเสี่ยง (Mitigation Action Plan : MAP)

2. เหตุการณ์/สถานการณ์ ที่มีนัยสำคัญที่พบในระยะติดตามผล หรือสิ่งที่ดำเนินการอย่างมีนัยสำคัญ

การประเมินความเสี่ยงก่อนและหลังการดำเนินการตาม MAP

	การประเมินครั้งล่าสุด	การประเมินครั้งนี้
วันที่ประเมิน		
โอกาสเกิด		
ผลกระทบ		
ระดับความเสี่ยง		

ข้อเสนอแนะการดำเนินการต่อเนื่อง และการปรับ MAP	ความสำคัญในช่วงถัดไป

ความคิดเห็นของ Risk Owner

มติที่ประชุมคณะกรรมการจัดการความเสี่ยง

ผู้บันทึก ..... **วันที่** .....

ผู้รายงาน	ผู้ช่วย Risk Owner ลงนาม	วันที่
	Risk Owner ลงนาม	วันที่
เอกสารแนบ	1) BTD 2) Mitigation Action Report : MAR 3) ข้อมูลประกอบอื่นๆ ตามความเหมาะสม	

แบบรายงานผลการจัดการความเสี่ยง (Mitigation Action Report)			MAR
ความเสี่ยง (Risk ID)		Risk Owner	
กลยุทธ์/แผนงาน			
แผนปฏิบัติการ/ กิจกรรมย่อย		ผู้รับผิดชอบ	
		กำหนดแล้วเสร็จ	
		ผู้รับผิดชอบ	
		กำหนดแล้วเสร็จ	
ตัวชี้วัด		เป้าหมาย	

แผนการดำเนินงาน ปีงบประมาณ .....

ไตรมาส 1	ไตรมาส 2	ไตรมาส 3	ไตรมาส 4

ผลการดำเนินงาน ปีงบประมาณ ..... ไตรมาส .....

ไตรมาส 1	ไตรมาส 2	ไตรมาส 3	ไตรมาส 4

สภาพปัญหา อุปสรรค ข้อเสนอแนะ แนวทางแก้ไข และความสำคัญในช่วงถัดไป

สรุปจุดที่น่าจะส่งผลต่อโอกาสเกิดและผลกระทบความเสี่ยงในรอบรายงานนี้

ผู้รายงาน ..... วันที่ .....

ภาคผนวก ฏ

แบบฟอร์มเกณฑ์การประเมินความเสี่ยง 8 × 8

เกณฑ์ประเมินโอกาสการเกิด (Likelihood)	
ตัวชี้วัดความเสี่ยง Key risk indicator (KRI)	
Level of likelihood	
8 โอกาสเกิดเป็นความเสี่ยงแน่นอน	
7 โอกาสเกิดเป็นความเสี่ยงสูงมาก	
6 โอกาสเกิดเป็นความเสี่ยงสูง	
5 โอกาสเกิดเป็นปัญหาปานกลาง	
4 ค่าเบี่ยงเบนจากเป้าหมายที่องค์กรยอมรับได้	
3 ค่าเป้าหมายที่องค์กรกำหนด	
2 โอกาสเกิดเป็นความเสี่ยงน้อย	
1 โอกาสเกิดเป็นความเสี่ยงน้อยมาก	

เกณฑ์ประเมินผลกระทบ (Impact)	
ตัวชี้วัดความเสี่ยง Key risk indicator (KRI)	
Level of Impact	
8 วิกฤต	
7 เสียหายรุนแรง/สูงมาก	
6 เสียหายสูง	
5 เสียหายปานกลาง	
4 ค่าเบี่ยงเบนจากเป้าหมายที่องค์กรยอมรับได้	
3 ค่าเป้าหมายที่องค์กรกำหนด	
2 ดีกว่าเป้าหมายอย่างมีนัยสำคัญ	
1 ดีกว่าเป้าหมายเป็นอย่างมาก	

อภิธานศัพท์บริหารความเสี่ยง ของ สวทช.

