เกณฑ์ประเมินผล Enabler ด้านการบริหารความเสี่ยงและการควบคุมภายใน (Risk Management & Internal Control: RM&IC)

สำหรับระบบประเมินผลการดำเนินงานรัฐวิสาหกิจ ปี 2563

ประเด็นนำเสนอ

01

หลักการ/แนวคิดในการพัฒนา

ทฤษฎี แนวความคิด มาตรฐาน และข้อมูลต่าง ๆ ที่นำมาประยุกต์ใช้ในการพัฒนาเกณฑ์ประเมินผลฯ ด้านบริหารความเสี่ยงและควบคุมภายใน

02

เกณฑ์ประเมินผลฯ ด้าน Risk & IC

รายละเอียดเกณฑ์ประเมินผลฯ ด้านด้านการบริหารความเสี่ยงและการควบคุมภายใน (Risk Management & Internal Control: RM&IC)) ทั้งด้าน ธรรมาภิบาลและวัฒนธรรมองค์กร การกำหนดยุทธศาสตร์และวัตถุประสงค์/เป้าประสงค์เชิงยุทธศาสตร์ กระบวนการบริหารความเสี่ยง **การทบทวนการบริหารความเสี่ยง รวมทั้งสารสนเทศ และการรายงานผล**

การบริหารความเสี่ยง และการควบคุมภายใน

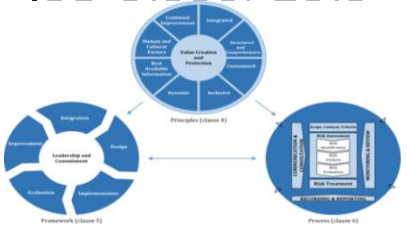
เกณฑ์การประเมินผลการบริหารความเสี่ยงและการควบคุมภายใน พัฒนาตามมาตรฐานใด

?

หลักการ/แนวคิด

COSO 2017

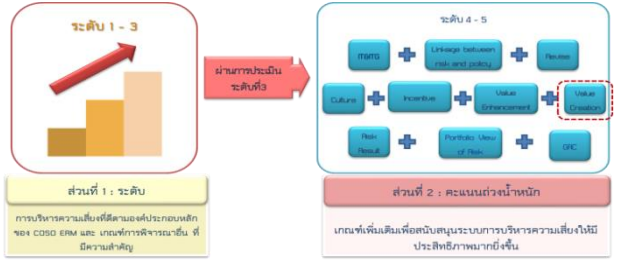
ISO 31000: 2018



COSO 2013

COBIT 5
AN ISACA® FRAMEWORK

Risk Management



Internal Control

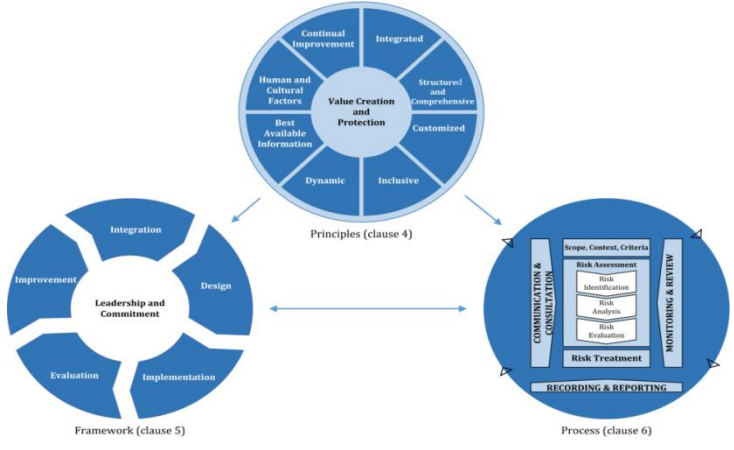
SEPA-หมวด 2

เกณฑ์การประเมินการบริหารความเสี่ยงการควบคุมภายในประยุกต์มาจากเกณฑ์ของ COSO (The Committee of Sponsoring Organization of Treadway Commission) โดยพัฒนามาจาก

- COSO 2013- internal Control และ
- COSO 2017 Enterprise Risk Management integrating with Strategy and Performance
- รวมทั้งการประยุกต์เกณฑ์ที่สอดคล้องตามมาตรฐาน ISO31000 version 2018

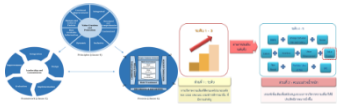
COSO 2017 - Enterprise Risk Management integrating with Strategy and Performance

ทั้งนี้เกณฑ์ประเมินผลระบบใหม่ ใช้พื้นฐานตามกรอบแนวคิดของ COSO 2017 ซึ่งให้ความสำคัญกับการมุ่งสร้างมูลค่าเพิ่มให้กับองค์กร และการดำเนินงานที่สอดคล้องไปกับกระบวนการจัดทำยุทธศาสตร์ และการควบคุมภายในไปพร้อมๆกัน โดยการเริ่มตั้งแต่คณะกรรมการ /ผู้บริหาร คือ การมีธรรมาภิบาล และการสร้างวัฒนธรรมองค์กร ให้เห็นถึงความสำคัญของการบริหารความเสี่ยง ว่าความเสี่ยงไม่ใช่จุดด้อย /จุดอ่อนขององค์กร แต่เป็นการสร้างความมั่นใจ หรือการประกันผลการดำเนินงานในระดับหนึ่งว่าเป้าหมายองค์กรตามยุทธศาสตร์ที่กำหนดไว้ จะสามารถบรรลุได้อย่างชัดเจน ไปจนถึงการเชื่อมโยงการทำแผนยุทธศาสตร์องค์กร ที่ไปในทิศทางเดียวกับกระบวนการบริหารความเสี่ยง และการกำหนดระดับความเสี่ยง/เป้าหมายความเสี่ยงที่เป็นรูปธรรม มีแผนงานที่ชัดเจน สามารถปรับเปลี่ยนแปลงได้ทันท่วงที จนถึงการมีระบบในการเตือนภัยล่วงหน้า ว่าองค์กรมีแนวโน้มการบรรลุเป้าหมาย ได้ตามที่กำหนดไว้หรือไม่



ISO 31000: 2018 – Risk Management

การเปรียบเทียบองค์ประกอบภาพรวมด้านการบริหารความเสี่ยงและการควบคุมภายในที่ดีของหลักการที่เป็นที่ยอมรับทั้งในและต่างประเทศ



เกณฑ์การประเมินผล	COSO 2017 ERM	ISO 31000:2018 RM	SEPO RM	COBIT 5	SEPO Strategic planning	COSO 2013 IC	SEPO IC
1. ธรรมาภิบาล และวัฒนธรรมองค์กร (Governance & Culture)	✓	✓	✓	✓	-	✓	✓
2. การกำหนดยุทธศาสตร์และวัตถุประสงค์เชิงยุทธศาสตร์ (Strategy & Objectives Setting)	✓	✓	✓	✓	✓	✓	-
3. กระบวนการบริหารความเสี่ยง (Performance)	✓	✓	✓	✓	-	✓	✓ -
4. การทบทวนการบริหารความเสี่ยง (Review & Revision)	✓	✓	✓	✓	✓	-	-
5. ข้อมูลสารสนเทศ การสื่อสาร และการรายงานผล (Information Communication & Reporting)	✓	✓	✓	✓	-	✓	✓

ร่างเกณฑ์ประเมินผลการบริหารความเสี่ยงและการควบคุมภายใน (Risk Management & Internal Control : Risk &IC

COSO 2017

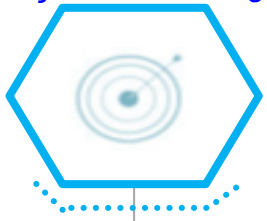
ISO 31000: 2018

COSO 2013

1. Governance & Culture

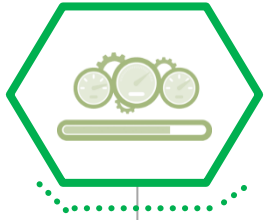
1. บทบาทหน้าที่คณะกรรมการในการบริหารความเสี่ยงและการควบคุมภายในการกำหนดนโยบาย GRC โครงสร้าง บทบาทหน้าที่ การกำหนด RA ระดับองค์กร จัดให้มีบรรยากาศและวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยงและการควบคุมภายใน (Culture) รวมถึงการกำหนดแรงจูงใจสำหรับการบริหารความเสี่ยง

2. Strategy & Objectives Setting



2. การวิเคราะห์ และเชื่อมโยงกระบวนการบริหารความเสี่ยงและกลยุทธ์การบริหารความเสี่ยง กับนโยบายวัตถุประสงค์เชิงยุทธศาสตร์ ยุทธศาสตร์ แผนงานโครงการ และแผนการลงทุน การกำหนด Risk Appetite/Risk Tolerance และการบริหารความเสี่ยงเป็นการสนับสนุนการบริหารเพื่อสร้างสรรค์มูลค่าให้กับองค์กร (Value Creation) - การสนับสนุนการบริหารฯ เพื่อเพิ่มมูลค่า (Value Enhancement)

3. Performance



3. องค์ประกอบการบริหารความเสี่ยงที่ครบถ้วนตั้งแต่การระบุความเสี่ยงที่ครอบคลุมตามวัตถุประสงค์ และเป้าหมายองค์กร การพิจารณาความเพียงพอของกิจกรรมควบคุม ประเมินระดับความเสี่ยงการจัดลำดับความสำคัญการกำหนดแผนจัดการความเสี่ยง โดยมีกระบวนการวิเคราะห์ Cost Benefit ที่ชัดเจนในแต่ละทางเลือก การจัดทำ Risk correlation map และ Portfolio view of risk

4. Review & Revision

4. การรายงานผลการบริหารความเสี่ยง ที่สอดคล้องพร้อมรายงานผลการดำเนินงานองค์กร เพื่อให้สามารถวิเคราะห์ประเด็นที่อาจเกิดขึ้นใหม่ การเปลี่ยนแปลงที่สำคัญ รวมทั้งการทบทวนและปรับปรุงการบริหารความเสี่ยงสม่ำเสมอและทำการปรับปรุงเมื่อจำเป็น

5. Information Communication & Reporting

5. การสื่อสารการบริหารความเสี่ยงองค์กร การรายงานผลการบริหารความเสี่ยง และการประเมินผลการควบคุมภายใน ทั้งการประเมินเป็นรายครั้ง และประเมินแบบต่อเนื่อง โดยมีการวิเคราะห์เพื่อปรับปรุง และทบทวนกระบวนการบริหารความเสี่ยงและการควบคุมภายในองค์กร รวมทั้งการใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนการบริหารความเสี่ยงที่ดี

TRIS CORP

TRIS CORP Idea Solution Performance

ร่างเกณฑ์ประเมินผลการบริหารความเสี่ยงและการควบคุมภายใน (Risk Management & Internal Control : Risk &IC

1. Governance & Culture

- 1.1 Exercises Board Risk & internal Control Oversight
- 1.2 Establishes Operating structures
- 1.3 Defines Desired Culture
- 1.4 Demonstrates Commitment to Core Values
- 1.5 Attracts, Develops, and Retains Capable Individuals

2. Strategy & Objectives Setting

- 2.1 Analyzes Business Context
- 2.2 Defines Risk Appetite
- 2.3 Evaluates Alternative Strategies
- 2.4 Formulates Business Objectives

3. Performance

- 3.1 Identifies Risk
- 3.2 selects and develops control activities
- 3.3 Assesses Severity of Risk
- 3.4 Prioritizes Risks
- 3.5 Implements Risk Responses
- 3.6 Develops Portfolio View- Risk Correlation Map & Portfolio view of Risk

4. Review & Revision

- 4.1 Reviews Risk and Performance
- 4.2 Pursues Improvement in Enterprise Risk Management
- 4.3 Assesses Substantial Change

5. Information Communication & Reporting

- 5.1 Communicates Risk Information
- 5.2
- 5.3 Leverages Information and Technology and Early warning system

what's important: Enterprise risk management is as much about understanding the *implications from the strategy and the possibility of strategy not aligning* as it is about managing risks to set objectives. The figure below illustrates these considerations in the context of mission, vision, core values, and as a driver of an entity's overall direction and performance.

Enterprise risk management enhances strategy selection. Choosing a strategy calls for structured decision-making that analyzes risk and aligns resources with the mission and vision of the organization.

Enterprise Risk Management—Integrating with Strategy and Performance clarifies the importance of enterprise risk management in strategic planning and embedding it throughout an organization—because risk influences and aligns strategy and performance across all departments and functions

ENTERPRISE RISK MANAGEMENT

Governance & Culture | Strategy & Objective-Setting | Performance | Review & Revision | Information, Communication, & Reporting

1. Governance and Culture
ธรรมาภิบาลและวัฒนธรรมองค์กร

1. Governance & Culture

ENTERPRISE RISK MANAGEMENT

1. **Exercises Board Risk Oversight:**
   The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes Operating Structures:**
   The organization establishes operating structures in the pursuit of strategy and business objectives.
3. **Defines Desired Culture:**
   The organization defines the desired behaviors that characterize the entity's desired culture.
4. **Demonstrates Commitment to Core Values:**
   The organization demonstrates a commitment to the entity's core values.
5. **Attracts, Develops, and Retains Capable Individuals:**
   The organization is committed to building human capital in alignment with the strategy and business objectives.

กระบวนการสร้างธรรมาภิบาล (Governance)

SIPOC

Process

การกำหนด**นโยบายที่บูรณาการในเรื่องกำกับดูแลกิจการที่ดีการบริหารความเสี่ยง และการควบคุมภายใน (GRC)**

1) การกำหนดนโยบาย GRC องค์กร โดยคณะกรรมการรัฐวิสาหกิจ คณะกรรมการบริหารความเสี่ยงหรือคณะกรรมการที่เกี่ยวข้อง
2) การกำหนด Risk Appetite (RA) ระดับองค์กร โดยคณะกรรมการรัฐวิสาหกิจ คณะกรรมการบริหารความเสี่ยงหรือคณะกรรมการที่เกี่ยวข้อง
3) นำไปสื่อสารและติดตามผล

การนำไปสู่การปฏิบัติ

ฝ่ายงานที่เกี่ยวข้องมีการดำเนินงานตามแนวทาง G R C ตามแนวทางที่กำหนดครบถ้วน

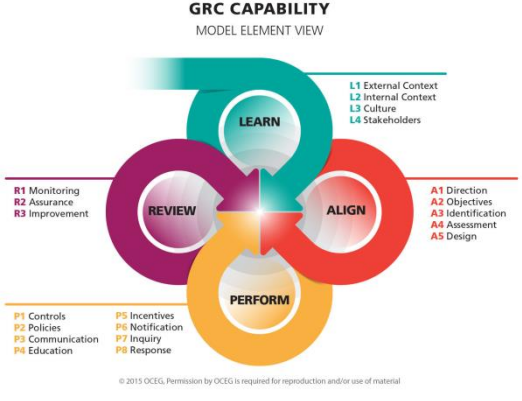
ทบทวนกระบวนการ

มีการทบทวนนโยบายกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการควบคุมภายใน (GRC) เพื่อให้เหมาะสมกับ นโยบายอื่นๆที่เกี่ยวข้องขององค์กร

