

Executive Summary

The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

บทสรุปสำหรับผู้บริหาร

หลักการพื้นฐานที่สำคัญของการบริหารความเสี่ยงขององค์กร ก็ คือ องค์กรทั้งหลายนั้นดำรงอยู่เพื่อสร้างมูลค่าให้กับผู้มีส่วนได้เสีย องค์กรทุกแห่งต่างก็เผชิญกับความไม่แน่นอน และความท้าทายต่อฝ่ายบริหารก็คือจะต้องกำหนดให้ได้ว่าจะยอมรับความไม่แน่นอนเพียงใดในขณะที่กำลังพยายามเพิ่มมูลค่าของผู้มีส่วนได้เสียให้สูงขึ้น ความไม่แน่นอน เป็นทั้งความเสี่ยงและโอกาสคือมีศักยภาพที่จะลดหรือเพิ่มมูลค่า ให้ กับ องค์กร ก็ ได้ การบริหารความเสี่ยงขององค์กรจะช่วยให้ฝ่ายบริหารสามารถ จัด การ กับ ความ ไม่ แน่ นอน และความเสี่ยงกับโอกาสที่มาพร้อมกับความไม่แน่นอนนั้นได้อย่า ง มี ประ สัต ธิ ผล

เพื่อยกระดับขีดความสามารถในการสร้างมูลค่าให้กับองค์กรของตนเอง

Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives.

องค์กรจะสามารถสร้างมูลค่าให้สูงสุดได้ก็ต่อเมื่อฝ่ายบริหารได้กำหนดกลยุทธ์และวัตถุประสงค์ให้เกิดดุลยภาพที่สูงสุดระหว่างการเติบโตและเป้าหมายผลตอบแทนกับความเสี่ยงที่เกี่ยวข้อง รวมถึงการใช้ทรัพยากรอย่างมีประสิทธิภาพและประสิทธิผลเพื่อให้เกิดบรรลุตามวัตถุประสงค์ขององค์กร

Enterprise risk management encompasses:

การบริหารความเสี่ยงขององค์กรประกอบด้วยเรื่องต่างๆ
ดังต่อไปนี้

- Aligning risk appetite and strategy – Management considers the entity’s risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- *การกำหนดกลยุทธ์และระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) ให้เป็นไปในทิศทางเดียวกัน - ฝ่ายบริหารจะต้องพิจารณาระดับความเสี่ยงที่องค์กรยอมรับได้เพื่อใช้ในการประเมินทางเลือกของกลยุทธ์ต่างๆ และการกำหนดวัตถุประสงค์ที่เกี่ยวข้อง รวมทั้งการพัฒนากลไกการบริหารจัดการความเสี่ยงที่เกี่ยวข้อง*
- Enhancing risk response decisions – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.
- *การช่วยให้ตัดสินใจตอบสนองต่อความเสี่ยงได้ดีขึ้น – การบริหารความเสี่ยงขององค์กรช่วยให้เกิดความแม่นยำในการระบุและเลือกวิธีการตอบสนองความเสี่ยงจากทางเลือกที่มีอยู่ ได้แก่ การหลีกเลี่ยงความเสี่ยง*

การลดความเสี่ยง การหาผู้ร่วมรับความเสี่ยง และการยอมรับความเสี่ยง

- Reducing operational surprises and losses – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- *การลดเหตุที่ไม่คาดฝันและผลขาดทุนจากการปฏิบัติการ*
-
องค์กรจะสามารถยกระดับขีดความสามารถในการระบุเหตุการณ์ที่อาจจะเกิดขึ้น และกำหนดวิธีการตอบสนองต่อเหตุการณ์นั้นๆ เพื่อลดเหตุอันไม่คาดฝันและต้นทุนหรือการสูญเสียที่เกี่ยวข้อง
- Identifying and managing multiple and cross-enterprise risks – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated

impacts, and integrated responses to multiple risks.

- *การระบุและจัดการกับความเสี่ยงที่หลากหลายและครอบคลุมทั่วทั้งองค์กร* - องค์กรทุกแห่งต่างเผชิญกับความเสียงจำนวนมากมายันับไม่ถ้วนที่มีผลกระทบต่อหน่วยงานต่างๆ ในองค์กร การบริหารความเสี่ยงขององค์กรจะเอื้ออำนวยให้การตอบสนองต่อผลกระทบที่มีความเกี่ยวพันซึ่งกันและกันและผสมผสานการตอบสนองต่อความเสี่ยงที่หลากหลายได้อย่างมีประสิทธิภาพ
- Seizing opportunities – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- *การฉวยโอกาส* - ในการพิจารณาถึงเหตุการณ์ที่อาจเกิดขึ้นทั้งหมด จะทำให้ฝ่ายบริหารอยู่ในสถานะที่สามารถระบุ รับรู้และฉวยโอกาสที่มีนั้นดำเนินการเชิงรุกได้ทันทั่วทั้ง
- Improving deployment of capital – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.
- *การปรับปรุงการบริหารเงินทุนให้ดีขึ้น* - การได้รับข้อมูลความเสี่ยงที่แม่นยำจะช่วยให้ฝ่ายบริหารสามารถประเมินจำนวนเงินทุนที่จำเป็นต้องใช้ทั้งหมดได้

อย่างมีประสิทธิภาพและช่วยให้สามารถจัดสรรเงินทุนได้ดีขึ้น

These capabilities inherent in enterprise risk management help management achieve the entity's performance and profitability targets and prevent loss of resources. Enterprise risk management helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the entity's reputation and associated consequences. In sum, enterprise risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.

