Enterprise and Strategic Risk Management: A Proposal for Maturing Risk Management in Belgian Defence

David Nyikos

Colonel David Nyikos received his master after master degree of arts (Master ès arts in political and military sciences) as a member of the 130th division of the Advanced Staff Course at the Belgian Royal Military Academy. He holds an MSc in engineering management from the Air Force Institute of Technology (USA) and a BSc in engineering sciences from the United States Air Force Academy. He is currently Strategic Policy Planner for the U.S. Military Delegation to NATO[1].

Terwijl de Belgische Defensie haar wettelijke bevoegdheden uitoefent, kampt ze met nakende fiscale en organisatorische veranderingen die de ontwikkeling van technieken voor strategisch risicomanagement vereisen. Het academisch onderzoek naar een dergelijk ondernemingsbreed risicomanagement staat nog in zijn kinderschoenen, met schaarse resultaten tot gevolg. De resultaten van vijf casestudy's van organisaties met ongeveer even veel werknemers als de Belgische Defensie en die daarenboven erin geslaagd zijn om programma's op het gebied van bedrijfsrisicobeheer of strategisch risicomanagement uit te voeren, worden vergeleken zowel met benchmarks van de Verenigde Naties als met een op maat gemaakte maturiteitsmatrix. Op basis van de beste praktijken van en geleerde lessen uit de casestudy's wat betreft de beoordeling van de maturiteit van bedrijfsrisicobeheer (in het Engels enterprise risk management of, afgekort, ERM) binnen de Belgische Defensie, doet de auteur drie aanbevelingen om de kennis van strategisch risicomanagement binnen Defensie te verrijken, uit te breiden en tot volledige ontwikkeling te laten komen.

La Défense belge fait face à ses mandats légaux alors que se profilent à l'horizon des changements financiers et organisationnels qui sont de nature à encourager la mise au point de techniques de gestion des risques stratégiques. Les recherches académiques sur ce type de gestion des risques à l'échelle d'une entreprise sont en plein développement, mais encore limités. Les résultats de cinq études de cas traitant d'entreprises d'un volume de personnel similaire à celui de la Défense belge et qui sont parvenues à mettre en place des programmes de gestion des risques d'entreprise ou stratégiques, sont confrontés aux normes des Nations unies et à une matrice de maturité définie sur mesure. À la lumière des meilleurs enseignements de ces cas d'école au niveau de la maturité de la gestion des risques d'entreprise (en anglais, enterprise risk management, ERM) constatée à la Défense belge, l'auteur propose trois pistes pour enrichir, étendre et mûrir l'usage de la gestion des risques stratégiques pour l'ensemble de la Défense.

In December 2015 the Belgian Minister of Defence outlined a new strategic plan for Defence. Among other changes, the plan calls for a reduction of military personnel from the current end strength of approximately 32,000 servicemen and women to 25,000 by 2030. While the Minister's plan forecasts budget increases beginning in 2019, the September 2013 monetary figures released by the Belgian Defence Staff Department for Strategy (ACOS Strat) show that defence spending decreased steadily from 1.5 percent of gross domestic product to approximately 0.75 percent from 1990 to 2011. At the same time, the list of tasks for the military continues to grow, and leaders seek methods to eliminate waste and maximise efficiencies. In addition to shepherding Defence into realising the new strategic plan, leaders are also addressing legal compliance. A Belgian Royal Decree requires that Defence implement measures to control risk at all levels[2]. Subordinate units currently carry out and are evaluated on their use of such measures, but the highest staff organisations have only just begun such management practice. In order to seek solutions, the Office of the Director of Staff (DOS) in the Office of the Belgian Chief of Defence began investigating risk management at the highest executive level. As a result, Defence will implement strategic risk management (SRM) processes at its Steering Committee (CoDir) level over the next year. Certainly, there are examples to draw upon, but first: what exactly is SRM?

