Updated COSO Enterprise Risk Management:

Integrating with Strategy and Performance

Enterprise Risk Management-Integrated Framework ซึ่งจัดทำโดย The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ตั้งแต่ปี 2004 ถือเป็นเครื่องมือที่หลายบริษัทนำไปใช้เป็นกรอบในการบริหารความเสี่ยง เพื่อสร้างความมั่นใจให้กับผู้มีส่วนได้เสียว่าบริษัทจะสามารถบรรลุวัตถุประสงค์ที่ตั้งไว้ อย่างไรก็ตาม สภาพแวดล้อมทางธุรกิจมีการเปลี่ยนแปลงไปจากเดิมเป็นอย่างมากอันนำมาซึ่งความเสี่ยงที่รุนแรงมากกว่าเดิม โดยเฉพาะความเสี่ยงในระดับกลยุทธ์ ดังนั้น COSO จึงได้ปรับปรุงกรอบการบริหารความเสี่ยงอีกครั้งโดยเมื่อวันที่ 6 กันยายน 2560 และได้เผยแพร่กรอบฉบับใหม่ภายใต้ชื่อ "Enterprise Risk Management — Aligning Risk with Strategy and Performance"

IOD เห็นว่า COSO ERM Framework ฉบับใหม่ดังกล่าว จะเป็นประโยชน์ต่อการทำหน้าที่ในการกำกับดูแลกิจการของคณะกรรมการ ซึ่งปัจจุบันได้รับความคาดหวังจากผู้มีส่วนได้เสียในการทำหน้าที่ดังกล่าวมากขึ้น เมื่อวันที่ 8 พฤศจิกายน 2560 IOD จึงได้จัดการประชุม Independent Director Forum นี้ขึ้นภายใต้หัวข้อ "Updated COSO Enterprise Risk Management: Integrating with Strategy and Performance"

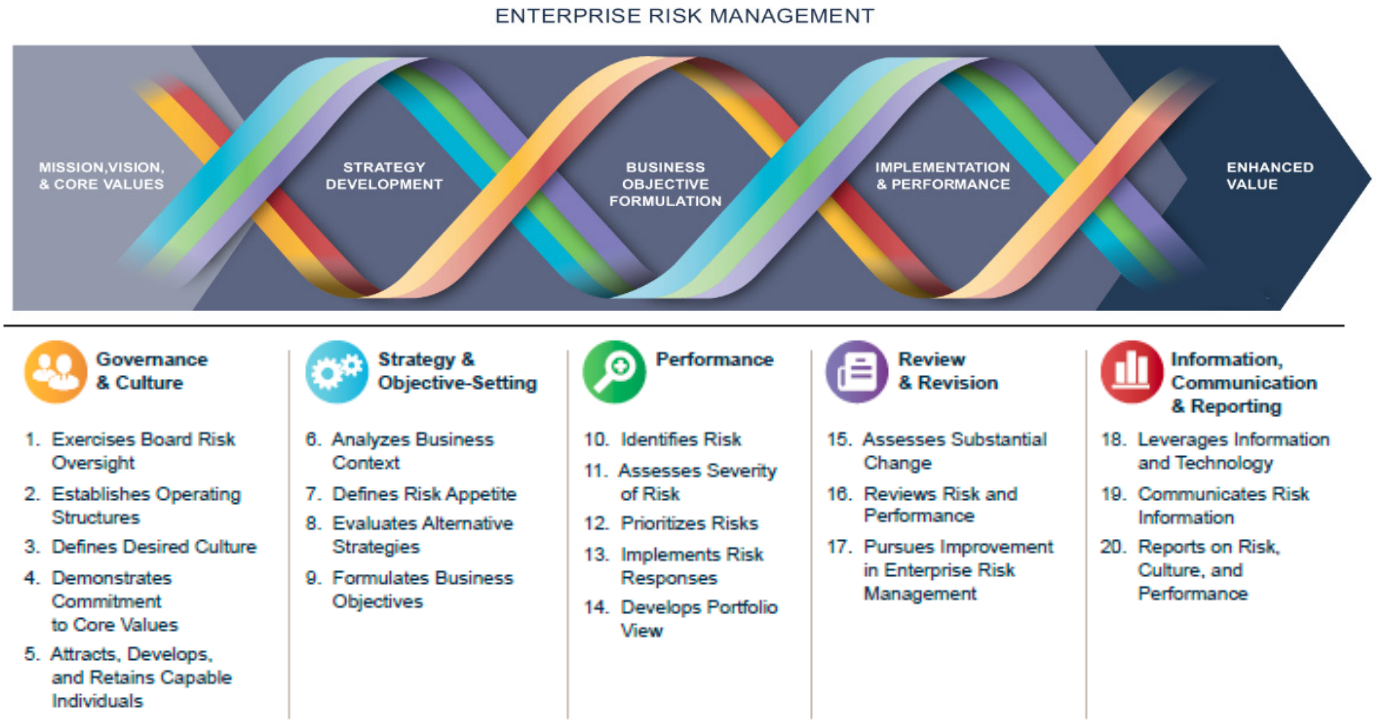
การบรรยายในช่วงแรกโดย Mr. Edward Clayton, Strategy& Managing Partner, PwC SE Asia ได้อธิบายถึงความสำคัญของกลยุทธ์ เนื่องจากปัจจุบันสภาพแวดล้อมทางธุรกิจ มีการเปลี่ยนแปลงในอัตราเร่งที่สูงขึ้น องค์กรต้องทำความเข้าใจและสามารถเชื่อมโยงกลยุทธ์กับความเสี่ยงเข้าด้วยกัน ถือเป็นความท้าทายที่องค์กรต่างๆ ต้องเผชิญ การวางกลยุทธ์ต้องฉลาดมากขึ้น ประกอบกับความไม่แน่นอนของการเมืองในเอเชีย ยุโรป เช่น การแยกตัวออก EU ของอังกฤษ แรงกดดันด้านกฎระเบียบต่างๆ การเปลี่ยนแปลงด้านดิจิตอล และความคาดหวังของลูกค้า