จากข้อดีดังกล่าวข้างต้นของการบริหารความเสี่ยงขององค์กร จะช่วยให้ฝ่ายบริหารบรรลุเป้าหมายในการดำเนินการและมีความสามารถในการทำกำไรและป้องกันการสูญเสียวัตถุภาพขององค์กรได้ การบริหารความเสี่ยงขององค์กรช่วยให้เกิดความมั่นใจได้ว่า การจัดทำรายงานมีประสิทธิภาพ มีการปฏิบัติตามกฎหมายและระเบียบข้อบังคับ รวมทั้งช่วยหลีกเลี่ยงความเสียหายเกี่ยวกับชื่อเสียงขององค์กร และเหตุการณ์ต่อเนื่องอื่น ๆ ที่เกี่ยวข้อง โดยสรุปแล้วการบริหารความเสี่ยงขององค์กรช่วยให้องค์กรบรรลุจุดมุ่งหมายตามที่ต้องการและหลีกเลี่ยงกับดักหลุมพรางและเหตุไม่คาดคิดที่อาจเกิดขึ้นในระหว่างนั้น ได้

Events – Risks and Opportunities

Events can have negative impact, positive impact, or both. Events with a negative impact represent risks, which can prevent value creation or erode existing value. Events with positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation. Management channels opportunities back to its strategy or objective-setting processes, formulating plans to seize the opportunities.

เหตุการณ์- ความเสี่ยงและโอกาส

เหตุการณ์ที่เกิดขึ้นอาจมีผลกระทบในเชิงลบหรือเชิงบวกหรือทั้ง สอง อย่าง ก็ได้ เหตุการณ์ที่ให้ผลกระทบในเชิงลบก็คือความเสี่ยงซึ่งเป็นอุปสรรคต่อการสร้างมูลค่าหรืออาจไปลดมูลค่าที่มีอยู่ลง ในขณะที่เหตุการณ์ที่ให้ผลกระทบในเชิงบวกอาจไปชดเชยผลกระทบในเชิงลบ หรืออาจหมายถึงโอกาสก็ได้ โอกาสคือความเป็นไปได้ที่เหตุการณ์ใดเหตุการณ์หนึ่งจะเกิดขึ้นแล้วมีผลกระทบในเชิงบวกต่อการบรรลุวัตถุประสงค์และสนับสนุนการสร้างมูลค่าหรือการดำรงรักษามูลค่าไว้ ผู้บริหารอาจนำเอาโอกาสนั้นไปกำหนดกลยุทธ์หรือวัตถุประสงค์ ข อง ก ะ บ ว น ก า ร ป ฎิ บั ตี ง าน ต่ า ง ๆ หรือนำไปวางแผนงานเพื่อให้ได้ประโยชน์จากโอกาสนั้นต่อไป

Enterprise Risk Management Defined

Enterprise risk management deals with risks and opportunities affecting value creation or preservation, defined as follows:

Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

คำจำกัดความของการบริหารความเสี่ยงขององค์กร
การบริหารความเสี่ยงขององค์กรเกี่ยวข้องกับความเสี่ยงและโอกาส ที่มีผลต่อการสร้างหรือการดำรงรักษามูลค่าไว้
ดังคำจำกัดความดังนี้

การบริหารความเสี่ยงขององค์กร คือ กระบวนการที่กำหนดขึ้นและนำไปใช้โดยคณะกรรมการ

ฝ่ายบริหารและบุคลากรอื่นๆ ขององค์กร
เพื่อกำหนดกลยุทธ์และใช้กับหน่วยงานทั้งหมดในองค์กร
โดยได้รับการออกแบบมาเพื่อระบุเหตุการณ์ที่อาจเกิดขึ้น
ซึ่งอาจมีผลกระทบต่อองค์กร
รวมทั้งการบริหารความเสี่ยงให้อยู่ภายใต้ระดับความเสี่ยง
ที่องค์กรยอมรับได้ (Risk Appetite) ทั้งนี้
เพื่อให้ความมั่นใจอย่างสมเหตุสมผลว่าองค์กรจะบรรลุ
วัตถุประสงค์ที่ตั้งไว้

The definition reflects certain fundamental concepts.

Enterprise risk management is:

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors

- Geared to achievement of objectives in one or more separate but overlapping categories

คำจำกัดความดังกล่าวสะท้อนให้เห็นถึงแนวคิดพื้นฐานบางประการ หลักการบริหารความเสี่ยงขององค์กร คือ:

- กระบวนการที่ดำเนินอยู่และกระทำอย่างต่อเนื่องทั่วทั้งองค์กร
- กำหนดขึ้นและนำไปใช้โดยบุคลากรทุกระดับขององค์กร
- ใช้ในการกำหนดกลยุทธ์ขององค์กร
- ใช้ทั่วทั้งองค์กร ทุกระดับ และทุกหน่วยงาน รวมถึงการจัดการความเสี่ยงในระดับองค์กรด้วย
- ได้รับการออกแบบมาเพื่อระบุเหตุการณ์ที่อาจเกิดขึ้นซึ่งหากเกิดขึ้นแล้วจะมีผลกระทบต่อองค์กร และเพื่อบริหารความเสี่ยงที่อาจเกิดขึ้นนั้นให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)
- สามารถให้ความมั่นใจอย่างสมเหตุสมผลต่อฝ่ายบริหาร และคณะกรรมการขององค์กร
- มุ่งสู่การบรรลุวัตถุประสงค์ประเภทใดประเภทหนึ่ง หรือ หลาย ประเภท ที่อาจแยกจากกันทับซ้อนกันหรือเชื่อมโยงกัน

This definition is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries, and sectors. It focuses directly on achievement of

objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.