เชื่อมโยง

- แผนแม่บท CG
- แผนแม่บท HR

ตัวอย่างองค์ประกอบ GRC



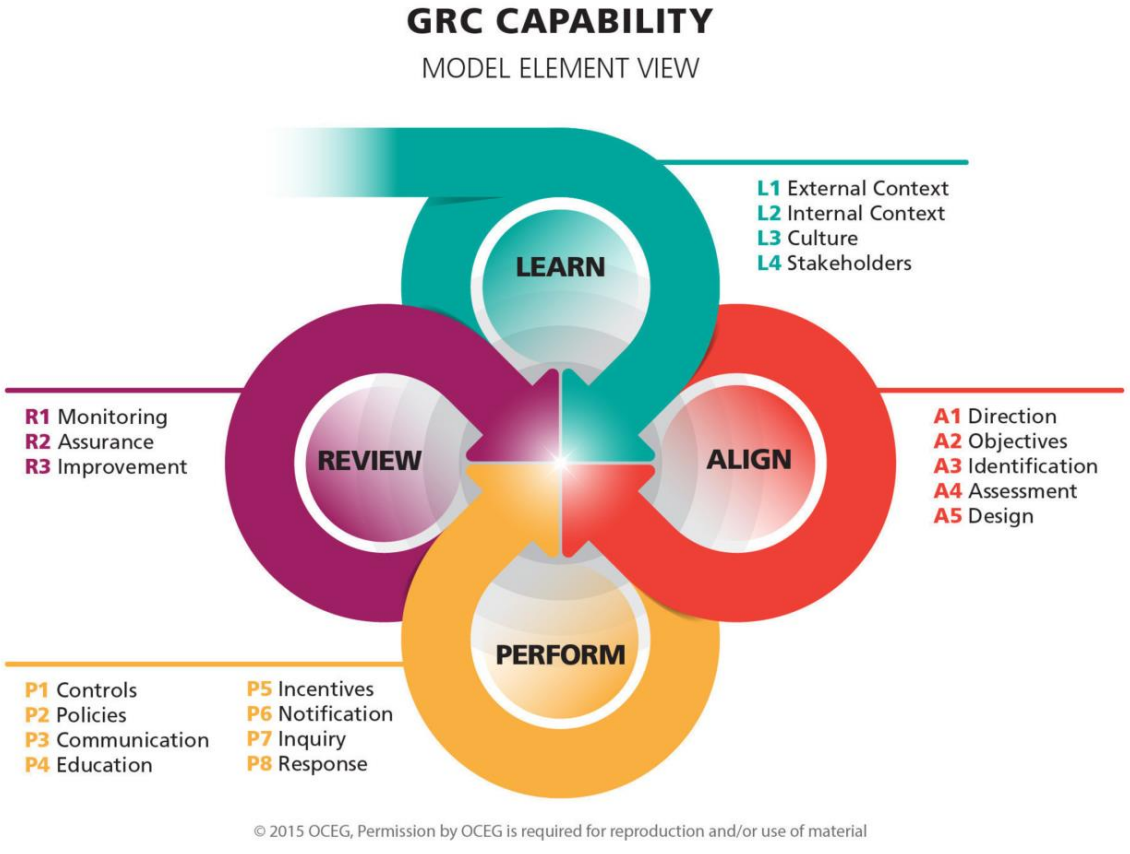
1. Governance and Culture
ธรรมาภิบาลและวัฒนธรรมองค์กร

1.1 Exercises Board Risk Oversight and the development and performance of Internal control (บทบาทคณะกรรมการในการกำกับติดตามการบริหารความเสี่ยงและการพัฒนาระบบการควบคุมภายใน)

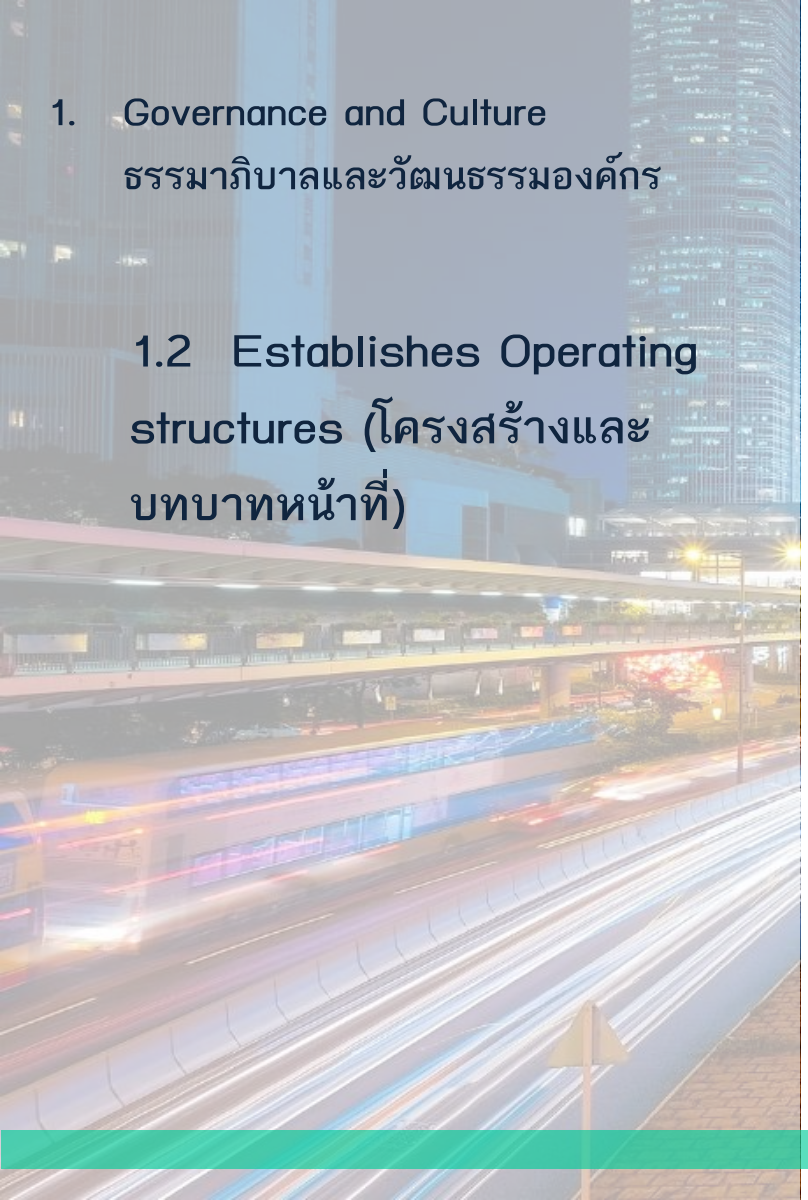
กระบวนการกำหนดนโยบายและการกำกับดูแลด้านการบริหารความเสี่ยงและการควบคุมภายในแบบบูรณาการ (GRC)
การกำหนดโครงร้างและบทบาทหน้าที่ที่เกี่ยวข้องกับการบริหารความเสี่ยงและการควบคุมภายใน การกำหนด RA ระดับองค์กร กระบวนการจัดทำคู่มือและการสื่อสาร คู่มือที่เป็นแนวปฏิบัติที่ดีและชัดเจน การสร้างบรรยากาศ วัฒนธรรม ความตระหนักในการบริหารความเสี่ยง และมีการติดตามประเมินระดับการรับรู้ ความเข้าใจ ความตระหนักที่เป็นระบบ รวมทั้งการพัฒนาและสร้างแรงจูงใจในการบริหารความเสี่ยงกับผลการดำเนินงานขององค์กรที่เป็นรูปธรรม

1) การกำหนดนโยบายที่บูรณาการในเรื่องกำกับดูแลกิจการที่ดีการบริหารความเสี่ยง และการควบคุมภายใน (GRC) รวมทั้งการกำหนดหลักการในการกำหนด Risk Appetite (RA) ระดับองค์กร โดยคณะกรรมการรัฐวิสาหกิจ คณะกรรมการบริหารความเสี่ยงหรือคณะกรรมการที่เกี่ยวข้อง
2) การเผยแพร่นโยบาย กำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการควบคุมภายใน (GRC) แก่พนักงาน และหน่วยงานที่เกี่ยวข้องภายนอกอย่างทั่วถึง
3) นำนโยบายที่บูรณาการในเรื่องกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการควบคุมภายใน (GRC) ไปปฏิบัติอย่างเป็นรูปธรรม
4) การทบทวนโยบายกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการควบคุมภายใน (GRC) เพื่อให้เหมาะสมกับ นโยบายอื่นๆที่เกี่ยวข้องขององค์กร
5) การปรับปรุงนโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการควบคุมภายใน (GRC) ให้สอดคล้องกับบริบทของรัฐวิสาหกิจและมาตรฐานสากลที่เปลี่ยนแปลงไป

GRC



การกำหนดนโยบายที่มีความเชื่อมโยงและสอดคล้องในนโยบายเดียวกันที่มุ่งเน้นการบูรณาการทั้ง 3 เรื่อง ทั้ง Governance Risk Compliance



1. Governance and Culture
ธรรมาภิบาลและวัฒนธรรมองค์กร

1.2 Establishes Operating structures (โครงสร้างและบทบาทหน้าที่)

1) การมีหน่วยงานเพื่อจัดการความเสี่ยงและการควบคุมภายในที่ชัดเจน โดยกำหนดโครงสร้าง บทบาทหน้าที่ของมีผู้ที่ที่รับผิดชอบการบริหารจัดการความเสี่ยง และการควบคุมภายในที่ชัดเจน
2) การกำหนดและสรรหาบุคลากรที่มีคุณสมบัติ และความรู้ความสามารถในการบริหารความเสี่ยงและการควบคุมภายใน และมีการทำงานที่เป็นรูปธรรมอย่างจริงจัง รวมทั้งกำหนดบทบาท อำนาจหน้าที่ และ กระบวนการในการดำเนินงาน ที่ชัดเจนเป็นรูปธรรม (มีการกำหนดหน้าที่งาน (Job Description:JD มีโครงสร้างความรับผิดชอบ มีแผนงานรองรับ) และการกำหนดแผนงานของการดำเนินงานตามโครงสร้างผู้รับผิดชอบที่ชัดเจน รวมถึงสามารถบรรลุเป้าหมายในแผนงานได้ครบถ้วน และกระบวนการจัดทำคู่มือการบริหารความเสี่ยงที่มีองค์ประกอบที่ครบถ้วน เพื่อให้สามารถนำไปปฏิบัติได้อย่างชัดเจน
3) โครงสร้างหน่วยงาน/คณะทำงานฯ มีการทำงานมีการทำงานที่เป็นรูปธรรมอย่างจริงจัง
4) โครงสร้างและบทบาทหน้าที่ด้านการบริหารความเสี่ยงและการควบคุมภายใน สอดคล้องกับการกำหนดโครงสร้างและบทบาทหน้าที่ของกระบวนการทำงานอื่นรวมทั้งมีการสื่อสารผู้บริหารมีการติดตามติดตามผลการดำเนินงานของหน่วยงาน/คณะทำงนที่รับผิดชอบฯ โดยสามารถดำเนินงานตามแผนงานของหน่วยงาน และสามารถบรรลุเป้าหมายตามแผนการปฏิบัติงานนั้นได้ครบถ้วน และมีกระบวนการในการตรวจสอบถึงความเข้าใจของผู้บริหารและพนักงานในคู่มือดังกล่าว
5) การประเมินประสิทธิผลของการกำหนดโครงสร้างและบทบาทหน้าที่ โดยมีการติดตามผลการดำเนินงานของหน่วยงาน/คณะทำงนที่รับผิดชอบ และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ กำหนดโครงสร้างและบทบาทหน้าที่ รวมทั้งทบวนการจัดทำแผนปฏิบัติการของปีต่อไปพื่อให้เกิดกระบวนการจัดการความเสี่ยงที่บูรณาการจากทุกหน่วยงาน และการทบทวน /ปรับปรุง คู่มือการบริหารความเสี่ยง

1. Governance and Culture
ธรรมาภิบาลและวัฒนธรรมองค์กร

1.3 Defines Desired Culture (บรรยากาศและวัฒนธรรมสนับสนุนการบริหารความเสี่ยง)

1) จัดให้มีบรรยากาศและวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยง (Culture)
2) การกำหนดกระบวนการ/ดำเนินการสร้างความตระหนักเกี่ยวกับความสำคัญหรือความรู้ความเข้าใจของการบริหารความเสี่ยงในองค์กร ครอบคุลมทั้งคณะกรรมการ รส. คณะกรรมการบริหารความเสี่ยง ผู้บริหาร และพนักงาน
3) การฝึกอบรม/ชี้แจง/ทำความเข้าใจถึงพื้นฐานด้านการบริหารความเสี่ยง โดยมีการให้ความรู้กับผู้บริหาร (3 อันดับแรก) และพนักงานที่เกี่ยวข้อง (Risk Owner) และประเมินความรู้ความเข้าใจ
4) กระบวนการ/ดำเนินการสร้างความตระหนักเกี่ยวกับความสำคัญ/ความรู้ความเข้าใจของการบริหารความเสี่ยงในองค์กร มีความสอดคล้องกับกระบวนการพัฒนาบุคลากร และหัวข้ออื่นที่เกี่ยวข้อง เช่น เช่น แผนยุทธศาสตร์ด้าน HR แผนแม่บทเทคโนโลยีดิจิทัล เป็นต้น
5) การสำรวจทัศนคติของพนักงานในเรื่องการบริหารความเสี่ยงขององค์กร และสามารถสรุปผลการสำรวจเสนอผู้บริหารในสายงานที่เกี่ยวข้อง โดยมีแผนงานในการปรับปรุงจากข้อสังเกตที่ได้จากการสำรวจ รวมถึงผลการสำรวจต้องดีขึ้นจากปีที่ผ่านมา หรือ จากผลการสำรวจครั้งก่อน แล้วแต่ว่าครั้งใดเป็นครั้งล่าสุด

Governance

Operating Structure and Reporting Lines

Enterprise Risk Management Structures

Accountability and Responsibility

Skills, Experience, and Business Knowledge

Independence

Suitability of Enterprise Risk Management

Organizational Bias

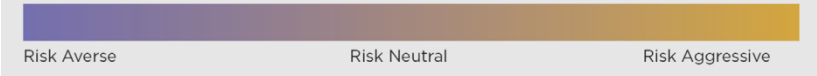
Risk Culture

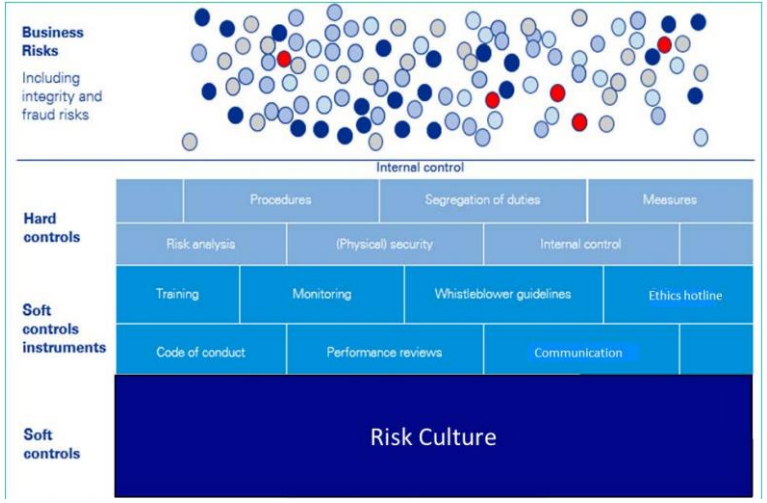
Culture

Instilling more transparency and risk awareness into an entity's culture requires actions such as:

- Implementing forums or other mechanisms for sharing information, making decisions, and identifying opportunities.
- Encouraging people to escalate issues and concerns without fear of retribution.
- Clarifying and communicating roles and responsibilities for the achievement of strategy and business objectives, including responsibilities for the management of risk.
- Aligning core values, behaviors, and decision-making with incentives and remuneration models.
- Developing and sharing a strong understanding of the business context and drivers of value creation.