ระหว่างการบรรยาย มีการสำรวจความเห็นของผู้เข้าร่วมงาน ซึ่งสามารถสรุปได้ ดังนี้

1. ร้อยละ 57 เห็นว่าความเสี่ยงด้านดิจิตอลเป็นความเสี่ยงที่สำคัญที่สุดของบริษัทไทย ส่วนอีกร้อยละ 21 ให้ความสำคัญกับความเสี่ยงที่ไม่คาดคิดว่าจะเกิดขึ้น ทั้งนี้ Mr. Edward Clayton ได้ยกตัวอย่างบริษัท บล็อกบัสเตอร์ ที่ต้องปิดตัวลง เนื่องจากมีการเปลี่ยนแปลงด้านเทคโนโลยี แต่ผู้นำไม่มีกลยุทธ์ในการรองรับและปฏิเสธที่จะเปลี่ยนแปลงตัวเอง

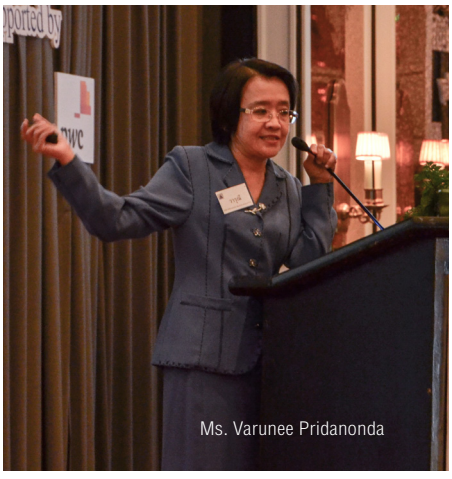

Mr. Edward Clayton

2. ร้อยละ 52 ระบุถึงความถี่ที่คณะกรรมการได้รับรายงานเรื่องความเสี่ยงของบริษัทจากฝ่ายบริหารว่า ได้รับรายงานทุก 6 เดือน และร้อยละ 33.3 ได้รับรายงานเป็นรายปี



3. มีเพียงร้อยละ 28.6 พึงพอใจในคุณภาพรายงานการบริหาความเสี่ยงของฝ่ายบริหาร ส่วนอีกร้อยละ 65 เห็นว่าควรปรับปรุง