COSO

ได้ตั้งใจกำหนดนิยามของการบริหารความเสี่ยงขององค์กรไว้
อย่างกว้างๆ โดยให้แนวคิดหลักๆ
ที่สำคัญเป็นพื้นฐานว่าบริษัทและองค์กรอื่นๆ
จะบริหารความเสี่ยงได้อย่างไร
และให้หลักเกณฑ์ในการนำไปประยุกต์ใช้กับองค์กรทุกๆ
อุตสาหกรรมและภาคส่วนอื่นๆ (Sectors)
โดยให้ความสำคัญต่อการบรรลุวัตถุประสงค์ที่องค์กรนั้นๆ
กำหนดขึ้น
รวมทั้งให้หลักเกณฑ์ในการกำหนดความมีประสิทธิภาพของกา
รบริหารความเสี่ยงขององค์กรด้วย

Achievement of Objectives

Within the context of an entity's established mission or vision, management establishes strategic objectives, selects strategy, and sets aligned objectives cascading through the enterprise. This enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:

- Strategic – high-level goals, aligned with and supporting its mission
- Operations – effective and efficient use of its resources
- Reporting – reliability of reporting
- Compliance – compliance with applicable laws and regulations.

การบรรลุวัตถุประสงค์

ภายใต้บริบทของพันธกิจหรือวิสัยทัศน์ที่องค์กรกำหนดขึ้น ฝ่ายบริหารกำหนดวัตถุประสงค์เชิงกลยุทธ์ เลือกกลยุทธ์และกำหนดวัตถุประสงค์ที่เชื่อมโยงและลดหลั่นลง ไป ทั่ว ทั้ง องค์กร กรอบโครงสร้างการบริหารความเสี่ยงขององค์กรนี้จะช่วยนำไปสู่การบรรลุวัตถุประสงค์ขององค์กร โดยแบ่งออกได้เป็น 4 ประเภท คือ :

- *ด้านกลยุทธ์* - เป้าหมายระดับสูง ต้องสอดคล้องและสนับสนุนพันธกิจขององค์กร
- *ด้านกระบวนการปฏิบัติ* - การใช้ทรัพยากรอย่างมีประสิทธิภาพและมีประสิทธิผล
- *ด้านการรายงาน* - ความน่าเชื่อถือของรายงาน
- *ด้านกระบวนการปฏิบัติตามกฎหมายระเบียบ* - การปฏิบัติให้ถูกต้องตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

This categorization of entity objectives allows a focus on separate aspects of enterprise risk management. These distinct but overlapping categories – a particular objective can fall into more than one category – address different entity needs and may be the direct responsibility of different executives. This categorization also allows distinctions between what can be expected from each category of objectives. Another category, safeguarding of resources, used by some entities, also is described.

การแบ่งประเภทวัตถุประสงค์ดังกล่าวข้างต้นขององค์กรช่วยให้สามารถมุ่งเน้นไปที่มุมมองต่างๆของการบริหารความเสี่ยงขององค์กร ซึ่งมีบางส่วนแยกกันและบางส่วนทับซ้อนกันอยู่ชัดเจน วัตถุประสงค์หนึ่งๆอาจสามารถจัดอยู่ในวัตถุประสงค์หลายประเภทซึ่งแสดงให้เห็นถึงความต้องการที่แตกต่างกันขององค์กรซึ่งอาจเป็นความรับผิดชอบโดยตรงของผู้บริหารตำแหน่งต่างๆที่จะต้องพิจารณาเรื่องดังกล่าว การจัดประเภทองค์ประกอบของวัตถุประสงค์เหล่านี้ยังสร้างความเด่นชัดระหว่างอะไรคือสิ่งที่สามารถคาดหวังว่าจะได้รับจากวัตถุประสงค์แต่ละประเภท นอกจากนี้ยังได้มีการอธิบายถึงวัตถุประสงค์อีกประเภทหนึ่งที่ใช้ในบางองค์กรไว้ด้วย คือวัตถุประสงค์เรื่องการปกป้องทรัพยากร

Because objectives relating to reliability of reporting and compliance with laws and regulations are within

the entity's control, enterprise risk management can be expected to provide reasonable assurance of achieving those objectives. Achievement of strategic objectives and operations objectives, however, is subject to external events not always within the entity's control; accordingly, for these objectives, enterprise risk management can provide reasonable assurance that management, and the board in its oversight role, are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of the objectives.

เนื่องจากวัตถุประสงค์ที่เกี่ยวข้องกับความน่าเชื่อถือของการรายงานและการปฏิบัติตามกฎหมายและระเบียบข้อบังคับอยู่ภายใต้การควบคุมขององค์กร จึงคาดหวังว่าการบริหารความเสี่ยงขององค์กรจะให้ความเชื่อมั่นได้อย่างสมเหตุสมผลว่าจะบรรลุวัตถุประสงค์เหล่านี้ อย่างไรก็ตามการบรรลุวัตถุประสงค์ด้านกลยุทธ์และวัตถุประสงค์ด้านกาดำเนินงานนั้นยังขึ้นอยู่กับเหตุการณ์ภายนอกที่ไม่ได้อยู่ภายใต้การควบคุมขององค์กรด้วย ดังนั้นสำหรับวัตถุประสงค์ด้านกลยุทธ์และด้านการปฏิบัติการบริหารความเสี่ยงขององค์กรจะให้ความเชื่อมั่นอย่างสมเหตุสมผลว่าฝ่ายบริหารและคณะกรรมการในฐานะที่มีบทบาทกำกับดูแลให้องค์กรมุ่งไปสู่การบรรลุวัตถุประสงค์จะได้รับรู้ข้อมูลเกี่ยวกับความเสี่ยงนั้น ๆ อย่างทันเวลา

Components of Enterprise Risk Management

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. These components are:

องค์ประกอบของการบริหารความเสี่ยงขององค์กร

การบริหารความเสี่ยงขององค์กรประกอบด้วย 8 องค์ประกอบที่มีความเกี่ยวข้องซึ่งกันและกัน องค์ประกอบเหล่านี้ได้มาจากวิธีการที่ฝ่ายบริหารดำเนินธุรกิจ และนำมาผสมผสานเข้ากับกระบวนการบริหารจัดการ องค์ประกอบเหล่านี้ ได้แก่

- Internal Environment – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

- *ส ภา ว พ แ ว ด ล ้อ ม ภา ย ใน* -
 สภาพแวดล้อมภายในครอบคลุมถึงแนวนโยบายโดยทั่วไป
 ข อ ง อ ง ก ษ ัต ริ
 ซึ่งเป็นพื้นฐานของการมองความเสี่ยงและการจัดการกับ
 ความเสี่ยงโดยบุคลากรทั้งหมดในองค์กร
 รวมไปถึงปรัชญาการบริหารความเสี่ยง
 กับระดับความเสี่ยงที่ยอมรับได้
 ความซื่อสัตย์กับคุณค่าทางจริยธรรม
 และสภาพแวดล้อมในการปฏิบัติงานของบุคลากรเหล่านี้
 น
- Objective Setting – Objectives must exist before
 management can identify potential events
 affecting their achievement. Enterprise risk
 management ensures that management has in
 place a process to set objectives and that the
 chosen objectives support and align with the
 entity’s mission and are consistent with its risk
 appetite.
- *ก า ร ก ำ ห น ด วั ต ฤ ป ระ ส ง ค์* -
 วัตถุประสงค์ต้องมีอยู่ก่อนที่ฝ่ายบริหารจะสามารถระบุเห
 ตุ ก า ร ณ์ ซึ่ง มี ผล ต่ อ ก า ร บ ร ร ลู วั ต ฤ ป ระ ส ง ค์
 การบริหารความเสี่ยงขององค์กรทำให้มั่นใจว่าฝ่ายบริหาร
 มีกระบวนการกำหนดวัตถุประสงค์อยู่พร้อมแล้ว
 และวัตถุประสงค์ที่เลือกจะเป็นสิ่งสนับสนุนและไปในทิศทาง
 เดียวกันกับพันธกิจขององค์กรและสอดคล้องระดับความ
 เสี่ยงที่ยอมรับได้

- Event Identification – Internal and external events affecting achievement of an entity’s objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management’s strategy or objective-setting processes.
- ก ำ ร ะ บ ุ เ ห ตุ ก ำ ร ณ์ - เหตุการณ์ภายในและภายนอกที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กรต้องได้รับการระบุและมีการแยกแยะความเสี่ยงกับโอกาสออกต่างหากจากกัน ส ำ ห รั บ โ อ ก ำ ส ั น ั น ฝ่ายบริหารจะนำไปพิจารณาในการกำหนดกลยุทธ์หรือในกระบวนการกำหนดวัตถุประสงค์ต่อไป
- Risk Assessment – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- ก ำ ร ปร ะ เ มื น ค ว ำ ม เสี ย ง - จะต้องมีการวิเคราะห์ความเสี่ยงพิจารณาโอกาสที่จะเกิดและผลกระทบเพื่อเป็นพื้นฐานในการตัดสินใจว่าจะบริหาร ค ว ำ ม เสี ย ง ั น ั น อ ย ำ ง ไ ร การประเมินความเสี่ยงจะประเมินทั้งความเสี่ยงที่มีอยู่ตามธรรมชาติ (Inherent Risk) และความเสี่ยงที่เหลืออยู่ (Residual Risk)

- Risk Response – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.
- *การตอบสนองต่อความเสี่ยง* - ฝ่ายบริหารเลือกวิธีการตอบสนองต่อความเสี่ยงได้หลายวิธี - เช่น หลีกเลี่ยง ยอมรับ ลด หรือหาผู้ร่วมรับความเสี่ยงโดยการพัฒนากระบวนการบริหารความเสี่ยงให้สอดคล้องกับช่วงความเบี่ยงเบนที่ยอมรับได้ (Risk Tolerance) และระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite)
- Control Activities – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- *กิจกรรมควบคุม* - จะต้องมีการกำหนดนโยบายและขั้นตอนการปฏิบัติไว้และนำไปดำเนินการเพื่อให้เกิดความมั่นใจว่ามีการดำเนินการตามวิธีการตอบสนองต่อความเสี่ยงเหล่านั้นอย่างมีประสิทธิภาพ
- Information and Communication – Relevant information is identified, captured, and

It is a multidirectional, iterative process in which almost any component can and does influence another.

การบริหารความเสี่ ยง ของ องค์ กร ไม่ใช่กระบวนการที่ต้องดำเนินการเรียงไปตามลำดับ คือ องค์ประกอบหนึ่งจะมีผลกระทบเฉพาะต่อองค์ประกอบถัดไปเท่านั้น แต่ทว่าเป็นกระบวนการที่เกิดขึ้นได้หลายทิศทางและอาจซ้ำไป โดยที่องค์ประกอบใดองค์ประกอบหนึ่งล้วนแต่มีอิทธิพลต่อองค์ประกอบอื่น ๆ

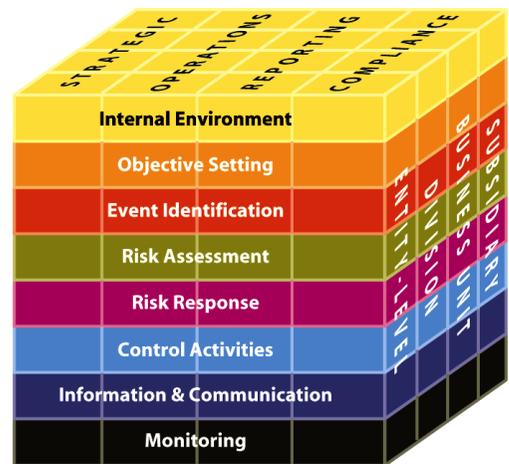
Relationship of Objectives and Components

There is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix, in the form of a cube.

