Using enterprise risk management to strengthen organisational resiliency: One institution's story

Received (in revised form): 30th April, 2023

Melanie J. Lucht

Associate Vice President for Enterprise Risk Management and Chief Risk Officer, Carnegie Mellon University, USA

Melanie Lucht *is the Associate Vice President for Enterprise Risk Management and Chief Risk Officer at Carnegie Mellon University. In this role, Melanie oversees environmental health and safety, disaster recovery, business continuity, emergency preparedness and risk operations. A risk management executive with nearly 25 years of experience, Melanie is a Master Business Continuity Professional (MBCP), a member of the Business Continuity Institute (MBCI), a Certified Insurance Counselor (CIC) and a Certified Continuity Manager (CCM), who also holds the Associate in Risk Management (ARM) designation. She serves on the Fusion Risk Management Executive Peer Exchange and the* Disaster Recovery Journal *editorial advisory board; as a coach and guest lecturer for the Carnegie Mellon University Chief Risk Officer Executive Education Program through the Heinz College; and as a board member for the New Hazlett Theater in Pittsburgh.*

Abstract

This paper discusses how Carnegie Mellon University launched a cyclical enterprise risk management framework that incorporates both emergency preparedness and response and business continuity into its purview, to deliver greater organisational resiliency. The paper goes on to describe the governance structure that defines roles and responsibilities throughout the organisation, before discussing how faculty, staff and students are engaged and educated to sense risks, and to collaborate with leadership at all levels in prioritising risks for deep-dive assessments and employing feedback loops to support continuous process improvement. As the paper will show, these cyclical practices support organisational resiliency and a greater sense of risk consciousness.

Keywords: enterprise risk management, organisational resiliency, business continuity planning, business impact analysis, three lines of defence, feedback loops, risk consciousness, risk sensing, risk assessment, risk prioritisation, risk profiles

Melanie J. Lucht

INTRODUCTION

Implementing and sustaining enterprise risk management (ERM) can feel like a complex and daunting undertaking. Those tasked with developing and implementing ERM into their organisation often have current or previous risk-based responsibilities such as audit, insurance, compliance or business continuity. While these disciplines have commonalities and may support one another, ERM can serve as an umbrella over them in a way that strengthens organisational resiliency.

Carnegie Mellon University's (CMU) ERM journey has led to strengthened organisational resiliency. Using the principles of enterprise risk management as

Carnegie Mellon University,
4615 Forbes Avenue,
Suite 123,
Pittsburgh, PA 15213,
USA

Tel: +1 412 268 5939;
E-mail: mlucht@andrew.cmu.edu

Journal of Business Continuity & Emergency Planning
Vol. 17, No. 1, pp. 61–73

1749–9216

an art rather than a science has resulted in a programme that aligns with the institution's culture, strategic mission and goals. A built-in feedback loop allows for continuous improvement and stakeholder engagement. Carnegie Mellon's route is not the only way to leverage ERM to strengthen organisational resiliency, but it demonstrates what worked for one organisation.

WHAT IS ENTERPRISE RISK MANAGEMENT?

ERM is an integrated and continuous process for managing enterprise-wide risks — including strategic, financial, operational, compliance and reputational risks — to minimise unexpected performance variance and maximise intrinsic firm value. The process empowers the board and management to make more informed risk/return decisions by addressing fundamental requirements with respect to governance, including risk appetite, risk analytics and risk management monitoring and reporting.[1] Each of theses risk areas is its own unique discipline of risk management. Some organisations have even more areas of concern, such as credit risk, market risk and cyber risk.

Each industry, whether financial, manufacturing, higher education or utility, has its own culture that sets the tone for how risks are identified, assessed, mitigated and managed.

Risks have traditionally been perceived as negative because they are either pure or speculative in nature. With pure risk, there are only two possibilities: something bad happens or nothing happens. It is unlikely that any measurable benefit will arise from a pure risk. Speculative risk has three possible outcomes: something good (gain), something bad (loss) or nothing (staying even). Gambling and investing in the stock market are examples of speculative risks.[2]

In practice, an individual or organisation more concerned with the potential downside of a risk than any benefit can either avoid or transfer the risk through insurance. However, ERM can help lift the veil off such decisions and foster collaborative discussions on acceptable levels of risk and how to make risk-informed decisions. Establishing these agreed-upon risk levels and policies does not happen overnight — it is often the result of a multiyear strategic process to enhance the maturity of an ERM programme that fits with the organisational culture and aligns to the strategic objectives of the institution.