จากนั้นคุณวารุณี ปรีดานนท์ หุ้นส่วน-ที่ปรึกษาการกำกับดูแลกิจการ การบริหารความเสี่ยง การควบคุมภายในและการตรวจสอบภายใน บริษัท ไพร้ซวอเตอร์เฮาส์คูเปอร์ส เอบีเอเอส จำกัด ได้นำเสนอหัวข้อ "What's new in COSO ERM 2017" ซึ่งมีสาระสำคัญว่า ประเด็นสำคัญที่ COSO มีการปรับเปลี่ยน คือ การเชื่อมโยงการวางแผนกลยุทธ์กับความเสี่ยงเข้าด้วยกัน ดังแผนภาพ


Ms. Varunee Pridanonda

กระบวนการวางกลยุทธ์นั้นเริ่มตั้งแต่การกำหนดวิสัยทัศน์ พันธกิจ ค่านิยม จากนั้นก็พัฒนาเป็นกลยุทธ์ กำหนดเป็นวัตถุประสงค์ นำไปปฏิบัติ วัดผล และติดตามผลว่า สามารถนำไปปฏิบัติตามกลยุทธ์ที่วางไว้ และกลยุทธ์นั้นสามารถเพิ่มมูลค่าให้กับองค์กรได้ อย่างไรก็ตาม ที่ผ่านมา การเชื่อมโยงระหว่างกลยุทธ์กับความเสี่ยงในองค์กรส่วนใหญ่ ยังไม่มีประสิทธิภาพเท่าที่ควร COSO จึงได้นำเสนอแนวคิดให้พิจารณากลยุทธ์กับความเสี่ยงไปพร้อมๆ กัน เมื่อกระบวนการของกลยุทธ์ก้าวไป กระบวนการบริหารความเสี่ยงก็จะต้องก้าวไปด้วย

COSO ได้แบ่งกระบวนการบริหารความเสี่ยง ออกเป็น 5 ขั้นตอน (5 Components) ตามกระบวนการพัฒนากลยุทธ์ ซึ่งจะมีรายละเอียด 20 องค์ประกอบ (20 Supporting Principles) ดังนี้

1. การกำหนด วิสัยทัศน์และพันธกิจองค์กร เป็นช่วงเวลาเดียวกันกับที่องค์กรจะต้องมีการกำหนดกรอบการกำกับดูแลความเสี่ยงและวัฒนธรรมองค์กรที่ต้องให้ความสำคัญต่อการกำกับดูแลความเสี่ยง

2. ในช่วงที่มีการพัฒนาและกำหนดกลยุทธ์องค์กรจะต้องมีการพัฒนาสภาพแวดล้อมในการดำเนินธุรกิจเพื่อที่จะกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk appetite) ซึ่งจะช่วยในการตีกรอบการประเมินทางเลือกกลยุทธ์ต่างๆ ขององค์กรผ่านการประเมินความเสี่ยงของแต่ละทางเลือก ทำให้องค์กรสามารถพิจารณาได้ว่าทางเลือกกลยุทธ์ใดที่องค์กรจะจัดการความเสี่ยงได้ดีที่สุด

3. ช่วงการปฏิบัติเพื่อให้เป็นไปตามเป้าประสงค์ในระดับธุรกิจ ความเสี่ยงอาจกระทบต่อความสำเร็จในการดำเนินตามกลยุทธ์ได้ทุกเมื่อ ดังนั้นระหว่างนำกลยุทธ์ไปปฏิบัติจะต้องมีการระบุความเสี่ยง ประเมินความเสี่ยงและตอบสนองความเสี่ยงควบคู่กันไป รวมถึงต้องดูภาพของการบริหารความเสี่ยงเป็นภาพใหญ่ทั้งหมด อันจะส่งผลให้กระบวนการบริหารความเสี่ยงทั่วทั้งองค์กรและการจัดการกลยุทธ์เป็นไปอย่างมีประสิทธิภาพยิ่งขึ้น

4. ในช่วงที่มีการดำเนินกลยุทธ์ การทบทวนและการปรับปรุงการจัดการกลยุทธ์เป็นเรื่องที่เกิดขึ้นได้ องค์กรจะต้องประเมินความเสี่ยงที่อาจเปลี่ยนแปลงตามไปด้วย เพื่อพัฒนาและปรับปรุงกระบวนการบริหารความเสี่ยงให้เหมาะสม