ความสัมพันธ์ระหว่างวัตถุประสงค์และองค์ประกอบ

วัตถุประสงค์และองค์ประกอบการบริหารความเสี่ยงขององค์กร มีความสัมพันธ์กันโดยตรง เนื่องจากวัตถุประสงค์คือสิ่งที่องค์กรมุ่งมั่นที่จะทำให้บรรลุผลสำเร็จ และองค์ประกอบการบริหารความเสี่ยงขององค์กรก็คือสิ่งจำเป็นที่จะทำ ให้บรรลุวัตถุประสงค์นั้น ๆ ได้ ความสัมพันธ์ดังกล่าวแสดงให้เห็นเป็นภาพสามมิติได้ ดังนี้

The four objectives categories – strategic, operations, reporting, and compliance – are represented by the vertical columns, the eight components by horizontal rows, and an entity’s units by the third dimension. This depiction portrays the ability to focus on the entirety of an entity’s enterprise risk management, or by objectives category, component, entity unit, or any subset thereof.



ประเภทของวัตถุประสงค์สี่ประเภท – กลยุทธ์ การปฏิบัติการ การจัดทำรายงานและการปฏิบัติตามกฎระเบียบจะแสดงอยู่ใน แนวนอน ส่วนแนวดิ่ง และองค์ประกอบทั้งแปดประการของการบริหารความเสี่ยงขององค์กรจะแสดงอยู่ในแนวนอน ส่วนหน่วยงานต่างๆ ขององค์กรจะแสดงอยู่ในแกนมิติที่สาม รูปภาพนี้ช่วยให้สามารถมุ่งความสนใจไปที่การบริหารความ

เสี่ยงขององค์กร หรือที่ประเภทของวัตถุประสงค์ องค์ประกอบ
หน่วยงาน หรือหน่วยงานย่อยใด ๆ ขององค์กรก็ได้

Effectiveness

Determining whether an entity's enterprise risk management is "effective" is a judgment resulting from an assessment of whether the eight components are present and functioning effectively. Thus, the components are also criteria for effective enterprise risk management. For the components to be present and functioning properly there can be no material weaknesses, and risk needs to have been brought within the entity's risk appetite.

ความมีประสิทธิภาพ

การจะตัดสินว่าการบริหารความเสี่ยงขององค์กร
“มี ประสิทธิภาพ” หรือ ไม่นั้น
ตัดสินได้จากการประเมินว่ามีองค์ประกอบทั้งแปดหรือไม่
และองค์ประกอบเหล่านั้นทำงานได้อย่างมีประสิทธิภาพหรือไม่
ดังนั้นองค์ประกอบจึงเป็นเงื่อนไขสำหรับความมีประสิทธิภาพของ
การบริหารความเสี่ยงขององค์กรเช่นกัน
องค์ประกอบที่แสดงบทบาทและทำหน้าที่ได้อย่างถูกต้องเหมาะสม

ะ ส ม จ ะ ต ่ อ ง ไ ม ่ มี จ ุ ด อ ่ น ที่ เ ป ็ น ส ำ ร ะ ส ำ ค ัญ
และ ความ เส ี ย ง จะ ต ่ อ ง ไ ด้ ร ับ การ บริ หาร จ ั ด การ ให้ อยู่ ภาย ไ ต รั ด ด้
บ ความ เส ี ย ง ที่ อ ง ค ์ กร ย อ ม ร ับ ไ ด้

When enterprise risk management is determined to be effective in each of the four categories of objectives, respectively, the board of directors and management have reasonable assurance that they understand the extent to which the entity's strategic and operations objectives are being achieved, and that the entity's reporting is reliable and applicable laws and regulations are being complied with.

เมื่อได้พิจารณาว่าการบริหารความเสี่ยงขององค์กรมีประสิทธิภาพ
ผลในแต่ละวัตถุประสงค์ ทั้งสี่ประเภทตามลำดับแล้ว
คณะกรรมการและฝ่ายบริหารจะเข้าใจว่าองค์กรจะบรรลุวัตถุประสงค์
ด้านกลยุทธ์และด้านการปฏิบัติการได้เพียงใดด้วยความ
มั่นใจอย่างสมเหตุสมผล
รวมถึงเข้าใจว่ารายงานที่องค์กรจัดทำขึ้นมีความน่าเชื่อถือและ
ถูกต้องตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

The eight components will not function identically in every entity. Application in small and mid-size entities, for example, may be less formal and less structured. Nonetheless, small entities still can have effective

enterprise risk management, as long as each of the components is present and functioning properly.

องค์ประกอบทั้งแปดประการไม่ได้ทำหน้าที่แบบเดียวกันในทุก
องค์กร ตัวอย่างเช่น
การประยุกต์ใช้ในองค์กรขนาดเล็กและขนาดกลาง
อาจมีความเป็นทางการและเป็นแบบแผนน้อยกว่า
ตัวอย่าง ไร ก็ ต าม
องค์กรขนาดเล็กยังสามารถมีการบริหารความเสี่ยงขององค์กร
ที่มีประสิทธิผลได้ตรงเท่าที่องค์ประกอบแต่ละองค์ประกอบยัง
คงแสดงบทบาทและทำหน้าที่ได้อย่างถูกต้องเหมาะสม

Limitations

While enterprise risk management provides important benefits, limitations exist. In addition to factors discussed above, limitations result from the realities that human judgment in decision making can be faulty, decisions on responding to risk and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions. These limitations preclude a board and management from having

absolute assurance as to achievement of the entity's objectives.