HOW ERM CAN STRENGTHEN ORGANISATIONAL RESILIENCY

Going back to the definition of ERM, how does one 'minimise unexpected performance variance', and what might that mean to various organisations? Organisational resiliency refers to an organisation's ability to anticipate, prepare for, respond to and recover from disruptive events, whether it is a natural disaster, cyber attack, financial crisis or something else. It encompasses the capacity of an organisation to withstand and adapt to changes in the external environment to maintain operations and to continue to pursue its strategic goals and objectives.[3] Organisational resilience is not a single discipline but rather a blended consideration of the risks facing an organisation. It is both a forward and backward-looking approach to managing risk to achieve an organisation's objectives. It is about maximising opportunities and minimising likelihood and consequences by removing the silos and finding the appropriate balance of adaptive, proactive and reactive strategies.[4] Given the similarities in how ERM and organisational resiliency are defined, there are clear opportunities to leverage one to strengthen the other.

In establishing CMU's ERM framework, organisational resiliency was intentionally placed at the top, alongside risk consciousness. Risk consciousness is akin to risk awareness and creating a culture of risk-informed decision making. Culture is what weaves the business of managing risk into the everyday routines of all employees.[5] Having a high level of risk consciousness requires a culture of transparency and open communication, as well as a willingness to embrace change and adapt to new circumstances. It also requires a continuous process of learning and improvement in order to stay ahead of emerging threats.[6] When the opportunity arose to re-imagine ERM at CMU six years ago, a culture of risk-informed decision making was already blossoming from the business continuity plan (BCP) which began in 2013. The ERM reorganisation provided an opportunity to reinforce organisational resilience by leveraging the common language and risk-conscious culture established through the BCP and integrating that into the new ERM framework.

CMU'S JOURNEY STARTED WITH BUSINESS CONTINUITY

When CMU's ERM programme was restructured in 2017, a multiyear strategy to roll out a sustainable business continuity programme (BCP) to the university was about halfway complete. The central administration had plans in place that were being exercised regularly and work was well underway in academic departments to socialise the programme and begin planning efforts. Essentially, conversations around risk were happening daily.

So how did the BCP begin in 2013? As with many organisations, business continuity planning began in the central Information Technology (IT) Division, with an initial focus on disaster recovery for critical IT assets. However, leadership recognised that recovery prioritisation for disaster recovery was challenging (and full of assumptions) without having an understanding of business recovery needs and priorities. One full-time employee was dedicated to launching a sustainable BCP for the university, starting with a pilot in the Finance Division. Over a period of eight months, 14 plans were developed and exercised. In parallel, a cross-functional Disaster Recovery and Business Continuity Steering Committee was formed to help establish the mission and objectives of the BCP, as well as develop a multiyear strategy as to how the programme would expand throughout the university.

The mission of the BCP is to provide the guidance, tools and governance commensurate with the strategic mission and risk tolerance of the university and its divisional units so that they may continue to provide critical services in the event of a disaster or significant business disruption. This is one of the first things shared with constituents when business continuity training or socialisation of the BCP occurs. To take it a step further, the BCP has three objectives:

- *Partner* with business functions to execute the recurring processes and activities (the business continuity life cycle) designed to mitigate the risk associated with disruptive incidents and enable the organisation to respond and recover within recovery objectives;
- *Provide* centralised governance and oversight while enabling business ownership; and
- *Manage* guidelines and tools that provide for assessment and mitigation of business continuity risks and development of recovery and continuity strategies.

The approach toward achieving these objectives included building relationships

and active listening. Sitting down one-on-one with colleagues or in small groups to conduct business analyses provided a valuable perspective into operational risk exposures (ie cross-training, record-keeping, etc). It is even more valuable to learn what your colleagues do, how they contribute to the institution, what challenges they face and what they value. Conducting part or all of a business impact analysis (BIA) during coffee or lunch and sharing personal stories forges connections that demonstrate you are invested not only in building the programme but in learning about your colleagues and the institution you are all a part of. It also serves as another opportunity to establish a common language around risk and to build risk consciousness.

When the BIAs are completed for a department or division, the business continuity function consolidates and prioritises the data based on the criticality of recovery needs. A risk assessment is developed and compared against recovery capabilities. The sponsor is able to see where there is resiliency and where there are potential recovery gaps and can decide whether to accept a risk or implement additional remediation strategies. As an added benefit, colleagues will see ideas from their BIA conversations show up in the risk assessment.