An evolution

Literature suggests that academic study on risk management began in earnest after the Second World War. Since the end of the war, there have been a number of evolutions which furthered our understanding of risk within organisations. While financial and operational risk analysis are considered a prudent aspect of ordinary management practice, recent global crises brought attention to how risk can integrate across different units in order to combine and result in significant positive and negative impacts to the entirety. Left unaddressed, such risks can lead to organisational failure and arguably have led to global impacts, such as the financial crisis of 2008 and 2009. Seeking an all-encompassing definition of SRM is not the intent of this paper, but framing its discussion is helpful. Enterprise risk management (ERM) combines risk management and internal control across all elements of an organisation to maximise value, and it enables SRM. Senior executive leaders apply SRM by using input from ERM processes. They manage risks to organisational strategies through periodic reviews of possible events which identify both opportunities to succeed as well as options to mitigate potential misfortune.

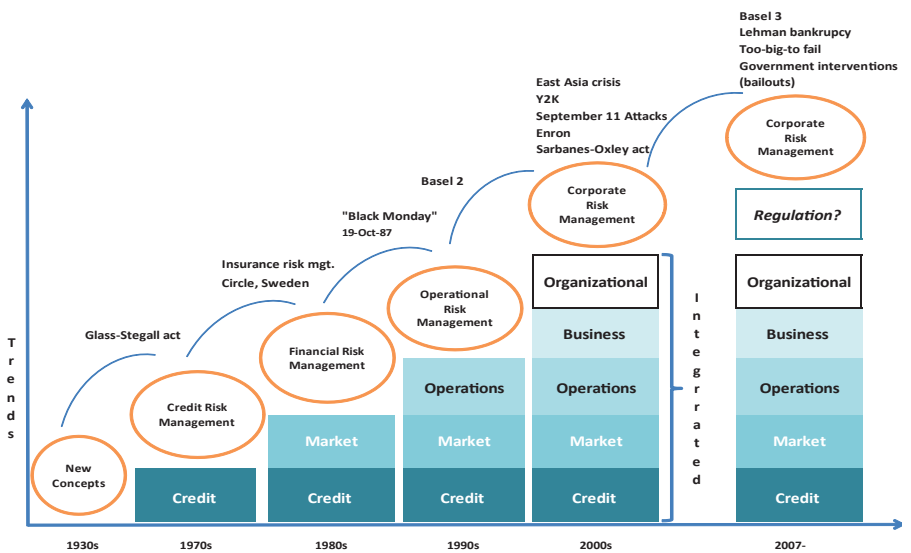

Figure 1. Evolution of risk management.[3]

The academic world has unfortunately only just begun to attempt rigorous analysis of this premise, but after recent global crises, governments wasted little time enacting new oversight. As such, keepers of industrial standards, including the International Organization for Standardization (ISO), the International

Organization of Supreme Audit Institutions (INTOSAI), and Committee of Sponsoring Organizations of the Treadway Commission (COSO) have codified best practices and lessons learned from anecdotal experiences and practitioner implementation of new techniques. Furthermore, the government of some countries, including the United Kingdom, Australia, and Canada, mandated their use. The United Nations (UN) even conducted a 2010 study[4] to identify benchmarks for governmental organisations launching ERM. Lacking a body of academic research to point a way ahead, the next best option is to identify how similar organisations successfully implemented processes to manage enterprise and strategic risk through case study.

Case study

Thankfully, practitioners also utilise case studies. In their 2015 book[5], John Fraser, Betty Simkins, and Kristina Narvaez compiled thirty-three case studies that detail successful implementation of ERM and SRM into a single book covering a variety of different organisations. Generally speaking, risk varies greatly based upon what an entity does. Therefore, benchmarking representative case studies ideally identifies more applicable best practices.