ข้อจำกัด

แม้ว่าการบริหารความเสี่ยงขององค์กรจะให้ประโยชน์อย่างใหญ่หลวง แต่ก็ยังมีข้อจำกัดอยู่บ้าง นอกจากนี้ปัจจัยที่กล่าวถึงข้างต้นแล้วยังมีข้อจำกัดจากความจริงที่ว่า ใน การ ใ ช้ ดุลยพินิจและการตัดสินใจของมนุษย์เรานั้นอาจผิดพลาดได้ การตัดสินใจในการตอบสนองต่อความเสี่ยงและการควบคุมที่กำหนดขึ้นจำเป็นต้องพิจารณาถึงต้นทุนและประโยชน์ที่เกี่ยวข้อง ความล้มเหลวจึงอาจเกิดขึ้นได้จากความผิดพลาดหรือความคลาดเคลื่อนเล็กๆ น้อยๆ ของมนุษย์ การหลีกเลี่ยงไม่ปฏิบัติตามมาตรการควบคุมโดยการสมคบกันของคนที่ตั้งแต่สองคนหรือมากกว่าสองคนขึ้นไป และการที่ฝ่ายบริหารใช้อำนาจฝ่าฝืนมาตรการในการบริหาร ความเสี่ยง ข้อจำกัดเหล่านี้เป็นอุปสรรคที่ทำให้คณะกรรมการและฝ่ายบริหารไม่สามารถมั่นใจได้อย่างเต็มที่ที่ว่าองค์กรจะสามารถบรรลุวัตถุประสงค์ขององค์กรได้

Encompasses Internal Control

Internal control is an integral part of enterprise risk management. This enterprise risk management

framework encompasses internal control, forming a more robust conceptualization and tool for management. Internal control is defined and described in Internal Control – Integrated Framework. Because that framework has stood the test of time and is the basis for existing rules, regulations, and laws, that document remains in place as the definition of and framework for internal control. While only portions of the text of Internal Control – Integrated Framework are reproduced in this framework, the entirety of that framework is incorporated by reference into this one.

การบริหารความเสี่ยงครอบคลุมถึงการควบคุมภายใน
การควบคุมภายในคือส่วนประกอบที่สำคัญส่วนหนึ่งของการบริหารความเสี่ยงขององค์กร กรอบโครงสร้างการบริหารความเสี่ยงขององค์กรนี้ได้นำเอาการควบคุมภายในมารวมไว้เพื่อเสริมแนวคิดและสร้างเครื่องมือที่แข็งแกร่งยิ่งขึ้นให้กับฝ่ายบริหาร โดยให้คำจำกัดความและการอธิบายอย่างละเอียดของการควบคุมภายในไว้ในกรอบโครงสร้างการควบคุมภายในเชิงบูรณาการ (Internal Control – Integrated Framework) เนื่องจากกรอบโครงสร้างดังกล่าวได้ผ่านการทดลองใช้มาระยะหนึ่งแล้ว และเป็นพื้นฐานสำหรับการออกกฎระเบียบ ข้อบังคับ และกฎหมาย และเอกสารเหล่านั้นยังคงมีอยู่เพื่อใช้อธิบายความหมายของกรอบโครงสร้างของการควบคุมภายใน ในขณะที่มีการนำเนื้อหาบางส่วนของกรอบโครงสร้างการคว

บทความภายในเชิงบูรณาการ (Internal Control – Integrated Framework) มากำหนดเป็นกรอบโครงสร้างใหม่นี้ ก็ได้มีการนำเนื้อหาทั้งหมดของกรอบโครงสร้างนั้นมาผนวกและอ้างอิงในกรอบโครงสร้างการบริหารความเสี่ยงขององค์กรนี้ด้วย

Roles and Responsibilities

Everyone in an entity has some responsibility for enterprise risk management. The chief executive officer is ultimately responsible and should assume ownership. Other managers support the entity's risk management philosophy, promote compliance with its risk appetite, and manage risks within their spheres of responsibility consistent with risk tolerances. A risk officer, financial officer, internal auditor, and others usually have key support responsibilities. Other entity personnel are responsible for executing enterprise risk

management in accordance with established directives and protocols. The board of directors provides important oversight to enterprise risk management, and is aware of and concurs with the entity's risk appetite. A number of external parties, such as customers, vendors, business partners, external auditors, regulators, and financial analysts often provide information useful in effecting enterprise risk management, but they are not responsible for the effectiveness of, nor are they a part of, the entity's enterprise risk management.

บทบาทและความรับผิดชอบ

ทุกคนในองค์กรมีความรับผิดชอบต่อการบริหารความเสี่ยงของ
อ ก ก ร
ประธานเจ้าหน้าที่บริหารมีความรับผิดชอบสูงสุดและควรถือว่าเป็น
เจ้าของเรื่อง ผู้จัดการฝ่ายอื่น ๆ
เป็นผู้สนับสนุนปรัชญาการบริหารความเสี่ยงขององค์กรและส่งเสริมให้มีการปฏิบัติตามมาตรฐานต่าง ๆ
ที่กำหนดไว้ตามระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk
Appetite)