Figure 6.1: Culture Spectrum





Source: Deloitte (2012) 'Cultivating a Risk Intelligent Culture: Understand, measure, strengthen, and report'
Source: McKinsey (2015) 'Managing the People Side of Risk: Risk Culture Transformation'

Source: M. Kaptein, Professor Business Ethics at Erasmus University, Feb 10th, 2017

1. Governance and Culture
ธรรมาภิบาลและวัฒนธรรมองค์กร

1.4 Demonstrates Commitment to Core Values (ความมุ่งมั่นต่อค่านิยมองค์กร)

1) การกำหนดกระบวนการในการสร้างวัฒนธรรมองค์กรด้านความเสี่ยงที่มุ่งตอบสนองและส่งเสริมค่านิยมองค์กร
2) การทบทวนสถานการณ์ความเสี่ยงที่จะช่วยให้ทุกคนเข้าใจถึงความสัมพันธ์และผลกระทบของความเสี่ยงก่อนตัดสินใจ ของคณะกรรมการ คณะกรรมการบริหารความเสี่ยง ผู้บริหาร และพนักงาน และกระบวนการในการกระตุ้นให้เกิดการรับรู้ถึงความเสี่ยงในองค์กรและการสร้างบรรยากาศและวัฒนธรรมสนับสนุนการบริหารความเสี่ยง
3) การพัฒนาและสร้างพฤติกรรมในการสร้างวัฒนธรรมองค์กรด้านความเสี่ยงที่มุ่งตอบสนองและส่งเสริมค่านิยมองค์กร ครอบคลุมทั้งคณะกรรมการ รส. คณะกรรมการบริหารความเสี่ยง ผู้บริหาร และพนักงาน
4) ระบวนการ/ดำเนินการสร้างความตระหนักเกี่ยวกับความสำคัญ/ความรู้ความเข้าใจของการบริหารความเสี่ยงในองค์กร มีความสอดคล้องกับกระบวนการพัฒนาบุคลากร และหัวข้ออื่นที่เกี่ยวข้อง เช่น แผนยุทธศาสตร์ด้าน HR แผนแม่บทเทคโนโลยีดิจิทัล เป็นต้น
5) การสำรวจทัศนคติ/พฤติกรรมของพนักงานในเรื่องการส่งเสริมพฤติกรรมในการสร้างวัฒนธรรมองค์กรด้านความเสี่ยงที่มุ่งตอบสนองค่านิยมองค์กร และสามารถสรุปผลการสำรวจเสนอผู้บริหารในสายงานที่เกี่ยวข้อง โดยมีแผนงานในการปรับปรุงจากข้อสังเกตที่ได้จากการสำรวจ รวมถึงผลการสำรวจต้องดีขึ้นจากปีที่ผ่านมา หรือ จากผลการสำรวจครั้งก่อน แล้วแต่ว่าครั้งใดเป็นครั้งล่าสุด

1. Governance and Culture
ธรรมาภิบาลและวัฒนธรรมองค์กร

1.5 Attracts, Develops, and Retains Capable Individuals (แรงจูงใจ การพัฒนาและการรักษาบุคลากร)

1) การกำหนดแผนงานในการเชื่อมโยงผลการประเมินเฉพาะการบริหารความเสี่ยงกับผลตอบแทน/แรงจูงใจในการประเมินผู้บริหารแต่ละระดับอย่างชัดเจน (Incentive)
2) ดำเนินการได้จริงในการเชื่อมโยงผลการประเมินเฉพาะการบริหารความเสี่ยงกับผลตอบแทน/แรงจูงใจในการประเมินผู้บริหารแต่ละระดับอย่างชัดเจน
3) การถ่ายทอดตัวชี้วัดระดับองค์กรลงสู่ระดับสายงาน โดยเฉพาะตัวชี้วัดการบริหารความเสี่ยงทั้งในลักษณะของปัจจัยเสี่ยงของสายงาน และกิจกรรมที่สายงานต้องสนับสนุนการบริหารความเสี่ยง โดยทุกฝ่ายงาน/สายงานที่องค์กรต้องมีการจัดทำ Risk Profile ของแต่ละสายงาน และสามารถผูกแรงจูงใจในแต่ละขั้นกับ Risk Profile ของฝ่ายงานในแต่ละระดับที่สามารถลดระดับความรุนแรงลงได้ครบถ้วน
4) กระบวนการเชื่อมโยงผลการประเมินเฉพาะการบริหารความฯ มีความเชื่อมโยงกับกระบวนการบริหารทุนมนุษย์ ในการประเมินผลการดำเนินงานและการถ่ายทอดความเสี่ยงระดับสายงานสอดคล้องกับการวิเคราะห์แผนงานโครงการและการประเมินความเสี่ยงแผนงานของแต่ละสายงาน
5) การทบทวนแนวทางการกำหนดการเชื่อมโยงผลการประเมินเฉพาะการบริหารความเสี่ยงกับผลตอบแทน/แรงจูงใจในการประเมิน

Enterprise risk management[1] **is defined here as:**

The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value.

[1]*Souce: Enterprise Risk Management – Integrating with Strategy and Performance COSO2017 , june 2017*

2. Strategy & Objectives Setting
การกำหนดยุทธศาสตร์และวัตถุประสงค์/เป้าประสงค์เชิงยุทธศาสตร์

ENTERPRISE RISK MANAGEMENT

STRATEGY & OBJECTIVE SETTING

6. **Analyzes Business Context:**
   The organization considers potential effects of business context on risk profile.
7. **Defines Risk Appetite:**
   The organization defines risk appetite in the context of creating, preserving, and realizing value.
8. **Evaluates Alternative Strategies:**
   The organization evaluates alternative strategies and potential impact on risk profile.
9. **Formulates Business Objectives:**
   The organization considers risk while establishing the business objectives at various levels that align and support strategy.

2. Strategy &
Objectives Setting

กระบวนการการระบุเป้าหมายการบริหารความเสี่ยง (Risk Appetite :RA))

SIPOC

Process

กระบวนการในการกำหนดความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite: RA) ในลักษณะของระดับที่เป็นเป้าหมาย (ค่าเดียว) หรือช่วง (Risk Appetite) และการกำหนดช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้นั้น (Risk Tolerance: RT)

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

2) คำนึงถึงความต้องการของผู้มีส่วนได้เสียทุกกลุ่ม ต้องมีการถ่ายทอด Risk Appetite/ Risk Tolerance ที่ถ่ายทอดจากวัตถุประสงค์เชิงธุรกิจ Business Objective โดยสามารถระบุได้ว่าเป็น Strategic Risk/ Operational Risk/Financial Risk และ Compliance Risk (S-O-F-C) หรือประเภทความเสี่ยงตามที่กำหนด

การนำไปสู่การปฏิบัติ

การสื่อสารและถ่ายทอด RA RT ต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ที่สอดคล้องตามสาเหตุของแต่ละปัจจัยเสี่ยงที่กำหนด

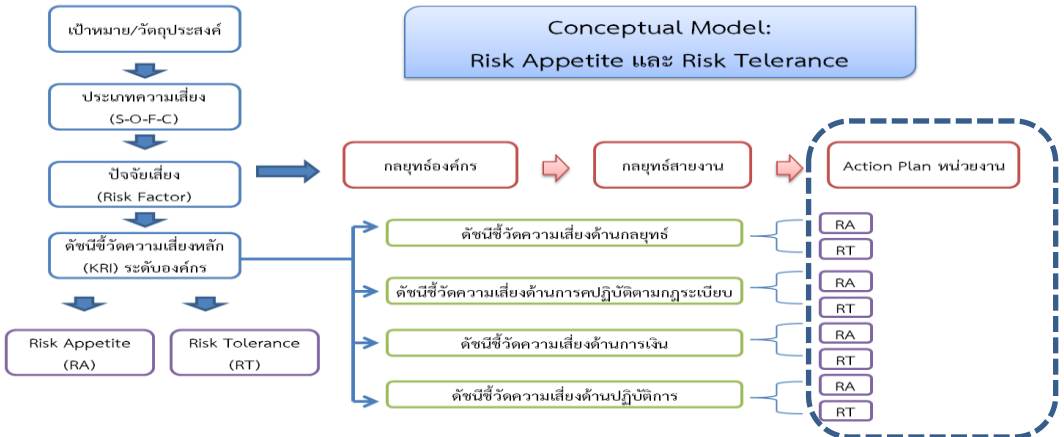
ทบทวนกระบวนการ

มีการประเมินประสิทธิผลของการกำหนดค่า RA RT ที่สอดคล้องกับเป้าหมายองค์กร (Business Objective) ที่มีการเปลี่ยนแปลงระหว่างปีได้ทันกาล และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

เชื่อมโยง

- แผนยุทธศาสตร์
- แผนแม่บทต่างๆ

ตัวอย่างการกำหนด RA RT ที่เชื่อมโยงกับเป้าหมายองค์กร



2.1 Analyzes Business Context

(การวิเคราะห์ธุรกิจ) (ประเมินในหัวข้อการวางแผนเชิงกลยุทธ์
-การวิเคราะห์ธุรกิจการวางแผนเชิงกลยุทธ์ หัวข้อย่อย-การวิเคราะห์สภาพแวดล้อม (Environmental Scanning)

2.2 Defines Risk Appetite

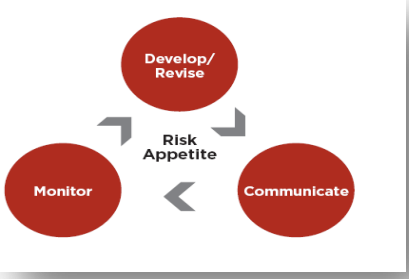
(การระบุเป้าหมายการบริหารความเสี่ยง (Risk Appetite :RA))

1) กระบวนการในการกำหนดความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite: RA) ในลักษณะของระดับที่เป็นเป้าหมาย (ค่าเดียว) หรือช่วง (Risk Appetite) และการกำหนดช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้นั้น (Risk Tolerance: RT)
2) การระบุ Risk Appetite และ Risk Tolerance โดยสามารถแสดงให้เห็นถึงความเชื่อมโยง/ความสอดคล้องกับเป้าหมาย/วัตถุประสงค์ขององค์กรได้อย่างชัดเจน (Business Objective) และคำนึงถึงความต้องการของผู้มีส่วนได้เสียทุกกลุ่ม ต้องมีการถ่ายทอด Risk Appetite/ Risk Tolerance ที่ถ่ายทอดจากวัตถุประสงค์เชิงธุรกิจ Business Objective โดยสามารถระบุได้ว่าเป็น Strategic Risk/ Operational Risk/ Financial Risk และ Compliance Risk (S-O-F-C) หรือประเภทความเสี่ยงตามที่กำหนด
3) รวมทั้งมีกระบวนการในการสื่อสารและถ่ายทอด RA RT ต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ที่สอดคล้องตามสาเหตุของแต่ละปัจจัยเสี่ยงที่กำหนด
4) การดำเนินการกำหนด Risk Appetite ต้องสอดคล้องกับเป้าหมายขององค์กรประจำปีบัญชี (Business Objective) ที่ระบุในแผนยุทธศาสตร์ (แผนระยะยาว) และแผนปฏิบัติการประจำปี และมีการกำหนด Risk Tolerance โดยมีความสอดคล้องกับระดับขององค์กรที่ยอมให้เบี่ยงเบนได้ที่ระบุในแผนปฏิบัติการประจำปี หรือเป็นค่าที่ผ่านการอนุมัติจากคณะกรรมการ
5) มีการประเมินประสิทธิผลของการกำหนดค่า RA RT ที่สอดคล้องกับเป้าหมายองค์กร (Business Objective) ที่มีการเปลี่ยนแปลงระหว่างปีได้ทันกาล และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

2. Strategy & Objectives Setting
การกำหนดยุทธศาสตร์และวัตถุประสงค์/เป้าประสงค์เชิงยุทธศาสตร์

กระบวนการในการกำหนดวัตถุประสงค์เชิงยุทธศาสตร์ และยุทธศาสตร์ การวางแผนการลงทุนที่สำคัญ ที่เชื่อมโยงกับการกระบวนการบริหารความเสี่ยงองค์กร รวมทั้งการกำหนดเป้าหมายการบริหารความเสี่ยง (Risk Appetite) ที่สอดคล้องกับเป้าประสงค์/เป้าหมายขององค์กร รวมทั้งการสร้างมูลค่าเพิ่มองค์กรด้วยการบริหารความเสี่ยง Value Creation และ Value Enhancement เพื่อให้สามารถตอบสนองและเชื่อมโยงกับวัตถุประสงค์เชิงยุทธศาสตร์ และสร้างมูลค่าเพิ่มให้กับองค์กร ได้

Risk Appetite



> Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so.

Factors to consider in setting Risk appetite

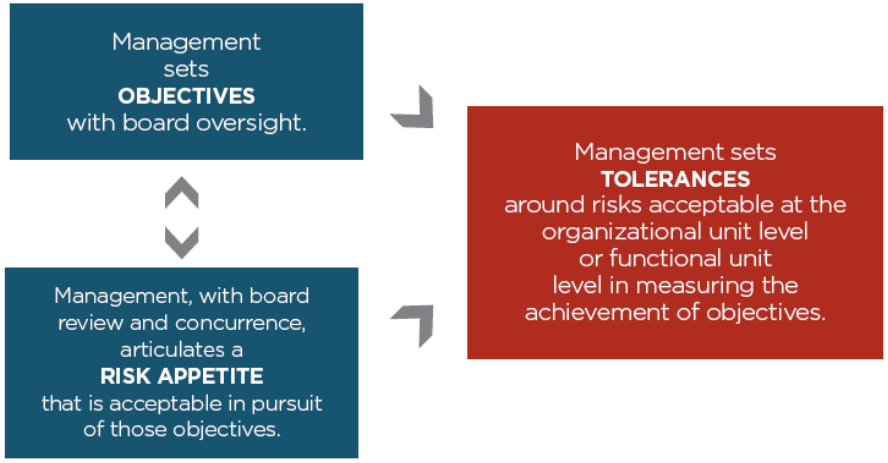
Overview of Considerations Affecting Risk Appetite

Existing Risk Profile	The current level and distribution of risks across the entity and across various risk categories
Risk Capacity	The amount of risk that the entity is able to support in pursuit of its objectives
Risk Tolerance	Acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives
Attitudes Towards Risk	The attitudes towards growth, risk, and return

Determination of Risk Appetite

Source: Dr. Larry Rittenberg and Frank Martens . Understanding and Communicating Risk Appetite, Enterprise Risk Management.

Risk Tolerance



Risk tolerance is the risk exposure an organization determines appropriate to take or avoid. Clarity enables an organization to know with certainty what risk exposure it can take and what risk exposures it must avoid.

Determining risk tolerance involves applying judgment giving careful consideration to five key factors.

- Your organization's attitude toward taking risk.
- Your organization's goals
- Your organization's capability to manage the risk.
- Your organization's capacity to absorb the impact of potential loss related to taking the risk.
- The Cost/benefit of managing the risk.

Cascading Risk Appetite

Example 7.5: Cascading Risk Appetite

Mission: To provide healthy, great-tasting premium organic foods made from locally sourced ingredients.

Vision: To be the largest producer of sustainably sourced organic products in the markets we serve.

Core Values: We work to achieve a healthy environment that is sustainable. We will use ingredients grown only in natural composts, non-altered crops, and soil rich in organic life.

Strategy: To build brand loyalty by producing food that is delicious and exciting, that people want to eat because it tastes good, not because it is good for them.

Risk Appetite: Brand is essential to us. We have a lower risk appetite for making any decisions that challenge our brand. We will not make decisions that put cost above our core values, product quality, or ingredient choice. Nor will we make decisions that put growth above sustainable operations. However, we will strive to be innovative to develop products that meet customers' preferences and accept risk viewed as moderately severe (or less) that leads to impacts on brand.

Business Objective: To continue to develop new, innovative products that interest and excite consumers.