Robert Camp, whom many consider to be the father of benchmarking, recommended in a 2008 interview to limit study to between three and six entities. Additionally, a Belgian Royal Decree and Chief of Defence policy require using either INTOSAI or COSO frameworks. Most organisations tailor their implementation to their unique structure and business, but those who utilised ISO standards were excluded from selection. Even with these limitations, it is possible to select organisations of similar size and operational scope within the above-mentioned thirty-three case studies. Defence previously looked at other military examples, but this study focused on non-military examples. In order to approximate a Defence consisting of 25,000 personnel, case selection included organisations ranging from 10,000 to 75,000 employees. While governmental organisations might be considered ideal cases, public and private companies with multiple divisions or multinational presence offer potentially similar organisational characteristics. These criteria produced five suitable cases from Fraser, Simkins, and Narvaez, and each offers insight into successful implementation of enterprise and SRM.

Five examples

City of Edmonton

The capital city of the Canadian province of Alberta, Edmonton is home to around 800,000 people. The city government consists of 11,000 employees working in five different departments across twelve geographic regions. Ken Baker, the city's ERM program manager, described how Edmonton implemented their system. In 2003, the Office of the City Auditor initiated a project to create an ERM framework. The result was a COSO-based model named Corporate Business Risk Planning, but the associated pilot initiative launched in 2005 was never fully implemented. In 2011 the city created an ERM programme manager position and working committee consisting of subject-matter experts from across the city administration. A programme manager was hired in 2012, and the programme was reinvigorated by initiating a new ERM framework. While Edmonton is still in the process of establishing their programme, it offers good examples. A city government that is smaller than the proposed 2030 Belgian Defence, successfully incorporated ERM. The manager began with a formal programme and tailored it to the city requirements. Moreover, the committee achieved subject-matter expert participation and senior leader buy-in, while also working risk assessment, prioritisation and treatment at an executive level.

LEGO group, Danish toy company

Hans Læssøe and Mark Frigo reviewed how LEGO Group integrated SRM into their existing ERM programme. LEGO group is family-owned and consists of 12,500 employees working in facilities in Denmark, the Czech Republic, Hungary, and Mexico. They describe their risk management model as an umbrella where stovepipes feed risks into a central location named ERM, but there was no centralised review of strategic risk. After adding it as a new wedge in the umbrella, they incorporated Monte Carlo simulation and evaluation of strategic objectives against the mega trends identified by the World Economic Forum. LEGO Group aligned the risk management function at the executive level, incorporated risk into their standard meeting rhythm, gave it an executive sponsor, mandated each business section to share their risks with the other major divisions, and ensured that risk ownership remained outside the risk management division's responsibility. It is a good example of how stovepipe systems can evolve to incorporate both enterprise and SRM processes.

Mars Incorporated, American privately held, multinational company

Mars Incorporated (Mars) transitioned from a family owned and managed company to a privately-held global conglomerate. Operating globally in North America, Europe, Russia, China, and Australia, it employs approximately 72,000 people. Larry Warner[6] described how Mars began in 2002. Vendors presented two options to introduce ERM, and the leadership chose a tailored ERM framework, specifically to avoid the impression the initiative was just another risk compliance programme. Over the next four years, Warner worked with small group workshops and executive leadership to install ERM across all eighteen business units, and it was standardised across the company by 2007. Beginning with 10-15 risks, each unit is forced to narrow these down to just 3-4 risks that the risk professionals brief to the president quarterly. Furthermore, Mars tracks and trends their strategic risks, and uses colour coding to help visualise over time how risk treatments are working. The Mars journey illustrates that when building an ERM programme, it is important to gain and maintain senior leader support, under promise, and over deliver. Additionally, the drive for continual improvement enables an on-going evolution, and the risk management team and leadership should expect a living process.