รวมทั้งบริหารจัดการความเสี่ยงภายใต้ขอบเขตความรับผิดชอบ
ของตนโดยให้อยู่ภายใต้ช่วงความเบี่ยงเบนของความเสี่ยงที่
ยอมรับได้ (Risk Tolerance)
โดยปกติเจ้าหน้าที่บริหารความเสี่ยง เจ้าหน้าที่การเงิน
ผู้ตรวจสอบภายในและบุคลากรอื่น ๆ
มีหน้าที่เป็นผู้ให้การสนับสนุนหลัก

ส่วนบุคลากรของหน่วยงานอื่น ๆ มีความรับผิดชอบต่อการปฏิบัติตามมาตรการบริหารความเสี่ยง ของ องค์กร โดยให้สอดคล้องกับคำสั่งและระเบียบวิธีที่กำหนดไว้ คณะกรรมการมีหน้าที่ในการสอดส่องดูแลระบบการบริหาร ความเสี่ยง ของ องค์กร รับรู้และเห็นชอบกับระดับความเสี่ยงที่องค์กรยอมรับได้ บุคคลภายนอกจำนวนมาก อาทิเช่น ลูกค้า ผู้ขาย คู่ค้า ทางธุรกิจ ผู้สอบบัญชีภายนอก เจ้าหน้าที่ผู้ออกกฎระเบียบและนักวิเคราะห์การเงิน มักให้ข้อมูลที่เป็นประโยชน์สำหรับการบริหารความเสี่ยงของ องค์กร อย่างไรก็ตาม มีประสิทธิผล แต่บุคคลเหล่านี้ไม่ต้องรับผิดชอบต่อประสิทธิภาพของการบริหาร ความเสี่ยง รวมทั้งไม่ได้เป็นส่วนหนึ่งของการบริหารความเสี่ยงขององค์กรแต่ประการใด

Organization of This Report

This report is in two volumes. The first volume contains the Framework as well as this Executive Summary. The Framework defines enterprise risk management and describes principles and concepts, providing direction for all levels of management in businesses and other organizations to use in evaluating and enhancing the effectiveness of enterprise risk management. This Executive Summary is a high-level overview directed to chief executives, other senior executives, board members, and

regulators. The second volume, Application Techniques, provides illustrations of techniques useful in applying elements of the framework.

การจัดระบบรายงานฉบับนี้

รายงานนี้ได้จัดทำขึ้นเป็นสองเล่ม เล่มแรกประกอบด้วยกรอบโครงสร้างและบทสรุปสำหรับผู้บริหาร กรอบโครงสร้างให้คำจำกัดความของการบริหารความเสี่ยงขององค์กร และอธิบายถึงหลักเกณฑ์และแนวคิดให้แนวทางกับฝ่ายบริหารทุกระดับในองค์กรธุรกิจและองค์กรอื่น ๆ เพื่อใช้ในการประเมินและส่งเสริมประสิทธิผลของการบริหารความเสี่ยงขององค์กร บทสรุปสำหรับผู้บริหารนี้คือบทสรุปในภาพรวมสำหรับประธานเจ้าหน้าที่บริหาร ผู้บริหารระดับสูง กรรมการ และหน่วยงานกำกับดูแลหรือผู้มีหน้าที่กำกับดูแลอื่น ๆ เล่มที่สองคือแนวทางปฏิบัติซึ่งอธิบายให้เห็นอย่างชัดเจนถึงเทคนิคที่เป็นประโยชน์ในการนำองค์ประกอบพื้นฐานของกรอบโครงสร้างไปประยุกต์ใช้

Use of This Report

Suggested actions that might be taken as a result of this report depend on position and role of the parties involved:

การใช้รายงานฉบับนี้

การจะนำข้อเสนอแนะจากรายงานฉบับนี้ไปปฏิบัติขึ้นอยู่กับตำแหน่งและบทบาทของฝ่ายที่เกี่ยวข้อง ดังนี้

- Board of Directors – The board should discuss with senior management the state of the entity’s enterprise risk management and provide oversight as needed. The board should ensure it is apprised of the most significant risks, along with actions management is taking and how it is ensuring effective enterprise risk management. The board should consider seeking input from internal auditors, external auditors, and others.
- คณะกรรมการตรวจสอบหรือกับผู้บริหารระดับสูงถึงสถานภาพของการบริหารความเสี่ยงขององค์กรของตนและคอยสอดส่องดูแลตามที่จำเป็น คณะกรรมการควรแน่ใจว่ากระบวนการบริหารความเสี่ยงได้ครอบคลุมความเสี่ยงที่มีนัยสำคัญส่วนใหญ่แล้วและมาตรการที่ฝ่ายบริหารเลือกใช้เหมาะสมรวมทั้งทำอย่างไรจึงจะมั่นใจได้ว่าการบริหารความเสี่ยงขององค์กรมีประสิทธิภาพ

คณะกรรมการควรพิจารณาแสวงหาข้อมูลจากผู้ตรวจสอบภายใน ผู้สอบบัญชีภายนอกและบุคคลอื่นๆ

- Senior Management – This study suggests that the chief executive assess the organization's enterprise risk management capabilities. In one approach, the chief executive brings together business unit heads and key functional staff to discuss an initial assessment of enterprise risk management capabilities and effectiveness. Whatever its form, an initial assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation.
- ผู้บริหารระดับสูง – รายงานฉบับนี้เสนอแนะให้ประธานเจ้าหน้าที่บริหารประเมินศักยภาพในการบริหารความเสี่ยงขององค์กรทั้งหมด วิธีการหนึ่งคือประธานเจ้าหน้าที่บริหารร่วมกับหัวหน้าหน่วยงานและพนักงานที่ปฏิบัติหน้าที่สำคัญปรึกษาหารือกันเกี่ยวกับประเด็นที่จะประเมินความสามารถและความมีประสิทธิผลของการบริหารความเสี่ยงขององค์กร แต่ไม่ว่ารูปแบบและประเด็นของการประเมินขั้นต้นจะถูกกำหนดขึ้นมาในรูปแบบใด ก็ควรพิจารณาว่ามีความจำเป็นหรือไม่และจะดำเนินการอย่างไรให้มีการประเมินที่ลึกและกว้างยิ่งขึ้น