As the BCP at CMU gained traction and more plans were being developed, the data gathered from the BIAs and their resulting risk assessments identified areas of potential enterprise risk that could be managed at a higher level in order to benefit multiple business functions (ie data integrity and governance). This provided a natural bridge to ERM's work. CMU integrated this essential risk mitigation technique (business continuity planning, which encompasses the BIA) into the re-imagined ERM framework. It was included as part of a continuous cycle, following risk treatment and mitigation and emergency preparedness and response (see Figure 1). While this may not be a traditional ERM approach, it aligned well with the culture, organisational structure and current level of risk consciousness. Colleagues knew and understood the BCP, so if they saw that a re-imagined ERM included the work they were already doing, it would be received more favourably.

LEADERSHIP SUPPORT AND GOVERNANCE

As many risk professionals know, leadership support is an important key to an effective risk and resiliency programme (in whatever shape it takes). This support may not happen right away, but as the programme matures and you demonstrate the value of ERM and how it supports organisational resiliency, momentum in gaining support will increase. This is where persistence and patience play a key role. Never assume that you cannot further your ERM programme because you do not have leadership support. That support needs to be earned, and you earn it by clearly articulating your vision of the ERM programme, outlining a strategy for achieving that vision and showing the projected outcomes. It is also critical to establish a governance structure that depicts where accountability of ERM resides, up to and including the board.

In re-imagining the ERM programme at CMU, it became clear that adopting a 'three lines of defence' approach (Figure 2) would provide an optimum way of engaging leadership, soliciting support and establishing who does what. Effective governance requires appropriate assignment of responsibilities as well as strong alignment of activities through cooperation, collaboration and communication.[7]

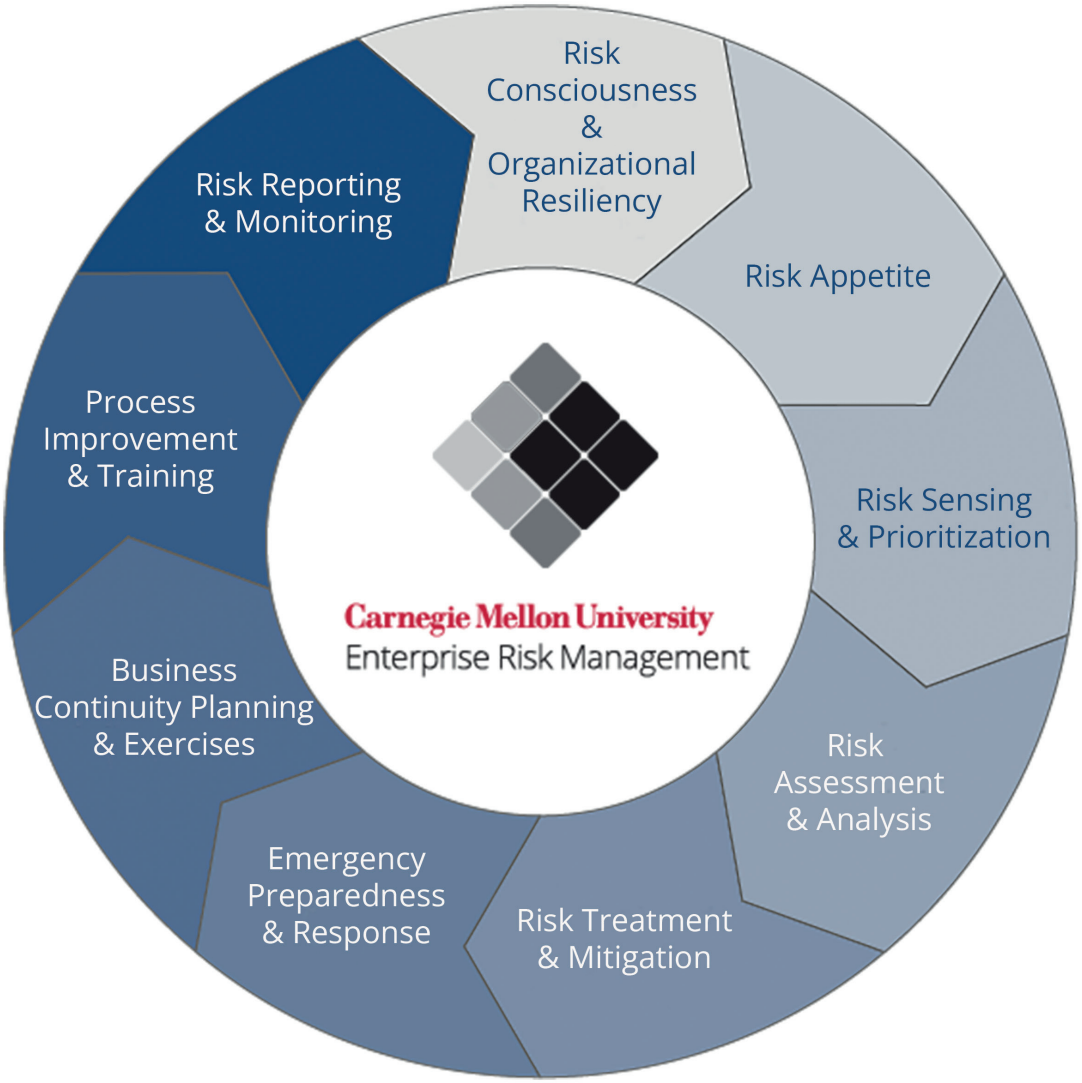

Figure 1 CMU's ERM framework

The approach to introducing this model to stakeholders was to keep it simple and straightforward.