Risk Appetite: We will continue to strive to be innovative and find new tastes. We understand that such a focus has a more moderate risk profile and will manage the risk of failing to develop new tastes our customers desire with the opportunity to enhance our product offerings.

Risk Appetite: We will not make decisions that compromise our brand by using products that are not certified organic. We accept that this may increase our cost.

Business Objective: To expand our retail presence in the higher-end health food sector.

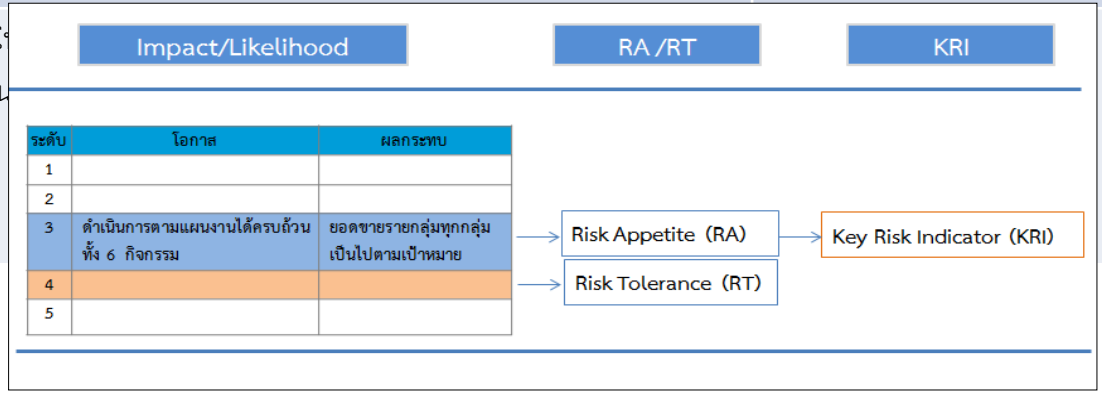
Risk Appetite: We value our brand as a premium product and will focus only on those retailers that share our core values. We have a lower risk appetite relating to decisions impacting our retail presence. We will only accept risks that impact retail presence where we believe that we can increase the long-term value of the company and those retailers share our values. We understand that making decisions in this manner may affect our sales channel.

Figure 7.4 Risk Appetite, Tolerance, and Limits and Triggers

Appetite	• Applies through development of strategy and setting of objectives • Focuses on overall goals of the business (objective-centric) • Aids in decision-making • Aids in evaluation at the portfolio level • Ties strategy to measures
Tolerance	• Applies in the implementation of strategy • Focuses on objectives and variation from plan (objective-centric) • Aids in decision-making and in evaluation • Ties strategy to measures
Indicators and Triggers	• Applies at any level of the business • Considers specific risks, usually in isolation (risk-centric) • Ties risks to measures (e.g., key indicators)

การระบุ Risk Appetite และ Risk Tolerance

ประเภทความเสี่ยง	ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)	ช่วงเบี่ยนเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance)
ด้านกลยุทธ์ (Strategic Risk)	สอดคล้องตามเป้าประสงค์ในแผนยุทธศาสตร์	ค่าระดับ 3 ตาม BSC (หากเชื่อมโยงกับเกณฑ์ชี้วัดใน Balanced Scorecard องค์กร)
ด้านการเงิน (Financial Risk)	สามารถรักษาระดับความสามารถในการสร้างความมั่นคงทางการเงินในระยะยาว (ตามแผนยุทธศาสตร์ ที่ระบุในแต่ละปี)	ค่าระดับ 3 ตาม BSC (หากเชื่อมโยงกับเกณฑ์ชี้วัดใน Balanced Scorecard องค์กร)
ด้านการดำเนินงาน (Operation Risk)	คุณภาพการให้บริการ ประสิทธิภาพการดำเนินงาน (ตามแผนยุทธศาสตร์ ที่ระบุในแต่ละปี)	ค่าระดับ 3 ตาม BSC (หากเชื่อมโยงกับเกณฑ์ชี้วัดใน Balanced Scorecard องค์กร)
ด้านการปฏิบัติตามกฎระเบียบที่เกี่ยวข้อง (Compliance Risk)	การดำเนิ หน่วยงาน	



2.3 Evaluates Alternative Strategies

(การประเมินทางเลือกและกำหนดยุทธศาสตร์) - ประเมินในหัวข้อการวางแผนเชิงกลยุทธ์ หัวข้อย่อย-การกำหนดยุทธศาสตร์ /กลยุทธ์ (Strategic Formulation))

2.4 Formulates Business Objectives

(การกำหนดวัตถุประสงค์ในการดำเนินธุรกิจเพื่อสร้างมูลค่าเพิ่มให้กับองค์กร) - ในส่วนการกำหนด Business Objectives ประเมินในหัวข้อการวางแผนเชิงกลยุทธ์ หัวข้อย่อย - การกำหนดวัตถุประสงค์เชิงยุทธศาสตร์ (Strategic Objective)

1) การทำ Value Creation และ Value Enhancement เพื่อให้เชื่อมโยงกับวัตถุประสงค์เชิงยุทธศาสตร์ ในการนำมาบริหารและสร้างมูลค่าเพิ่มให้กับองค์กร ได้
2) การระบุเหตุการณ์ที่เป็นโอกาสของธุรกิจ ซึ่งมีความสัมพันธ์กับการระบุโอกาส (Opportunity)ใน SWOT ขององค์กร และได้มีการวิเคราะห์ถึงปัจจัยเสี่ยงของเหตุการณ์ดังกล่าว และนำมาเข้ากระบวนการบริหารความเสี่ยง จนสามารถทำให้ระดับความรุนแรงของปัจจัยเสี่ยงดังกล่าวลดลง ด้วยการวิเคราะห์สภาพแวดล้อมทั้งภายในและภายนอกธุรกิจอีกครั้ง หลังจากที่ได้มีการบริหารความเสี่ยงแล้ว รวมถึงเสนอคณะกรรมการ รส. เพื่ออนุมัติ
3) การกำหนดแผนบริหารความเสี่ยงสำหรับความเสี่ยงที่ส่งผลในการที่สร้างความมั่นใจถึงการเป็นองค์กรแห่งการเรียนรู้ (Learning Organization) และได้ดำเนินการตามแผนการบริหารความเสี่ยงดังกล่าวครบถ้วน ระดับความรุนแรงของความเสี่ยงที่ส่งผลในการที่สร้างความมั่นใจถึงการเป็นองค์กรแห่งการเรียนรู้ (Learning Organization) ลดลงได้ตามเป้าหมายที่กำหนด
4) กระบวนการ/ดำเนินการการทำ Value Creation และ Value Enhancement มีความสอดคล้องกับกระบวนการกำหนดตำแหน่งเชิงยุทธศาสตร์ วัตถุประสงค์เชิงยุทธศาสตร์ แผนยุทธศาสตร์องค์กร รวมถึงแผนแม่บทที่เกี่ยวข้อง เช่น แผนงาน KM เป็นต้น
5) มีการประเมินประสิทธิผลของการทำ Value Creation และ Value Enhancement เพื่อให้เชื่อมโยงกับวัตถุประสงค์เชิงยุทธศาสตร์ ในการนำมาบริหารและสร้างมูลค่าเพิ่มให้กับองค์ก ที่สอดคล้องกับเป้าหมายองค์กร (Business Objective) รวมทั้งวัตถุประสงค์เชิงยุทธศาสตร์ และยุทธศาสตร์ ที่มีการเปลี่ยนแปลงระหว่างปีได้ทันกาล และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

2. Strategy & Objectives Setting
การกำหนดยุทธศาสตร์และวัตถุประสงค์/เป้าประสงค์เชิงยุทธศาสตร์

2.4 Formulates Business Objectives

(การกำหนดวัตถุประสงค์ในการดำเนินธุรกิจเพื่อสร้างมูลค่าเพิ่มให้กับองค์กร)

3. Performance
(กระบวนการบริหารความเสี่ยง)

3. Performance

ENTERPRISE RISK MANAGEMENT

10. **Identifies Risk:**
    The organization identifies risk that impact the performance of strategy and business objectives.
11. **Assesses Severity of Risk:**
    The organization assesses the severity of risk.
12. **Prioritizes Risks:**
    The organization prioritizes risks as a basis for selecting responses to risks.
13. **Implements Risk Responses:**
    The organization identifies and selects risk responses.
14. **Develops Portfolio View:**
    The organization develops and evaluates a portfolio view of risk.

** เกณฑ์การประเมินผลมีประเด็นของการพิจารณาเพิ่มเติมจาก 5 องค์ประกอบย่อยข้างต้น

การพิจารณาความเพียงพอของกิจกรรมควบคุม (Design Control Activity)

กระบวนการการระบุปัจจัยเสี่ยง

SIPOC

Process

กระบวนการในการระบุความเสี่ยงระดับองค์กรที่สอดคล้องกับประเภทความเสี่ยงที่องค์กรกำหนดและการกำหนดประสิทธิผลของความเพียงพอของการควบคุม

1) พิจารณาว่ามีความเสี่ยงใดบ้างที่เกี่ยวข้องกับการดำเนินกิจการขององค์กร โดยต้องมีการพิจารณาที่มาที่ครอบคลุม ทั้งจากปัจจัยภายในปัจจัยภายนอก ยุทธศาสตร์และเป้าหมายที่สำคัญขององค์กร จุดอ่อน ความต้องการความคาดหวังของผู้มีส่วนได้ส่วนเสีย ตัวชี้วัดที่สำคัญขององค์กร (Inherent Risk) เพื่อกำหนด Risk Universe
2) พิจารณาประสิทธิผลของการควบคุมภายใน โดยมีความเชื่อมโยงกับเป้าหมายประจำปีขององค์กร และสามารถแสดงถึงความเชื่อมโยงระหว่างปัจจัยเสี่ยงที่เหลืออยู่ในปีก่อนหน้ากับปีที่ประเมินได้ชัดเจน

เชื่อมโยง

แผนยุทธศาสตร์ และแผนต่างๆ ที่เกี่ยวข้อง

นโยบาย และสภาพแวดล้อมภายนอก

การนำไปสู่การปฏิบัติ

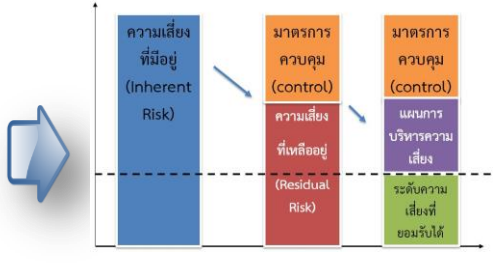
การถ่ายทอดความเสี่ยงระดับองค์กร ให้กับสายงานที่รับผิดชอบ และมีการระบุความเสี่ยงในระดับสายงาน ที่รองรับความเสี่ยงองค์กรและยุทธศาสตร์องค์กร และแผนงานของสายงาน

ทบทวนกระบวนการ

มีการประเมินประสิทธิผลของการระบุปัจจัยเสี่ยงระดับองค์กร และระดับสายงาน และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

ตัวอย่างการระบุปัจจัยเสี่ยง (Risk Identification) ที่ครอบคลุม

Risk Universe



Corporate Risk

3. Performance
(กระบวนการบริหารความเสี่ยง)

การระบุขั้นตอนในการระบุความเสี่ยงระดับองค์กรที่สอดคล้องกับประเภทความเสี่ยงที่องค์กรกำหนด โดยต้องพิจารณาว่ามีความเสี่ยงใดบ้างที่เกี่ยวข้องกับยุทธศาสตร์ ทิศทาง และการดำเนินกิจการขององค์กร (Risk Universe) การกำหนด/ประเมินกิจกรรมการควบคุมภายในที่ครอบคลุมกิจกรรมขององค์กร การประเมินระดับความรุนแรงของความเสี่ยงโดยการใช้ฐานข้อมูลในอดีตในการพิจารณา การจัดลำดับความสำคัญในการจัดการความเสี่ยงระดับองค์กร จนสามารถนำไปกำหนดแผนในการจัดการ/ตอบสนองความเสี่ยงที่เชื่อมโยงกับกิจกรรมการควบคุมภายในที่มี และสัมพันธ์ตามสาเหตุที่ได้กำหนดใน การจัดทำการบริหารความเสี่ยงเชิงบูรณาการ (Risk Correlation Map) รวมทั้งการพัฒนาเป็น Portfolio View of Risk) เพื่อให้รู้จักองค์กรสามารถวิเคราะห์และบริหารความเสี่ยงได้ครบกระบวนการที่ดี ที่สามารถสร้างความมั่นใจการบรรลุเป้าหมายองค์กร

3.1 Identifies Risk (การระบุปัจจัยเสี่ยง)

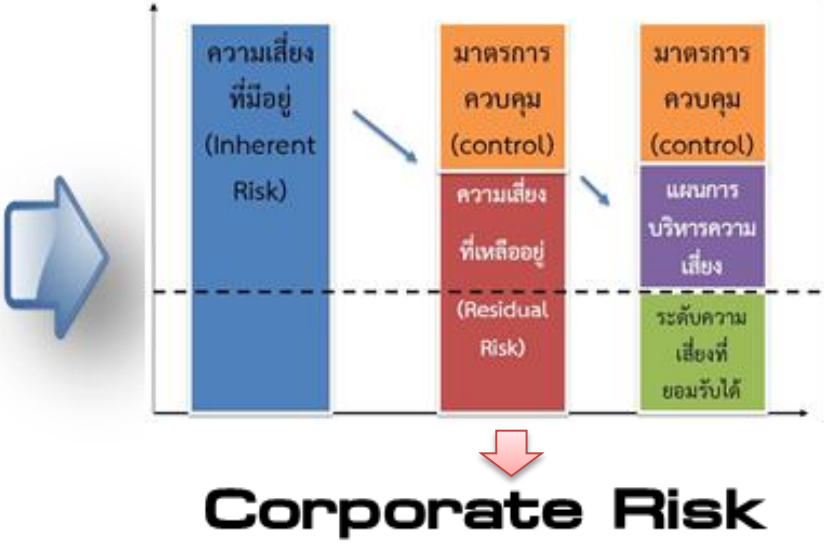
- การระบุความเสี่ยงระดับองค์กรที่สอดคล้องกับประเภทความเสี่ยงที่องค์กรกำหนด โดยต้องพิจารณาว่ามีความเสี่ยงใดบ้างที่เกี่ยวข้องกับการดำเนินกิจการขององค์กร โดยต้องมีการพิจารณาที่มาที่ครอบคลุม ทั้งจากปัจจัยภายใน ปัจจัยภายนอก ยุทธศาสตร์และเป้าหมายที่สำคัญขององค์กร จุดอ่อน ความต้องการความคาดหวังของผู้มีส่วนได้ส่วนเสีย ตัวชี้วัดที่สำคัญขององค์กร (Inherent Risk) เพื่อกำหนด Risk Universe
- กำหนดประสิทธิผลของความเพียงพอของการควบคุม รวมทั้งการพิจารณาถึงระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) หลังจากพิจารณาประสิทธิผลของการควบคุมภายใน โดยมีความเชื่อมโยงกับเป้าหมายประจำปีขององค์กร และสามารถแสดงถึงความเชื่อมโยงระหว่างปัจจัยเสี่ยงที่เหลืออยู่ในปีก่อนหน้ากับปีที่ประเมินได้ชัดเจน มีการประเมินประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด มีการสื่อสารปัจจัยเสี่ยงที่มีการระบุต่อผู้รับผิดชอบ (Risk Owner) ที่เกี่ยวข้อง
- กระบวนการในการถ่ายทอดความเสี่ยงระดับองค์กร ให้กับสายงานที่รับผิดชอบ และมีการระบุความเสี่ยงในระดับสายงาน ที่รองรับความเสี่ยงองค์กรและยุทธศาสตร์องค์กร และแผนงานของสายงาน นอกจากนี้ กรณีที่ รส. มีบริษัทลูก ต้องมีการกำหนดความเสี่ยงองค์กรที่ครอบคลุม
- การดำเนินการระบุความเสี่ยงองค์กร ที่สอดคล้องกับกระบวนการและกิจกรรมควบคุมภายในกระบวนการประเมินประสิทธิผลการควบคุมภายใน รวมทั้งการพิจารณาถึงระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) หลังจากการควบคุมภายใน โดยมีความเชื่อมโยงกับเป้าหมายประจำปีขององค์กร และสามารถแสดงถึงความเชื่อมโยงระหว่างปัจจัยเสี่ยงที่เหลืออยู่ในปีก่อนหน้ากับปีที่ประเมินได้ชัดเจน
- มีการประเมินประสิทธิผลของการระบุความเสี่ยงระดับองค์กร และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