- Other Entity Personnel – Managers and other personnel should consider how they are conducting their responsibilities in light of this framework and discuss with more-senior personnel ideas for strengthening enterprise risk management. Internal auditors should consider the breadth of their focus on enterprise risk management.
- *บุคลากรอื่นๆในหน่วยงาน – ผู้จัดการและบุคลากรอื่นๆ ควรพิจารณาว่าจะสามารถปฏิบัติงานในความรับผิดชอบที่เกี่ยวข้องกับกรอบโครงสร้างการบริหารความเสี่ยงขององค์กรนี้ได้อย่างไร และปรึกษากับบุคลากรในระดับสูงกว่าถึงแนวคิดในการเสริมสร้างความแข็งแกร่งให้กับการบริหารความเสี่ยงขององค์กร ผู้ตรวจสอบภายในควรพิจารณาถึงขอบเขตที่จะต้องให้ความสนใจในเรื่องการบริหารความเสี่ยงทั่วทั้งองค์กรด้วย*
- Regulators – This framework can promote a shared view of enterprise risk management, including what it can do and its limitations. Regulators may refer to this framework in

establishing expectations, whether by rule or guidance or in conducting examinations, for entities they oversee.

- *หน่วยงานกำกับดูแล* – กรอบโครงสร้างนี้สามารถส่งเสริมให้เกิดมุมมองร่วมกันของการบริหารความเสี่ยงขององค์กร ซึ่งประกอบด้วยสิ่งที่สามารถทำได้และข้อจำกัดต่าง ๆ หน่วยงานกำกับดูแลอาจอ้างถึงกรอบโครงสร้างนี้เพื่อกำหนดสิ่งที่คาดหวังขึ้น ไม่ว่าจะด้วยการออกกฎการกำหนดแนวทางหรือการกำหนดวิธีการตรวจสอบขององค์กรที่ตนกำกับดูแลอยู่
- Professional Organizations – Rule-making and other professional organizations providing guidance on financial management, auditing, and related topics should consider their standards and guidance in light of this framework. To the extent diversity in concepts and terminology is eliminated, all parties benefit.
- *ออกกฏระเบียบหรือองค์กรวิชาชีพ* – ผู้ออกกฏระเบียบหรือองค์กรวิชาชีพอื่น ๆ ซึ่งเป็นผู้กำหนดแนวทางการบริหารจัดการทางการเงิน การตรวจสอบ และเรื่องอื่นที่เกี่ยวข้อง ควรคำนึงถึงมาตรฐานและแนวทางของตนเกี่ยวกับกรอบโครงสร้างนี้ และเมื่อได้ขจัดความแตกต่างหลากหลายในแนวคิดและศัพท์บัญญัติให้หมดไปแล้วทุกฝ่ายก็จะได้รับประโยชน์

- Educators – This framework might be the subject of academic research and analysis, to see where future enhancements can be made. With the presumption that this report becomes accepted as a common ground for understanding, its concepts and terms should find their way into university curricula.
- *นักวิชาการคือกษัตริย์* – กรอบโครงสร้างนี้อาจเป็นหัวข้อของการวิเคราะห์หรือวิจัยเชิงวิชาการเพื่อดูว่าจะสามารถยกระดับการพัฒนาในอนาคตเป็นแบบใดบ้าง โดยอนุমানว่ารายงานฉบับนี้เป็นที่ยอมรับให้เป็นพื้นฐานสำหรับการทำความเข้าใจจึงควรนำเอาแนวคิดและขอบเขตเนื้อหาของเรื่องนี้ไปบรรจุอยู่ในหลักสูตรของมหาวิทยาลัย

With this foundation for mutual understanding, all parties will be able to speak a common language and communicate more effectively. Business executives will be positioned to assess their company's enterprise risk management process against a standard, and strengthen the process and move their enterprise toward established goals. Future research can be leveraged off an established base. Legislators and

regulators will be able to gain an increased understanding of enterprise risk management, including its benefits and limitations. With all parties utilizing a common enterprise risk management framework, these benefits will be realized.

ด้วยรากฐานการเข้าใจร่วมกันนี้ทุกฝ่ายจะสามารถพูดภาษาเดียวกันและสื่อสารกันได้อย่างมีประสิทธิภาพ ผลลัพธ์ยิ่งขึ้นผู้บริหารธุรกิจมีหน้าที่เป็นผู้ประเมินกระบวนการบริหารความเสี่ยงขององค์กรของตนเทียบกับมาตรฐานและปรับปรุงกระบวนการปฏิบัติให้แข็งแกร่งยิ่งขึ้นรวมทั้งนำองค์กรของตนมุ่งไปยังเป้าหมายตามที่ได้ตั้งไว้ งานวิจัยจะสามารถต่อยอดไปจากพื้นฐานที่วางไว้แล้ว นักกฎหมายและหน่วยงานกำกับดูแลจะสามารถใช้ประโยชน์และทำความเข้าใจในเรื่องการบริหารความเสี่ยงขององค์กร รวมถึงผลประโยชน์และข้อจำกัดต่าง ๆ เพิ่มมากขึ้น เมื่อทุกฝ่ายใช้ประโยชน์จากกรอบโครงสร้างการบริหารความเสี่ยงขององค์กรในลักษณะเดียวกันแล้วคุณประโยชน์ต่าง ๆ ดังกล่าวก็จะเกิดกับทุกฝ่าย