Statoil, Norwegian petroleum company

Statoil, formerly a state-owned Norwegian petroleum company, has evolved into a publicly traded organisation with partial state ownership and approximately 23,000 employees. In their case study, Alviniussen and Jankensgård[7] identified lessons learned from overcoming the inherent resistance to organisational change. Statoil began in 1999 with the creation of a CFO chaired Risk Committee tasked to advise executive leaders on risk. In 2000, Statoil built a risk department, staffed with risk professionals from across the organisation, which helped to break down silo risk management and encouraged organisational-wide buy-in of the risk management process. Statoil created unique risk heat maps that consider risk twice on the same diagram (visually depicting the positive and negative outcomes of the same event). The risk department reviews all risk maps which provides a company-wide risk perspective, while also allowing members to spread risk management best practices across the organisation. Managers of each business unit report risk at quarterly meetings using their risk heat map and must describe and justify the risks they identify. Statoil identifies risk owners, and when risks potentially affect the core business, the chief executive officer (CEO) takes ownership. This potentially overly centralised control, but Statoil ensured that balanced scorecards and key performance

indicators remained separated from the management of core risks so that the performances of individual business units were not affected by the executive decision to take large risks.

British Columbia Lottery Corporation, Canadian Crown Corporation

The British Columbia Lottery Corporation (BCLC) is a state-owned gaming company that manages provincial lotteries, casinos, and online gambling. It employs about 850 corporate staff members and 37,000 employees. The former senior manager for risk advisory services in British Columbia, Jacquetta Goy, summarised[8] the provincial lottery's implementation of ERM which began in 2003 with a consultant-driven, untailored risk assessment. While the consultant generated a risk universe containing seventy risk descriptions and provided recommendations on ERM implementation, the combination of an organisational change initiative with a known end point and the lack of a tailored approach led to the initiative losing momentum and was never fully implemented. A second 2006 ERM attempt directed each vice-president to submit three strategic and operational risks. Using a voting system, the group narrowed thirty-seven risks down to nine prioritised risks to be integrated into the company's audit plan. However, the ERM programme began to stagnate in 2008 after the enterprise risk manager took the job as director of Audit Services and left the enterprise risk manager position vacant. It was not until he left the company in 2009 that the ERM programme truly spread across the organisation. By 2011, division vice-presidents solidified the bottom-up aspect by requiring their division risk owners to present division risks prior the quarterly executive meetings. The CEO incorporated strategic risk and cemented a top-down perspective in 2012 by hosting an off-site event where facilitators helped executive members to develop eleven strategic risks and identify appropriate sponsors for each risk. Corporate leaders then used the strategic risks to further develop their strategic plan.

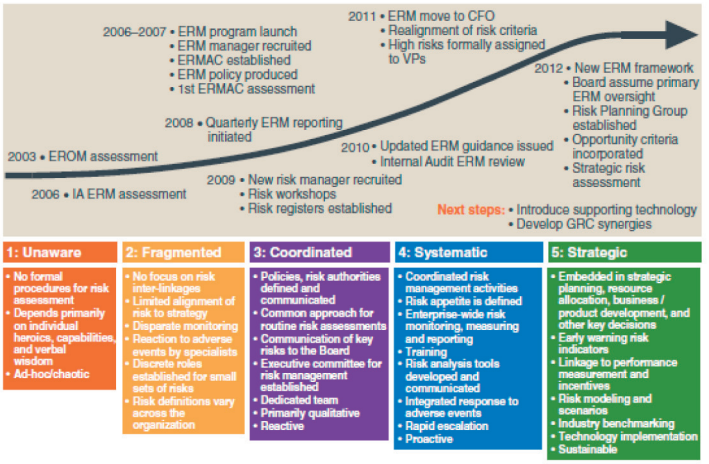

Figure 2. BCLC Path to ERM maturity.[9]

As seen in the other case studies, BCLC maintained SRM at the executive level and succeeded in evolving its risk assessment tools slowly through iterative implementation. Most notably, BCLC began with a simple 2 x 2 matrix risk heat map, and as they gained experience and confidence, they expanded it to incorporate five colour-coded categories that visualised risk appetite while simultaneously identifying the approval authority for each level of risk. Risks that fall in the low range are acceptable as such. Those that fall in the medium range are still tolerable, but a cost-benefit analysis must be conducted in order to determine if treatment is required. While risks are primarily seen as negative, the use of cost-benefit analysis allows leaders to account for potentially positive effects. As a result, managers can confidently take more and greater risks as long as the benefit is deemed worthy. Finally, risks that fall in the highest categories are deemed unacceptable and therefore must be mitigated through action to move it into an acceptable region.