The first line of defence *owns and manages risk*. Contrary to how risk management is perceived, risk or compliance professionals do not own individual risks and the controls that mitigate. Rather, operational management and senior leadership are responsible for ongoing activities that include:

- Owning and managing risks, including BCPs for their business function(s);
- Identifying, assessing and mitigating risks;
- Implementing corrective actions;
- Implementing and maintaining internal controls;
- Conducting evaluations of internal controls; and
- Executing risk and control procedures daily.

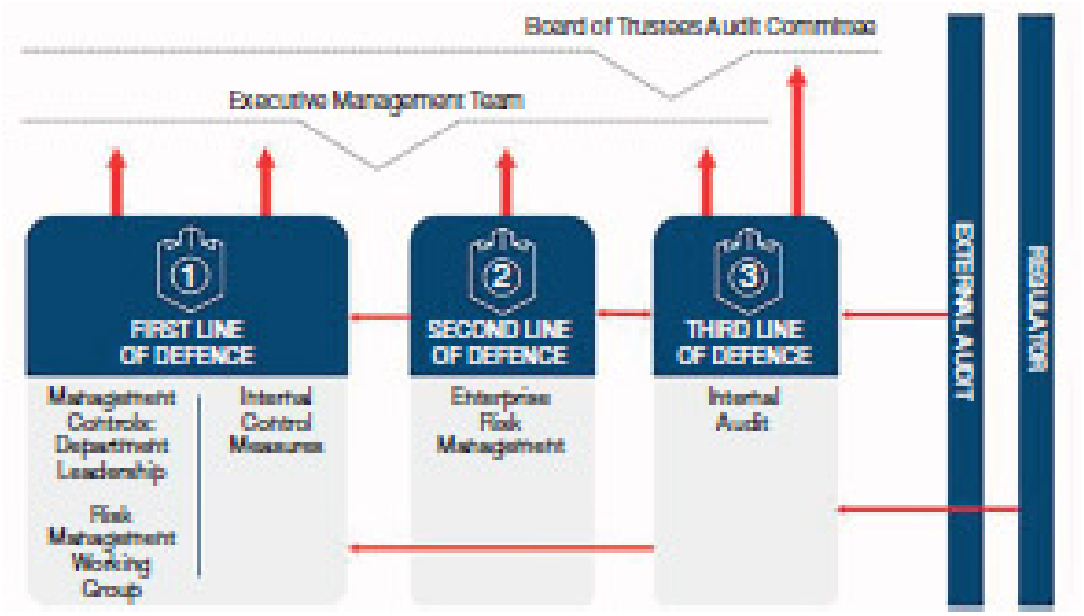

Figure 2 CMU's three lines of defence

The second line of defence *oversees risks*. At this line of defence, functions associated with risk are found, including ERM. Functions of the second line of defence include:

- Ensuring that operational management and senior leadership are implementing effective risk management practices;
- Executing the objectives of the BCP;
- Assisting risk owners with risk evaluation by taking into account the institution's risk appetite;
- Helping risk owners report risk-related information throughout the institution; and
- Providing updates on the status of risk and resiliency to executive management and the Board of Trustees Audit Committee.

The third line of defence provides independent assurance. Internal audit forms the third line of defence, and provides *assurance on the effectiveness of governance, risk management and internal controls*. It assesses the effectiveness of the first and second lines of defence in achieving risk management objectives and the effectiveness of the risk management and internal control framework.

Two characteristics of the three lines of defence that aligned to CMU culture were the development of a risk management working group in the first line and ERM residing exclusively within the second line. Other approaches to a three lines of defence model may include other disciplines such as information security, compliance, privacy, ethics, etc. However, CMU's top priority was to keep the structure as simple as possible to ensure clarity about each line's function.