Risk Identification : Tools

1. Documentation reviews
2. Information-gathering techniques
   - Brainstorming
   - Delphi technique
   - Interviewing
   - Root cause Analysis
3. Checklists
4. Assumptions analysis
5. Diagramming techniques
   - Cause-and-effect diagrams
   - Influence diagrams
   - System or process flow charts
6. Strengths, weaknesses, opportunities and threats (SWOT) analysis
7. Expert judgment

ตัวอย่างการระบุปัจจัยเสี่ยง (Risk Identification) ที่ครอบคลุม

Risk Universe



3. Performance
(กระบวนการบริหารความเสี่ยง)

3.2 Selects and Develops Control Activities (การกำหนดกิจกรรมการควบคุม

- การกำหนดและพัฒนากิจกรรมการควบคุม เพื่อควบคุมความเสี่ยงในแต่ละกิจกรรมขององค์กร
- มีกระบวนการในการประเมินความเพียงพอของระบบการควบคุมภายใน ประกอบการระบุปัจจัยเสี่ยงระดับองค์กร และทุกสายงานมีการประเมินกิจกรรมการควบคุมประกอบการวิเคราะห์ปัจจัยเสี่ยงระดับสายงาน ได้ครบถ้วนทุกสายงาน
- ทุกสายงานมีการประเมินกิจกรรมการควบคุมประกอบการวิเคราะห์ปัจจัยเสี่ยงระดับสายงาน ได้ครบถ้วนทุกสายงาน การประเมินประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด (ความครบถ้วนของปัจจัย , กระบวนการ , ผลผลิต , ระยะเวลาที่แล้วเสร็จ)
- กิจกรรมการควบคุมที่กำหนด มีการบูรณาการกับกระบวนการพัฒนาเทคโนโลยีดิจิทัลในการนำระบบเทคโนโลยีดิจิทัล มาพัฒนากิจกรรมการควบคุม และกิจกรรมการควบคุมสอดคล้องกับแผนงาน/แผนปฏิบัติการประจำปีที่เกี่ยวข้อง
- มีการทบทวนกิจกรรมการควบคุมระหว่างปี เพื่อให้กิจกรรมการควบคุมเป็นส่วนหนึ่งของแผนงานจัดการความเสี่ยงที่สนับสนุนให้ความเสี่ยงบรรลุตามเป้าหมายที่กำหนด

3. Performance
(กระบวนการบริหารความเสี่ยง)

3.3 Assesses Severity of Risk (การประเมินระดับความรุนแรงของปัจจัยเสี่ยง)

- การกำหนดเกณฑ์ประเมินระดับความรุนแรง ทั้งในเชิงโอกาส และผลกระทบแยกรายปัจจัยเสี่ยง
- การกำหนดเกณฑ์ประเมินระดับความรุนแรง โดยการใช้ฐานข้อมูลในอดีต หรือ การคาดการณ์ในอนาคตเพื่อประกอบกับการกำหนดระดับความรุนแรงของแต่ละปัจจัยเสี่ยง ทั้งนี้การกำหนดระดับความรุนแรง (โอกาส และผลกระทบ) ต้องสัมพันธ์กับขอบเขตระดับความเสี่ยงที่องค์กรสามารถรับได้ (Risk Boundary) เพื่อจัดลำดับความเสี่ยง และกำหนดเป้าหมายในเชิงระดับความรุนแรงที่คาดหวังของทุกปัจจัยเสี่ยงได้อย่างชัดเจนการดำเนินการประเมินระดับความรุนแรงรายปัจจัยเสี่ยงได้ครบถ้วนตามกระบวนการที่กำหนด
- มีการสื่อสารเกณฑ์การประเมินระดับความรุนแรงของแต่ละปัจจัยเสี่ยง ต่อผู้รับผิดชอบ (Risk Owner) ที่เกี่ยวข้อง
- การกำหนดระดับความรุนแรง มีความเชื่อมโยงกับฐานข้อมูลองค์กรในการใช้ระบบเทคโนโลยีดิจิทัลในการนำระบบเทคโนโลยีดิจิทัล มาพัฒนาการกำหนดเกณฑ์วัดระดับความรุนแรง เพื่อกำหนดเป็นฐานข้อมูล
- การรายงานผลระดับความรุนแรงของแต่ละปัจจัยเสี่ยงรายไตรมาส เทียบกับเป้าหมายที่คาดหวัง พร้อมวิเคราะห์ถึงปัญหา/อุปสรรค และแนวทางที่จะบรรลุถึงเป้าหมาย และมีการประเมินประสิทธิผลของการกำหนดเกณฑ์ประเมินระดับความรุนแรง ทั้งในเชิงโอกาส และผลกระทบและนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

3. Performance
(กระบวนการบริหารความเสี่ยง)

3.4 Prioritizes Risks (การจัดลำดับความเสี่ยง)

1) การกำหนดขอบเขตระดับความเสี่ยงที่องค์กรสามารถรับได้ (Risk Boundary) การกำหนดระดับความเสี่ยง (สูง ปานกลาง ต่ำ) และการจัดลำดับความเสี่ยง ของแต่ละปัจจัยเสี่ยง และการจัดทำแผนภาพความเสี่ยง (Risk Profile)
2) การดำเนินการตามขั้นตอนที่สำคัญครบถ้วน และทุกขั้นตอนสามารถเป็นไปตามกระบวนการที่กำหนด
3) การแสดงผลการจัดลำดับความเสี่ยง และรายงานผลรายไตรมาส
4) การบูรณาการกำหนดขอบเขตระดับความเสี่ยงที่องค์กรสามารถรับได้ (Risk Boundary) การกำหนดระดับความเสี่ยง (สูง ปานกลาง ต่ำ) กับเป้าประสงค์ และวัตถุประสงค์เชิงยุทธศาสตร์ขององค์กร และค่าความเสี่ยงที่ยอมรับได้ (Risk Appetite)
5) การประเมินประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด (ความครบถ้วนของปัจจัย , กระบวนการ , ผลผลิต , ระยะเวลาที่แล้วเสร็จ) การประเมินประสิทธิผลของการการกำหนดขอบเขตระดับความเสี่ยงที่องค์กรสามารถรับได้ (Risk Boundary) และการจัดลำดับความเสี่ยง ของแต่ละปัจจัยเสี่ยง และการจัดทำแผนภาพความเสี่ยง (Risk Profile) และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ "

3. Performance
(กระบวนการบริหารความเสี่ยง)

3.5 Implements Risk Responses (การกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยงที่ระบุไว้)

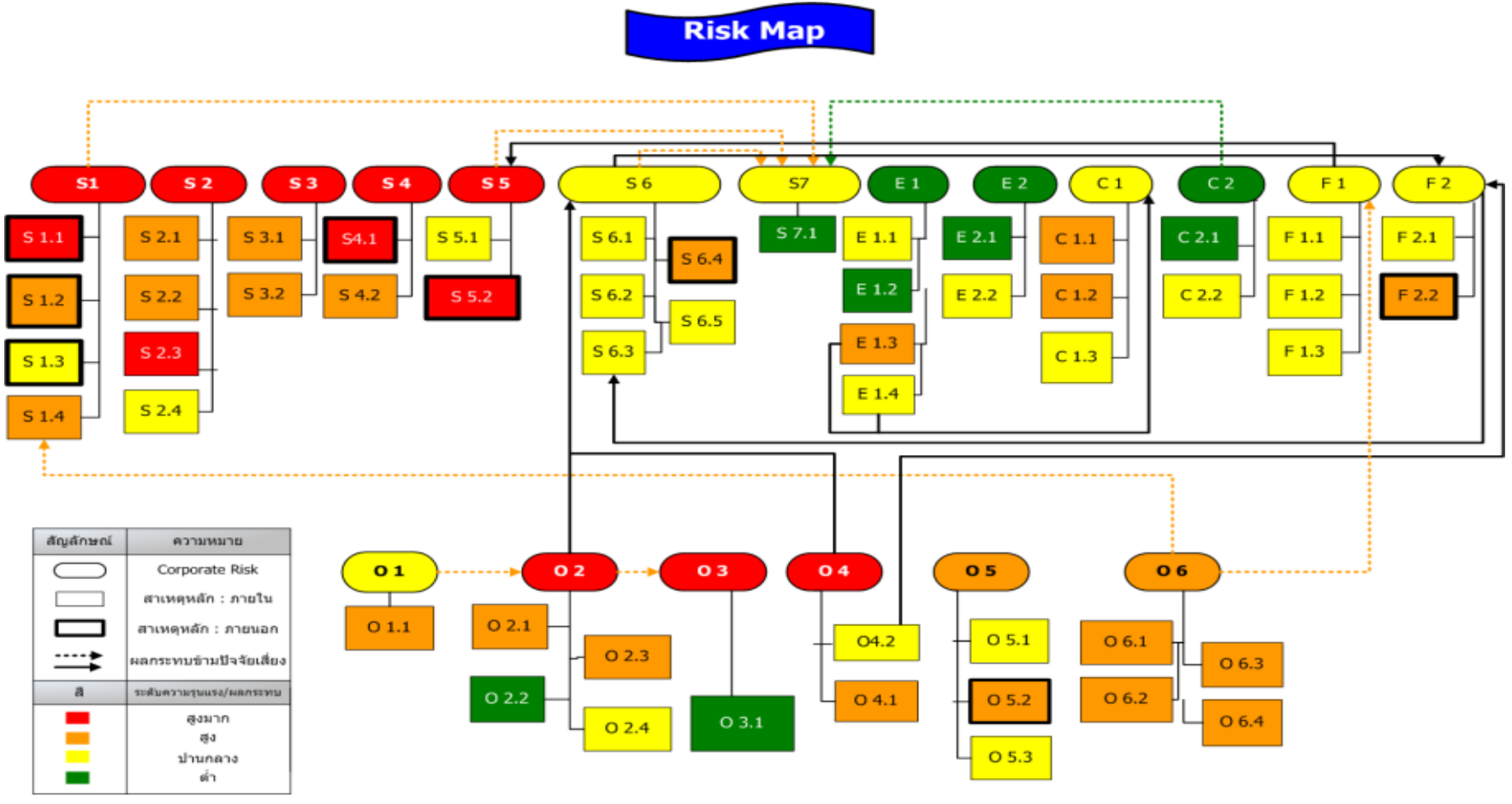
1) การกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยง (Mitigation) ที่ระบุไว้
2) พิจารณาถึงวิธีการ/แผนงานจัดการความเสี่ยงเพื่อลดผลกระทบ หรือลดโอกาสที่จะเกิด รวมทั้งกระบวนการและหลักเกณฑ์ในการประเมินค่าใช้จ่ายและผลประโยชน์ที่ได้ (Cost Benefit) ในการจัดการความเสี่ยงในแต่ละทางเลือก ในทุกความเสี่ยงที่เหลืออยู่ (Residual Risk) ที่ผ่านการจัดลำดับความเสี่ยงในการกำหนดเป็นความเสี่ยงระดับองค์กร และสรุปเป็นแผนงานจัดการความเสี่ยงในแต่ละความเสี่ยงระดับองค์กร
3) การกำหนดเกณฑ์ในการพิจารณาแผนงาน/กิจกรรมการควบคุม (ประสิทธิผลการควบคุมภายใน) ร่วมกับการพิจารณาเพื่อกำหนด/คัดเลือกวิธีการจัดการความเสี่ยง ในการคัดเลือกวิธีการจัดการความเสี่ยงที่ชัดเจน
4) การบูรณาการการ การกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยง (Mitigation) กับการวิเคราะห์ความเสี่ยงเชิงบูรณาการ (Risk Correlation Map) และกระบวนการอื่น เช่น การกำหนดกิจกรรมการควบคุม แผนปฏิบัติการต่างๆ ที่เกี่ยวข้อง รวมทั้งการออกแบบระบบงาน (Work System) และกระบวนการ (Work Process) ในการดำเนินงานขององค์กร เป็นต้น
5) มีการประเมินประสิทธิผลของการกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยง (Mitigation) และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

3. Performance
(กระบวนการบริหารความเสี่ยง)

3.6 Develops Portfolio View
(การบริหารความเสี่ยงแบบบูรณาการ (Risk Correlation Map) และการจัดทำ Portfolio View of Risk)

- การกำหนดกระบวนการในการพิจารณาถึงความสัมพันธ์ของความเสี่ยงและผลกระทบที่มีระหว่างหน่วยงานต่างๆ ภายในองค์กร โดย Risk Correlation Map ขององค์กร ที่มีการกำหนดสาเหตุของความเสี่ยงในทุกปัจจัยเสี่ยง และสามารถกำหนดระดับความรุนแรงของแต่ละสาเหตุในทุกปัจจัยเสี่ยง การวิเคราะห์ความสัมพันธ์ของปัจจัยเสี่ยงและสาเหตุ การวิเคราะห์ผลกระทบทั้งในเชิงปริมาณและเชิงคุณภาพระหว่างปัจจัยเสี่ยงและผลกระทบของสาเหตุ และกระบวนการในการแสดงผลดังกล่าวผ่านแผนภาพ Risk Correlation Map และนำไปกำหนดแผนจัดการความเสี่ยง
- การดำเนินการจัดทำ Risk Correlation Map ขององค์กร ได้ตามกระบวนการครบถ้วนและดำเนินงานร่วมกันเจ้าของความเสี่ยง (Risk Owner)
- การกำหนดกระบวนการในการวิเคราะห์ถึงภาพรวมของความเสี่ยง (Portfolio View of Risk) โดยผ่านการวิเคราะห์ถึงในช่วงความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ในแต่ละปัจจัยเสี่ยง กับช่วงความเบี่ยงเบนของความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ในระดับองค์กร และการจัดทำแบบจำลองที่เหมาะสม/นำแบบจำลองดังกล่าวไปใช้ในการบริหารความเสี่ยงในภาพรวม เพื่อสะท้อนถึงช่วงเบี่ยงเบนที่ยังอยู่ในวิสัยที่องค์กรสามารถจัดการได้
- การสื่อสารและสร้างความเข้าใจกับ Risk Owner ในการพิจารณาถึงความสัมพันธ์ของความเสี่ยงและผลกระทบที่มีระหว่างหน่วยงานต่างๆ ภายในองค์กร โดย Risk Correlation Map ขององค์กร
- มีการประเมินประสิทธิผลของการกำหนดการพิจารณาถึงความสัมพันธ์ของความเสี่ยงและผลกระทบที่มีระหว่างหน่วยงานต่างๆ ภายในองค์กร โดย Risk Correlation Map และการวิเคราะห์ถึงภาพรวมของความเสี่ยง (Portfolio View of Risk) ขององค์กร และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

ตัวอย่าง Risk Map: Conceptual



2. Review & Revision
(การทบทวนการบริหารความเสี่ยง)

15. **Assesses Substantial Change:**
    The organization identifies and assesses changes that may substantially effect strategy and business objectives.
16. **Reviews Risk and Performance:**
    The organization reviews entity performance results and considers risk.
17. **Pursues Improvement in Enterprise Risk Management:**
    The organization pursues improvement of enterprise risk management.