Simplifying complexity

The 2010 UN study developed ten benchmarks that the authors believed were hallmarks of successful ERM programs. Furthermore, a number of consultants have created matrices to measure client ERM maturity. The concept of a maturity matrix is also found in the Belgian Defence internal control evaluation of risk management. In fact, the Chief of Defence's current internal control risk management target is a level three. It follows that the creation of a maturity

matrix to measure strategic risk management practices within Defence could provide a useful and likely acceptable tool to prioritise initiatives to develop enterprise-wide appreciation of risk.

Using available practitioner maturity matrices and the UN study, the author created a five-level maturity matrix and incorporated most attributes of successful implementation programmes. Interviews with the Defence internal control coordinator (DOS-ICS) placed Belgian Defence SRM maturity between level two and level three, and as a result, level three became the target. The five cases offered a number of lessons and best practices to leverage against, but there was little to describe how to categorise and prioritise initiatives. A SWOT analysis uncovered and helped to prioritise potential recommendations.

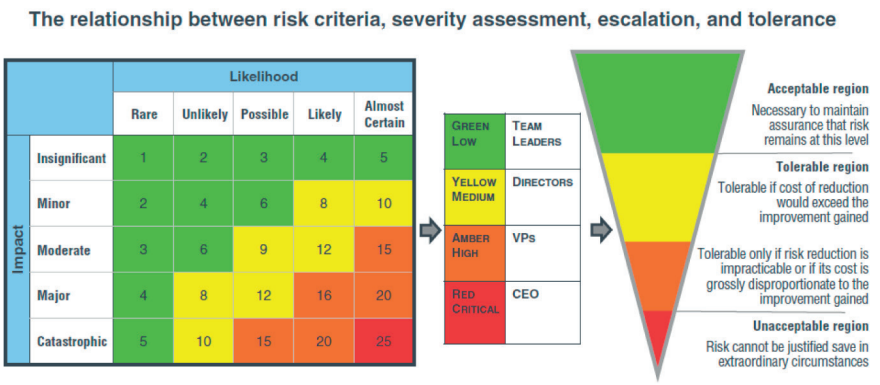

Figure 3. Implementing the ALARP approach to risk response[10].

In their 2010 paper, Marilyn Helms and Judy Nixon[11] summarised the advantages of strengths, weaknesses, opportunities and threats (SWOT) analysis. A SWOT analysis simplifies complex situations by reducing the amount of information, organising what remains into four categories, and placing it into a 2 x 2 matrix. The goal is to identify how strengths and opportunities can be used to overcome or eliminate weaknesses, while avoiding or removing threats. In other words, organisations can seek to realise opportunities, minimise threats, and reduce weaknesses in order to grow strengths. Knowing the existing strengths, weaknesses, opportunities and threats enabled the creation of recommended initiatives based on achieving maturity level three through the application of benchmarked case study best practices and lessons learned.

Looking forward – a way ahead

First, executive support of holistic risk management should be introduced in published guidance from the CHOD by updating the CHOD Guidance[12]. It should be explicitly added that Defence must consider risk across all aspects and components. Furthermore, the result of such assessment must be completed in a standardised manner that enables a holistic appreciation, across traditionally stove-piped hierarchies, of the risks to achievement of Defence strategic objectives. The Office of Internal Control (DOS-ICS) should be named as the lead office to coordinate risk management. Doing so does not require changes to organisational structure, and the standardisation of risk assessment and reporting can be done via regular internal control assessment and normal risk management courses. Moreover, standardising risk management compliments achieving internal control risk management maturity level three.