The Risk Management Working Group was established shortly after ERM launched its new organisational structure in 2017, evolving from the Disaster Recovery and Business Continuity Steering Committee mentioned earlier. Given the synergies between disaster recovery/business continuity and ERM, it did not make sense to establish another

committee that would burden colleagues already wearing multiple hats. Other institutions have versions of CMU's Risk Management Working Group, such as a risk committee. However, it was intentionally called a working group to live up to how the first line of defence was defined.

The Risk Management Working Group, as shown in Figure 3, is composed of a cross-functional representation of administrative and academic campus leaders who provide strategic direction and insight to achieve the following goals:

- Apply their lens of expertise to an identified risk to assess if the risk is actual or perceived;
- Validate the likelihood and impact a risk could impart upon the university;
- Prioritise risks based on alignment with strategic priorities;
- Identify gaps between risks that are actively being mitigated and controlled and those that may not be;
- Represent their vice president/provost and risk owner as managers/custodians of risks that apply to their domain area;

Figure 3 CMU'S risk management working group

- Aid in the development and communication of plans or actions to mitigate the actualised risk and present the risk owner with recommendations of risk tolerance vs further risk mitigation techniques;
- Assist in the monitoring and tracking of risks within their domain area and recalibrate as needed;
- Increase the university's adoption of a risk-conscious culture, including how risks are identified and managed; and
- Oversee the strategic direction of the BCP.

This chartered group meets every quarter and, over time, has got into a rhythm of executing the ERM Framework on an annual basis. This starts with risk sensing, which includes identifying and prioritising which areas of risk should be assessed.

ANTICIPATE RISKS AND OPPORTUNITIES THROUGH RISK SENSING

Risk sensing employs human insights and advanced analytics capabilities to identify, analyse and monitor emerging risks to the organisation's business model, long-term viability and ability to create value.[8] Flaws with human insights include not sharing information due to silos and not knowing how to share it, lack of comfort with sharing information for fear of retaliation, or not sharing information in a misguided attempt to gain a strategic advantage over colleagues.

While CMU is not yet in a state of maturity to employ advanced analytics that identify and analyse risk, the Risk Management Working Group was intentionally designed to reduce silos and facilitate open discussion of areas of risk and opportunity in a collaborative environment. This group of leaders and subject matter experts also includes representation from the student community, which provides excellent insight into opportunities to ensure student safety, security and overall wellbeing.

So how does CMU do this? Each spring (May), the Risk Management Working Group convenes to kick off risk sensing. A 90-minute open discussion captures areas of risk or opportunity not previously assessed by ERM. This list is used to facilitate one-on-one discussions with each member of university executive leadership, both administrative (Vice Presidents) and academic (Provost, Vice Provosts, Deans). Conducted throughout the summer (July and August), these conversations parse out what resonates among the already-assessed areas of risk and opportunity, new areas identified by the Risk Management Working Group, and any other risks and opportunities not yet identified. These meetings generate a more extensive list of risks and opportunities that goes back to the Risk Management Working Group for review and prioritisation (August).

CMU's ERM programme intentionally prioritises five areas of risk (not previously assessed) for a deep dive assessment in the following calendar year. This effort focuses on areas of risk and opportunity that resonate strongly with constituents due to their relevance to the university or to higher education. They could be areas of risk and opportunity present within our organisational culture or risks and opportunities that are emerging within higher education and society at large.

Following active and open discussions within the Risk Management Working Group, each member independently votes for their top five risks and opportunities. ERM compiles the votes and shares results with the Risk Management Working Group for further comment.

Once the top five areas of risk and opportunity are selected, they are shared

with executive leadership (October to January) to affirm that these are the right priorities for ERM's time and resources. This also gives executive leadership the chance to weigh in on what aspects of the selected areas would be valuable to assess. Once affirmed by executive leadership, these five prioritised areas of risk and opportunity are shared with the Board of Trustees Audit Committee for affirmation (February). Finally, kickoff meetings are scheduled with the appropriate risk owners and their identified subject matter experts to begin the risk assessment (March/April).

This cycle of risk sensing occurs while other areas of risk and opportunity are going through initial assessment and those previously assessed are going through reassessment to ensure that ERM is capturing the most up-to-date and relevant information. This cycle of ongoing sensing, discussion, prioritisation and assessment strengthens organisational resiliency in several ways. First, it raises the level of risk consciousness throughout the organisation and fosters thoughtful and engaging conversations. These conversations bring together people who share different perspectives, subject matter expertise, institutional knowledge and personal experience. Secondly, it helps to reduce the noise associated with conducting surveys that can elicit risks that are not at an enterprise level and grievances that do not add value to the conversation. Thirdly, it provides a sense of inclusion as leaders with different subject matter expertise can highlight potential risks and opportunities that others may not be aware of and bring in perspectives not previously considered.