5. สุดท้ายแล้วการบริหารความเสี่ยงเป็นกระบวนการที่ต้องการความต่อเนื่องการจัดเก็บข้อมูล การสื่อสารข้อมูลทั้งภายในและภายนอกเป็นเรื่องสำคัญซึ่งจะส่งผลให้การจัดการกลยุทธ์มีประสิทธิผลและส่งผลต่อการเพิ่มคุณค่าให้กับองค์กรในที่สุด

เป็นที่แน่นอนว่าแผนกลยุทธ์นั้น ต้องมีการปรับแผนกันทุก 6 เดือน หรือทุกไตรมาส หากเห็นว่าแผนกลยุทธ์ไม่เป็นไปตามเป้าหมาย หรือมีความเสี่ยงเพิ่มขึ้นเพราะเหตุการณ์เปลี่ยนแปลงไป จำเป็นจะต้องมีการสอบทาน ซึ่งบางครั้งต้องกลับไปสอบทานที่ตัวกลยุทธ์ รวมทั้งต้องมีการพิจารณาที่กระบวนการจัดการความเสี่ยงขององค์กรรวมด้วย

จากกรณีตัวอย่างของ Kobe Steel ทำให้เห็นว่าคณะกรรมการต้องมีบุคคลจากภายนอกเพื่อคอยตั้งคำถามที่คนภายในอาจมองข้าม สังคมคาดหวังบทบาทของกรรมการอิสระว่าท่านจะถามคำถามที่เกี่ยวข้องกับความเสี่ยงของบริษัท เช่น ในกรณีของ GM เป็นบทเรียนของความล้มเหลวของการบริหารความเสี่ยง เนื่องจากมีการเรียกรถคืน แต่หากองค์กรมีการบริหารความเสี่ยงที่ดีก็จะไม่เกิดความเสียหาย ไม่ต้องเสียค่าปรับ ไม่ส่งผลเสียต่อชื่อเสียงและฐานะทางการเงิน เป็นต้น

ดังนั้นบทบาทของกรรมการอิสระจึงมีความสำคัญอย่างมากในการบริหารความเสี่ยง ในคู่มือกรรมการอิสระของตลาดหลักทรัพย์ฯ มีการระบุถึงหน้าที่ของกรรมการอิสระว่า ต้องดูแลให้กิจการมีระบบการควบคุมภายในและการบริหารความเสี่ยงที่เหมาะสม และ CG Code ที่ ก.ล.ต. จัดทำขึ้นได้มีการนำเสนอถึงบทบาทของกรรมการในเรื่องของการบริหารความเสี่ยงด้วย

สำหรับประเด็นสำคัญที่คณะกรรมการต้องให้ความสำคัญ คือ

- คณะกรรมการจะให้ความเชื่อมั่นแก่นักลงทุนได้อย่างไรว่า ได้มีการกำกับดูแลความเสี่ยงอย่างมีประสิทธิภาพ ข้อแนะนำ คือ กรรมการต้องพิจารณาเรื่องการเปิดเผยข้อมูลว่า ได้อธิบายความเสี่ยงให้ผู้ถือหุ้น นักลงทุนเข้าใจเรื่องความเสี่ยงอย่างครบถ้วน และคณะกรรมการได้กำกับดูแลความเสี่ยงอย่างไร

- พิจารณาองค์ประกอบของคณะกรรมการว่า มีองค์ประกอบของความเชี่ยวชาญด้านต่างๆ และมีองค์ประกอบที่เหมาะสมหรือไม่

- มีความเสี่ยงใดที่แม้แต่ในระดับกรรมการอาจมองไม่เห็น คณะกรรมการต้องมอบหมายหรือจัดสรร การบริหารความเสี่ยงนั้นให้อยู่ในความรับผิดชอบในคณะกรรมการชุดย่อยต่างๆ ตามความเชี่ยวชาญ