Second, Steering Committee members should introduce and conduct routine risk assessments at the Directorate level. Taking what they have learned and practiced during the executive risk assessment with the CHOD, they can apply the same techniques at routine directorate level meetings. This allows the communication of risk appetite from the executive to lower levels, and it further demonstrates senior leader support for and the importance of an enterprise view of risk. Additionally, it enables Steering Committee leaders to either delegate management of lower risks, or, if the risk is great enough to threaten directorate level objectives, they can take a more proactive role in handling the risk.

Third, when resources allow, risk reporting should be accomplished in a manner that enables true bottom-up expression of risk that is also visible across the Defence enterprise. The case studies suggest that this may involve the creation of a tool or expansion of the current CHOD "Cockpit", and, perhaps more importantly, it requires a cultural acceptance of transparency related to risk.

Finally, there are opportunities for Defence to study SRM further. The governmental organisations reviewed by the UN in 2009 and 2010 have been applying ERM for at least six years. An in-depth case study into one or more of these organisations could illuminate how Defence could further mature SRM and perhaps align management techniques across other governmental organisations. Furthermore, a number of systems owned or used by Defence that could be applied for reporting purposes likely already exist. Potentially, Defence could identify an existing compatible system to communicate risk assessments and analyses enterprise-wide. Such a system would be more cost-effective than build-

ing a unique or new system and training personnel to use it. Additionally, more research is necessary to develop commonly used key risk indicators applicable to the risks faced by Defence. These indicators could be used to better monitor high risks, thereby enabling earlier intervention if mitigation or treatments are not proceeding as desired.

Overall, SRM is the next evolution in managing risk. Defence has begun to internalise its use, but much remains in the journey towards full adoption.

Reageren? Réagir?: **BMT-RMB@mil.be**

❑

Keywords: strategic risk management (SRM) – enterprise risk management (ERM)

---

[1] The views expressed are those of the author and do not necessarily reflect the official policy or position of the United States Air Force, the United States Department of Defense, or the United States Government.

[2] Articles 1 & 5 of the royal decree of 17 October 2007, Moniteur belge, 18 October 2007, pp. 53949, 53968.

[3] Adapted from Kalia & Müller, Risk Management at Board Level: A Practical Guide for Board Members, Haupt, 2007, Bern.

[4] Cihan Terzim and Istvan Posta, Review of Enterprise Risk Management in the United Nations System, Benchworking Framework, United Nations Joint Inspection Unit Report. 2010. Geneva.

[5] John Fraser, Betty Simkins, and Kristina Narvaez, editors. Implementing Enterprise Risk Management: Case Studies and Best Practices, John Wiley & Sons, Hoboken, NJ (2015), pp. 59-73.

[6] Larry Warner, "ERM at Mars, Incorporated, ERM for Strategy and Operations.", Implementing Enterprise Risk Management: Case Studies and Best Practices. Op. cit.

[7] Alf Alviniussen and Håkan Jankensgård, "Value and Risk, Enterprise Risk Management at Statoil." in Implementing Enterprise Risk Management: Case Studies and Best Practices. Op. cit.

[8] Jacquetta Goy, "Developing Accountability in Risk Management: The British Columbia Lottery Corporation Case Study." in Implementing Enterprise Risk Management: Case Studies and Best Practices. Op. cit.

[9] Ibid.,p. 203.

[10] Ibid., p. 201.

[11] Marilyn Helms and Judy Nixon, "Exploring SWOT analysis-where are we now? A review of academic research from the last decade." Journal of strategy and management 3, no. 3 (2010). pp. 215-251.

[12] CHOD Guidance Defensie: Risico's & Uitdagingen, Government of Belgium, Brussels, 2014.


FRIENDLY +++ ECO FRIENDLY +++ ECO FRIENDLY +++ ECO FRIENDL
eco friendly