This approach toward risk sensing removes the silos and makes ERM relevant from the executive level to the community level. It gives all constituents a voice and reinforces that everyone is a risk manager.

CONDUCTING ERM ASSESSMENTS LIKE A BUSINESS IMPACT ANALYSIS

In redesigning the ERM programme six years ago, there was an opportunity to leverage existing processes to support the ERM assessment process. The goal was to make the ERM process simple, collaborative and insightful, and to avoid the potential fatigue from exposure to similar processes with seemingly siloed sources. The BIA techniques used to launch the BCP in 2013 offered a roadmap for the ERM assessment. A risk assessment and a BIA are both risk-based assessments, but they have different purposes: BIAs deal with what is impacted, while risk assessments examine how impacts occur.[9] For example, a BIA will identify dependencies (facility needs, technology needs, vendor needs, etc), recovery time objectives and workarounds in the absence of those dependencies. A risk assessment identifies the external threats and internal vulnerabilities that dependencies are exposed to, consequences if those risks are realised and mitigation strategies to reduce the impact. While the output might be slightly different, the format and process to collect the information that manufactures that output are similar.

The interview approach used to conduct the BIA at CMU has served as an excellent opportunity to build relationships, enable bidirectional learning and establish the foundation of a business continuity plan. While it takes a bit more time, the payback cannot be overstated. Why could not this same approach be used to conduct an ERM assessment? During a BIA interview, a spreadsheet is used to capture information from the interviewee. This is intentional so the person being interviewed is not distracted by filling out a form or inputting data. They are simply sharing their story about what they do, what they depend upon to deliver their services, how they do it, and what would

be impacted in the event of a disruption. The BIA captures service delivery information, location, technology, people and third-party dependencies, specialised equipment, critical process periods and recovery needs. The ERM assessment captures threats, vulnerabilities and mitigations (existing and future) and maps connections to residual risks, the institution's strategic goals and the likelihood, impact and trend of risks and opportunities.

One difference between an ERM assessment and a BIA is the number of people that could be involved. Because an ERM assessment is done at an enterprise level, there could be one or several groups of subject matter experts weighing in. To keep the process streamlined, the ERM assessment is broken into two sections: qualitative and quantitative. The qualitative section focuses on discussions (60 minutes at a time) of the various threats, vulnerabilities, mitigations, etc, that make the risk what it is. The quantitative section begins with a training session about how likelihood, impact and trend are defined and used in the assessment. As shown in Figure 4, participants then evaluate each risk using a manageable set of choices: rating likelihood and impact as low, moderate, or high and trend as worse, stable or better.

RISK PROFILES AND THE INEFFECTIVENESS OF HEAT MAPS

A critical risk today might be old news tomorrow. For this reason, heat maps — which illustrate just a moment in time — are not always effective due to limitations in providing detail, context, reliability, actionability and accuracy. A more comprehensive approach to enterprise risk assessment, mitigation strategies and risk treatment plans can add more value to ERM and to organisational resiliency.

In the early days of CMU's ERM programme, stakeholders received a detailed management and monitoring report after an assessment. It became clear that most stakeholders focused only on the headlines (eg is it a high, moderate or low area of risk, and how is it trending). Through feedback loops and continuous process improvement, the report evolved into a two-page PowerPoint risk profile that highlights every aspect of the risk as well