4. Review & Revision

การกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยง

SIPOC

Process

การกำหนดขั้นตอนในการปรับปรุงกระบวนการบริหารความเสี่ยงองค์กร

1) กระบวนการบริหารความเสี่ยงและการสร้างวัฒนธรรม ความตระหนักในองค์กร รวมทั้งศักยภาพบุคลากรในด้านการบริหารความเสี่ยง

การนำไปสู่การปฏิบัติ

การสื่อสารและถ่ายทอด กระบวนการบริหารความเสี่ยงทั้งระดับองค์กร และสายงาน ต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ที่สอดคล้องตามแนวทางที่กำหนด

ทบทวนกระบวนการ

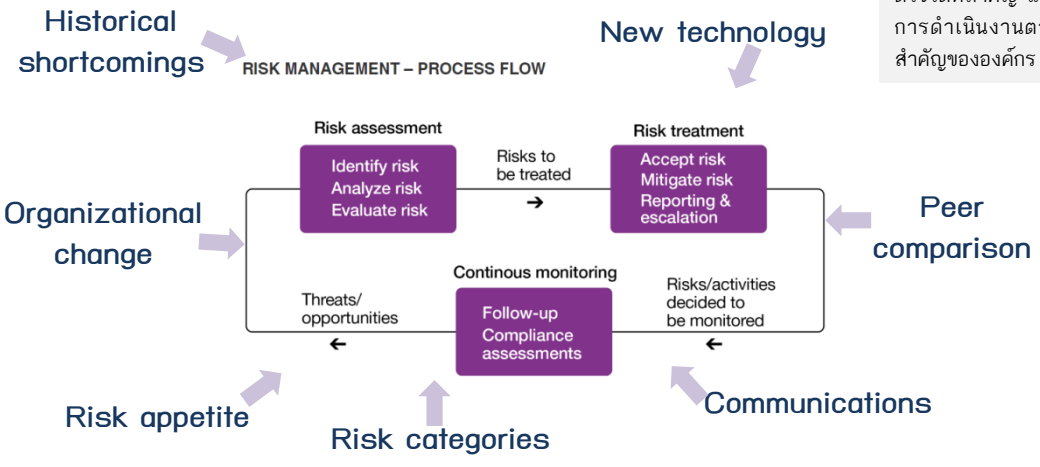
ทบทวนกระบวนการของการกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยง มีความเชื่อมโยงกับกระบวนการปรับเปลี่ยนแผนงาน วัตถุประสงค์เชิงยุทธศาสตร์ขององค์กร วิสัยทัศน์ และตัวชี้วัดที่สำคัญ และกระบวนการติดตามผลการดำเนินงานตามแผนงานและตัวชี้วัดที่สำคัญขององค์กร

เชื่อมโยง

แผนดิจิทัล

แผนแม่บทต่างๆ

ตัวอย่างการกำหนดกระบวนการบริหารความเสี่ยง



4. Review & Revision (การทบทวนการบริหารความเสี่ยง)

การรายงานผลการบริหารความเสี่ยง ที่สอดคล้องพร้อมรายงานผลการดำเนินงานองค์กร เพื่อให้สามารถวิเคราะห์ประเด็นที่อาจเกิดขึ้นใหม่ การเปลี่ยนแปลงที่สำคัญ รวมทั้งการทบทวนและปรับปรุงการบริหารความเสี่ยงสม่ำเสมอ และทำการปรับปรุงเมื่อจำเป็น

4.1 Reviews Risk and Performance (การทบทวนและปรับปรุงผลการบริหารความเสี่ยง)

- การกำหนดกระบวนการในการทบทวนและปรับปรุงผลความเสี่ยงสม่ำเสมอ ตามสภาพแวดล้อมที่เปลี่ยนแปลงไป โอกาสที่เกิดขึ้น หรือในกรณีที่ผลการบริหารความเสี่ยงไม่เป็นไปตามเป้าหมายที่กำหนด
- การบริหารและประเมินผลการบริหารความเสี่ยงที่เกิดขึ้นจริงโดยการติดตามผลการดำเนินงานตามตามกิจกรรมในแผนบริหารความเสี่ยง รวมทั้งเป้าหมายการบริหารความเสี่ยงทั้งในเชิงของระดับความรุนแรง และค่าเป้าหมาย (Risk Appetite) ที่กำหนด พร้อมรายงานผลการดำเนินงานขององค์กร (Performance) เพื่อให้สามารถวิเคราะห์ประเด็นความเสี่ยงที่อาจเกิดขึ้นใหม่ จากการเปลี่ยนแปลงที่สำคัญ
- การประเมินประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด (ความครบถ้วนของปัจจัย , กระบวนการ , ผลผลิต , ระยะเวลาที่แล้วเสร็จ)
- การทบทวนและปรับปรุงผลความเสี่ยง และผลการบริหารความเสี่ยงที่เกิดขึ้นจริง มีความเชื่อมโยงกับกระบวนการปรับเปลี่ยนแผนงาน (ตามปกติ และสถานการณ์เปลี่ยนแปลงอย่างรวดเร็ว) วัตถุประสงค์เชิงยุทธศาสตร์ขององค์กร วิสัยทัศน์ และตัวชี้วัดที่สำคัญ และกระบวนการติดตามผลการดำเนินงานตามแผนงานและตัวชี้วัดที่สำคัญขององค์กร เช่น แผนปฏิบัติการที่สำคัญ แผนการบริหารทรัพยากรบุคคล แผนแม่บทเทคโนโลยีดิจิทัล เป็นต้น
- มีการประเมินประสิทธิผลของการทบทวนและปรับปรุงผลการบริหารความเสี่ยง และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

4. Review & Revision
(การทบทวนการบริหารความเสี่ยง)

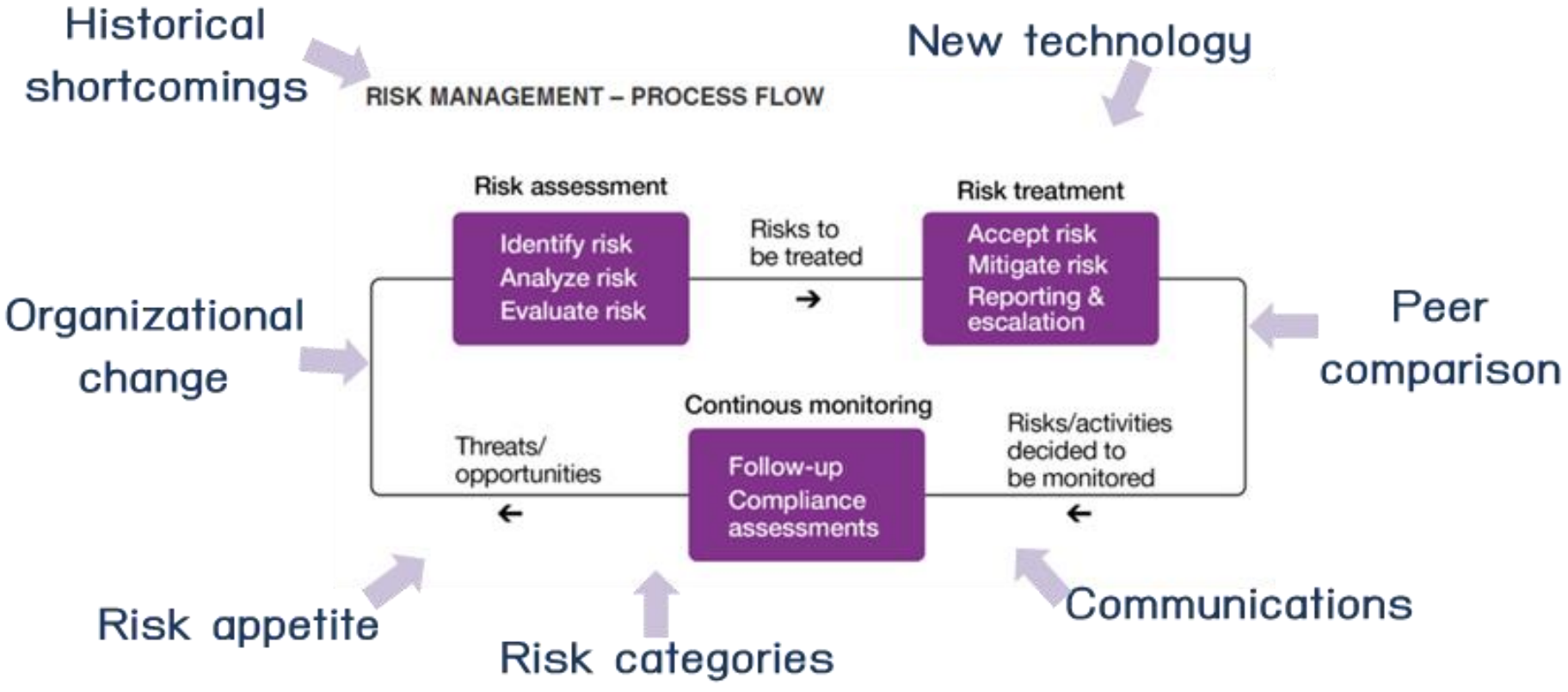
4.2 Pursues Improvement in Enterprise Risk Management
(การกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยง)

- การกำหนดขั้นตอนในการปรับปรุงกระบวนการบริหารความเสี่ยงองค์กร ทั้งในเชิงกระบวนการบริหารความเสี่ยงและการสร้างวัฒนธรรม ความตระหนักในองค์กร รวมทั้งศักยภาพบุคลากรในด้านการบริหารความเสี่ยง
- การดำเนินงานปรับปรุงและพัฒนากระบวนการบริหารความเสี่ยงองค์กร ตามขั้นตอนที่กำหนดได้ครบทุกขั้นตอน
- การประเมินประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด (ความครบถ้วนของปัจจัย , กระบวนการ , ผลผลิต , ระยะเวลาที่แล้วเสร็จ)
- การทบทวนกระบวนการของการกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยง มีความเชื่อมโยงกับกระบวนการปรับเปลี่ยนแผนงาน วัตถุประสงค์เชิงยุทธศาสตร์ขององค์กร วิสัยทัศน์ และตัวชี้วัดที่สำคัญ และกระบวนการติดตามผลการดำเนินงานตามแผนงานและตัวชี้วัดที่สำคัญขององค์กร
- มีการประเมินประสิทธิผลของการกำหนดแนวทางในการปรับปรุงกระบวนการบริหารความเสี่ยงและนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

4.3 Assesses Substantial Change
(การประเมินการเปลี่ยนแปลงที่มีนัยสำคัญ)

ประเมินในหัวข้อการวางแผนเชิงกลยุทธ์ หัวข้อย่อย-กระบวนการติดตามผลสำเร็จตามแผนปฏิบัติการ และปรับเปลี่ยนแผนงาน(Monitoring & Review)

ตัวอย่างการกำหนดกระบวนการบริหารความเสี่ยง



5. Information Communication & Reporting (ข้อมูลสารสนเทศ การสื่อสาร และการรายงานผล)

5. Information Communication & Reporting

** เกณฑ์การประเมินผลมีประเด็นของการพิจารณาเพิ่มเติมจาก 3 องค์ประกอบย่อยข้างต้น รวมในส่วนของการรายงานความเสี่ยง (องค์ประกอบที่ 20) ในส่วนของการพิจารณา การประเมินผลการควบคุมภายใน ทั้งการประเมินเป็นรายครั้ง และประเมินแบบต่อเนื่อง (Control Self Assessment)

การติดตาม ประเมินผลและรายงานผลการบริหารความเสี่ยง การควบคุมภายใน วัฒนธรรม และผลการดำเนินงาน

SIPOC

Process

กระบวนการรายงานผลการบริหารความเสี่ยง ตามแผนจัดการความเสี่ยง Mitigation Plan) และกิจกรรมการควบคุม (Existing Control) และนำส่งรายงานการประเมินผลการควบคุมภายใน ตามหลักเกณฑ์การปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ

1) โดยรายงานผลต่อผู้บริหารสายงาน คณะกรรมการบริหาร (Management Committee) และคณะกรรมการบริหารความเสี่ยงเป็นรายไตรมาส

2) นำส่งรายงานการประเมินผลการควบคุมภายใน ตามหลักเกณฑ์การปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ ได้ครบถ้วนและเป็นไปตามระยะเวลาที่กำหนด

การนำไปสู่การปฏิบัติ

การสื่อสารและถ่ายทอดการรายงานผลการบริหารความเสี่ยง และการรควบคุมภายในต่อผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ที่สอดคล้องตามระยะเวลาและองค์ประกอบที่กำหนด

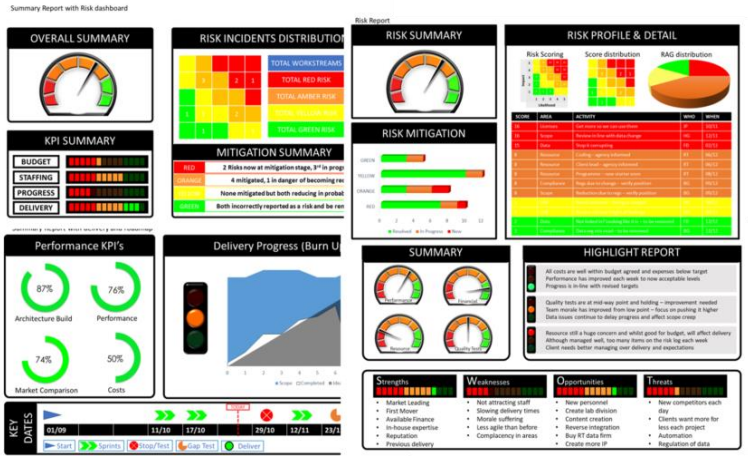
ทบทวนกระบวนการ

การรายงานผลการบริหารความเสี่ยง สามารถเชื่อมโยงกับการพัฒนาระบบสารสนเทศ/ระบบดิจิทัลขององค์กรในการติดตามและรายงานผลการดำเนินงาน

เชื่อมโยง

- ระบบเตือนภัยล่วงหน้า (Early Warning System : EWS)
- กระบวนการรายงานผลการดำเนินงานอื่น

ตัวอย่างการการติดตาม ประเมินผลและรายงานผลการบริหารความเสี่ยง การควบคุมภายใน วัฒนธรรม และผลการดำเนินงาน



5.1 Communicates Risk Information
(การสื่อสารการบริหารความเสี่ยงองค์กร)

1) การกำหนดกระบวนการการและช่องทางในการสื่อสารการบริหารความเสี่ยงองค์กร ในการสร้างความรู้ความเข้าใจ ความตระหนักเรื่องการบริหารความเสี่ยง รวมทั้งกระบวนการสำรวจระดับการรับรู้ ความตระหนักและทัศนคติของพนักงานในเรื่องการบริหารความเสี่ยงและการควบคุมภายใน
2) การสื่อสารและสร้างความรู้ความเข้าใจ ความตระหนักเรื่องการบริหารความเสี่ยงและการควบคุมภายในครอบคลุมทุกกลุ่มบุคลากร และหน่วยงานเจ้าของความเสี่ยง (Risk Owner) และผู้บริหารเกิดขึ้นจริง
3) การสื่อสารและสร้างความรู้ความเข้าใจ ความตระหนักเรื่องการบริหารความเสี่ยงและการควบคุมภายในฯ มีผลของระดับความรู้ความเข้าใจและความตระหนักเป็นไปตามเป้าหมายที่กำหนด และดีกว่าปีที่ผ่านมา
4) การทบทวนและปรับปรุงช่องทางในการสื่อสาร มีความเชื่อมโยงกับกระบวนการพัฒนาบุคลากร และการพัฒนาเทคโนโลยีดิจิทัล เช่น แผนการบริหารทรัพยากรบุคคล แผนแม่บทเทคโนโลยีดิจิทัล เป็นต้น
5) การประเมินประสิทธิผลของทุกขั้นตอน และทุกขั้นตอนได้ประสิทธิผลตามที่กำหนด (ความครบถ้วนของปัจจัย , กระบวนการ , ผลผลิต , ระยะเวลาที่แล้วเสร็จ)