- คณะกรรมการได้ดูแลความเสี่ยงเรื่องการปฏิบัติตามกฎระเบียบต่างๆ หรือไม่

ความท้าทายของคณะกรรมการในการกำกับดูแลความเสี่ยง คือ กรรมการจะทราบได้อย่างไรว่า ระบบการบริหารความเสี่ยงสร้างมูลค่าให้กับองค์กรจริงๆ เพราะเป้าหมายของการบริหารความเสี่ยง คือ การทำให้กลยุทธ์สำเร็จ คณะกรรมการต้องสังเกตว่า องค์กรมีลักษณะต่อไปนี้หรือไม่ เช่น

- ในการพูดคุยเรื่องกลยุทธ์ มีแต่เรื่องโอกาส แต่ไม่มีประเด็นความเสี่ยง

- มีความเสี่ยงแต่ไม่มีผลการวิเคราะห์ไม่มีความเชื่อมโยงให้เห็นว่า หากความเสี่ยงเกิดขึ้นจะมีผลกระทบต่อองค์กรอย่างไร

- เน้นเฉพาะความเสี่ยงที่เห็นได้ง่าย ระบุความเสี่ยงเหมือนกันในทุกปี ดังนั้นคณะกรรมการต้องถามว่ามีความเสี่ยงใหม่อะไรบ้าง

- ERM ไม่ได้รับความสนใจจากผู้บริหาร ควรสอบถามผู้บริหารว่าระบบบริหารความเสี่ยงเป็นอย่างไร นำสิ่งที่ปฏิบัติอยู่กับแนวปฏิบัติระดับสากลที่ COSO แนะนำมาเทียบกัน วิเคราะห์ว่า ประเด็นใดที่แตกต่างกันบ้างหรือไม่ หากยังไม่มีภาพความเสี่ยงระดับองค์กรหรือความเสี่ยงระดับกลยุทธ์ ต้องให้ฝ่ายบริหารแก้ไขปรับปรุงก่อน

องค์กรที่มีการบริหารที่ดีนั้น คือ องค์กรที่มีการบริหารความเสี่ยงที่เชื่อมโยงกับกลยุทธ์วางแผนไปพร้อมๆ กัน และเรื่องของความเสี่ยงควรถูกให้ความสำคัญในระดับบนก่อน จึงจะสามารถสร้างวัฒนธรรมในการคำนึงถึงความเสี่ยงให้เกิดขึ้นทั่วทั้งองค์กรได้

"Good ERM starts at the top of the company, then quickly becomes part of how everyone thinks and treats the risks they face in their day-to-day work."

Enterprise Risk Management-Integrated Framework which has been made by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) since 2004 is a tool that many companies use as a risk management framework to ensure the stakeholders that the companies could achieve their goal. However, the business environment has changed drastically. As a consequence, the risks are more severe, especially the risk at strategic level. Thus, COSO has adjusted risk management framework again on September 6, 2017 and publicized the new framework under the name "Enterprise Risk Management – Aligning Risk with Strategy and Performance"

IOD considers a new COSO ERM Framework as a useful tool for the duty of the board of directors in corporate governance which they are expected more from the stakeholders for this duty. On November 8, 2017, IOD organized a meeting Independent Director Forum on the topic "Updated COSO Enterprise Risk Management: Integrating with Strategy and Performance"

The talk at the beginning was given by Mr. Edward Clayton, strategy& managing partner, PwC SE Asia. He explained the importance of the strategy because the business environment had changed with a higher acceleration. The organizations have to understand it and be able to connect the strategy with the risk. It was a challenge for the organizations that they had to deal with the situation with a smarter strategy. Besides, there were the instability of politics in Asia and Europe such as, Brexit, pressure from regulations, digital change and expectation from the customers.


Ms. Pinpradab Chotiprasidhi

During the talk, there was an opinion survey of the attendants which could be summarized as follows,

1. Fifty seven percent had an opinion that digital risk was the most important risk for Thai companies. Other 21 percent focused on the unexpected risk. Nevertheless, Mr. Edward Clayton raised an example of Blockbuster that had closed because of the technological change but the leaders did not have a strategy to deal with it and denied to change themselves.

2. Fifty two percent indicated the frequency that the board of directors received a risk report from the management every 6 months and 33.3 percent received a report annually.