(Glossary for NSTDA Risk Management)

Bow Tie Diagram : BTD

แผนภาพแสดงสรุปการวิเคราะห์และประเมินความเสี่ยง เป็นเครื่องมือในการวางแผนจัดการความเสี่ยงขององค์กร สามารถประเมินสาเหตุ ผลกระทบ และการควบคุมที่มีอยู่ พร้อมกับวางมาตรการในการควบคุม/ลดความเสี่ยง

Causes

สาเหตุของความเสี่ยง สาเหตุต่างๆ ที่สามารถจะส่งผลให้เกิดความเสี่ยง

Compliance Risk

ความเสี่ยงทางด้านการปฏิบัติตามกฎระเบียบ

ความเสี่ยงเนื่องจากการฝ่าฝืนหรือไม่สามารถปฏิบัติตามกฎหมาย กฎระเบียบ ระเบียบข้อบังคับ ข้อกำหนดของทางการ หรือสัญญาที่เกี่ยวข้องกับการปฏิบัติงาน

Control Owner

ผู้ที่รับผิดชอบ/หน่วยงานที่รับผิดชอบกลไกนั้นๆ

Due Date

กำหนดวันสิ้นสุดของการดำเนินการ/กิจกรรม

Enterprise Risk Management : ERM

การบริหารความเสี่ยงระดับองค์กร

กระบวนการที่บุคลากรทั่วทั้งองค์กรได้มีส่วนร่วมในการคิด วิเคราะห์ และคาดการณ์ถึงเหตุการณ์หรือความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งการระบุแนวทางในการจัดการกับความเสี่ยงดังกล่าว ให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ เพื่อช่วยให้องค์กรบรรลุในวัตถุประสงค์ที่ต้องการ ตามกรอบวิสัยทัศน์ และพันธกิจขององค์กร

Existing Preventative Controls

กลไกการควบคุมเชิงป้องกันที่มีอยู่แล้ว ที่ใช้ในการควบคุม/ป้องกันมิให้เกิดสาเหตุ (Causes)

Existing Mitigating Controls

กลไกการควบคุมเชิงแก้ไขที่มีอยู่แล้ว ที่ใช้ในการแก้ไขผลกระทบ/ดำเนินการมิให้เกิดผลกระทบที่รุนแรง

Financial Risk

ความเสี่ยงทางด้านการเงิน

ความเสี่ยงเนื่องจากสถานะและการดำเนินการงานทางการเงิน หรือ งบประมาณเกิดความขัดข้องจนกระทบการดำเนินงานขององค์กรในการบรรลุเป้าหมายตามพันธกิจ อันเนื่องมาจากการขาดการจัดหาข้อมูล การวิเคราะห์ การวางแผน การควบคุม และการจัดทำรายงานเพื่อนำมาใช้ในการบริหารการเงินได้อย่างถูกต้องเหมาะสม ทำให้ขาดประสิทธิภาพ และไม่ทันต่อสถานการณ์ ซึ่งส่งผลต่อการตัดสินใจทางการเงิน หรือการบริหารงบประมาณที่ผิดพลาด ส่งผลกระทบต่อสถานะการเงินขององค์กร หรือเป็นความเสี่ยงที่เกี่ยวข้องกับการเงินขององค์กร

Impact

ผลกระทบ

ความเสียหายที่จะเกิดขึ้น หากความเสี่ยงนั้นเกิดขึ้น เป็นการพิจารณาระดับความรุนแรงและมูลค่าความเสียหายจากความเสี่ยงที่คาดว่าจะได้รับ

Key Risk Indicator : KRI

ตัวชี้วัดระดับความเสี่ยง

มาตรวัดหรือจุดเตือนภัย (Trigger Point) ของระดับหรือสถานความเสี่ยง

Likelihood

โอกาสที่จะเกิด

โอกาสของเหตุการณ์ที่จะเกิดขึ้น โดยการพิจารณาจากสถิติการเกิดเหตุการณ์ในอดีต ปัจจุบัน หรือการคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต

Likelihood Rating

ระดับของโอกาสเกิด

ผลการประเมินโอกาสของเหตุการณ์ที่จะเกิดขึ้น โดยการพิจารณาจากสถิติการเกิดเหตุการณ์ในอดีต ปัจจุบัน หรือ การคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต

Link to Causes

กลไกการควบคุมเชิงป้องกันเชื่อมโยงกับสาเหตุเรื่องใดและกลไกนั้นสามารถช่วยป้องกัน/มีส่วนช่วยป้องกันสาเหตุเรื่องใด

Link to Impact

กลไกที่องค์กรมีอยู่แล้ว สามารถเชื่อมโยงในการช่วยแก้ไข/มีส่วนช่วยแก้ไขผลกระทบเรื่องใด

Major Program And Project : MPP

การบริหารจัดการความเสี่ยงในระดับโปรแกรม/โครงการขนาดใหญ่

การบริหารจัดการความเสี่ยงในระดับโปรแกรม/โครงการ จะดำเนินการเฉพาะโปรแกรมขนาดใหญ่ที่มีขอบเขตการดำเนินงาน วัตถุประสงค์ งบประมาณ บทบาทหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องอย่างชัดเจน

Mitigation Action Report : MAR

รายงานผลการจัดการความเสี่ยง

Mitigation Action Plan : MAP

แผนบริหารจัดการความเสี่ยง

Operational Risk

ความเสี่ยงด้านปฏิบัติการ

ความเสี่ยงเนื่องจากการปฏิบัติงานภายในองค์กร อันเกิดจากกระบวนการ บุคลากร ความเพียงพอของข้อมูล ส่งผลต่อประสิทธิภาพและประสิทธิผลในการดำเนินธุรกิจ เช่น ความเสี่ยงของกระบวนการบริหารโครงการ การบริหารงานวิจัย ระบบงานต่างๆ ที่สนับสนุนการดำเนินงาน

Residual Risk Rating

ผลคูณระหว่างโอกาสเกิดและผลกระทบ เป็นระดับคะแนนของความเสี่ยง

Risk Analysis

การวิเคราะห์ความเสี่ยง

การวิเคราะห์ความเสี่ยงจะเป็นข้อมูลเพื่อใช้ในการประเมินความเสี่ยง และการตัดสินใจในการจัดการกับความเสี่ยง โดยการพิจารณาถึงโอกาสในการเกิด (Likelihood) และผลกระทบ (Impact)

Risk Appetite : RA

ค่าระดับความเสี่ยงที่องค์กรต้องการ

ค่าระดับความเสี่ยงในเชิงปริมาณหรือเชิงคุณภาพที่องค์กรสามารถยอมรับความเสียหาย/สูญเสียจากความเสี่ยง

Risk Assessment

การประเมินความเสี่ยง

กระบวนการการประมาณระดับความเสี่ยง และการตัดสิน ว่าความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้หรือไม่

Risk Boundary

ขอบเขตของคะแนนระดับความเสี่ยงที่องค์กรยอมรับได้

ขอบเขตของคะแนนระดับความเสี่ยงที่ยอมรับได้ตามที่องค์กร/หน่วยงานกำหนด

Risk Identification

การระบุความเสี่ยง

เป็นการระบุถึงแหล่งที่มาของความเสี่ยง และระบุปัจจัยเสี่ยง ตลอดจนพื้นที่ที่ได้รับผลกระทบ เหตุการณ์อาจทำให้ความสำเร็จของวัตถุประสงค์เปลี่ยนแปลงไป และสาเหตุรวมถึงผลที่จะตามมา

Risk Identification : Risk ID

เป็นการกำหนดรหัสชื่อเรียก (Code) เพื่อให้เข้าใจตรงกันอย่างชัดเจนว่ารายการความเสี่ยงที่จัดการอยู่นี้เกี่ยวข้องกับความเสี่ยงเรื่องใด ตัวอย่างเช่น RES-1

ตัวที่ 1 แทนด้วยตัวอักษร R = Risk เพื่อแสดง ว่าเป็นรหัสในระบบบริหารความเสี่ยง

ตัวที่ 2 แทนระดับองค์กร E = Enterprise เพื่อแสดงว่าเป็นระบบบริหารความเสี่ยงระดับองค์กร

ตัวที่ 3 แทนประเภทของความเสี่ยง S-O-F-C

ตัวที่ 4 แทนลำดับที่ของรายการความเสี่ยงแต่ละประเภท (ระบุหมายเลข 1,2,3.....ตามลำดับที่ได้รับ)