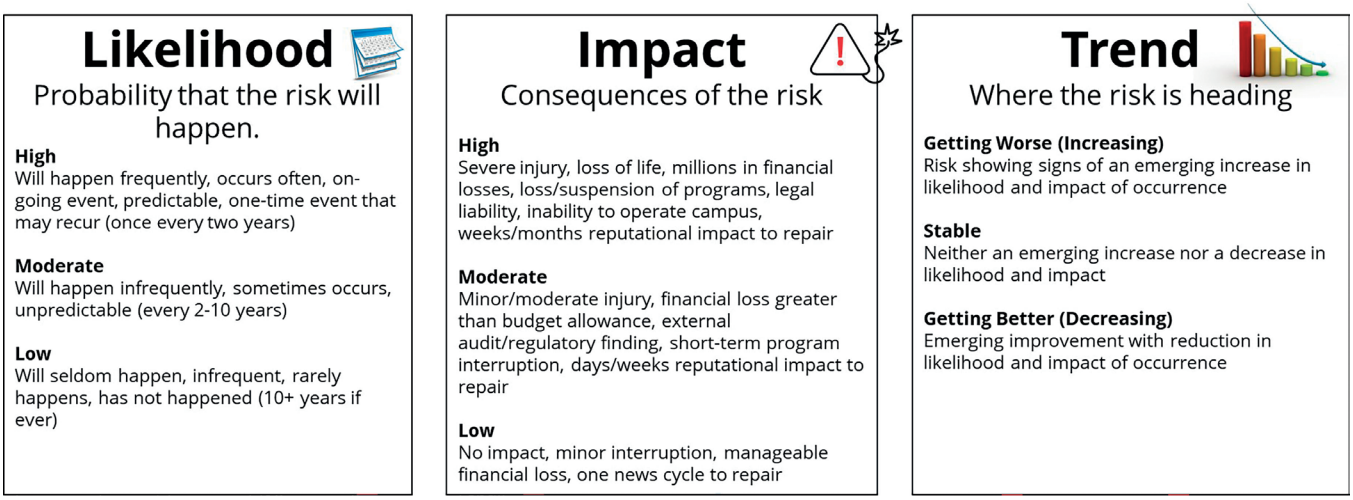

Figure 4 Likelihood, impact and trend

as the opportunity. The report includes the likelihood, impact and trend of the risk, a hypothesis about why the risk is rated as it is, and a summary of the risk treatment plan. These risk profiles provide a straightforward but comprehensive tool to facilitate discussions with ERM stakeholders on how their areas of risk are being managed and what emerging risks or opportunities need to be addressed.

SCENARIO ANALYSES CAN BE YOUR BUSINESS CONTINUITY EXERCISES

One technique used to test the effectiveness of an ERM programme is scenario analysis. Specific risks or risk scenarios are evaluated to understand potential consequences and develop continuity plans to manage them.[10] For example, a specific scenario outlining a ransomware attack on a critical IT service could be used to conduct a tabletop exercise with business continuity stakeholders to evaluate the impact of losing access to that service and how well their BCPs address their response, recovery and communication procedures. For business continuity professionals, this may seem like an obvious approach, but in larger organisations with silos, scenario analyses used for operational risk management purposes are not typically leveraged for business continuity exercises, and vice versa.

Using scenario analysis to exercise a BCP can identify lessons learned and potential gaps. That information can be used to strengthen both the BCP and overall organisational resiliency.

THE VALUE OF FEEDBACK LOOPS

CMU's ERM programme has evolved as it became clear what does and does not work. This is due in large part to the use of feedback loops. A feedback loop is a closed-loop system in which information is collected, analysed and used to make improvements. Feedback loops are used to monitor and evaluate the effectiveness of the ERM process. Data collected on the results of risk assessments, control testing and other activities can be analysed to identify areas for process improvement. Feedback loops can be used to review and improve the ERM process itself, ensuring it remains relevant and effective. Feedback loops can also be used to engage stakeholders to provide feedback on the ERM process.[11] ERM, business continuity and improved organisational resiliency cannot be accomplished in a vacuum. They require stakeholder and leadership support, along with engagement and feedback to ensure that a programme designed to strengthen organisational resiliency is tailored to the culture of the organisation.

IF YOU'VE SEEN ONE ERM PROGRAMME, YOU'VE SEEN ONE ERM PROGRAMME

Every organisation has its own culture. A combination of historical, leadership, demographic, geographic and value-based factors shape that culture. As a result, organisations differ in their approach to ERM based on stakeholder expectations and different risks, priorities and approaches to risk assessment and mitigation.

For example, look at an institute of higher education (IHE) and a financial services institution. IHEs operate like small (and sometimes large) cities. IHEs may prioritise risks associated with safety, compliance, student wellbeing and reputation, while financial institutions may prioritise risks related to financial stability, protecting customer information and satisfying regulatory requirements. They may have different approaches to how risks are assessed and mitigated. IHEs may prioritise qualitative assessments that focus on understanding the impact of risks, while

financial institutions may use quantitative assessments that focus on the financial impact of risks. There are also different stakeholder expectations. IHEs answer to students and their families, faculty and the public. Financial institutions answer to regulators and customers.

Even within IHEs, there are different approaches toward strengthening organisational resiliency through ERM. Some depend on whether the IHE is public or private, large or small. CMU invited chief risk officers from six top-tier peer institutions to conduct a peer review of its ERM programme in January 2019. The goal was to assess organisational structure and resource allocation, strategic approach and planning, risk management methodologies and processes, technology and vendor capabilities, programme strengths and weaknesses, and leadership and campus support/partnerships. At the time of the review, CMU was early in its ERM maturity, working to re-imagine an unsuccessful programme that used operational risk-based approaches from different reporting structures.