3. Only 28.6 percent was satisfied with the quality of the risk management report from the management and other 65 percent had an opinion that it should be improved.

Then, Ms. Varuni Preedanon, corporate governance, risk management, internal control and internal audit advisor-partner, PricewaterhouseCoopers ABAS Company Limited presented the topic "What's new in COSO ERM 2017". The key issue that COSO had been adjusted was connecting strategic planning and risk as following diagram.

Strategic planning begins with vision, mission and value. From these, the organization develops strategy and objective. Then, the strategy is implemented, evaluated and monitored if it could be done according to the strategic planning and the strategy could increase value for the organization. However, in the past, the connection between strategy and risk in most organizations was not so effective. Thus, COSO presented a concept to consider strategy and risk simultaneously. When the process of the strategy goes forward, the risk management process must also be stepped up.

COSO has divided the risk management process into 5 components according to the strategy development which consists of 20 principles as follows,

1. Vision and mission statement, the organization must set a framework for risk management and corporate culture to address the risk management.

2. During the development and setting of strategy, the organization has to create an environment for business operation to determine the risk appetite which helps to make a framework for assessing the strategies of the organization through risk assessment of each choice. This allows the organization to consider which strategy is the best for the organization to manage the risk.

3. During the implementation to achieve the objective at business level, the risk might have an effect on the success in strategy implantation at any time. Thus, the risk has to be indicated, assessed and responded at the same time. We also have to look at the risk management with the bird-eye view. This will make the risk management throughout the organization and strategy management more effective.

4. During the strategy implementation, revision and improvement of the strategy management is possible. The organization has to assess the changing risk in order to develop and improve the appropriate risk management process.

5. Finally, risk management is a process that needs continuity. Data storage and internal and external information communication is an important issue which will have an effect on the effectiveness of the strategy management and effect on value creation of the organization in the end.

Certainly, the strategic plan has to be adjusted every 6 months or every quarter. If the strategic plan does not meet the goal or it becomes riskier because of the changing situation, it needs to be revised. Sometimes, the strategy itself has to be

revised. The risk management process of the organization has to be considered as well.

From the case study of Kobe Steel, the board has to include people from outside to ask questions that people inside may overlook. The society expects the role of independent directors that they will ask questions related to the company's risk, such as in the case of GM, as a lesson of failing to manage the risk because there is a call back of cars. If the organization has a good risk management, there will be no damage, fine or effect on the reputation and financial status etc.

Therefore, the role of independent directors is very important in risk management. In the manual of independent directors of the Stock Exchange of Thailand (SET), the duty of the independent director is indicated that he/she has to ensure that the company has an appropriate internal control and risk management system. Besides, the CG Code prepared by the Securities and Exchange Commission also presents the role of directors in risk management.

The key issues that the board has to focus on are as follows,

- How can the board ensure the investor confidence that there is an effective risk management? The recommendation is that the directors have to consider the information disclosure how to explain the risk to the shareholders and investors to understand the risk completely and how the board manages the risk.

- Consider the composition of the board if the board is composed of directors with expertises from different fields and the composition is appropriate.

- The risk that the director might not see, the board has to assign or allocate the risk management to different subcommittees based on their expertise

- The board has to consider if they take care of the risk in regulation compliance.

The challenge of the board in risk management is how to know if the risk management system really creates value for the organization because the goal of risk management is to make the strategy successful. The board has to notice if the organization has the following characteristics,

- The talk about strategy has only opportunity but not risk.

- There is a risk but there is no analysis and the link to show how the risk affects the organization

- Focus on the risk that could be seen easily, indicate the same risk every year. Thus, the board has to ask for new risks.

- The executives do not focus on ERM. The executive should be asked how the risk management is. Compare the current practice with the international practice recommended by COSO, analyze if there is a different issue. If there is no risk at organization level or strategic level, the executives have to improve it first.

A good organization with a good management is the organization that has the risk management linking with strategic planning. Both are planned simultaneously. The risk management should be a priority from the upper level first, and then it could create a culture of risk awareness throughout the organization.

Event Supported by

pwc ptt

นางวีรินทร์ ศิริพันธ์
Mrs. Veerin Siriphan

Sr. CG Analyst
Research & Policy
Thai IOD