Risk Management

การบริหารจัดการความเสี่ยง

กระบวนการบริหารจัดการองค์กรโดยมีการวางแผนป้องกันและรองรับผลกระทบที่อาจเกิดขึ้นในอนาคต เพื่อลดความเสียหายที่อาจเกิดขึ้น

Risk Mitigation Tasks

กิจกรรม/การดำเนินงานเพิ่มเติมเพื่อปรับปรุงแก้ไขและบรรเทาความเสี่ยง (รวมทั้งการปรับปรุงกลไกที่มีอยู่เดิม) เพื่อใช้ในการป้องกันสาเหตุ และแก้ไขผลกระทบหรือการดำเนินการมิให้เกิดผลกระทบที่รุนแรง

Risk Monitor Report : RMR

รายงานการติดตามความเสี่ยง

Risk Rating "Before" Mitigation

ระดับคะแนนของความเสี่ยงก่อนดำเนินการจัดการความเสี่ยงตามมาตรการที่กำหนด

Risk Rating "After" Mitigation

ระดับคะแนนของความเสี่ยงหลังจากได้ดำเนินการจัดการความเสี่ยงตามมาตรการที่กำหนด

Risk owner

ชื่อและตำแหน่งของผู้รับผิดชอบความเสี่ยง โดยมีหน้าที่ระบุสาเหตุ ปัจจัยของความเสี่ยง รับผิดชอบในการดูแลควบคุมมาตรการจัดการความเสี่ยง พร้อมทั้งประเมินและตัดสินใจตามแนวทางการลดหรือควบคุมความเสี่ยง

ผู้ช่วย Risk owner

ชื่อของผู้ช่วยผู้รับผิดชอบความเสี่ยง เพื่อช่วยผู้รับผิดชอบความเสี่ยง (Risk owner) จัดเตรียมข้อมูลสำหรับการวิเคราะห์ ประเมิน จัดทำแผนบริหารจัดการความเสี่ยง และติดตามผลการดำเนินงาน รวมทั้งประสานงานผู้เกี่ยวข้องในการจัดประชุม/หารือตามความเหมาะสม

Risk Profile

ผังภูมิความเสี่ยง

ผังภูมิแสดงสถานะของระดับความเสี่ยง โดยแสดงเป็นพิกัดของโอกาสและผลกระทบของความเสี่ยง เทียบเป็นสี 4 ระดับ คือ สีแดง ระดับสูงมาก (Very high) สีส้ม ระดับสูง (High) สีเหลือง ระดับปานกลาง (Medium) และสีเทา ระดับต่ำ (Low)

Risk Tolerance : RT

ค่าระดับความเสี่ยงที่องค์กรยอมรับได้

ค่าเบี่ยงเบนสูงสุด/ต่ำสุดของระดับความเสี่ยงที่ยอมรับได้จากเป้าหมายหรือวัตถุประสงค์ที่กำหนดไว้

Strategic Business Unit : SBU

การบริหารจัดการความเสี่ยงในระดับศูนย์แห่งชาติ/หน่วยงานหลัก

บทบาทการบริหารจัดการความเสี่ยงในระดับศูนย์แห่งชาติ/หน่วยงานหลัก ตามโครงสร้างการบริหารงานของ สวทช. ประกอบด้วย สำนักงานกลาง 1 หน่วย และศูนย์ 5 ศูนย์แห่งชาติ

Strategic Risk

ความเสี่ยงด้านกลยุทธ์

ความเสี่ยงที่มีผลกระทบต่อทิศทาง หรือ ภารกิจหลักขององค์กร หรือมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร อันเนื่องมาจาก การเมือง เศรษฐกิจ ความเปลี่ยนแปลงของสถานการณ์ เหตุการณ์ภายนอก ผู้ใช้บริการ ฯลฯ หรือความเสี่ยงที่เกิดจากการตัดสินใจผิดพลาดหรือนำการตัดสินใจนั้นมาใช้อย่างไม่ถูกต้อง

Task Owner

ผู้ที่รับผิดชอบ/หน่วยงานที่รับผิดชอบการดำเนินงาน/กิจกรรม