5. Information Communication & Reporting (ข้อมูลสารสนเทศ การสื่อสารและการรายงานผล)

การสื่อสารการบริหารความเสี่ยงองค์กร การรายงานผลการบริหารความเสี่ยง และการประเมินผล การควบคุมภายใน ทั้งการประเมินเป็นรายครั้ง และประเมินแบบต่อเนื่อง โดยมีการวิเคราะห์เพื่อปรับปรุง และทบทวนกระบวนการบริหารความเสี่ยงและการควบคุมภายในองค์กร รวมทั้งการบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการและการบริหารความเสี่ยงที่ดี

1) มีกระบวนการรายงานผลการบริหารความเสี่ยง ตามแผนจัดการความเสี่ยง Mitigation Plan) และกิจกรรมการควบคุม (Existing Control) ที่กำหนดครบถ้วน โดยรายงานผลต่อผู้บริหารสายงาน คณะกรรมการบริหาร และคณะกรรมการบริหารความเสี่ยงเป็นรายไตรมาส และนำส่งรายงานการประเมินผลการควบคุมภายใน ตามหลักเกณฑ์การปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ ได้ครบถ้วนและเป็นไปตามระยะเวลาที่กำหนด
2) แนวทางแก้ไขเพื่อให้มั่นใจว่าจะบรรลุเป้าหมายการบริหารความเสี่ยงได้ตามแผนงานที่กำหนด โดยรายงานผลต่อคณะกรรมการบริหารความเสี่ยงเป็นรายไตรมาส ครบทุกไตรมาส
3) กระบวนการรายงานผลการบริหารความเสี่ยงสามารถเชื่อมโยงกับการพัฒนาระบบสารสนเทศ/ระบบดิจิทัลขององค์กรในการติดตามและรายงานผลการดำเนินงาน
4) การรายงานผลการบริหารความเสี่ยงมีองค์ประกอบที่ครบถ้วน และรายงานผลได้ครบทุกไตรมาส โดยมีความเชื่อมโยงและสอดคล้องกับความคืบหน้าของการติดตามผลตามแผนปฏิบัติการประจำปีที่เกี่ยวข้อง และรายงานผลพร้อมการรายงานผลการดำเนินงานขององค์กร (Performance) และเชื่อมโยงกับการพัฒนาระบบเทคโนโลยีดิจิทัลที่สนับสนุนกระบวนการบริหารความเสี่ยง และระบบเตือนภัยล่วงหน้า (Early Warning System : EWS)
5) มีการทบทวน/ปรับปรุง กระบวนการรายงานผลการบริหารความเสี่ยง

5. Information Communication & Reporting (ข้อมูลสารสนเทศ การสื่อสาร และการรายงานผล)

5.2 Reports on Risk, Internal Control, Culture, and Performance (การติดตามประเมินผลและรายงานผลการบริหารความเสี่ยง การควบคุมภายใน วัฒนธรรม และผลการดำเนินงาน)

1) การกำหนดกระบวนการพัฒนาระบบเทคโนโลยีดิจิทัล ที่สนับสนุนกระบวนการบริหารความเสี่ยง และกระบวนการพัฒนาระบบเตือนภัยล่วงหน้า (Early Warning System : EWS) ที่เชื่อมโยงกับเป้าหมายองค์กร
2) ดำเนินการพัฒนากระบบเทคโนโลยีสารสนเทศที่สนับสนุนการเก็บรวบรวมข้อมูล การรายงานและวิเคราะห์ระดับความรุนแรง และระบบ Early Warning System รวมทั้งกระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management :BCM) และใช้งานระบบได้จริง รวมทั้งข้อมูลมีความทันกาล
3) พัฒนาระบบเทคโนโลยีสารสนเทศที่สนับสนุนการเก็บรวบรวมข้อมูล การรายงานและวิเคราะห์ระดับความรุนแรง และระบบ Early Warning System รวมทั้งกระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management :BCM) และใช้งานระบบได้จริง รวมทั้งข้อมูลมีความทันกาล และมีการสื่อสารให้หน่วยงานที่เกี่ยวข้องใช้งานระบบได้อย่างครบถ้วน
4) การพัฒนากระบบเทคโนโลยีสารสนเทศที่สนับสนุนการเก็บรวบรวมข้อมูล การรายงานและวิเคราะห์ระดับความรุนแรง และระบบ Early Warning System รวมทั้งกระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management :BCM) มีความเชื่อมโยงและสอดคล้องกับแผนปฏิบัติการดิจิทัล รวมทั้งการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation)
5) มีการประเมินประสิทธิผลของ การกำหนดกระบวนการพัฒนาระบบเทคโนโลยีดิจิทัล ที่สนับสนุนกระบวนการบริหารความเสี่ยง และนำข้อมูลไปใช้เพื่อปรับปรุงกระบวนการฯ

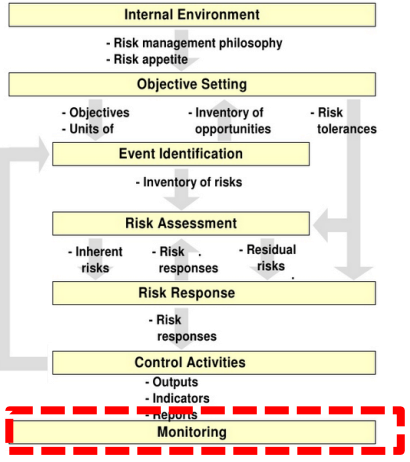
5. Information Communication & Reporting (ข้อมูลสารสนเทศ การสื่อสารและการรายงานผล)

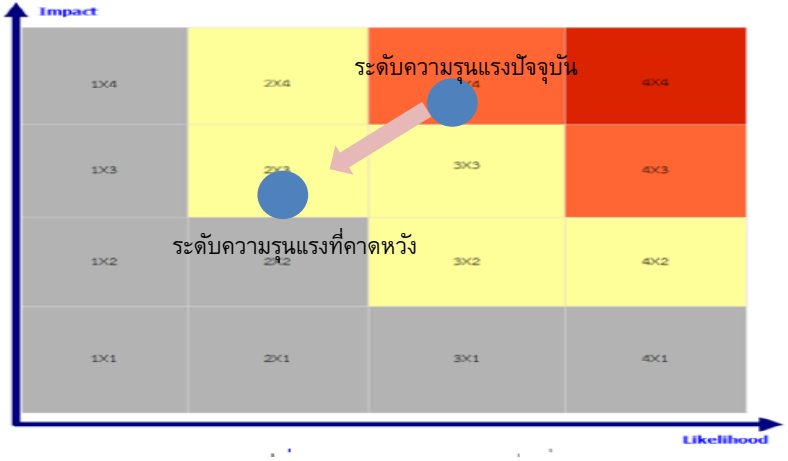
5.3 Leverages Information and Technology (ข้อมูลและเทคโนโลยีในการสนับสนุนการบริหารความเสี่ยง)

การติดตามและการรายงานผล (Monitoring and Reporting)

องค์ประกอบการรายงานและติดตามผลการบริหารความเสี่ยง

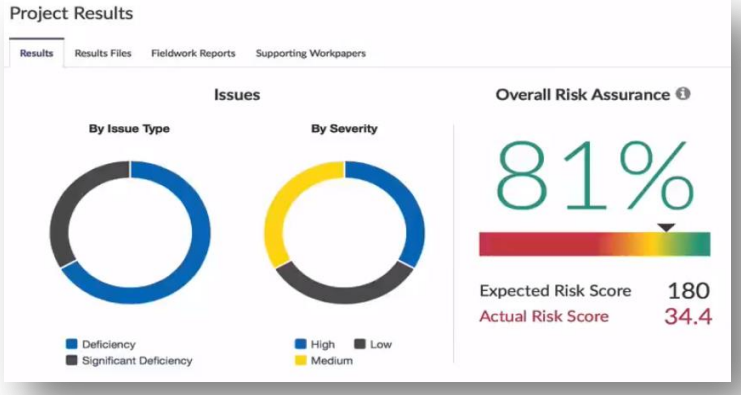
1. รายงานระดับความรุนแรงของแต่ละปัจจัยเสี่ยงรายไตรมาส เทียบกับเป้าหมายที่คาดหวัง
2. การรายงานความคืบหน้าการดำเนินงานตามมาตรการบริหารความเสี่ยงที่กำหนด
3. การวิเคราะห์ถึงปัญหา/อุปสรรค และแนวทางที่จะบรรลุถึงเป้าหมาย





มาตรการรองรับปัจจุบัน	ผลการดำเนินงานตามมาตรการรองรับปัจจุบัน	ระบุมาตรการจัดการเพิ่มเติม
แผนปฏิบัติการ 2.1.1 พัฒนาประสิทธิภาพช่องทางการจำหน่าย	- เป้าหมายยอดจำหน่าย 32,320 ล้านมวนผลยอดจำหน่ายสะสม ต.ค.56-ก.พ.57 = 11,592 ล้านมวน (ฝ่ายขาย) - ศึกษาช่องทางการจำหน่ายร้านค้าประเภท Modern Trade (ฝ่ายตลาด) - ดำเนินกิจกรรมตามแผนการสร้างความแข็งแกร่งของ Supply Chain แบบ CRM (ฝ่ายขาย)	- ส่งพนักงานลงพื้นที่ผลักดันยอด - ปรับแผนส่งเสริมการขาย - ฝ่ายขายและฝ่ายตลาดประชุมร่วมกันเพื่อหาแนวทางผลักดันยอดขายโดยเฉพาะภาคที่มียอดขายลดลงมาก - จัดหาวัสดุส่งเสริมการขายในวันที่ 11 มี.ค. 57 ด้วยวิธีทางอิเล็คทรอนิคส์ E-Auction
แผนปฏิบัติการ 2.2.1 งานตลาดและกิจกรรมสร้างความสัมพันธ์ กับ agent และเครือข่าย	ดำเนินกิจกรรมตามแผนฯ ในเดือน ก.พ. 57 แล้วเสร็จ (ฝ่ายขาย)	

From manual works to IT



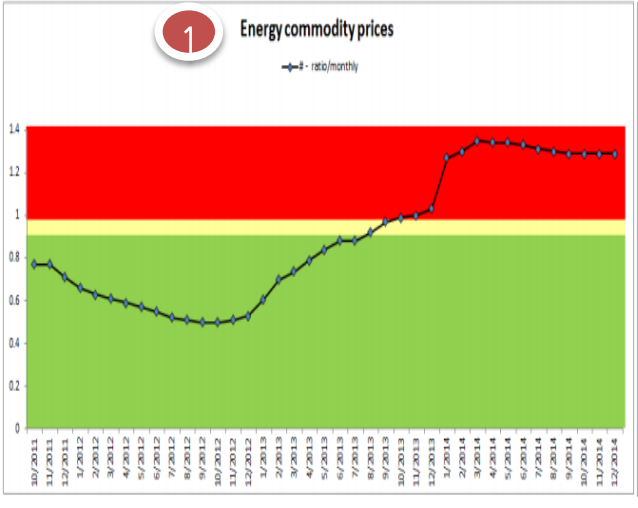
TRIS CORP Idea Solution Performance

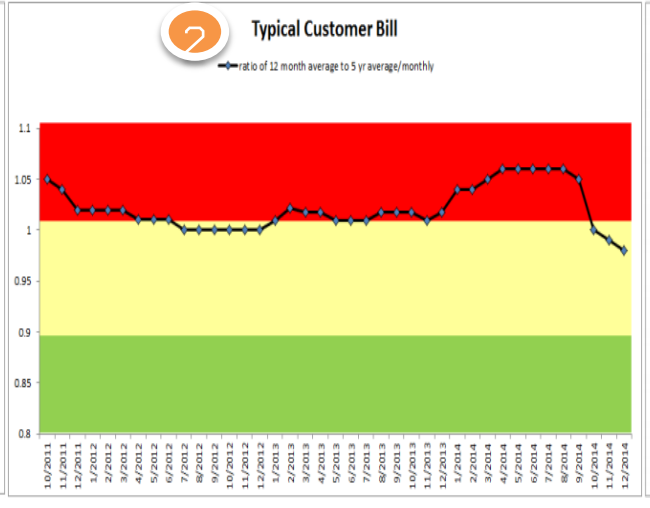
KRI Program

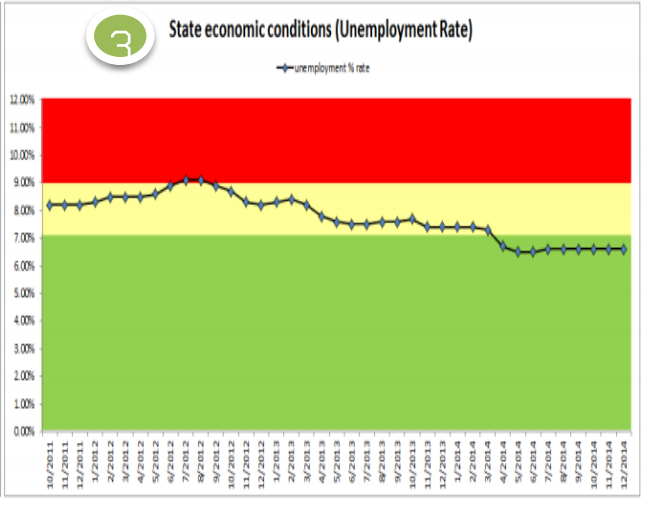
Determined by risk owners

Determined by experts

	Description	Measure	Goal	Thresholds	Weighting
1	Energy commodity prices	# - Ratio / monthly	N/A	Red: x>=1 Yellow: 0.9<x<1 Green: x<=0.9	High
2	Typical customer bill	Ratio of 12-month average to 5 yr. average / monthly	N/A	R: x>=1 Y: 0.9<x<1 G: x<=0.9	High
3	State economic conditions	Unemployment % rate / monthly	N/A	R: x>=9 Y: 7<x<9 G: x<=7	Medium
	Exceedance of performance thresholds	# per every 3 years / monthly	N/A	R: x>=4 Y: 1<=x<=3 G: x=0	Medium
	State regulatory success rate for prior 12 months	% of success rate / monthly	70%	R: <25% Y: 25-70% G: >=70%	Low