The peer group concluded that the ERM programme was on an appropriate trajectory to achieve the status desired by key stakeholders and noted no obvious weaknesses or deficiencies in the programme design or execution. They did offer recommendations for continuous improvement, including but not limited to empowering risk owners and custodians to lead their own risk assessments, continuing to simplify risk criteria and methodology to expand participation, and working to align risk and internal controls with internal audit and compliance. These recommendations were a significant feedback loop that provided a blueprint for strategic programme maturity.

The review also demonstrated that no two institutions approach ERM in the same way. As evidenced by an organisational benchmarking exercise with the peer-review team, CMU aligned in organisational and reporting structure with only one other institution. At that institution (letter E in Figure 5) and at CMU, ERM oversees both environmental health and safety and business continuity.

					Companion Functions (organizationally co-located)					
Institution	Title	Reporting To	Board Oversight Committee	FTEs (approx.)	Counsel	Internal Audit	Compliance	Insurance	EH&S	Business Continuity
Carnegie Mellon	AVP and Chief Risk Officer	VP for Operations	Audit	1.00	✗	✗	✗	✗	✓	✓
A	Chief Audit, Risk & Compliance Officer	President	Executive	0.75	✗	✓	✓	✗	✗	✗
B	Chief Risk Officer	Executive Vice President	Audit & Compiance	0.66	✗	✗	✗	✓	✗	✗
C	Associate Director, Risk & Compliance Services	Chief Audit Executive	Audit	1.25	✗	✓	✗	✓	✗	✗
D	Institute Risk Officer	Chief Counsel	Risk and Audit	2.00	✓	✗	✗	✗	✗	✗
E	Senior AVP, Chief Risk & Compliance Officer	Executive Vice President	Audit, Risk & Compliance	0.33	✗	✓	✓	✓	✓	✓
F	University Risk Officer	Chief Financial Officer	Audit & Risk	0.50	✗	✗	✗	✓	✗	✗

Figure 5 ERM peer benchmarking analysis

While there are contrasts with how IHEs approach ERM and its reporting structure, risk professionals at these and other top-tier institutions continue to share a strong and communicative network for benchmarking, sharing best practices and identifying continuous improvement opportunities.

CONCLUSION

Implementing and sustaining ERM can feel like a complex and daunting undertaking, but those tasked with the job have a unique opportunity to leverage current or previous risk-based responsibilities such as audit, insurance, compliance or business continuity to support and strengthen organisational resiliency. Identifying and capitalising on existing methodologies (eg BIA, scenario analyses) has the potential to reduce fatigue for stakeholder groups and strengthen the value of those methodologies. While no two ERM programmes are the same, benchmarking against peers can help to gauge organisational structure, resource allocation and risk management methodologies. As evidenced by the CMU journey, applying these principles along with appreciating the value of feedback loops allows for continuous improvement. Carnegie Mellon's route is not the only way to use ERM to strengthen organisational resiliency, but it demonstrates what worked for one organisation.

References

(1) Lam, J. (2017) *Implementing Enterprise Risk Management*, John Wiley & Sons, Hoboken, NJ.

(2) Boggs, C. J. (2008) 'Pure vs speculative risk', available at: https://www.mynewmarkets.com/articles/92443/pure-vs-speculative-risk (accessed 25th January 2023).

(3) Tichansky, H. (2022) 'What is organizational resilience?', available at: https://aravo.com/blog/what-is-organizational-resilience/ (accessed 9th February, 2023).

(4) Leflar, J. J. and Siegel, M. H. (2013) *Organizational Resilience: Managing the Risks of Disruptive Events — A Practitioner's Guide*, CRC Press, Boca Raton, FL.

(5) Dunkin, R. (2020) '7 steps to create a risk-aware culture', available at: https://www.treasuryandrisk.com/2020/09/21/7-steps-to-create-a-risk-aware-culture/?slreturn=20230030135437 (accessed 30th January, 2023).

(6) *Ibid*.

(7) Institute of Internal Auditors (2020) 'The IIA's three lines model: An update of the three lines of defense', available at: https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf (accessed 3rd February, 2023).

(8) Deloitte Touche Tohmatsu Limited (2015) 'Risk sensing: The (evolving) state of the art', available at: https://nacm.org/pdfs/surveyResults/us-risk-sensing.pdf (accessed 3rd February, 2023).

(9) Long, R. (2022) 'BIA and risk assessment: Why both are important', available at: https://www.mha-it.com/2017/03/14/bia-and-risk-assesment/ (accessed 3rd February, 2023).

(10) Ali, R. (2020) 'Scenario analysis explained', available at: https://www.netsuite.com/portal/resource/articles/financial-management/scenario-analysis.shtml (accessed 9th February, 2023).

(11) Lam, ref. 1 above.