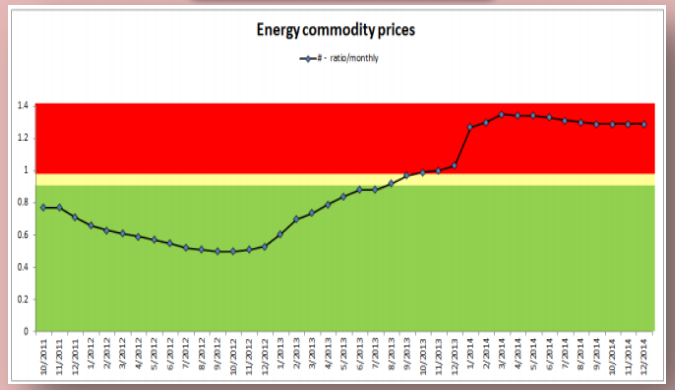






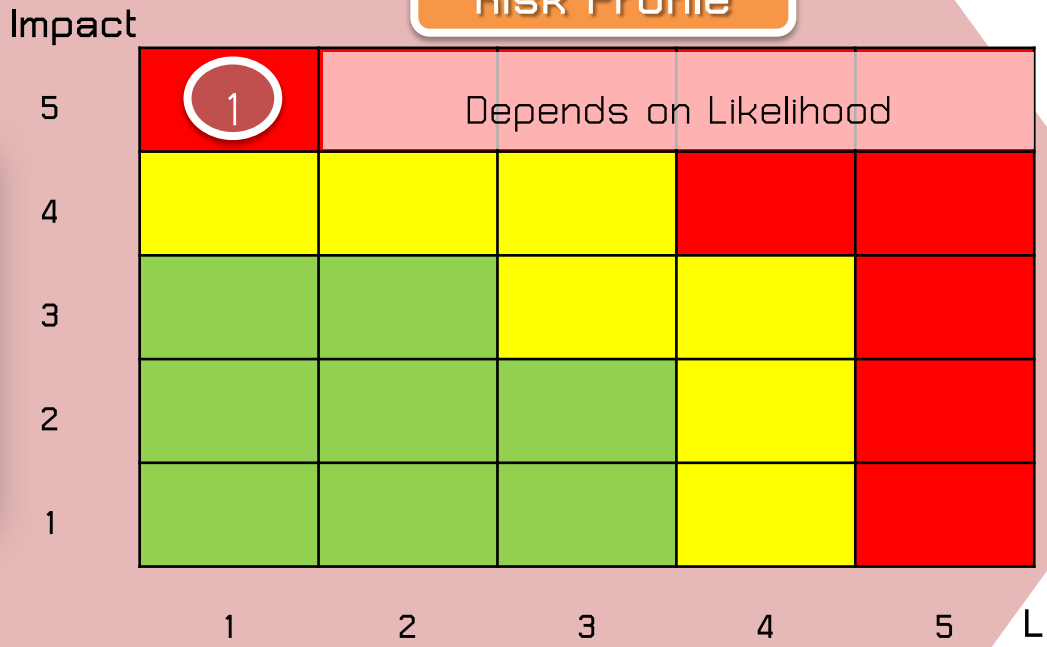
KRI and Risk Profile

KRI



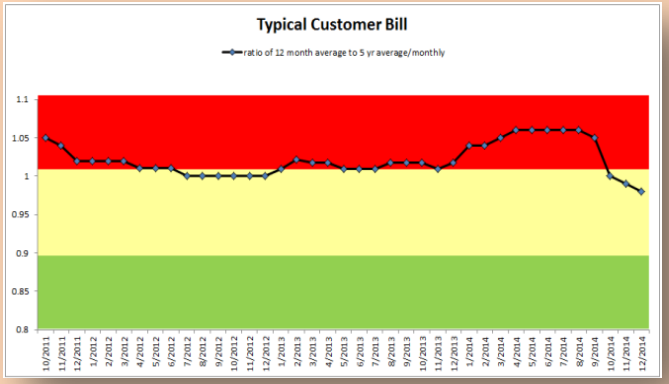
KRI = Impact

Risk Profile



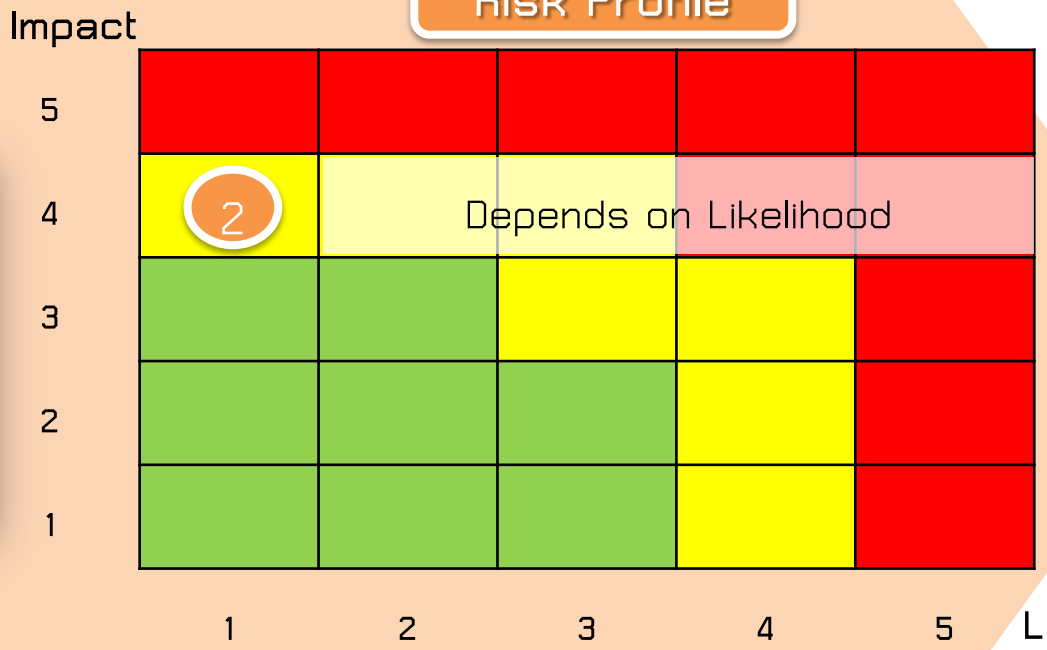
KRI and Risk Profile

KRI



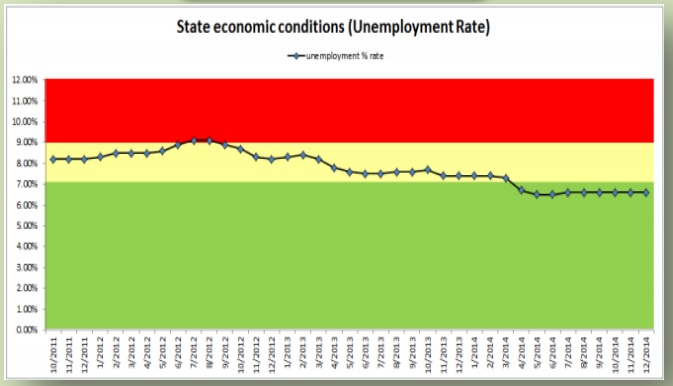
KRI = Impact

Risk Profile



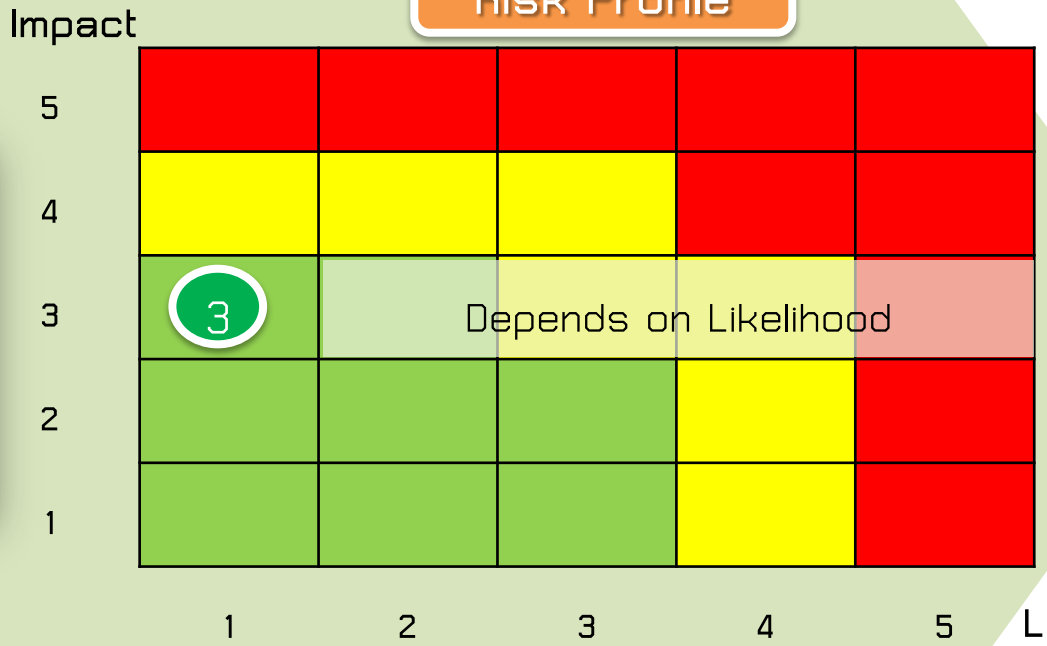
KRI and Risk Profile

KRI



KRI = Impact

Risk Profile

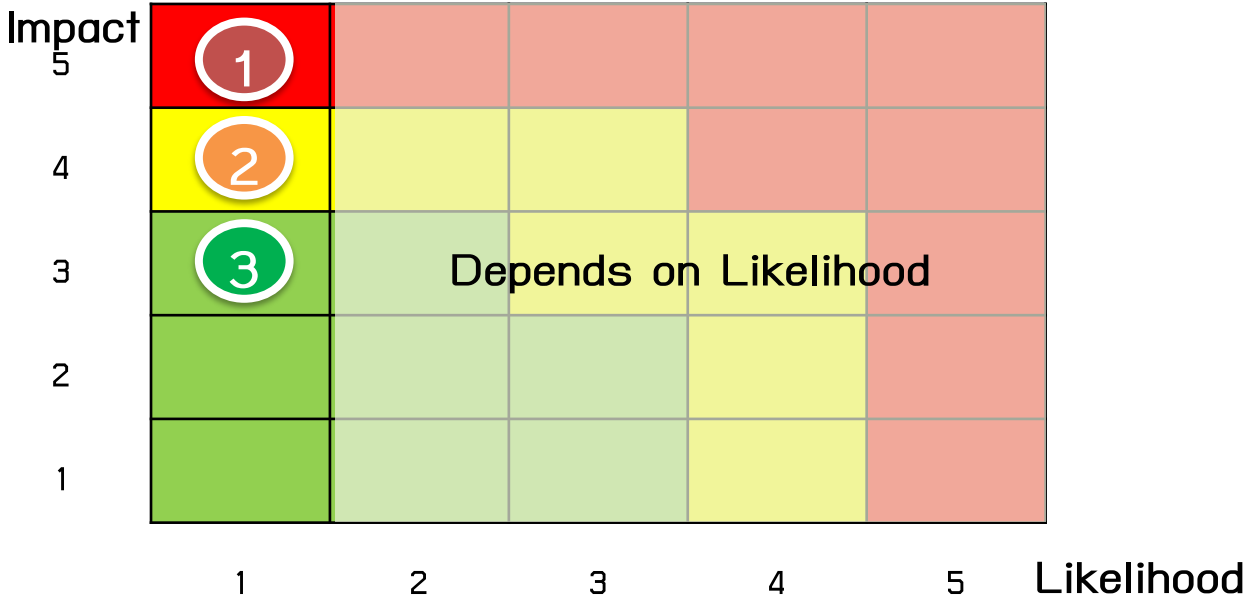


KRI Dashboard vs Risk Profile

KRI Dashboard

KRI's	High		Medium		Low	Overall Risk Assessment
	Energy Commodity Prices	Typical Customer Bill	State Economic Conditions	Performance Threshold Number of Times Exceeded in Last Year	Advocacy Success Rate Regarding Regulatory Issues	
Regulatory Risk	result	result	result	result	result	result

Risk Profile



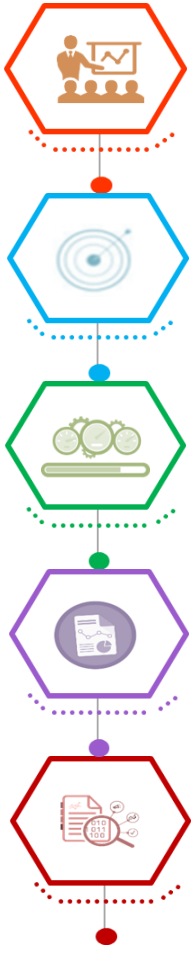
TRIS CORP Idea Solution Performance

Tips & Trick

ความเชื่อมโยงของเกณฑ์การบริหารความเสี่ยงและการควบคุมภายใน กับเกณฑ์ อีก 7 หัวข้อ

?

เกณฑ์การบริหารความเสี่ยงและการควบคุมภายใน



1. Governance & Culture

- 1.1 Exercises Board Risk & internal Control Oversight — CG
- 1.2 Establishes Operating structures — HR
- 1.3 Defines Desired Culture — CG
- 1.4 Demonstrates Commitment to Core Values — HR
- 1.5 Attracts, Develops, and Retains Capable Individuals — HR

2. Strategy & Objectives Setting

- 2.1 Analyzes Business Context — Strategic
- 2.2 Defines Risk Appetite — Strategic
- 2.3 Evaluates Alternative Strategies — Strategic
- 2.4 Formulates Business Objectives — Strategic

3. Performance

- 3.1 Identifies Risk — Strategic, Stakeholder
- 3.2 selects and develops control activities — IA
- 3.3 Assesses Severity of Risk
- 3.4 Prioritizes Risks — IA
- 3.5 Implements Risk Responses — Strategic, HR, Digital, IA
- 3.6 Develops Portfolio View- Risk Correlation Map & Portfolio view of Risk

4. Review & Revision

- 4.1 Reviews Risk and Performance — CG, Strategic
- 4.2 Pursues Improvement in Enterprise Risk Management
- 4.3 Assesses Substantial Change — Strategic

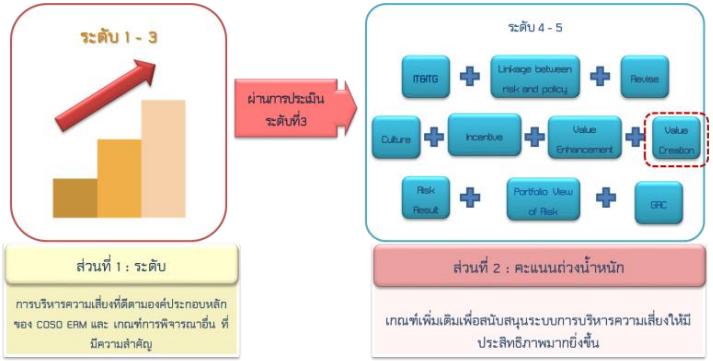
5. Information Communication & Reporting

- 5.1 Communicates Risk Information
- 5.2 Reports on Risk, Internal control. Culture, and Performance — HR, CG
- 5.3 Leverages Information and Technology and Early warning system — Digital

เกณฑ์ที่เพิ่มขึ้นจากข้อ 3 (การบริหารความเสี่ยง) เดิม

?

การบริหารความเสี่ยง (ข้อ3) เดิม



เกณฑ์การบริหารความเสี่ยงและการควบคุมภายใน (ใหม่)

เกณฑ์ที่มีการเปลี่ยนแปลง

1. การกำหนดนโยบาย GRC
2. จัดให้มีบรรยากาศและวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยง
3. การเชื่อมโยงกระบวนการบริหารความเสี่ยงและกลยุทธ์การบริหารความเสี่ยง กับนโยบายวัตถุประสงค์เชิงยุทธศาสตร์ ยุทธศาสตร์ แผนงานโครงการ
4. การพิจารณาความเพียงพอของกิจกรรมควบคุม ประเมินระดับความเสี่ยงการจัดลำดับความสำคัญ และการประเมินความเสี่ยงสายงาน
5. การวิเคราะห์ประเด็นที่อาจเกิดขึ้นใหม่ การเปลี่ยนแปลงที่สำคัญ
6. การสื่อสารการบริหารความเสี่ยงองค์กร
7. การใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนการบริหารความเสี่ยงที่ดี

TRIS CORP Idea Solution Performance

SEPO

Q&A